O dziesiątym problemie Hilberta

*Joanna OCHREMIAK**

* LaBRI, Bordeaux

Podczas odbywającego się w 1900 roku w Paryżu Drugiego Międzynarodowego Kongresu Matematyków jeden z referatów wygłosił wybitny niemiecki matematyk David Hilbert. W swoim wystąpieniu zawarł on listę dwudziestu trzech zagadnień matematycznych stanowiących, jego zdaniem, szczególne wyzwanie dla matematyków w rozpoczynającym się XX wieku. Większość z nich doczekała się rozwiązania. Inne, jak słynna hipoteza Riemanna, pozostają otwarte, inspirując kolejne pokolenia naukowców.

Dziesiąty spośród problemów Hilberta dotyczy *równań diofantycznych*, czyli równań postaci $P(x_0, \ldots, x_n) = 0$, gdzie P jest wielomianem o współczynnikach całkowitych. Przykładem równania diofantycznego jest więc $2x_0^2x_1 - x_1^5 + 1 = 0$ oraz $5x_0x_1x_2^2 - x_0x_2 + x_1^2 = 0$. Hilbert postulował znalezienie procedury, która pozwalałaby dla dowolnego równania diofantycznego rozstrzygnąć w skończonej liczbie kroków, czy równanie to ma rozwiązanie w zbiorze liczb naturalnych, czy też nie. Problem ten jest o tyle wyjątkowy, że jako jedyny na liście Hilberta odwołuje się do pojęcia *algorytmu*, które na przełomie XIX i XX wieku nie miało jeszcze formalnej definicji. W przypadku wynalezienia postulowanej metody (czego, jak możemy się domyślać, spodziewał się Hilbert) byłoby intuicyjnie jasne, że stanowi ona pozytywne rozwiązanie problemu. Negatywne rozwiązanie dziesiątego problemu Hilberta nie byłoby jednak możliwe bez doprecyzowania jego sformułowania w języku matematycznym.

Oryginalne pytanie postawione przez Hilberta dotyczyło istnienia rozwiązań równania diofantycznego w zbiorze liczb całkowitych. Nietrudno jednak wykazać, że obie wersje problemu są równoważne.

Współcześnie powszechnie przyjęte definicje pozwalają w sposób całkowicie formalny stwierdzić, że nie istnieje algorytm, który mając dane na wejściu równanie diofantyczne, rozstrzyga, czy ma ono rozwiązanie w liczbach naturalnych. Negatywne rozwiązanie dziesiątego problemu Hilberta jest konsekwencją słynnego twierdzenia z roku 1970, wieńczącego wiele lat pracy czwórki matematyków: Jurija Matijasiewicza, Julii Robinson, Martina Davisa oraz Hilarego Putnama.

Celem tego artykułu jest sformułowanie tak zwanego *twierdzenia MRDP* (od Matijasiewicz, Robinson, Davis, Putnam), wyjaśnienie zawartej w nim fascynującej idei rozwiązania dziesiątego problemu Hilberta oraz przedstawienie pewnych jego zaskakujących konsekwencji.

Intuicyjnie, algorytm to po prostu skończony zbiór instrukcji. Powszechnie znany jest algorytm dodawania pisemnego, zwany „dodawaniem pod kreską”, czy też algorytm Euklidesa wyznaczania największego wspólnego dzielnika dwóch liczb. Pojęcie algorytmu zostało sformalizowane w latach trzydziestych XX wieku niezależnie przez Kurta Gödla, Alana Turinga, Emila Posta oraz Alonzo Churcha. Zaproponowane definicje, na pozór bardzo różne, okazały się równoważne i stanowią dziś podstawę zarówno sposobu funkcjonowania komputerów, jak i teoretycznych badań nad ich możliwościami. Na potrzeby tego artykułu pozostańmy jednak przy intuicyjnym rozumieniu pojęcia algorytmu, pamiętając, że kryje się za nim dobrze zdefiniowany obiekt matematyczny.

