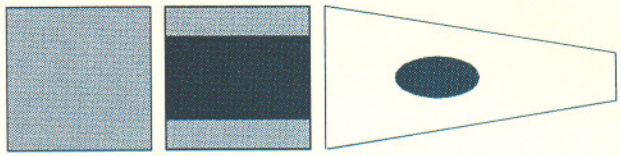


QD1 – Moje maszyny pracują naprzód.

SPIS TREŚCI

NUMERU 3(274)

W następnym numerze:

Pozytony

Okładkę i ilustracje wykonał
Krzysztof BIESAGA

Wybór artykułów z *Delty* ukazuje się w języku angielskim w sieci Internet pod adresem
http://sunsite.icm.edu.pl/~delta/

Wydawca:
Uniwersytet Warszawski

„Delta" – matematyczno-fizyczno-astronomiczny miesięcznik popularny Polskiego Towarzystwa Matematycznego, Polskiego Towarzystwa Fizycznego i Polskiego Towarzystwa Astronomicznego,
wydawany przy poparciu Ministerstwa Edukacji Narodowej.
Wydanie publikacji dofinansowane przez Komitet Badań Naukowych.

Adres Redakcji:
ul. Smyczkowa 5/7, 02-678 Warszawa
tel. 43-02-41(-2) wewn. 21
PAWELST@MIMUW.EDU.PL
Wydrukowano w Drukarni Naukowo-Technicznej w Warszawie, ul. Mińska 65
Skład systemem TEX wykonała Redakcja.

Szyfry z publicznym kluczem

Wojciech GUZICKI

W poprzednim artykule (*Delta* 1/1997) poznaliśmy przykłady tzw. szyfrów klasycznych. Popatrzmy jeszcze raz, na czym polega szyfrowanie za pomocą takich szyfrów. Przede wszystkim dzielimy tekst, który chcemy zaszyfrować, na tzw. jednostki tekstu. W naszych przykładach były to pojedyncze litery, ale można też używać par, trójek, czwórek liter itd. Każdą jednostkę tekstu zastępowaliśmy inną jednostką tekstu i z nich składaliśmy tekst zaszyfrowany. Na przykład, w klasycznym szyfrze Cezara jednostkę tekstu A zastępowaliśmy jednostką tekstu D, a jednostkę K – jednostką N.

Spróbujmy teraz sformalizować pojęcie systemu kryptograficznego. Niech $\mathcal{P}$ będzie zbiorem wszystkich jednostek tekstu używanych w tekstach jawnych, a $\mathcal{C}$ zbiorem wszystkich jednostek tekstu używanych w tekstach zaszyfrowanych (te dwa zbiory mogą być równe, jak w dotychczasowych przykładach, a mogą też być różne). Niech $\mathcal{E}$ będzie zbiorem kluczy szyfrowania i $\mathcal{D}$ zbiorem kluczy rozszyfrowywania. Szyfrowanie polega wtedy na obliczaniu wartości pewnej funkcji $f : \mathcal{P} \times \mathcal{E} \to \mathcal{C}$, a rozszyfrowywanie – na obliczaniu wartości funkcji w pewnym sensie odwrotnej $g : \mathcal{C} \times \mathcal{D} \to \mathcal{P}$. Jeżeli mamy dany pewien klucz szyfrowania $e \in \mathcal{E}$ i odpowiadający mu klucz rozszyfrowywania $d \in \mathcal{D}$, to jednostkę tekstu jawnego P szyfrujemy jako $f(P, e)$, a jednostkę tekstu zaszyfrowanego C rozszyfrowujemy jako $g(C, d)$. Oczywiście, dla każdej jednostki tekstu P musi zachodzić równość

$$g(f(P, e), d) = P\,.$$

Klasyczne systemy szyfrowania to takie systemy, w których klucze e i d albo są identyczne, albo jeden z nich można łatwo otrzymać z drugiego. Co to znaczy, że jeden z tych kluczy można łatwo otrzymać z drugiego? Otóż znaczy to, że istnieje szybko działający algorytm, za pomocą którego możemy wyznaczyć klucz d, jeśli znamy klucz e. Na przykład, jeśli kluczem szyfrowania była pewna permutacja liter alfabetu łacińskiego, to klucz rozszyfrowywania wyznaczamy szybko, znajdując permutację odwrotną. Szyfry z publicznym kluczem to takie szyfry, dla których nie znamy żadnego szybko działającego algorytmu, za pomocą którego moglibyśmy znaleźć klucz rozszyfrowywania, jeśli znamy klucz szyfrowania.

Zobaczymy teraz przykład takiego szyfru. Ten system kryptograficzny, opracowany w 1978 roku przez trzech matematyków (R.L. Rivesta, A. Shamira i L.M. Adlemana) i nazywany w skrócie (od nazwisk autorów) szyfrem RSA, jest dziś jednym z najbardziej popularnych szyfrów z publicznym kluczem. Główny pomysł tego szyfru polega na tym, że wybieramy dużą liczbę złożoną n, której rozkład na czynniki pierwsze znamy; dużą na tyle, by nikt inny nie umiał rozłożyć jej na czynniki. Okazuje się bowiem, że dotychczas nie znamy żadnego szybko działającego algorytmu, za pomocą którego moglibyśmy rozkładać na czynniki liczby mające nieco ponad 100 cyfr (w systemie dziesiętnym). Klucz szyfrowania możemy dobrać prawie dowolnie. Jednak aby z tego klucza szyfrowania otrzymać klucz rozszyfrowywania, potrzebna jest znajomość czynników pierwszych liczby n. My te czynniki znamy i dlatego umiemy szybko ten klucz znaleźć. Nikt inny tych czynników nie zna, więc nie potrafi znaleźć klucza rozszyfrowywania. Klucz szyfrowania może więc być podany do wiadomości wszystkim, a tylko my będziemy znali klucz rozszyfrowywania. Przyjrzyjmy się teraz temu systemowi dokładniej.

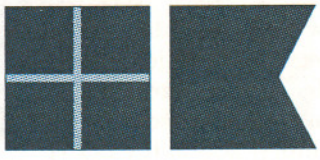
Jednostki tekstu kodujemy za pomocą liczb naturalnych. Każdej literze przypiszemy ciąg dwóch cyfr: A = 01, B = 02, ..., Z = 26. Przyjmijmy na początek, że jednostkami tekstu będą pary liter. Parę WG kodujemy za pomocą czterech cyfr: 2307. Parę AB kodujemy za pomocą cyfr 0102, czyli po prostu za pomocą liczby 102. W ten sposób każda jednostka tekstu zostanie zakodowana za pomocą liczby trzycyfrowej lub czterocyfrowej. Następnie wybieramy dwie liczby pierwsze p i q i mnożymy je: $n = p \cdot q$. Liczby p i q dobieramy w taki

Oto przykład, w którym jednostkami tekstu są pary liter. Nie rozróżniamy liter I oraz J; zawsze piszemy I. Litery takiego uproszczonego alfabetu zapisujemy w dowolnej kolejności w tabelce o pięciu wierszach i pięciu kolumnach:

R V M H Y
F A S U Q
P Z D N K
T G L B C
E I O W X

Pary liter szyfrujemy następująco: jeśli obie znajdują się w jednym wierszu, jak np. FU, to zamiast każdej bierzemy następną literę z tego samego wiersza. Zamiast FU weźmiemy więc AQ. Oczywiście, zamiast ostatniej litery bierzemy pierwszą. Jeśli obie znajdują się w tej samej kolumnie, to bierzemy następne litery z tej samej kolumny: zamiast DO – LM. Wreszcie, jeśli obie litery znajdują się w różnych wierszach i różnych kolumnach, np. FB, to zamiast pierwszej litery F bierzemy literę z tego wiersza co F i z tej kolumny co B, a więc U, a zamiast drugiej litery B bierzemy literę z tego wiersza co B i tej kolumny co F, czyli T. Parę FB szyfrujemy więc jako UT. Ten system szyfrowania nazywany jest szyfrem Playfaira.

Korzystając z tablic częstości występowania par liter również taki szyfr można złamać metodami statystycznymi.



RB – Wlokę moją kotwicę.

Rozwiązanie zadania F 448. Na rakietę spadającą swobodnie w tunelu działa siła

$$F = \frac{mgr}{R}$$

(m jest masą rakiety, a r odległością od środka Ziemi), a jej energia potencjalna wynosi

$$E_p = \frac{mgr^2}{2R}.$$

Korzystając z zasady zachowania energii

$$\frac{1}{2}mgR = \frac{1}{2}mv_0^2$$

wyznaczamy prędkość rakiety w środku Ziemi. Otrzymujemy

$$v_0 = \sqrt{gR}$$

(jest ona równa pierwszej prędkości kosmicznej).

Niech Δv będzie przyrostem prędkości, jakiego musi doznać rakieta mijając środek Ziemi, aby na jej powierzchni uzyskała wartość v_{II}. Z zasady zachowania energii

$$\frac{1}{2}m(v_0 + \Delta v)^2 = \frac{1}{2}mv_{II}^2 + \frac{1}{2}mgR$$

otrzymujemy

$$\Delta v = \frac{\sqrt{3}-1}{\sqrt{2}}v_{II} \approx 5{,}8 \text{ km/s}.$$

Żeby zrozumieć ten wynik, zauważmy, że dla rakiety startującej z powierzchni Ziemi, zgodnie z zasadą zachowania pędu, część energii wytworzonej w silniku zostanie zużyta na nadanie energii kinetycznej gazom wypływającym z dysz silnika.

Jeśli jednak rakieta ma pewną prędkość, to energia przekazywana gazom jest mniejsza. Na przykład, gdyby prędkość wypływu gazów względem rakiety była równa prędkości rakiety względem Ziemi, to prędkość gazów względem Ziemi byłaby równa zeru, czyli cała energia wytworzona w silniku zostałaby przekazana rakiecie. Zadanie to pokazuje, że pole grawitacyjne można wykorzystać w nawigacji międzyplanetarnej, co rzeczywiście czyni się wykorzystując pole grawitacyjne ciężkich planet (Jowisz, Saturn) w misjach sond takich, jak Voyager.

sposób, by wszystkie jednostki tekstu były kodowane liczbami mniejszymi niż n. Na przykład, możemy wziąć $p = 109$ i $q = 137$. Wtedy liczba $n = 14933$ jest większa od największego możliwego kodu pary liter: dla pary ZZ tym kodem jest liczba 2626.

Liczby p i q trzymamy w tajemnicy, natomiast ujawniamy wszystkim liczbę n. Oczywiście, jeśli liczby p i q są małe, to liczbę n bez trudu możemy rozłożyć na czynniki. Nawet korzystając tylko z niewielkiego kalkulatora, zrobiłby to Czytelnik w podanym wyżej przypadku nie dłużej niż w parę minut. Jednak w poważnych zastosowaniach wybieramy znacznie większe liczby pierwsze, np. stucyfrowe. Rozłożenie liczby n na czynniki jest wtedy praktycznie niemożliwe.

Teraz znajdujemy klucze: szyfrowania i rozszyfrowywania. W tym celu obliczamy najpierw wartość tzw. funkcji Eulera $\varphi(n)$ dla liczby n. Liczba $\varphi(n)$ jest liczbą tych liczb dodatnich i nie większych od n, które są względnie pierwsze z liczbą n, tzn. nie mają wspólnych z n dzielników większych od 1. Nietrudno stwierdzić, że jeśli liczba n jest iloczynem dwóch liczb pierwszych p i q, to $\varphi(n) = (p-1)\cdot(q-1)$. Ponieważ znamy liczby p i q, to możemy łatwo obliczyć $\varphi(n)$. Zauważmy jednak, że nikt inny nie będzie umiał tego zrobić. Nie znamy bowiem dotychczas właściwie żadnej innej metody obliczania $\varphi(n)$.

Następnie wybieramy jakąkolwiek liczbę e względnie pierwszą z $\varphi(n)$. O tym, czy dwie liczby są względnie pierwsze, możemy przekonać się łatwo (i szybko) za pomocą algorytmu Euklidesa. W naszym przykładzie mamy $\varphi(n) = 14688$ i jako liczbę e możemy wziąć np. 13. Łatwo sprawdzić, że 13 nie jest dzielnikiem liczby 14688. Ponieważ 13 to liczba pierwsza, więc jest też względnie pierwsza z liczbą 14688. Liczba e będzie wraz z liczbą n kluczem szyfrowania. Wreszcie musimy znaleźć odpowiadający temu kluczowi klucz rozszyfrowywania. Korzystamy w tym celu z następującego prostego twierdzenia:

Twierdzenie. Jeśli liczby a i m są względnie pierwsze, to istnieje taka liczba b, że $ab \equiv 1 \pmod{m}$.

Uwaga: Przypominamy, że $x \equiv y \pmod{m}$ wtedy i tylko wtedy, gdy m dzieli $x - y$.

Szkic dowodu. Korzystając z algorytmu Euklidesa znajdujemy takie liczby b i c, że $ab + mc = 1$. Wtedy $ab \equiv 1 \pmod{m}$.

