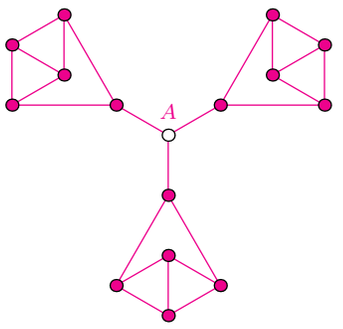
Rozwiązanie zadania M 1605.
Odpowiedź: Nie wynika.

Na poniższym obrazku zilustrowana jest przykładowa sieć znajomości (uczestnikom konferencji odpowiadają punkty, a znajomościom – odcinki), dla której stosowne zakwaterowanie nie istnieje.



Rzeczywiście, niezależnie od sposobu zakwaterowania osoby A, pozostali uczestnicy dzielą się na dwie grupy 5-osobowe i jedną 4-osobową o tej własności, że każdy ma niezakwaterowanych dotąd znajomych tylko w obrębie danej grupy. Żadnej z grup 5-osobowych nie da się zakwaterować w dwuosobowych pokojach.

Wykorzystując przedstawioną teorię, możemy zaproponować następujący protokół prywatnego uzyskiwania informacji dla jednej bazy danych (Dobromira):

(a) Bogumił i Dobromir umawiają się na reprezentację ciągu $\boldsymbol{x}$ w postaci tablicy $\boldsymbol{X} = [\overline{x}_{k,l}]_{k\leqslant s, l\leqslant t}$. Załóżmy, że $x_i = \overline{x}_{\alpha,\beta}$;

(b) Bogumił wybiera duże liczby pierwsze p, q (których reprezentacja dwójkowa ma K bitów) i oblicza $n = pq$, po czym wybiera losowo $y_1, \ldots, y_s \leqslant n$ w taki sposób, że $y_\alpha \in \mathcal{O}_n$ oraz $y_k \in \mathcal{Q}_n$ dla $k \neq \alpha$. Następnie przekazuje n oraz wszystkie liczby $y_1, \ldots, y_s$ Dobromirowi. Zauważmy, że zgodnie z naszą uwagą Dobromir (nieznający p, q) dla żadnego $k \leqslant s$ nie jest w stanie stwierdzić, czy $y_k \in \mathcal{Q}_n$, nie dowie się zatem niczego o α;

(c) Dla każdego $r \leqslant t$ Dobromir oblicza $z_r = \prod_{k=1}^{s} y_k^{1+\overline{x}_{k,r}}$ modulo n. Jest to iloczyn wszystkich wysłanych liczb y_k, przy czym niektóre – te, którym w r-tej kolumnie odpowiada jedynka – mnożone są „w kwadracie”. Ponieważ tylko y_α nie jest kwadratem modulo n, więc z_r jest kwadratem tylko wtedy, gdy y_α jest mnożone „w kwadracie”, czyli gdy $x_{\alpha,r} = 1$;

(d) Bogumił sprawdza, czy z_β jest kwadratem (może to uczynić, gdyż zna p, q). Jeśli tak, to $x_{\alpha,\beta}$ wynosi 1, w przeciwnym przypadku 0.

Przedstawiona komunikacja zajmuje $Ks + Kt$ bitów, czyli w ten sposób, biorąc $s = t \approx \sqrt{n}$, możemy już osiągnąć komunikację rozmiaru $2K\sqrt{n}$. A można jeszcze lepiej! Zauważmy, że spośród skonstruowanych przez Dobromira liczb $z_1, \ldots, z_t$ Bogumiła interesuje tylko z_β, przy czym nie chce on, by Dobromir poznał β. Toż to brzmi dokładnie jak wyjściowy problem, więc rzecz pachnie rekurencją na kilometr! Bogumił może zastosować ten sam protokół dla ciągu $z_1, \ldots, z_t$, aby poznać z_β. Wówczas rozmiar komunikacji jest rzędu $Ks + K \cdot 2K\sqrt{t}$; optymalizując ze względu na s, t, pod warunkiem $st = n$, dostajemy koszt $3K^{5/3}\sqrt[3]{n}$. W ten rekurencyjny sposób możemy dowolnie zbijać wykładnik przy n (odwrotnie proporcjonalnie do głębokości rekurencji); niestety, kosztem puchnącego (z grubsza liniowo wraz z głębokością rekurencji) wykładnika przy K. Cóż, odwołując się do klasyka, nie udało nam się przyrządzić zupełnie darmowego obiadu, mamy jednak nadzieję, że Czytelnicy i tak docenią (podobnie jak Bogumił) chytrość i elegancję przedstawionych protokołów.

