10. problem Hilberta

Leszek KOŁODZIEJCZYK, Warszawa*

Wśród 23 problemów, które na Międzynarodowym Kongresie Matematyków w 1900 r. przedstawił Dawid Hilbert, przynajmniej kilka wiąże się z logiką i podstawami matematyki. Związki te są szczególnie silne w przypadku trzech problemów: pierwszego, drugiego i dziesiątego. O ile jednak pierwsze dwa problemy – hipoteza continuum i dowód niesprzeczności aksjomatów arytmetyki – dotyczyły podstaw matematyki w sposób ewidentny od samego początku, o tyle problem dziesiąty z pozoru mieścił się całkowicie w obrębie teorii liczb czy ewentualnie algebry. Przypomnijmy bowiem, że sformułowanie 10. problemu Hilberta brzmiało:

Warto jednak wspomnieć także przynajmniej o tzw. 24. problemie, który ostatecznie nie został wymieniony podczas paryskiego wykładu. Problem dotyczył kryteriów prostoty dowodów i metod wykazywania, że dany dowód jest najprostszym z możliwych – a zatem zagadnień, które weszły później w skład zainicjowanej przez Hilberta teorii dowodu.

Dane jest równanie diofantyczne o dowolnej liczbie zmiennych i o współczynnikach całkowitych: należy podać metodę, zgodnie z którą da się w skończonej liczbie operacji rozstrzygnąć, czy istnieje rozwiązanie tego równania w dziedzinie liczb całkowitych.

Równanie diofantyczne to po prostu równanie postaci $p_1(x_1,\dots,x_n) = p_2(x_1,\dots,x_n)$, gdzie n jest dowolną liczbą naturalną i gdzie $p_1, p_2 \in \mathbb{Z}[x_1,\dots,x_n]$. Interesują nas wyłącznie całkowitoliczbowe rozwiązania równania, tj. takie n-tki $(k_1,\dots,k_n) \in \mathbb{Z}^n$, dla których $p_1(k_1,\dots,k_n) = p_2(k_1,\dots,k_n)$. Hilbert oczekiwał podania algorytmu, który dla danego równania diofantycznego rozstrzygałby, czy rozwiązanie całkowitoliczbowe istnieje. Na pierwszy rzut oka mogłoby się wydawać, że to problem nie aż tak bardzo odmienny od takich, jak np. poszukiwanie największego wspólnego dzielnika albo (dla wielomianów jednej zmiennej) ustalanie liczby pierwiastków rzeczywistych. Problemy te da się bez większego trudu rozwiązywać algorytmicznie, a konstrukcja i analiza odpowiednich algorytmów nie wymagają żadnych odwołań do logiki czy pokrewnych dziedzin. Dlaczego zatem wtedy, gdy pytamy o rozwiązania w liczbach całkowitych, związki z logiką miałyby się pojawić?

Zanim zaczniemy to wyjaśniać, dokonajmy drobnej modyfikacji problemu. Przenosząc niektóre współczynniki na drugą stronę równania, możemy bez straty ogólności przyjąć, iż wszystkie współczynniki w p_1, p_2 są naturalne, a nie tylko całkowite. Co więcej, skupimy się także na poszukiwaniu rozwiązań w liczbach *naturalnych*. Pytamy się więc o algorytm, który rozstrzyga, czy dane równanie diofantyczne o naturalnych współczynnikach ma rozwiązanie naturalnoliczbowe. Zauważmy, że jest to nie trudniejsze niż poszukiwanie rozwiązań całkowitych: na mocy twierdzenia Lagrange'a o czterech kwadratach, aby wiedzieć, czy $p_1(x_1,\dots,x_n) = p_2(x_1,\dots,x_n)$ ma rozwiązanie naturalne, wystarczy wiedzieć, czy

$$p_1(x_{1,1}^2 + x_{1,2}^2 + x_{1,3}^2 + x_{1,4}^2, \dots, x_{n,1}^2 + x_{n,2}^2 + x_{n,3}^2 + x_{n,4}^2) = \\ = p_1(x_{1,1}^2 + x_{1,2}^2 + x_{1,3}^2 + x_{1,4}^2, \dots, x_{n,1}^2 + x_{n,2}^2 + x_{n,3}^2 + x_{n,4}^2)$$

ma rozwiązanie całkowite.