Kluczem rozszyfrowywania będzie liczba d, dla której zachodzi kongruencja $ed \equiv 1 \pmod{\varphi(n)}$. Zauważmy, że jeśli znamy klucz e i chcemy poznać klucz d, to najpierw powinniśmy obliczyć $\varphi(n)$, a dopiero potem zastosować algorytm Euklidesa. Nie znamy przy tym właściwie żadnej innej metody znajdowania klucza d. Tak więc, jeśli będziemy trzymać w tajemnicy obie liczby pierwsze p i q, to nikt inny nie będzie mógł obliczyć $\varphi(n)$ i tym samym nie będzie mógł znaleźć klucza d.

Mamy już oba klucze e i d. Trzeba tylko pokazać, w jaki sposób ich używamy. Przypuśćmy więc, że jakąś jednostkę tekstu zakodowaliśmy za pomocą pewnej liczby a mniejszej niż n. Definiujemy

$$f(P,e) = (P^e \bmod n) \qquad \text{oraz} \qquad g(C,d) = (C^d \bmod n).$$

Zarówno dziedziną, jak i przeciwdziedziną obu tych funkcji jest zbiór liczb naturalnych mniejszych od n. Każda jednostka tekstu jawnego ma kod należący do tego zbioru, więc może być zaszyfrowana. Po zaszyfrowaniu otrzymamy liczbę mniejszą od n, możemy więc ją rozszyfrować za pomocą funkcji g. Czy otrzymamy z powrotem tę samą jednostkę tekstu jawnego? Okazuje się, że tak i wynika to dość łatwo z następującego twierdzenia Eulera:

Twierdzenie. Jeśli liczby a i m są względnie pierwsze, to $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Nietrudny dowód tego twierdzenia można znaleźć w każdym podręczniku elementarnej teorii liczb. Niech teraz P będzie kodem dowolnej jednostki tekstu. Załóżmy przy tym, że liczby P i n są względnie pierwsze.
To założenie nie ogranicza w istotny sposób zakresu stosowalności szyfru RSA. Prawdopodobieństwo znalezienia jednostki tekstu, której kod byłby liczbą podzielną przez p lub przez q, jest tak małe, że można się tym nie przejmować.

W naszym przykładzie kluczem szyfrowania była liczba 13. Zastosowanie algorytmu Euklidesa daje nam klucz rozszyfrowywania: $d = 7909$. Jednostkę tekstu o kodzie 2307 szyfrujemy podnosząc liczbę 2307 do potęgi 3 modulo 14933. Nietrudno przekonać się za pomocą krótkiego programu komputerowego, że otrzymamy wynik 11596. Aby go rozszyfrować, musimy podnieść liczbę 11596 do potęgi 7909 modulo 14933. Za pomocą tego samego programu komputerowego przekonamy się, że ta potęga jest równa 2307.

Rozwiązanie zadania F 447. Niech x_1 i x_2 oznaczają położenia przednich zderzaków każdego z samochodów, natomiast v_1 i v_2 prędkości obu samochodów. Ruch pierwszego samochodu opisują równania

$$v_1 = at\,,$$
$$x_1 = \frac{1}{2}at^2\,.$$

Drugi samochód startuje z położenia $x_2 = -l$. Jego prędkość jest związana z położeniami obu samochodów zależnością

$$v_2 = \frac{\mathrm{d}x_2}{\mathrm{d}t} = k(x_1 - x_2 - l)\,,$$

gdzie $k = \text{const}$. Niech $f = (x_2 + l)\mathrm{e}^{kt}$. Funkcja ta spełnia równanie

$$\frac{\mathrm{d}f}{\mathrm{d}t} = \frac{1}{2}kat^2\mathrm{e}^{kt}\,.$$

Całkując je i korzystając z warunków początkowych otrzymujemy

$$x_2 = \frac{1}{2}at^2 - \frac{at}{k} + \frac{a}{k^2}\left(1 - \mathrm{e}^{-kt}\right) - l\,.$$

Z tego, że $ed \equiv 1 \pmod{\varphi(n)}$, wynika, iż istnieje taka liczba naturalna k, że $ed = k \cdot \varphi(n) + 1$. Mamy wtedy na mocy twierdzenia Eulera

$$g(f(P,e),d) \equiv f(P,e)^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{k\varphi(n)+1} \equiv$$
$$\equiv \left(P^{\varphi(n)}\right)^k \cdot P \equiv 1 \cdot P \equiv P \pmod{n}\,.$$

Zatem rzeczywiście operacja rozszyfrowywania jest operacją odwrotną do szyfrowania.

A oto przykład poważniejszy. Weźmy znów zdanie `ALEA IACTA EST` i potraktujmy je jako jedną jednostkę tekstu. Kodem tego zdania, po opuszczeniu przerw i zera na początku, będzie liczba $P = 112050109010320010519 20$. Wybieramy w tajemnicy dwie liczby pierwsze p i q i podajemy ich iloczyn: $n = 24543265623376954208 3107$. Kluczem szyfrowania będzie znów liczba 13. Tym razem podniesienie liczby P do potęgi 13 jest trochę bardziej pracochłonne, ale znów krótki program komputerowy poradzi sobie z tym zadaniem w mgnieniu oka. Oczywiście, ten program musi korzystać z jakichś procedur umożliwiających wykonywanie podstawowych działań arytmetycznych na bardzo dużych liczbach. Problem pojawi się chwilę później. Po zaszyfrowaniu otrzymamy liczbę $C = 29070537299022241578466$. Aby rozszyfrować nasze zdanie, będziemy musieli podnieść liczbę C do potęgi d. Tym razem jednak d jest bardzo dużą liczbą: ma ona 23 cyfry! Jak więc podnieść liczbę C do tak dużej potęgi? Ile czasu będzie to trwało?

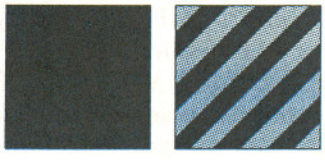
Zastanówmy się przez chwilę, ile mnożeń trzeba wykonać, by podnieść daną liczbę a do potęgi k. Wydaje się w pierwszej chwili, że musimy wykonać $k-1$ mnożeń: najpierw obliczyć $a^2 = a \cdot a$, potem $a^3 = a^2 \cdot a$, potem $a^4 = a^3 \cdot a$ itd. A jednak można to zrobić znacznie szybciej. Popatrzmy na przykład. Aby obliczyć a^{16}, wystarczą cztery mnożenia. Obliczamy kolejno: $a^2 = a \cdot a$, $a^4 = a^2 \cdot a^2$, $a^8 = a^4 \cdot a^4$ i wreszcie $a^{16} = a^8 \cdot a^8$. W podobny sposób, podwajając za każdym razem wykładnik, możemy bardzo szybko obliczyć potęgę a^k modulo n dla wykładnika k będącego potęgą liczby 2. Jeśli teraz pomnożymy odpowiednie takie potęgi (oczywiście, nadal modulo n), to otrzymamy potęgę o zadanym z góry wykładniku k. Wynika to stąd, że każda liczba k jest sumą pewnych potęg liczby 2. Ten algorytm pozwala na wykonanie w krótkim czasie dowolnego potęgowania modulo n, a więc umożliwia dość szybkie szyfrowanie i rozszyfrowywanie.

Aby sobie lepiej uzmysłowić, co to znaczy, niech Czytelnik spróbuje znaleźć klucz rozszyfrowywania w powyższym przykładzie. Liczba n jest iloczynem dwóch dwunastocyfrowych liczb pierwszych p i q. Może komuś uda się rozłożyć liczbę n na czynniki pierwsze i znaleźć następnie klucz d! Za miesiąc podam te liczby p i q.

Zauważmy, że nie tylko sam algorytm szyfrowania jest znany wszystkim. Znany jest też klucz szyfrowania. A mimo to klucz rozszyfrowywania jest znany tylko „właścicielowi" szyfru.

Jakie jest znaczenie takich szyfrów z publicznym kluczem? Przypuśćmy, że chcemy wysłać do kogoś pocztą elektroniczną zaszyfrowaną wiadomość. W tym celu musielibyśmy najpierw spotkać się z tą osobą, wymienić klucze szyfrowania i rozszyfrowywania, a potem dopiero używać ich do korespondencji. To byłoby bardzo niewygodne. Bardzo często łączymy się z osobami znajdującymi się na innych kontynentach, lub z osobami czy instytucjami (np. z bankami), z którymi spotykamy się bardzo rzadko. Otóż systemy kryptograficzne z publicznym kluczem umożliwiają następującą wymianę korespondencji. Najpierw piszemy do kogoś, że mamy dla niego poufną wiadomość. Umawiamy się, że do zaszyfrowania użyjemy szyfru RSA. Następnie prosimy tego kogoś o przysłanie nam (w jawny sposób!) jego klucza szyfrowania. Oczywiście, swoje liczby p, q, $\varphi(n)$ i d trzyma on w tajemnicy. Teraz możemy zaszyfrować wiadomość i przesłać mu ją powszechnie dostępnym kanałem informacyjnym. Nikt jednak, nawet jeśli podpatrzył całą naszą wcześniejszą korespondencję, nie będzie umiał rozszyfrować tekstu raz zaszyfrowanego. Rozszyfrować potrafi tylko adresat: właściciel liczb pierwszych p i q i tym samym jedyny właściciel klucza d.

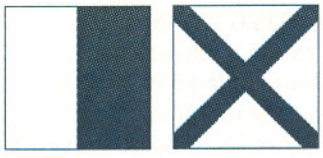
Do wyjaśnienia pozostaje właściwie tylko jedna kwestia. Jak znaleźć te duże liczby pierwsze p i q i jak przekonać się, że są one naprawdę pierwsze? Wspomniałem wyżej, że nie umiemy rozkładać dużych liczb na czynniki i ten właśnie fakt decydował o bezpieczeństwie szyfru RSA. Czy potrafimy zatem przekonać się, że duża liczba jest pierwsza, w inny sposób, niż próbując rozłożyć ją na czynniki? Tym problemem zajmiemy się w następnym artykule.



EY – Jestem pewien swojej pozycji.

O organizowanym od 1989 roku przez Komisję Europejską Konkursie Prac Młodych Naukowców, obejmującym wszystkie dziedziny nauk ścisłych i przyrodniczych, pisaliśmy m.in. w *Delcie* 5/1995, stwierdzając wtedy:

> „Konkurs polega na współzawodnictwie napisanych wcześniej prac uczestników. Szansę na nagrody mają prace stanowiące kompletne rozwiązanie ciekawego zagadnienia. Na konkurs trafiają, oczywiście, prace o rozmaitym poziomie, jednakże zdobywcy nagród prezentują dzieła na poziomie (co najmniej) niezłej polskiej pracy magisterskiej. Stanowi to poważne wyzwanie dla ewentualnych polskich uczestników."



HV – Czy zderzyliście się?

Po blisko dwóch latach, które minęły od tamtej pory, wygląda na to, że *Polacy nie gęsi*. Nasi młodzi reprezentanci potrafią się świetnie odnaleźć w szerokiej stawce żądnych nagród finalistów konkursu. Polska, korzystając z możliwości stworzonej przez stowarzyszenie ze Wspólnotą Europejską, dwukrotnie wzięła udział w finałach konkursu (Newcastle, wrzesień 1995 r.; Helsinki, wrzesień 1996 r.). Za każdym razem nie obyło się bez nagród. O szczegółach za chwilę; przypomnijmy najpierw jeszcze jeden fragment tekstu sprzed dwóch lat.

> „W krajach Wspólnoty Europejskiej konkurs ma bardzo dużą rangę: zdobycie nagrody w Konkursie Europejskim jest cenione wyżej, niż laury z międzynarodowych Olimpiad. Rangę konkursu zapewnia z jednej strony wysoki poziom nagradzanych prac, z drugiej – Jury złożone z wybitnych naukowców. Nie bez znaczenia są wysokie nagrody: trzy pierwsze po 5000 ECU, trzy drugie po 3000 ECU oraz sześć trzecich po 1500 ECU (Czytelnicy zechcą sięgnąć do dowolnej gazety po tabelę kursów i przeliczyć te sumy na stare i nowe złotówki)."

W Newcastle, gdzie Polskę reprezentowały trzy prace (z biologii, fizyki i matematyki), trzecią nagrodę wywalczyli matematycy z Warszawy, Marcin Kowalczyk i Marcin Sawicki. Obszerny skrót ich pracy pt. *Siła zbioru*, poświęconej wspólnemu uogólnieniu takich pojęć, jak charakterystyka Eulera, moc, miara, czy prawdopodobieństwo, zaczyna się na następnej stronie.

Jak pisaliśmy przed dwoma miesiącami, podczas finału w Helsinkach obie startujące w nim polskie prace zdobyły nagrody, dzięki czemu znaleźliśmy się na drugim miejscu, wśród trójki największych łowców nagród, ex aequo z Wielką Brytanią. Wyprzedzili nas tylko Niemcy. O sukcesach matematyków, Macieja Kurowskiego i Tomasza Osmana, oraz paleontologa, Radosława Skibińskiego, można zresztą było dowiedzieć się w poniedziałek 30 września 1996 r. z *Gazety Wyborczej* czy głównego wydania Wiadomości TV.

