Ivan M. Havel

O desátém Hilbertově problému

Pokroky matematiky, fyziky a astronomie, Vol. 18 (1973), No. 4, 185--192

Persistent URL: http://dml.cz/dmlcz/138822

Hilbertovy problémy

O desátém Hilbertově problému

Ivan Havel, Praha

1. Desátý Hilbertův problém se týká řešitelnosti diofantických rovnic. Může být zformulován takto: Požaduje se udání metody, která by pro každou diofantickou rovnici umožnila po konečném počtu kroků rozhodnout, zda tato rovnice má řešení, či nikoliv.

Diofantickou rovnicí se zde míní rovnice tvaru

$$P(x_1, \ldots, x_n) = 0 ,$$

kde P je polynom v $x_1, \ldots, x_n$ s celočíselnými koeficienty; řešením této rovnice rozumíme každou n-tici celých čísel $(x_1, \ldots, x_n)$, která anuluje polynom P. Tak například

$$xy^2 - 2y + x^2 - 1 = 0$$

je diofantická rovnice, která má řešení (např. $x = 1$, $y = 2$), zatímco diofantická rovnice

$$u^4 + u^2v^2 + 1 = 0$$

zřejmě žádné řešení nemá.

Desátý Hilbertův problém byl vyřešen teprve nedávno, v r. 1970; přitom řešení je daleko od toho, co Hilbert pravděpodobně očekával. Odpověď zní: Metoda požadovaných vlastností neexistuje. Původní Hilbertova formulace problému ponechává stranou otázku existence takové metody patrně jako apriorně kladně zodpovědělnou a nezmiňuje se o ní.

Skutečnost je ovšem taková, že v době, kdy Hilbert přednesl své problémy, nebylo ještě možné tuto otázku existence metody exaktně položit. Teprve rozvíjející se matematická logika a teorie algoritmů a rekursivních funkcí dodaly potřebné pojmy a důkazové postupy, a tím umožnily matematicky se zabývat podobnými otázkami existence metod či přesněji otázkami existence algoritmů pro řešení různých úloh. Vyřešení 10. problému by tedy nebylo možné bez výsledků GÖDELOVÝCH, CHURCHOVÝCH, KLEENEHO, POSTOVÝCH, TURINGOVÝCH a jiných, kteří podstatně přispěli k rozvoji matematické logiky a teorie rekursivních funkcí.

V práci bezprostředně související s 10. problémem největšího pokroku dosáhli američtí matematikové J. ROBINSONOVÁ, M. DAVIS a H. PUTNAM. Poslední krok nezbytný k úplnému vyřešení problému se podařilo provést mladému leningradskému matematikovi J. V. MATIJASEVIČOVI (mimochodem držiteli 1. ceny mezinárodní matematické olympiády z r. 1964).

Nejstručněji se Matijasevičův výsledek dá vyložit takto: Z prací Davisových, Putnamových a Robinsonové (viz např. [1]) vyplývalo, že k negativní odpovědi na 10. problém, tj. k důkazu neexistence metody ve formulaci problému požadované stačí odpovědět kladně na tuto otázku:

Je pravda, že pro nějaké m existuje polynom $P(x, y, z, u_1, \ldots, u_m)$ s celočíselnými koeficienty takový, že pro všechna přirozená x, y, z platí

$$z = x^y \Leftrightarrow (\exists u_1, \ldots, u_m)\, P(x, y, z, u_1, \ldots, u_m) = 0\,?$$

Jinými slovy: je predikát $z = x^y$ diofantický?*)

Matijasevičovi se podařilo na tuto otázku odpovědět kladně a tak úspěšně korunovat mnohaleté úsilí matematiků pracujících na vyřešení 10. problému. Zajímavé je, že jeho důkaz je poměrně jednoduchý a v podstatě nepoužívá metod moderní matematiky. Hlavní roli v něm hrají vlastnosti Fibonacciových čísel.