Powyższa modyfikacja problemu jest dobrą okazją, by odnotować, że algorytm, którego oczekiwał Hilbert, musiałby odpowiadać na pewne dość niebanalne pytania. Dla każdego n umiałby na przykład ustalić, czy równanie

$$(x+1)^n + (y+1)^n = (z+1)^n$$

ma rozwiązania naturalne. Można się spodziewać, że robiłby to nie czekając na opinię Andrew Wilesa.

*Wydział Matematyki, Informatyki i Mechaniki UW, lak@mimuw.edu.pl

Zadanie, które postawił przed matematykami Hilbert, było więc raczej ambitne. Ostatecznie okazało się, że wręcz zbyt ambitne. W 1970 r. dwudziestodwuletni Rosjanin, Jurij Matijasiewicz, udowodnił, że pytanie, czy dane równanie diofantyczne ma rozwiązanie naturalnoliczbowe, jest *nierozstrzygalne*. Innymi słowy, algorytm, który spełniałby wymogi 10. problemu Hilberta, nie istnieje! Kiedy już się to wie, można zacząć się domyślać, dlaczego rozwiązanie tego akurat problemu wiąże się z przełomowymi odkryciami dwudziestowiecznej logiki i teorii obliczeń.

Drogę, która doprowadziła do rozwiązania 10. problemu Hilberta, warto w skrócie przypomnieć, nie tylko ze względu na rangę samego wyniku. Stanowi ona ciekawy przykład „zagnieżdżonego" zastosowania jednej dziedziny matematyki w drugiej: w celu rozwiązania problemu z teorii liczb, trzeba było odwołać się do fundamentalnych, ale technicznie prostych pojęć logiki i teorii obliczeń; żeby jednak dało się do nich odwołać, niezbędne były elementarne pojęciowo, ale bardzo pomysłowe rozumowania teorioliczbowe. Zanim pojawił się Matijasiewicz, autorami kluczowych pomysłów byli Martin Davis, Hilary Putnam i Julia Robinson. Dlatego też twierdzenie Matijasiewicza, czyli negatywne rozwiązanie 10. problemu Hilberta, nazywa się też niekiedy twierdzeniem MRDP albo DPRM.

Spotyka się też inne permutacje liter, ale nie wszystkie: związane z 10. problemem Hilberta prace Putnama były współautorskie z Davisem, więc D stoi zawsze bezpośrednio przed P.

Dowodzenie nierozstrzygalności problemów algorytmicznych stało się możliwe dzięki pojęciom i wynikom ze słynnej pracy Alana Turinga z 1936 r. *Maszyny Turinga* nie będziemy tu definiować bardzo dokładnie. Wystarczy wiedzieć, że jest to matematyczny model urządzenia dokonującego obliczeń na nieskończonej taśmie, składającej się z dyskretnych, uporządkowanych tak jak $\mathbb{N}$, komórek. Każda z komórek może być pusta lub zawierać jeden z symboli 0 lub 1. Maszyna otrzymuje jako wejście n-tkę $(k_1, \ldots, k_n) \in \mathbb{N}^n$ daną za pomocą zapisu binarnego, a następnie wykonuje obliczenie, w którego każdym kroku realizuje jedną ze skończenie wielu instrukcji, umożliwiających przesuwanie się po taśmie w obu kierunkach, a także czytać i modyfikować symbole zapisane w poszczególnych komórkach. W każdym momencie obliczenia maszyna znajduje się w jednym ze skończenie wielu *stanów*, z których jeden wyróżniony jest jako stan *początkowy*, a niektóre inne – jako *końcowe*. Powiemy, że zbiór $S \subseteq \mathbb{N}^n$ (który utożsamiamy z problemem algorytmicznym „czy dana n-tka $(k_1, \ldots, k_n)$ należy do S?") jest *nierozstrzygalny*, jeśli nie istnieje maszyna Turinga, która na wejściu $(k_1, \ldots, k_n) \in S$ kończy obliczenie z 1 w jedynej niepustej komórce taśmy, a na wejściu $(k_1, \ldots, k_n) \notin S$ kończy obliczenie z 0 w jedynej niepustej komórce.

