KALEIDOSKOP TEORIE ČÍSEL (3. kapitola)

Martin Klazar

Vím, že čísla jsou krásná. A jestliže krásná nejsou, pak není krásné nic.

(Paul Erdős, *Sunday Times Magazine,* 27. listopadu 1988.)

Analogicky prožíval pan Š. číslice.
„Pro mne 2, 4, 6, 5 nejsou pouhá čísla. Mají tvar …
1 — to je ostré číslo, nezávisle na jeho grafickém vyjádření,
je to něco ukončeného, tvrdého.
2 — to je plošší, čtverhranné, bělavé, bývá trochu našedlé …
3 — to je zaostřený úlomek a točí se.
4 — to je opět čtvercové, tupé, podobné 2, ale mohutnější, tlusté …
5 — plné zakončení v podobě kužele, věže, masívní.
6 — to následuje první za „5“, je bělavé.
8 — to je nevinné, modravě mléčné, podobné vápnu.“

(A. R. Lurija, *Malá knížka o velké paměti.*)

Toto je předběžný text 3. kapitoly (diofantické rovnice) skript k mé přednášce *Úvod do teorie čísel*, kterou jsem konal na MFF UK v Praze v zimních semestrech školních roků 1996/97, 1998/99 a 1999/00. Zatím v preprintové řadě KAM-DIMATIA Series vyšly kapitoly 1 (základní pojmy a obraty) a 2 (diofantické aproximace) a budou v ní postupně vydány zbylé kapitoly: 4 (kongruence), 5 (prvočísla), 6 (geometrie čísel), 7 (číselné rozklady), 8 (medailony matematiků) a 9 (návody k řešením úloh). Obtížnost úloh je bodována 0 (nejlehčí) až 5 (nejtěžší).

duben 2000 Martin Klazar

Obsah

Kapitola 3

Řešení rovnic celými čísly

Třetí kapitola se zabývá diofantickými rovnicemi. Přívlastek „diofantický“ znamená „celočíselný“. Máme dán *celočíselný* polynom $P \in \mathbf{Z}[x_1, \ldots, x_r]$ a hledáme *celočíselná* řesení rovnice $P = 0$, což jsou r-tice $(a_1, a_2, \ldots, a_r) \in \mathbf{Z}^r$ splňující $P(a_1, a_2, \ldots, a_r) = 0$. Zkoumají se samozřejmě i soustavy rovnic a i jiné rovnice než polynomiální, ale diofantické problémy s jednou polynomiální rovnicí jsou nejčastější. Jak uvidíme, polynomiální soustavy se dají převést na jedinou rovnici. Není-li řečeno jinak, řešením rozumíme celočíselné řešení.

Jde o problémy velmi staré a nezřídka i velmi těžké. Už staří Babylóňané uměli vytvářet řešení rovnice $x^2 + y^2 = z^2$. Klamavě podobný tvar má i notoricky známá *Fermatova poslední věta* (FPV), jež tvrdí, že $x^n + y^n = z^n$ nemá pro žádný exponent $n > 2$ řešení x, y, z s nenulovými složkami. Důkaz, který v r. 1995 publikoval Andrew Wiles, užívá komplikovaných a abstraktních nástrojů, k nimž se v tomto textu nepřiblížíme ani na dohled. Je to jeden z největších úspěchů moderní matematiky.

Obtížnost diofantických problémů příliš nesouvisí s velikostí stupně polynomu P. Jako příklad vezmeme diofantickou rovnici

$$x^{13} + y^{13} = 19z^{13}$$

a ukážeme, jak ji převést na ekvivalentní rovnici stupně 4. Použijeme k tomu soustavu pěti rovnic s šesti neznámými

$$x_1 - x^2 = 0 \;\&\; x_2 - x_1^2 = 0 \;\&\; x_3 - x_2^2 = 0 \;\&\; x_4 - x_2x_3 = 0 \;\&\; x_5 - x_4x = 0\ .$$

Je jasné, že $x, x_1, \ldots, x_5 \in \mathbf{Z}$ je její řešení, právě když $x_5 = x^{13}$. Vezmeme dvě analogické soustavy s neznámými $y, y_1, \ldots, y_5$ a $z, z_1, \ldots, z_5$ a levé strany příslušných 15 rovnic označíme jako $L_1, L_2, \ldots, L_{15}$. Vše shrneme do jediné velerovnice

$$L_1^2 + L_2^2 + \cdots + L_{15}^2 + (x_5 + y_5 - 19z_5)^2 = 0 \; .$$

Ta má řešení, právě když ho má soustava $L_1 = 0, L_2 = 0, \ldots, L_{15} = 0$ a $x_5 + y_5 - 19z_5 = 0$. A to nastane, právě když $x^{13} + y^{13} = 19z^{13}$ má řešení. Původní rovnice je řešitelná tehdy a jen tehdy, je-li řešitelná velerovnice. Víc než to, z množiny řešení velerovnice umíme snadno odvodit všechna řešení původní rovnice a naopak. Velerovnice má stupeň 4.

Je jasné, že zobecněním tohoto postupu umíme jakoukoli diofantickou rovnici (nebo soustavu) převést na ekvivalentní rovnici se stupněm ≤ 4. Za snížení stupně však zaplatíme mnoha novými neznámými. (Nedal by se nějak redukovat i počet neznámých? Bláznivý nápad?)

Místo velerovnice můžeme vzít soustavu

$$L_1 = 0 \; \& \; L_2 = 0 \; \& \; \ldots \; \& \; L_{15} = 0 \; \& \; u_1 = x_5 + y_5 \; \&$$
$$u_2 = (-19)z_5 \; \& \; u_3 = u_1 + u_2 \; \& \; u_3 = 0 \; .$$

Ta je opět ve zmíněném smyslu ekvivalentní původní rovnici $x^{13} + y^{13} = 19z^{13}$. Obecně opět umíme jakoukoli diofantickou rovnici (nebo soustavu) zredukovat na ekvivalentní soustavu rovnic typu $\alpha = \beta + \gamma$ a $\alpha = \beta \cdot \gamma$, kde α, β, γ jsou neznámé nebo konstanty ze $\mathbf{Z}$. Této redukce si povšiml ve třicátých letech 20. století Thoralf Skolem. Je zajímavé, že redukce se dá stále provést, ikdyž povolené typy rovnic v soustavě jsou jen $\alpha = \beta + 1$ a $\alpha = \beta \cdot \gamma$ (úloha 17).

Uvedené redukce rovnic a „konverze“ řešení se dají bez obtíží naprogramovat. Nedal by se naprogramovat sám proces hledání řešení diofantických rovnic? Nebo (proč příštipkařit) přímo celá matematika? První otázka je slavný desátý Hilbertův problém z r. 1900. Zápornou odpověď nalezl v r. 1970 Jurij Matijasevič: Neexistuje algoritmus, který by pro každý vstupní celočíselný polynom $P(x_1, \ldots, x_r)$ v konečném čase rozhodl, zda $P = 0$ má celočíselné řešení. Matijasevičův překvapivý a krásný výsledek popíšeme v oddílu 3.5.

V oddílu 3.1 diskutujeme řešení rovnice $x^n + y^n = z^n$ pro $n = 2, 3$ a 4. Pomocí kongruencí ukážeme, že pro řadu prvočísel p rovnice $x^p + y^p + z^p = 0$ nemá řešení splňující $xyz \not\equiv 0 \bmod p$. V 3.2 dokážeme klasickou Lagrangeovu větu, podle níž je rovnice $x^2 + y^2 + z^2 + t^2 = n$ řešitelná pro každé $n \in \mathbf{N}_0$. V 3.3 vyložíme teorii Pellovy rovnice $x^2 - dy^2 = 1$ ($d \in \mathbf{N}$ není čtverec) a převedeme na ni několik složitějších diofantických úloh.

Nekonečnost počtu řešení plyne pomocí Dirichletovy věty z oddílu 2.1. V 3.4 použijeme Thueho větu z oddílu 2.7 a ukážeme, že $x^3 - 2y^3 = 1$ má jen konečně mnoho řešení, stejně jako spousta podobných diofantických rovnic. V 3.5 dokážeme již zmíněnou Matijasevičovu větu.

Všechny důkazy jsou elementární. V oddílu 3.5, který je náročnější, pomůže znalost základů predikátové logiky prvního řádu a teorie rekurze. Mnoho se ale nepotřebuje a vše nezbytné stručně zopakujeme. Diofantických rovnic se týkají rovněž výsledky v šesté kapitole v oddílu 6.?.

3.1 O Fermatově poslední větě

Nechť $x, y, z \in \mathbf{Z}$ jsou nenulová čísla, která splňují rovnici

$$x^2 + y^2 = z^2 \ .$$

Můžeme předpokládat, že $x, y, z \in \mathbf{N}$, $x \perp y$ a x je sudé (x a y nemohou být současně lichá, 2 není modulo 4 čtverec). Takové trojici se říká *Pythagorejská trojice*. Každé jiné řešení rovnice je odvozeno z Pythagorejské trojice změnou znamének, prohozením x a y a vynásobením x, y a z společným činitelem. Ukážeme si, že existuje nekonečně mnoho Pythagorejských trojic a že se všechny dají jednoduše popsat.

Tvrzení 48 (popis Pythagorejských trojic). *Trojice $x, y, z \in \mathbf{N}$ je Pythagorejská, právě když*

$$x = 2ab \ , \ y = a^2 - b^2 \ \& \ z = a^2 + b^2 \ ,$$

kde $a > b \geq 1$ jsou nesoudělná celá čísla s opačnou paritou.

Důkaz. Zřejmě

$$(2ab)^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2$$

a zpětná implikace je jasná. Nechť naopak $x, y, z \in \mathbf{N}$ je Pythagorejská trojice. Protože y a z jsou nesoudělná a lichá, jsou nesoudělná i přirozená čísla $(z - y)/2$ a $(z + y)/2$. Protože

$$\left(\frac{x}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2} \ ,$$

dostáváme pro vhodná čísla $a, b \in \mathbf{N}$ (podle tvrzení 3 z 1. kapitoly), že

$$\frac{z+y}{2} = a^2 \ \& \ \frac{z-y}{2} = b^2 \ .$$

Odtud plynou vztahy pro x, y a z a vlastnosti a a b. $\diamondsuit$

Například pro $a \leq 5$ dostáváme Pythagorejské trojice (x, y, z)

$$(4,3,5),\ (12,5,13),\ (8,15,17),\ (24,7,25),\ (20,21,29) \ \text{ a } \ (40,9,41) \ .$$

Nekonečný sestup je metoda důkazu neexistence řešení diofantické rovnice, již vymyslel Fermat. Pro danou diofantickou rovnici najdeme způsob, jak z řešení vyrobit menší řešení. Postup opakujeme a dostaneme nekonečnou klesající posloupnost přirozených čísel. Taková posloupnost ovšem neexistuje (princip indukce) a tedy rovnice nemá řešení. Pěkným příkladem je následující věta, která je o trochu silnější než FPV pro $n = 4$.

Věta 49 (Fermat, 17. st.). *Diofantická rovnice*

$$x^4 + y^4 = z^2$$

nemá řešení s kladnými složkami.