Radosław Skibiński odnalazł w rejonie Rudawki Rymanowskiej (Beskid Niski) szczątki nie znanych do tej pory ryb oligoceńskich oraz odtworzył ich tryb życia i budowę anatomiczną.

Tomasz Osman i Maciej Kurowski przedstawili rozszerzoną wersję pracy pt. *Wielowymiarowe uogólnienie twierdzenia Bezout*, za którą wcześniej, w 1995 roku, T. Osman zdobył złoty medal w Konkursie Prac Uczniowskich z Matematyki, współorganizowanym przez redakcję *Delty*. Oto niezbyt precyzyjne streszczenie najważniejszego wyniku ich pracy. Jeśli wielomian n zmiennych rzeczywistych W_1 jest nierozkładalny (tzn. nie jest iloczynem dwóch innych niższego stopnia), oraz przyjmuje zarówno wartości dodatnie, jak i ujemne, a wielomian W_2 zeruje się wszędzie tam, gdzie zeruje się W_1, to wtedy wielomian W_2 dzieli się bez reszty przez wielomian W_1, tzn. istnieje taki wielomian D zależny od n zmiennych rzeczywistych, że dla wszystkich $x_1, \ldots, x_n$ mamy

$$W_2(x_1, \ldots, x_n) = D(x_1, \ldots, x_n) \cdot W_1(x_1, \ldots, x_n) .$$

Kluczowy etap dowodu polega na tym, by zbadać, w jaki sposób zbiór Z wszystkich zer wielomianu W_1 jest położony w przestrzeni $\mathbf{R}^n$. Autorzy dowodzą, że rzut zbioru Z na pewną $(n-1)$-wymiarową podprzestrzeń utworzoną przez wszystkie prócz jednej osie układu współrzędnych w $\mathbf{R}^n$ zawiera $(n-1)$-wymiarową kulę otwartą. Czytelnik zainteresowany szczegółami może zajrzeć do marcowego numeru *Delty* sprzed roku.

Rozwiązanie zadania M 803. Jeśli $g : \mathbf{R} \to \mathbf{R}$ jest funkcją okresową o okresie 1, to wówczas przekształcenie f prostej rzeczywistej dane wzorem $f(x) = g(x) + x$ spełnia dla każdego $x \in \mathbf{R}$ warunek

$$f(x+1) = g(x+1) + (x+1) = \\ = g(x) + x + 1 = f(x) + 1 .$$

Mówiąc inaczej, obrazy przy przekształceniu f odległych o 1 punktów x i $x+1$ też są odległe o 1.

Jeśli przyjmiemy dodatkowo, że $g(0) = 0$, to $f(0) = 0$, a $f(1) = 1$. Jedyną izometrią prostej rzeczywistej zachowującą punkty 0 i 1 jest przekształcenie identycznościowe $f(x) = x$. Zatem, jeśli g nie znika tożsamościowo, np. $g(x) = x - [x]$, czy też $g(x) = \frac{1}{10}\cos(2\pi x)$, to f nie jest izometrią.

Uwaga. Czytelnik zechce wskazać przykład przekształcenia f spełniającego warunki zadania i takiego, że $g(x) = f(x) - x$ nie jest funkcją okresową.

Coroczne sukcesy młodych polskich matematyków w finałach Europejskiego Konkursu zachęcają do wysunięcia następującej nieśmiałej hipotezy: złoty medal w Konkursie Prac Uczniowskich z Matematyki, poparty wiarą w siebie i wyszlifowaną angielskojęzyczną wersją pracy, pozwala przy odrobinie szczęścia na zdobycie przynajmniej trzeciej nagrody w Konkursie Europejskim. Zobaczymy, czy hipoteza ta potwierdzi się w czasie finałów IX Europejskiego Konkursu Prac Młodych Naukowców w Mediolanie, w dniach 9–14 września 1997 roku – być może weźmie w nich udział kolejny złoty medalista Konkursu Prac Uczniowskich, Michał Stukow z Gdańska (protokół z finału konkursu opublikowany jest w *Delcie* 1/1997). Skrót jego zwycięskiej pracy opublikujemy za miesiąc; teraz godzi się wspomnieć, że główny wynik polega – jak w przypadku T. Osmana i M. Kurowskiego – na ciekawym, nie znanym wcześniej uogólnieniu osiemnastowiecznego rezultatu „z nazwiskiem".

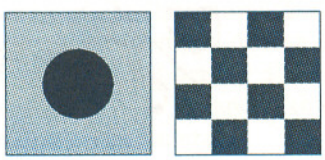
M. Stukow uogólnił, mianowicie, na przypadek czworokąta tzw. wzór Eulera, orzekający, że w dowolnym trójkącie promień okręgu opisanego R, promień okręgu wpisanego r i odległość d środków obu tych okręgów powiązane są zależnością $d^2 = R^2 - 2Rr$. Okazuje się, że jeśli (skądinąd dowolny) czworokąt ma tę własność, że można zarówno opisać na nim okrąg, jak i wpisać weń okrąg, to wtedy odległość d środków obu okręgów wyraża się wzorem

$$d^2 = R^2 + r^2 - r\sqrt{r^2 + 4R^2}$$

(R i r oznaczają, odpowiednio, promienie okręgu opisanego i wpisanego).

Redaktorom *Delty*, nie licząc wszelkich innych ważniejszych powodów, choćby i metryka nie pozwala marzyć o zdobywaniu laurów w Europejskim Konkursie, przeznaczonym dla osób w wieku 15–21 lat. Czytelników w odpowiednim wieku, którzy mają w dodatku pomysły, umiejętności i dobre chęci, zachęcamy do doświadczalnego weryfikowania naszej hipotezy. Wystarczy brać udział najpierw w jednym, a potem w drugim konkursie.

Szczegółowe informacje na temat warunków uczestnictwa w Europejskim Konkursie Prac Młodych Naukowców można uzyskać w biurze Krajowego Funduszu na Rzecz Dzieci (ul. Chocimska 14, 00-791 Warszawa).

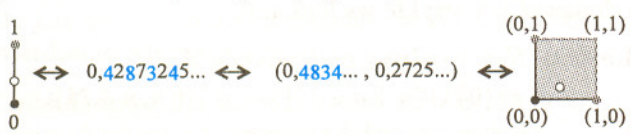


IN – Potrzebuję nurka.

Siła zbioru

Marcin KOWALCZYK i Marcin SAWICKI

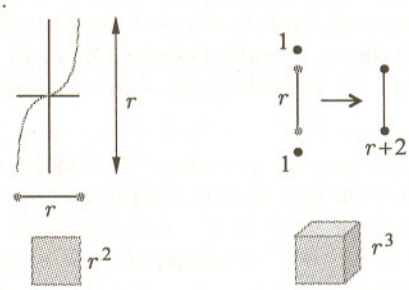
Zapewne wielu Czytelników *Delty* było kiedyś szczerze zaskoczonych dowiedziawszy się, że odcinek i kwadrat są zbiorami równolicznymi, czyli że istnieje między nimi bijekcja (rys. 1). Cóż dziwnego, skoro sam odkrywca tego faktu, Georg Cantor, miał napisać w swoim liście do Dedekinda: „widzę to, lecz nie wierzę w to" (cytat za [5]). Oba zbiory rozróżnia pojęcie wymiaru, lecz ono z kolei utożsamia np. odcinek otwarty z domkniętym, a ten ostatni ma przecież o dwa punkty więcej, nieprawdaż?



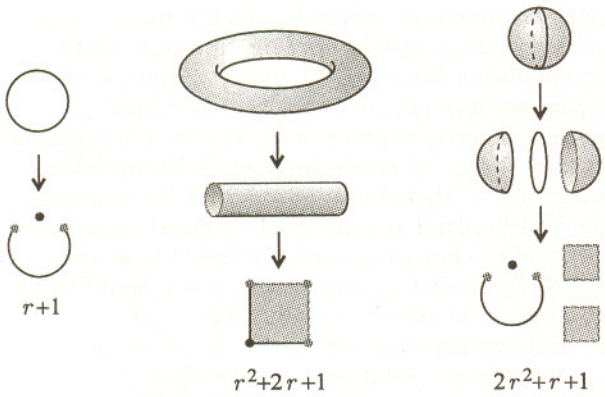
Rys. 1

W niniejszej pracy wprowadzamy pojęcie siły zbioru. Jest to charakterystyka pewnych zbiorów, uwzględniająca zasugerowane powyżej intuicje i będąca w istocie połączeniem wymiaru i charakterystyki Eulera. Siła zbioru będzie zawsze pewnym wielomianem jednej zmiennej r.

Spróbujmy na początek przyjąć, że siła zbioru liczb rzeczywistych jest równa r. Intuicja podpowiada wówczas, by siłę odcinka otwartego, odcinka domkniętego, kwadratu i kostki obliczyć tak, jak to pokazuje rysunek 2. Kolejne sugestie obliczenia siły, dla zbiorów bardziej skomplikowanych, przedstawia rysunek 3.

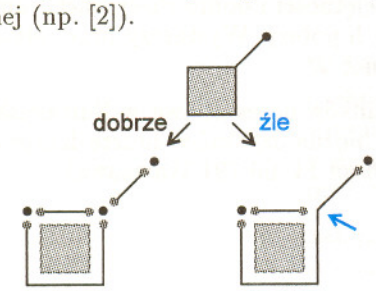


Rys. 2



Rys. 3

Uściślijmy te rozważania. Skończony CW-kompleks to, mówiąc obrazowo, przestrzeń, która jest sumą skończonej rodziny rozłącznych, „zachowujących się przyzwoicie" komórek (czyli zbiorów homeomorficznych z kostkami różnych wymiarów). W szczególności, skończony CW-kompleks jest zwarty, a brzeg każdej z komórek jest sumą podzbioru komórek o mniejszych wymiarach. Na rysunku 4 przedstawiamy, na czym to polega. Miłośnicy ścisłości zechcą zajrzeć do podręczników topologii algebraicznej (np. [2]).



Rys. 4

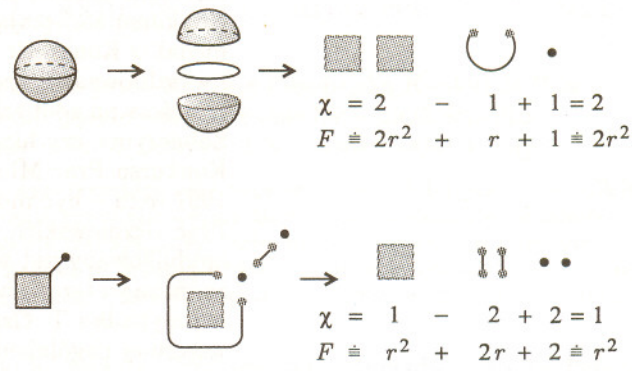
Na komórkach CW-kompleksu (e^m, dla $m \geq 1$, oznacza otwartą komórkę m-wymiarową; e^0 to punkt) określimy funkcję f o wartościach w pewnym zbiorze Y (z dodawaniem i mnożeniem) spełniającą warunek $f(e^{k+l}) = f(e^k) \cdot f(e^l)$. Siłę F definiujemy jako

$$F(K) = \sum_K f(e^k)\,.$$

Sumowanie rozciąga się na wszystkie komórki tworzące kompleks K. Łatwo wykazać, że $F(A \cup B) = F(A) + F(B)$ dla A, B rozłącznych, oraz $F(A \times B) = F(A) \cdot F(B)$.

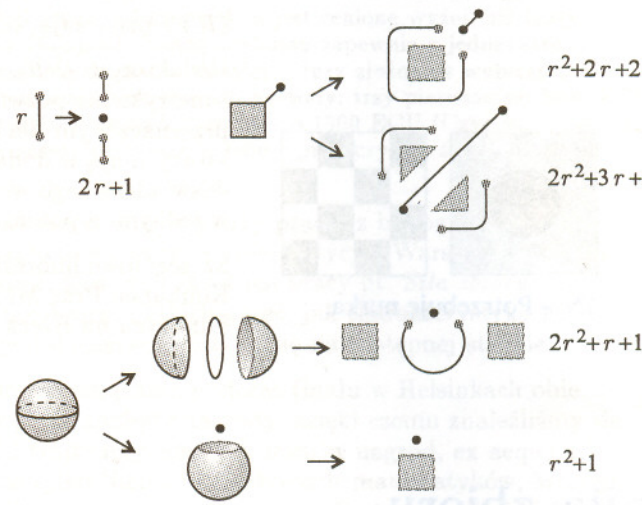
Definicja jest dość ogólna; dobierając Y oraz f możemy otrzymać wiele różnych pojęć. Jeśli np. Y jest zbiorem liczb całkowitych, $f(\emptyset) = 0$, $f(e^k) = (-1)^k$, to otrzymana tak funkcja siły jest skądinąd dobrze znana: nazywa się charakterystyką Eulera i jest oznaczana $\chi(K)$; przykłady jej obliczania pokazuje rysunek 5.

O ile nie będziemy się ograniczać do CW-kompleksów, to można w podobny sposób zdefiniować np. miarę zbioru, prawdopodobieństwo, moc. Nie są to wprawdzie praktyczne definicje, ale pokazują ogólność wprowadzanego pojęcia.