Wracając do zagadnienia, z którym mierzyli się Matijasiewicz, Robinson, Davis oraz Putnam – w języku współczesnej informatyki dotyczy ono tak zwanego *problemu decyzyjnego*: chcemy wiedzieć, które elementy zbioru A mają interesującą nas własność w. Dziesiąty problem Hilberta to problem decyzyjny (A, w), gdzie zbiór A to zbiór wszystkich równań diofantycznych, a własność w to posiadanie co najmniej jednego rozwiązania w liczbach naturalnych. Innym znanym przykładem problemu decyzyjnego jest *problem pierwszości*: interesuje nas w tym przypadku zbiór A wszystkich liczb naturalnych oraz własność w bycia liczbą pierwszą.

Problem decyzyjny (A, w) jest *rozstrzygalny*, jeśli istnieje algorytm, który, mając dany na wejściu dowolny element a zbioru A, po wykonaniu skończonej liczby operacji rozstrzyga, czy element a ma własność w, czy też nie. Bezpośrednią

Rozwiązanie zadania F 989.
Masy atomowe pierwiastków występujących naturalnie w przyrodzie wypełniają przedział od 1 (wodór) do 244 (pluton), a promienie atomowe, przedział od $0{,}5 \cdot 10^{-10}$ m (wodór) do $2{,}67 \cdot 10^{-10}$ m (cez) – wynik oszacowania zależy od charakteru wiązań, jakie atom tworzy, gdy wchodzi w związki chemiczne. Masy atomów nie zależą od tworzonych przez nie wiązań, a więc w obliczeniach posłużymy się ich masami. Spróbujmy oszacować „typową" masę atomów wchodzących w skład Ziemi.
W atmosferze mamy niemal wyłącznie azot i tlen o masach atomowych 14 i 16, w skorupie Ziemi dominuje tlen oraz krzem o masie atomowej 28, a jądro Ziemi składa się głównie z żelaza i niklu o masach atomowych 56 i 59. Przyjmijmy, że typowa liczba masowa to 50, i obliczmy, ile takich atomów „składa" się na masę Ziemi:

$$N = \frac{M}{50 \cdot u} = \frac{6{,}0 \cdot 10^{24}\ \mathrm{kg}}{50 \cdot 1{,}7 \cdot 10^{-27}\ \mathrm{kg}} \approx 7 \cdot 10^{49}.$$

Dla „sprawdzenia" oszacujmy, ile „typowych atomów" wypełni objętość Ziemi. Promienie atomów najczęściej występujących na Ziemi mieszczą się w przedziale od $1{,}0 \cdot 10^{-10}$ m do $2{,}0 \cdot 10^{-10}$ m. Przyjmijmy promień „typowego" atomu $r = 1{,}5 \cdot 10^{-10}$ m. Otrzymujemy, że do „wypełnienia" objętości Ziemi potrzeba:

$$N' = R^3/r^3 \approx \frac{(6{,}4 \cdot 10^6\ \mathrm{m})^3}{(1{,}5 \cdot 10^{-10}\ \mathrm{m})^3} \approx 8 \cdot 10^{49}.$$

Przyjęliśmy kulisty kształt atomów i pominęliśmy fakt, że ciasno upakowane kule wypełniają „tylko" około 3/4 objętości przestrzeni, oraz wpływ ogromnych ciśnień we wnętrzu Ziemi (do około 330 GPa). Zgodność otrzymanych wartości N i N' jest nawet nieco zaskakująca.