2. Pro jakkoli stručný a heslovitý výklad řešení 10. problému je nezbytné vyjasnit si základní pojmy teorie algoritmů (nebo rekursivních funkcí), totiž pojmy „rekursivní množina", „rekursivně spočetná množina", „algoritmická (či rekursivní) řešitelnost problému" apod., jakož i pojmy spojené s 10. problémem těsněji — např. „diofantická množina", „diofantický predikát" apod.

Především poznamenejme, že řešitelnost diofantických rovnic v celých číslech je ekvivalentní řešitelnosti v přirozených číslech v tomto smyslu: Ke každé diofantické rovnici R_1 (připomeňme si, že to je rovnice tvaru $P(x_1, \ldots, x_n) = 0$, kde P je polynom s celočíselnými koeficienty) se dá efektivně sestrojit rovnice R_2 taková, že R_1 má řešení v celých číslech, právě když R_2 je řešitelná v přirozených číslech, a podobně i naopak (blíže je možné se s tímto obratem seznámit např. v [2]). Proto se můžeme od této chvíle zabývat řešitelností diofantických rovnic pouze v oboru přirozených čísel. (Vysvětleme ekvivalenci obou úloh poněkud podrobněji: Předpokládejme, že umíme v konečném počtu kroků pro libovolnou diofantickou rovnici rozhodnout, zda má řešení v celých číslech. Je-li nyní dána libovolná diofantická rovnice R a je o ní třeba rozhodnout, zda je řešitelná v přirozených číslech, sestrojíme k ní nejprve efektivně — podle výše uvedené poznámky — diofantickou rovnici R' takovou, že R' je řešitelná v celých číslech, právě když R má řešení v přirozených číslech, a na R' aplikujeme postup, jehož existenci před-

*) Symbol $\exists$ je znakem tzv. existenčního kvantifikátoru, čte se „existuje" nebo „existují". Druhý kvantifikátor, tzv. všeobecný, $\forall$, který se v tomto článku nepoužívá, znamená „pro každé" nebo „pro všechna". „Predikáty" můžeme chápat jako zobrazení k-tic ($k \geqq 1$) přirozených čísel do dvouprvkové množiny {pravda, lež}. Je-li $k = 1$, resp. 2, resp. 3, hovoříme o unárních, resp. binárních, resp. ternárních predikátech. Např. ternární predikát $z = x^y$ je pravdivý pro tyto trojice (x, y, z): (1, 1, 1), (2, 3, 8), (10, 3, 1000), nepravdivý pro trojici (2, 2, 2).

pokládáme. Protože R byla libovolná a přechod od R k R' je efektivní, umíme rozhodovat pro libovolnou diofantickou rovnici v konečném počtu kroků, zda je řešitelná v přirozených číslech. Podobná úvaha je správná i v opačném směru.)

V teorii rekursivních funkcí se vyšetřují různé třídy funkcí. Pro naši potřebu vystačíme jen s třídou tzv. obecně rekursivních funkcí, které budeme nazývat prostě „rekursivními funkcemi". Množinu přirozených čísel (s nulou) označíme N, její k-tou kartézskou mocninu jako N^k. Zajímáme se o funkce různého počtu argumentů, nabývajících pouze přirozených hodnot, s funkčními hodnotami opět v N. Konstrukce množiny rekursivních funkcí probíhá pak takto: Vychází se ze souboru jistých tzv. základních funkcí – je to konstantní nulová funkce jedné proměnné $O(x) = 0$, funkce následníka $S(x) = x + 1$ a spočetný soubor „projektivních" funkcí $I_n^m(x_1, \ldots, x_n) = x_m$. Pomocí operátorů substituce, primitivní rekurse a efektivní minimalizace použitých konečněmnohokrát se pak induktivně vytvoří množina rekursivních funkcí. Poznamenejme zde, že operátor substituce je vlastně dobře známé tvoření složené funkce, primitivní rekurse, s kterou je možné se již setkat v úvahách Dedekindových, je jisté zobecnění rekurentní definice. A konečně operátor minimalizace umožňuje přecházet od již sestrojené funkce $F(x_1, \ldots, x_{n+1})$ k funkci $G(x_1, \ldots, x_n)$ takto: Předpokládejme, že ke každému výběru n-tice argumentů $(x_1, \ldots, x_n)$ existuje aspoň jedno x_{n+1} takové, že $F(x_1, \ldots, x_n, x_{n+1}) = 0$. Funkční hodnotu $G(x_1, \ldots, x_n)$ pak definujeme jako nejmenší x_{n+1} takové, že $F(x_1, \ldots$ $\ldots, x_n, x_{n+1}) = 0$.

