

SPIS TREŚCI NUMERU 1 (320)

Najbliższe gwiazdy <i>Tomasz Kwast</i>	str. 1
Zabawy z kalkulatorem (I) <i>Piotr Hajłasz</i>	str. 2
Krzywe eliptyczne <i>Jerzy Konarski</i>	str. 4
Krzywe eliptyczne i kryptografia <i>Wojciech Guzicki</i>	str. 6
Mała Delta	str. 7
Błysk szybszy niż światło <i>Stanisław Mrówczyński</i>	str. 8
Tylko Pitagoras	str.10
Zadania	str.11
Aktualności (nie tylko) fizyczne	str.12
Konkurs Uczniowskich Prac z Matematyki	str.13
Klub 44	str.14
Patrz w niebo	str.16
Styczeń	str.16
Gammalimatias	str.17

W następnym numerze:
Wszechświat i pustka

Okładki i ilustracje: *Anna Ludwicka*
Rysunki techniczne: *Marcin Adamski*

Wybór artykułów w języku angielskim
<http://www.mimuw.edu.pl/delta/>

Wydawca: Uniwersytet Warszawski

Cena 1 egzemplarza 3 zł

„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.

Komitet Redakcyjny:

Redaguje kolegium w składzie:

Andrzej Białynicki-Birula
Bogdan Cichocki
– wiceprzewodniczący
Krzysztof Ciesielski
Jan A. Gaj
Piotr Goldstein
Andrzej Hryniewicz
Wiesław A. Kamiński
Marta Kicińska-Habior
Krzysztof Maślanka
Janusz Matkowski
Andrzej Mąkowski
Zdzisław Pogoda
Michał Różycka
Konrad Rudnicki
Grzegorz Sitarski
Andrzej Woszczyk
Eligiusz Złotkiewicz
Wiesław Żelazko – przewodniczący

Wiktor Bartol
Krzysztof Biesaga
Ewa Czuchry
Krystyna Kordos – sekr. red.
Marek Kordos – red. nac.
Tomasz Kwast
Anna Ludwicka
Anna Rudnik
Witold Sadowski
Joanna Udalska
Anna Wojtyra
Piotr Zalewski – z-ca red. nac.

Adres Redakcji:
ul. Smyczkowa 5/7, 02-678 Warszawa
tel. 853-59-61
BARTOL@MIMUW.EDU.PL
Skład systemem T_EX wykonała Redakcja.

Wydrukowano
w Drukarni Naukowo-Technicznej S.A.
w Warszawie, ul. Mińska 65.

WARUNKI PRENUMERATY W FIRMIE AMOS

01-806 Warszawa, ul. Zuga 12 (tel. 834-65-21)
Wpłaty przyjmowane są non-stop, do 10. dnia miesiąca poprzedzającego okres prenumeraty. **Okres prenumeraty wynosi co najmniej trzy (3) miesiące.** Cena jednego numeru w 2001 roku wynosi 3 zł. Przy wpłacie prosimy o zaznaczenie okresu prenumeraty.

W prenumeracie zagranicznej (też przez okres **co najmniej trzech miesięcy**) cena numeru w 2001 r. wynosi 6 zł. W przypadku życzenia dostawy drogą lotniczą odpowiednią dopłatę ponosi zamawiający.

Uwaga! Dla zamawiających minimum 10 egzemplarzy każdego numeru AMOS funduje dodatkowo jeden egzemplarz pisma.

Konto AMOS-u: **PKO BP VIII O/W-wa, nr 10201084-77578-270-1-111**

WARUNKI PRENUMERATY W RUCH-u

1. Wpłaty na prenumeratę przyjmowane są tylko na okresy kwartalne.
2. Cena prenumeraty na II kwartał 2001 r. wynosi 9 zł.
3. Wpłaty na prenumeratę przyjmują na teren kraju jednostki kolportażowe „Ruch” S.A. właściwe dla miejsca zamieszkania lub siedziby prenumeratora.
4. Cena prenumeraty ze zleceniem dostawy za granicę: cena prenumeraty + rzeczywiste koszty wysyłki. Zlecenia na prenumeratę dewizową, przyjmowane od osób zamieszkałych za granicą, realizowane są od dowolnego numeru.

Wpłaty przyjmuje Oddział Krajowej Dystrybucji Prasy „RUCH” SA na konto: Pekao SA IV O/W-wa 12401053-40060347-2700-401112-001 lub kasa Oddziału.

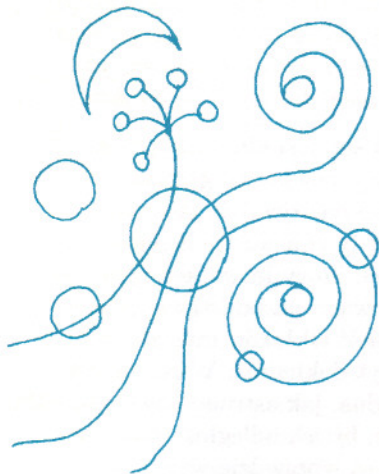
5. Informacji o warunkach prenumeraty i sposobie zamawiania udziela „RUCH” SA OKDP, 00-958 Warszawa, skrytka pocztowa 12, ul. Jana Kazimierza 31/33, lub telefonicznie: (22) 5328-731, 5328-820, 5328-816, fax: 5328-732, internet: www.ruch.pol.pl, e-mail: prenumerata@okdp.ruch.com.pl
6. Terminy przyjmowania wpłat na prenumeratę krajową i zagraniczną

do 5 XII	– na I	kwartał roku następnego,
do 5 III	– na II	kwartał roku bieżącego,
do 5 VI	– na III	kwartał roku bieżącego,
do 5 IX	– na IV	kwartał roku bieżącego,

Numery archiwalne (od 1985 r.) można nabyć w Redakcji osobiście lub listownie.

Najbliższe gwiazdy

Tomasz KWAST



Nie ma chyba prostszej metody pomiaru odległości niż na zasadzie dalmierza. Wynik pomiaru nie zależy od cech mierzonego obiektu, od przezroczystości przestrzeni, po prostu z dwóch miejsc obserwacji, które dzieli znana odległość (jest to tzw. baza), mamy dwa kierunki ku obiektowi i z prostej trygonometrii wyznacza się „długość” zazwyczaj bardzo spiczastego trójkąta, czyli odległość obiektu. Baza dalmierzy stosowanych w aparatach fotograficznych wynosi kilka centymetrów, co wystarcza, by ustawić ostrość w aparacie. Aby trafić w nieprzyjacielski okręt z odległości kilku mil, trzeba jego odległość znać dokładniej, dlatego morskie dalmierze mają już kilka metrów. A do wyznaczania odległości kosmicznych trzeba dalmierza o rozmiarach też kosmicznych. Przyroda stworzyła taki dalmierz – jest nim Ziemia, której położenie dziś i za pół roku wyznacza bazę o długości średnicy ziemskiej orbity, czyli 300 mln km. Przy takiej zmianie miejsca obserwator powinien dostrzec przesunięcia gwiazd bliskich na tle bardzo odległych. Zdziwiająco, jak długo nie dawało się tych przesunięć (paralaks) zaobserwować i zmierzyć. Teraz wiemy, jaką naiwnością były próby mierzenia paralaks gwiazd w czasach przedteleskopowych. Oko jest w stanie zauważyć kąt nie mniejszy od $1'$, a brak takich paralaks uważany był za dowód nieruchomości Ziemi. W tym m.in. genialność Kopernika, że wbrew powszechnej opinii pisał w I księdze „O obrotach”: *Jeżeli zaś nic podobnego nie dostrzegamy u gwiazd stałych, dowodzi to, że się znajdują niezmiernie wysoko nad nami...* Jeszcze długo po Koperniku nawet astronomom w głowach nie mieściło się, że gwiazdy mogą być tak daleko.

Pierwsze udane pomiary paralaks datują się na rok 1837. Wymienia się tu zazwyczaj trzy nazwiska: Bessela, Struvego i Hendersona, którzy niemal jednocześnie wyznaczyli odległości trzech gwiazd. Dość niezwykły – z naszego punktu widzenia – był przyrząd użyty przez Bessela. Był to tzw. heliometr, czyli teleskop, którego obiektyw rozcięty był wzdłuż średnicy, obie jego połówki można było przesuwać za pomocą śruby mikrometrycznej, a całość można było jeszcze obracać wokół osi optycznej teleskopu. Każda połówka obiektywu dawała niezależny obraz np. dwóch gwiazd, których kątową odległość należało zmierzyć. W tym celu należało przede wszystkim obrócić obiektyw tak, by kierunek jego rozcięcia pokrył się z kierunkiem łuku łączącego obie gwiazdy, a następnie przesunąć połówki obiektywu tak, by np. lewy obraz jednej gwiazdy pokrył się z prawym obrazem drugiej. Przy znanej ogniskowej teleskopu można było stąd określić kątową odległość gwiazd. Struve mierzył kątowne odległości gwiazd mikrometrem umieszczonym w polu widzenia okularu teleskopu. Tak czy inaczej paralaksy trzech gwiazd, skądinąd podejrzanych o to, że są stosunkowo bliskie, okazały się poniżej $1''$. Bessel wyznaczył paralaksę gwiazdy 61 Cygni ($0''35$), Struve Węgi ($0''25$). Henderson trafił najlepiej, bo w Capetown obserwował α Centauri, czyli Tolimana ($1''$), która jest w ogóle gwiazdą najbliższą Słońca („z dokładnością do Proximy”, która znajduje się trochę bliżej, ale należy do układu α Centauri). Przytoczone tu wartości paralaks trochę różnią się od przyjmowanych obecnie.

I tak przez lata w wyniku mozolnych pomiarów powstawała stale uaktualniana tabela gwiazd najbliższych Słońca. Łatwo się domyślić, że znalazły się w niej gwiazdy najjaśniejsze, ze słabszych natomiast już tylko niektóre. Dopiero niedawno satelita Hipparcos (*Delta 7/2000*) wykonał ogromną pracę precyzyjnego zmierzenia położenia miliona gwiazd, w wyniku czego poznane zostały paralaksy, a więc i odległości wielu tysięcy gwiazd „za jednym zamachem”. Tabela najbliższych gwiazd gwałtownie się zmieniła. Na czele stoi nadal α Centauri (dwa składniki) i Proxima, ale już Gwiazda Barnarda, czwarta na liście w najpopularniejszym akademickim podręczniku astronomii Eugeniusza Rybki, znalazła się w katalogu Hipparcosa na miejscu 18. Kolejna, piąta gwiazda z „Rybki”, Wolf 359, w ogóle w katalogu Hipparcosa się nie znalazła jako zbyt słaba (13,5 mag), a miałyby paralaksę równą $0''430$. Szóstej z kolei,

Turniej młodych fizyków 2001

Pod auspicjami Polskiego Towarzystwa Fizycznego jest od kilku lat organizowany Turniej Młodych Fizyków dla uczniów szkół średnich. Jest to impreza różniąca się od Olimpiady Fizycznej m.in. charakterem zadań i sposobem prezentacji wyników. Zawody turniejowe przypominają konferencje naukowe z referatami i gorącą dyskusją, a uczestniczą w nich kilkoosobowe (z reguły pięcioosobowe) drużyny szkolne. W pierwszym etapie uczestnicy opracowują w domu lub szkole rozwiązania zadań turniejowych korzystając z wszelkich możliwych pomocy; z reguły wiąże się to z wykonywaniem doświadczeń. Prace turniejowe powinny być przesłane do jednego z dwóch ośrodków (w Katowicach lub Warszawie) w terminie do 15 lutego 2001 r. Na podstawie oceny nadesłanych prac nastąpi zakwalifikowanie drużyn do udziału w zawodach turniejowych organizowanych przez dany ośrodek. Najlepsze cztery drużyny zmierzą się następnie w finale Turnieju, w którym zarówno prezentacja, jak i dyskusja odbywają się po angielsku. Zwycięska drużyna będzie reprezentowała nasz kraj w Międzynarodowym Turniej Młodych Fizyków, który odbędzie się w Finlandii w maju 2001 r. Bliższe informacje oraz tematy zadań turniejowych można znaleźć na stronie internetowej <http://www.fuw.edu.pl/ptf/tmf.html>. Ewentualne zapytania można kierować do pana Andrzeja Nadolnego nadola@ifpan.edu.pl.



BD+36°2147, z paralaksą 0,402, też nie ma w spisie Hipparcosa zawierającym najbliższe 173 gwiazdy o paralaksach równych lub większych od 0,4 – widocznie jej paralaksa okazała się mniejsza. W sumie w tym spisie Hipparcosa gwiazd odległych najwyżej o 2,5 pc są tylko trzy gwiazdy jaśniejsze od 10 mag: dwa Tolimany i Gwiazda Barnarda. Jeśli otoczenie Słońca jest dość typowe, to w Galaktyce występuje bardzo wiele gwiazd znacznie słabszych od Słońca.

Odległości większe, międzygalaktyczne, wyznacza się pośrednio np. przez porównanie jasności obserwowanej i absolutnej najjaśniejszych gwiazd w galaktykach. Takimi „dobrymi” do tego celu, bo rzeczywiście jasnymi gwiazdami, są cefeidy, szczególnego rodzaju gwiazdy zmienne pulsujące. Ich jasności absolutne zależą od okresu zmian jasności, który łatwo jest zmierzyć. Ta zależność okres-jasność została kiedyś wyskalowana na podstawie cefeid należących do Obłoków Magellana, jednak odległość Obłoków musiała być już znana uprzednio i była znana, niestety, niezbyt dokładnie. W rezultacie fotometryczna skala odległości nie jest tak dokładna, jak astronomowie chcieliby, a to dlatego, że najbliższe cefeidy są zbyt odległe, by ich odległość dało się wyznaczyć z zadowalającą dokładnością. Hipparcos wprowadził paralaksy niemal 300 cefeid, gwiazdy te leżą jednak dość daleko, a wtedy ich paralaksy, ocenione formalnie np. na 0,002 i mniej, wyznaczane są już ze sporym błędem. Jedynie trzy cefeidy mają paralaksy wyznaczone z błędem mniejszym od 10% (najbliższą jest Gwiazda Polarna o paralaksie 0,007). Dlatego tak ważne są następne projekty satelitów zdolnych bezpośrednimi pomiarami sięgnąć jeszcze dalej.