Rozwiązanie zadania F 990.
W sieci fcc atomy obsadzają wierzchołki sześcianu i środki jego ścian bocznych. Najbliższe atomy znajdują się więc w odległości

$$d_F = a_F \frac{\sqrt{2}}{2} = 2{,}5786 \cdot 10^{-10}\ \mathrm{m}.$$

W sieci bcc atomy obsadzają wierzchołki sześcianu i jego środek. Najbliższe atomy są więc odległe o

$$d_B = a_B \frac{\sqrt{3}}{2} = 2{,}5152 \cdot 10^{-10}\ \mathrm{m}.$$

Różnica odległości między atomami jest bardzo mała i odpowiada stosunkowi gęstości fazy fcc do fazy bcc, równemu 0,928. Warto zauważyć, że w sieci bcc przypadają 2 atomy na jedną komórkę elementarną (atom w środku należy do komórki, a każdy z atomów „narożnych" należy do ośmiu sąsiadujących komórek), a w sieci fcc 4 atomy (każdy „narożny" należy do ośmiu komórek, a te w środkach ścian do dwóch sąsiadujących komórek).

konsekwencją twierdzenia MRDP (do którego sformułowania zmierzają nasze rozważania) jest nierozstrzygalność dziesiątego problemu Hilberta.

Zwróćmy jednak uwagę, że zdefiniowane powyżej pojęcie rozstrzygalności jest stosunkowo restrykcyjne. Mniej satysfakcjonujące rozwiązanie problemu decyzyjnego (A, w) otrzymamy, wymagając jedynie, żeby algorytm po skończonej liczbie kroków zwrócił pozytywną odpowiedź dokładnie wtedy, gdy na wejściu ma dany element zbioru A o własności w. Natomiast jeśli dany element nie spełnia w, to algorytm może się nie zatrzymać. Problem decyzyjny, dla którego taki algorytm istnieje, nazywamy *częściowo rozstrzygalnym*. Łatwo stwierdzić, że dziesiąty problem Hilberta jest częściowo rozstrzygalny: wystarczy rozważyć algorytm, który dla danego równania diofantycznego sprawdza po kolei wszystkie możliwe wartościowania w liczbach naturalnych występującego w nim zbioru niewiadomych. Jeśli któreś z kolei wartościowanie spełni równanie, algorytm zwraca odpowiedź pozytywną, natomiast w przeciwnym przypadku nigdy nie zakończy on swojego działania.

Dziesiąty problem Hilberta jest więc przykładem problemu decyzyjnego, który jest częściowo rozstrzygalny, ale nie jest rozstrzygalny. Wynika to jednak dopiero z udowodnionego w 1970 roku twierdzenia MRDP. Na długo przed rokiem 1970 matematycy zdawali sobie sprawę z istnienia częściowo rozstrzygalnych, ale nierozstrzygalnych problemów decyzyjnych postaci $(\mathbb{N}, w)$, gdzie w jest pewną własnością liczb naturalnych. Twierdzenie MRDP potwierdza odważną hipotezę, według której zbiór wszystkich częściowo rozstrzygalnych problemów decyzyjnych dotyczących liczb naturalnych jest w pewien sposób silnie powiązany ze zbiorem równań diofantycznych.

Każda własność w liczb naturalnych definiuje podzbiór A_w liczb naturalnych o własności w. Jednocześnie, każdy podzbiór A liczb naturalnych definiuje własność w_A należenia do podzbioru A. Upraszczając nieco terminologię, zamiast o rozstrzygalnych lub częściowo rozstrzygalnych problemach decyzyjnych postaci $(\mathbb{N}, w)$ możemy więc mówić o rozstrzygalnych lub częściowo rozstrzygalnych podzbiorach zbioru liczb naturalnych. W 1950 roku Martin Davis sformułował hipotezę, zgodnie z którą każdy częściowo rozstrzygalny podzbiór zbioru liczb naturalnych jest tak zwanym *zbiorem diofantycznym*.