Blíže se o těchto základních pojmech teorie rekursivních funkcí může čtenář poučit např. v [2], [5]. Rekursivní funkce jsou všude definované a mají ještě jednu důležitou vlastnost – jsou tzv. efektivně vyčíslitelné. Základní funkce jsou totiž natolik jednoduché, že je bezpochyby umíme „vyčíslit". Operátory, s jejichž pomocí se rekursivní funkce tvoří, rovněž zachovávají vlastnost „být vyčíslitelnou funkcí". Zde se stýká přesný matematický formalismus (totiž definice rekursivní funkce jakožto matematického objektu) s pojmy intuitivního charakteru (vyčíslitelný). Dokud nedáme pojmu „vyčíslitelný" přesný význam (tj. dokud nepodáme jeho matematickou definici), nemohou mít tvrzení týkající se efektivní vyčíslitelnosti charakter matematických vět.

Výrok typu „Každá efektivně vyčíslitelná funkce je rekursivní" (zaručující spolu s předcházejícím odstavcem rovnost množiny všude definovaných tzv. efektivně vyčíslitelných funkcí a množiny rekursivních funkcí) má tedy spíše charakter přírodovědného principu, který zobecňuje lidskou zkušenost. Je mnoho rozumných důvodů věřit tomuto principu, zvanému Churchova teze, ale podobná diskuse není tématem tohoto článku. Přijměme tedy Churchovu tezi a můžeme si být pak jisti, že máme-li funkci f zobrazující N^k do N a tato funkce je nějakým efektivním způsobem vyčíslitelná (např. jistou procedurou mechanického charakteru, při které pro každý soubor argumentů výpočet končí po konečném počtu kroků), je f rekursivní funkce.

Množina $A \subset N$ se nazývá rekursivní, jestliže je rekursivní její charakteristická funkce χ_A definovaná takto: $\chi_A(x) = 1$, jestliže $x \in A$ a $\chi_A(x) = 0$ pro $x \in N - A$. Množina $A \subset N$ se nazývá rekursivně spočetná, jestliže může být získána jako množina hodnot jisté rekursivní funkce. Tedy $A \subset N$ je rekursivně spočetná, jestliže existuje rekursivní funkce $f(x)$ taková, že $A = \{f(x);\ x \in N\}$. Dá se dokázat, že každá rekursivní množina

je rekursivně spočetná a že opak není pravdou. Existují rekursivně spočetné množiny, které nejsou rekursivní.

Předpokládejme nyní, že je dána množina $A \subset N$. Pro každé $x \in N$ si pak můžeme položit otázku: je $x \in A$? Dostaneme tak nekonečný soubor jednotlivých konkrétních problémů:

je $1 \in A$?

je $2 \in A$?

.....

.....

Odpověď na každý „jednotkový" problém je buď ano, nebo ne. Můžeme ovšem též shrnout jednotkové problémy a zformulovat tzv. hromadný problém: udejte efektivní metodu, která by pro každé $x \in N$ po konečném počtu kroků stanovila, zda $x \in A$ či $x \notin A$. Řešení hromadného problému pak spočívá buď v sestrojení efektivní metody (neboli algoritmu) požadovaných vlastností, nebo v důkazu, že takový algoritmus neexistuje. V prvním případě říkáme, že hromadný problém je algoritmicky (nebo též rekursivně) řešitelný, ve druhém hovoříme o algoritmické neřešitelnosti problému.