Zabawy z kalkulatorem (I)

Piotr HAJŁASZ

Proponuję zabawę z kalkulatorem. Zamiast gry komputerowej. Może nie będzie aż tak fascynująca, ale wciągnąć też potrafi.

Jak znaleźć na kalkulatorze przybliżoną wartość $\sqrt{2}$, korzystając jedynie z dodawania, mnożenia i dzielenia?

Proponuję metodę prób i błędów, a raczej metodę kolejnego przybliżania się do oczekiwanego wyniku.

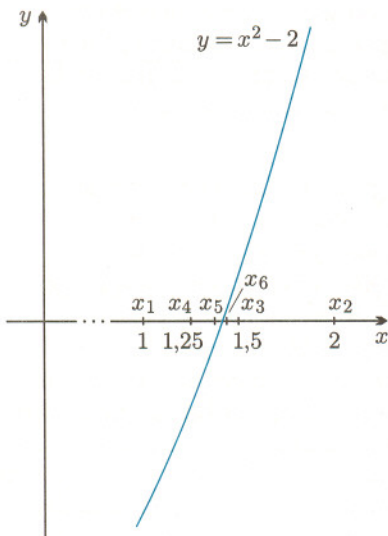
Popatrzmy: $1^2 < 2$, $2^2 > 2$, więc z rysunku widać, że $\sqrt{2}$ leży gdzieś między 1 i 2. Oznaczmy $x_1 = 1$ i $x_2 = 2$ i jako kolejnego kandydata na przybliżenie $\sqrt{2}$ weźmy punkt na środku $x_3 = \frac{1}{2}(x_1 + x_2) = 1,5$. Tym razem $x_3 = 2,25 > 2$, a więc powinniśmy szukać punktu na lewo od x_3 , kładziemy więc $x_4 = \frac{1}{2}(x_1 + x_3) = 1,25$. Skoro $x_4^2 = 1,5625 < 2$, więc szukamy na prawo od x_4 , a mianowicie $x_5 = \frac{1}{2}(x_4 + x_3) = 1,357$ itd.

Mam nadzieję, że procedura jest jasna. Kolejne punkty dzielą na pół przedział, do którego należy $\sqrt{2}$.

Najpierw mamy przedział $[x_1, x_2] = [1, 2]$ długości 1. Potem $[x_1, x_3] = [1, 1,5]$ długości 0,5. Następnie $[x_4, x_3] = [1,25, 1,5]$ długości 0,25 itd.

Na moim kalkulatorze można wyświetlić 8 cyfr, a więc $\sqrt{2}$ będzie mieć 7 cyfr po przecinku, czyli mogę podać przybliżenie $\sqrt{2}$ z dokładnością do $0,0000001 = 10^{-7}$. Zastanówmy się, jak dużo punktów x_1, x_2, x_3, \dots musimy znaleźć, zanim osiągniemy taką dokładność?

Długość przedziału, do którego należy $\sqrt{2}$, powinna się skrócić do długości mniejszej niż 10^{-7} . Po wyznaczeniu x_1 i x_2 mieliśmy przedział długości 1; po wyznaczeniu x_3 przedział długości $1/2 = 0,5$; po x_4 przedział długości $1/2^2 = 0,25$; po x_5 przedział długości $1/2^3$. Stąd już łatwo odczytać zależność: po wyznaczeniu x_n będziemy mieć przedział długości $1/2^{n-2}$.



Poniżej podajemy wartości liczb $x_1, x_2, x_3, x_4, \dots$. Dla zwięzłości będziemy używać pewnych skrótów w zapisie. I tak, na przykład, napis

$$x_{12} \{11, 9\} = 1,415039 \uparrow$$

będzie oznaczać, że $x_{12} = \frac{1}{2}(x_{11} + x_9)$, a strzałka do góry \uparrow , że $x_{12}^2 > 2$. Strzałka w dół \downarrow przy x_{15} będzie oznaczać, że $x_{15}^2 < 2$.

$$x_1 = 1 \downarrow$$

$$x_2 = 2 \uparrow$$

$$x_3 \{1, 2\} = 1,5 \uparrow$$

$$x_4 \{3, 1\} = 1,25 \downarrow$$

$$x_5 \{4, 3\} = 1,375 \downarrow$$

$$x_6 \{5, 3\} = 1,4375 \uparrow$$

$$x_7 \{6, 5\} = 1,40625 \downarrow$$

$$x_8 \{7, 6\} = 1,421875 \uparrow$$

$$x_9 \{8, 7\} = 1,4140625 \downarrow$$

$$x_{10} \{9, 8\} = 1,4179687 \uparrow$$

$$x_{11} \{10, 9\} = 1,4160156 \uparrow$$

$$x_{12} \{11, 9\} = 1,415039 \uparrow$$

$$x_{13} \{12, 9\} = 1,4145507 \uparrow$$

$$x_{14} \{13, 9\} = 1,4143066 \uparrow$$

$$x_{15} \{14, 9\} = 1,4141845 \downarrow$$

$$x_{16} \{15, 14\} = 1,4142455 \uparrow$$

$$x_{17} \{16, 15\} = 1,414215 \uparrow$$

$$x_{18} \{17, 15\} = 1,4141997 \downarrow$$

$$x_{19} \{18, 17\} = 1,4142073 \downarrow$$

$$x_{20} \{19, 17\} = 1,4142111 \downarrow$$

$$x_{21} \{20, 17\} = 1,414213 \downarrow$$

$$x_{22} \{21, 17\} = 1,414214 \uparrow$$

$$x_{23} \{22, 21\} = 1,4142135 \downarrow$$

$$x_{24} \{23, 22\} = 1,4142137 \uparrow$$

$$x_{25} \{24, 23\} = 1,4142136 \uparrow$$

$$x_{26} \{25, 23\} = 1,4142135 \downarrow$$

Otóż otrzymaliśmy dwie kolejne liczby x_{25} i x_{26} różniące się o 10^{-7} i takie, że $x_{25}^2 > 2$, $x_{26}^2 < 2$. A więc

$$1,4142135 < \sqrt{2} < 1,4142136$$

i nic lepszego już nie uzyskamy.

Chcemy, aby $1/2^{n-2} < 10^{-7}$, czyli $2^n > 40\,000\,000$. Mnożąc na kalkulatorze kolejno dwójki, widzimy, że

$$2^{25} = 33\,554\,432 < 40\,000\,000,$$

$$2^{26} = 67\,108\,864 > 40\,000\,000.$$

Przypuszczamy więc, że oczekiwane przybliżenie dostaniemy po znalezieniu x_{26} , czyli w 26 krokach. Wyniki kolejnych obliczeń na kalkulatorze podajemy na marginesie.

Tę samą metodę można, oczywiście, zastosować do rozwiązania innych problemów, takich jak, na przykład, znalezienie przybliżonej wartości $\sqrt[5]{7}$. Cóż, jeśli jednak nasz kalkulator wyposażony jest w funkcję obliczania pierwiastków, to powyższe zadanie można rozwiązać nieco szybciej...

Na szczęście, nawet dla bardzo zaawansowanych kalkulatorów inżynierskich łatwo jest wymyślić zadanie, którego nie da się na nim bezpośrednio rozwiązać, a które łatwo rozwiązać, stosując powyżej opisaną metodę kolejnych przybliżeń. Na przykład

Znajdź przybliżone rozwiązanie równania $2^x + x = 10$.

Ponieważ funkcja $y = 2^x + x$ jest ściśle rosnąca (bo ma dodatnią pochodną), równanie ma co najwyżej jedno rozwiązanie. Podstawiając $x_1 = 2$ i $x_2 = 3$, otrzymujemy kolejno wartości mniejszą i większą niż 10, co oznacza, że równanie ma (jedyne) rozwiązanie leżące pomiędzy 2 i 3. Jego przybliżoną wartość można wyznaczyć opisaną powyżej metodą kolejnych podziałów odcinka $[2, 3]$. Oczywiście, aby móc to zrobić, kalkulator musi być wyposażony w funkcję 2^x . Również i tym razem trzeba wykonać w przybliżeniu 26 kroków. To naprawdę dużo rachunków.

Cóż, nawet w przypadku znajdowania przybliżonej wartości $\sqrt{2}$ powyższa metoda prowadzi do mozolnych rachunków. Czy można znaleźć jakąś inną metodę, pozwalającą na szybsze rozwiązywanie zadań tego typu, co omawiane powyżej?

Tak, takie metody istnieją! Wymagają one użycia nieco bardziej zaawansowanych metod matematycznych. Tak to już z tą matematyką, niestety, jest. Trzeba się najpierw pomęczyć, ucząc się rzeczy, co do których nie zawsze jest jasne, po co one są, aby dopiero potem ujrzyć ich piękno i zdumiewającą użyteczność.

A propos tej użyteczności, to jak to w końcu jest z tym błyskawicznym znajdowaniem rozwiązań powyższych zadań? Cierpliwości! Ciąg dalszy w *Delcie* 3/2001.



Droga Redakcjo,

piszę ten list, gdyż jedna z informacji podanych w notce o liczbach Fermata w numerze 9/2000 (który z przyjemnością przeczytałem na tzw. obczyźnie) jest nieaktualna.

Mianowicie, wiadomo w tej chwili ponad wszelką rozsądną wątpliwość, że liczba $F_{24} = 2^{2^4} + 1$ jest złożona. Panowie Richard Crandall, Ernst Mayer i Jason Papadopoulos piszą w swoim preincipie z grudnia 1999 roku, że stwierdzili ów fakt korzystając z jednej z wersji tzw. testu Pepina (konkretnie, z twierdzenia głoszącego, że liczba $F_n = 2^{2^n} + 1$ jest pierwsza wtedy i tylko wtedy, gdy liczba $3^{(F_n-1)/2} + 1$ jest podzielna przez F_n). Potęgowanie trójki i obliczanie reszty z dzielenia zostało wykonane dwukrotnie, w sierpniu 1999 roku, za pomocą dwóch różnych programów, na dwóch różnych, fizycznie odseparowanych komputerach, z tym samym

wynikiem. Jak podaje Crandall, wymagało to około 10^{17} operacji – z grubsza biorąc tyle, ile potrzeba do wykonania cyfrowej wersji pełnometrażowego filmu Disneya. Dużo, biorąc pod uwagę, że uzyskana odpowiedź składa się w istocie z jednego bitu. Żaden czynnik pierwszy F_{24} oczywiście nie jest znany.

Następną w kolejce liczbą Fermata, o której nie wiadomo, czy jest pierwsza, czy złożona, jest teraz F_{31} , która ma 646 456 994 cyfry. Natomiast największą liczbą Fermata, o której coś jednak wiadomo, jest przypuszczalnie F_{35563} : 27 sierpnia 2000 roku niejaki Nestor Sergio de Aranjó Melo dowiedział się od swego komputera, że jest to liczba złożona, podzielna przez $357 \cdot 2^{35567} + 1$.

Serdeczne pozdrowienia,
Paweł STRZELECKI
18.09.2000 r.

Krzywe eliptyczne

Jerzy KONARSKI

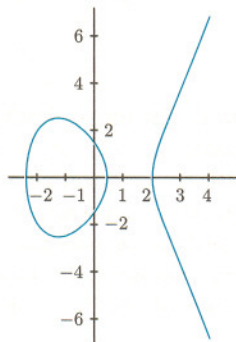
Za płaską krzywą algebraiczną stopnia n uważa się zwykle zbiór rozwiązań równania postaci $w(x, y) = 0$, gdzie $w(x, y)$ jest dowolnym wielomianem dwóch zmiennych stopnia $n > 0$. Na przykład równania $y - x^2 = 0$, $xy - 1 = 0$ i $xy = 0$ opisują krzywe stopnia 2 (parabolę, hiperbolę oraz parę prostych). Jedną z podstawowych własności płaskich krzywych algebraicznych to zależność między stopniem krzywej a liczbą jej punktów wspólnych z linią prostą. Mianowicie, dowolna prosta L albo przecina daną krzywą stopnia n w co najwyżej n punktach, albo jest w niej zawarta. Aby się o tym przekonać, wystarczy do równania krzywej $w(x, y) = 0$ podstawić postać parametryczną $x = at + b$, $y = ct + d$ prostej L . Otrzymujemy równanie zmiennej t , w którym po lewej stronie stoi wielomian $w_L(t) = w(at + b, ct + d)$ stopnia nie większego niż n . Jeśli ten wielomian nie jest wielomianem zerowym, to ma co najwyżej n pierwiastków, a każdemu pierwiastkowi odpowiada punkt przecięcia prostej L z krzywą.

Są trzy powody, dla których liczba punktów przecięcia może być mniejsza niż n . Po pierwsze, wielomian $w_L(t)$ może mieć stopień niższy niż n . Po drugie, nawet jeśli jest stopnia n , może się nie rozkładać na czynniki liniowe i w konsekwencji mieć mniej pierwiastków niż n . Po trzecie, może mieć tzw. pierwiastki wielokrotne. Sytuacja, w której jest mniej punktów przecięcia, sprawia pewien kłopot – wymyka się spod kontroli. W celu jej uniknięcia stosuje się następujące środki.

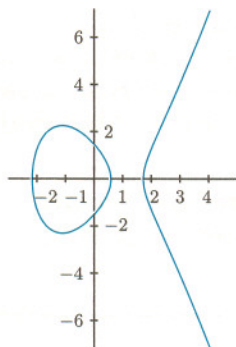
Po pierwsze, pierwiastki wielokrotne liczy się z ich krotnościami. Wtedy np. jedyny punkt wspólny paraboli $y - x^2 = 0$ i prostej $x = t + 1$, $y = 2t + 1$, który odpowiada pierwiastkowi podwójnemu $t = 0$ wielomianu $2t + 1 - (t + 1)^2$, jest liczony podwójnie. Sytuacja taka ma miejsce zawsze wtedy, gdy dana prosta jest styczna do krzywej – algebraiczna definicja prostej stycznej jest następująca: prosta $x = at + b$, $y = ct + d$ jest styczną do krzywej $w(x, y) = 0$ w punkcie (b, d) , jeśli krotność pierwiastka $t = 0$ równania $w(at + b, ct + d) = 0$ jest większa niż 1 (czyli wielomian $w_L(t)$ dzieli się przez t^2).

