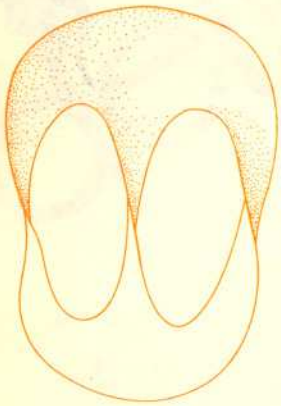
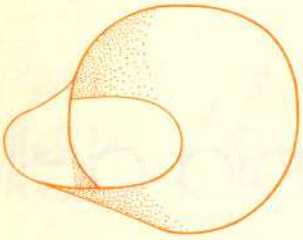
Rozwiązanie zadania M 216

a)



b)



Pochwała ścisłości

Fizykę przenikają dwa nurty, dwa różne style tworzenia nowych odkryć. Jeden z nich — to wykrywanie ścisłych, na ogół prostych, matematycznych reguł, które przyroda realizuje tylko w przybliżeniu albo w skrajnie wyidealizowanych i praktycznie nieosiągalnych warunkach. Drugi — to próby uchwycenia rzeczywistych procesów zachodzących w przyrodzie, w całej ich komplikacji i złożoności, jednak przy niedokładnej znajomości rządzących nimi ogólnych praw. Przykładem odkrycia pierwszego typu jest teoria grawitacji Newtona. To prawda, że stosuje się ona do rzeczywistości tylko w przybliżeniu, ponieważ żaden realny układ fizyczny nie spełnia jej założeń.

Na przykład, ruch Ziemi wokół Słońca da się opisać przez ścisłe rozwiązanie równań ruchu Newtona dla punktu materialnego w polu grawitacyjnym o symetrii kulistej. Opis ten jest jednak tylko przybliżony, nie uwzględnia bowiem faktu, że oprócz Ziemi okrążają Słońce inne planety, które także oddziałują grawitacyjnie z Ziemią i zaburzają jej orbitę. Nie uwzględnia faktu, że Ziemia krąży wokół wspólnego środka masy z Księżycem, faktu, że Słońce nie jest dokładnie kulą, że przestrzeń międzyplanetarna nie jest dokładnie pusta, lecz wypełniona cząstkami pyłu i wiatru słonecznego, które hamują obieg Ziemi przez tarcie. Jeśli wziąć pod uwagę te wszystkie efekty, opis orbity Ziemi staje się dokładniejszy, lecz tak skomplikowany, że mogą się nim posługiwać tylko komputery. A mimo to ...

Ten skomplikowany opis powstaje po prostu przez sumowanie oddziaływań grawitacyjnych Ziemi ze Słońcem, Księżycem i planetami, z których każde osobno wyraża się tym samym, genialnie prostym i łatwym do zapamiętania prawem

$$F = -G \cdot m_1 \cdot m_2 \cdot \frac{r}{r^3}.$$

Mimo więc, że nie potrafimy ująć jednym równaniem rzeczywistych torów planet, potrafimy je sobie poskładać z prostszych elementów, które dobrze znamy i rozumiemy dzięki Newtonowi. Jakże prymitywnie i ubogo wygląda w porównaniu z tym taki np. opis profilu prędkości dla przepływu turbulentnego cieczy ponad płaską powierzchnią szorstką, oparty na równaniu:

$$\frac{u}{\sqrt{\tau_0/\varrho}} = 8{,}48 + 5{,}75 \ln\left(\frac{y}{K}\right),$$

gdzie u — prędkość cieczy w punkcie odległym o y od powierzchni, K — charakterystyczny rozmiar elementów szorstkich (ziarna piasku lub zagłębienia), τ_0 — naprężenie na powierzchni dna, ϱ — gęstość cieczy.