Rys. 5

Można sądzić, że do uściślenia definicji siły zasugerowanej na rysunkach 2 i 3 należy przyjąć za Y pierścień wielomianów zmiennej r i położyć $f(e^k) = r^k$, $f(\emptyset) = 0$. Rysunek 6 pokazuje, że nie jest to określenie jednoznaczne. Jak więc zmienić definicję?



Rys. 6

Zauważmy, że w podanych przykładach wszystkie siły danego zbioru są tego samego stopnia i w dodatku przystają modulo $(r+1)$. To spostrzeżenie pozwala rozwiązać problem. Niech $\overline{Y}$ będzie zbiorem wielomianów zmiennej r o współczynnikach całkowitych nieujemnych; odpowiedni dla naszych potrzeb zbiór Y otrzymujemy utożsamiając te wielomiany P i Q równego stopnia, których różnica dzieli się bez reszty przez dwumian $(r+1)$. Dla krótkości piszemy wtedy $P \dot{=} Q$. Elementy zbioru Y (dla wtajemniczonych: klasy abstrakcji relacji równoważności $\dot{=}$) można, oczywiście, mnożyć i dodawać jak zwykłe wielomiany.

Lemat. *Jeśli z rodziny wielomianów* $\mathcal{F}$,

$$\mathcal{F} = \{0\} \cup \{a \mid a \in \mathbf{N}\} \cup \{ar^n \mid a, n \in \mathbf{N}\} \cup \{r^n + br^{n-1} \mid b, n \in \mathbf{N}\} \tag{1}$$

wybierzemy dwa różne wielomiany tego samego stopnia, to będą one przyjmować różne wartości w punkcie $r = -1$. *Ponadto, dla każdego* $n \in \mathbf{N}$ *i każdego całkowitego* m *istnieje taki wielomian* Q *postaci* (1) *i stopnia* n, *że* $Q(-1) = m$.

Dowód polegający na rozpatrzeniu kilku prostych przypadków pomijamy.

Twierdzenie. *Dla każdego wielomianu $P \in \overline{Y}$ istnieje dokładnie jeden wielomian Q należący do rodziny $\mathcal{F}$ określonej wzorem (1) o tej własności, że $P \doteq Q$.*

Dowód. Gdy wielomian $P = \text{const.}$, to teza jest oczywista. Gdy stopień P jest dodatni, to wybieramy wielomian Q tego samego stopnia i postaci (1) tak, by mieć $Q(-1) = P(-1)$. Na mocy Lematu wielomian Q jest określony jednoznacznie, a z twierdzenia Bezout wynika, że różnica wielomianów P i Q dzieli się bez reszty przez dwumian $(r+1)$. Zatem, $P \doteq Q$. ■

Definicji samej funkcji f nie musimy zmieniać; przyjmujemy nadal $f(e^k) = r^k$. Możemy już udowodnić

Twierdzenie. *Siła skończonego CW-kompleksu jest dobrze określona.*

Dowód. Pokażemy, że siła zbioru jest dobrze określona dla przestrzeni, których charakterystyka Eulera i wymiar (tzn. największy z wymiarów wszystkich komórek) są dobrze określone. Weźmy wielomian $F(A)$ obliczony dla konkretnego rozbicia $e^{k_1}, \ldots, e^{k_n}$ danego zbioru A oraz charakterystykę Eulera A:

$$F(A) = \sum_{i=1}^{n} r^{k_i}, \qquad \chi(A) = \sum_{i=1}^{n} (-1)^{k_i}.$$

Jak widać, $\chi(A) = F(-1)$ (zob. też rys. 6). Ale charakterystyka Eulera $\chi(A)$ jest dobrze określona, toteż dla dwóch różnych rozbić zbioru A otrzymujemy wielomiany F_1, F_2 przyjmujące równe wartości w punkcie $r = -1$, czyli przystające modulo $(r+1)$. W dodatku stopnie tych wielomianów są równe (dobrze określonemu!) wymiarowi zbioru A. Zatem $F_1 \doteq F_2$, czyli wielomiany F_1 i F_2 określają ten sam element zbioru Y. ■

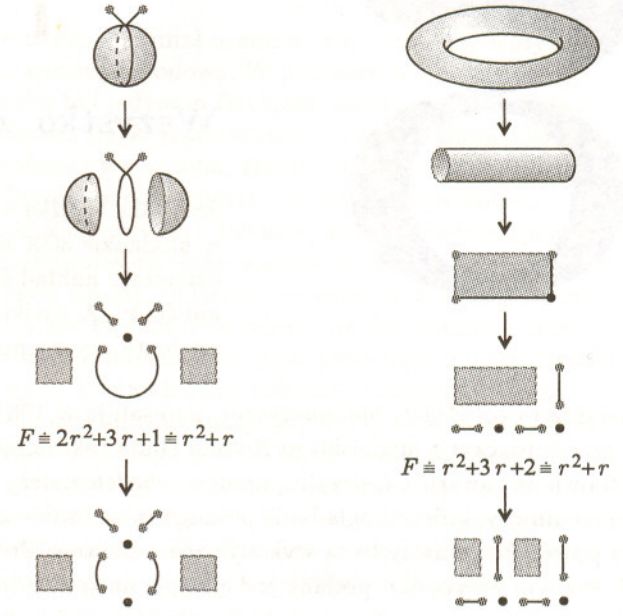
Wniosek. Znając wymiar zbioru A i jego charakterystykę Eulera, można siłę $F(A)$ określić jednoznacznie.

Uwaga. Charakterystyka Eulera jest niezmiennikiem homotopii, ale wymiar nim nie jest, więc siła zbioru nie może być niezmiennikiem homotopii.

Jeśli dwa zbiory mają identyczne CW-kompleksowe rozbicia, to mają, oczywiście, równe siły. Pojęcie siły jest na tyle trafne i naturalne, że zachodzi także twierdzenie odwrotne.

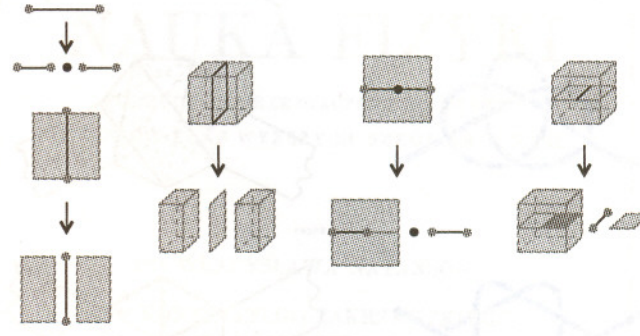
Twierdzenie. *Dla każdych dwóch zbiorów A i B mających równe siły istnieją identyczne rozbicia $A_1, \ldots, A_n$ zbioru A i $B_1, \ldots, B_n$ zbioru B (słowo „identyczne" oznacza, że oba zestawy komórek są identyczne).*

Działanie twierdzenia ilustruje rysunek 7. Zachęcamy Czytelników do próby samodzielnego przeprowadzenia nieco technicznego dowodu. Podamy tylko wskazówkę.



Rys. 7

Lemat. *Dla dowolnych $0 \leq m < n$ można rozłożyć kostkę e^n na trzy rozłączne zbiory: kostkę e^n, kostkę e^m i kostkę e^{m+1}* (patrz rys. 8).



Rys. 8

I jeszcze jedno: zbiór z lewej strony rysunku 7 nie jest CW-kompleksem. W istocie, charakterystyka Eulera i siła zbioru zdają się działać dla niektórych innych sytuacji, np. dla rozbić, które nie są CW-kompleksowe (por. rys. 4), albo rozbić zbiorów, które nie są zwarte. Autorzy nie wiedzą, jak rozszerzyć klasę CW-kompleksów tak, aby objąć i te przypadki.

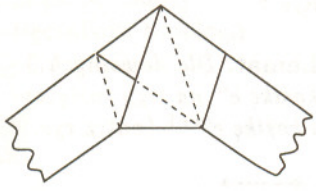
Literatura

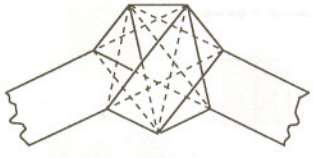
[1] E.H. Spanier, *Algebraic topology*, McGraw-Hill, New York 1966.
[2] A.T. Fomenko, D.B. Fuchs, V.L. Gutenmacher, *Homotopic topology*, Budapest 1986.
[3] K. Kuratowski, *Wstęp do teorii mnogości i topologii*, PWN 1965.
[4] R. Duda, *Wstęp do topologii*, PWN 1992.
[5] J. Górnicki, *Okruchy matematyki*, PWN 1995.

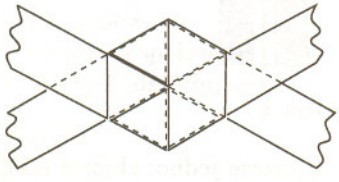
Wszystko z paska papieru

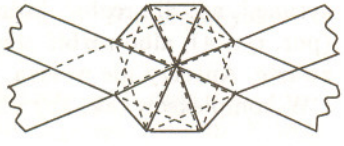
Jest taka książka o matematyce, którą wydano w Polsce w 1967 roku w nakładzie 3000 egzemplarzy, co dziś znaczyłoby ogromny nakład, a wtedy oznaczało nakład śladowy. Nic przeto dziwnego, że po książce tej nie zostało ani śladu. A wielki mógłby być z niej pożytek dla każdego nauczyciela, ucznia, studenta czy po prostu miłośnika matematyki.

Książka ta to *Modele matematyczne*, napisali ją w 1961 roku H.M. Cundy i A.P. Rollet, wydało ją PWN, a przetłumaczył z angielskiego Roman Duda (aktualnie rektor Uniwersytetu Wrocławskiego). Tytuł książki odpowiada zawartości, przy czym słowo *modele* należy rozumieć w najbardziej potoczny sposób – chodzi o przedmioty, których oglądanie pomaga radzić sobie z matematyką lub łatwiej dostrzegać piękno i bogactwo jej pojęć. Przedmioty te są wykonywane z kartonu, drutu, papieru itp. powszechnie dostępnych materiałów. W każdym przypadku podany jest przepis na sporządzenie sobie takiego modelu. A bogactwo przykładów jest niemal niezmierzone. Może warto byłoby wznowić tę książkę?









A oto konkretny przykład. Gdy dysponujemy pewną ilością taśmy papierowej, możemy za jej pomocą skonstruować wszystkie wielokąty foremne. Instrukcję stanowią zamieszczone obok rysunki. To, co z lewej strony, to sposób zaplecenia taśmy. To, co z prawej strony, to wskazówki, jak taśmę spłaszczyć: chodzi o to, by jej krawędzie wypadły wszystkie na brzegu węzła. Te krawędzie to właśnie teoretycznie dokładny brzeg wielokąta foremnego. Autorzy pokazują, jak zrobić pięciokąt, jak zrobić siedmiokąt, a zrobienie „reszty" wielokątów foremnych o nieparzystej liczbie boków pozostawiają inwencji swoich czytelników. Dalej informują, że do zrobienia wielokątów foremnych o parzystej liczbie boków potrzebne są dwie taśmy i pokazują to na przykładzie sześcio- i ośmiokąta foremnego – reszta znów dla nas. I faktycznie, po chwili namysłu można zaproponować paskową konstrukcję „pozostałych" wielokątów foremnych.

A potem dopiero przychodzi refleksja: *jak to? – przecież cyrklem i linijką nie wszystkie wielokąty foremne można skonstruować. To pasek papieru ma większe możliwości?*

Przypominamy sobie, że wielokąt foremny można skonstruować cyrklem i linijką jedynie wtedy, gdy liczba jego boków to

$$2^k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_m,$$

gdzie liczby k i m to dowolne liczby naturalne, mnożone zaś liczby p_i to różne liczby pierwsze postaci $2^{2^n}+1$ – dotychczas znamy tylko pięć takich liczb pierwszych: 3, 5, 17, 257, 65537 i wiemy, że ewentualne następne byłyby ogromnie ogromne. I wtedy można odczuć motywację do udowodnienia, że konstrukcje z pasków papieru są naprawdę poprawne.

Małą Deltę przygotował Marek KORDOS

Wspomnienie o Władysławie Natansonie (1864–1937)

Pan M. Karpiniec z Kielc przypomniał nam o sześćdziesiątej rocznicy śmierci Władysława Natansona – profesora fizyki teoretycznej na Uniwersytecie Jagiellońskim i rektora tej uczelni, pisząc m.in.: „Napomknę tylko, że do przypomnienia tej rocznicy skłania mnie wdzięczność za trzytomowy podręcznik fizyki dla szkół średnich – napisany przez prof. Natansona – z którego niegdyś uczyłem się, który do dziś posiadam i wypożyczam moim uczniom, ku ich wielkiemu zadowoleniu z jasności wykładu." Poniżej zamieszczamy dwa fragmenty z przesłanych nam przez niego materiałów.

O moim ojcu

W pokoju mojego ojca w Krakowie, w domu przy ulicy Studenckiej, bawiła się cichutko najstarsza wnuczka, pięcioletnia wówczas Elżunia. Pewnego dnia, wiedziona dziecięcą ciekawością, zajrzała dziadkowi przez ramię.

– Co piszesz? – zapytała.