Po drugie, zamiast zwykłej płaszczyzny rozważa się tzw. płaszczyznę rzutową, która powstaje ze zwykłej płaszczyzny przez dołączenie tzw. punktów w nieskończoności, po jednym dla każdego kierunku prostych zawartych w płaszczyźnie. Wtedy uzyskujemy dodatkowe punkty przecięcia: np. prosta „pionowa” $x = 1$ przecina parabolę $y - x^2 = 0$ nie tylko w punkcie $(1, 1)$, ale także w punkcie w nieskończoności (nazwijmy go P) odpowiadającym kierunkowi „pionowemu”. Punkt P należy do prostej $x = 1$ i do paraboli, bo zarówno ta prosta, jak i parabola „mają w nieskończoności kierunek pionowy”. W przestrzeni rzutowej (w odpowiednio dobranym układzie współrzędnych) wielomian $w_L(t)$ będzie miał zawsze stopień n .

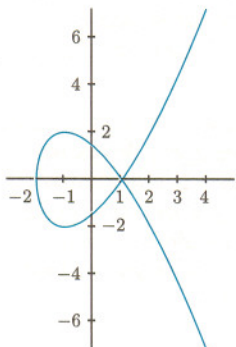
Trzecim środkiem jest stosowanie liczb zespolonych zamiast rzeczywistych jako współrzędnych punktów przestrzeni. Zachodzi twierdzenie: w zespolonej przestrzeni rzutowej dowolna prosta przecina krzywą stopnia n w dokładnie n punktach (licząc z krotnościami). Na przykład krzywa opisana równaniem $x^2 + y^2 = -2$ nie ma z prostą $x = y$ żadnych punktów wspólnych o współrzędnych rzeczywistych (bo sama krzywa nie ma takich punktów), ma natomiast punkty wspólne o współrzędnych zespolonych (i, i) oraz $(-i, -i)$.



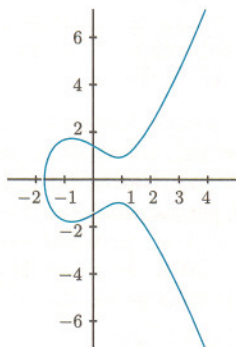
Rys. 1. $y^2 = x^3 - 5x + 2$.



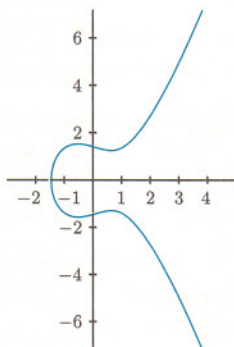
Rys. 2. $y^2 = x^3 - 4x + 2$.



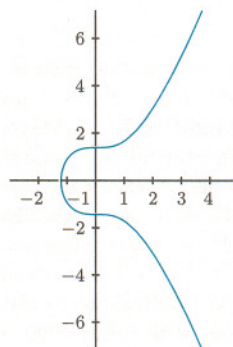
Rys. 3. $y^2 = x^3 - 3x + 2$.



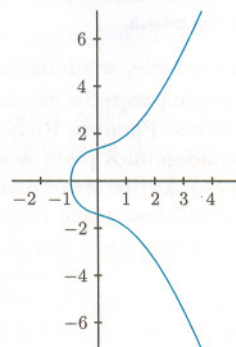
Rys. 4. $y^2 = x^3 - 2x + 2$.



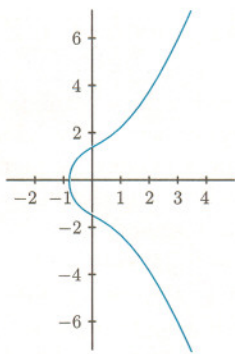
Rys. 5. $y^2 = x^3 - x + 2$.



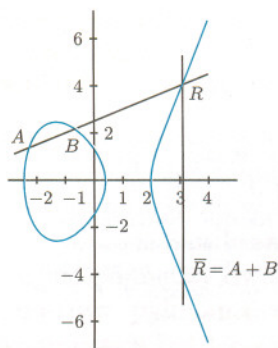
Rys. 6. $y^2 = x^3 + 2$.



Rys. 7. $y^2 = x^3 + x + 2$.



Rys. 8. $y^2 = x^3 + 2x + 2$.



Rys. 9. Dodawanie na krzywej $y^2 = x^3 - 5x + 2$. Elementem neutralnym jest punkt P w nieskończoności (kierunek pionowy).

Twierdzenie Mordella–Weila mówi, że grupa $E(\mathbb{Q})$ punktów \mathbb{Q} -wymiernych (czyli o obu współrzędnych będących liczbami wymiernymi) na krzywej eliptycznej E określonej nad ciałem liczb wymiernych jest grupą (przemianą) skończenie generowaną. Wiadomo, że każda taka grupa jest izomorficzna (może być ułożona) z grupą postaci $\mathbb{Z} \times \dots \times \mathbb{Z} \times \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r}$, gdzie \mathbb{Z} oznacza grupę liczb całkowitych z działaniem dodawania, a \mathbb{Z}_{m_i} oznacza grupę złożoną z liczb całkowitych $0, 1, 2, \dots, m_i - 1$ z działaniem dodawania modulo m_i . W przypadku grup $E(\mathbb{Q})$ liczby m_i nie mogą być dowolne: albo występuje tylko jedna i jest mniejsza od 13 i różna od 11, albo występują dwie i jedna z nich jest równa 2, a druga jest nie większa od 4. Czynniki postaci \mathbb{Z} może być nawet więcej niż 10, może ich też wcale nie być. Na przykład grupa punktów \mathbb{Q} -wymiernych krzywej opisanej równaniem $y^3 + x^3 = 1$ ma trzy elementy, a więc pasuje do powyższego opisu – jest izomorficzna z grupą \mathbb{Z}_3 .

Uwaga: niektóre stwierdzenia wymienione powyżej, np. postać równania opisującego krzywą eliptyczną, nie są prawdziwe dla ciał charakterystyki 2 i 3.

Ciekawszy przykład otrzymamy, biorąc krzywą $x^2 - y^2 = 2$. Ze wspomnianego twierdzenia wynika, że prosta $x = y$ ma z tą krzywą (w przestrzeni rzutowej nad ciałem liczb zespolonych) dwa punkty wspólne. Sprzeczność otrzymana z podstawienia $x = y$ oznacza tylko, że nie ma punktów wspólnych na zwykłej (afinicznej) płaszczyźnie, pozostaje więc tylko możliwość, iż jedynym punktem wspólnym jest punkt w nieskończoności odpowiadający prostej $x = y$ i liczony z krotnością dwa. Znaczy to, że nasza krzywa jest styczna do prostej $x = y$ w jej punkcie w nieskończoności.

Krzywe eliptyczne to krzywe opisane w płaszczyźnie rzutowej przez wielomian nierozkładalny stopnia 3 (a więc krzywe stopnia 3, nie zawierające prostej) i spełniające dodatkowo warunek gładkości: w każdym punkcie krzywej istnieje dokładnie jedna prosta styczna do niej. Nie są gładkie np. krzywe opisane równaniami $y^2 - x^3 - x^2 = 0$ oraz $y^2 - x^3 = 0$. Pierwsza ma w punkcie $(0, 0)$ dwie styczne $y = x$ i $y = -x$, druga ma w punkcie $(0, 0)$ styczną podwójną $y = 0$. Pomijając szczegóły, wspomnimy tylko, że gładkość jest równoważna gładkości w sensie intuicyjnym (tzn. brakowi ostrzy i punktów samoprzecięcia).

Własnością wyjątkową wśród krzywych jest to, że każda krzywa eliptyczna E ma naturalną strukturę grupy przemiennej, tzn. można określić działanie dodawania punktów, które jest łączne, przemienne, ma element neutralny oraz element przeciwny dla każdego elementu. Konstrukcja tego działania dodawania opiera się na tym, że dowolna prosta przechodząca przez dwa punkty A i B , leżące na E , ma z E jeszcze dokładnie jeden punkt wspólny (wielomian $w_L(t)$ jest stopnia 3 i ma dwa pierwiastki, więc na mocy twierdzenia Bézouta musi mieć także i trzeci). Punkty liczymy, oczywiście, z krotnościami, a więc np. jeśli $A = B$, mamy na myśli prostą styczną do E w punkcie A . Najpierw wybieramy dowolny punkt $O \in E$, który będzie pełnił rolę elementu neutralnego działania. Dla każdego punktu $C \in E$ symbolem \bar{C} oznaczamy trzeci punkt wspólny z E prostej OC . Niech A i B będą punktami E i niech prosta AB przecina E jeszcze w punkcie R (rys. 9). Sumę $A + B$ określamy jako \bar{R} . Bardzo łatwe sprawdzenie przemienności ($A + B = B + A$) i neutralności zera ($A + O = A$) oraz nieco trudniejsze – istnienia elementu przeciwnego – zostawiamy Czytelnikowi. Dowód łączności (opuszczamy go ze względu na brak miejsca) wymaga już skorzystania z pewnych, nietrudnych zresztą, twierdzeń geometrii algebraicznej. W odpowiednim układzie współrzędnych każda krzywa eliptyczna jest opisana na płaszczyźnie równaniem postaci $y^2 = x^3 + ax + b$, w którym a i b są takimi liczbami, że wielomian $x^3 + ax + b$ nie ma pierwiastków wielokrotnych. Mówiąc ściślej, krzywa składa się z punktów (x, y) płaszczyzny spełniających to równanie oraz z punktu P w nieskończoności odpowiadającego kierunkowi pionowemu. Punkt P jest punktem przegięcia, tzn. styczna w tym punkcie przecina krzywą z krotnością 3. Wygodnie jest wybrać właśnie punkt P jako element neutralny działania dodawania. Wtedy, po pierwsze, dla każdego punktu R punkt \bar{R} jest położony symetrycznie do R względem osi x , a po drugie, jest to element przeciwny do R (rys. 9).

Na rysunkach 1–8 przedstawione są krzywe $y^2 = x^3 + ax + b$ dla $b = 2$ i a całkowitych od -5 do 2 . Dla $a = -3$ otrzymujemy krzywą z punktem samoprzecięcia, która nie jest krzywą eliptyczną. Do tej pory (nie mówiąc tego wyraźnie) rozpatrywaliśmy krzywe eliptyczne określone nad ciałem liczb rzeczywistych, tzn. takie, że współczynniki równań opisujących krzywe były liczbami rzeczywistymi. Również współrzędne wszystkich punktów na krzywej były liczbami rzeczywistymi, czyli rozpatrywaliśmy tylko tzw. punkty \mathbb{R} -wymierne. Otóż krzywe eliptyczne można w zasadzie bez żadnych kłopotów zdefiniować nad dowolnym ciałem, np. liczb zespolonych, wymiernych lub też jednym z ciał skończonych. Mimo że często nie przypominają krzywych jako zbiory, używa się dla nich nazwy „krzywe”. Krzywe eliptyczne określone nad ciałem liczb wymiernych, a także nad ciałami skończonymi odgrywają bardzo ważną rolę w teorii liczb ze względu na różne związki z innymi pojęciami.

Krzywa eliptyczna określona nad ciałem skończonym F ma, oczywiście, tylko skończenie wiele punktów F -wymiernych (o współrzędnych z ciała F). Krzywe takie znalazły zastosowanie m.in. w kryptografii.

Z artykułu J. Konarskiego dowiedzieliśmy się, że każda krzywa eliptyczna jest tzw. grupą przemienną, co oznacza, że punkty tej krzywej można elegancko dodawać.

Działanie dodawania w grupie przemienniej E ma następujące własności:

1. jeśli $P \in E$ i $Q \in E$, to $P + Q \in E$,
2. $P + Q = Q + P$,
3. $(P + Q) + R = P + (Q + R)$,
4. istnieje taki punkt $O \in E$, że $P + O = P$ dla każdego $P \in E$,
5. dla każdego $P \in E$ istnieje taki punkt $-P \in E$, że $P + (-P) = O$.

Warto wspomnieć, że punkty krzywej eliptycznej można również dość łatwo reprezentować w komputerze (za pomocą ich współrzędnych, tzn. jako pary liczb) oraz że działanie dodawania jest opisane stosunkowo prostymi wzorami, a więc czas wykonania działania dodawania dwóch punktów przez komputer nie jest bardzo długi.

Te własności krzywych eliptycznych pozwalają wykorzystać je w kryptografii. Spróbujmy zatem popatrzeć, jak można wykorzystać dowolną grupę E do szyfrowania. Częstym problemem, z jakim muszą zmierzyć się osoby korespondujące w sposób tajny, jest przesłanie klucza. Jeśli, na przykład, osoba A często wysyła do osoby B zaszyfrowane komunikaty i każdy z tych komunikatów szyfruje za pomocą innego klucza (a w przypadku wielu systemów kryptograficznych jest to niezbędny warunek bezpieczeństwa), to osoba B musi równie często przysyłać osobie A klucze używane do szyfrowania. Oczywiście, osoba A mogłaby sama tworzyć te klucze, ale musiałaby przysyłać je osobie B w sposób całkowicie bezpieczny – tylko po co wtedy całe to szyfrowanie, jeśli można po prostu przesyłać w ten bezpieczny sposób każdy list? Na ogół jednak jest tak, że używamy szyfrowania wtedy, gdy nie jesteśmy w stanie przesyłać bezpiecznie wiadomości w żadną stronę i osoba B nie będzie mogła przesyłać kluczy osobie A . Co w takim razie zrobić? Odpowiedzią może być zastosowanie metody wymiany klucza Diffiego i Hellmana, opracowanej w 1976 roku, pozwalającej ponadto na jednakowy wpływ osoby A i B na tworzenie klucza.