Důkaz. Nechť řešení $x, y, z \in \mathbf{N}$ existuje. Můžeme předpokládat, že tato čísla jsou po dvou nesoudělná. Není možné, aby x a y byla lichá (viz modul 4). Nechť x je liché a y sudé, pak je z liché. Protože

$$y^4 = (z - x^2)(z + x^2)$$

a $(z - x^2, z + x^2) = 2$, jsou podle vhodné varianty tvrzení 3 dvě možnosti:

$$z - x^2 = 2a^4 \ \& \ z + x^2 = 8b^4 \ \text{nebo} \ \ z - x^2 = 8b^4 \ \& \ z + x^2 = 2a^4,$$

přičemž a a b jsou nesoudělná přirozená čísla a a je liché. První případ je nemožný, odečtením bychom dostali $x^2 = -a^4 + 4b^4$, čili $1 \equiv -1 \bmod 4$. Druhá eventualita dává

$$z = a^4 + 4b^4 \ \& \ x^2 = a^4 - 4b^4 \ . \tag{1}$$

Druhou rovnici přepíšeme na

$$4b^4 = (a^2 - x)(a^2 + x) \ .$$

Z $a \perp b$ plyne $a \perp x$. Čísla a a x jsou lichá. Odtud $(a^2-x, a^2+x) = 2$. Nutně

$$a^2 - x = 2c^4 \quad \text{a} \quad a^2 + x = 2d^4 \ ,$$

kde $c, d \in \mathbf{N}$ a $cd = b$. Sečtením rovnic získáme

$$c^4 + d^4 = a^2.$$

Ale z první rovnice v (1) plyne, že $a < z$. Od x, y, z jsme dospěli k menšímu netriviálnímu řešení c, d, a. Celý postup lze opakovat nekonečněkrát. Nekonečná posloupnost přirozených čísel $z > a > \cdots$ je nemožná. Řešení v $\mathbf{N}$ neexistuje. $\diamondsuit$

Nekonečným sestupem teď dokážeme FPV pro $n = 3$. Pro lichý exponent se rovnice FPV nechá psát ekvivalentně v symetrickém tvaru $x^n + y^n + z^n = 0$.

Věta 50 (Euler, 1770). *Diofantická rovnice*

$$x^3 + y^3 + z^3 = 0$$

nemá řešení splňující $xyz \neq 0$.

Důkaz věty se opírá o pomocné tvrzení, jehož důkaz na chvíli odsuneme.

Tvrzení 51 (čtverce a třetí mocniny). *Pokud $a^2 + 3b^2 = c^3$ pro $a, b, c \in \mathbf{Z}$ a $a \perp b$, pak existují $p, q \in \mathbf{Z}$, že*

$$a + b\sqrt{-3} = (p + q\sqrt{-3})^3 \ ,$$

to jest

$$a = p(p-3q)(p+3q) \quad \text{a} \quad b = 3q(p-q)(p+q) \ .$$

Důkaz věty 50. Nechť $x, y, z \in \mathbf{Z}, xyz \neq 0$, splňují rovnici $x^3 + y^3 + z^3 = 0$. Můžeme předpokládat, že tato tři čísla jsou po dvou nesoudělná a právě jedno z nich je sudé, třeba z. Položíme $x + y = 2a$ a $x - y = 2b$ a z $(x+y)(x^2 - xy + y^2) = (-z)^3$ dostaneme $2a(a^2 + 3b^2) = (-z)^3$. Je lehké vidět, že $a \perp b$ a mají opačnou paritu (neboť $x = a + b$ a $y = a - b$). Odtud dostáváme dvě možnosti: $(2a, a^2 + 3b^2) = 1$ nebo 3.

V prvním případě $(2a, a^2 + 3b^2) = 1$ jsou $2a$ i $a^2 + 3b^2$ třetí mocniny (varianta tvrzení 3) a podle tvrzení 51 máme, pro nějaká $p, q \in \mathbf{Z}$,

$$a = p(p-3q)(p+3q) \quad \text{a} \quad b = 3q(p-q)(p+q) \ .$$

Patrně $p \perp q$, čísla p a q mají opačnou paritu (jinak by a i b byly sudé) a 3 nedělí p. Takže $2p, p-3q$ a $p+3q$ jsou po dvou nesoudělná a — protože $2a$ je třetí mocnina — každé z nich je třetí mocnina, $2p = \alpha^3, p-3q = \beta^3$ a $p+3q = \gamma^3$. Odtud $\beta^3 + \gamma^3 + (-\alpha)^3 = 0$ a $\alpha, \beta, \gamma \in \mathbf{Z}$ jsou jistě nenulová. Protože $(\alpha\beta\gamma)^3 = 2a = x+y$ dělí $(-z)^3$, máme $|\alpha\beta\gamma| \le |z|$ a $0 < |\alpha\beta\gamma| < |xyz|$ ($|x| > 1$ nebo $|y| > 1$).

Pokud $(2a, a^2+3b^2) = 3$, položíme $a = 3c$. Zřejmě 3 nedělí b a $c \perp b$. Dále c a b mají opačnou paritu. Protože $(-z)^3 = 2a(a^2+3b^2) = 18c(3c^2+b^2)$ a $(18c, 3c^2+b^2) = 1$, jsou oba činitelé třetí mocniny. Podle tvrzení 51 opět

$$b = p(p-3q)(p+3q) \quad \text{a} \quad c = 3q(p-q)(p+q)\ ,$$

kde $p \perp q$ a čísla p a q mají opačnou paritu. Protože $18c$ je třetí mocnina, je třetí mocnina i $18c/27 = 2q(p-q)(p+q)$. Činitelé jsou po dvou nesoudělní a proto $2q = \alpha^3, p-q = \beta^3$ a $p+q = \gamma^3$. Máme $\gamma^3 + (-\beta)^3 + (-\alpha)^3 = 0$. Opět zjevně $0 < |\alpha\beta\gamma| < |xyz|$.

V obou případech jsme z $(x,y,z) \in \mathbf{Z}^3$ dostali menší řešení $(\alpha,\beta,\gamma) \in \mathbf{Z}^3$. Nekonečný sestup ukazuje, že netriviální řešení neexistuje. $\diamondsuit$

Zbývá dokázat tvrzení 51. Odvodíme ho z následujícího tvrzení.

Tvrzení 52 (faktorizace v kvadratickém tělese). *Nechť $a, b \in \mathbf{Z}$ jsou nesoudělná a $a^2 + 3b^2 = pm$, kde $p = 4$ nebo p je liché prvočíslo a $m \in \mathbf{N}$.*

1. *Existují čísla $u, v \in \mathbf{N}_0$ taková, že $u^2 + 3v^2 = p$.*

2. *Pro každou takovou reprezentaci p čísly u, v existují nesoudělná čísla $r, s \in \mathbf{Z}$ a volba znaménka tak, že*

$$a + b\sqrt{-3} = (u \pm v\sqrt{-3})(r + s\sqrt{-3})$$

a $r^2 + 3s^2 = m$.

Důkaz. Nejprve dokážeme 1 a 2 pro $p = 4$. Bod 1 je jasný, $u = v = 1$. Co se týče 2, rozlišíme dva případy: $a \equiv b \bmod 4$ a $a \equiv -b \bmod 4$ (čísla a a b jsou zjevně lichá). V prvním případě volíme znaménko $+$ a 2 platí s $r = (a+3b)/4$ a $s = (b-a)/4$. V druhém případě volíme znaménko $-$ a 2 platí s $r = (a-3b)/4$ a $s = (a+b)/4$. Je zřejmé, že $r \perp s$.

Nyní nechť p je liché prvočíslo. Začneme bodem 2. Máme vztahy $a^2+3b^2 = pm$ a $u^2+3v^2 = p$. Vyjdeme z kongruence

$$(ub - va)(ub + va) = b^2(u^2+3v^2) - v^2(a^2+3b^2) \equiv 0 \bmod p\ .$$

Tudíž

$$ub - va \equiv 0 \bmod p \quad \text{nebo} \quad ub + va \equiv 0 \bmod p \ .$$

Nastává-li $ub - va \equiv 0 \bmod p$, volíme znaménko $+$ a položíme $r = (3vb + au)/(u^2 + 3v^2)$ a $s = (bu - av)/(u^2 + 3v^2)$ (je to řešení lineární soustavy ekvivalentní rovnici 2). Zřejmě $s \in \mathbf{Z}$ a protože $3vb + au \equiv a^{-1}u(3b^2 + a^2) \equiv 0 \bmod p$, rovněž $r \in \mathbf{Z}$. Z nesoudělnosti a a b plyne nesoudělnost r a s. Rovnici 2 vynásobíme komplexně sdruženou rovnicí a dostaneme

$$a^2 + 3b^2 = (u^2 + 3v^2)(r^2 + 3s^2) = pm \ .$$

Takže $r^2 + 3s^2 = m$.

Případ $ub + va \equiv 0 \bmod p$ je obdobný, volíme znaménko $-$ a $r = (au - 3vb)/(u^2 + 3v^2)$ a $s = (av + ub)/(u^2 + 3v^2)$. Opět se snadno vidí, že $r, s \in \mathbf{Z}$, $r \perp s$ a $r^2 + 3s^2 = m$.

Dokážeme 1. Můžeme předpokládat, že $p \neq 3$ — vlastnost 2 jsme již dokázali a 1 pro $p = 3$ platí s $u = 0, v = 1$. Postupujeme stejně, jako v důkazu věty 20 v kapitole 2. Protože $a^2 + 3b^2 \equiv 0 \bmod p$, máme číslo $c \in \mathbf{Z}$ takové, že $c^2 \equiv -3 \bmod p$, totiž $c \equiv a/b$. Z teorie kvadratických zbytků, kterou popíšeme v příští kapitole, plyne, že $p \equiv 1 \bmod 3$. Část 1 věty 19 použijeme opět s $\alpha = c/p$ a $Q = \lceil \sqrt{p}\, \rceil$. Existují celá čísla x, y taková, že $1 \le y < \sqrt{p}$ a

$$\left| \frac{c}{p} - \frac{x}{y} \right| < \frac{1}{y\sqrt{p}} \ .$$

Opět máme $0 \le |cy - px| < \sqrt{p}$. Takže

$$0 < z = (cy - px)^2 + 3y^2 < 4p \ .$$

Vzhledem k volbě c je z dělitelné p a mohou nastat tři možnosti: $z = p, 2p$ nebo $3p$. Jak víme, $p \equiv 1 \bmod 3$. Pokud $cy - px \not\equiv 0 \bmod 3$, je $z \equiv 1 \bmod 3$ a nutně $z = p$, čímž jsme hotovi. Pokud 3 dělí $cy - px$, máme $z = 3p$. Pak ale $cy - px = 3d$ a $z/3 = 3d^2 + y^2 = p$ a jsme rovněž hotovi. $\diamondsuit$

Důkaz tvrzení 51. Z předešlého tvrzení plyne, že 2 má v prvočíselném rozkladu čísla $a^2 + 3b^2$ sudý exponent $2a_0$. Ovšem $a^2 + 3b^2$ je třetí mocninou a proto $3 \backslash a_0$. Stejně pro lichá prvočísla. Tedy $a^2 + 3b^2 = 4^{a_0} p_1^{a_1} \cdots p_k^{a_k}$, kde čísla $a_i \in \mathbf{N}$ jsou dělitelná třemi a p_i jsou různá lichá prvočísla. Opakovaným užitím 1 a 2 z posledního tvrzení, přičemž při odštěpování téhož p v 2 bereme stále stejnou reprezentaci 1, dostaneme rozklad

$$a + b\sqrt{-3} = \pm(u_1 \pm v_1\sqrt{-3})(u_2 \pm v_2\sqrt{-3}) \cdots (u_n \pm v_n\sqrt{-3}) \ ,$$

kde $u_i, v_i \in \mathbf{N}_0$, pro každé i je $u_i^2 + 3v_i^2 = p_j$ pro nějaké j ($p_0 = 4$) a každému p_j odpovídá a_j činitelů, kteří se vzájemně liší nejvýše znaménkem. Všech a_j činitelů však musí mít totéž znaménko: Kdyby se v rozkladu objevili současně činitelé $u + v\sqrt{-3}$ i $u - v\sqrt{-3}$, mohli bychom z celého součinu vytknout $(u+v\sqrt{-3})(u-v\sqrt{-3}) = p_j$ a dostali bychom, že p_j dělí a i b, spor s $a \perp b$.