Není-li hromadný problém algoritmicky řešitelný, neznamená to ještě, že jeho „jednotkové" komponenty nebude možné rozhodnout. Nepůjde to však jedinou obecnou napřed sestrojenou efektivní metodou (algoritmem), nýbrž každý jednotkový problém pak bude obecně vyžadovat jiný tvůrčí postup.

Přesvědčíme se ještě, že výše formulovaný tzv. rozhodovací problém je algoritmicky řešitelný právě pro rekursivní množiny. Skutečně, buď nejprve $A \subset N$ rekursivní. Pak existuje jednoduchý obecný postup, jak pro libovolné $x \in N$ rozhodnout, zda $x \in A$. Návod zní: dosaď x do charakteristické funkce množiny A. Ta je rekursivní, tedy efektivně vyčíslitelná a pro každé $x \in N$ tak známe po konečném počtu kroků odpověď. Buď naopak $A \subset N$ taková, že je k dispozici algoritmus, který pro každé $x \in N$ rozhoduje, zda $x \in A$, či nikoliv. To zaručuje efektivní vyčíslitelnost charakteristické funkce množiny A. Pro dané $x \in N$ totiž nejprve algoritmem rozhodneme, zda $x \in A$ nebo $x \notin A$. V prvním případě položíme $\chi_A(x) = 1$, ve druhém $\chi_A(x) = 0$. Podle Churchovy teze je pak χ_A rekursivní, tedy i A je rekursivní, cbd.

Závěrem této krátké exkurze do teorie rekursivních funkcí zformulujeme některé hromadné problémy:

1. Sestrojit algoritmus, který by pro každé přirozené číslo rozpoznával, zda je prvočíslem. Problém je algoritmicky řešitelný, čtenář si jistě snadno uvědomí, jak vypadá příslušný algoritmus pracující např. pomocí dělitelnosti.
2. Sestrojit algoritmus, který by pro každou formuli výrokového počtu rozhodoval, zda je ve výrokovém počtu dokazatelná (algoritmicky řešitelný problém, jak se dokazuje ve výrokové logice).
3. Totéž pro predikátový počet (algoritmicky neřešitelný problém, jak bylo dokázáno v průběhu 30. let).

4. Rozhodnout pro libovolnou kvadratickou rovnici s racionálními koeficienty, zda má dva různé reálné kořeny (algoritmicky řešitelné, algoritmus je jednoduchý: vypočítej diskriminant).
5. Sestrojit algoritmus, který by rozhodoval pro libovolnou diofantickou rovnici, zda má řešení (algoritmicky neřešitelné, požadovaný algoritmus neexistuje).

3. Čtenář jistě postřehl, že poslední příklad je modernizovanou verzí 10. problému. Přejdeme nyní k bližšímu rozboru tohoto problému a zavedeme ještě některé pojmy:

Množina $A \subset N$ se nazývá diofantická, jestliže pro jisté $m \geqq 0$ existuje polynom $P(y, u_1, \ldots, u_m)$ s celočíselnými koeficienty takový, že

$$y \in A \Leftrightarrow (\exists u_1, \ldots, u_m \in N)\, P(y, u_1, \ldots, u_m) = 0\,.$$

Například množina všech úplných čtverců $\{0, 1, 4, 9, 16, \ldots\}$ je diofantická (příslušný polynom je $y - u^2$).