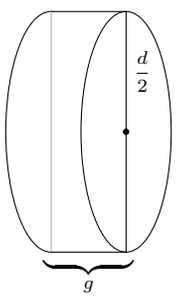
Kto ma rację?

*Jarosław GÓRNICKI**

* Wydział Matematyki i Fizyki Stosowanej, Politechnika Rzeszowska

Skończył się mecz – najważniejsze wydarzenie tygodnia. Po burzliwej wymianie zdań na jego temat trzej przyjaciele: Długi, Gruby i Ludek wracali do domu. Nagle Ludek zapytał o zadanie z matematyki, które było na jutro. Długi i Gruby stanęli jak zaczarowani. Zapomnieli o zadaniu. W necie na chwilę się zagotowało! Nastała cisza przerywana wiadomościami przychodzącymi na komórki. Nikt z klasy jeszcze zadania nie zrobił. Zadanie było krótkie:

Jak gruba powinna być moneta, aby szansa, że wyląduje ona na krawędzi, wynosiła $\frac{1}{3}$?

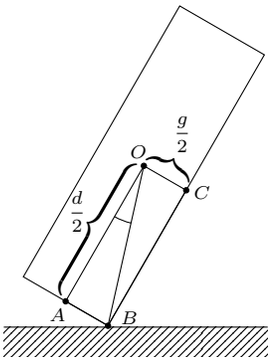


Rys. 1

Wszyscy zgodzili się przyjąć uproszczenie, że moneta jest jednorodnym, symetrycznym walcem. Gruby, który początkowo zbladł i spocił się, nieśmiało zgłosił pomysł. Posmarujemy deskę miodem (by rzucana moneta nie odbijała się i nie toczyła), sklejając pięciogroszówki stworzymy kilka wariantów „grubych” monet i na podstawie eksperymentu wybierzemy odpowiedź.

Długi uznał, że zadanie jest łatwe i szkoda miodu. To, na której „stronie” wyląduje moneta, jest proporcjonalne do pola powierzchni poszczególnych „stron”. Zatem warunki zadania będą spełnione, gdy pole powierzchni bocznej walca będzie równe polu podstawy. Obliczył (rys. 1):

$$2 \cdot \pi \cdot \frac{d}{2} \cdot g = \pi \cdot \left(\frac{d}{2}\right)^2, \quad \text{zatem} \quad 2g = \frac{d}{2}, \quad \text{skąd} \quad g = \frac{1}{4}d.$$



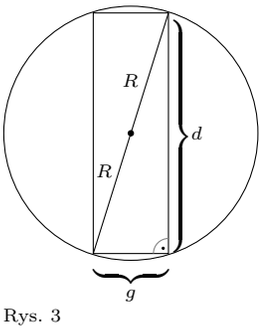
Rys. 2

I triumfalnie oznajmił: grubość monety powinna stanowić 25% długości jej średnicy. Życie jest piękne, a my jesteśmy genialni! Jednak Ludek, który lubił fizykę, nad czymś rozmyślał. Po chwili powiedział, że widzi inne rozwiązanie. Poza przypadkiem, gdy moneta wylądowała od razu na swojej podstawie lub na krawędzi, musiała wylądować koślawie. Miodek chwyta koślawie padającą monetę, która pod wpływem siły ciężkości ostatecznie wyląduje na tej stronie, na której rzut jej środka ciężkości znajdzie się we wnętrzu powłoki wypukłej rzutu tej strony. To zaś zależy od kąta $\sphericalangle AOB$, i tu zrobił rysunek (rys. 2). Warunki zadania będą spełnione, gdy kąt $\sphericalangle AOB$ będzie równy $\frac{1}{3}$ kąta prostego $\sphericalangle AOC$. Przy oznaczeniach z rysunku

$$\frac{\frac{1}{2}g}{\frac{1}{2}d} = \operatorname{tg} 30^\circ = \frac{\sqrt{3}}{3}, \quad \text{skąd } g = \frac{\sqrt{3}}{3}d \approx 0{,}577 \cdot d.$$

Oznacza to, że grubość monety spełniającej warunki zadania powinna wynosić 57,7% długości jej średnicy. *No to mamy problem*, przyznali chłopcy, ale najważniejsze było dla nich, że na lekcję nie pójdą z niczym.

