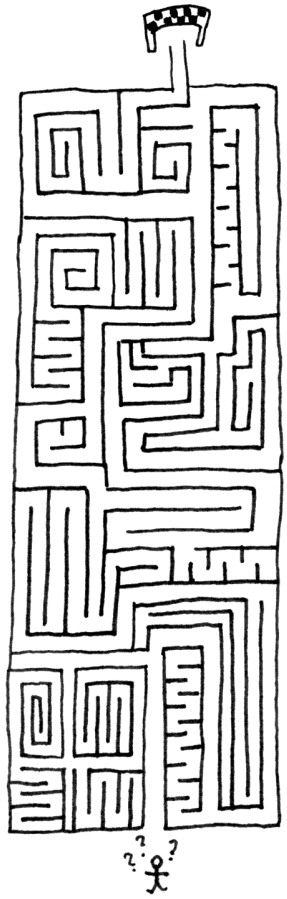
Czy każdy problem da się rozwiązać?

Wojciech CZERWIŃSKI

Czy każdy problem da się rozwiązać? Pesymiści odpowiedzą, że nie – życie nie jest łatwe. A optymiści? Być może niektórzy powiedzą, że przy odpowiednim podejściu tak. Nie będziemy jednak z nimi dyskutować, bo Czytelnicy *Delty* dobrze wiedzą, że nie chodzi nam tutaj przecież o życiowe problemy. Trzeba więc sprecyzować pytanie: co uważamy za problem i czym miałoby być jego rozwiązanie?



Przyjrzymy się najpierw kilku przykładom problemów, którymi będziemy się zajmować.

1. Dana jest liczba naturalna, czy jest to liczba pierwsza?
2. Dana jest liczba naturalna, oblicz jej kwadrat.
3. Dane jest słowo, czy jest ono palindromem (palindrom to słowo, które brzmi tak samo czytane od tyłu, np. kajak)?
4. Dane jest słowo, oblicz, ile ma różnych liter.
5. Dana jest liczba rzeczywista, oblicz jej pierwiastek.
6. Dany jest graf, czy z każdego wierzchołka da się przejść do każdego?

Już na tych przykładach możemy zauważyć, że nasze problemy są różnorakich rodzajów. Jedne domagają się jedynie odpowiedzi TAK lub NIE, inne natomiast chcą, żeby podać im jakiś bardziej skomplikowany obiekt, często liczbę. Pierwszy rodzaj problemów będziemy nazywać *problemami decyzyjnymi*, a drugi *problemami obliczeniowymi*. Wśród naszych przykładów problemy decyzyjne mają numery 1, 3 i 6, a problemy obliczeniowe 2, 4 i 5. Skupimy się głównie na problemach decyzyjnych.

Czym jednak ma być rozwiązanie takiego problemu? Domyślni Czytelnicy pewnie już wiedzą: oczekiwanym rozwiązaniem jest program, który wczytuje wejście, np. liczbę naturalną, a na końcu swojego działania zwraca odpowiedź TAK lub NIE. Czy więc każdy problem da się rozwiązać? Okazuje się, że nie!

Najprostszy argument za tym, że istotnie nie każdy problem można rozwiązać, jest taki, że możliwych problemów jest więcej niż możliwych rozwiązań (czyli programów). To stwierdzenie może nam się wydać dziwne, przecież zarówno problemów, jak i programów jest nieskończenie wiele. Czy możemy w ogóle mówić, że jedna nieskończoność jest większa niż druga i co by to miało znaczyć? Możemy! Żeby to zrozumieć, musimy zagłębić się trochę w *teorię mocy*, dziedzinę matematyki, która zajmuje się wielkościami zbiorów. A teoria, którą zobaczymy, sama w sobie jest niezwykle ciekawa.