Każdą maszynę Turinga można zakodować za pomocą pojedynczej liczby naturalnej, co oznacza, że wszystkich maszyn jest przeliczalnie wiele, a zatem prawie wszystkie pozdbiory $\mathbb{N}^n$ są nierozstrzygalne. Co jednak ważne, Turing podał także konkretny przykład zbioru nierozstrzygalnego:

$$\mathrm{STOP} = \{(k_1, k_2) \in \mathbb{N}^2 : \text{ maszyna o kodzie } k_1 \text{ osiąga stan końcowy w trakcie obliczenia na wejściu } k_2\}.$$

Dowód nierozstrzygalności jest w tym przypadku dość elementarnym rozumowaniem przekątniowym.

Kluczową z naszego punktu widzenia cechą zbioru STOP jest to, że można go zdefiniować w stosunkowo prosty sposób. Dokładniej, zbiór STOP jest definiowalny formułą logiczną postaci

$$\exists x_1 \in \mathbb{N} \ldots \exists x_m \in \mathbb{N}\, \Phi(k_1 \ldots, k_n, x_1, \ldots, x_m),$$

gdzie formuła $\Phi(k_1 \ldots, k_n, x_1, \ldots, x_m)$ jest zbudowana ze zmiennych $k_1 \ldots, k_n, x_1, \ldots, x_m$ (w naszym przypadku $n = 2$), ewentualnych zmiennych pomocniczych $y_1, \ldots, y_m$ oraz stałych $0, 1$ za pomocą: symboli arytmetycznych $+, \cdot, =$, spójników logicznych $\wedge, \vee, \neg$ oraz *kwantyfikatorów ograniczonych*, czyli postaci $\forall y_j \leqslant k_i, \forall y_j \leqslant x_i, \exists y_j \leqslant k_i$ lub $\exists y_j \leqslant x_i$. Każdą formułę tego typu nazywać będziemy formułą *klasy* Σ_1 bądź po prostu formułą Σ_1. Przykładem formuły Σ_1 (skądinąd zdegenerowanym, bo pozbawionym początkowych kwantyfikatorów egzystencjalnych) jest poniższa formuła definiująca zbiór liczb pierwszych:

$$k \neq 0 \wedge k \neq 1 \wedge \forall y_1 \leqslant k\, \forall y_2 \leqslant k\, [y_1 = 1 \vee y_2 = 1 \vee k \neq y_1 \cdot y_2].$$

Zbiory Σ_1-definiowalne nazywa się również *rekurencyjnie przeliczalnymi* lub *częściowo rozstrzygalnymi*. Formuła Σ_1 definiująca zbiór STOP orzeka istnienie liczby x kodującej zakończone obliczenie maszyny k_1 na wejściu k_2. W celu stwierdzenia „istnieje x" używamy początkowego kwantyfikatora $\exists$, ale cała trudność w konstrukcji formuły polega na wyrażeniu treści „x jest kodem obliczenia maszyny k_1 na wejściu k_2" za pomocą środków dopuszczonych przez definicję klasy Σ_1. Sednem problemu jest reprezentowanie ciągów liczb naturalnych dowolnej długości za pomocą pojedynczych liczb, a rozwiązanie, wywodzące się z przełomowej pracy Kurta Gödla na temat niezupełności teorii aksjomatycznych, polega na twórczym wykorzystaniu elementarnej teorii liczb. Chińskie twierdzenie o resztach mówi, że jeśli liczby $m_0, m_1, \ldots, m_n$ są względnie pierwsze i zachodzi $n < m_0, k_1 < m_1, \ldots, k_n < m_n$, to istnieje liczba m taka, że $m \equiv n \pmod{m_0}$ oraz $m \equiv k_i \pmod{m_i}$ dla $i = 1, \ldots, n$. Liczbę m chcielibyśmy uznać za kod ciągu $\langle k_1, \ldots, k_n\rangle$. W tym celu musimy jednak umieć odwołać się do pewnych konkretnych względnie pierwszych liczb $m_0, \ldots, m_n$, ale *bez* kodowania ciągu $\langle m_0, \ldots, m_n\rangle$; inaczej grozi nam popadnięcie w błędne koło w definicji. Trudność tę udaje się pokonać za pomocą faktu, że dla dowolnego $\ell \geqslant n+1$ względnie pierwsze są elementy ciągu arytmetycznego $\ell! + 1, 2\ell! + 1, \ldots, (n+1)\ell! + 1$.

