Twierdzenie Matijasiewicza, czyli zastosowanie teorii liczb w zastosowaniu logiki w teorii liczb

Leszek Kołodziejczyk

56. Szkoła Matematyki Poglądowej
Wola Ducka, sierpień 2017

O czym będzie?

O dwu zastosowaniach matematyki, a dokładniej o:

(2) rozwiązaniu 10. problemu Hilberta, czyli wymagającym licznych tricków teorioliczbowych zastosowaniu pojęć logiki/teorii obliczeń do rozstrzygnięcia problemu z teorii liczb,

O czym będzie?

O dwu zastosowaniach matematyki, a dokładniej o:

(2) rozwiązaniu 10. problemu Hilberta, czyli wymagającym licznych tricków teorioliczbowych zastosowaniu pojęć logiki/teorii obliczeń do rozstrzygnięcia problemu z teorii liczb,

(1) zastosowaniu podstaw matematyki do żartów z Dawida Hilberta.

Dawid Hilbert

Dawid Hilbert wielkim matematykiem był...

Dawid Hilbert

W matematyce nie ma żadnego *ignorabimus*.

Dawid Hilbert wielkim matematykiem był...
...a zarazem niepoprawnym optymistą w teorii poznania.

Dawid Hilbert

W matematyce nie ma żadnego *ignorabimus*.

Wir müssen wissen. Wir werden wissen.

Dawid Hilbert wielkim matematykiem był...
...a zarazem niepoprawnym optymistą w teorii poznania.

Problemy Hilberta zwiazane z podstawami matematyki

Problem 1. Rozstrzygnąć hipotezę continuum.

Problemy Hilberta zwiazane z podstawami matematyki

Problem 1. Rozstrzygnąć hipotezę continuum.

Rozwiązanie. Nie da się tego zrobić używając przyjętych aksjomatów matematyki (Gödel 1940, Cohen 1963).

Problemy Hilberta zwiazane z podstawami matematyki

Problem 1. Rozstrzygnąć hipotezę continuum.
Rozwiązanie. Nie da się tego zrobić używając przyjętych aksjomatów matematyki (Gödel 1940, Cohen 1963).

Problem 2. Udowodnić niesprzeczność aksjomatów arytmetyki.

Problemy Hilberta zwiazane z podstawami matematyki

Problem 1. Rozstrzygnąć hipotezę continuum.
Rozwiązanie. Nie da się tego zrobić używając przyjętych aksjomatów matematyki (Gödel 1940, Cohen 1963).

Problem 2. Udowodnić niesprzeczność aksjomatów arytmetyki.
Rozwiązanie. Nie da się tego zrobić metodami, które zaakceptowałby Hilbert (Gödel 1931).

Problemy Hilberta zwiazane z podstawami matematyki

Problem 1. Rozstrzygnąć hipotezę continuum.
Rozwiązanie. Nie da się tego zrobić używając przyjętych aksjomatów matematyki (Gödel 1940, Cohen 1963).

Problem 2. Udowodnić niesprzeczność aksjomatów arytmetyki.
Rozwiązanie. Nie da się tego zrobić metodami, które zaakceptowałby Hilbert (Gödel 1931).

Problem 10. Podać algorytm, który rozstrzyga, czy dane równanie diofantyczne ma rozwiązanie o współrzędnych całkowitych.

Problemy Hilberta zwiazane z podstawami matematyki

Problem 1. Rozstrzygnąć hipotezę continuum.
Rozwiązanie. Nie da się tego zrobić używając przyjętych aksjomatów matematyki (Gödel 1940, Cohen 1963).

Problem 2. Udowodnić niesprzeczność aksjomatów arytmetyki.
Rozwiązanie. Nie da się tego zrobić metodami, które zaakceptowałby Hilbert (Gödel 1931).

Problem 10. Podać algorytm, który rozstrzyga, czy dane równanie diofantyczne ma rozwiązanie o współrzędnych całkowitych.
Rozwiązanie. Nie ma takiego algorytmu (Matijasiewicz 1970).

Problemy Hilberta zwiazane z podstawami matematyki

Problem 1. Rozstrzygnąć hipotezę continuum.
Rozwiązanie. Nie da się tego zrobić używając przyjętych aksjomatów matematyki (Gödel 1940, Cohen 1963).

Problem 2. Udowodnić niesprzeczność aksjomatów arytmetyki.
Rozwiązanie. Nie da się tego zrobić metodami, które zaakceptowałby Hilbert (Gödel 1931).

Problem 10. Podać algorytm, który rozstrzyga, czy dane równanie diofantyczne ma rozwiązanie o współrzędnych całkowitych.
Rozwiązanie. Nie ma takiego algorytmu (Matijasiewicz 1970).

Problem 17. Opis pomijamy, bo akurat tu Hilbert nie popełnił gafy.

Równania diofantyczne

Równanie diofantyczne[1] jest postaci $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$, gdzie $f, g \in \mathbb{Z}[x_1, \ldots, x_n]$.

Interesują nas tylko rozwiązania należące do $\mathbb{Z}^n$.

Przykłady:

- $x^2 + 1 = 0$,
- $x^3 + y^3 = z^3$,
- $x^2 - 8y^2 = 1$.