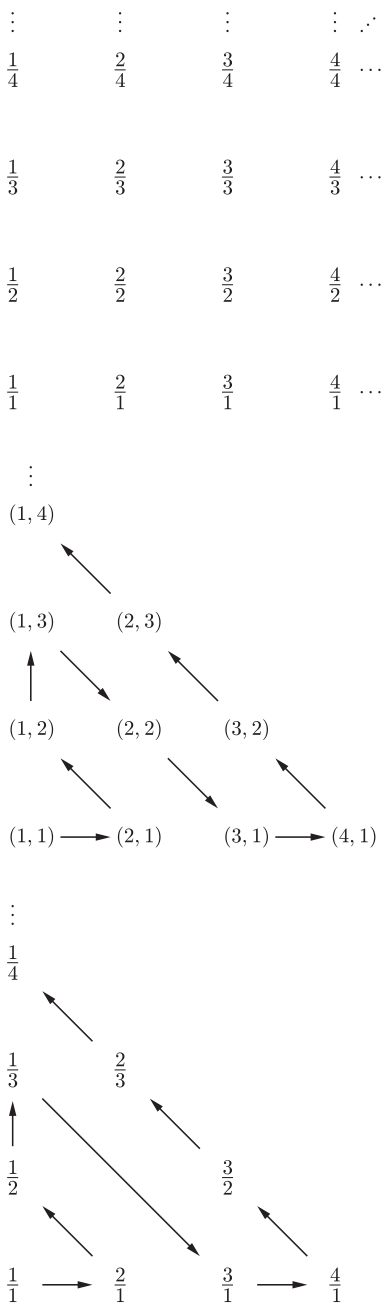
Równoliczność

Dla dwóch zbiorów skończonych A i B intuicyjnie mówimy, że są równoliczne, jeśli po prostu wielkość jednego jest równa wielkości drugiego. Można jednak powiedzieć, że A i B są równoliczne, jeśli elementy A i elementy B da się połączyć w pary: w każdej parze jeden element z A i jeden z B, tak, żeby wszystkie elementy trafiły do którejś pary, ale żaden nie trafił do dwóch par. Okazuje się, że ta druga definicja jest właściwym spojrzeniem na sprawę i bardzo dobrze zachowuje się również dla zbiorów nieskończonych. Spójrzmy teraz na kilka przykładów nieskończonych zbiorów równolicznych. Czy zbiór liczb całkowitych dodatnich $A = \{1, 2, 3, \ldots\}$ i zbiór liczb całkowitych większych od dziesięciu $B = \{11, 12, 13, \ldots\}$ są równoliczne? Tak, łatwo zobaczyć, że można elementy obu zbiorów poustawiać w nieskończenie wiele par: $(1, 11), (2, 12), (3, 13), \ldots$. To już może nam się wydać dziwne, przecież zbiór $\{11, 12, 13, \ldots\}$ powstał przez usunięcie ze zbioru $\{1, 2, 3, \ldots\}$ dziesięciu liczb: $1, 2, \ldots, 10$, jak więc może być równoliczny? Może – taka jest nasza definicja, musimy po prostu pożegnać się z intuicją wziętą ze skończonych zbiorów, że jeśli usuwamy coś ze zbioru, to staje się on istotnie mniejszy. Teraz będą się działy rzeczy jeszcze dziwniejsze. Czy zbiór dodatnich liczb całkowitych $A = \{1, 2, 3, \ldots\}$ jest równoliczny ze zbiorem dodatnich liczb parzystych $B = \{2, 4, 6, \ldots\}$? Nietrudno zauważyć, że tak, połączenie w pary wygląda następująco: $(1, 2), (2, 4), (3, 6), \ldots$, każda liczba ze zbioru A jest w parze

Rozwiązanie zadania M 1508.
Niech r_i, p_i i S_i oznaczają dla $i = 1, 2, 3, 4$ odpowiednio promienie okręgów wpisanych, obwody i pola powstałych czterech trójkątów. Wiemy, że wówczas dla każdego i zachodzi równość $S_i = \frac{1}{2} r_i p_i$. W takim razie

$$q \geqslant 2 \sum_{i=1}^{4} r_i = 4 \sum_{i=1}^{4} \left(\frac{S_i}{p_i} \right) > \\ > 4 \sum_{i=1}^{4} \left(\frac{S_i}{p} \right) = \frac{4S}{p},$$

co daje tezę.



W ogólności ta sama liczba może mieć dwa różne rozwinięcia dziesiętne, np. $0,4999\ldots = 0,5000\ldots$, jednak nie jest to możliwe wśród rozwinięć zawierających jedynie zera i jedynki.

z dwa razy większą liczbą ze zbioru B. Możemy teraz dokonać obserwacji, dzięki której później łatwiej będzie nam sprawdzać, czy pewien zbiór S jest równoliczny ze zbiorem liczb naturalnych $\mathbb{N}$ (zakładamy tu, że 0 też jest liczbą naturalną). Zauważmy mianowicie, że nieskończony zbiór S jest równoliczny z $\mathbb{N}$ wtedy i tylko wtedy, gdy da się ustawić elementy S w nieskończony ciąg. Po pierwsze, jeśli istotnie S jest równoliczny z $\mathbb{N}$, to ustawienie w nieskończony ciąg jest łatwe: najpierw stoi element będący w parze z 0, potem element będący w parze z 1, potem element będący w parze z 2 itd. Z drugiej strony jeśli umiemy ustawić elementy S w nieskończony ciąg, to możemy połączyć je w pary w elementami $\mathbb{N}$: pierwszy element ciągu będzie w parze z 0, drugi będzie w parze z 1, a ogólnie k-ty element ciągu będzie w parze z liczbą naturalną $k-1$.