Osoby A i B uzgadniają wspólnie pewną grupę E i wybierają element $P \in E$. Mogą to zrobić jawnie. Następnie osoba A wybiera dowolną liczbę naturalną a i osoba B wybiera liczbę b . Te liczby są wybierane w sposób tajny i nieujawniane nikomu. Następnie osoba A tworzy element $a \cdot P$ grupy E (używamy tu oczywiście skrótu: $2 \cdot P = P + P$, $3 \cdot P = P + P + P$ itd.) i podobnie osoba B tworzy element $b \cdot P$. Teraz osoby A i B wysyłają do siebie tak utworzone elementy. Na końcu osoby A i B tworzą element $Q = a \cdot b \cdot P$. Każda z nich ma wystarczającą ilość informacji potrzebnych do tego: osoba A zna liczbę a i element $b \cdot P$, osoba B zna liczbę b i element $a \cdot P$.

Na ogół wybiera się bardzo dużą grupę E , np. mającą około 10^{100} elementów i odpowiednio duże liczby a i b .

Mimo tego, że te liczby są bardzo duże, istnieją sposoby pozwalające dość szybko wyznaczyć element $a \cdot P$. Teraz cała korespondencja między osobami A i B może odbywać się w sposób jawny. Każdy będzie znał grupę E , element P oraz elementy $a \cdot P$ i $b \cdot P$. Nie będzie jednak mógł poznać elementu $a \cdot b \cdot P$. Do tego, gdyby chciał powtórzyć postępowanie którejs z osób A i B , musiałby poznać jedną z liczb a i b , a te liczby są przecież trzymane w tajemnicy! Okazuje się, że nie znamy dotychczas żadnej wystarczająco szybkiej metody obliczania liczby a , gdy znane są elementy P i $a \cdot P$. Podobnie nie znamy żadnej wystarczająco szybkiej metody wyznaczania $a \cdot b \cdot P$, gdy znane są $a \cdot P$ i $b \cdot P$. Na tym polega bezpieczeństwo tej metody wymiany klucza.

Żeby szybko wyznaczyć element $a \cdot P$, obliczamy elementy

$$2 \cdot P, 4 \cdot P, 8 \cdot P, \dots, 2^n \cdot P$$

dla takiej liczby n , by $2^{n+1} > a$. Następnie dodajemy pewne z tak wyznaczonych elementów (w zależności od postaci rozkładu dwójkowego liczby a), otrzymując $a \cdot P$. Jeśli, na przykład, chcemy wyznaczyć element $11 \cdot P$, to obliczamy $2 \cdot P$, $4 \cdot P$ i $8 \cdot P$, a następnie dodajemy $8 \cdot P$, $2 \cdot P$ i P : bowiem

$$11 = 8 + 2 + 1 = 2^3 + 2^1 + 2^0.$$

Ta metoda obliczania wielokrotności elementu P jest bardzo szybka: wymaga liczby dodawań równej co najwyżej, podwojonej liczbie cyfr w rozwinięciu dwójkowym liczby a .

Teraz, gdy obie osoby A i B wspólnie stworzyły tylko im znany sekret, mogą wykorzystać go w taki sam, wcześniej uzgodniony, sposób do stworzenia klucza szyfrującego. Można powiedzieć, że element $a \cdot b \cdot P$ grupy E jest tym kluczem. System wymiany klucza Diffiego i Hellmana został stworzony dla grupy reszt z dzielenia przez dużą liczbę pierwszą p z działaniem mnożenia, ale, oczywiście, może być zastosowany do dowolnej grupy. Warunkiem jest to, by grupa była duża (a dokładniej, by istniały takie elementy P , że jest dużo różnych elementów postaci P , $2P$, $3P$ itd. – mówimy wtedy, że element P ma duży rząd). Oczywiście, wszystkie te działania muszą być wykonywane za pomocą komputera, więc elementy grupy muszą się dawać łatwo reprezentować i działanie grupowe musi być wykonywane łatwo i szybko. Grupy punktów krzywych eliptycznych mają te wszystkie własności i dlatego już dość dawno (w końcu lat osiemdziesiątych) dostrzeżono ich zalety kryptograficzne.

Wielką zaletą krzywych eliptycznych jest to, że jest ich bardzo dużo. Można się obawiać, że systemy kryptograficzne wykorzystujące wyłącznie grupę reszt z dzielenia przez p z działaniem mnożenia zostaną kiedyś złamane. Ta grupa ma stosunkowo najlepiej poznaną strukturę i dlatego najbardziej możemy się obawiać o bezpieczeństwo systemów wykorzystujących ją. Różnych rodzajów krzywych eliptycznych jest bardzo wiele i możemy mieć nadzieję, że będzie znacznie trudniej znaleźć jakąś metodę ogólną pozwalającą złamać wszystkie systemy kryptograficzne wykorzystujące te krzywe.



Schemat mostu wiszącego.

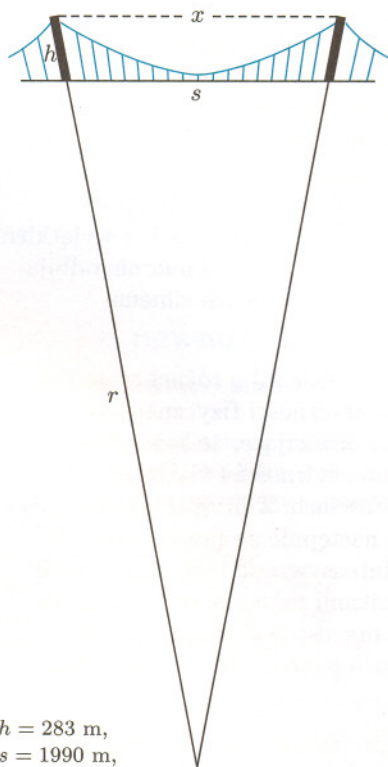
A jednak jest okrągła

Jednymi z najokazalszych budowli są mosty wiszące. Wśród nich bodajże najbardziej znanym jest oddany do użytku w 1937 roku Golden Gate Bridge w Zatoce San Francisco. Główne przęsło zawieszone pomiędzy dwiema monumentalnymi wieżami (tzw. pylonami) ma 1280 m długości. W swoim czasie był to rekord, został on jednak wielokrotnie pobity. Obecnym rekordzistą jest japoński most Akashi Kaikyo ukończony w 1998 r. Cały most liczy 3910 m długości, a jego główne przęsło o rekordowej długości 1990 m zawieszone jest pomiędzy pylonami wysokimi na 283 metry. Aby wyobrazić sobie wielkość tej konstrukcji, pomyśl, Drogi Czytelniku, o dwóch konkretnych miejscach w Twoim mieście odległych o cztery

kilometry. Pomiedzy nimi zawieś w wyobraźni most. Podczep go do dwóch stalowych lin, każdej grubej na metr, a liny te przeciągnij przez wierzchołki dwóch wież Eiffła odległych o dwa kilometry!

Na tym jednak nie koniec! W fazie projektów czai się kolejny rekordzista. Ma nim być most łączący Sycylię z czubkiem włoskiego buta. Łącznie pięć kilometrów z głównym przęsłem długim na 3300 m.

Zastanówmy się, czy przy tak olbrzymich konstrukcjach da się zauważyć kulistość Ziemi. Przeprowadźmy obliczenia dla mostu Akashi Kaikyo. Olbrzymie pylony, na których zawieszona jest cała konstrukcja, są skierowane do środka



Ziemi. Ponieważ Ziemia jest (w przybliżeniu) kulą, więc nie są one idealnie równoległe. Czy da się to zauważyć? Obliczmy różnicę pomiędzy odległościami podstaw pylonów i odległościami ich wierzchołków.

Pylony mają wysokość $h = 283$ m, a ich podstawy odległe są o $s = 1990$ m. Przyjmijmy, że obwód Ziemi to 40 000 km, skąd promień wynosi (w przybliżeniu) $40\,000/2\pi \approx 6\,366$ km, czyli $r = 6\,366\,000$ m. Przyjrzyjmy się rysunkowi obok. Chcemy znaleźć długość oznaczoną przez x , a raczej różnicę $x - s$ pomiędzy odległościami wierzchołków i podstaw pylonów. Korzystając z twierdzenia Talesa, otrzymujemy

$$\frac{x}{r+h} = \frac{s}{r},$$

skąd

$$x - s = \frac{sh}{r} = \frac{1990 \cdot 283}{6\,366\,000} \text{ m} \approx 0,088 \text{ m} = 8,8 \text{ cm}.$$

Różnica wynosi więc prawie 9 cm! Aparatura pomiarowa obecnie używana przy tego typu budowlach pozwala na wyznaczanie odległości z dokładnością do ułamków milimetra, więc owe 9 cm trzeba uwzględnić przy projektowaniu tak olbrzymich konstrukcji. I rzeczywiście, pierwszą budowlą, w której uwzględniono kulistość Ziemi, był ukończony w 1964 roku nowojorski most Verrazano Narrows Bridge! Więc gdyby nawet Magellan nie opłynął Ziemi dookoła, to i tak Ziemia już dłużej płaska być nie mogła.

Małą Deltę przygotował Piotr HAJŁASZ

$h = 283$ m,
 $s = 1990$ m,
 $r = 6\,366\,000$ m,
 $x - s = ?$

W lipcu 2000 roku doniesiono o niezwykłym eksperymencie przeprowadzonym w laboratorium firmy NEC. Impuls świetlny przechodzący przez sześciocentymetrową komorę wypełnioną wzbudzonymi atomami cezu, był szybszy niż światło; poruszał się tak szybko, że opuszczał komorę, zanim zdążył do niej wejść. Wynik doświadczenia, choć sprzeczny ze zdrowym rozsądkiem, pozostaje w zgodzie z prawami fizyki.

Teoria względności, przynajmniej w swej standardowej postaci, wyklucza istnienie obiektów poruszających się szybciej niż światło w próżni. Ich obecność jest nie do pogodzenia z zasadą przyczynowości, czyli banalną prawdą, że przyczyna poprzedza skutek. Rzecz w tym, że obiekt, który dla jednego obserwatora jest tylko szybszy niż światło, dla innego cofa się w czasie. Na gruncie teorii względności ruch z prędkością większą od prędkości światła i podróżowanie wstecz w czasie są nierozdzielnie związane. (Szczegółowe omówienie tego problemu zawarłem w artykule „Szybciej niż światło?”, *Delta* 8/1991.)

Możliwość zaś powrotu do przeszłości prowadzi do konfliktu z zasadą przyczynowości. Aby zrozumieć, dlaczego tak się dzieje, wyobraźmy sobie, że jakiś szalony konstruktor buduje wehikuł czasu i rusza w przeszłość. Spotyka tam swego dziadka i zabija go, nim ten zdążył spłodzić ojca konstruktora. Mordując dziadka, unicestwia również ojca, więc sam nie może istnieć. A przecież istnieje! Całe zamieszanie wynikało z naruszenia chronologii przyczyn i skutków – wnuczek pojawił się przed swą przyczyną, czyli ojcem. Aby pogwałcić zasadę przyczynowości, nie trzeba nawet podróżować wstecz w czasie, wystarczy przesłać informację do przeszłości. Jeśli by Ewę powiadomić o wszelkich konsekwencjach zjedzenia feralnego jabłka, może nie uległaby podszeptom węża. My pozostalibyśmy w raju, lecz odbyta już pokuta za grzech pierwotny straciłaby wszelką rację istnienia. Teoria względności pozwala uniknąć takich kłopotliwych sytuacji, orzekając, że przesyłanie sygnałów szybszych niż światło, a zatem i wstecz w czasie, jest niemożliwe. Jednak fizycy od dawna zastanawiają się, czy nie można jakoś „obejść” owego zakazu einsteinowskiej teorii. W ostatnich latach poczynili na tej drodze spore postępy.

Jak ustalono jeszcze na początku XIX wieku, światło ma naturę falową. Światłu monochromatycznemu (jednobarwnemu) odpowiada fala elektromagnetyczna o ściśle ustalonej długości i częstotliwości. W przypadku światła białego mamy do czynienia ze złożeniem fal o różnych częstotliwościach, co uwidacznia się przy przechodzeniu takiego światła przez pryzmat. Rozszczepienie na różnobarwne składowe jest przejawem tzw. dyspersji szkła – współczynnik załamania zmienia się wraz z długością fali. Świat jest tak wielobarwny, gdyż substancje nas otaczające bardzo różnie reagują na fale świetlne zależnie od ich długości. Pomidory są czerwone, bo pochłaniają fale o wszystkich długościach z wyjątkiem tej odpowiadającej czerwieni, którą odbijają. Biała kreda równomiernie odbija fale o różnych długościach, węgiel zaś zawdzięcza swój kolor ich silnemu pochłanianiu.

Każdy impuls świetlny można przedstawić jako złożenie fal o różnej częstotliwości. Stanowi to niezwykle sugestywny przejaw matematyczności fizycznego świata. Z jednej strony mamy matematyczne twierdzenie orzekające, że każdą funkcję gładką i całkowalną, niech to będzie zależność intensywności światła od czasu, można przedstawić jako sumę fal o różnych częstotliwościach. Z drugiej strony można wytworzyć światło o żądanej charakterystyce, a następnie za pomocą filtrów wydzielić składowe o określonych częstotliwościach. Intensywność tych składowych okazuje się, oczywiście, całkowicie zgodna z wynikami matematycznej analizy. Oznacza to, że dowolny sygnał nie tylko można przedstawić jako sumę fal, lecz że dowolny sygnał jest sumą fal. Brak sygnału oznacza zaś, że różne fale wzajemnie się znoszą.

Falę o określonej częstotliwości charakteryzuje prędkość fazowa równa szybkości, z jaką poruszają się jej góry i doliny. W przypadku impulsu, będącego złożeniem wielu fal, posługujemy się pojęciem prędkości grupowej, która określa szybkość,



Rozwiązanie zadania M 940.