– Zobacz!

Władysław Natanson podał jej kartkę papieru, zapisaną od góry do dołu wzorami różniczek czy całek.

Dziewczynka przyjrzała się uważnie. Już trochę znała alfabet, używany w elementarzach, i od razu dostrzegła, że coś się nie zgadza. Gdzież są przyzwoicie napisane litery?

– Ależ dziadku – powiedziała z wyrzutem – ty wcale nie umiesz pisać!

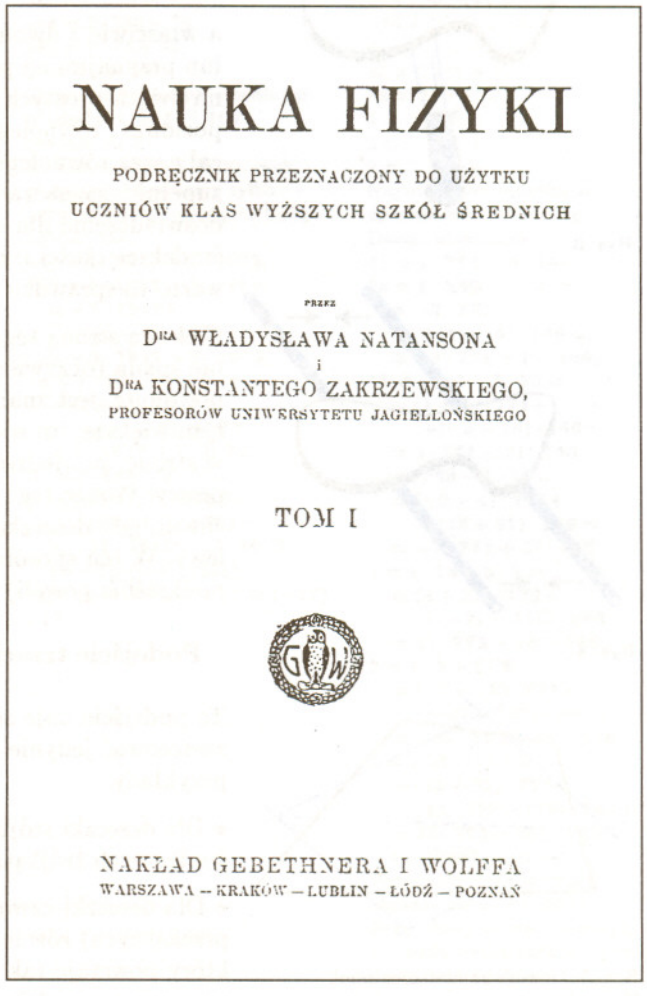
Ojciec mój bardzo lubił tę historię. I swoiście ją interpretował jako dowód względności wszelkich kryteriów. Co dla jednego jest wiedzą, dla innego może być dowodem niewiedzy. Dziecko ma rację ze swojego punktu widzenia, podobnie jak ją ma uczony matematyk. [...]

(Wojciech Natanson (1904–1996) *Hierarchie i sylwety*, Ludowa Spółdzielnia Wydawnicza, Warszawa 1985)

Mój profesor – Władysław Natanson

[...] Dzisiaj dopiero oceniam lepiej skomplikowany charakter mego profesora. Widzę w nim człowieka niezdolnego do intryg, rycerskiego i szlachetnego. Człowieka wychowanego w dobrobycie, który obawia się kontaktu z życiem i jego brutalnością i bezwzględnością. Człowieka samotnego, tak w nauce, jak i w życiu, dla którego bezosobowość w stosunkach z ludźmi była pancerzem ochronnym; takim pancerzem była jego niesłychana grzeczność, posunięta do upokarzającej przesady. Naukowo był blisko, bardzo blisko wielkich odkryć, np. sformułowania statystyki Bosego. Z powodu izolacji naukowej, braku osobistych kontaktów, nie rozwinął w pełni swych zdolności naukowych; rozwinął natomiast w pełni swe zdolności pisarskie. Nie miał uczniów, ale miał duży wpływ na kulturę narodową. W pierwszych latach naszego wieku był jedynym fizykiem teoretycznym w Polsce. Historia fizyki teoretycznej w Polsce zaczyna się od profesora Natansona. Dał on jej chlubny początek. Obecnie, w dwadzieścia pięć lat po jego śmierci, mamy już młodych fizyków, którzy dzieło rozpoczęte przez profesora Natansona poprowadzą dalej. Nie ma obawy dzisiaj, że fizyka teoretyczna w Polsce zamrze. Włączyć się ona musi silniej niż dotychczas w nurt światowy, unikać izolacji lat przeszłych i dogmatyzmu. Z życia i działalności profesora Natansona młodzi naukowcy mogą nauczyć się wiele; przede wszystkim humanistycznego podejścia do nauki, pięknego wyrażania myśli, szacunku dla pracy naukowej, skromności i zrozumienia, że w nauce staramy się nieudolnie znaleźć odzwierciedlenie piękna przyrody, że nauka jest pomocą i pożytkiem dla ludzi.

(Leopold Infeld (1898–1968) *Szkice z przeszłości*, PIW, Warszawa 1964)


NAUKA FIZYKI

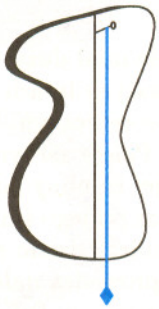
PODRĘCZNIK PRZEZNACZONY DO UŻYTKU
UCZNIÓW KLAS WYŻSZYCH SZKÓŁ ŚREDNICH

PRZEZ

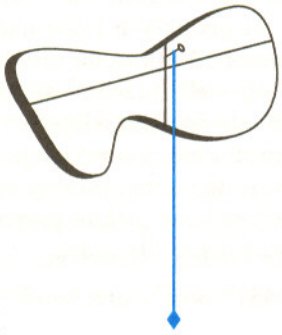
DRA WŁADYSŁAWA NATANSONA
i
DRA KONSTANTEGO ZAKRZEWSKIEGO,
PROFESORÓW UNIWERSYTETU JAGIELLOŃSKIEGO

TOM I

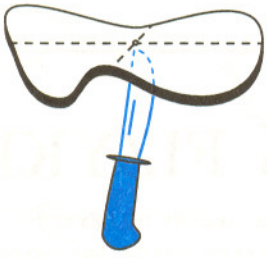
NAKŁAD GEBETHNERA I WOLFFA
WARSZAWA – KRAKÓW – LUBLIN – ŁÓDŹ – POZNAŃ



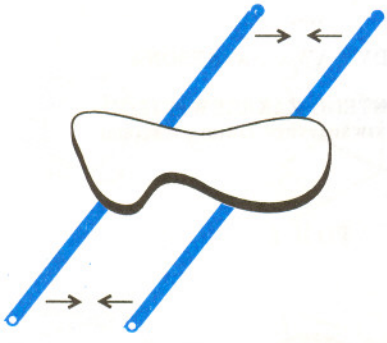
Rys. 1



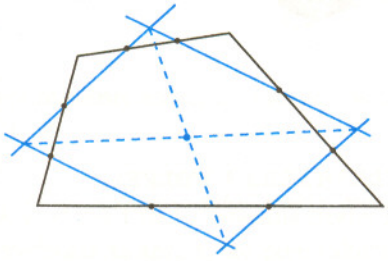
Rys. 2



Rys. 3



Rys. 4



Rys. 5. Dowód, że równoległobok Wittenbauera ma opisaną obok własność, leży w zasięgu elementarnego rozumowania.

Środek ciężkości

– Podejście pierwsze: z pionem

Środek ciężkości to punkt, który ze wszystkich punktów sztywnego ciała **najbardziej lubi być jak najniżej**.

Zawieszone ciało nazywa się wahadłem i może – jak z samej nazwy wynika – wahać się. Jeśli wahania wygasną (albo je sami stłumimy), to środek ciężkości znajdzie się dokładnie pionowo pod punktem zawieszenia. Pozwala to na szybkie znalezienie środka ciężkości za pomocą, oczywiście, pionu. Bardzo to wygląda efektownie, gdy badane ciało jest płaskie, gdy jest to deseczka. Zawieszamy mianowicie tę deseczkę w jakimś punkcie, przykładamy do tego punktu pion (sznurek z ciężarkiem) i zaznaczamy na deseczce położenie sznurka (rys. 1). Potem robimy to po raz drugi (oczywiście, zawieszamy w innym punkcie – rys. 2). Tam, gdzie przetną się zaznaczone linie, znajduje się środek ciężkości – dokładniej: w połowie grubości deseczki.

Należy to, rzecz jasna, sprawdzić. W tym celu umieszczamy deseczkę poziomo i opieramy ją w znalezionym punkcie na czymś ostrym, np. na ostrzu noża fińskiego (rys. 3). Jeśli deseczka nie spadnie, będzie to oznaczało, że środek ciężkości zlokalizowaliśmy prawidłowo.

– Podejście drugie: z kijem,

a właściwie z dwoma. Do tego potrzebny jest nam kolega-eksperymentator lub przynajmniej pomocnik-laborant. Tę samą deseczkę kładziemy poziomo na dwóch prostych i dość gładkich kijach (np. od szczotki). Kije trzymamy poziomo i równolegle. Następnie bardzo powoli zsuwamy je dbając, by były cały czas równoległe i cały czas na tym samym poziomie (rys. 4). Gdy się zsuną zupełnie, zaznaczamy na deseczce linię, pod którą stykają się kije. Ponawiamy doświadczenie dla innego położenia deseczki na kijach. Podobnie jak poprzednio, środek ciężkości leży w przecięciu otrzymanych linii. I, podobnie jak poprzednio, warto to sprawdzić.

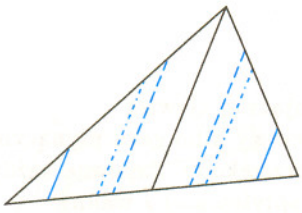
Ciekawą stroną tego doświadczenia jest fakt, iż podczas zsuwania kijów deseczka nie spada (oczywiście, gdy robimy to powoli). Zjawisko fizyczne, które to powoduje, jest znane jako **tarcie**. Można się przekonać mianowicie, iż jest ono tym większe, im większa jest siła nacisku. Jeśli deseczka przechyla się lekko w stronę, powiedzmy, lewego kija, to na niego wywiera większy nacisk niż na kij prawy. Wobec tego kij prawy przesuwa się pod deseczką łatwiej, szybciej, aż do chwili, gdy deseczka zacznie się przechylać w jego stronę. Wtedy przyspiesza lewy. W ten sposób deseczka leżąc na przesuwających się (jeszcze raz warto podkreślić: powoli) kijach sama łapie równowagę.

– Podejście trzecie: z geometrią

To podejście daje się, przy stosowaniu wyłącznie elementarnych środków, zastosować jedynie dla niewielu kształtów jednorodnych deseczek. Oto dwa przykłady.

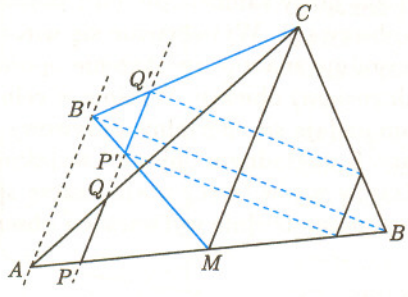
- Dla deseczki trójkątnej środek ciężkości znajduje się w punkcie przecięcia środkowych trójkąta.

- Dla deseczki czworokątnej jest on w środku (czyli w punkcie przecięcia przekątnych) równoległoboku, zwanego równoległobokiem Wittenbauera, który powstaje tak: każdy bok czworokąta dzielimy na trzy równe części, po czym prowadzimy proste łączące punkty sąsiadujące z tym samym wierzchołkiem (rys. 5).



Rys. 6

Powstaje pytanie: dlaczego tak właśnie jest? Łatwiejszy jest dowód pierwszego stwierdzenia. I starszy: został uzyskany wtedy, gdy Hannibal przeprowadzał słonie przez Alpy, a więc ponad 2200 lat temu. Jego autorem jest Archimedes. A dowód ten w gruncie rzeczy opiera się na doświadczeniu z kijami. Wystarczy wykazać, że kije mogłyby się zejść właśnie wzdłuż środkowej. Inaczej: trójkąt położony płasko na kiju wzdłuż którejkolwiek ze swoich środkowych z tego kija nie spadnie.



Rys. 7

Jest tak dlatego, że w każdej odległości od kija znajduje się tyle samo deseczki (rys. 6). Aby to udowodnić, należy – w wyobraźni – złożyć deseczkę na pół. Teraz mamy (rys. 7)

$$\frac{PQ}{CM} = \frac{AP}{AM} = \frac{B'P'}{B'M} = \frac{P'Q'}{CM},$$

a więc $PQ = P'Q'$ i po dowodzie. Trzeba, oczywiście, znać twierdzenie Talesa, ale Archimedes je znał. No i zauważyć, że $AB' \parallel CM \parallel PQ'$, ale tak jest – prawda?

Najmniejszy wynik

Dane są dwie liczby całkowite dodatnie M i N. Pytanie jest następujące:

jaką najmniejszą liczbę dodatnią można uzyskać mnożąc M i N przez liczby całkowite i dodając (bądź odejmując) *otrzymane iloczyny*?