Zastanówmy się teraz, czy zbiór liczb naturalnych jest równoliczny ze zbiorem wszystkich liczb całkowitych $\mathbb{Z}$. Nietrudno zobaczyć, że tak, elementy zbioru liczb całkowitych da się ustawić w nieskończony ciąg, na przykład w taki sposób:

$$-1, 0, -2, 1, -3, 2, -4, 3, -5, 4, -6, 5, -7, 6, -8, 7, -9, 8, -10, 9, -11, 10, -12, 11, -13, 12, -14, 13, \ldots$$

na miejscach nieparzystych będziemy ustawiać coraz większe liczby nieujemne, a na miejscach parzystych coraz mniejsze liczby ujemne. Pokażemy teraz nawet więcej: że zbiór dodatnich liczb wymiernych $\mathbb{Q}_+$ jest równoliczny ze zbiorem liczb naturalnych. To wygląda bardzo dziwnie, bo przecież liczb wymiernych wydaje się dużo więcej, przyjrzyjmy się jednak konstrukcji. Wyobraźmy sobie nieskończoną tablicę ułamków, gdzie w k-tej kolumnie i n-tym wierszu od dołu wpisujemy ułamek $\frac{k}{n}$. Pokażemy teraz, jak wszystkie elementy $\mathbb{Q}_+$ ustawić w nieskończony ciąg. Będziemy chodzić po tablicy zygzakiem i dodawać nowe liczby wymierne do ciągu. Najpierw ustalmy trasę przemarszu. Zaczniemy z pola $(1,1)$, pójdziemy w prawo do $(2,1)$ i po skosie do $(1,2)$. Teraz w górę do $(1,3)$ i po skosie przez $(2,2)$ do $(3,1)$. Teraz w prawo do $(4,1)$ i po skosie przez dwa pola do $(1,4)$. W ten sposób kontynuujemy chodzenie po kolejnych skosach coraz dalszych od pola $(1,1)$. A jak tworzymy ciąg? Jeśli wchodzimy na pewne pole i ułamek przez nas zobaczony jest nową liczbą (czasem może się zdarzyć, że tę liczbę już widzieliśmy, np. $\frac{2}{2} = \frac{1}{1}$), to dodajemy go na koniec i idziemy dalej. Czyli początkowe wartości nieskończonego ciągu wyglądają następująco: $1/1 = 1$, $2/1 = 2$, $1/2$, $1/3$ ($2/2$ nie ustawiamy, bo $2/2 = 1 = 1/1$ i ta liczba już jest w ciągu), $3/1 = 3$, $4/1$, $3/2$ itd. Nietrudno zauważyć, że wszystkie dodatnie liczby wymierne zostaną kiedyś dodane do ciągu, bo nasz zygzak dojdzie w końcu do każdego ułamka. Co więcej, żadna liczba nie zostanie przydzielona więcej niż raz. Pokazaliśmy więc, że liczby naturalne i dodatnie liczby wymierne są równoliczne. Niewiele więcej wysiłku potrzeba, żeby pokazać, że zbiór wszystkich liczb wymiernych jest również równoliczny z $\mathbb{N}$ (Czytelników Ambitnych zachęcamy do samodzielnego stworzenia odpowiedniego ciągu).

Metoda przekątniowa

Czyż więc istnieją w ogóle zbiory nieskończone, które nie są równoliczne z $\mathbb{N}$? Tak, i to jest treścią słynnej konstrukcji Georga Cantora, który w roku 1891 wskazał pierwszy taki przykład. Konstrukcja zwana jest *przekątniową*, zaraz zobaczymy dlaczego. Metoda przekątniowa, czyli konstrukcje tego typu stały się standardem w matematyce, zresztą i w naszej historii jeszcze się pojawią. Pokażemy teraz, że liczby rzeczywiste nie są równoliczne z liczbami naturalnymi, a konkretnie, że nie da się ustawić ich w ciąg. Wystarczy wykazać, że nawet liczb rzeczywistych, które zaczynają się od 0 i mają rozwinięcia dziesiętne po przecinku zawierające tylko zera i jedynki, nie da się ustawić w nieskończonym ciągu.