[1] Diofantos – matematyk aleksandryjski III w. n.e. Na marginesach jego *Arytmetyki* zapiski robił między innymi Fermat.

Twierdzenie Matijasiewicza

Obserwacja:

Jeśli umiemy rozstrzygać, czy równania diofantyczne mają rozwiązania w $\mathbb{Z}$, to umiemy rozstrzygać, czy mają rozwiązania w $\mathbb{N}$ (*twierdzenie Lagrange'a o czterech kwadratach*!).

Twierdzenie Matijasiewicza

Obserwacja:

Jeśli umiemy rozstrzygać, czy równania diofantyczne mają rozwiązania w $\mathbb{Z}$, to umiemy rozstrzygać, czy mają rozwiązania w $\mathbb{N}$ (*twierdzenie Lagrange'a o czterech kwadratach*!).

Twierdzenie (Matijasiewicz 1970, dość słaba wersja)

Nie istnieje algorytm rozstrzygający, czy dane równanie diofantyczne ma rozwiązanie o współczynnikach naturalnych.

- Dowód polega na odwołaniu się do fundamentalnych, ale technicznie prostych pojęć z logiki i teorii obliczeń.
- Żeby się można było do nich odwołać, potrzebne są elementarne, ale niezwykle pomysłowe rozumowania teorioliczbowe.

Krok 1: istnienie problemów nierozstrzygalnych

Twierdzenie (Turing 1936)

Nie istnieje algorytm rozstrzygający, czy dana liczba naturalna należy do zbioru

$$\text{STOP} = \{k \in \mathbb{N} : \ \textit{program o kodzie } k \textit{ zatrzymuje się na wejściu } k\}.$$

Dowód jest dość prostą adaptacją metody przekątniowej Cantora.

Krok 2: problemy nierozstrzygalne a definiowalność

Zbiór STOP można zdefiniować w $\mathbb{N}$ formułą Σ_1, czyli postaci

$$\exists x_1 \ldots \exists x_n \, \Phi(k, x_1, \ldots, x_n),$$

gdzie:

- zmienne $x_1, \ldots, x_n$ przebiegają liczby naturalne,
- Φ jest formułą zbudowaną z:
  - zmiennych $k, x_1, \ldots, x_n, y_1, \ldots, y_m$,
  - stałych 0, 1,
  - operacji $+, \cdot$ oraz relacji $=$,
  - spójników $\wedge, \vee, \neg$
  - kwantyfikatorów ograniczonych, czyli postaci $\forall y_j \leq x_i$.

Krok 2: problemy nierozstrzygalne a definiowalność (c.d.)

W Dowodzie definiowalności zbioru STOP formułą Σ_1 główną trudnością jest kodowanie ciągów liczb za pomocą pojedynczych liczb (i odkodowywanie za pomocą dostatecznie prostych formuł).

Rozwiązania dostarcza:

- *Chińskie twierdzenie o resztach* (układ kongruencji modulo liczby parami względnie pierwsze ma rozwiązanie)
- oraz obserwacja, że dla danego ℓ oraz $k \geq \ell$ liczby $k! + 1, \ldots, \ell k! + 1$ są parami względnie pierwsze.

Formuły diofantyczne

Czy dałoby się zdefiniować STOP formułą diofantyczną, czyli taką Σ_1

$$\exists x_1 \ldots \exists x_n \, \Phi(k, x_1, \ldots, x_n),$$

w której Φ używa tylko zmiennych oraz $0, 1, +, \cdot, =$?

- Jeśli tak, to 10. problem Hilberta jest nierozstrzygalny!
- Sednem sprawy jest eliminacja jednego kwantyfikatora ograniczonego.

Błaganie (Post 1944)

10. problem Hilberta błaga o dowód nierozstrzygalności!

Hipoteza (M. Davis 1949)

Każda formuła Σ_1 jest równoważna diofantycznej.

Krok 4: redukcja do funkcji wykładniczej

Twierdzenie (Davis, Putnam, Robinson 1957–61)

Każdy zbiór Σ_1-definiowalny da się opisać formułą

$$\exists x_1 \ldots \exists x_n \, \Phi(k, x_1, \ldots, x_n),$$

w której Φ używa tylko zmiennych oraz $0, 1, +, \cdot, x^y, =$.

Julia Robinson (1919-1985)

Martin Davis (ur. 1928)

Hilary Putnam (1926-2016)

Krok 4: redukcja do funkcji wykładniczej (c.d.)

Twierdzenie (Davis, Putnam, Robinson 1957–61)

Każdy zbiór Σ_1-definiowalny da się opisać formułą

$$\exists x_1 \ldots \exists x_n \, \Phi(k, x_1, \ldots, x_n),$$

w której Φ używa tylko zmiennych oraz $0, 1, +, \cdot, x^y, =$.