Označíme-li tedy činitele odpovídajícího p_j jako $r_j \pm s_j\sqrt{-3}$, máme

$$\begin{aligned} a + b\sqrt{-3} &= \pm \prod_{j=0}^{k} (r_j \pm s_j\sqrt{-3})^{a_j} = \left(\pm \prod_{j=0}^{k} (r_j \pm s_j\sqrt{-3})^{a_j/3} \right)^3 \\ &= (p + q\sqrt{-3})^3 \ . \end{aligned}$$

Tím je dokázáno tvrzení 51 a dokončen důkaz věty 50. $\diamondsuit$

Různým souvislostem FPV se věnují úlohy 1 až 4.

Pokud by $x^n + y^n = z^n$ měla řešení $x, y, z \in \mathbf{N}$ pro nějaké $n > 2$, mohli bychom rozložením n dosáhnout toho, že $n = 4$ nebo n je liché prvočíslo. První možnost je vyloučena větou 49. Takže se lze vždy omezit na lichý prvočíselný exponent.

Prvním případem FPV pro prvočíselný exponent $p > 2$ se rozumí tvrzení, že

$$x^p + y^p + z^p = 0$$

nemá celočíselné řešení x, y, z splňující $xyz \not\equiv 0 \bmod p$. Zbývající *druhý případ* FPV vylučuje řešení s právě jednou složkou dělitelnou p a je obtížnější. Uvádíme klasický výsledek o prvním případu.

Věta 53 (Germain, 1823). *Nechť $p > 2$ a q jsou prvočísla splňující dvě podmínky: (i) platí implikace*

$$x^p + y^p + z^p \equiv 0 \bmod q \implies xyz \equiv 0 \bmod q$$

a (ii) kongruence

$$x^p \equiv p \bmod q$$

nemá řešení x. Pak pro exponent p platí první případ FPV. To jest, neexistuje celočíselné řešení rovnice $x^p + y^p + z^p = 0$, které by mělo všechny složky nenulové modulo p.

Důkaz. Nechť čísla $x, y, z \in \mathbf{Z}$ jsou nenulová modulo p a splňují rovnici $x^p+y^p+z^p = 0$. Můžeme předpokládat, že jsou po dvou nesoudělná. Vezmeme prvočíslo q mající vlastnost (i) a odvodíme, že se porušuje (ii).

Nejdříve si uvědomíme, že v rovnosti $(-x)^p = (y+z)(z^{p-1} - z^{p-2}y + z^{p-3}y^2 - \cdots + y^{p-1})$ jsou oba faktory nesoudělné. (Dělilo-li by je nějaké prvočíslo r, měli bychom $y \equiv -z \bmod r$ a z druhého faktoru $py^{p-1} \equiv 0 \bmod r$. Tedy r dělí p nebo y. První nelze, protože pak by $r = p$ dělilo x. Ani druhé nelze, protože $(z, y) = 1$.) Takže, podle verze tvrzení 3, oba faktory jsou p-tými mocninami. Tutéž úvahu použijeme pro rovnice $(-y)^p = x^p + z^p$ a $(-z)^p = y^p + x^p$ a dostáváme existenci takových celých čísel a, b, c, α, β a γ, že

$$\begin{aligned}
y + z &= a^p \ , & y^{p-1} - y^{p-2}z + \cdots + z^{p-1} &= \alpha^p \ , & x &= -a\alpha \ , \\
x + z &= b^p \ , & z^{p-1} - z^{p-2}x + \cdots + x^{p-1} &= \beta^p \ , & y &= -b\beta \ , \\
x + y &= c^p \ , & x^{p-1} - x^{p-2}y + \cdots + y^{p-1} &= \gamma^p \ , & z &= -c\gamma \ .
\end{aligned}$$

Protože $x^p + y^p + z^p \equiv 0 \bmod q$ a platí (i), je některé z čísel x, y a z dělitelné q. Bez újmy na obecnosti to buď x. Pak

$$2x = b^p + c^p + (-a)^p \equiv 0 \bmod q$$

a opět podle (i) je některé z čísel a, b a c dělitelné q. Ani b ani c to být nemohou (podle hořejších rovnic by pak q dělilo y nebo z). Takže q dělí a. Pak ale hořejší rovnice dávají kongruence $y \equiv -z \bmod q$ a $\alpha^p \equiv py^{p-1} \equiv p\gamma^p \bmod q$. Protože q nedělí γ, existuje $g \in \mathbf{Z}$, že $g\gamma \equiv 1 \bmod q$. Pak ale $(\alpha g)^p \equiv p \bmod q$, ve sporu s (ii). $\diamondsuit$

Tvrzení 54 (použití věty Sofie Germainové). *Je-li $p > 2$ prvočíslo takové, že i $q = 2p + 1$ je prvočíslo, platí pro exponent p první případ FPV.*

Důkaz. Použijeme předešlou větu. Je-li $x \perp q$, platí podle malé Fermatovy věty z první kapitoly, že $x^{2p} = x^{q-1} \equiv 1 \bmod q$. Nutně $x^p \equiv \pm 1 \bmod q$. Takže podmínka (i) ve větě je splněna ($q > 3$). Je splněna i (ii), protože $x^p \equiv \pm 1 \not\equiv p = (q-1)/2 \bmod q$. $\diamondsuit$

Prvočísla p mající právě popsanou vlastnost se někdy nazývají *prvočísla Germainové*. Jejich řada začíná

$$3 \ , \ 5 \ , \ 11 \ , \ 23 \ , \ 29 \ , \ 41 \ , \ 53 \ , \ 83 \ , \ \ldots$$

Zda jich je nekonečně mnoho se neví. Větou Germainové se dá dokázat více (úloha 5).

3.2 Čtyři čtverce stačí

Metodu nekonečného sestupu použijeme nyní tvořivě pro důkaz existence řešení. Dokážeme, že každé přirozené číslo je součet čtyř čtverců.

Věta 55 (Lagrange, 1770). *Pro každé $n \in \mathbf{N}_0$ má diofantická rovnice*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

řešení $x_i \in \mathbf{N}_0$.

Lemma 56. *Pro každé prvočíslo $p > 2$ má kongruence*

$$a^2 + b^2 + 1 \equiv 0 \bmod p$$

řešení $a, b \in \mathbf{N}_0$, přičemž $0 \leq a, b < p/2$.

DŮKAZ. Čísla $0^2, 1^2, \ldots, ((p-1)/2))^2$ jsou vzájemně nekongruentní modulo p (proč?), totéž platí pro čísla $-1-0^2, -1-1^2, \ldots, -1-((p-1)/2)^2$. Dohromady jich je $p+1$ a některý zbytek se musí vyskytovat v obou množinách: $a^2 \equiv -1 - b^2 \bmod p$. $\diamondsuit$

DŮKAZ VĚTY 55. Začneme *Eulerovou identitou*. Nechť $x_1, \ldots, x_4$ a $y_1, \ldots, y_4$ jsou proměnné. Splňuje se tato pozoruhodná rovnost:

$$\begin{gathered}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ +(x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2 \ .\end{gathered}$$

Nahlédne se bezprostředním ověřením. Vlastnost „být součtem čtyř čtverců“ se zachovává součiny a stačí se omezit na prvočíselné $n = p$. Podle předešlého lemmatu existují celá čísla a, b a celé číslo $m, 0 < m < p$ tak, že

$$a^2 + b^2 + 1^2 + 0^2 = mp \tag{2}$$

(pro $p = 2$ vezmeme $a = 1, b = 0$ a platí to také).

Dokážeme implikaci

$$\begin{gathered} mp \text{ je součet 4 čtverců pro } 1 < m < p \\ \Downarrow \\ \exists\, n \in \mathbf{N}, n < m, \text{ a } np \text{ je součet 4 čtverců .}\end{gathered}$$

Vyjdeme z (2) a po implikacích sestoupíme až k $n = 1$. Potom $np = p$ je součtem 4 čtverců a věta je dokázána.

Zbývá dokázat implikaci. Nechť

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \ , \ 1 < m < p \ . \tag{3}$$

Čísla $y_i \in \mathbf{Z}$ definujeme pomocí vztahů

$$y_i \equiv x_i \bmod m \ , \ -\frac{m}{2} < y_i \leq \frac{m}{2} \ .$$

Jistě m dělí $y_1^2 + y_2^2 + y_3^2 + y_4^2$. Tedy

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = nm \ , \ 0 \leq n \leq m \ . \tag{4}$$

Nelze $n = 0$, pak každé $y_i = 0$ a m by dělilo každé x_i a tedy i p (viz (3)). Nelze ani $n = m$, pak by každé y_i muselo být $m/2$, odtud by plynulo $x_i^2 \equiv m^2/4 \bmod m^2$ (jak?) a opět by m dělilo p. Proto jsou v (4) obě nerovnosti ostré. Vynásobením obou vztahů dostaneme

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 = m^2 np \ , \tag{5}$$

kde $z_i \in \mathbf{Z}$ jsou vyjádřena pomocí x_i a y_i v Eulerově identitě. Z těchto vyjádření a z toho, že x_i a y_i jsou kongruentní modulo m plyne, že m dělí každé z_i. Po zkrácení m^2 v (5) dostáváme, že i np je součet 4 čtverců. Víme, že $0 < n < m$. Tím je dokázána implikace a věta 55. $\diamondsuit$

Tři čtverce nestačí, jak ukazují čísla typu $8n+7$. Rovnice $8n+7 = x_1^2+x_2^2+x_3^2$ nemá řešení $x_i \in \mathbf{Z}$ pro žádné $n \in \mathbf{N}_0$, protože modulo 8 jsou čtverce rovny jen $0, 1$ nebo 4. Reprezentací čísel dvěma čtverci jsme se dotkli ve větě 20, jsou jim věnovány úlohy 6 a 7.

3.3 Pelliána

neboli *Pellova rovnice* je diofantická rovnice

$$x^2 - dy^2 = 1 \ , \tag{6}$$

kde $d \in \mathbf{N}$ je parametr. Pro $d = e^2$ jde o nezajímavý problém, neboť pak $x^2 - dy^2 = (x - ey)(x + ey) = 1$ a $x = \pm 1, y = 0$. Proto dále předpokládáme, že d není čtverec. Vidíme, že (6) má vždy řešení $(\pm 1, 0)$. Je to *triviální řešení Pelliány*.

Pomocí Dirichletovy věty z první kapitoly nyní dokážeme, že vždy existuje netriviální řešení. Z tohoto faktu již snadno vyplyne nekonečnost množiny řešení a její struktura.