Wypada teraz wskazać na związek między pewnymi szczególnymi formułami klasy Σ_1 a równaniami diofantycznymi. Powiemy, że formuła Σ_1 jest *diofantyczna*, jeśli jest postaci

$$(1)\quad \exists x_1 \in \mathbb{N} \ldots \exists x_m \in \mathbb{N}\, [p_1(k_1 \ldots, k_n, x_1, \ldots, x_m) = p_2(k_1 \ldots, k_n, x_1, \ldots, x_m)]\,,$$

gdzie p_1, p_2 są napisami zbudowanymi ze zmiennych $k_1 \ldots, k_n, x_1, \ldots, x_m$ oraz stałych $0, 1$ za pomocą symboli $+, \cdot$ (a więc, w istocie, wielomianami o współczynnikach naturalnych). Przykładowo, zbiór liczb złożonych można zdefiniować formułą diofantyczną:

$$\exists x_1 \in \mathbb{N}\, \exists x_2 \in \mathbb{N}\, [y = (x_1 + (1+1)) \cdot (x_2 + (1+1))].$$

Zauważmy, że ewentualny algorytm spełniający wymagania 10. problemu Hilberta umiałby, dla danej formuły diofantycznej takiej jak w (1) i danych $k_1 \ldots, k_n$, rozstrzygnąć, czy formuła ta jest prawdziwa o $k_1, \ldots, k_n$. Innymi słowy, jeśli 10. problem Hilberta ma pozytywne rozwiązanie, to żaden zbiór definiowalny formułą diofantyczną – w skrócie: zbiór diofantyczny – nie może być nierozstrzygalny!

Zgodnie z definicją, formuła diofantyczna różni się od ogólnej formuły Σ_1 zakazem używania spójników logicznych oraz kwantyfikatorów ograniczonych. Brak spójników nie jest istotnym problemem: zarówno koniunkcja, jak i alternatywa formuł diofantycznych są równoważne formułom diofantycznym, z grubsza dlatego, że dla danych wielomianów p, q mamy:

$$p^2 + q^2 = 0 \ \text{ wtw } \ p = 0 \wedge q = 0,$$
$$pq = 0 \ \text{ wtw } \ p = 0 \vee q = 0.$$

Co więcej, negacja równości $p_1 = p_2$ też jest diofantyczna: jest równoważna alternatywie $p_1 < p_2 \vee p_2 < p_1$, a z kolei $p_1 < p_2$ jest równoważne $\exists x \in \mathbb{N}\, [p_2 = p_1 + (x+1)]$. Innymi słowy, formuły diofantyczne w zasadzie różnią się od ogólnych formuł Σ_1 tylko brakiem kwantyfikatorów ograniczonych. Różnica spora – z całą pewnością za pomocą kwantyfikatorów ograniczonych da się powiedzieć więcej niż bez kwantyfikatorów w ogóle – ale może nie aż tak, by całkowicie wyeliminować nierozstrzygalność? Około 1944 r. Emil Post miał zasugerować, że 10. problem Hilberta wręcz błaga o dowód nierozstrzygalności.

Pod koniec lat 40. Martin Davis, który logiki uczył się między innymi od Posta, był już w stanie wyjść poza obszar sugestii czy błagań. Davis badał w swoim doktoracie ogólne własności klasy zbiorów diofantycznych. Dowiódł, że klasa ta, choć domknięta na przecięcie i sumę, nie jest domknięta na dopełnienie – podobnie jak klasa zbiorów rekurencyjnie przeliczalnych. Udowodnił ponadto, że każda formuła Σ_1 jest równoważna takiej, która różni się od diofantycznej tylko obecnością *jednego* ograniczonego kwantyfikatora $\forall$. Innymi słowy, z rezultatów

Davisa wynikało, że jeśli każda formuła postaci

$$(2)\quad \forall y \leqslant k_1\, \exists x_1 \in \mathbb{N} \ldots \exists x_m \in \mathbb{N}\, [p_1(k_1 \ldots, k_n, x_1, \ldots, x_m, y) = \\ = p_2(k_1 \ldots, k_n, x_1, \ldots, x_m, y)]$$

jest równoważna diofantycznej, to każdy zbiór rekurencyjnie przeliczalny jest diofantyczny – a zatem w szczególności zbiór STOP jest diofantyczny i 10. problem Hilberta ma negatywne rozwiązanie. Davis postawił niezwykle śmiałą jak na owe czasy hipotezę, że tak właśnie jest!