Definicja zbioru diofantycznego wymaga rozważenia równań diofantycznych z parametrem. Parametrem nazwiemy po prostu jedną, wyróżnioną niewiadomą. Równanie diofantyczne z parametrem jest więc postaci $P(a, x_1, \ldots, x_k) = 0$. Definiuje ono całą rodzinę równań diofantycznych: podstawiając za parametr a dowolną liczbę naturalną n, otrzymamy równanie diofantyczne (bez parametru), które oznaczać będziemy przez $P_n(x_1, \ldots, x_k) = 0$. Dla dowolnego równania diofantycznego z parametrem $P(a, x_1, \ldots, x_k) = 0$, zbiór tych liczb naturalnych n, dla których równanie $P_n(x_1, \ldots, x_k) = 0$ ma rozwiązanie w liczbach naturalnych, nazywamy *zbiorem diofantycznym*. Przykładem zbioru diofantycznego jest zatem zbiór drugich potęg liczb naturalnych odpowiadający równaniu $x_1^2 - a = 0$, a także zbiór liczb złożonych odpowiadający równaniu $(x_1 + 2)(x_2 + 2) - a = 0$.

Zauważmy, że każdy zbiór diofantyczny jest częściowo rozstrzygalny. Rzeczywiście, przypuśćmy, że mamy dany zbiór diofantyczny zadany przez równanie diofantyczne z parametrem $P(a, x_1, \ldots, x_k) = 0$. Algorytm świadczący o tym, że zbiór ten jest częściowo rozstrzygalny, dla danej na wejściu liczby naturalnej n oblicza równanie diofantyczne $P_n(x_1, \ldots, x_k) = 0$, a następnie sprawdza po kolei wszystkie wartościowania jego niewiadomych w liczbach naturalnych. Jeśli któreś wartościowanie spełni równanie $P_n(x_1, \ldots, x_k) = 0$, algorytm zwraca odpowiedź pozytywną, zaś w przeciwnym przypadku nie zakończy on swojego działania.

Hipoteza Davisa, jak już wspomnieliśmy, dotyczy implikacji przeciwnej: każdy częściowo rozstrzygalny podzbiór zbioru liczb naturalnych jest diofantyczny. Została ona udowodniona po dwudziestu latach intensywnych badań. Jej potwierdzenie stanowi treść twierdzenia MRDP, które możemy zatem sformułować następująco:

Twierdzenie MRDP. *Podzbiór zbioru liczb naturalnych jest częściowo rozstrzygalny wtedy i tylko wtedy, gdy jest zbiorem diofantycznym.*

Uwzględniając fakt istnienia częściowo rozstrzygalnych, ale nierozstrzygalnych podzbiorów zbioru liczb naturalnych, twierdzenie MRDP implikuje istnienie nierozstrzygalnych zbiorów diofantycznych i w konsekwencji negatywne rozwiązanie dziesiątego problemu Hilberta. Zanim jednak prześledzimy dokładniej tę ostatnią implikację, przyjrzyjmy się, jak zaskakująca jest w istocie treść twierdzenia MRDP.

Wspomniany powyżej problem pierwszości jest z pewnością rozstrzygalny: dla danej na wejściu liczby naturalnej n trywialny algorytm sprawdza po kolei, czy n jest podzielne przez jakąkolwiek liczbę ze zbioru $\{2, \ldots, n-1\}$. W szczególności, zbiór liczb pierwszych jest częściowo rozstrzygalny. Z twierdzenia MRDP wynika zatem, że istnieje równanie diofantyczne z parametrem $P(a, x_1, \ldots, x_k) = 0$, które ma rozwiązanie w liczbach naturalnych wtedy i tylko wtedy, gdy a jest liczbą pierwszą! Podobnie ma się sprawa ze zbiorem wszystkich potęg liczby 2, zbiorem liczb Fibonacciego... i przypuszczalnie z każdym innym podzbiorem zbioru liczb naturalnych, którego definicja przychodzi nam łatwo do głowy.

Zdefiniowanie zbioru, który nie jest częściowo rozstrzygalny, jest zadaniem zdecydowanie nietrywialnym.