Oznaczmy środki okręgów odpowiednio przez A' , B' , C' . Niech D będzie rzutem prostokątnym C na AA' . Z twierdzenia Pitagorasa mamy

$$AC^2 = C'D^2 = C'A'^2 - A'D^2 = (a+c)^2 - (a-c)^2 = 4ac.$$

Analogicznie otrzymujemy $AB^2 = 4ab$ i $BC^2 = 4bc$. Wobec tego

$$\sqrt{4ab} = AB = AC + BC = \sqrt{4ac} + \sqrt{4bc}.$$

Dzieląc otrzymaną równość przez $\sqrt{4abc}$ otrzymujemy tezę.

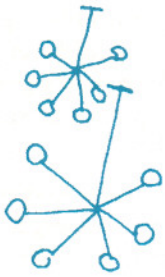


Rozwiązanie zadania M 941.

Odbijamy punkt C symetrycznie względem prostej AB otrzymując punkt C' . Ponieważ $\angle C'MD = 90^\circ$ więc z twierdzenia Pitagorasa otrzymujemy

$$CM^2 + DM^2 = C'M^2 + DM^2 = C'D^2.$$

Zauważmy jednak, że $\angle C'CD = 45^\circ$, a wszystkie kąty o tej rozwartości, wpisane w okrąg o , wyznaczają jednakowe cięciwy (można oczywiście obliczyć ich długość, choć i bez tego teza jest dowiedziona).

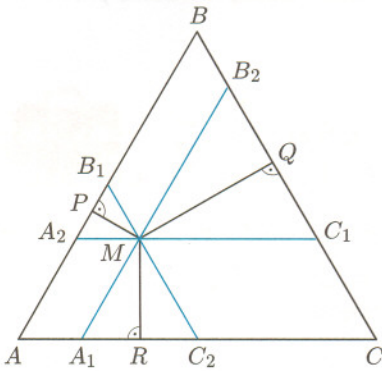


z jaką przemieszcza się maksimum intensywności impulsu. Prędkość fazowa fali świetlnej, rozchodzącej się w próżni, jest równa prędkości grupowej dowolnego impulsu. Prędkość ta, oznaczana tradycyjnie literą c , wynosi 300 000 km/s. W ośrodku dyspersyjnym fale o różnych częstościach różnie się propagują. Sprawia to, że impuls będący sumą różnych fal ulega w takim ośrodku modyfikacji, zmienia się jego prędkość grupowa. Gdy staje się mniejsza od c , mówimy o zwykłej dyspersji. Przed laty już jednak zauważono, że prędkość grupowa mogłaby być większa od c , jednak takiej anomalnej dyspersji towarzyszy bardzo silna absorpcja. Szybki impuls świetlny jest więc niemal całkowicie pochłaniany przez materiał, w którym się rozchodzi.

Wspomniany na wstępie sukces fizyków z laboratorium NECA w Princeton polegał właśnie na stworzeniu ośrodka, w którym z anomalną dyspersją nie wiąże się silna absorpcja. Zamknięte w niewielkiej komorze opary cezu wprowadzono w stan przypominający gotowy do pracy laser – znaczna część atomów została wzbudzona. Światło o częstości zbliżonej do częstości światła owego lasera nie tylko nie było absorbowane, lecz nawet ulegało wzmocnieniu. Przez tak przygotowany ośrodek przepuszczano impuls światła. Zgodnie z oczekiwaniami, jego prędkość grupowa była większa od szybkości rozchodzenia się światła w próżni; na tyle duża, że szczyt impulsu opuszczał komorę, nim zdążył do niej wejść. Ośrodek powodował wzmacnianie początkowej części impulsu i osłabianie końcowej. W rezultacie szczyt impulsu przesunął się do przodu. Należy jednak podkreślić, że zysk ten był dużo mniejszy od długości trwania całego impulsu. Choć więc prędkość grupowa była większa od c , to szybkość, z jaką impuls mógł przenieść informację, nie przekraczała c . Wyjaśnijmy to nieco dokładniej.



Rozwiązanie zadania M 942.



Przyjmijmy, że informację nadajemy w postaci błysków; błysk bądź jego brak stanowi jeden bit informacji. Załóżmy, że odbiornikiem odległym o l od nadajnika jest urządzenie, które reaguje na światło o odpowiednio dużej intensywności, bliskiej maksimum wysyłanych błysków. Niech czas, w jakim szczyt impulsu pokonuje odległość od nadajnika do odbiornika, wynosi t . Prędkość, z jaką podróżuje maksimum, jest większa od c , tj. $l/t > c$. Gdy jednak obliczamy czas potrzebny na przesłanie informacji, musimy uwzględnić czas Δt między rozpoczęciem nadawania sygnału świetlnego a wysłaniem jego maksimum. Wtedy okazuje się, że $l/(t + \Delta t) < c$. Wbrew więc sensacyjnym doniesieniom prasowym wyniki przedstawionego eksperymentu żadnego z fundamentalnych praw fizyki nie naruszają.

Zacznijmy od drugich potęg. Z twierdzenia Pitagorasa mamy

$$AP^2 + BQ^2 + CR^2 = (AM^2 - MP^2) + (BM^2 - MQ^2) + (CM^2 - MR^2) = (BM^2 - MP^2) + (CM^2 - MQ^2) + (AM^2 - MR^2) = PB^2 + QC^2 + RA^2.$$

Dla sprawdzenia równości sum pierwszych potęg dogodnie jest przez M poprowadzić proste równoległe do każdego z boków trójkąta, jak na rysunku. Punkty P, Q, R są, odpowiednio środkami odcinków A_2B_1, B_2C_1, C_2A_1 . Ponadto $AA_1 = BB_2, BB_1 = CC_2, CC_1 = AA_2$. Wobec tego

$$AP + BQ + CR = AA_2 + A_2P + BB_2 + B_2Q + CC_2 + C_2R = PB_1 + B_1B + QC_1 + C_1C + RA_1 + A_1A = PB + QC + RA.$$

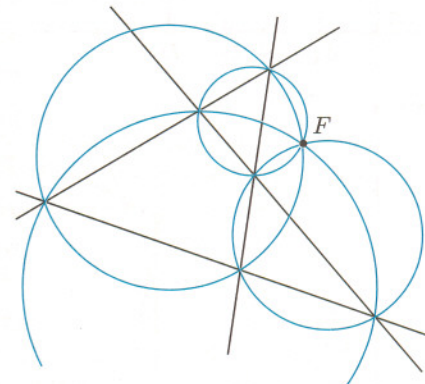
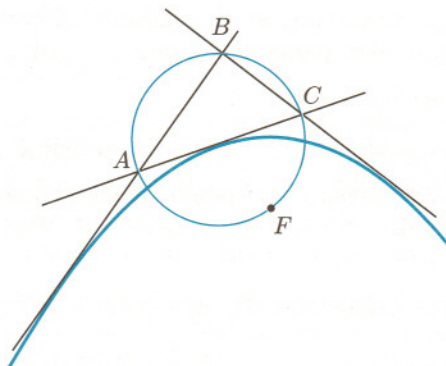
Czy na pewno?

Oto pogląd dotyczący znanej ze szkoły paraboli:

Jeśli parabola jest styczna do prostych zawierających boki trójkąta ABC , to jej ognisko F leży na okręgu opisanym na ABC .

A oto mocniejsza opinia:

Dane są cztery proste, z których żadne trzy nie przechodzą przez jeden punkt, ani żadne dwie nie są równoległe; wówczas cztery okręgi opisane odpowiednio na utworzonych przez proste trójkątach przecinają się w jednym punkcie – jest to ognisko F paraboli stycznej do każdej z tych prostych.



Czy to prawda? Jedyнным sposobem, aby się o tym przekonać jest spróbować to udowodnić. Gdy się udowodni pierwsze, to do drugiego potrzebny będzie tylko fakt(?), że istnieje parabola styczna do takich czterech prostych.

Tylko Pitagoras

Parabolę można określić jako zbiór tych punktów płaszczyzny, które są jednakowo odległe od pewnego ustalonego punktu (zwanego ogniskiem) i pewnej ustalonej prostej nieprzechodzącej przez ognisko (zwanej kierownicą paraboli). Oś, czyli prosta prostopadła do kierownicy i przechodząca przez ognisko, przecina parabolę w punkcie zwanym wierzchołkiem paraboli.

Dość rozpowszechnione jest mniemanie, że ognisko jest środkiem krzywizny wierzchołka paraboli. Środek krzywizny dla jakiegoś punktu krzywej to środek okręgu najlepiej ją przybliżającego w otoczeniu tego punktu. W przypadku wierzchołka paraboli będzie to punkt jej osi położony możliwie najdalej od wierzchołka, taki jednak, że najbliższym mu punktem paraboli jest jej wierzchołek. Inaczej rzecz ujmując, chodzi o taki najdalszy punkt osi paraboli, że największe koło o środku w tym punkcie, mieszczące się między ramionami paraboli, przechodzi przez wierzchołek paraboli.

Otóż środkiem krzywizny paraboli w jej wierzchołku jest punkt osi oddalony od wierzchołka dwa razy bardziej niż ognisko. I aby się o tym przekonać, nie potrzeba niczego więcej niż twierdzenie Pitagorasa. Oto ten dowód.

Na potrzeby tej notatki ustalmy dowolną parabolę i oznaczmy przez S jej ognisko, przez A jej wierzchołek, przez X przecięcie jej osi z kierownicą oraz dla dowolnego jej punktu P oznaczmy przez M jego rzut prostokątny na kierownicę, a przez D – na oś paraboli, wreszcie przez O oznaczmy dowolny punkt jej osi.

Najpierw udowodnimy lemat prezentujący raczej mało znaną własność paraboli.

Lemat: $PD^2 = 4AS \cdot AD$.

Dowód. Istotnie (rys. 1 lub rys. 2)

$$\begin{aligned} PD^2 &= PS^2 - DS^2 = PM^2 - DS^2 = XD^2 - DS^2 = \\ &= (AX + AD)^2 - (AS - AD)^2 = (AS + AD)^2 - (AS - AD)^2 = 4AS \cdot AD. \end{aligned}$$

Wykażemy teraz, że jeśli $AO \leq 2AS$, to najbliższym O punktem paraboli jest jej wierzchołek, czyli

Twierdzenie 1: $(AO \leq 2AS \text{ i } P \neq A) \Rightarrow AO < OP$.

Dowód. Istotnie, gdy $AD < AO$ (rys. 3), mamy

$$\begin{aligned} AO^2 &= (AD + OD)^2 = AD^2 + 2AD \cdot OD + OD^2 = \\ &= AD((AD + OD) + OD) + OD^2 = AD(AO + OD) + OD^2 < \\ &< AD(AO + AO) + OD^2 = 2AD \cdot AO + OD^2 \leq 4AD \cdot AS + OD^2 = \\ &= PD^2 + OD^2 = OP^2. \end{aligned}$$

Z kolei, gdy $AD \geq AO$ (rys. 4), mamy

$$AO^2 < 2AO^2 \leq 4AS \cdot AO \leq 4AS \cdot AD = PD^2 \leq OD^2 + PD^2 = OP^2.$$

Wreszcie wykażemy, że dla punktów osi spełniających warunek $AO > 2AS$ istnieją punkty paraboli tak samo od nich odległe,

jak wierzchołek, czyli

Twierdzenie 2: $AO > 2AS \Rightarrow (\text{istnieje } P \neq A : AO = OP)$.

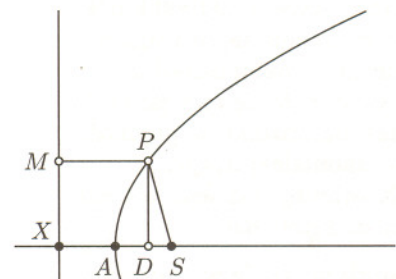
Dowód. Wskażemy taki punkt, podając odległość jego rzutu na oś od wierzchołka: $AD = 2(AO - 2AS) > 0$. Można to zapisać jako $AD = AO + (AO - 4AS)$.

Gdy $AO < 4AS$ (rys. 5), mamy $AD < AO$ i

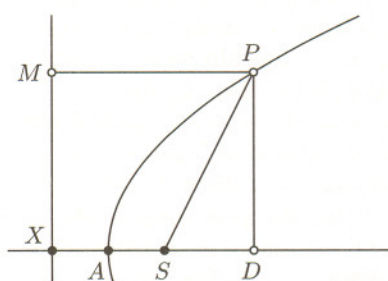
$$OD = AO - AD = 4AS - AO.$$

Gdy z kolei $AO \geq 4AS$ (rys. 6), mamy $AD \geq AO$ i

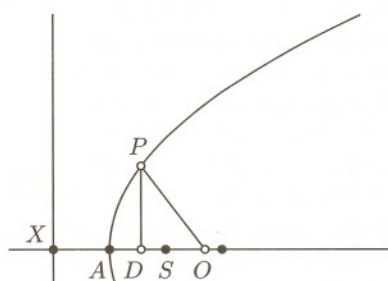
$$OD = AD - AO = AO - 4AS.$$



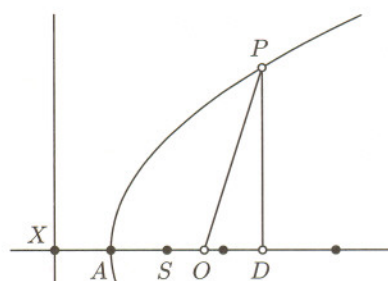
Rys. 1



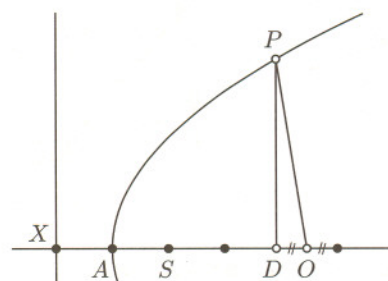
Rys. 2



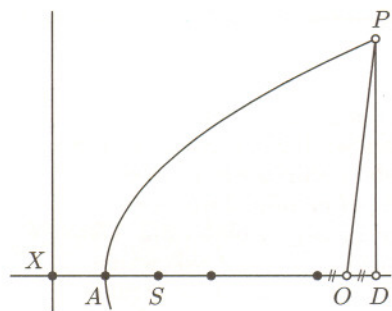
Rys. 3



Rys. 4



Rys. 5



Rys. 6

W obu więc przypadkach

$$\begin{aligned} OP^2 &= OD^2 + PD^2 = OD^2 + 4AS \cdot AD = \\ &= 16AS^2 - 8AS \cdot AO + AO^2 + 4AS \cdot AD = \\ &= AO^2 + 4AS(4AS - 2AO + AD) = AO^2 + 4AS(-AD + AD) = AO^2. \end{aligned}$$

Elipsę i hiperbolę podobnie określa się za pomocą ogniska i kierownicy. W tym przypadku chodzi o punkty, których stosunek odległości od ogniska i od kierownicy jest stały; gdy ten stosunek jest mniejszy od 1 – otrzymujemy elipsę, gdy większy – hiperbolę (a gdy równy 1 – parabolę). Definicja wierzchołka i osi jest taka sama jak dla paraboli. A gdzie leżą środki krzywizny tych krzywych w ich wierzchołkach? Redakcja będzie wdzięczna Czytelnikom nie tyle za odpowiedź na to pytanie, co za wskazanie równie elementarnych dowodów odpowiednich faktów.