Całkiem niezależnie od prac Davisa, Julia Robinson, doktorantka Tarskiego, próbowała ustalić, czy pewne konkretne zbiory są diofantyczne. Interesował ją zwłaszcza wykres funkcji wykładniczej $x^y = z$. W opublikowanej w 1952 r. w *Transactions of the AMS* pracy Robinson użyła teorii równań Pella, by wykazać między innymi, że pewne ciekawe zbiory, takie jak zbiór liczb pierwszych, relacja $x = y!$ i relacja $\binom{x}{y} = z$, są *wykładniczo diofantyczne*, tj. zdefiniowane formułą

$$\exists x_1 \in \mathbb{N} \ldots \exists x_m \in \mathbb{N}\, [r_1(k_1 \ldots, k_n, x_1, \ldots, x_m) = r_2(k_1 \ldots, k_n, x_1, \ldots, x_m)],$$

gdzie r_1, r_2 zbudowane są ze zmiennych i stałych za pomocą $+, \cdot$ oraz właśnie x^y. Jeżeli więc relacja $x^y = z$ jest diofantyczna, to wszystkie te zbiory również. Główny wynik Robinson mówił z kolei, że diofantyczność $x^y = z$ wynikałaby z istnienia jakiejkolwiek relacji diofantycznej $S \subseteq \mathbb{N}^2$ *wykładniczego wzrostu*, czyli takiej, że:

(i) jeśli $(x, y) \in S$, to $y < x^x$,
(ii) dla każdego $k \in \mathbb{N}$ istnieje para $(x, y) \in S$ taka, że $y > x^k$.

(Warunek (i) można było nawet dość znacząco osłabić.) Stwierdzenie, że taka relacja istnieje, bywa nazywane *hipotezą Julii Robinson* bądź w skrócie *hipotezą JR*. Hipoteza JR wydawała się istotnie słabsza od hipotezy Davisa – wykres funkcji wykładniczej jest nieprzeciętnie prostym przykładem zbioru rekurencyjnie przeliczalnego – co bynajmniej nie oznaczało, że powszechnie uważano tę hipotezę za prawdziwą.

Kolejny ważny etap zmagań z 10. problemem to późne lata 50. Zaczęło się od wspólnych badań Davisa i Hilary'ego Putnama, którzy postanowili wnikliwie przeanalizować formuły postaci (2). Jak można by pozbyć się ograniczonego kwantyfikatora $\forall$ z (2)? Załóżmy dla uproszczenia, że $n = m = 1$. Wiadomo, że formuła

$$\forall y \leqslant k\, \exists x\, [p_1(k, x, y) = p_2(k, x, y)]$$

jest równoważna

$$(3)\qquad \exists \langle x_0, \ldots, x_k \rangle\, \forall y \leqslant k\ [p_1(k, x_y, y) = p_2(k, x_y, y)]\,,$$

gdzie $\langle x_0, \ldots, x_k \rangle$ jest kodem dla ciągu odpowiedniej długości. Postać (3) ma tę niewątpliwą zaletę, że kwantyfikator $\exists$ znalazł się na początku. Zdecydowanie wciąż nie jest to jednak formuła diofantyczna: nie dość, że nie pozbyliśmy się ograniczonego $\forall$, to jeszcze pojawiły nam się napisy x_y oznaczające y-ty wyraz ciągu, które trzeba zastąpić ich potencjalnie dość skomplikowaną definicją. Co z tym można zrobić?