Věta 57 (Lagrange, 1770). *Každá Pellova rovnice $x^2 - dy^2 = 1$, $d \in \mathbf{N}$ a není čtverec, má netriviální celočíselné řešení.*

Důkaz. Podle věty 19 pro nekonečně mnoho zlomků $p/q \in \mathbf{Q}$ v základním tvaru platí

$$\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2} \; .$$

Pak je ale veličina $|p^2 - dq^2|$ omezená:

$$\begin{aligned} |p^2 - dq^2| &= |p - q\sqrt{d}| \cdot |p + q\sqrt{d}| < \frac{|p + q\sqrt{d}|}{q} \\ &\le \frac{p}{q} + \sqrt{d} < 2\sqrt{d} + 1 \; . \end{aligned}$$

Proto (holubníkový princip) existuje nekonečně mnoho dvojic $(p, q) \in \mathbf{N}^2$, $p \perp q$, takových, že $p^2 - dq^2$ je rovno pevné konstantě c. Mezi nimi najdeme jistě dvě dvojice (p_1, q_1) a (p_2, q_2) takové, že

$$p_1 \equiv p_2 \bmod |c| \quad \text{a} \quad q_1 \equiv q_2 \bmod |c| \; .$$

Položíme

$$\alpha = p_1 + q_1\sqrt{d} \quad \text{a} \quad \beta = p_2 + q_2\sqrt{d} \; .$$

Uvážíme číslo

$$\begin{aligned} \varepsilon &= \frac{\alpha}{\beta} = \frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}} = \frac{(p_1 + q_1\sqrt{d})(p_2 - q_2\sqrt{d})}{c} \\ &= \frac{p_1p_2 - q_1q_2d}{c} + \frac{q_1p_2 - p_1q_2}{c}\sqrt{d} \; . \end{aligned}$$

Oba poslední zlomky však jsou, vzhledem k volbě p_i a q_i, celá čísla. Tedy $\varepsilon = a + b\sqrt{d}$, kde $a, b \in \mathbf{Z}$. Jistě $b \neq 0$, protože p_1/q_1 a p_2/q_2 jsou různé zlomky v základním tvaru. Dále

$$a^2 - b^2d = (a + b\sqrt{d})(a - b\sqrt{d}) = \frac{(p_1 + q_1\sqrt{d})(p_1 - q_1\sqrt{d})}{(p_2 + q_2\sqrt{d})(p_2 - q_2\sqrt{d})} = \frac{c}{c} = 1 \; .$$

Máme netriviální řešení (a, b). ◊

Jsou-li $a_1, b_1 \in \mathbf{N}$ a $a_2, b_2 \in \mathbf{N}$ dvě řešení (6) a $a_1 < a_2$, platí i $b_1 < b_2$. Proto lze definovat *minimální řešení* jako řešení z $\mathbf{N}$ s nejmenšími složkami. Označíme ho a_d^*, b_d^* a položíme $\varepsilon_d = a_d^* + b_d^*\sqrt{d}$. Dává předchozí důkaz efektivní odhad a_d^* a b_d^*? (úloha 8)

Uvažme nyní netriviální celočíselná řešení $a, b \in \mathbf{Z}$. Povšimněme si, že z $a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d}) = 1$ plyne, že reálná čísla $a + b\sqrt{d}$ a $a - b\sqrt{d}$ mají totéž znaménko a číslo 1 nebo -1 je odděluje. Rozklad množiny

$$R = \{a + b\sqrt{d} : \ a, b \in \mathbf{Z} \ \& \ a^2 - db^2 = 1\}$$

(pomineme na chvíli prvky -1 a 1) na čtyři podmnožiny podle intervalů $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$ a $(1, \infty)$ tedy souhlasí s rozkladem podle znamének složek $ab = --$, $-+$, $+-$ a $++$. Ekvivalentní a vhodnější definice ε_d je tedy ta, že to je nejmenší prvek množiny $R \cap (1, \infty)$. Vezmeme horní polovinu řešení $U = R \cap (0, \infty)$,

$$\begin{aligned} U &= \{a + b\sqrt{d} : \ a \in \mathbf{N} \ \& \ b \in \mathbf{Z} \ \& \ a^2 - db^2 = 1\} \\ &= \{a + b\sqrt{d} > 0 : \ a, b \in \mathbf{Z} \ \& \ a^2 - db^2 = 1\} \ . \end{aligned}$$

Tvrzení 58 (struktura řešení Pelliány). $(U, \cdot)$ *je nekonečná multiplikativní cyklická grupa s generátorem* $\varepsilon_d = a_d^* + b_d^*\sqrt{d}$. *Zobrazení* $\varepsilon_d^m \to m$ *je izomorfismus grup* $(U, \cdot)$ *a* $(\mathbf{Z}, +)$. *Grupa všech řešení* $(R, \cdot)$ *je izomorfní součinu grup* $(\mathbf{Z}, +) \times (\mathbf{Z}_2, +)$.

Důkaz. Pokud $a_i + b_i\sqrt{d} \in U$, $i = 1, 2$, padne do U i $a + b\sqrt{d} = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})$, protože $a + b\sqrt{d} > 0$ a

$$a^2 - db^2 = (a_1 + b_1\sqrt{d})(a_1 - b_1\sqrt{d})(a_2 + b_2\sqrt{d})(a_2 - b_2\sqrt{d}) = 1 \cdot 1 = 1 \ .$$

U je uzavřená i na dělení — $(a_1 + b_1\sqrt{d})^{-1} = a_1 - b_1\sqrt{d}$. Vzhledem k $\cdot$ tedy U tvoří grupu.

Z věty 57 a grupovosti U plyne, že U je nekonečná. Nechť $\alpha \in U$, $\alpha > 1$ (pro $\alpha < 1$ přejdeme k $1/\alpha$). Vezmeme největší $n \in \mathbf{N}_0$, že $\varepsilon_d^n \leq \alpha$. Kdyby platila ostrá nerovnost, dostali bychom $\alpha/\varepsilon_d^n \in U$ a $1 < \alpha/\varepsilon_d^n < \varepsilon_d$, spor s definicí ε_d. Takže $\varepsilon_d^n = \alpha$. $(U, \cdot)$ je proto cyklická, generovaná ε_d. Poznámka o izomorfismu je jasná. Rovněž je jasné, že $(R, \cdot)$ je grupa izomorfní součinu $(\mathbf{Z}, +)$ a cyklické dvojgrupy. ◊

Jako příklad si vezmeme Pelliánu

$$x^2 - 2y^2 = 1 \ .$$

Generátor se zde nalezne snadno: $\varepsilon_2 = 3 + 2\sqrt{2}$. Umocňováním ε_2 dostáváme postupně další řešení,

$$\begin{aligned}
(3+2\sqrt{2})^2 &= 17 + 12\sqrt{2} \\
(3+2\sqrt{2})^3 &= 99 + 70\sqrt{2} \\
(3+2\sqrt{2})^4 &= 577 + 408\sqrt{2} \\
&\vdots
\end{aligned}$$

O minimálních řešeních dá představu tabulka $(\mathbf{d}, a_d^*, b_d^*)$ pro $d \leq 30$:

$(\mathbf{2}, 3, 2)$	$(\mathbf{3}, 2, 1)$	$(\mathbf{5}, 9, 4)$	$(\mathbf{6}, 5, 2)$	$(\mathbf{7}, 8, 3)$
$(\mathbf{8}, 3, 1)$	$(\mathbf{10}, 19, 6)$	$(\mathbf{11}, 10, 3)$	$(\mathbf{12}, 7, 2)$	$(\mathbf{13}, 649, 180)$
$(\mathbf{14}, 15, 4)$	$(\mathbf{15}, 4, 1)$	$(\mathbf{17}, 33, 8)$	$(\mathbf{18}, 17, 4)$	$(\mathbf{19}, 170, 39)$
$(\mathbf{20}, 9, 2)$	$(\mathbf{21}, 55, 12)$	$(\mathbf{22}, 197, 42)$	$(\mathbf{23}, 24, 5)$	$(\mathbf{24}, 5, 1)$
$(\mathbf{26}, 51, 10)$	$(\mathbf{27}, 26, 5)$	$(\mathbf{28}, 127, 24)$	$(\mathbf{29}, 9801, 1820)$	$(\mathbf{30}, 11, 2)$.

Tvrzení 59 (zobecněná Pelliána). *Nechť $d \in \mathbf{N}$ není čtverec. Má-li diofantická rovnice*

$$x^2 - dy^2 = m$$

(d a $m \in \mathbf{Z}$ jsou parametry) řešení $x, y \in \mathbf{N}$, má nekonečně mnoho řešení.

Důkaz. Nechť $(a, b) \in \mathbf{N}^2$ je její řešení, $(a_n, b_n) \in \mathbf{N}^2, n \in \mathbf{N}$, buďte nekonečně mnoho řešení Pelliány $x^2 - dy^2 = 1$. Pak

$$c_n + d_n\sqrt{d} = (a + b\sqrt{d})(a_n + b_n\sqrt{d})$$

dává nekonečně mnoho řešení $(c_n, d_n) \in \mathbf{N}^2$ zobecněné Pelliány, protože

$$\begin{aligned}
c_n^2 - dd_n^2 &= (c_n + d_n\sqrt{d})(c_n - d_n\sqrt{d}) \\
&= (a + b\sqrt{d})(a - b\sqrt{d})(a_n + b_n\sqrt{d})(a_n - b_n\sqrt{d}) \\
&= m \cdot 1 = m \ .
\end{aligned}$$

$\diamondsuit$

Jednu třídu zobecněných Pellián s pravou stranou -1 a nekonečně mnoha řešeními popisuje úloha 9.

Důležitost Pellovy rovnice spočívá ve skutečnosti, že se některé složitější diofantické problémy dají na ni převést. Uvádíme dva příklady této metody. V prvním nám Pelliána $x^2 - 5y^2 = 1$ poskytne nekonečně mnoho řešení rovnice $x^3 + y^3 + x^3 + w^3 = 2$. V druhém analýzou řešení Pelliány $x^2 - 3y^2 = 1$ dokážeme, že $x^2 - y^3 = 1$ nemá jiná řešení kromě triviálních.

Tvrzení 60 (čtyři třetí mocniny). *Diofantická rovnice*

$$x^3 + y^3 + z^3 + w^3 = 2 \tag{7}$$

má nekonečně mnoho řešení.

Důkaz. Vyjdeme z rovnosti

$$1^3 + 9^3 + 10^3 + (-12)^3 = 2 \ .$$

Řešení rovnice (7) budeme hledat ve tvaru

$$x = 1 + X \ , \ y = 9 - X \ , \ z = 10 + Y \ , \ w = -12 - Y \ .$$

Dosazením do (7) a zjednodušením získáme

$$10X^2 - 80X - 2Y^2 - 44Y = 0 \ ,$$

což se dá dále zjednodušit na

$$(Y + 11)^2 - 5(X - 4)^2 = 41 \ .$$

Úlohu jsme převedli na zobecněnou Pelliánu

$$A^2 - 5B^2 = 41 \ . \tag{8}$$

Nabíledni je netriviální řešení $(11, 4)$ odpovídající výchozí rovnosti. Další řešení z něj získáme vynásobením mocninami ε_5. Víme, že $\varepsilon_5 = 9 + 4\sqrt{5}$. Další řešení (8) jsou tedy například $(179, 80)$ a $(3211, 1436)$. Ta nám pro (7) dají řešení

$$(85, -75, 178, -180) \ \text{ a } \ (1441, -1431, 3210, -3212) \ .$$

Takto generujeme nekonečně mnoho celočíselných čtveřic splňujících (7). ◇

Tvrzení 61 (čtverec a kub). *Diofantická rovnice*

$$x^2 - y^3 = 1$$

má jen pět řešení: $(\pm 1, 0), (0, -1)$ *a* $(\pm 3, 2)$.