Pozostaje nam przyjrzeć się, w jaki sposób z twierdzenia MRDP wynika negatywne rozwiązanie dziesiątego problemu Hilberta. Przypuśćmy, że odpowiedź ta byłaby pozytywna, i niech $\mathcal{A}$ oznacza algorytm, który dla dowolnego równania diofantycznego rozstrzyga, czy ma ono rozwiązanie w liczbach naturalnych, czy też nie. Rozważmy równanie diofantyczne z parametrem $P(a, x_1, \ldots, x_k) = 0$ definiujące pewien zbiór diofantyczny X. Zauważmy, że następujący algorytm rozstrzyga przynależność do zbioru X: dla danej na wejściu liczby naturalnej n oblicz równanie diofantyczne $P_n(x_1, \ldots, x_k) = 0$, a następnie za pomocą algorytmu $\mathcal{A}$ rozstrzygnij, czy ma ono rozwiązanie w zbiorze liczb naturalnych. Odpowiedź pozytywna oznacza, że $n \in X$, natomiast odpowiedź negatywna oznacza, że $n \notin X$. Wykazaliśmy w ten sposób, że każdy zbiór diofantyczny jest rozstrzygalny. Na mocy twierdzenia MRDP oznacza to, że każdy częściowo rozstrzygalny podzbiór zbioru liczb naturalnych jest rozstrzygalny. Otrzymana sprzeczność implikuje nierozstrzygalność dziesiątego problemu Hilberta.

Jak uniknąć częściowej rozstrzygalności?

W artykule powyżej wspomniano, że prawie każdy zbiór liczb naturalnych, który przyjdzie nam na myśl, jest częściowo rozstrzygalny. Spróbujmy jednak pokazać, że słowo *prawie* jest tu istotne, czyli że możliwa jest konstrukcja zbioru $S \subseteq \mathbb{N}$, który nie jest częściowo rozstrzygalny.

Po pierwsze zauważmy, że jeśli zarówno zbiór S, jak i jego dopełnienie $\mathbb{N} \setminus S$ są częściowo rozstrzygalne, to wówczas S jest nawet rozstrzygalny. To, że S jest częściowo rozstrzygalny, oznacza, że istnieje algorytm (nazwijmy go *pozytywnym*), który dla danej liczby $n \in \mathbb{N}$ zatrzyma się i odpowie „n należy do S”, jeśli $n \in S$ (ale być może nie zatrzyma się, jeśli $n \notin S$). Podobnie, skoro $\mathbb{N} \setminus S$ jest częściowo rozstrzygalny, to istnieje algorytm (nazwijmy go *negatywnym*), który dla danej liczby $n \in \mathbb{N}$ zatrzyma się i odpowie „n należy do $\mathbb{N} \setminus S$”, o ile $n \in \mathbb{N} \setminus S$. A zatem jeśli puścimy naraz oba algorytmy, pozytywny i negatywny, to któryś z nich się zatrzyma i zwróci poprawną odpowiedź (zakładamy, że wtedy automatycznie zatrzymujemy również drugi algorytm). To pokazuje, że istotnie w takiej sytuacji S jest rozstrzygalny.

A zatem do konstrukcji zbioru, który nie jest nawet częściowo rozstrzygalny, wystarczy znaleźć $S \subseteq \mathbb{N}$ taki, że jest on częściowo rozstrzygalny, ale nie jest rozstrzygalny. Wówczas $\mathbb{N} \setminus S$ nie będzie nawet częściowo rozstrzygalny. Aby skonstruować taki zbiór S, potrzebna jest pewna wiedza; zakładamy, że Czytelnik Doświadczony zna definicję i podstawowe intuicje związane z maszynami Turinga. Zbiór maszyn Turinga, które akceptują słowo puste, jest częściowo rozstrzygalny (wystarczy znaleźć bieg akceptujący dla tego słowa pustego), ale nie jest rozstrzygalny (uzasadnienie można znaleźć np. w artykule Szymona Toruńczyka „Paradoks Russella” w Δ^{11}_{17}). Każdą maszynę Turinga można jednoznacznie zakodować jako liczbę naturalną. Zatem zbiór zakodowań maszyn Turinga, które akceptują słowo puste, jest częściowo rozstrzygalny, ale rozstrzygalny już nie jest.

Wojciech CZERWIŃSKI