Wojciech GUZICKI i Marek KORDOS



W tablicach Księżycowych publikowanych w rocznikach astronomicznych znajduje się sporo luk oznaczających, że jakiegoś dnia Księżyc nie wschodzi, innego dnia nie góruje itd. Jak to możliwe? Nie zapominajmy, że Księżyc porusza się po niebie dość szybko ($13^\circ/176$ na dobę) i w dodatku z zachodu na wschód. Dlatego jeżeli pewnego dnia np. górował tuż przed północą, to następane jego górowanie wypadnie tuż po północy, ale nie zaraz następnego dnia, lecz jeszcze następnego. To samo dotyczy wschodów i zachodów, stąd luki w tablicach.



Zadania

Redaguje Łukasz WIECHECKI

M 940. Okręgi o promieniach a , b , c są parami zewnętrznje styczne i wszystkie są styczne do prostej k odpowiednio w punktach A , B , C , przy czym punkt C leży między punktami A i B . Wykazać, że

$$\frac{1}{\sqrt{c}} = \frac{1}{\sqrt{a}} + \frac{1}{\sqrt{b}}.$$

Rozwiązanie na str. 8

M 941. Na średnicy AB okręgu o dany jest punkt M . Przez M poprowadzona jest cięciwa CD przecinająca AB pod kątem 45° . Wykazać, że suma $CM^2 + DM^2$ nie zależy od wyboru punktu M .

Rozwiązanie na str. 8

M 942. Rzutami dowolnie obranego we wnętrzu trójkąta równobocznego punktu M na boki AB , BC i CA tego trójkąta są, odpowiednio, punkty P , Q , R . Wykazać, że suma zarówno pierwszych, jak i drugich, potęg długości jest taka sama dla odcinków AP , BQ , CR , jak dla odcinków PB , QC , RA .
Rozwiązanie na str. 9

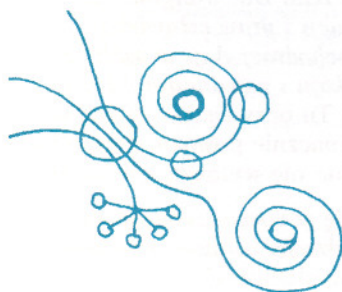
Redaguje Ewa CZUCHRY

F 539. Wyznaczyć ciśnienie w pęcherzyku powietrza o średnicy $d = 0,01$ mm znajdującym się 20 cm pod powierzchnią wody. Ciśnienie zewnętrzne wynosi $p_1 = 765$ mm Hg (1 mm Hg = 133 N/m²). Napięcie powierzchniowe wody $\alpha = 0,073$ N/m.

Rozwiązanie na str. 13

F 540. Ze zbiornika, przez pionową rurkę o średnicy $d = 2$ mm, wycieka kropla po kropli alkohol. Znaleźć czas, po jakim wypłynie 10 g alkoholu, jeśli odstęp czasu między kapiącymi kroplami wynosi 1 s. Zakładamy, że kropla odrywa się wzdłuż wewnętrznego przekroju rurki. Napięcie powierzchniowe alkoholu $\alpha = 0,02$ N/m.

Rozwiązanie na str. 13



Noble końca wieku

W październiku, jak co roku, przyznano Nagrody Nobla. Wbrew moim (żartobliwym) przewidywaniom nagrody z fizyki nie przyznano za odkrycie bozonu Higgsa. (*Delty* 1, 5/2000; info.fuw.edu.pl/HEP/cms/edu).

Niestety, nie udało się go odkryć. Sprawozdawcy sportowi powiedzieliby jednak: „niewiele brakowało!”. Sytuacja była podbramkowa. Na miesiąc przed planowanym zamknięciem LEPu, czyli Wielkiego Zderzacza Elektronów i Pozytonów, jeden z czterech eksperymentów (ALEPH) zaprezentował wyniki zgadzające się z obserwacją poszukiwanej cząstki i wskazujące, że jej masa powinna wynosić około $115 \text{ GeV}/c^2$, czyli dokładnie tyle, ile wynosi granica kinematyczna LEPu. Cięższy higgs nie mógłby zostać wyprodukowany, a trochę lżejszy zostałby odkryty bez większego problemu. Informacja ta zelektryzowała nie tylko fizyków cząstek, ale nawet środki masowego przekazu. LEP zyskał miesiąc życia. Dogrywka nie zmieniła jednak wyniku meczu. Po dwunastu latach odgrywania przez LEP kluczowej roli w doświadczalnej fizyce cząstek 2 listopada 2000 roku została podjęta decyzja o definitywnym zakończeniu zbierania danych. Sygnał produkcji bozonu Higgsa nie został ani ostatecznie potwierdzony, ani obalony. Jeżeli poszukiwana cząstka ma masę nie większą, niż wskazują to obecne wyniki, to LEP mógłby ją odkryć, gdyby zdecydowano się na zbieranie danych przez jeszcze jeden sezon. Niestety, na to nie ma pieniędzy. Nie tylko na samo działanie akceleratora, ale przede wszystkim na kary umowne, które właściciel LEPu – CERN – musiałby zapłacić, powstrzymując konstrukcję LHC – zderzacza protonów mającego zastąpić LEP na froncie badania mikroświata. Przez najbliższe pięć lat bozon Higgsa może zostać odkryty przez zmodernizowany Tevatron działający pod Chicago. W 2005 roku piłka wróci do Europy. Nastanie era LHC.

Tegorocznych Nagród Nobla nie przyznano nie tylko za (nie)znalezienie bozonu Higgsa. Żadne z naprawdę świeżych osiągnięć nie dostało tego zaszczytu. W setnym roku przyznawania nagrody dokonano swoistego remanentu. Trudno oprzeć się wrażeniu, że komitety przyznające nagrody z poszczególnych dziedzin wybrały tematycznie podobne dokonania sprzed 20–30 lat. Tym wspólnym mianownikiem jest, moim zdaniem, postęp w szeroko rozumianej komunikacji.

Dziedziną fizyki, która najbardziej wpłynęła na życie przeciętnego człowieka w ostatnich trzydziestu latach, jest niewątpliwie fizyka fazy skondensowanej.

Nagrodę Nobla 2000 z Fizyki przyznano właśnie reprezentantom tej gałęzi: w połowie Zhoresowi I. Alferowowi i Herbertowi Kroemerowi za *prace nad heterostrukturami półprzewodnikowymi wykorzystywanymi w ultra-szybkiej elektronice i optoelektronice*, a w połowie Jackowi S. Kilby'emu za *udział w wynalezieniu obwodów scalonych*. To im i ich kolegom po fachu zawdzięczamy postępującą rewolucję informatyczną, łącza światłowodowe, odtwarzacze DVD, telefony komórkowe itd. Nie byłoby tego wszystkiego bez osiągnięć badań podstawowych.

Natomiast **Nagrodę Nobla 2000 z Chemii** przypadła w udziale Alanowi J. Heegerowi, Alanowi G. MacDiarmidowi i Hideki Shirakawie za *odkrycie i badania przewodzących polimerów*. Tworzywa sztuczne kojarzą się nam raczej z izolatorami. Okazuje się jednak, że przez odpowiednie domieszkowanie łańcuchów węglowych połączonych naprzemiennie wiązaniami pojedynczymi i podwójnymi można je namówić do przesyłania prądu. Rozwój tej dziedziny zawdzięczamy bardziej tradycyjnym sposobom komunikowania: dwaj tegoroczni Nobliści spotkali się kiedyś przypadkiem na kawie... Przewiduje się, że przewodzące polimery mogą w najbliższej przyszłości m.in. zastąpić tradycyjne układy półprzewodnikowe w zadaniach, w których szybkość nie jest najważniejsza, czy pozwolić na masową produkcję tanich wyświetlaczy.

Z kolei **Nagrodę Nobla 2000 z Fizjologii i Medycyny** otrzymali Arvid Carlsson, Paul Greengard i Eric Kandel za odkrycia dotyczące *przewodzenia sygnałów w systemie nerwowym*. Ich badania pozwoliły lepiej zrozumieć, jak działa najbardziej skomplikowany układ komunikacyjny Wszechświata – nasz mózg. Ich odkrycia doprowadziły do opracowania nowych leków pomocnych np. w łagodzeniu objawów choroby Parkinsona.

Kolejni wyróżnieni naukowcy rozwijali mikroekonometrię. **Nagrodę Banku Szwecji 2000 z Nauk Ekonomicznych im. A. Nobla** przyznano Jamesowi Heckmanowi i Danielowi McFaddenowi za *rozwój teorii i metod statystycznej analizy zachowania jednostek i gospodarstw domowych, szeroko stosowanych w ekonomii oraz innych naukach społecznych*. Najprościej mówiąc, ich metody pozwalają na wyłuskanie z danych statystycznych rzetelnych informacji. Dzięki nim można wiarygodnie sprawdzać, jak np. informatyczna globalizacja wpływa na życie jednostek.

Pozostałe dwie Nagrody Nobla zawsze w jakimś sensie dotyczą międzyludzkiej komunikacji. Tym razem jest to jednak szczególnie widoczne, gdyż nagrodzeni niewątpliwie przyczynili się do pokonania komunikacyjnych barier. Mianowicie **Nagrodę Nobla 2000 z Literatury** uhonorowano Gao Xingjiana za *dorobek o uniwersalnej wartości, gorzkiej głębi i językowej oryginalności, który otworzył nowy rozdział chińskiej powieści i dramatu*. Noblista nie tylko przybliżył nam hermetyczny świat jednej czwartej ludzkości, ale również odkrywa w nowy sposób nasze własne nieproste wnętrza. Natomiast **Pokojową Nagrodę Nobla** przyznano Kim Dae Jungowi za *działania na rzecz demokracji i praw człowieka w Korei Południowej i Wschodniej Azji w ogólności, a za działania na rzecz pokoju i pojednania z Koreą Północną w szczególności*. Tu oczywistość dokonania w przełamywaniu czegoś znacznie poważniejszego niż tylko bariera komunikacyjna nie wymaga komentarza.

Jeżeli chodzi o komunikację w rozpoczynającym się tysiącleciu, to mam nadzieję, że może wreszcie nauczymy się wzajemnie wysłuchiwać.

Piotr ZALEWSKI

Jury Konkursu Uczniowskich Prac z Matematyki w składzie: Antoni Leon Dawidowicz – przewodniczący, Marek Kordos, Witold Sadowski, Agnieszka Wojciechowska, Jarosław Wróblewski, na posiedzeniu w dniu 30 sierpnia 2000 roku w Warszawie, po wysłuchaniu prezentacji prac zakwalifikowanych do finału Konkursu, postanowiło:

- 1) nie przyznawać medalu złotego,
- 2) przyznać srebrny medal i nagrodę w kwocie 300 złotych **Piotrowi Sulichowi** z II LO im. Ziemi Olkuskiej w Olkuszu za pracę pt. *Obrót o kąt na płaszczyźnie: zastosowania i własności* oraz **Mirosławowi Żwirynowi** z XXVI LO w Łodzi za pracę pt. *Wstęp do teorii macierzy nD* ,
- 3) nie przyznawać medalu brązowego,
- 4) przyznać dwa równorzędne wyróżnienia i nagrody w kwocie 175 złotych każda: **Sławomirowi Kurasiowi** z Zespołu Szkół im. Oddziału Partyzanckiego AK „Jędrusie” w Połańcu za pracę pt. *Wybrane własności trójkątów* oraz **Michałowi Staromiejskiemu** z V LO w Krakowie za pracę pt. *O czworościanie Pascala*,
- 5) przyznać nagrody w kwocie 150 złotych opiekunom prac zakwalifikowanych do finału: mgr. Ryszardowi Grucy, mgr. Henrykowi Pawłowskiemu, mgr Danucie Przybylskiej, mgr Sabinie Sierant.

(-) podpisy członków Jury

Tradycyjnie redakcja *Delty* ogłasza Konkurs Uczniowskich Prac z Matematyki. Zachęcamy uczniów zainteresowanych matematyką do opracowywania swoich matematycznych rozważań i nadsyłania rezultatów do redakcji *Delty*. Poniżej przypominamy szczegółowy regulamin konkursu.