Inaczej: jaka jest najmniejsza dodatnia wartość liczby

$$X = k \cdot M + l \cdot N,$$

dla całkowitych (niekoniecznie dodatnich) wartości k i l?

Odpowiedź brzmi: tą najmniejszą liczbą jest największy wspólny dzielnik M i N. Rzeczywiście, X dzieli się przez NWD(M, N), nie może więc być od niego mniejszy. Ale czy zawsze znajdą się takie liczby k i l, by X było równe akurat NWD(M, N)?

To da się zrobić. W tym celu dogodnie jest wykonać pewną operację zwaną *algorytmem Euklidesa*. Robi się to tak. Niech np. będzie $M > N$. Będziemy wielokrotnie dzielili z resztą.
$M = a_1 \cdot N + r_1$,
$N = a_2 \cdot r_1 + r_2$,
$r_1 = a_3 \cdot r_2 + r_3$,
$r_2 = a_4 \cdot r_3 + r_4$, itd.
To się musi skończyć, bo kolejne reszty są coraz mniejsze, a nigdy nie są ujemne. Więc w końcu będzie
$r_{k-1} = a_{k+1} \cdot r_k + r_{k+1}$,
$r_k = a_{k+2} \cdot r_{k+1} + 0$.
W tej sytuacji

$$r_{k+1} = \text{NWD}\,(M, N),$$

a z całego rachunku (czyli z działania algorytmu Euklidesa) można odtworzyć potrzebne k i l.
Podajemy obok dwa przykłady zostawiając odszukanie ogólnej metody chętnym Czytelnikom.

1517 = 1 · **1073** + 444,
1073 = 2 · 444 + 185,
444 = 2 · 185 + 74,
185 = 2 · 74 + 37,
74 = 2 · 37 + 0.
Zatem największym wspólnym dzielnikiem **1517** i **1073** okazało się 37.
Te same rachunki, w których podstawiać będziemy tylko „grube" liczby, wyglądać będą kolejno tak:
444 = 1 · **1517** − 1 · **1073**,
185 = 1 · **1073** − 2 · 444 =
= −2 · **1517**+
+(1 + 2) · **1073** =
= −2 · **1517** + 3 · **1073**,
74 = 1 · 444 − 2 · 185 =
= (1 + 4) · **1517**+
+(−1 − 6) · **1073** =
= 5 · **1517** − 7 · **1073**,
37 = 1 · 185 − 2 · 74 =
= (−2 − 10) · **1517**+
+(3 + 14) · **1073** =
= −12 · **1517** + 17 · **1073**
(= −18204 + 18241),
czyli poszukiwane k i l to (−12) i 17.

Analogicznie
771 = 5 · **146** + 41,
146 = 3 · 41 + 23,
41 = 1 · 23 + 18,
23 = 1 · 18 + 5,
18 = 3 · 5 + 3,
5 = 1 · 3 + 2,
3 = 1 · 2 + 1
2 = 2 · 1 + 0.
Największym wspólnym dzielnikiem okazało się 1.
Dalsze obliczenia:
41 = 1 · **771** − 5 · **146**,
23 = 1 · **146** − 3 · 41 =
= −3 · **771**+
+(1 + 15) · **146** =
= −3 · **771** + 16 · **146**,
18 = 1 · 41 − 1 · 23 =
= (1 + 3) · **771**+
+(−5 − 16) · **146** =
= 4 · **771** − 21 · **146**,
5 = 1 · 23 − 1 · 18 =
= (−3 − 4) · **771**+
+(16 + 21) · **146** =
= −7 · **771** + 37 · **146**
3 = 1 · 18 − 3 · 5 =
= (4 + 21) · **771**+
+(−21 − 111) · **146**
= 25 · **771** − 132 · **146**,
2 = 1 · 5 − 1 · 3
= (−7 − 25) · **771**+
+(37 + 132) · **146** =
= −32 · **771** + 169 · **146**,
1 = 1 · 3 − 1 · 2 =
= (25 + 32) · **771**+
+(−132 − 169) · **146** =
= 57 · **771** − 301 · **146**,
(= 43947 − 43946).
Poszukiwanymi liczbami okazały się 57 i (−301).
Przy okazji warto zauważyć, że każdą liczbę całkowitą można przedstawić jako

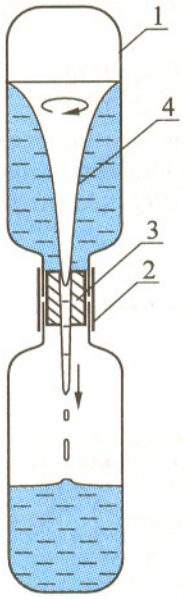
$$k \cdot \mathbf{771} + l \cdot \mathbf{146}$$

dla pewnych całkowitych k i l.

Obserwujemy wiry

Stanisław BEDNAREK

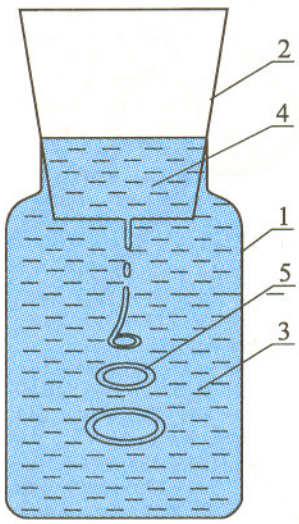
Wiry należą do bardzo efektownych i często występujących zjawisk fizycznych. Mogą one tworzyć się np. w strumieniu cieczy albo gazu płynącym z dostatecznie dużą prędkością lub napotykającym przeszkody. Zapewne każdy widział wiry w rzece czy strumieniu, albo w wodzie spływającej z wanny. Wiry powstają także w powietrzu podczas jazdy samochodu, lotu samolotu czy pocisku, ale są one trudniejsze do obserwacji. Wytworzenie się wirów jest na ogół niekorzystne, ponieważ powoduje znaczne zwiększenie oporów towarzyszących przepływowi cieczy lub ruchowi obiektu. Właśnie w celu ograniczenia tego zjawiska samochodom nadaje się specjalny, opływowy kształt i wyposaża w różne spojlery i deflektory. Z dokładnym opisem i wyjaśnieniem przyczyn powstawania niektórych rodzajów wirów fizycy mają jeszcze spore kłopoty. Nie przeszkadza to jednak, żeby samodzielnie wytwarzać i obserwować wiry w warunkach domowych.



Rys. 1

W celu zbudowania prostego przyrządu do wytwarzania wirów cieczy (rys. 1) potrzebne są dwie przezroczyste plastykowe butelki od napojów (1). Najlepsze są butelki o pojemności 1,5–2 l mające środkową część w kształcie zbliżonym do cylindrycznego. Do jednej z butelek nalewamy wody wypełniając nią około 3/4 objętości. Obie butelki należy połączyć wciskając ich szyjki w kawałek gumowego węża lub plastykowej rurki (2). Przedtem dobrze jest umieścić w szyjkach butelek korek (3) z otworem o średnicy 8–10 mm. Pozwoli to otrzymać dłużej trwające wiry. Zamiast naturalnego korka można użyć plastykowych zakrętek do butelek. W zakrętkach należy wywiercić otwory, co można łatwo zrobić końcem nożyczek lub noża. Butelki zamyka się zakrętkami i podobnie jak poprzednio, łączy kawałkiem węża lub rurki o odpowiedniej średnicy.

Gdy chcemy wytworzyć wir, należy szybko odwrócić przyrząd tak, żeby butelka zawierająca wodę znalazła się u góry. Następnie trzymając jedną ręką za rurkę lub wąż, a drugą za dno górnej butelki wykonujemy kilka energicznych obrotów przyrządem wokół jego osi pionowej. Woda zawarta w górnej butelce zostanie w ten sposób wprawiona w ruch i wytworzy wir w kształcie leja. Wir ten można wygodnie obserwować przez kilkadziesiąt sekund lub dłużej. Po przepłynięciu wody do dolnej butelki ponownie odwracamy przyrząd i wytwarzamy wir w poprzednio opisany sposób.



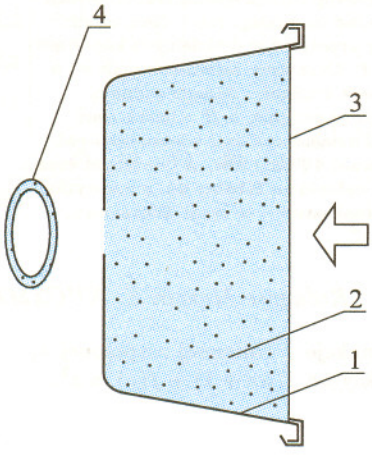
Rys. 2

Cząsteczki wody tworzącej wir poruszają się po spiralach. Żeby lepiej uwidocznić ten ruch, można przed połączeniem butelek wrzucić do wody trochę okruchów korka lub styropianu. Zastosowanie zasady zachowania momentu pędu i równania Bernoulliego prowadzi do wniosku, że wewnętrzna powierzchnia leja (4) jest częścią hiperboloidy obrotowej. Daje się ona opisać w przybliżeniu wzorem

$$h = \frac{A}{r^2} + B\,,$$

w którym r oznacza promień hiperboloidy mierzony na wysokości h liczonej od jej podstawy, natomiast A i B są to stałe, zależne od prędkości początkowej, ilości wody i rozmiarów butelki.

Bardzo interesujące samoorganizujące się wiry powstają podczas wpływania strumienia nasyconego roztworu soli kuchennej do czystej wody (rys. 2). Żeby je zaobserwować, potrzebny będzie szklany słoik typu „twist-off" (1) i okrągły plastykowy kubek jednorazowego użytku (2), np. od jogurtu lub kawy. Najlepiej dobrać dość wysoki słoik o takiej średnicy, żeby w jego otwór można było lekko wcisnąć kubek. W środku dna kubka należy wykonać igłą otworek o średnicy około 0,5 mm. Słoik napełnia się czystą wodą (3) i umieszcza w nim kubek. Teraz trzeba przygotować w oddzielnym naczyniu nasycony roztwór soli kuchennej. W tym celu do wody należy stopniowo dosypywać soli i mieszać



Rys. 3

tak długo, aż przestanie się rozpuszczać. Dla lepszej widoczności roztwór ten zabarwia się odrobiną atramentu. Zabarwiony roztwór (4) trzeba powoli wlewać do kubka. Zauważamy, że w pewnej chwili przez otwór w dnie zaczyna wypływać cienka strużka roztworu. Wypływ ten ulega okresowym przerwom, a strużka co pewien czas samorzutnie tworzy wiry (5) w kształcie zbliżonym do pierścieni. Wiry te opadają w dół i powoli rozpływają się w wodzie. Przyczyny tego zjawiska nie są jeszcze w pełni ilościowo wyjaśnione.

Pierścieniowe wiry można również wytworzyć w gazie (rys. 3). Do tego celu wystarczy okrągłe plastykowe pudełko od margaryny (1). W środku jego dna należy wyciąć otwór o średnicy 8–10 mm. Pudełko trzeba napełnić dymem. Stanowczo odradzam używanie do tego celu dymu papierosowego. Sformułowana przez Hipokratesa zasada *primum non nocere* (przede wszystkim nie szkodzić) obowiązuje również prowadzących badania naukowe i amatorskie eksperymenty. Lepiej zamknąć pudełko pokrywką (3), wsunąć do niego przez otwór w dnie trzymany w ręku tlący się zwitek papieru lub popularne ostatnio kadzidełko zapachowe. Po kilkudziesięciu sekundach „zadymiacz" należy usunąć. Dla ułatwienia obserwacji otwór pudełka dobrze jest skierować pod światło, np. lampy lub latarki kieszonkowej. Teraz trzeba lekko uderzyć palcami w wieczko pudełka w kierunku wskazanym strzałką. Zauważymy wówczas pierścieniowe wiry (4) utworzone z wypływającego przez otwór dymu. Wiry te oddalają się od dna i powoli rozpływają w powietrzu. Na zakończenie warto zadać sobie pytanie, czy występują jakieś analogie między wirami tworzonymi przez dym i roztwór soli?

Zadania

Redaguje Krzysztof OLESZKIEWICZ

M 801. Dane są liczby rzeczywiste $a_1, \ldots, a_n$, parami różne. Niech J będzie zbiorem wszystkich przedziałów postaci $(a_i, a_i + 1)$. Udowodnić, że można ze zbioru J wybrać dwa rozłączne podzbiory $\mathcal{A}$ i $\mathcal{B}$ o następujących własnościach:
(i) przedziały należące do $\mathcal{A}$ (odpowiednio do $\mathcal{B}$) są parami rozłączne,
(ii) suma wszystkich przedziałów należących do zbioru $\mathcal{A} \cup \mathcal{B}$ jest równa sumie wszystkich przedziałów należących do J.
Rozwiązanie na str. 14

M 802. Przekątne czworokąta wypukłego $ABCD$ przecinają się w punkcie P. Dane są pola S_1, S_2, S_3 trójkątów ABP, BCP, CDP. Znaleźć pole trójkąta DAP.
Rozwiązanie na str. 16

M 803. Podać przykład przekształcenia prostej p w p nie będącego izometrią i spełniającego warunek: odległość punktów $f(x)$ i $f(y)$ jest równa 1 dla każdych dwóch punktów x i y, których odległość jest równa 1.
Rozwiązanie na str. 4

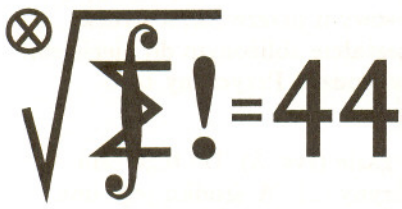
Redaguje Krzysztof REJMER

F 447. Dwa samochody stoją „na czerwonym świetle" stykając się zderzakami. Po zmianie światła na zielone pierwszy z nich zaczyna się poruszać ze stałym przyspieszeniem a. Drugi samochód podąża za nim z prędkością proporcjonalną do odległości dzielącej oba samochody. Opisać ruch drugiego samochodu. Długość pierwszego samochodu jest równa l.
Rozwiązanie na str. 3

JW – Mam przeciek.