Ukážeme si nyní, že nutnou podmínkou pro kladné řešení 10. problému je rekursivnost každé diofantické množiny. Skutečně, předpokládejme, že disponujeme algoritmem, který pro každou diofantickou rovnici umí říci po konečném počtu kroků, zda je řešitelná v oboru celých čísel či nikoliv. Víme již, že potom by nutně musel existovat také algoritmus, který by pro každou diofantickou rovnici rozhodoval, zda je řešitelná v přirozených číslech. Buď nyní A diofantická množina s definujícím polynomem $P(y, u_1, \ldots$ $\ldots, u_m)$. Ukážeme, jak se sestrojí rozhodovací procedura pro množinu A. Pro $k \in N$ utvoříme rovnici $P(k, u_1, \ldots, u_m) = 0$, zapojíme základní algoritmus, který řekne, zda tato rovnice má či nemá řešení a podle toho konstatujeme buď $k \in A$, nebo $k \notin A$ – to vše v konečném počtu kroků, neboli A je rekursivní.

Pro důkaz neexistence metody požadované 10. problémem neboli pro negativní řešení 10. problému stačí tedy nalézt aspoň jednu diofantickou množinu, která by nebyla rekursivní. Existenci takové množiny zaručuje věta, která tvrdí, že dokonce každá rekursivně spočetná množina je diofantická. Tato věta má pro 10. problém základní význam. Již dříve jsme totiž řekli, že existují rekursivně spočetné množiny, které nejsou rekursivní. Každá taková množina je pak příkladem nerekursivní diofantické množiny. Nutná podmínka tedy není splněna a efektivní metoda požadovaná ve formulaci 10. problému nemůže existovat.

Pro vysvětlení historie důkazu základní věty „Každá rekursivně spočetná množina je diofantická" potřebujeme ještě další pojmy.

Zřejmým způsobem nejprve rozšíříme pojem diofantické množiny na množiny n-tic přirozených čísel: $A \subset N^n$ je diofantická, jestliže pro jisté $m \geqq 0$ existuje polynom $P(y_1, \ldots, y_n, u_1, \ldots, u_m)$ s celočíselnými koeficienty takový, že $(y_1, \ldots, y_n) \in A \Leftrightarrow$ $\Leftrightarrow (\exists u_1, \ldots, u_m)\, P(y_1, \ldots, y_n, u_1, \ldots, u_m) = 0$. n-ární predikát $(n \geqq 1)$ $\varrho(y_1, \ldots, y_n)$ nazveme diofantickým, jestliže jeho extenze, tj. množina $\{(y_1, \ldots, y_n);$ platí $\varrho(y_1, \ldots, y_n)\}$ je diofantická.

Nejjednodušší diofantické množiny jsou např. $\{(x, y, z);\ z = x + y\}$, $\{(x, y, z);$ $z = x \,.\, y\}$; diofantické jsou predikáty $\varrho_1(x, y, z) \Leftrightarrow z = x^2 + y^2$, $\varrho_2(x, y) \Leftrightarrow x < y$ i $\varrho_3(x, y) \Leftrightarrow x \leqq y$.

Zajímavý a jak se později ukázalo velmi důležitý je problém množiny

$$E = \{(x, y, z);\ z = x^y\}\ .$$

Je tato množina diofantická?

J. Robinsonová již v r. 1952 dokázala (viz [7]), že jestliže existuje aspoň jeden diofantický predikát exponenciálního růstu, pak E je diofantická. Zde se dvoumístný predikát $\varrho(x, y)$ nazývá predikátem exponenciálního růstu, jestliže z platnosti $\varrho(x, y)$ vyplývá $y \leqq x^x$ a přitom pro každé přirozené k existují x, y taková, že $x \geqq 1$, platí $\varrho(x, y)$ a $x^k < y$.