Pomohou nám čtyři lemmata, poslední dvě jsou sama zajímavými diofantickými výsledky.

Lemma 62. *Splňují-li čísla* $x, y \in \mathbf{N}$ *vztah* $2x^2 - y^2 = 1$*, existují čísla* $a, b \in \mathbf{N}_0$ *splňující vztahy* $a^2 - 2b^2 = 1$ *a* $x = a^2 \pm 2ab + 2b^2$.

DŮKAZ. Nechť $x, y \in \mathbf{N}$ splňují $2x^2 - y^2 = 1$. Zřejmě $y = 2z + 1, z \in \mathbf{N}_0$, a tedy $x^2 = (1 + y^2)/2 = z^2 + (z + 1)^2$. Podle tvrzení 48 se najdou $u, v \in \mathbf{N}_0$ taková, že $x = u^2 + v^2$ a (i) $z = 2uv$ & $z + 1 = u^2 - v^2$ nebo (ii) $z = u^2 - v^2$ & $z + 1 = 2uv$. V prvém případě $1 = u^2 - v^2 - 2uv = (u - v)^2 - 2v^2$ a v druhém $1 = 2uv - u^2 + v^2 = (u + v)^2 - 2u^2$. Nyní stačí položit $a = u - v$ & $b = v$ nebo $a = u + v$ & $b = u$ a vyjádřit x pomocí a a b. ♢

Lemma 63. *Všechna nezáporná řešení Pelliány* $x^2 - 3y^2 = 1$ *jsou obsažena v posloupnosti* $(x_n, y_n) \in \mathbf{N}_0^2, n \in \mathbf{N}_0$*, která je dána rekurencí* $(x_0, y_0) = (1, 0)$,

$$x_{n+1} = 2x_n + 3y_n \quad a \quad y_{n+1} = x_n + 2y_n \ . \tag{9}$$

Tato řešení navíc splňují vztahy

$$x_{2n+1} = (y_n + y_{n+1})^2 + 1 \ , \ y_{2n+1} = 2x_n y_{n+1} - 1 \tag{10}$$

a

$$x_{2n} = 2x_n^2 - 1 \ , \ y_{2n} = 2x_n y_n \ . \tag{11}$$

Číslo x_n *je sudé, právě když je* n *liché a* y_n *je sudé, právě když je* n *sudé.*

DŮKAZ. Jak víme z tvrzení 58, všechna nezáporná řešení jsou dána rovnostmi $x_n + y_n\sqrt{3} = \varepsilon_3^n = (2 + \sqrt{3})^n, \ n \in \mathbf{N}_0$. Rekurence (9) je pouze do složek rozepsaná rekurence

$$x_{n+1} + y_{n+1}\sqrt{3} = (2 + \sqrt{3})(x_n + y_n\sqrt{3}) \ .$$

Vztahy (10) a (11) se dokážou přímočarou indukcí podle n. Protože $(x_0, y_0) = (1, 0)$ a $(x_1, y_1) = (2, 1)$, na začátku platí. Pro $n \geq 0$ máme, podle indukčního předpokladu (11), $x_{2n+1} = 2x_{2n} + 3y_{2n} = 4x_n^2 - 2 + 6x_n y_n$. Což je totéž (neboť $3 = 3x_n^2 - 9y_n^2$) jako $x_n^2 + 9y_n^2 + 6x_n y_n + 1 = (x_n + 2y_n + y_n)^2 + 1 = (y_{n+1} + y_n)^2 + 1$. Tím je dokázána první formule v (10). Zbylé tři formule se dokazují obdobně a jejich důkazy proto pomineme. Tvrzení o paritě plyne lehce ze vztahů (10) a (11). $\diamondsuit$

Lemma 64. *Diofantická rovnice* $x^4 - 2y^2 = 1$ *má jen triviální řešení* $(\pm 1, 0)$.

DŮKAZ. Nechť $x, y \in \mathbf{N}_0$ splňují $x^4 - 2y^2 = 1$. Protože je x liché, můžeme psát $x^2 = 8k + 1$ a substitucí dostáváme $(x^2 - 1)(x^2 + 1)/2 = 8k(4k + 1) = y^2$. Z $(8k, 4k + 1) = 1$ plyne (tvrzení 3), že $8k = a^2$, a tak $1 = 8k + 1 - a^2 = x^2 - a^2 = (x - a)(x + a)$. Nutně $x = \pm 1$. $\diamondsuit$

Lemma 65. *Diofantická rovnice* $x^4 - 3y^2 = 1$ *má jen triviální řešení* $(\pm 1, 0)$.

DŮKAZ. Nechť (x_n, y_n) je posloupnost z lemmatu 63. Pro nějaké $n \in \mathbf{N}_0$ platí $x_n = x^2$, kde $x \in \mathbf{N}_0$. Rozlišíme dva případy podle parity n. Pro $n = 2m + 1$ použijeme (10) a dostaneme $x^2 = x_n = x_{2m+1} = \Box + 1$. Z $x^2 - \Box = 1$ ovšem plyne hned $x = \pm 1$.

Pro $n = 2m$ použijeme (11): $x^2 = x_n = x_{2m} = 2x_m^2 - 1$. Z $2x_m^2 - x^2 = 1$ plyne (modul 4), že x_m je liché. Podle lemmatu 63, $m = 2p$. Podle lemmatu 62 a (11) máme $a^2 + 2b^2 \pm 2ab = x_m = x_{2p} = 2x_p^2 - 1$, kde $a, b \in \mathbf{N}_0$ splňují rovnici $a^2 - 2b^2 = 1$. Takže

$$2x_p^2 - 1 = a^2 + 2b^2 \pm 2ab = 2a^2 - 1 \pm 2ab$$

a $x_p^2 = a(a \pm b)$. Protože $a \perp b$, je i $(a, a \pm b) = 1$ a a je čtverec. To podle lemmatu 64 nastává jen pro $a = 1$. Proto $b = 0$, $x_n = x_m = x_p = 1$ a opět $x = \pm 1$. $\diamondsuit$

DŮKAZ TVRZENÍ 61. Nechť $x, y \in \mathbf{Z}$ a $x^2 - y^3 = 1$. Můžeme předpokládat, že $x \in \mathbf{N}_0$. Z faktorizace

$$x^2 = y^3 + 1 = (y + 1)(y^2 - y + 1) = (y + 1)((y + 1)(y - 2) + 3)$$

vyplývá, že $(y + 1, y^2 - y + 1) = 1$ nebo 3. V prvním případě je $y^2 - y + 1 = b^2$ čtverec a máme $(2b)^2 - (2y - 1)^2 = 3$. Ergo $(2b - 2y + 1)(2b + 2y - 1) = 3$ a $b = \pm 1$ a $y = 1, 0$. Ale $y = 1$ nedává řešení původní rovnice a $y = 0$ dává triválnί řešení $(\pm 1, 0)$.

Zajímavější a těžší je případ, kdy největší společný dělitel $y+1$ a y^2-y+1 je 3. Pak $y+1 = 3a^2$ a $y^2-y+1 = 3b^2$, kde $a, b \in \mathbf{N}_0$. Poslední vztah přepíšeme na $3(2b)^2 - (2y-1)^2 = 3$ a vidíme, že $3\backslash(2y-1)$. Čísla X a Y daná vztahy $2y-1 = 3Y$ a $2b = X$ splňují rovnice

$$X^2 - 3Y^2 = 1 \text{ a } Y = 2a^2 - 1 \ .$$

$Y = -1$ ($a = 0$, $X = 2$ a $b = 1$) vyhovuje a dostáváme řešení $(0, -1)$ původní rovnice. V dalším můžeme předpokládat, že $Y \in \mathbf{N}_0$.

Podle lemmatu 63 máme taková $a, n \in \mathbf{N}_0$, že $Y = y_n = 2a^2 - 1$. Protože je y_n liché, je liché i $n = 2m + 1$ a $m \in \mathbf{N}_0$. Díky (10) $y_n = y_{2m+1} = 2x_m y_{m+1} - 1 = 2a^2 - 1$ a

$$a^2 = x_m y_{m+1} \ .$$

Platí $(x_m, y_{m+1}) = (x_m, x_m + 2y_m) = 1$ nebo 2.

Opět máme dvě možnosti. Pokud $x_m \perp y_{m+1}$, je x_m čtverec a podle lemmatu 65 je $x_m = 1$. Takže $m = 0$, $n = 1$ a $Y = y_1 = 1$. Tedy $y = 2$ a máme řešení $(\pm 3, 2)$ původní rovnice.

Konečně, nechť $(x_m, y_{m+1}) = 2$. Máme $y_{m+1} = 2c^2$. Vidíme, že $m + 1 = 2k, k \in \mathbf{N}$. Podle (11) $2c^2 = y_{m+1} = y_{2k} = 2x_k y_k$ a $c^2 = x_k y_k$. Protože $x_k \perp y_k$, je x_k čtverec. Podle lemmatu 65 $x_k = 1$ a $k = 0$. Nyní ale $k > 0$, a tak dostáváme spor. Tímto jsou všechna řešení diofantické rovnice $x^2 - y^3 = 1$ nalezena. $\diamondsuit$

Další výsledky související s tvrzením 61 jsou obsaženy v úlohách 10 až 14. Posloupnost řešení Pelliány a vztahy mezi jejími členy — jako jsou například (10) a (11) — jsou základní technikou v důkazu Matijasevičovy věty a nadlouho se s nimi neloučíme.

3.4 Thueho rovnice

Uvidíme, jak z Thueho věty 42 (kapitola 2) plyne výsledek o rozsáhlé třídě diofantických rovnic.

Polynom o několika proměnných je *forma*, je-li homogení, to jest monomy mají týž stupeň. *Binární forma* stupně n je polynom o dvou proměnných

$$F(x, y) = a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \cdots + a_{n-1} x y^{n-1} + a_n y^n \ .$$

Thueho rovnice je diofantická rovnice tvaru

$$F(x, y) = m \ , \tag{12}$$

kde $F(x,y) \in \mathbf{Z}[x,y]$ je binární forma a $m \in \mathbf{Z}$.

Věta 66 (Thue, 1909). *Každá Thueho rovnice, v níž (i) stupeň $F(x,y)$ je alespoň 3 a (ii) $F(x,y)$ je ireducibilní nad $\mathbf{Q}[x,y]$ (viz úloha 16), má jen konečně mnoho řešení.*

Důkaz. Forma v (12) je zhomogenizovaný celočíselný polynom o jedné proměnné

$$P(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_{n-1} z + a_n \ ,$$

protože

$$F(x,y) = y^n P(x/y) \ .$$

Z ireducibility $F(x,y)$ plyne ireducibilita $P(z)$ (a naopak) a proto jsou všechny kořeny $P(z)$ vzájemně různé a $P(z)$ je po vydělení a_0 jejich minimální polynom. Všechny kořeny tedy mají stupeň $n \geq 3$. Označíme je jako $\alpha_1, \ldots, \alpha_n$.