Pomysł Davisa i Putnama był następujący. Użyjmy jeszcze raz kodowania ciągów za pomocą chińskiego twierdzenia o resztach: niech więc x_y oznacza resztę z dzielenia x przez y-ty wyraz jakiegoś łatwego do opisania ciągu arytmetycznego. Zauważmy, że dla dowolnej liczby ℓ dostatecznie dużej względem argumentów równość $p_1(k, x_y, y) = p_2(k, x_y, y)$ jest równoważna kongruencji $p_1(k, x_y, y) = p_2(k, x_y, y) \pmod{\ell}$, i spróbujmy wybrać ℓ tak, by ta kongruencja była z kolei dla każdego $y = 0, \ldots, k$ równoważna $p_1(k, x, Y) = p_2(k, x, Y) \pmod{\ell}$ dla pewnego Y niezależnego od y. W celu zdefiniowania ℓ spróbujmy skorzystać z tego, że wykresy różnych przydatnych operacji takich jak reszta z dzielenia, silnia czy symbole Newtona są diofantyczne bądź (na mocy wyników Robinson) wykładniczo diofantyczne. I... może coś wyjdzie?

Coś wyszło. Po dłuższym okresie intensywnych wysiłków Davisowi i Putnamowi udało się udowodnić, co następuje: jeśli istnieją dowolnie długie skończone ciągi

arytmetyczne złożone z liczb pierwszych, to każdy zbiór rekurencyjnie przeliczalny jest wykładniczo diofantyczny. Z dowodem zapoznała się Robinson, która zdołała wyeliminować założenie na temat ciągów arytmetycznych liczb pierwszych (jak wiadomo, do 2004 r. był to problem otwarty). Główny wynik wspólnej pracy trojga autorów, opublikowanej w 1962 r. w *Annals of Mathematics*, brzmiał więc: każdy zbiór rekurencyjnie przeliczalny jest wykładniczo diofantyczny! Oznaczało to, że w celu pokazania, że każdy zbiór rekurencyjnie przeliczalny jest po prostu diofantyczny, a zatem także rozwiązania 10. problemu Hilberta, wystarczało udowodnić hipotezę JR – a więc na przykład wskazać choć jeden przykład funkcji o wykładniczym tempie wzrostu i diofantycznym wykresie.

Należy w tym miejscu zaznaczyć, że nie wszyscy byli przekonani co do tego, iż praca Davis-Putnam-Robinson stanowiła istotny krok na drodze do rozwiązania 10. problemu. Najlepszą ilustracją stanowiska ówczesnych sceptyków była recenzja pracy DPR w *Mathematical Reviews*. Autor recenzji, znany logik Georg Kreisel, pisał między innymi: „Wyniki te mają powierzchowny związek z dziesiątym problemem Hilberta, dotyczącym zwykłych (tj. niewykładniczych) równań diofantycznych. Dowód (...) nie używa zaawansowanych faktów z zakresu teorii liczb czy teorii zbiorów rekurencyjnie przeliczalnych, a zatem jest prawdopodobne, że rezultat nie jest blisko związany z problemem Hilberta. Ponadto byłoby zaskakujące, gdyby wszystkie (zwykłe) problemy diofantyczne redukowały się jednostajnie do problemów o ustalonej liczbie zmiennych i ustalonego stopnia, a miałoby to miejsce, gdyby wszystkie zbiory rekurencyjnie przeliczalne były diofantyczne”.

Dla koneserów: MR0133227.

Lata 60. były okresem wytężonych prac nad hipotezą JR. Odkryto różne ciekawe warunki teorioliczbowe, które implikowały hipotezę, ale próby udowodnienia któregokolwiek z nich pozostawały daremne. W pewnym momencie sama Robinson straciła przekonanie, że hipoteza jest prawdziwa. Więcej optymizmu zachował Davis, który na pytania w tej sprawie miał odpowiadać: „sądzę, że hipoteza Julii Robinson jest prawdziwa, a udowodni ją jakiś bystry młody Rosjanin”.