Regulamin Konkursu Uczniowskich Prac z Matematyki

1. Konkurs organizowany jest corocznie przez Zarząd Główny Polskiego Towarzystwa Matematycznego i redakcję miesięcznika *Delta*, przy poparciu Ministerstwa Edukacji Narodowej.
2. W konkursie mogą brać udział uczniowie wszystkich typów szkół.
3. Konkurs składa się z eliminacji i finału.
4. W eliminacjach bierze udział każdy uczeń, który w terminie do 1 maja prześle pod adresem redakcji *Delty* jeden egzemplarz swojej pracy matematycznej. Do pracy należy dołączyć następujące informacje: adres prywatny autora, klasa, nazwa i adres szkoły; imię, nazwisko i adres opiekuna pracy.
5. Praca powinna zawierać samodzielny wkład ucznia i pełną informację o źródłach, z których korzystał jej autor. Prace czysto kompilacyjne nie będą dopuszczone do finału konkursu.
6. Prace nadesłane na eliminacje zostaną ocenione przez Jury Konkursu i kompetentnych recenzentów. Te spośród prac, które spełniają warunki konkursu, zostaną zakwalifikowane przez Jury do finału. Finał odbędzie się w trakcie dorocznej Sesji Naukowej Polskiego Towarzystwa Matematycznego.
7. Zawiadomienia o zakwalifikowaniu do finału zostaną przesłane autorom prac i ich opiekunom przed końcem roku szkolnego.
8. Finałiści i opiekunowie ich prac otrzymają od Zarządu Głównego PTM zaproszenia do udziału w Sesji na koszt Towarzystwa.
9. Finał polega na wygłoszeniu (nie odcytaniu) przez ucznia, podczas specjalnego otwartego posiedzenia Sesji, referatu (trwającego nie dłużej niż 15 minut) i wzięciu udziału w dyskusji na temat, któremu poświęcona była praca.
10. Rezultaty finału oceni Jury Konkursu. Jury będzie brało pod uwagę, oprócz merytorycznej wartości pracy, również samodzielność i oryginalność ujęcia tematu oraz przebieg referatu i dyskusji. Jury przyznaje medale: złoty, srebrny i brązowy, wyróżnienia oraz nagrody pieniężne ufundowane przez Ministerstwo Edukacji Narodowej.
11. Ogłoszenie wyników finału następuje w trakcie Walnego Zgromadzenia Polskiego Towarzystwa Matematycznego. Medale wręcza Prezes Towarzystwa. Wszyscy uczestnicy finału otrzymują dyplomy.
12. Wyniki konkursu i skrót zycyjskiej pracy będą opublikowane w miesięczniku *Delta*.
13. Jury Konkursu jest powoływane przez Zarząd Główny PTM na wniosek Komitetu Redakcyjnego *Delty*.

Skróty prac nagrodzonych srebrnym medalem zamieścimy w *Delcie* 3/2001 i 4/2001.

Przy okazji informujemy, że laureat poprzedniej edycji konkursu, Jakub Onufry Wojtaszczyk, uzyskał wyróżnienie w finale Konkursu na Najlepszego Młodego Uczzonego Europy, który odbył się we wrześniu 2000 r. w Amsterdamie.

W poprzednich latach laureaci Konkursu Uczniowskich Prac z Matematyki zdobyli medal srebrny i dwa medale brązowe.

Rozwiązanie zadania F 539.

Ciśnienie powietrza w pęcherzyku składa się z ciśnienia atmosferycznego p_1 , hydrostatycznego $p_2 = \rho gh$ (h jest głębokością pod powierzchnią wody) i dodatkowego ciśnienia $p_3 = 2\alpha/r = 4\alpha/d$ wywołanego napięciem powierzchniowym. Stąd

$$p = p_1 + \rho gh + \frac{2\alpha}{r} \approx 999 \text{ mm Hg.}$$

Rozwiązanie zadania F 540.

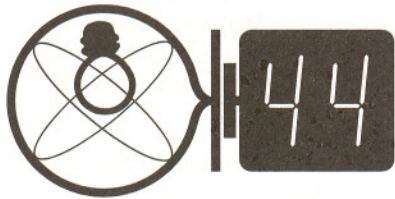
Cieężar kropli w czasie odpadania powinien być wystarczający, żeby zerwać błonę powierzchniową wzdłuż okręgu o długości $l = 2\pi r$, gdzie r jest promieniem kropli. Stąd ciężar kropli

$$G = 2\pi r \alpha = \pi d \alpha.$$

Liczba kropli alkoholu zawartego w M gramach wynosi

$$N = \frac{Mg}{G} = \frac{Mg}{\pi d \alpha}.$$

Podstawienie danych liczbowych daje $N = 780$ kropli. Ponieważ odstęp czasu między odrywaniem się poszczególnych kropeł wynosi 1 s, cały alkohol wypłynie po czasie $t = 780 \text{ s} = 13$ minut.



Termin nadsyłania rozwiązań:
31 III 2001

Skrót regulaminu

Każdy może nadsyłać rozwiązania zadań z numeru n w terminie do końca miesiąca $n + 2$. Szkice rozwiązań zamieszczamy w numerze $n + 4$. Można nadsyłać rozwiązania czterech, trzech, dwóch lub jednego zadania (każde na oddzielnej kartce), można to robić co miesiąc lub z dowolnymi przerwami. Rozwiązania zadań z matematyki i z fizyki należy przysyłać w oddzielnych kopertach, umieszczając na kopercie dopisek: **Klub 44 M** lub **Klub 44 F**. 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 2/2000.

Zadania z fizyki nr 310, 311

Redaguje Jerzy B. BROJAN

310. Z równi pochyłej o kącie nachylenia α wyrzucono małe ciało z ustaloną wartością prędkości początkowej. Jaki powinien być kąt nachylenia tej prędkości do poziomu, aby: a) rzut trwał maksymalnie długo, b) zasięg rzutu był maksymalny?

311. Promieniowanie jest pochłaniane w materii zgodnie ze wzorem

$$I = I_0 e^{-\mu x},$$

gdzie I_0 jest natężeniem wiązki padającej, a I - natężeniem wiązki przechodzącej przez warstwę o grubości x . Jeśli parametr μ opisujący pochłanianie promieni podczerwonych ma dla pewnego materiału wartość 2 mm^{-1} , a jego współczynnik przewodnictwa cieplnego wynosi $0,2 \text{ W/(m}\cdot\text{K)}$, to czy słuszne jest przypuszczenie, że w temperaturze pokojowej przewodnictwo cieplne tego materiału wynika głównie z przepływu energii w formie promieniowania podczerwonego? Wystarczy odpowiedź oparta na ocenie orientacyjnej.

Wskazówka: Współczynnikiem przewodnictwa cieplnego λ nazywamy współczynnik we wzorze Fouriera

$$\frac{\Delta Q}{\Delta t} = \lambda S \frac{\Delta T}{\Delta x},$$

gdzie ΔQ jest ilością ciepła przepływającą w ciągu czasu Δt przez powierzchnię S pod wpływem różnicy temperatur ΔT między punktami odległymi o Δx wzdłuż osi prostopadłej do tej powierzchni.

Rozwiązania zadań z fizyki z numeru 9/2000

Przypominamy treść zadań:

302. Przewodząca kula o promieniu r składa się z dwóch zetkniętych ze sobą półkul. Jaka jest wartość siły odpychającej te dwie półkule od siebie, jeśli ładunek całej kuli wynosi Q ?

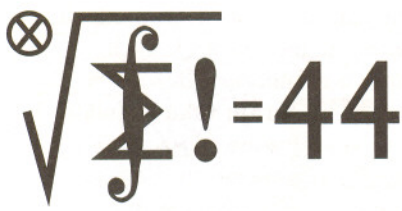
303. Dwa jednakowe naczynia o ściankach nie przewodzących ciepła są połączone rurką z zaworem (kranikiem). Początkowo w jednym naczyniu znajdował się gaz pod ciśnieniem p i w temperaturze T , a w drugim naczyniu była próżnia. Otwarto zawór, tak że ciśnienia się wyrównały. Jaka będzie wtedy wartość p' ciśnienia oraz temperatur T_1 i T_2 w naczyniach? Gaz jest doskonały, a stosunek jego ciepła właściwych wynosi $\gamma = c_p/c_v$.

302. Na kuli przewodzącej ładunek jest, oczywiście, rozłożony jednorodnie. Siła wywierana na mały element powierzchni kuli (zawierający ładunek dQ) przez resztę kuli jest równa $dF = (1/2)E_{zewn}dQ$, gdzie $E_{zewn} = Q/(4\pi\epsilon_0 r^2)$. Aby to wykazać, można odwołać się do bilansu energii: praca wykonana przy jednoczesnym przesunięciu wszystkich tych ładunków jest równa zmianie energii danej wzorem $E = Q^2/2Cr$, gdzie $C = 4\pi\epsilon_0 r$ jest pojemnością kuli. Składając siły działające na wszystkie elementy półkuli, należy wziąć ich składową wzdłuż odpowiedniej osi, tzn. $dF_z = dF \cos \theta$, a ponadto zgodnie z jednorodnym rozkładem ładunku dQ jest proporcjonalne do powierzchni dS danego elementu kuli, czyli podstawiamy $dQ = QdS/(4\pi r^2) = (1/2)Q \sin \theta d\theta$. Całkowanie po θ od 0 do $\pi/2$ prowadzi do wyniku

$$F_z = \frac{Q^2}{32\pi\epsilon_0 r^2}.$$

303. Przepływ gazu przez kranik nie zmienia jego całkowitej energii wewnętrznej. Ponieważ dla gazu doskonałego energia wewnętrzna jest dana wzorem $U = nC_V T = (C_V/R)pV$, a objętości naczyni są jednakowe, więc z bilansu energii natychmiast otrzymujemy $p' = (1/2)p$. Zauważmy dalej, że gaz pozostający w naczyniu, w którym był początkowo, uległ przemianie adiabatycznej (drugie naczynie jest znacznie trudniejsze do analizy pod tym kątem, gdyż wpływały do niego kolejne partie gazu, których temperatura się zmieniała). W zmiennych $p - T$ równanie przemiany adiabatycznej ma postać $p^{1-\gamma} T^\gamma = \text{const}$, zatem $T_1 = T/2^{(\gamma-1)/\gamma}$. Na koniec temperaturę drugiego naczynia T_2 można wyznaczyć z zachowania masy (liczby moli), co w naszym przypadku sprowadza się do równania

$$\frac{2}{T} = \frac{1}{T_1} + \frac{1}{T_2}.$$



Zadania z matematyki nr 413, 414

Redaguje Marcin E. KUCZMA

413. Liczby dodatnie a, b, c spełniają warunki $b > 2a, c > 2b$. Dowieść, że dla pewnej liczby dodatniej λ część ułamkowa każdego z iloczynów $\lambda a, \lambda b, \lambda c$ jest liczbą z przedziału $(1/3; 2/3)$.

(Część ułamkowa liczby x to różnica $x - [x]$, gdzie $[x]$ jest największą liczbą całkowitą nie przekraczającą x .)

414. Wewnątrz wielokąta wypukłego W znajduje się taki punkt O , że każda prosta przechodząca przez O dzieli wielokąt W na dwie części o równych polach. Czy stąd wynika, że punkt O jest środkiem symetrii wielokąta W ?

Zadanie 414 zaproponował pan Witold Bednarek z Łodzi.

Rozwiązania zadań z matematyki z numeru 9/2000

Przypominamy treść zadań:

405. Przez środek I okręgu wpisanego w nierównoramienny trójkąt ostrokątny ABC poprowadzono okręgi k_A, k_B, k_C : okrąg k_A jest mniejszym z dwóch okręgów przechodzących przez I , stycznych do prostych AB i AC ; okręgi k_B i k_C są określone analogicznie. Okręgi k_B i k_C przecinają się w punktach I, P ; okręgi k_C i k_A przecinają się w punktach I, Q ; okręgi k_A i k_B przecinają się w punktach I, R . Dowieść, że środki okręgów opisanych na trójkątach AIP, BIQ, CIR są współliniowe.

406. Czy istnieje rosnący ciąg liczb pierwszych p_1, p_2, p_3, \dots , w którym każdy wyraz (począwszy od drugiego) jest nie mniejszy od średniej arytmetycznej dwóch wyrazów z nim sąsiadujących?

Termin nadsyłania rozwiązań:

31 III 2001

Czołówka ligi zadaniowej

Klub 44 M

po uwzględnieniu ocen rozwiązań

zadań 401 (WT=2,54) i 402 (WT=1,71)

z numeru 5/2000

Bartłomiej Dyda	- Wrocław	41,52
Konrad Patkowski	- Gdańsk	41,43
Bartłomiej Marczak	- Warszawa	39,20
Paweł Kubit	- Kraków	35,01

405. Założenie, że trójkąt ABC nie jest równoramienny, gwarantuje, iż trójkąty AIP, BIQ, CIR są niezdegenerowane, więc opisane na nich okręgi są dobrze określone. Wykażemy, że te okręgi mają jeszcze jeden (oprócz I) wspólny punkt J . Stąd oczywiście wyniknie, że ich środki leżą na prostej symetralnej odcinka IJ .

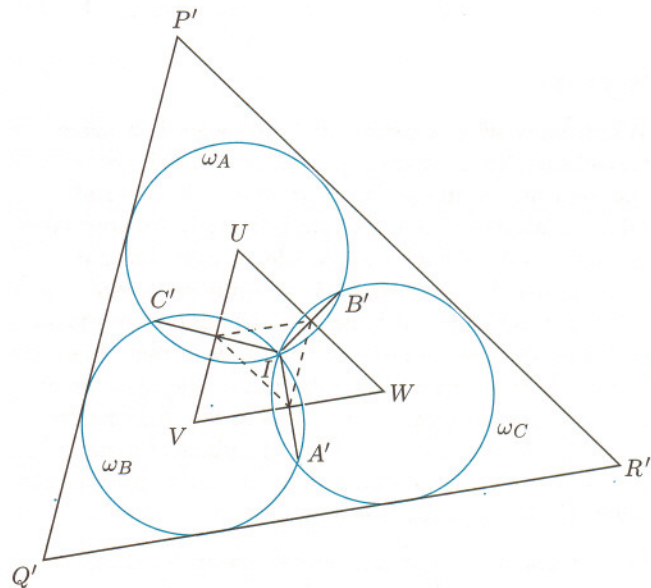
Stosujemy inwersję względem dowolnie ustalonego okręgu o środku I . Oznaczmy obrazy punktów A, B, C, P, Q, R odpowiednio przez A', B', C', P', Q', R' . Obrazami okręgów k_A, k_B, k_C są proste $Q'R', R'P', P'Q'$. Obrazami prostych BC, CA, AB są okręgi, które oznaczmy odpowiednio przez $\omega_A, \omega_B, \omega_C$. Przechodzą one przez punkt I ; ponadto przecinają się parami w punktach A', B', C' ; każdy z tych okręgów jest styczny do dwóch boków trójkąta $P'Q'R'$. Skoro proste BC, CA, AB były jednakowo odległe od punktu I (środku inwersji), to okręgi $\omega_A, \omega_B, \omega_C$ mają jednakowe promienie.