Przypuśćmy nie wprost, że jednak da się je ustawić w ciąg: $r_1, r_2, r_3, \ldots$. Przyjmijmy oznaczenie $r_i[j]$ na j-tą cyfrę po przecinku w rozwinięciu dziesiętnym liczby r_i. Skonstruujemy teraz liczbę r, która zawiera tylko zera i jedynki po przecinku, ale nie występuje w ciągu, co doprowadzi do sprzeczności. Zaczynamy zerem przed przecinkiem, a jej i-tą cyfrę po przecinku definiujemy jako $1 - r_i[i]$. Innymi słowy, zapewniamy, że i-ta cyfra r jest inna niż i-ta cyfra liczby r_i. Czy r może występować w naszym ciągu? Powiedzmy, że występuje, na pewnej pozycji o numerze n. Czyli $r = r_n$. Zaraz, ustaliliśmy jednak, że n-ta cyfra r jest różna od n-tej cyfry r_n. Zatem $r \neq r_n$ i otrzymujemy sprzeczność z założeniem, że wszystkie liczby występują w ciągu. Wykazaliśmy więc, że

zbiory liczb rzeczywistych $\mathbb{R}$ i naturalnych $\mathbb{N}$ nie są równoliczne. Tak naprawdę to wykazaliśmy, że zbiór $\mathbb{N}$ i zbiór nieskończonych ciągów zero-jedynkowych nie są równoliczne. A tak właściwie to wykazaliśmy nawet więcej: że zbiór nieskończonych ciągów zero-jedynkowych jest większy niż $\mathbb{N}$. Bo co oznacza, że nie można go ustawić w nieskończony ciąg? To, że jak byśmy nie wybrali nieskończonego ciągu nieskończonych ciągów zero-jedynkowych, to któreś ciągi zero-jedynkowe nie zostaną wybrane. Jeśli mamy N osób i K krzeseł i jakkolwiek byśmy nie wybrali K osób, by siadły na krzesłach, to pewne osoby będą stać, to znaczy, że $N > K$. Tę intuicję ze skończonych zbiorów możemy przenieść na zbiory nieskończone: nieskończonych ciągów zero-jedynkowych (i liczb rzeczywistych też) jest więcej niż liczb naturalnych. Pozostają tu pewne kłopoty techniczne, jednak da się je przezwyciężyć i pokazać, że z taką definicją większego zbioru wszystko jest w porządku (pisaliśmy o tym w *Delcie* 2/2016 w artykule *Czy trzeba dowodzić rzeczy oczywistych?*).

Problem bez rozwiązania

Jak to wszystko wykorzystać do pokazania, że nie każdy problem da się rozwiązać? Zastanówmy się najpierw, ile jest programów zapisanych za pomocą skończonego alfabetu? Takich ustalonej długości jest, oczywiście, skończenie wiele. Nietrudno więc zauważyć, że wszystkie programy można ustawić w nieskończony ciąg: zaczynamy od najkrótszych, a dla tej samej długości ustawiamy alfabetycznie. A więc programów jest tyle co liczb naturalnych. A ile jest problemów? Skupmy się na problemach decyzyjnych dla liczb naturalnych, już tych będzie dużo. Zauważmy, że dla każdego podzbioru liczb naturalnych $S \subseteq \mathbb{N}$ mamy inny problem decyzyjny: „Czy dana liczba naturalna n należy do zbioru S?" A zatem problemów jest przynajmniej tyle, co podzbiorów liczb naturalnych. Zauważmy jednak, że można łatwo wskazać odpowiedniość między nieskończonymi ciągami zero-jedynkowymi a podzbiorami liczb naturalnych. Zbiorowi $S \subseteq \mathbb{N}$ odpowiada ciąg, który ma jedynki dokładnie na miejscach o indeksach należących do S, a zera w pozostałych miejscach. A zatem problemów decyzyjnych jest przynajmniej tyle, co nieskończonych ciągów zero-jedynkowych, czyli więcej niż liczb naturalnych, czyli więcej niż programów. Tym samym wykazaliśmy, że nie dla każdego problemu decyzyjnego istnieje odpowiadający mu program!