Jak wiadomo, przeczucie Davisa było po raz kolejny zdumiewająco trafne. „Bystrym młodym Rosjaninem” był oczywiście Matijasiewicz, który myślał obsesyjnie o 10. problemie przez większość okresu studiów na Uniwersytecie Leningradzkim. Wkrótce po rozpoczęciu studiów doktoranckich i pozornie skutecznym uwolnieniu się od obsesji został poproszony o zrecenzowanie właśnie opublikowanego artykułu Robinson, w którym dostrzegł inspirujący nowy pomysł. Podanym przez Matijasiewicza przykładem relacji diofantycznej o wzroście wykładniczym był wykres funkcji $y = F_{2x}$, gdzie F_n oznacza n-tą liczbą Fibonacciego. Dowód diofantyczności był oparty na serii bardzo pomysłowych tricków i trudny do streszczenia, choć zarazem w pełni elementarny. Po drodze trzeba było odkryć niezane dotąd własności liczb Fibonacciego, na przykład to, że z podzielności F_m przez F_n^2 wynika podzielność m przez F_n. Sam autor dowodu stwierdził, że cała konstrukcja „nie używała żadnych głębokich osiągnięć dwudziestowiecznej teorii liczb i mogła być odkryta w poprzednim [tj. XIX – *LK*] wieku. Brakowało więc motywacji”. W wielu późniejszych źródłach używa się innych relacji, wśród których szczególnie popularna jest relacja „y jest drugą współrzędną x-tego dodatniego rozwiązania równania Pella $x^2 - (a^2 - 1)y^2 = 1$” (formalnie jest to relacja między trzema argumentami x, y, a, ale a można ustalić). Nie zmienia to jednak ogólnego charakteru dowodu.

Człowiek mniej utalentowany od Matijasiewicza może się zastanawiać, czy na pewno *tylko* motywacji.

Twierdzenie Matijasiewicza ma wiele interesujących konsekwencji w różnych dziedzinach matematyki, zwłaszcza w obrębie logiki i teorii liczb. Wymieńmy dwa przykłady. Ciekawym faktem teorioliczbowym wynikającym łatwo z diofantyczności zbiorów rekurencyjnie przeliczalnych jest istnienie wielomianu $p \in \mathbb{Z}[x_1, \ldots, x_n]$ (dla dostatecznie dużego n), dla którego przecięcie zbioru wartości przyjmowanych na argumentach całkowitych ze zbiorem liczb naturalnych to dokładnie zbiór liczb pierwszych. W logice z kolei wynik Matijasiewicza przynosi nowe przykłady zdań niedowodliwych w silnych teoriach

aksjomatycznych. Na mocy twierdzenia Gödla o niezupełności, dla każdej dostatecznie silnej teorii (spełniającej pewne minimalne warunki sensowności) istnieje zdanie w jej języku, którego teoria ta nie jest w stanie ani udowodnić, ani obalić. Zdania podane przez Gödla miały zawsze postać stwierdzenia, że pewien zbiór rekurencyjnie przeliczalny jest pusty. Na mocy twierdzenia Matijasiewicza możemy zatem stwierdzić, że dla każdej teorii istnieje równanie diofantyczne, które nie ma (całkowitoliczbowych) rozwiązań, ale teoria nie jest tego w stanie udowodnić.

Przynajmniej kilka ważnych zagadnień bliskich 10. problemowi Hilberta pozostaje otwartych. Najsłynniejszym przykładem jest zapewne odpowiednik 10. problemu dla liczb wymiernych, czyli pytanie o rozstrzygalność zbioru równań diofantycznych, które mają rozwiązania w $\mathbb{Q}$.

Znacznie więcej informacji na temat 10. problemu Hilberta zawierają prace, z których korzystałem pisząc niniejszy tekst, między innymi książka Matijasiewicza [4] i artykuł Davisa [2]. Sam dowód twierdzenia Matijasiewicza można też znaleźć w wybranych podręcznikach logiki, np. [3], a także w polskim [1].

Literatura

1. Z. Adamowicz, P. Zbierski. *Logika matematyczna*. PWN, 1991.
2. M. Dawis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80:233–269, 1973.
3. Yu. I. Manin. *A course in mathematical logic for mathematicians*. Springer, second edition, 2010. Chapters I–VIII translated from Russian by Neal Koblitz, With new chapters by Boris Zilber and the author.
4. Yu. V. Matiyasevich. *Hilbert's tenth problem*. MIT Press, 1993. Translated from the 1993 Russian original by the author, With a foreword by Martin Davis.