F 448. Druga prędkość kosmiczna, czyli prędkość ucieczki z powierzchni Ziemi, wynosi $v_{II} = \sqrt{2gR} = 11{,}2$ km/s, gdzie R jest promieniem Ziemi, g zaś przyspieszeniem grawitacyjnym na powierzchni Ziemi. Jaką dodatkową prędkość należy nadać rakiecie spadającej swobodnie (z zerową prędkością początkową) w tunelu przechodzącym przez środek Ziemi, w chwili gdy znajduje się ona dokładnie w samym środku planety tak, aby mogła opuścić Ziemię. Dla uproszczenia zakładamy, że rozkład masy we wnętrzu Ziemi jest jednorodny.
Rozwiązanie na str. 2

Klub 44



Termin nadsyłania rozwiązań:
31 V 1997

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 2/1997.

Zadania z matematyki nr 337, 338

Redaguje Marcin E. KUCZMA

337. Niech $\alpha = (i\sqrt{3}-1)/2$. Wyznaczyć wszystkie funkcje f zmiennej zespolonej z, o wartościach zespolonych, spełniające równanie funkcyjne $f(\alpha z+1)+f(z)=z^2$.

338. Dowieść, że dla każdej liczby naturalnej $n \geq 1$

$$\sum_{k=0}^{2n}(-1)^k\binom{2n}{k}k^n = 0\,.$$

Zadanie **338** zaproponował pan Krzysztof Oleszkiewicz z Warszawy.

Rozwiązania zadań z matematyki z numeru 11/1996

Przypominamy treść zadań:

329. Wyznaczyć wszystkie funkcje $f\colon \mathbf{R} \to \mathbf{R}$ o następującej własności: dla każdej pary różnych liczb rzeczywistych a, b prosta przechodząca przez punkty $(a, f(a))$ i $(b, f(b))$ przecina oś rzędnych w punkcie $(0, -ab)$.

330. Udowodnić, że dla każdej liczby naturalnej $n \geq 1$ liczba $N = \prod_{j=0}^{n-1}(2^n - 2^j)$ jest podzielna przez $n!$.

329. Prosta przechodząca przez punkty $(a, f(a))$ i $(b, f(b))$ przecina oś rzędnych w punkcie $(0, w)$, gdzie $w = (af(b) - bf(a))/(a-b)$. Jeśli funkcja f spełnia warunek zadania ($w = -ab$), to kładąc $a = 1$ obliczamy: $f(b) = bf(1) + b(b-1)$. Zatem f ma postać $f(x) = x^2 + cx$. Na odwrót, łatwo sprawdzić, że każda funkcja takiej postaci (z dowolną stałą c) spełnia postulowany warunek ($w = -ab$).

330. Wystarczy dowieść, że dla każdej liczby pierwszej p oraz dla każdego wykładnika naturalnego k w ciągu liczb

(1) $$1,\ 2,\ \ldots,\ n$$

jest nie więcej liczb podzielnych przez p^k niż jest ich w ciągu

(2) $$2^n-1,\quad 2^n-2,\quad 2^n-4,\quad \ldots,\quad 2^n-2^{n-1};$$

stąd już bowiem będzie wynikało, że w rozkładzie na czynniki pierwsze iloczynu wyrazów ciągu (1) liczba p występuje w potędze nie wyższej niż w rozkładzie iloczynu wyrazów ciągu (2), co wobec dowolności wyboru p da nam żądaną podzielność.

Jeżeli p jest liczbą pierwszą nieparzystą, to zgodnie z twierdzeniem Eulera

$$2^{\alpha_k} \equiv 1 \pmod{p^k} \qquad \text{dla } k = 1,2,3,\ldots,$$

gdzie

$$\alpha_k = \phi(p^k) = \begin{pmatrix}\text{ilość liczb naturalnych} \leq p^k \\ \text{względnie pierwszych z } p^k\end{pmatrix} = p^k - p^{k-1}.$$

Jeśli więc $n-j$ dzieli się przez α_k, to $2^{n-j} \equiv 1 \pmod{p^k}$, i wobec tego liczba $2^n - 2^j = 2^j(2^{n-j}-1)$ dzieli się przez p^k. Zatem w ciągu (2) jest co najmniej $[n/\alpha_k]$ wielokrotności liczby p^k, podczas gdy w ciągu (1) jest ich dokładnie $[n/p^k]$; nierówność $[n/\alpha_k] \geq [n/p^k]$ oczywiście zachodzi, skoro $\alpha_k < p^k$.

Trzeba jeszcze rozpatrzeć $p = 2$. Ciąg (1) zawiera $[n/2^k]$ liczb podzielnych przez 2^k; ciąg (2) zawiera ich $n-k$, jeśli $k < n$, a nie zawiera żadnej, jeśli $k \geq n$. Pozostaje więc wykazać, że

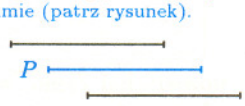
(3) $$n/2^k \leq n-k \qquad \text{dla } k < n\,.$$

To zaś wynika z monotoniczności ciągu $(c_i = i/2^i\colon\ i = 1,2,3,\ldots)$: jeśli $1 \leq k < n$, to $c_{n-k} \geq c_n$, co jest równoważnym zapisem nierówności (3).

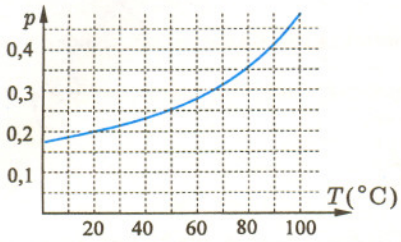
Rozwiązanie zadania M 801.
Rozważmy podzbiory zbioru J, które mają tę własność, że suma elementów każdego z nich jest równa sumie elementów J. Spośród nich (a istnieje co najmniej jeden taki podzbiór, mianowicie J) wybierzmy ten, który ma najmniejszą liczbę elementów i nazwijmy go I (wybór I nie musi być jednoznacznie zdeterminowany).

Przedziały należące do zbioru I leżą na prostej w pewnym porządku (wszystkie mają długość 1, więc wystarczy brać pod uwagę położenie ich środków). Niech $\mathcal{A}$ oznacza zbiór składający się z „co drugiego" (wg powyższego porządku) przedziału należącego do I i niech $\mathcal{B} = I \setminus \mathcal{A}$. Oczywiście, drugi warunek zadania jest spełniony.

Gdyby dwa różne przedziały należące do $\mathcal{A}$ przecinały się, to pewne dwa kolejne przedziały należące do $\mathcal{A}$ przecinałyby się, a wówczas leżący „między" nimi przedział p należący do I byłby zawarty w ich sumie (patrz rysunek).



Zatem suma elementów zbioru $I \setminus \{p\}$ byłaby taka sama jak suma elementów zbioru I (równa sumie elementów zbioru J), co przeczy minimalności zbioru I. W ten sam sposób dowodzimy, że przedziały należące do $\mathcal{B}$ są parami rozłączne.



Rys. 1

235. Rozpuszczalność cukru (sacharozy) w wodzie szybko rośnie ze wzrostem temperatury – zob. rys. 1, gdzie odłożona na osi pionowej wielkość p jest stosunkiem mas cukru i wody w roztworze nasyconym. Wynika stąd dość paradoksalny wniosek, że dolewając czystej, zimnej wody do gorącego roztworu cukru w wodzie można doprowadzić do jego przesycenia i krystalizacji nadwyżki cukru. Obliczyć maksymalną temperaturę wody, której dolanie do nasyconego roztworu cukru o temperaturze 100°C spowoduje krystalizację części cukru (choćby niewielkiej). Rozważyć dwa przypadki:
a) dolewamy niewielką ilość wody,
b) dolewamy ilość wody równą 1/3 początkowej ilości wody w roztworze.

Należy przyjąć, że ciepło pobrane lub oddane podczas zmiany temperatury roztworu jest równe sumie wyrażeń odpowiadających zmianie temperatury wody i cukru, przy czym ciepło właściwe cukru jest równe 0,30 ciepła właściwego wody, a oba ciepła właściwe nie zależą od temperatury. Pominąć efekty cieplne wynikające ze zmiany stężenia.

236. Napastnik biegnący w stronę bramki przeciwnika znajduje się na wprost niej i otrzymuje boczne podanie: piłka toczy się poziomo z prędkością 25 m/s równolegle do linii bramkowej w odległości 20 m od niej. Gdy napastnik kopie piłkę, jego noga porusza się do przodu z prędkością 15 m/s. Ocenić orientacyjnie niezbędną do zdobycia bramki dokładność czasu Δt, w którym noga przekracza dowolną linię. Szerokość bramki wynosi 7,3 m, a średnica piłki – 22 cm. Pominąć rolę bramkarza i kwestie związane z wysokością poprzeczki i nogi.

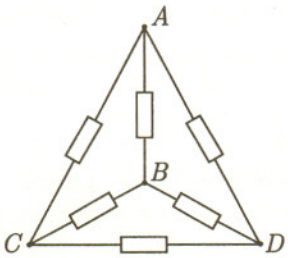
Rozwiązania zadań z fizyki z numeru 11/1996

Przypominamy treść zadań:

227. Wokół planety o masie M porusza się po okręgu księżyc o masie m i promieniu r, zwrócony do planety stale tą samą stroną. Jaki warunek musi spełniać promień R orbity księżyca (tzn. odległość środków obu ciał), aby kamienie leżące na powierzchni księżyca nie odrywały się od niego? Przyjąć, że planeta i księżyc są kuliste, $M \gg m$ i $R \gg r$.

228. Z pięciu oporników o oporze R i jednego o oporze R' utworzono obwód przedstawiony na rysunku 2; wiemy, że $R \neq R'$, ale nie znamy tych wartości. Oporniki wyglądają identycznie, więc aby ustalić, który jest „odmieńcem", mierzymy opór obwodu między dowolnie wybranymi węzłami (bez rozcinania połączeń i bez zwierania węzłów). W jaki sposób należy wykonywać te pomiary i jaka jest ich minimalna liczba gwarantująca możliwość wskazania opornika R' niezależnie od miejsca, gdzie jest ukryty?

Pytanie „poza konkursem": czy dopuszczenie możliwości zwierania węzłów pozwoli wykonać zadanie mniejszą liczbą pomiarów?



Rys. 2

227. Stosując II zasadę dynamiki do ruchu planety i księżyca wyznaczamy w standardowy sposób prędkość kątową wzajemnego obiegu ciał ω

$$\omega^2 = \frac{G(m+M)}{R^3} \approx \frac{GM}{R^3}.$$

Rozpatrzmy kamień o masie μ leżący na powierzchni księżyca w punkcie najbardziej odległym od planety. Będzie on pozostawał w spoczynku wtedy, gdy suma sił przyciągania go przez planetę i księżyc będzie większa od siły odśrodkowej (lub równa jej):

$$\frac{GM\mu}{(R+r)^2} + \frac{Gm\mu}{r^2} \geq \mu\omega^2(R+r).$$

Podstawmy tu ω^2 z poprzedniego wzoru oraz wprowadźmy przybliżenie

$$\frac{1}{(R+r)^2} \approx \frac{1}{R^2} - \frac{2r}{R^3}.$$

Po uproszczeniach otrzymujemy rozwiązanie w postaci warunku

$$\left(\frac{R}{r}\right)^3 \geq \frac{3M}{m}.$$

Łatwo sprawdzić, że warunek równowagi kamienia leżącego na księżycu w punkcie najbliższym planety ma identyczną postać. Spełnienie tego warunku gwarantuje też, że nie oderwą się od księżyca kamienie leżące w innych punktach.

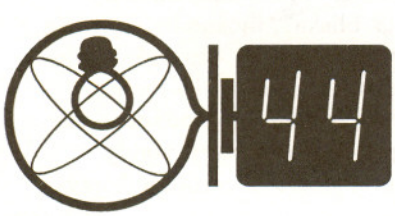
Jeśli dodatkowo założymy, że gęstość planety i księżyca jest taka sama, to warunek ten przyjmie postać

$$R \geq \sqrt[3]{3}R_p \approx 1{,}442R_p,$$

gdzie R_p jest promieniem planety. Otrzymany wynik dowodzi, że księżyc krążący zbyt blisko planety (wewnątrz tzw. strefy Roche'a) ulegnie rozerwaniu przez siły przypływowe. Podawana w podręcznikach wartość promienia strefy Roche'a to $2{,}455R_p$; różnica wynika stąd, że dopuszcza się możliwość płynnej zmiany kształtu księżyca, a nie tylko oderwania leżących kamieni od księżyca kulistego.