Problém diofantičnosti množiny E zůstal plných 18 let nerozřešen. Mezitím se ovšem podařilo zredukovat vše zbývající v 10. problému právě na tuto otázku. Podíváme-li se totiž na definici diofantické množiny (nebo predikátu), zjistíme, že je to taková množina, která se dá definovat pomocí operací sčítání, odčítání a násobení (neboť tak se tvoří polynom) a existenčního kvantifikátoru. Je zajímavé zeptat se, jak vypadají množiny, které lze definovat pomocí všeho právě vyjmenovaného a ještě navíc operace mocnění. Lze dokázat, že to jsou tzv. exponenciálně diofantické množiny (a podobně predikáty): $A \subset N^k$ je exponenciálně diofantická, jestliže existuje pro nějaké $m \geqq k$ polynom $P(x_1, \ldots, x_m, x_{11}, \ldots, x_{1m}, \ldots, x_{m1}, \ldots, x_{mm})$ takový, že

$$(x_1, \ldots, x_k) \in A \Leftrightarrow (\exists x_{k+1}, \ldots, x_m)\, P(x_1, \ldots, x_m, x_1^{x_1}, \ldots, x_1^{x_m}, \ldots, x_m^{x_1}, \ldots, x_m^{x_m}) = 0$$

(tj. v P např. místo x_{jk} dosazujeme $x_j^{x_k}$). První kroky ve zkoumání exponenciálně diofantických množin provedla opět J. Robinsonová. Dokázala v r. 1952 ([7]), že množiny $\{(x, y);\ y = x!\}$ a $\left\{(n, k, r);\ r = \binom{n}{k}\right\}$ jsou exponenciálně diofantické. Z roku 1961 je pak velmi důležitý tento výsledek Davisův, Putnamův a Robinsonové (viz [1]): „Každá rekursivně spočetná množina je exponenciálně diofantická". Jinými slovy: každou rekursivně spočetnou množinu lze definovat pomocí operací sčítání, odčítání, násobení, mocnění a pomocí existenčního kvantifikátoru. (Definici rekursivně spočetné množiny přitom přirozeným způsobem rozšíříme i na množiny k-tic přirozených čísel: $A \subset N^k$ je rekursivně spočetná, jestliže existují rekursivní funkce $f_1(x), \ldots, f_k(x)$ takové, že platí $A = \{(f_1(x), \ldots, f_k(x));\ x \in N\}$.) Zbýval problém, jak se zbavit operace mocnění, jak ji vyjádřit pomocí zbývajících; kdyby se to totiž podařilo, bylo by možné o každé exponenciálně diofantické množině tvrdit, že je diofantická. Lze ukázat, že tento problém je ekvivalentní problému diofantičnosti množiny E. Připomeňme, že J. Robinsonová dokázala, že pro důkaz diofantičnosti množiny E stačí nalézt aspoň jeden diofantický predikát exponenciálního růstu. Právě takový predikát nalezl J. Matijasevič (1970, [3]). Jeho výsledek je překvapující nikoli samotnou skutečností, že tento predikát existuje, ale především svým tvarem. Matijasevič definuje predikát $\Phi(u, v)$ takto:

$$\Phi(u, v) \Leftrightarrow v \text{ je v pořadí 2-}u\text{tým Fibonacciovým číslem.}$$

Z posloupnosti Fibonacciových čísel 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ... snadno nahlédneme, pro které dvojice (u, v) platí $\Phi(u, v)$. Jsou to (0, 0), (1, 1), (2, 3), (3, 8), (4, 21), (5, 55) atd.

Zbývá jen složit jednotlivé skutečnosti dohromady: z existence exponenciálně rostoucího diofantického predikátu plyne, že E je diofantická. Tedy každá exponenciálně diofantická množina je diofantická. Protože každá rekursivně spočetná množina je exponenciálně diofantická, je i diofantická. Odtud, jak jsme ukázali na začátku § 3, plyne neexistence algoritmu pro zjišťování řešitelnosti diofantických rovnic.