Obrazami okręgów opisanych na trójkątach AIP, BIQ, CIR są proste $A'P', B'Q', C'R'$. Zadanie sprowadza się do wykazania, że te proste mają wspólny punkt.

Oznaczmy środki okręgów $\omega_A, \omega_B, \omega_C$ odpowiednio przez U, V, W . Ich promienie są równe, więc punkt I jest środkiem okręgu opisanego na trójkącie UVW . Proste IA', IB', IC' są symetralnymi jego boków; a środki boków są jednocześnie środkami odcinków IA', IB', IC' . Zatem te środki są wierzchołkami trójkąta, który jest jednocześnie jednokładny i do trójkąta UVW (w skali $-1/2$), i do trójkąta $A'B'C'$ (w skali $1/2$). Wynika stąd, że boki

trójkąta $A'B'C'$ są odpowiednio równoległe do boków trójkąta UVW ; że zaś są z kolei równoległe do boków trójkąta $P'Q'R'$ (wobec równości promieni okręgów $\omega_A, \omega_B, \omega_C$).

Konkludując, stwierdzamy, że boki trójkątów $A'B'C'$ i $P'Q'R'$ są odpowiednio równoległe, i wobec tego trójkąty te są jednokładne. Środek owej jednokładności jest poszukiwanym punktem przecięcia prostych $A'P', B'Q', C'R'$.



406. Przypuśćmy, że p_1, p_2, p_3, \dots jest rosnącym ciągiem liczb naturalnych, w którym $2p_i \geq p_{i-1} + p_{i+1}$. Przyjmując $a_i = p_i - p_{i-1}$ widzimy, że $a_{i+1} \leq a_i$. Nierosnący ciąg liczb naturalnych a_1, a_2, a_3, \dots jest od pewnego miejsca stały: $a_i = r$ dla $i \geq i_0$. Tak więc $p_{i_0}, p_{i_0+1}, p_{i_0+2}, \dots$ jest ciągiem arytmetycznym o różnicy r . Wobec tego

$$p_{i_0+k} = p_{i_0} + kr \quad \text{dla } k = 0, 1, 2, \dots$$

Dla $k = k_0 = p_{i_0}$ otrzymujemy $p_{i_0+k_0} = p_{i_0} + p_{i_0}r = p_{i_0}(1+r)$; jest to liczba złożona. Zatem nie istnieje ciąg liczb pierwszych p_1, p_2, p_3, \dots o zadanej własności.

Większość galaktyk w dzisiejszym Wszechświecie jest skupiona w gromadach, supergromadach (gromadach gromad) i – zapewne – w jeszcze większych „ścianach” ograniczających ogromne pustki (*voids*) o rozmiarach liczonych w dziesiątkach megaparseków. Nasza Galaktyka leży na skraju takiej wielkiej struktury zwanej Supergromadą w Pannie. Jest to spłaszczone zgęszczenie galaktyk, którego centrum znajduje się w dość gęstej gromadzie (w Pannie) odległej od nas w przybliżeniu o 15 Mpc. Inne tego rodzaju zgrupowania znajdują się kilkakrotnie dalej.



Obserwując rozkład jeszcze odleglejszych, a więc jeszcze młodszych galaktyk, astronomowie nie przypuszczali, że odkryją wiele takich zgęszczeń, choć fluktuacje gęstości materii w dostatecznie zimnym ośrodku mają tendencję do narastania – jest to tzw. niestabilność Jeansa. Jeżeli ośrodek jest chłodny, to znaczy, że jego cząstki mają niedużą energię kinetyczną, a wtedy wzajemne ich przyciąganie grawitacyjne może spowodować zapadanie się odpowiednio wielkiej porcji tego ośrodka. Łatwo to się mówi, gdyż zazwyczaj zapomina się o tym, że gdy ośrodek jest bardzo rzadki, to proces taki toczy się niezwykle powoli – tak powoli, że nie należałoby oczekiwać istnienia wielkich zgrupowań galaktyk w dostatecznie wczesnym Wszechświecie.

Tymczasem niedawno grupa amerykańskich astronomów wykonując przegląd przesunąć ku czerwieni bardzo odległych galaktyk, znalazła w Wodniku zgrupowanie 15 galaktyk i jednego kwazara (o jasności w przybliżeniu 24 mag), których przesunięcia widm skupione są wokół wartości 3,09. Na podstawie odległości określonej przez tę wartość przesunięcia i rozmiarów kątowych gromady jej rozmiary liniowe oceniono na 10 Mpc. W odległości odpowiadającej $z = 3,09$ znajdują się obiekty, których wiek nie przekracza miliarda lat, a to jest stanowczo za mało, by od Wielkiego Wybuchu zdążyła utworzyć się normalna gromada galaktyk. Niewykluczone, że obserwowane tam galaktyki są na etapie skupiania się w jedną galaktykę olbrzymią, o masie rzędu 10^{12} mas Słońca – takie gigantyczne galaktyki znajdują się obecnie w centrum licznych gromad. Niemniej jednak zagadką pozostaje, jak do powstania tak zwartej gromady mogło dojść w tak krótkim czasie.

Tomasz KWAST

Styczeń

Wkraczamy więc w nowy rok 2001, wiek i zarazem tysiąclecie. Nie towarzyszą temu żadne efektowne zjawiska przyrodnicze, bo skąd właściwie przyroda miałaby wiedzieć, że tak sobie ponumerowaliśmy lata? Niemniej jednak chyba dla każdego takie okrągłe przełomowe daty są okazją do zadumy nad tym, co było, i nad tym, co będzie. Każdy zapewne ma nadzieję, że „będzie lepiej”, a w każdym razie nie gorzej. Życzymy więc sobie, aby naprawdę było lepiej i w tym celu „róbmy swoje”, bo bardzo dużo zależy tu właśnie od nas, a nie od układu planet i gwiazd. „Lepiej” nie robi się samo, można jednak mu pomóc, a wtedy efekty mogą być wspaniałe.

Obojętność Wszechświata wobec naszych problemów przejawia się choćby w tym, że mamy nad sobą to samo niebo, co rok temu. W styczniowe wieczory pięknie widać wysoko Plejady i Hiady, najlepiej zbadane otwarte gromady gwiazdowe, a na południowym wschodzie Oriona. Zdjęcia robione z długim czasem ekspozycji ukazują, że np. Plejady i praktycznie cały gwiazdozbiór Oriona spowijają obłoki materii międzygwiazdowej, tak kiedyś niedocenianego składnika naszej Galaktyki.

Co więcej, wszystko wskazuje na to, że w Galaktyce jest jeszcze więcej naprawdę niewidocznej (przy dzisiejszych środkach technicznych) materii o nieznannej naturze, która swoją obecność przejawia tylko grawitacyjnym oddziaływaniem na gwiazdy.

Inną natomiast, niż rok temu, konfigurację tworzą, oczywiście, planety. I tak Wenus jest w Wodniku i widać ją na zachodzie jako Gwiazdę Wieczorną. Mars jest w Wadze i wschodzi dopiero w drugiej połowie nocy. Jowisz jest w Byku, a Saturn na granicy Barana i Byka, zatem obie te planety widać wieczorem wysoko na niebie. 4 I Ziemia znajdzie się najbliżej Słońca, co – jak widać – nie przeszkadza, że jest środek zimy. 9 I wypada pełnia Księżyca, a 24 I nów. Podczas pełni nastąpi całkowite zaćmienie Księżyca, przy czym środek zaćmienia będzie o godz. 21:20. Jeżeli więc pogoda pozwoli, to zaćmienie będzie widać w całej okazałości. Można też w drugiej połowie stycznia próbować szukać na zachodnim niebie Merkurego, który znajdzie się wtedy w odległości „aż” 18° od Słońca. Żadnych jasnych gwiazd Księżyc w styczniu nie zakrywa.

T.K.

Oto ciąg dalszy 37 własności liczby 37:

15. Liczby postaci $2^p - 1$, gdzie p jest liczbą pierwszą, nie zawsze są pierwsze (takie liczby, o ile są pierwsze, nazywamy liczbami pierwszymi Mersenne'a). Jeśli jednak przy ustalonej liczbie pierwszej p przejrzymy liczby postaci $\frac{n^p - 1}{n - 1}$, gdzie $2 \leq n \leq p$, to szanse na znalezienie przynajmniej jednej liczby pierwszej są znakomite. Prawie na pewno nam się to uda przy $p < 100$. Jedynie dla $p = 37$ wszystkie liczby powyższej postaci są złożone. Najmniejsze n , dające według wzoru $\frac{n^{37} - 1}{n - 1}$ liczbę pierwszą, jest równe 61.

16. Liczby pierwsze p , dla których liczba $2p + 1$ też jest pierwsza, nazywamy liczbami pierwszymi Zofii Germain. Oto pełna lista liczb pierwszych Zofii Germain mniejszych od 1000: 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443, 491, 509, 593, 641, 653, 659, 683, 719, 743, 761, 809, 911, 953.

Nietrudno policzyć, że powyższa lista zawiera 37 pozycji.

17. Istnieje 37 czwórek nieparzystych liczb pierwszych różniących się ostatnią cyfrą i mniejszych od 100 000. Oto pełna lista tych liczb z usuniętą ostatnią cyfrą (ostatnia cyfra w poszczególnych liczbach każdej czwórki jest równa 1, 3, 7 i 9): 1, 10, 19, 82, 148, 187, 208, 325, 346, 565, 943, 1300, 1564, 1573, 1606, 1804, 1891, 1942, 2101, 2227, 2530, 3172, 3484, 4378, 5134, 5533, 6298, 6721, 6949, 7222, 7726, 7969, 8104, 8272, 8881, 9784, 9913.

18. Najmniejszą liczbą pierwszą, której pierwiastek kwadratowy ma na pierwszym miejscu po przecinku zero, jest 37. Mamy $\sqrt{37} = 6,08276253 \dots$

19. Wylosowano liczbę dwucyfrową, a następnie podniesiono ją do szóstej potęgi. Odgadnąć sumę cyfr tak otrzymanej liczby.

Rozwiązanie: No cóż, musimy zgadywać. Najlepiej powiedzieć 37, gdyż spośród 90 liczb dwucyfrowych aż 19 (ponad 20%) prowadzi do tego wyniku. Na drugim miejscu jest liczba 46, która pojawia się w 14 przypadkach.

20. Podobnie, sześciany liczb pierwszych mniejszych od 2000 mają najczęściej sumę cyfr 37 (w 53 przypadkach na 303). Drugie miejsce zajmuje liczba 35 z 45 wystąpieniami.

21. Cóżby miało znaczyć, że liczba pierwsza jest nietuzinkowa? Pewnie tyle, że nie jest ona dwunastą liczbą pierwszą. W takim razie 37 jest tuzinkową liczbą pierwszą.

22. Jeśli więc p_n oznacza n -tą liczbę pierwszą, to $p_{12} = 37$. Wzór ten jest odporny na zmianę kolejności cyfr, mamy bowiem $p_{21} = 73$.

23. Występujące powyżej liczby 37, 12 i 73 związane są zależnością: $12\sqrt{37} \approx 73$ (dokładniej: 72,993).

24. Nierówność $p_n > 3n$ zachodzi wtedy i tylko wtedy, gdy $p_n \geq 37$.

25. Jeżeli $p_n = 37$, to liczby $p_n - n$ i $p_n + n$ są kwadratami kolejnych liczb pierwszych p_3 i p_4 . Zauważmy, że przy tym $p_{3 \cdot 4} = 37$.

26. Kwadrat liczby pierwszej otrzymamy także dopisując do liczby 37 iloczyn jej cyfr: $3721 = 61^2$.

27. 37-mą liczbą nieparzystą jest 73.

28. Łatwo zapamiętać przybliżoną wartość pierwiastka sześciennego z 37. Mamy bowiem $\sqrt[3]{37} \approx 3,33$ (trochę dokładniej: 3,332222).

29. Liczba 37 jest różnicą kolejnych sześciątów: $37 = 4^3 - 3^3$.

30. Liczba 37 daje się zapisać za pomocą pięciu trójek $37 = \frac{333}{3 \cdot 3} = 33 + 3 + \frac{3}{3}$.

31. Liczba 37 daje się też zapisać za pomocą sześciu jedynek $37 = \frac{111}{1 + 1 + 1} = ((1 + 1 + 1)!)^{1+1} + 1$.

32. Suma liczb naturalnych mniejszych od 37 jest równa $\binom{37}{2} = 666$.

33. Równie ciekawą liczbę otrzymujemy, mnożąc 37 przez iloczyn jej cyfr: $37 \cdot 3 \cdot 7 = 777$.

34. Jak odwrócić 37 modulo 100 (tzn. znaleźć takie r , że $37r \equiv 1 \pmod{100}$)? Wystarczy odwrócić kolejność cyfr, mamy bowiem $37 \cdot 73 \equiv 1 \pmod{100}$.

35. A jak odwrócić 37 modulo 137? Wystarczy wykonać odejmowanie $137 - 37$, gdyż $37 \cdot 100 \equiv 1 \pmod{137}$.

36. Liczbę n -cyfrową zapisano trzy razy z rzędu, otrzymując liczbę $3n$ -cyfrową. Czy tak otrzymana liczba musi dzielić się przez n^2 ? Jeżeli $n = 37$, to tak. Nie sądzę, aby istniała inna liczba większa od 1 o tej własności.

37. Czy wielokąt może mieć wszystkie kąty wewnętrzne większe niż 170° ? Tak, ale musi to być co najmniej 37-kąt.

JWR