- D. i P. udowodnili to przy założeniu *istnienia dowolnie długich arytmetycznych ciągów l. pierwszych*, które R. wyeliminowała.
- Dowód używa Ch.T.oR. i tricków w stylu Gödla, np. do redukcji problemu do formuły $\forall y \leq x_1 \, f(y, x_1, \ldots, x_n) = 0$...
- ...i do zastąpienia jej formułą, w której są tylko kwantyfikatory $\exists$, a potem kongruencje, $x^y, x!$ oraz symbol Newtona.
- W zasadzie już z wcześniejszych prac J. R. wiadomo było, że jeśli x^y jest diofantyczne, to reszta powyższych też.

Krok 3: hipoteza Julii Robinson

Twierdzenie (Julia Robinson 1952)

Jeśli istnieje funkcja f o wzroście wykładniczym t. że $\{(n, f(n)) : n \in \mathbb{N}\}$ ma definicję diofantyczną, to $x^y = z$ też ją ma.

Dowód używa własności *równań Pella* $x^2 - (a^2 - 1)y^2 = 1$.
[Rozwiązania w $\mathbb{N}^2$ mają strukturę półgrupy cyklicznej z generatorem $(a, 1)$; druga współrzędna $(n+1)$-szego rozwiązania jest rzędu $(2a)^n$.]

Krok 3: hipoteza Julii Robinson

Twierdzenie (Julia Robinson 1952)

Jeśli istnieje funkcja f o wzroście wykładniczym t. że $\{(n, f(n)) : n \in \mathbb{N}\}$ ma definicję diofantyczną, to $x^y = z$ też ją ma.

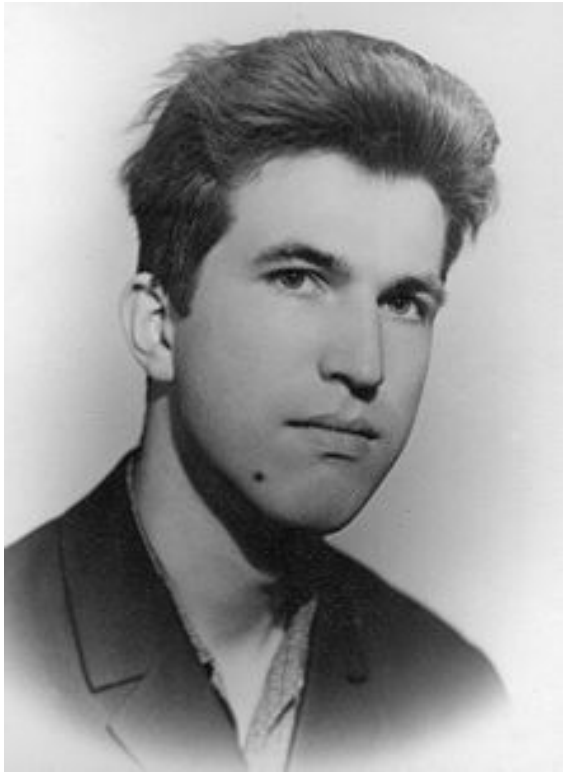
Dowód używa własności *równań Pella* $x^2 - (a^2 - 1)y^2 = 1$.
[Rozwiązania w $\mathbb{N}^2$ mają strukturę półgrupy cyklicznej z generatorem $(a, 1)$; druga współrzędna $(n+1)$-szego rozwiązania jest rzędu $(2a)^n$.]

Założenie o istnieniu f o pożądanych własnościach było znane jako Założenie Julii Robinson ("the Julia Robinson hypothesis").

Lata 60.

- Sporo daremnych prób dowodu Założenia J. R.
- W recenzji pracy DPR w Mathematical Reviews, G. Kreisel powątpiewał w diofantyczność $x^y = z$.
- Julia Robinson traciła wiarę w Założenie, próbowała nawet udowodnić istnienie algorytmu, którego żądał Hilbert.
- Martin Davis: „Myślę, że założenie J. R. jest prawdziwe i że udowodni je jakiś bystry młody Rosjanin”.

Bystry młody Rosjanin



Jurij Matijasiewicz (ur. 1947)

Krok 5: Matijasiewicz

Twierdzenie (Matijasiewicz 1970; znane też jako MRDP)

Każda Σ_1 formuła jest równoważna formule diofantycznej.

Dowód wymaga już „tylko” udowodnienia Założenia J. R.,
czyli znalezienia diofantycznej funkcji rosnącej wykładniczo.

- Pierwotny argument Matijasiewicza wykorzystywał funkcję $n \mapsto 2n$-ta liczba Fibonacciego.
- Obecnie często używa się od razu diofantycznej definicji funkcji $(a, n) \mapsto n$-te rozwiązanie r-nia Pella $x^2 - (a^2 - 1)y^2 = 1$. □

Wnioski

- Diofantyczny jest np. zbiór liczb pierwszych, a zatem istnieje wielomian o współczynnikach całkowitych, którego dodatnie wartości na argumentach z $\mathbb{N}$ to dokładnie liczby pierwsze.
- Istnieje (i da się wygenerować na komputerze) równanie diofantyczne, które ma rozwiązanie dokładnie wtedy, gdy hipoteza Riemanna jest fałszywa.
- Dla każdej dostatecznie silnej teorii aksjomatycznej T istnieje równanie diofantyczne, które nie ma rozwiązania, ale T o tym nie wie.