Mějme nekonečně mnoho řešení $(p,q) \in \mathbf{Z}^2$ rovnice (12). Každé p i q se opakuje nejvýše n krát. Můžeme také předpokládat, že vždy $q \neq 0$. Dosadíme p a q do (12) a rovnici přepíšeme pomocí faktorizace $P(z)$ jako

$$\left(\frac{p}{q} - \alpha_1\right)\left(\frac{p}{q} - \alpha_2\right)\cdots\left(\frac{p}{q} - \alpha_n\right) = \frac{m}{a_0 q^n} \ . \tag{13}$$

Jako v označíme minimum vzdáleností kořenů,

$$v = \min\left\{|\alpha_i - \alpha_j| :\ i \neq j\right\} > 0 \ .$$

Pro velké $|q|$ je absolutní hodnota pravé strany (13) menší než $(v/2)^n$, a proto pro některé i musí platit

$$\left|\alpha_i - \frac{p}{q}\right| < \frac{v}{2} \ .$$

Pak ovšem pro $j \neq i$ máme $|\alpha_j - p/q| \geq v/2$ a z (13) plyne, že dokonce

$$\left|\alpha_i - \frac{p}{q}\right| < \frac{m 2^{n-1}}{a_0 v^{n-1} q^n} \ll_{F,m} \frac{1}{q^n} \ . \tag{14}$$

Můžeme předpokládat (holubníkový princip), že pro jedno pevné i máme nekonečně mnoho dvojic $(p,q) \in \mathbf{Z}^2$ splňujících (14). Můžeme předpokládat, že $p/q \in \mathbf{Q}$. Nutně $\alpha_i \in \mathbf{R}$, jinak dostáváme pro $q \to \infty$ spor. Sporu se ale ani tak nevyhneme. Platnost (14) pro nekonečně mnoho zlomků $p/q \in \mathbf{Q}$ protiřečí větě 42, protože $\alpha_i \in \mathbf{R}$ je algebraické číslo stupně $n \geq 3$. Nekonečnost počtu řešení Thueho rovnice vede za uvedených předpokladů ke sporu. $\diamondsuit$

Proto má diofantická rovnice

$$x^3 - 2y^3 = 1$$

a jí podobné, narozdíl od $x^2 - 2y^2 = 1$, jen konečně mnoho řešení. Nedostatkem Thueho věty je neefektivnost způsobená neefektivností důkazu věty 42. Víme, že řešení je jen konečně mnoho, ale nemáme algoritmus, který by je nalezl, nebo alespoň rozhodl, zda nějaké řešení vůbec existuje.

3.5 Desátý Hilbertův problém

Věnováno památce Osvalda Demutha (1936–1988)

V tomto oddílu dokážeme Matijasevičovu větu (větu 83), která říká následující. Neexistuje algoritmus, jehož vstupy by byly celočíselné polynomy a který by se pro každý vstupní polynom $P(x_1, \ldots, x_m)$ zastavil po konečném výpočtu ve stavu ANO nebo ve stavu NE, přičemž ANO by znamenalo, že $P = 0$ má celočíselné řešení, a NE by znamenalo, že takové řešení není. Stručně řečeno, řešitelnost diofantických rovnic je algoritmicky nerozhodnutelná úloha. (V poznámce za větou 83 uvidíme, že se dokáže více.)

Matijasevičova věta je zápornou odpovědí na otázku, již položil o sedmdesát let dříve Hilbert. Náleží mezi hlavní výsledky matematiky 20. století. Pro její důkaz je zapotřebí vybudovat malou teorii. Čtenář, který se s ním chce seznámit, se musí obrnit určitou trpělivostí. Pro přehlednost jsme oddíl 3.5 rozdělili na pododdíly odpovídající jednotlivým fázím důkazu.

V 3.5.1 zavedeme základní pojmy, zejména diofantičnost relací, funkcí a formulí. V 3.5.2 dokážeme pozoruhodnou věc: exponenciální funkce x^y je diofantická a stejně tak i faktoriál a binomické koeficienty. Z toho v 3.5.3 odvodíme, že formule budované z diofantických formulí pomocí omezeného obecného kvantifikátoru jsou opět diofantické. V 3.5.4 připomeneme definici rekurzivních funkcí a dokážeme, že každá rekurzivní funkce je diofantická. Pak odvodíme univerzální diofantickou relaci, jejíž existence má některé paradoxní projevy, a dokážeme Matijasevičovu větu.

Dosud jsme se zabývali celočíselnými řešeními diofantických rovnic. Pro důkaz Matijasevičovy věty je jedno, zda řešení hledáme v $\mathbf{Z}$ nebo v $\mathbf{N}_0$. Ukážeme to dvěma jednoduchými redukcemi. Řekněme, že vždy umíme rozhodnout existenci řešení v $\mathbf{N}_0$. Rovnice $P(x_1, \ldots, x_m) = 0$ má celočíselné řešení, právě když

$$\prod_{\pm} P(\pm x_1, \ldots, \pm x_m) = 0$$

(násobíme přes všech 2^m voleb znamének) má nezáporné řešení. Jsme tedy vševědoucí i v oboru $\mathbf{Z}$. Nechť naopak vždy umíme rozhodnout existenci řešení v $\mathbf{Z}$. Rovnice $P(x_1, \ldots, x_m) = 0$ má nezáporné řešení, právě když

$$P(x_{1,1}^2 + x_{1,2}^2 + x_{1,3}^2 + x_{1,4}^2, \ldots, x_{m,1}^2 + x_{m,2}^2 + x_{m,3}^2 + x_{m,4}^2) = 0$$

($4m$ neznámých) má celočíselné řešení. To plyne z věty 55. Jsme tedy vševědoucí i v oboru $\mathbf{N}_0$. V dalších úvahách se proto bez újmy na obecnosti omezujeme na řešení ležící v $\mathbf{N}_0$.

3.5.1 Diofantičnost

Není-li výslovně stanoveno jinak, je oborem proměnných, parametrů a neznámých množina $\mathbf{N}_0$. Rovněž všechny funkce mají hodnoty v $\mathbf{N}_0$. Ne vždy tuto konvenci důsledně dodržíme, vždy ale bude jasné, jak formule modifikovat, abychom nedostali mezivýsledek mimo $\mathbf{N}_0$. Například rovnice $P = 0$ s celočíselným polynomem P se dá přepsat jako $R = S$, kde polynomy R a S mají koeficienty z $\mathbf{N}_0$.

Relací, přesněji řečeno n-ární relací, rozumíme množinu n-tic R, $R \subset \mathbf{N}_0^n$. Místo $(a_1, \ldots, a_n) \in R$ budeme psát $R(a_1, \ldots, a_n)$. Unárním relacím budeme říkat prostě *množiny*. *Funkci* $f : \mathbf{N}_0^n \to \mathbf{N}_0$ chápeme jako její graf

$$\{(a_1, a_2, \ldots, a_n, b) \in \mathbf{N}_0^{n+1} : \ f(a_1, a_2, \ldots, a_n) = b\} ,$$

který je $(n+1)$-ární relací.

Řekneme, že relace R je *diofantická*, existuje-li celočíselný polynom $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$ takový, že pro všechny n-tice $(a_1, \ldots, a_n) \in \mathbf{N}_0^n$ platí ekvivalence

$$R(a_1, \ldots, a_n) \iff \exists\, y_1, \ldots, y_m \,[P(a_1, \ldots, a_n, y_1, \ldots, y_m) = 0] .$$

(Pro přehlednost budeme formule, na něž se vztahuje kvantifikace, psát do hranatých závorek.) Řekneme, že P *reprezentuje* R. Proměnné x_i jsou *parametry* a proměnné y_i *neznámé*. Množina nebo funkce je diofantická, je-li odpovídající relace diofantická. Někdy lze diofantičnost dokázat snadno (úloha 18), jindy to je daleko obtížnější.

Budeme pracovat s relacemi popsanými formulemi predikátové logiky prvního řádu. Stručně zopakujeme její základy Je důležité jasně rozlišovat dvě strany věci: syntaktickou (formule jako formální slova nad jistou abecedou) a sémantickou (realizace funkcí, predikátů a formulí relacemi, to jest podmnožinami $\mathbf{N}_0^n$).

Formule jsou slova nad abecedou obsahující symboly konstant (pro každý prvek $\mathbf{N}_0$), symboly proměnných $(x, y, z, \ldots)$, funkční symboly $(f, x^y, +, \ldots)$, predikátové symboly $(p, <, \backslash, \ldots)$, symboly logických spojek (budeme používat jen konjunkci „a zároveň" $\&$ a disjunkci „nebo" $\vee$), kvantifikátorů („existuje" $\exists$ a „pro všechny" $\forall$) a pomocné symboly (hlavně závorky $[, (,),]$, oddělovací znaménka jako čárky apod.). Konkrétní seznam funkčních a predikátových symbolů, z nichž vybudujeme vše ostatní, uvedeme v závěru pododdílu.

Každý funkční a predikátový symbol má svou *aritu* (počet argumentů), což je přirozené číslo. Nejčastěji se objevují *binární* funkce a predikáty s aritou 2. Formule se budují z atomických formulí a ty z termů. Termy se budují z proměnných, konstant a funkcí.

Term vznikne opakovanou aplikací symbolů funkcí na konstanty, proměnné a již vytvořené termy. Příklad termu:

$$f(y + f(x)) + f(1) \ ,$$

kde 1 je konstanta, x a y jsou proměnné, f je unární a $+$ binární funkční symbol. Předpokládáme, že každému symbolu pro konstantu, funkci a predikát odpovídá obvyklá realizace relací. „Obvyklá" znamená, že symbol konstanty „6" je realizován jako prvek $6 \in \mathbf{N}_0$, funkční symbol $+$ jako ternární relace, která je grafem obvyklého sčítání v $\mathbf{N}_0$, predikátový symbol $<$ jako množina těch dvojic (a, b) z $\mathbf{N}_0^2$, že a je menší než b atd. Predikátový nebo funkční symbol je *diofantický*, je-li jej realizující relace diofantická. Symboly konstant jsou triviálně diofantické.

Každý term obsahující n proměnných je pak realizován n-ární funkcí, podmnožinou $\mathbf{N}_0^{n+1}$. Je-li diofantická, máme *diofantický term.* Například realizace termu

$$(x + 1)^2$$

sestaveného z konstanty 1, proměnné x, unárního funkčního symbolu $(\cdot)^2$ a binárního funkčního symbolu $+$ je (diofantická) relace

$$\{(n, n^2+2n+1) \in \mathbf{N}_0^2 : \ n \in \mathbf{N}_0\} \ .$$

Atomická formule vznikne aplikací symbolu predikátu na termy. Například

$$x + y \equiv f(a) \bmod z + 3$$

je atomická formule aplikující ternární predikát $\cdot \equiv \cdot \bmod \cdot$ na termy $x+y$, $f(a)$ a $z+3$. *Formule* se dostane z atomických formulí a již vytvořených formulí užitím logických spojek, kvantifikátorů a závorek. Každá atomická formule je tedy formule. Příklad formule:

$$\exists\, x\; \forall\, z\; [x < y \;\&\; z^2 \backslash a] \vee b = a \ .$$

Je to disjunkce dvou formulí, z nichž druhá je atomická a první je kvantifikovaná konjunkce dvou atomických formulí. Obsahuje tři nekvantifikované proměnné a, b a y. Definuje ternární relaci

$$\{(a,b,y) \in \mathbf{N}_0^3 : \ a = b \text{ nebo } (a = 0 \;\&\; y > 0)\} \ .$$

Spoustu dalších příkladů formulí uvidíme později

Vázaný výskyt proměnné x ve formuli φ je kvantifikovaný výskyt x, což znamená, že se x objevuje v podformuli $\exists\, x\, [\ldots]$ nebo $\forall\, x\, [\ldots]$. Nahrazením všech výskytů x v této podformuli zcela novou proměnnou se její význam nezmění. Můžeme tak dosáhnout toho, že každá proměnná vyskytující se ve φ tam má jen vázané nebo jen *volné* (nekvantifikované) výskyty. Proměnným druhého typu se říká *volné proměnné* formule φ.