Czołówka ligi zadaniowej
Klub 44 F
po uwzględnieniu ocen rozwiązań zadań 223 (WT=3,28), 224 (WT=2,26) z numeru 9/1996

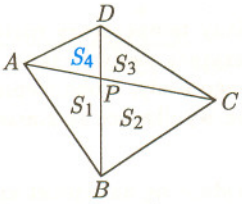
Aleksander Surma	– Myszków	43,62
Przemysław Gworys	– Częstochowa	38,52
Przemysław Gadziński	– Środa Śl.	31,28
Andrzej Idzik	– Bolesławiec	30,93

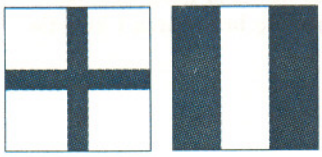


Rozwiązanie zadania M 802. Jeżeli dwa trójkąty mają wspólną wysokość, to stosunek ich pól jest równy stosunkowi długości ich podstaw. Stosując to twierdzenie dwukrotnie widzimy (patrz rysunek), że

$$\frac{S_1}{S_2} = \frac{AP}{PC} = \frac{S_4}{S_3}.$$

Stąd, oczywiście, $S_4 = S_1 S_3 / S_2$.





XT – Spodziewana jest zła pogoda.

228. Są trzy możliwe wyniki pomiaru:
a) Gdy opornik R' leży między węzłami pomiarowymi (oznaczamy je literami A i B), przez gałąź CD nie płynie prąd. Nietrudno sprawdzić, że opór jest wtedy dany wzorem $R_1 = RR'/(R+R')$.
b) Gdy opornik R' leży między węzłami C i D, prąd również tą gałęzią nie płynie, a opór między A a B wynosi $R_2 = (1/2)R$.
c) Gdy opornik R' zajmuje którekolwiek z pozostałych położeń, obliczenie oporu między A a B jest nieco bardziej pracochłonne, a w wyniku otrzymuje się

$$R_3 = \frac{R(3R+5R')}{8(R+R')}.$$

Minimalną liczbą pomiarów jest 4. Należy rozpocząć od dwóch pomiarów, dla których jeden węzeł jest wspólny – np. AB i AC. W razie stwierdzenia, że $R_{AB} = R_{AC}$, łatwo dojść do wniosku, że opornik R' może się ukrywać tylko w dwóch miejscach: między A a D lub między B a C. Mierzymy opory R_{AD} i R_{BC}, tak że dysponujemy kompletem wartości R_1, R_2 i R_3, a korzystając ze związku

$$(*) \qquad 4R_3 = R_1 + 3R_2$$

można ustalić, który ze zmierzonych oporów jest równy R_1, a który R_2 – co kończy poszukiwania. Jeśli natomiast okazało się, że $R_{AB} \neq R_{AC}$, to jako trzeci zmierzmy opór R_{BD} (można wybrać inaczej). Gdy ten opór jest różny od obu poprzednich, to czwarty pomiar okazuje się niepotrzebny, gdyż znów mamy komplet wyników R_1, R_2 i R_3 i możemy postępować tak, jak powyżej. Gdy zaś $R_{BD} = R_{AC}$ (przypadek $R_{BD} = R_{AB} \neq R_{AC}$ jest niemożliwy), opornik R' może się ukrywać zarówno między A a B, jak między C a D, więc konieczny jest jeszcze pomiar R_{CD}.

Wprowadzenie możliwości zwierania dwóch lub trzech węzłów bardzo komplikuje zadanie. W zasadzie można tak dokonać pomiarów (wszystkie z jednym zwarciem), aby dopasowując wyniki do wzorów analogicznych do związku $(*)$ można było rozwiązać zadanie trzema pomiarami. Wzory te są jednak o wiele bardziej skomplikowane, a ponadto przy „złośliwym" doborze stosunku R/R' rozwiązanie może nie być jednoznaczne.

Patrz w niebo

Merkury, najbliższa Słońca planeta, jest z natury rzeczy najsilniej wyprażonym globem w Układzie Słonecznym. Choć brzmi to nieprawdopodobnie, uzyskano niedawno argumenty za tym, że na biegunach Merkurego zalegają miejscami znaczne ilości wodnego lodu. Pierwsze informacje o tym pojawiły się w 1991 r., gdy przy obu biegunach planety stwierdzono obecność obszarów bardzo silnie odbijających fale radarowe. Dalsze badania potwierdziły, że tak odbijać fale radarowe może właściwie tylko lód.

Maksymalna temperatura gruntu na Merkurym przekracza 550°C, ale tak jest, oczywiście, w pasie równikowym, gdzie nasłonecznienie jest najsilniejsze. Od szerokości planetograficznej około ±80° ku biegunom rozciągają się tereny charakteryzujące się tym, że wnętrza występujących tam kraterów nigdy nie są wystawione na bezpośrednie promienie Słońca. Te wiecznie ocienione miejsca nigdy nie osiągają temperatury wyższej niż −160°C, przez co mogą stanowić przechowalnię zamarzającej wody pochodzącej bądź z wnętrza planety, bądź dostarczanej od przypadku do przypadku np. przez komety.

Okołobiegunowe obszary Merkurego są wprawdzie osłonięte przed Słońcem, lecz od czasu do czasu stają się widoczne z Ziemi, ponieważ orbita planety leży w płaszczyźnie tworzącej kąt 7° z płaszczyzną ekliptyki. Wtedy właśnie jest okazja wniknięcia falami radarowymi do wiecznie ciemnych wnętrz niektórych kraterów. Takie badania prowadzone były w latach 1991–92 za pomocą 300-metrowego radioteleskopu w Arecibo na Puerto Rico. Rozkład lodowych plam zgadzał się z konfiguracją biegunowych kraterów znaną od czasu, gdy Mariner 10 sfotografował powierzchnię planety. Dalsze prace polegały na badaniu zmian polaryzacji fal radarowych przy odbiciu od Merkurego. Używano do tego 70-metrowego radioteleskopu w Goldstone w Kalifornii. Potwierdzono w ten sposób, że fale odbijają się od lodu, gdyż podobne skutki oddziaływania fal radarowych z lodem obserwowano w przypadku czap polarnych Marsa oraz lodowych satelitów Jowisza. Lód w kraterach Merkurego ma co najmniej kilka metrów grubości, a przykrywa go zapewne kilkudziesięciocentymetrowa warstwa pyłu chroniąca go przed słabym, lecz nieustannym promieniowaniem z Kosmosu.

Uważa się, że gdyby dało się przebadać warstwy merkuriańskiego lodu „z bliska", można by się wiele dowiedzieć o ewolucji wewnętrznych obszarów Układu Słonecznego. O lądowaniu tam człowieka nie ma jeszcze co marzyć, lecz – jak sugerują badacze – już umieszczenie na okołoplanetarnej orbicie sondy z aparaturą radarową przyniosłoby ogromne korzyści naukowe.

Tomasz KWAST

epsilon

3/97
(72)

Waldkowe rozwiązania zadań świątecznych

W *Delcie* 12/1996 redakcja *EPSILONA* zaproponowała Czytelnikom konkurs świąteczny prezentując pięć zadań nadesłanych przeze mnie. „Waldkowe zadania na święta" nie są oryginalne i większość z nich zaczerpnąłem z kanadyjskiego czasopisma *Crux Mathematicorum*. Być może część Czytelników dopiero teraz polubi te zadania, widząc „epsilonowe" rozwiązania.

1. *Sześć spośród ośmiu wierzchołków równoległościanu leży na jednej sferze. Czy równoległościan ten musi być prostopadłościanem?*

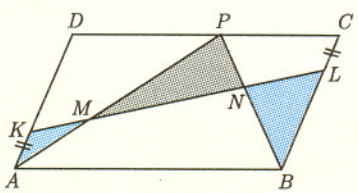
Nie. Na przykład wierzchołki dwóch sąsiednich ścian bocznych graniastosłupa prostego o podstawie równoległoboku leżą na jednej sferze. (Ściany boczne takiego graniastosłupa są prostokątami.)

2. *Na bokach AD i BC równoległoboku $ABCD$ tak obrano punkty K i L, że $AK = LC$. Niech P będzie dowolnym punktem leżącym na boku CD. Prosta KL przecina proste AP i BP odpowiednio w punktach M i N. Wykazać, że* pole$\triangle AKM$ + pole$\triangle BLN$ = pole$\triangle PMN$.

Dodając do obu stron powyższej równości pole czworokąta $ABNM$ (rys. 1) pozostaje do wykazania, że pole czworokąta $ABLK$ jest równe polu trójkąta ABP. A to już jest łatwe, bowiem obie te wielkości są równe połowie pola równoległoboku $ABCD$.

3. *Wewnątrz trójkąta równobocznego ABC obrano (w sposób dowolny) punkt P. Niech D, E, F będą rzutami prostokątnymi punktu P odpowiednio na boki BC, CA, AB. Udowodnić, że suma pól trójkątów PAF, PBD, PCE nie zależy od wyboru punktu P.*

Przez punkt P prowadzimy trzy proste równoległe do boków trójkąta ABC (rys. 2). Teraz już nietrudno zauważyć, że suma pól trójkątów PAF, PBD, PCE jest równa połowie pola trójkąta ABC, czyli nie zależy od wyboru punktu P.



Rys. 1

4. *Niech $n > 2$ będzie liczbą naturalną. Czy istnieją liczby całkowite x, y, z, wszystkie różne od zera, spełniające równanie: $(x^{2n} + y^{2n} + z^{2n})^2 = 2(x^{4n} + y^{4n} + z^{4n})$?*

Takie liczby nie istnieją. Dane równanie jest równoważne równaniu

$$(x^n+y^n+z^n)(-x^n+y^n+z^n)(x^n-y^n+z^n)(x^n+y^n-z^n)=0,$$

które, na mocy Wielkiego Twierdzenia Fermata, nie ma rozwiązań spełniających warunki zadania.

5. *Czy istnieją takie liczby naturalne $1 < k < l < n$, że liczby $\binom{n}{k}$ i $\binom{n}{l}$ są względnie pierwsze?*

Nie, nie istnieją! Z łatwej do sprawdzenia tożsamości $\binom{n}{k}\binom{n-k}{l} = \binom{n}{l}\binom{n-l}{k}$ wynika, że gdyby $\binom{n}{k}$ i $\binom{n}{l}$ były względnie pierwsze, to liczba $\binom{n}{k}$ musiałaby dzielić liczbę $\binom{n-l}{k}$. To jednak jest niemożliwe, gdyż $\binom{n-l}{k} < \binom{n}{k}$.

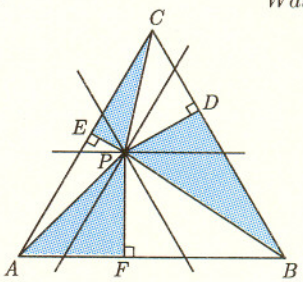
Autorem ostatniego zadania jest słynny węgierski matematyk Pál Erdős. Zwykł był on oferować (niekiedy bardzo wysokie) nagrody pieniężne za rozwiązania problemów matematycznych, z którymi sam się zmagał i których był autorem. Sam potrafił ocenić trudność danego problemu i oferować adekwatną sumę.

Na jednej z konferencji Erdős podzielił się powyższym problemem ze swoim przyjacielem, australijskim matematykiem, Georgem Szekeresem, zaznaczając, że nie zna rozwiązania i zadanie to może być nietrywialne. Podczas wykładu Szekeresowi udało się znaleźć rozwiązanie problemu Erdősa, podobne do powyższego. Na przerwie podszedł więc do autora zadania i z poważną miną powiedział:
– Wygląda mi to na interesujący problem. Ile zaoferowałbyś za rozwiązanie?
– Och, 5 dolarów... – odpowiedział bez wahania Erdős. *Muszę powiedzieć, że Paul mi zapłacił i był to jedyny raz, kiedy w ten sposób zarobiłem od niego pieniądze – niewątpliwie niezbyt uczciwie* – wspomina George Szekeres w liście do redaktora pisma *Crux Mathematicorum*.

Po 16 latach panowie spotkali się ponownie na konferencji w 1993 roku poświęconej 80. urodzinom Paula Erdősa. Erdős postawił ten sam problem raz jeszcze, po czym obaj z Szekeresem doszli do wniosku, że może on być niełatwy! Minęło kilka tygodni, zanim Erdős (przypadkowo, przeglądając swoje notatki) przypomniał sobie, że kilkanaście lat temu, razem z Szekeresem opublikowali to zadanie! Można o nim oraz o innych (otwartych) problemach dotyczących symboli Newtona przeczytać w pracy:

Paul Erdős, George Szekeres, *Some number theoretic problems on binomial coefficients*, Australian Math. Soc. Gazette **5(1978)**, str. 97–99.

Waldemar POMPE



Rys. 2