4. Závěrečnou část tohoto článku věnujeme stručnému naznačení Matijasevičova důkazu. Nejprve zopakujme známou rekurentní definici Fibonacciových čísel: položme $\varphi_0 = 0$, $\varphi_1 = 1$, $\varphi_{n+1} = \varphi_n + \varphi_{n-1}$. φ_j nazýváme j-tým Fibonacciovým číslem. Poměrně snadno lze dokázat, že predikát $\Phi(u, v)$, definovaný výše ($\Phi(u, v) \Leftrightarrow v = \varphi_{2u}$), je exponenciálního růstu. Platí totiž $\varphi_{2(n+1)} = 3\varphi_{2n} - \varphi_{2(n-1)}$, a tedy i $2\varphi_{2n} < \varphi_{2(n+1)} \leqq 3\varphi_{2n}$, odkud nalezneme indukcí meze pro φ_{2n}: $n \leqq 2^{n-1} \leqq \varphi_{2n} < 3^n$. S jejich pomocí se lehko ověří, že $\Phi(u, v)$ je predikát exponenciálního růstu. Důkaz diofantičnosti tohoto predikátu je rozsáhlejší, ale principiálně není obtížný. Čtenář, který se s ním bude chtít blíže seznámit, může poměrně snadno prostudovat 19 lemmat popisujících vlastnosti Fibonacciových čísel uvedených v [3], jež nakonec vedou k větě, kterou zde ze stejné práce citujeme:

K tomu, aby v bylo $2u$-tým Fibonacciovým číslem ($v = \varphi_{2u}$), je nutné a stačí, aby existovala přirozená čísla g, h, l, m, x, y a z taková, že platí těchto 9 vztahů:

(1) $u \leqq v < l$
(2) $l^2 - lz - z^2 = 1$
(3) $g^2 - gh - h^2 = 1$
(4) $l^2 \mid g$
(5) $l \mid (m - 2)$
(6) $(2h + g) \mid (m - 3)$
(7) $x^2 - mxy + y^2 = 1$
(8) $l \mid (x - u)$
(9) $(2h + g) \mid (x - v)$

Konjunkce podmínek (1)–(9) může být ovšem vyjádřena jako podmínka anulování jistého polynomu, čímž je důkaz diofantičnosti $\Phi(u, v)$ ukončen.

Závěrem naznačíme možné aplikace a dosah získaných výsledků. Ze základní věty o diofantičnosti každé rekursivně spočetné množiny a z jedné práce Putnamovy ([6]) vyplývá toto tvrzení: Je možné sestrojit polynom pátého stupně $Q(y_1, \ldots, y_k, z)$ s celočíselnými koeficienty takový, že libovolnou rekursivně spočetnou množinu M přirozených čísel lze získat jako množinu nezáporných hodnot polynomu $Q(y_1, \ldots, y_k, a_M)$, kde a_M je konstanta, kterou lze efektivně vypočíst na základě znalosti induktivní výstavby nějaké rekursivní funkce f takové, že $M = \{f(x);\ x \in N\}$.

Vezmeme-li tedy za M_1 např. množinu všech prvočísel, $M_1 = \{2, 3, 5, 7, \ldots\}$, za M_2 např. množinu všech úplných čtverců, $M_2 = \{0, 1, 4, 9, 16, \ldots\}$ (mimochodem obě jsou rekursivní), můžeme je vytvořit také tak, že v pevném polynomu $Q(y_1, \ldots, y_k, z)$ – zkonstruovaném předem „jednou provždy" – dosadíme za z nejprve $z = a_{M_1}$, a potom $z = a_{M_2}$ a v obou případech vezmeme množiny nezáporných funkčních hodnot takto sestrojených polynomů k proměnných. Poprvé tak dostaneme M_1 – všechna prvočísla, v druhém případě M_2 – množinu všech úplných čtverců.

Podobně lze převést na úlohu o polynomech také Fermatův problém: Má se rozhodnout, zda existují kladná celá čísla x, y, z a n, $n > 2$, taková, že $x^n + y^n = z^n$. Položme

$$M_2 = \{(x, y, z, n);\ x, y, z, n \text{ jsou celá kladná, } n > 2 \text{ a } x^n + y^n = z^n\}.$$

Fermatův problém pak zní: je $M_2 \neq \emptyset$?