Termy jsou realizovány funkcemi. Predikátové symboly arity n realizují n-ární relace. Významům logických spojek a kvantifikátorů rozumíme. Víme tedy, co znamená, že daná formule bez volných proměnných „platí". Formule $\varphi(a_1, \ldots, a_n)$ s n volnými proměnnými a_i se nazývá *diofantickou formulí*, pokud jí definovaná n-ární relace

$$\{(a_1, \ldots, a_n) \in \mathbf{N}_0^n : \ \varphi(a_1, \ldots, a_n) \text{ platí}\}$$

je diofantická. Například atomická formule $y = t$, kde y je proměnná, t je term a y se nevyskytuje v t, je podle našich definic diofantická, právě když je t diofantický term. Nebo atomická formule $p(x_1, \ldots, x_n)$, kde p je n-ární predikátový symbol, je diofantická, právě když p je diofantický predikát.

Jsou-li proměnné $x_1, \dots, x_n$ volné ve formuli φ a $t_1, \dots, t_n$ jsou termy neobsahující žádnou z proměnných, volných nebo vázaných, vyskytujících se v φ, řekneme, že tyto termy jsou *substituovatelné* (za proměnné $x_1, \dots, x_n$ do φ).

Tvrzení 67 (Diofantičnost $\exists$, & , $\vee$ a substituce).

1. *Je-li φ diofantická formule a x proměnná volná ve φ, je formule $\exists x\, [\varphi]$ též diofantická.*

2. *Jsou-li φ_1 a φ_2 diofantické formule, jsou i formule $\varphi_1 \,\&\, \varphi_2$ a $\varphi_1 \vee \varphi_2$ diofantické.*

3. *Jsou-li proměnné $x_1, \dots, x_n$ volné v diofantické formuli φ a a $t_1, \dots, t_n$ jsou substituovatelné diofantické termy, je formule vzniklá z φ náhradou každého výskytu x_i termem t_i rovněž diofantická.*

Důkaz. **1.** Reprezentující polynom zůstává týž, přidání existenčního kvantifikátoru pouze přesune parametr x mezi neznámé.

2. Nechť φ_1 má volné proměnné $a_1, \dots, a_k$ a φ_2 má volné proměnné $b_1, \dots, b_l$, přičemž oba seznamy mohou mít libovolný průnik. Nechť $P(a_1, \dots, a_k, y_1, \dots, y_m)$ a $Q(b_1, \dots, b_l, y_1, \dots, y_n)$ jsou polynomy reprezentující příslušné relace. Pak polynom

$$P(a_1, \dots, a_k, y_1, \dots, y_m)^2 + Q(b_1, \dots, b_l, z_1, \dots, z_n)^2$$

s $\leq k + l$ parametry $a_1, \dots, b_l$ a $m + n$ neznámými $y_1, \dots, z_n$ reprezentuje relaci definovanou konjunkcí $\varphi_1 \,\&\, \varphi_2$. Za povšimnutí stojí, že jsme museli přejmenovat neznámé v Q. Podobně součin PQ reprezentuje relaci definovanou disjunkcí $\varphi_1 \vee \varphi_2$. (Nyní není třeba neznámé přejmenovávat.)

3. Relace definovaná novou formulí je definována i formulí

$$\exists x_1, \dots, x_n\, [\varphi \,\&\, x_1 = t_1 \,\&\, \dots \,\&\, x_n = t_n] \ ,$$

která je diofantická díky předpokladům a výsledkům 1 a 2. $\diamondsuit$

Pro shodné seznamy volných proměnných φ_1 a φ_2 v bodu 2 dostáváme, že průnik a sjednocení diofantických relací se stejnou aritou je diofantická relace. Výsledek o formulích je mírně obecnější. Negace, implikace a obecný kvantifikátor $\forall$ diofantičnost formulí nezachovávají (úloha 20).

Pomocí &, $\vee$, $\exists$ a substituce budujeme diofantické formule a definujeme diofantické relace. Je však třeba mít k dispozici výchozí diofantické funkce a predikáty. Uvedeme seznam takových „elementárních" funkčních a predikátových symbolů a ukážeme, že jsou diofantické. Všechny následující diofantické formule budou vybudovány víceméně explicitně pouze z nich. Budeme samozřejmě užívat běžné konvence, jako je třeba vynechávání $\cdot$ při násobení, psaní „zkratky" x^3 místo $(x \cdot x) \cdot x$ atd., ale vždy bude jasné, že se definice dá rozvinout až do úrovně uvedených elementárních symbolů.

Funkční symboly: základní aritmetické operace $+$, $-$, $\cdot$, funkce $\mathrm{zby}(a, b)$ zbytku při dělení a číslem b se zbytkem a funkce $\mathrm{pod}(a, b)$ podílu při dělení a číslem b se zbytkem. Predikátové symboly: $=$, $\neq$, $<$, $>$, $\leq$, $\geq$, $\backslash$, $\equiv \mod$, $\perp$.

Diofantičnost binárních funkčních symbolů $+$, $-$, $\cdot$ je zřejmá. Binární predikát $=$ je zjevně diofantický, stejně jako binární predikáty $<$ a $\backslash$:

$$a < b \iff \exists\, x\, [a + x + 1 = y] \ \text{ a } \ a \backslash b \iff \exists\, c\, [b = ac] \ .$$

Diofantické jsou i binární predikáty $\leq$ a $\neq$:

$$a \leq b \iff \exists\, x\, [a + x = y] \ \text{ a } \ a \neq b \iff \exists\, x\, [(a - b)^2 = 1 + x]$$

(nemůžeme použít negaci). Diofantické jsou i ternární predikát $\equiv \mod$ a binární predikát $\perp$:

$$a \equiv b \mod c \iff \exists\, x\, [a = b + cx \vee a = b - cx]$$

a

$$a \perp b \iff \exists\, x, y\, [ax - by = 1 \vee ax - by = -1]$$

(díky tvrzení 4). Tedy i binární funkční symboly $\mathrm{zby}(a, b)$ a $\mathrm{pod}(a, b)$ jsou diofantické:

$$r = \mathrm{zby}(a, b) \iff r \equiv a \mod b \ \& \ r < b$$

a

$$c = \mathrm{pod}(a, b) \iff 0 \leq a - c \cdot b < b \ .$$

Všechny naše elementární funkční a predikátové symboly jsou diofantické.

U mnohých složitějších „neelementárních" predikátů a funkcí však toneme v nejistotě a pochybách. Je predikát „být prvočíslo" diofantický? A co funkce 2^x? Je diofantická? V obou případech zní odpověď překvapivě ANO. Pro nalezení diofantické reprezentace budeme ale muset vynaložit nemalé úsilí.

3.5.2 Exponenciála je diofantická

Pustíme se do důkazu diofantičnosti binární exponenciální funkce x^y. Jde o kontraintuitivní výsledek, který je nosným pilířem důkazu Matijasevičovy věty. Z diofantičnosti x^y (tvrzení 75) vyplyne diofantičnost kombinatorických funkcí $\binom{n}{m}$ a $n!$ (tvrzení 76 a 77).

Pro každé číslo $a \in \mathbf{N}_0$ definujeme dvě posloupnosti čísel z $\mathbf{N}_0$, totiž $(X_a(n), n = 0, 1, \ldots)$ a $(Y_a(n), n = 0, 1, \ldots)$. Pro $a = 0$ to jsou identické nuly. Pro $a = 1$ definujeme X_1 jako identickou jedničku a $Y_1(n) = n$. Pro $a > 1$ definujeme $X_a(n)$ a $Y_a(n)$ ze vzorce

$$X_a(n) + Y_a(n)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n \; . \tag{15}$$

Z teorie v oddílu 3.3 dobře víme, že jde o posloupnosti složek nezáporných řešení Pelliány $x^2 - (a^2 - 1)y^2 = 1$. Pro $d = a^2 - 1$ je totiž generátorem množiny řešení $\varepsilon_d = a + 1 \cdot \sqrt{a^2 - 1}$. V následujících lemmatech je vždy $a > 0$, není-li stanoveno jinak. Speciálním případem $a = 2$ této Pelliány jsme se zabývali v lemmatu 63.

Stejné posloupnosti dostaneme, změníme-li v (15) znaménko + na −. Z (15) se snadno odvodí součtové vzorce ($d = a^2 - 1$)

$$\begin{aligned} X_a(n \pm m) &= X_a(n)X_a(m) \pm dY_a(n)Y_a(m) && (16)\\ Y_a(n \pm m) &= Y_a(n)X_a(m) \pm X_a(n)Y_a(m) \; . && (17) \end{aligned}$$

V (16) a (17) položíme $m = 1$ a eliminací $Y_a(n)$ dostaneme rekurenci pouze pro $X_a(n)$. Podobně dostaneme rekurenci pouze pro $Y_a(n)$. Sice

$$\begin{aligned} X_a(n+1) &= 2aX_a(n) - X_a(n-1) && (18)\\ Y_a(n+1) &= 2aY_a(n) - Y_a(n-1) \; , && (19) \end{aligned}$$

přičemž $X_a(0) = 1$, $X_a(1) = a$, $Y_a(0) = 0$ a $Y_a(1) = 1$.

Z (16) a (17) také lehce odvodíme povědomé formule

$$\begin{aligned} X_a(2n) &= 2X_a(n)^2 - 1 && (20)\\ Y_a(2n) &= 2X_a(n)Y_a(n) \; . && (21) \end{aligned}$$

Pro stručnost v následujících důkazech pomíjíme index a.

Lemma 68. *Pro každé $n \in \mathbf{N}_0$ platí kongruence*

$$\begin{aligned} Y_a(n) &\equiv Y_b(n) \bmod a-b && (22)\\ Y_a(n) &\equiv n \bmod a-1\ . && (23) \end{aligned}$$

Důkaz. Z (19) je jasné, že pro pevné n je funkce $Y_a(n)$ celočíselný polynom v a stupně $n-1$. Proto první kongruence. Druhá plyne z první, protože $Y_1(n) = n$. ♢

Lemma 69.

$$n \backslash m \iff Y_a(n) \backslash Y_a(m)\ .$$

Důkaz. Podle (17) máme

$$Y(k+n) = X(n)Y(k) + X(k)Y(n) \equiv X(n)Y(k) \bmod Y(n)\ .$$

Protože $X(n) \perp Y(n)$, máme $Y(n)\backslash Y(k+n)$, právě když $Y(n)\backslash Y(k)$. Tudíž $Y(n)\backslash Y(m)$, právě když $Y(n)\backslash Y(r)$, kde $r = \mathrm{zby}(m,n)$. Z $0 \leq r < n$ plyne $0 \leq Y(r) < Y(n)$, a tak $Y(n)\backslash Y(m)$, právě když $r = 0$, to jest $n\backslash m$. ♢

Lemma 70.

$$Y_a^2(n)\backslash Y_a(m) \iff (nY_a(n))\backslash m\ .$$

Důkaz. Podle definice $X_a(n)$ a $Y_a(n)$

$$X_a(nj) + Y_a(nj)\sqrt{d} = (X_a(n) + Y_a(n)\sqrt{d})^j\ .$$

Takže

$$Y_a(nj) = \sum_{i=1}^{j} \langle i \text{ je liché} \rangle \binom{j}{i} X_a(n)^{j-i} Y_a(n)^i d^{(i-1)/2}\ .$$

Dostáváme kongruenci

$$Y_a(nj) \equiv jX_a(n)^{j-1}Y_a(n) \bmod Y_a^3(n)\ .$$

Nechť $Y^2(n)\backslash Y(m)$. Podle lemmatu 69 máme $m = nj$. S tímto j použijeme odvozenou kongruenci a dostaneme $Y^2(n)\backslash jY(n)$ (protože $Y(n) \perp X(n)$). Takže $Y(n)\backslash j$ a $(nY(n))\backslash m$.