Gruby po powrocie do domu zaczął szukać czegoś na temat zadania w necie. Znalazł fascynującą historię. Pewnego razu, gdy John von Neumann wraz z uczonymi kolegami wysiadał z taksówki, taksówkarz zadał mu pytanie, które jest treścią naszego zadania. Ku niemałemu zdziwieniu kolegów, po jakichś 15–20 sekundach von Neumann ocenił, że grubość takiej monety powinna stanowić około 35% długości jej średnicy. Jak rozumował von Neumann, możemy się tylko domyślać.



Rys. 3

Federick Mosteller widział to tak (*Fifty challenging problems in probability with solutions*, Dover Publ., N. York, 1965, Problem 38). Na monecie (= walcu) opisana jest sfera o promieniu R (rys. 3). Tę sferę tworzą wszystkie możliwe wektory momentu siły znormalizowane do długości R, zaczepione w środku ciężkości walca. Są to też wszystkie możliwe kierunki rzutu środka ciężkości walca. Aby spełnić warunki zadania, trzecia część powierzchni kuli powinna przypadać na sytuację, gdy rzut środka ciężkości pozwala na lądowanie monety na krawędzi. Ponieważ pole warstwy kulistej jest proporcjonalne do jej grubości ($= 2\pi Rg$), więc nasza moneta powinna mieć grubość równą $\frac{1}{3}$ średnicy sfery opisanej na monecie. Zatem

$$g = \frac{1}{3} \cdot 2R, \quad \text{czyli } 2R = 3g.$$

Pozostaje obliczyć grubość takiej monety w stosunku do jej średnicy. Tu wystarczy Pitagoras:

$$g^2 + d^2 = (2R)^2, \quad \text{skąd } g = \frac{1}{2\sqrt{2}}d \approx 0{,}353 \cdot d.$$

Kto ma rację?

Dowody „just-do-it” w zadaniach o przeliczalności

*Robert CRUMPLIN**

*student, Uniwersytet Cambridge

We wrześniu 2018 *roku miał miejsce kolejny, trzeci międzynarodowy obóz matematyczny Maths Beyond Limits, odbywający się corocznie w Milówce koło Żywca. W zeszłym roku wzięło w nim udział* 60 *licealistów z* 12 *europejskich państw. Rekrutacja uczestników na tegoroczny obóz jest już zakończona, natomiast potencjalni tutorzy wciąż mogą zgłaszać się do prowadzenia zajęć. Szczegóły dotyczące aplikacji oraz obozu dostępne są na stronie* `mathsbeyondlimits.eu`

Przeliczalnie wiele, czyli tyle, że można je ponumerować liczbami naturalnymi.

W zeszłym roku (już po raz drugi!) miałem przyjemność pełnić funkcję tutora podczas obozu Maths Beyond Limits. Poprowadziłem dwie serie zajęć, z których jedna dotyczyła teorii mnogości. Starając się dać uczestnikom podstawy arytmetyki zbiorów nieskończonych w zajmujący i bezbolesny, mam nadzieję, sposób, pokazałem ciekawe zadania, wykorzystujące różne metody i pomysły. Jeden z nich jest szczególnie warty uwagi...

Zadając proste pytanie „Czy istnieje zbiór [...] spełniający warunki [...]?”, można wygenerować wiele zadań. Niektórzy nawet zaznaczą, że *przeliczalnie* wiele. Struktura zbiorów jest na tyle prosta, że jeśli rozwiązanie istnieje (i przypadkiem nie jest równoważne *hipotezie continuum*), prawdopodobnie znajdziemy je, korzystając z podstawowych własności funkcji działających