Všimněme si nejprve, že ačkoli o M_2 nevíme, zda je prázdná, či nikoliv, můžeme konstatovat, že je to rekursivní množina. Snadno se totiž sestrojí algoritmus, který bude pro čtveřice přirozených čísel (x, y, z, n) rozhodovat, zda $x^n + y^n = z^n$. Jakožto rekursivní (a tedy i rekursivně spočetná) množina je M_2 diofantická. Dá se tedy sestrojit polynom $P(x, y, z, n, u_1, \ldots, u_m)$ takový, že $(x, y, z, n) \in M_2 \Leftrightarrow (\exists u_1, \ldots, u_m)(P(x, y, z, n, u_1, \ldots, u_m) = 0)$.

Platí potom zřejmě, že M_2 je neprázdná, právě když diofantická rovnice $P(x, y, z, n, u_1, \ldots, u_m) = 0$ má aspoň jedno řešení.

Zjednodušení Fermatova problému touto cestou získané je ovšem pouze zdánlivé. Problém je sice převeden na otázku, zda existuje řešení jedné konkrétní diofantické rovnice, avšak kdyby se tuto rovnici vůbec podařilo napsat, měla by pravděpodobně velký počet neznámých a dále pak z dokázaného faktu, že není možný algoritmus, který by pro každou diofantickou rovnici rozhodoval, zda je, či není řešitelná, se dá usoudit, že i jednotlivé „jednotkové" problémy, pro každou konkrétní rovnici zvlášť, mohou být značně obtížné.

Vyřešení 10. Hilbertova problému je cenným úspěchem matematiky našeho století. Dá se očekávat, že bude mít vliv na mnohé otázky ve více či méně příbuzných partiích matematiky, jak tomu ostatně nasvědčují práce, které se již začínají objevovat.

Literatura

[1] Davis M., Putnam H., Robinson J., *The decision problem for exponential Diophantine equations*, Ann Math. *74* (1961), 425—436, ruský překlad ve sb. „Matematika", No *5* (1964).

[2] Malcev A. I., *Algoritmy i rekursivnyje funkcii*, Nauka, Moskva, 1965.

[3] Matijasevič J. V., *Diofantovosť perečislimych množestv*, DAN SSSR, 1970, (*191*), No 2.

[4] Matijasevič J. V., *Diofantovo predstavlenije perečislimych predikatov*, Izvestija AN SSSR, ser. mat., *35*, No 1, 1971.

[5] Péter Rózsa, *Rekursive Funktionen*, Budapest 1951, ruský překlad IL, Moskva, 1954.

[6] Putnam H., *An unsolvable problem in number theory*, J. Symbolic Logic, *25*, 3 (1960).

[7] Robinson J., *Existential Definability in Arithmetic*, Trans. Amer. Math. Soc. *72* (1952), 437—439.

Myšlenka, že fyzika musí být čistá, aby to byla skutečná fyzika, že výzkum na hranici mezi fyzikou a biologií je pod důstojnost správného fyzika, byla stejně nesprávná v roce 1946, jako je i dnes. Nedávný článek Williama Spohna nazvaný „Může být matematika zachráněna?" vyvolal rozruch v matematickém světě. Spohnova hlavní teze spočívá v tom, že puritáni, kteří vládnou ve většině matematických institucí, odcizili matematiku natolik od zbývající lidské kultury, že se ocitla v nebezpečí stát se sterilní. Mnohé z toho, co tvrdí Spohn, stejně dobře platí, když změníme název jeho článku na „Může být fyzika zachráněna?" a dosadíme si místo „moderní matematiky" „fyziku vysokých energií". Nejjistější cesta, jak zachránit fyziku od katastrofální stagnace či sestupu během následujících třiceti let, podle mého názoru je donutit mladé fyziky pracovat na pomezí, kde se fyzika překrývá s jinými vědami...

F. J. DYSON