Równanie to ma odtwarzać pewne cechy przepływu ściśle i wiernie, lecz w rzeczywistości nie pozwala nam zrozumieć elementów dynamiki przepływu i odzwierciedla tylko naszą słabość i bezradność, której wyrazem są całkowicie niezrozumiałe współczynniki liczbowe. Zostało ono dopasowane do pewnego małego zbioru wyników doświadczalnych i nie jest w stanie objaśnić niczego ponadto. Wystarczy, żeby dno kanału stało się gładkie lub przestało być płaskie, i już trzeba uciekać się do całkiem innych równań, w żaden widoczny sposób nie powiązanych z powyższym. Jest to sytuacja typowa dla drugiego spośród omawianych stylów pracy naukowej. Stanowczo opowiadam się za pierwszym.

Uniwersalny szyfr

W naszych czasach coraz więcej rzeczy staje się tajnych. To dlatego, że nasze życie jest coraz bardziej uzależnione od setek i tysięcy drobiazgów, a kontrolę nad nimi każdy chce zachować dla siebie. Przyjdzie może czas, kiedy na posiadanie tablic logarytmicznych wymagane będzie zezwolenie. Żarty? Mam nadzieję. Na razie grozi nam utajnienie tablic rozkładów liczb na czynniki pierwsze. A oto dlaczego.

Każdy szyfr ma jedną zasadniczą wadę: jeżeli znamy sposób szyfrowania, to i deszyfrowania. Dlatego im więcej osób może przesyłać nam zaszyfrowane wiadomości, tym łatwiej policja rozpracuje naszą siatkę. Nawet, gdy używamy tak doskonałego szyfru, jak ten opisany w przygodach dzielnego wojaka Szwejka (tom III, „*Przesławne lanie*"). Każdy z nas bez wahania założyłby się, że znajomość sposobu szyfrowania umożliwia odczytanie każdej zaszyfrowanej wiadomości. A tymczasem rzecz ma się trochę inaczej. Oto jak grupa osób może ustalić system szyfrów tak, by

1) każda z osób mogła ogłosić publicznie (na przykład w gazecie): adresowane do mnie wiadomości proszę szyfrować tak a tak. Szyfrowaną wiadomość (adresowaną do jednej z osób tej grupy) może wysłać dowolna, niekoniecznie wtajemniczona osoba. Dowolna osoba może ogłosić: przystępuję do spółki; proszę przeznaczone dla mnie wiadomości szyfrować tak a tak, oraz, by

2) zaszyfrowanego komunikatu nie mógł odczytać nikt poza adresatem.

Do zbudowania takiego szyfru posłużono się teorią liczb. Oto nieskomplikowane twierdzenie: *Jeżeli liczba naturalna N jest iloczynem dwu liczb pierwszych p, q, to dla* $M = (p-1)(q-1)+1$ *i dla każdego* $n < N$ *zachodzi*

$$n^M \equiv n \pmod{N};$$

tj. n^M i n dają z dzielenia przez N tę samą resztę.

Każda z osób, chcących mieć własny szyfr, wybiera sobie dwie dość duże liczby pierwsze (co najmniej kilkudziesięciocyfrowe) p, q, oblicza ich iloczyn N, oraz liczbę $M = (p-1)(q-1)+1$. Do wiadomości ogólnej podaje N i pewien dzielnik liczby M, oznaczmy go przez K. Dla siebie zachowuje rozkład N na p i q oraz liczbę M.

Gdy nadawca **NAD** chce wysłać wiadomość do odbiorcy **ODB**, postępuje tak. Zamienia tekst słowny na ciąg cyfr w jakiś standardowy, ustalony i jawny sposób, np. A = 1, B = 2 itd. Otrzymaną tak dużą liczbę (komunikat nie może być długi) podnosi do potęgi K_{ODB} i bierze resztę z dzielenia przez N_{ODB}. Potrzebna jest do tego maszyna matematyczna, ale nic ponadto. Tak zakodowaną wiadomość (będącą teraz liczbą mniejszą niż N_{ODB}) wysyła się do odbiorcy lub publikuje w gazecie. Odbiorca winien podnieść tę liczbę do potęgi $\frac{M_{ODB}}{K_{ODB}}$ — otrzyma wtedy ciąg liczb wysłany przez nadawcę. Przetworzenie go na tekst słowny odbywa się we wspomniany jawny i standardowy sposób.