Zastanówmy się jednak chwilę, czy to jest naprawdę satysfakcjonująca odpowiedź. Powinny nas tak naprawdę interesować nie dowolne problemy, tylko takie, które jesteśmy w stanie wyrazić. Wyrazić w jakiś rozsądny, skończony sposób. Czyli właściwie tytułowe pytanie powinno brzmieć: „czy każdy opisany w skończony sposób problem da się rozwiązać?" Tu jednak widać od razu mankamenty naszej metody. Sensownie opisywalnych problemów jest co najwyżej tyle, ile skończonych opisów, więc co najwyżej tyle, ile skończonych tekstów. A skończone teksty, jak już wcześniej mówiliśmy, dadzą się ustawić w nieskończony ciąg (coraz dłuższe, a równie długie alfabetycznie), więc jest ich tyle co liczb naturalnych. Czyli sensownie opisywalnych problemów i ich potencjalnych rozwiązań (programów) jest tyle samo.

Czyżby to jednak oznaczało, że całe wcześniejsze rozważania przydały nam się tylko do tego, żeby rozwiązać głupio sformułowany problem? Bynajmniej! Oprócz tego, że poznaliśmy kawałek ciekawej teorii matematycznej, to użyjemy teraz opisanej wyżej metody przekątniowej, żeby rozwiązać ten już właściwie sformułowany problem.

Nierozstrzygalność

Zdefiniujemy teraz pewną dziwną funkcję, która posłuży nam później do dalszych konstrukcji. Zachęcamy Czytelników do tropienia podobieństw z konstrukcją Cantora. Rozważmy wszystkie programy, które na wejściu oczekują liczby naturalnej i na wyjściu zwracają też liczbę naturalną (zapewne inną). Istnieje ustawienie takich programów od najkrótszych do coraz dłuższych; niech będzie to ciąg $P_1, P_2, P_3, \ldots$. Zdefiniujmy funkcję $F : \mathbb{N} \to \mathbb{N}$ jako $F(n) = 1 + P_n(n)$, czyli 1 plus to, co n-ty program zwraca, gdy dostaje liczbę n. Zastanówmy się teraz, czy istnieje pewien program, który oblicza naszą funkcję, czyli gdy dostanie liczbę k na wejściu, to zwróci liczbę $F(k)$. Zauważmy, że nie

Rozwiązanie zadania F 913.
Kulka, dzięki zapasowi energii kinetycznej, będzie wykonywała pracę qV przeciw siłom pola elektrycznego (q – ładunek kulki, V – przebyta przez nią różnica potencjałów). Energia kulki będzie malała zgodnie ze wzorem $mv_1^2/2 - mv_2^2/2 = qV$. Kulka dosięgnie sfery, jeżeli na jej powierzchni prędkość v_2 jest nieujemna. Dla granicznego przypadku mamy $v_2 = 0$, więc $mv_1^2/2 = qV$, gdzie V – potencjał sfery (przyjęliśmy, że potencjał odległego punktu wystrzelenia kulki wynosi zero). Korzystając z tego, że potencjał sfery wyraża się jako $V = Q/4\pi\epsilon_0 R$, gdzie R to promień sfery, otrzymamy $R = 2qQ/4\pi\epsilon_0 mv_1^2 = 54$ cm. Jeżeli sfera będzie miała mniejszy promień, kulka do niej nie doleci. Zatrzyma się w odległości 54 cm od środka sfery i poleci z powrotem.

jest to możliwe. Przypuśćmy, że pewien program P_j oblicza funkcję F. Wtedy dla każdego $i \in \mathbb{N}$ mamy $P_j(i) = F(i)$. Z drugiej jednak strony z definicji funkcji F otrzymujemy $F(j) = 1 + P_j(j)$. A zatem $P_j(j) = F(j) = 1 + P_j(j)$, sprzeczność. Już tu widać, że pewnych sensownych problemów nie da się rozwiązać, to znaczy nie istnieje program, który oblicza funkcję F. My szukamy jednak problemu decyzyjnego, który nie ma rozwiązania, a obliczenie funkcji F to problem obliczeniowy.