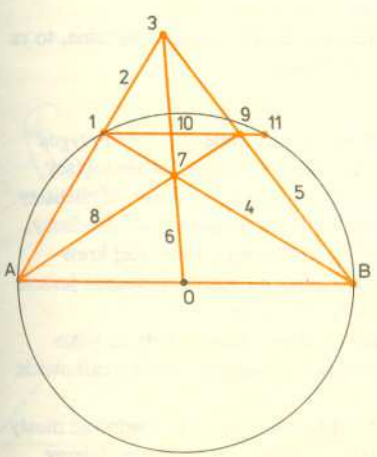
Co w tym takiego rewelacyjnego? — zapytacie. A to, że podniesienie nawet bardzo dużej liczby do bardzo dużej potęgi M jest dla maszyny matematycznej mało pracochłonne, zwłaszcza że wszystkie obliczenia robi się i tak modulo N. Wynik dostaje się w ułamku sekundy. Osoba postronna nie zna jednak liczby M; mogłaby ją obliczyć, znając p i q. Ale zna tylko N, równe pq. Gdy p i q mają po kilkadziesiąt cyfr, N ma sto kilkadziesiąt. Znalezienie rozkładu takiej liczby na czynniki nawet najszybciej działającej maszynie zajęłoby (przy obecnym stanie techniki, informatyki i organizacji maszyn cyfrowych) wiele, wiele lat pracy.

Szyfr ten nie daje się złamać najgroźniejszą bronią: analizą statystyczną, rozpracowującą szybko wszystkie szyfry polegające na stałym przyporządkowaniu litera-liczba. Autorzy tego szyfru napisali (w *Scientific American*), że są niezbicie pewni, iż nikt nie potrafi odczytać zaszyfrowanej przez nich do samych siebie wiadomości.

Tylko linijką

Jeżeli mamy na kartce papieru narysowany okrąg z zaznaczonym środkiem O, to możemy bez trudu samą linijką wpisać w ten okrąg kwadrat. Robi się to w następujący sposób (rysunek podzieliliśmy na dwa etapy): Prowadzimy dowolną średnicę. Jej końce oznaczamy A i B. Obieramy na okręgu jeszcze jeden punkt *1*. Na prostej *2* przechodzącej przez A i *1* obieramy na zewnątrz okręgu punkt *3*. Łączymy *1* z B prostą *4*, *3* z B prostą *5* i *3* z O prostą *6*. Przez punkt *7* leżący na prostych *4* i *6* prowadzimy prostą *8* do przecięcia z *5* w punkcie *9*. Prosta *10* łącząca *1* i *9* przecina okrąg w punkcie *11*. Przez B i *11* prowadzimy prostą *12* do przecięcia z *2* w punkcie *13*. Prosta *14* łącząca O i *13* przecina okrąg w punktach C i D. Czworokąt $ACBD$ jest kwadratem, co Czytelnik z łatwością udowodni wykazując, że prosta *10* jest równoległa do AB (pierwszy rysunek), zaś kąt AOC jest prosty (drugi rysunek).

Półtora wieku temu Steiner wykazał, że każda konstrukcja wykonalna cyrklem i linijką jest wykonalna samą linijką, o ile tylko mamy do dyspozycji (być może nawet dość daleko, ale na tej samej karcie) jeden narysowany okrąg z zaznaczonym środkiem. Można spróbować dowieść, że tak jest w istocie, lub znaleźć steinerowską konstrukcję dla jakiegoś wybranego zadania.



W okrąg z zaznaczonym środkiem można wpisać kwadrat za pomocą samej linijki