O taki jednak nietrudno. Udowodnimy, że słynny `Problem Stopu` jest nierozstrzygalny, to znaczy, że nie istnieje żaden program, który go rozwiązuje. Problem ten jest następujący: mamy dany program P, pytanie brzmi, czy P zatrzymuje się dla dowolnego wejścia, tzn. czy nie działa przypadkiem w nieskończoność dla któregoś z nich. Wróćmy jednak na chwilę do poprzedniego rozważanego zagadnienia: jak to – nie można obliczyć funkcji F? Jeśli chcemy obliczyć $F(j)$, to wystarczy przeglądać programy od najkrótszych aż w końcu znajdziemy ten j-ty, czyli P_j. Wtedy każemy mu obliczyć $P_j(j)$ i na końcu dodamy 1. Coś tu nie gra, gdzie jest błąd? Błąd jest w założeniu, że możemy znaleźć j-ty program. Trochę wynika on z tego, że nie zdefiniowaliśmy porządnie, czym jest program. Nie każdy przecież tekst jest programem. Przyjmijmy więc, że program to poprawny tekst w pewnym ustalonym języku programowania. To można łatwo sprawdzić, są kompilatory różnych języków programowania, które sprawdzają, czy dany tekst jest istotnie kodem programu w wybranym języku. Wymagamy jednak jeszcze od programu, żeby zawsze się kończył i zwracał jakąś liczbę. Istotnie: to wymaganie jest konieczne, żeby w ogóle mówić, iż program definiuje jakąś funkcję. I tu właśnie jest haczyk. Gdybyśmy umieli sprawdzać, czy dany program zawsze się kończy, to umielibyśmy zrealizować opisaną wyżej procedurę obliczania funkcji F. Wiemy jednak, że funkcja F jest nieobliczalna, więc nie może istnieć metoda sprawdzania, czy dany program się zawsze kończy.

Zazwyczaj w Problemie Stopu pyta się, czy program P zatrzymuje się dla konkretnego wejścia, opisana wersja jest jednak równoważna, a nam wygodniej z niej korzystać.

W ten sposób wykazaliśmy, że problem stopu istotnie jest nierozstrzygalny. Pierwszy zrobił to Alan Turing, jeden z pionierów informatyki, w 1936 roku. Przedstawiony dowód jest jednak nieco inny, bardziej bezpośrednio stosuje metodę przekątniową.

Problemów nierozstrzygalnych jest wiele, problem stopu nie jest tu jakiś wyjątkowy. Nierozstrzygalne są m.in. problem istnienia rozwiązań równań diofantycznych, obliczania złożoności Kołmogorowa (patrz *Delta* 8/2012, artykuł *Niemożliwy skrót*), pytanie, czy da się ułożyć nieskończoną płaszczyznę z ustalonego zbioru kolorowych kafelków, tak by kolory do siebie pasowały i wiele, wiele innych. To jednak temat na zupełnie inną opowieść.

Bajka o Gadającym Neutrinie

Nigdy już się nie spotkamy – rzuciło Neutrino do Kwantu wyjątkowo twardego promieniowania gamma – i od razu uciekło ze Słońca. Osiem minut później przeleciało na wskroś jądro Ziemi i śpiącego Autora tej bajki i pomknęło dalej w kierunku granic Galaktyki. Kwant nie odpowiedział, zajęty przeciskaniem się przez potworny tłok cząstek stłamszonych w środku Słońca. Dopiero za tysiąc lat miał szansę wydostać się na powierzchnię chromosfery, osłabiony, pożółkły, oklapły i wyglądający jak – za przeproszeniem – Foton. Ale wtedy to już szukaj wiatru w polu.

Neutrino zaś gnało przed siebie z szybkością światła. W tym samym czasie naukowcy kłócili się, czy Neutrino oprócz nazwy i odrobiny energii ma cokolwiek jeszcze. Nawet przyznali sobie Nagrodę Nobla za odkrycie, że Neutrino potrafi oscylować, więc masę mieć musi. Ale skoro tak, to nie może mieć szybkości światła. Neutrino miało to w nosie. To znaczy, nosa nie miało, ale to też miało w nosie.

Może Cię dziwić, dlaczego zawracam Ci głowę losami Neutrina. Zastanów się chwilę. Co sekundę przez każdy centymetr kwadratowy przekroju Twojego ciała przenika 70 000 000 000 neutrin. Prędzej czy później ktoś odkryje, jak je wykorzystać w praktyce. A zaraz potem powiedzą Ci, że masz od tego płacić podatki. Wcale nie żartuję – z elektrycznością to jak było?

Co prawda, na Słońcu neutrina i kwanty gamma powstają razem w ekstremalnych warunkach, ale na Ziemi łatwiej o neutrina z rozpadu atomów potasu. Dlatego jeżeli ktoś zapyta Cię, co to jest – małe, czerwone, okrągłe i emituje neutrina – odpowiedz śmiało: Pomidor.

Krzysztof KICIAK