Naopak, nechť $(nY(n))\backslash m$. Položíme $j = Y(n)$ a použijeme kongruenci. Dostaneme $Y^2(n)\backslash Y(nY(n))$. Podle Lemmatu 69 máme $Y^2(n)\backslash Y(m)$. ♢

Lemma 71.

1. *Pro* $a > 1$ *a* $n > 0$ *platí* $Y_a(n-1) + Y_a(n) < X_a(n)$.

2.

$$\begin{aligned} Y_a(4ni \pm m) &\equiv Y_a(m) \bmod X_a(n) \\ Y_a(4ni + 2n \pm m) &\equiv \mp Y_a(m) \bmod X_a(n) \ ; \end{aligned}$$

znaménka si odpovídají.

DŮKAZ. **1.** Podle (17) (s $+$, $n := n-1, m := 1$) máme

$$2Y(n-1) \leq aY(n-1) \leq aY(n-1) + X(n-1) = Y(n) \ .$$

Proto $Y(n-1) < Y(n) - Y(n-1)$. Tudíž, opět podle (17) (s $-$, $n := n, m = 1$),

$$Y(n-1) + Y(n) < 2Y(n) - Y(n-1) \leq aY(n) - Y(n-1) = X(n) \ .$$

2. Podle formulí (20) a (21) $Y(2n) \equiv 0$ a $X(2n) \equiv -1 \bmod X(n)$. Takže, podle (17),

$$Y(2n \pm m) \equiv \mp Y(m) \bmod X(n) \ .$$

Opakovaným užitím dostáváme obě kongruence. ♢

Lemma 72. *Nechť* $a > 1$ *a* $n > 0$. *Pak*

$$Y_a(k) \equiv \pm Y_a(m) \bmod X_a(n) \iff k \equiv \pm m \bmod 2n \ ;$$

znaménka si nemusejí odpovídat.

DŮKAZ. Nejprve dokážeme zpětnou implikaci. Nechť $k = 2nj \pm m$. Pro $j = 2i$ máme podle 2 předchozího lemmatu $Y(k) = Y(4ni \pm m) \equiv \pm Y(m) \bmod X(n)$. Pro $j = 2i + 1$ máme $Y(k) = Y(4ni + 2n \pm m) \equiv \mp Y(m) \bmod X(n)$.

Naopak, nechť $Y(k) \equiv \pm Y(m) \bmod X(n)$. Zvolíme k' a m', že $0 \leq k', m' \leq n$, $k \equiv \pm k' \bmod 2n$ a $m \equiv \pm m' \bmod 2n$. Podle předpokladu a již dokázané zpětné implikace máme $Y(k') \equiv \pm Y(m') \bmod X(n)$. Takže $X(n)$ dělí $Y(k') \pm Y(m')$, což implikuje $k' = m'$, protože z $k' \neq m'$ by plynul spor (viz 1 předchozího lemmatu) $0 < |Y(k') \pm Y(m')| \leq Y(n-1) + Y(n) < X(n)$. Z $k' = m'$ hned plyne $k \equiv \pm m \bmod 2n$. ♢

Tvrzení 73 (diofantičnost funkce $Y_a(b)$). *Binární funkce $Y_a(b)$ je diofantická. Konkrétně,*

$$
\begin{aligned}
& c = Y_a(b) \iff (a = 0 \;\&\; c = 0) \vee (a = 1 \;\&\; c = b) \\
& \vee(a > 1 \;\&\; \exists\, d, e, f, g, h, i, j \\
& [(\alpha)\; d^2 - (a^2-1)c^2 = 1 \;\&\; (\beta)\; f^2 - (a^2-1)e^2 = 1 \\
& \;\&\; (\gamma)\; i^2 - (g^2-1)h^2 = 1 \\
& \;\&\; (\delta)\; e = (j+1)2c^2 \;\&\; (\epsilon)\; g \equiv a \bmod f \;\&\; (\zeta)\; g \equiv 1 \bmod 2c \\
& \;\&\; (\eta)\; h \equiv c \bmod f \;\&\; (\theta)\; h \equiv b \bmod 2c \;\&\; (\iota)\; b \leq c]) \;.
\end{aligned}
$$

DŮKAZ. Napravo od $\iff$ stojí zjevně diofantická formule, stačí dokázat ekvivalenci. Pro $a = 0, 1$ platí. Nechť $a > 1$ a existují $d, \ldots, j$ splňující (α) až (ι). Podle Pellián $(\alpha), (\beta), (\gamma)$ existují čísla p, q a r, že $d = X_a(p), c = Y_a(p), f = X_a(q), e = Y_a(q), i = X_g(r)$ a $h = Y_g(r)$. Platí $0 \leq p \leq c$ a, podle (ι), $0 \leq b \leq c$. Dokážeme, že $b \equiv r \equiv \pm p \bmod 2c$. Odtud vyplývá $b = p$ a $c = Y_a(p) = Y_a(b)$.

Pro $c = 0$ jsme hotovi hned, (ι) dává $b = 0$. Nechť $c > 0$. Podle (δ) $c^2 \backslash e$. Lemma 70 nám dává $c \backslash q$, protože

$$Y_a^2(p) \backslash Y_a(q) \implies Y_a(p) \backslash q \;.$$

Podle (θ) platí $b \equiv h = Y_g(r) \bmod 2c$. Podle (23) máme $Y_g(r) \equiv Y_1(r) = r \bmod (g-1)$. Platí však (ζ), a tak

$$b \equiv r \bmod 2c \;.$$

Podle (ϵ) a (22) máme $Y_a(r) \equiv Y_g(r) \bmod f = X_a(q)$. Podle (η) máme $Y_g(r) = h \equiv c = Y_a(p) \bmod f = X_a(q)$. Takže $Y_a(r) \equiv Y_a(p) \bmod X_a(q)$ a lemma 72 dává

$$r \equiv \pm p \bmod 2q \;.$$

Jak víme, $c \backslash q$. Takže $r \equiv \pm p \bmod 2c$. Odtud a z $b \equiv r \bmod 2c$ plyne $b \equiv \pm p \bmod 2c$.

Nechť naopak $a > 1$ a $c = Y_a(b)$. Položíme $d = X_a(b)$. Pak (α) a (ι) platí. Položíme $q = bY_a(b), f = X_a(2q)$ a $e = Y_a(2q)$. Platí (β). V lemmatu 70 položíme $m = bY_a(b)$ a $n = b$. Lemma říká, že $Y_a^2(b) \backslash Y_a(bY_a(b))$. Takže $c^2 \backslash Y_a(q)$. Podle (21) $(2Y_a(q)) \backslash Y_a(2q)$, a proto $2c^2 \backslash e$. Tudíž se (δ) dá splnit vhodným j. Položíme $g = a + f^2(f^2 - a)$. Nyní platí i (ϵ). (β) a (δ) spolu dávají $f^2 \equiv 1 \bmod 2c$ a volba g tedy dává (ζ). Položíme $i = X_g(b)$ a $h = Y_g(b)$. Pak platí (γ). Podle (23) $h = Y_g(b) \equiv b \bmod (g-1)$. Podle ($\zeta$) je $h \equiv b \bmod 2c$ a tedy platí (θ). Z (22) máme, že $h = Y_g(b) \equiv Y_a(b) = c \bmod (g-a)$ a to spolu s (ϵ) implikuje $h \equiv c \bmod f$. (η) platí a vše je splněno. $\diamondsuit$

Pomocí (19) indukcí snadno plyne odhad

$$(2a-1)^n \leq Y_a(n+1) < (2a)^n \ . \tag{24}$$

Lemma 74. *Pro všechna $a, k, n \in \mathbf{N}_0$ platí kongruence*

$$X_a(n) - (a-k)Y_a(n) \equiv k^n \bmod 2ak - k^2 - 1 \ .$$

DŮKAZ. Postupujeme indukcí podle n. Pro $n = 0$ a $n = 1$ kongruence platí. Pomocí rovnic (18) a (19) dostáváme

$$\begin{aligned} & X(n+1) - (a-k)Y(n+1) \\ = \ & 2aX(n) - X(n-1) - (a-k)(2aY(n) - Y(n-1)) \\ = \ & 2a(X(n) - (a-k)Y(n)) - (X(n-1) - (a-k)Y(n-1)) \\ \equiv \ & 2ak^n - k^{n-1} = k^{n-1}(2ak-1) \\ \equiv \ & k^{n+1} \bmod 2ak - k^2 - 1 \ . \end{aligned}$$

$\diamondsuit$

Tvrzení 75 (diofantičnost exponenciály). *Exponenciální funkce x^y je diofantická, protože pro $y > 0$ a $x > 1$ máme*

$$z = x^y \iff \exists\, a \, [a \geq Y_x(y+1) \ \& \ z = \mathrm{zby}(X_a(y) - (a-x)Y_a(y), 2ax - x^2 - 1)] \ .$$

DŮKAZ. Z předešlých výsledků, zejména z tvrzení 73, je jasné, že formule vpravo je diofantická. Hodnoty exponenciály pro $y = 0$ a $x = 0, 1$ se přidají disjunkcemi. Stačí ukázat platnost ekvivalence. Dokážeme, že pro každé $a \geq Y_x(y+1)$ se x^y rovná zbytku popsanému v druhé klauzuli konjunkce. Mohli jsme tedy vystačit jen s ní, kdybychom v ní a nahradili $Y_x(y+1)$. Podle (24) a předpokladů

$$x \leq x^y < (2x-1)^y \leq Y_x(y+1) \leq a \ .$$

Odtud $x + 1 \leq a$ a proto

$$a < ax < ax + (x+1)x - x^2 - 1 \leq 2ax - x^2 - 1 \ .$$

Proto je x^y menší než modul $2ax - x^2 - 1$. Podle kongruence v lemmatu 74 se x^y rovná příslušnému zbytku. $\diamondsuit$

Teď vidíme, že formule

$$n > 2 \;\&\; xyz > 0 \;\&\; x^n + y^n = z^n$$

definující 4-ární relaci všech porušení FPV je diofantická. Proto existuje celočíselný polynom $P(n, x, y, z, x_1, \ldots, x_m)$ takový, že první čtyři souřadnice řešení rovnice $P = 0$ dávají právě všechna porušení FPV. FPV se dá zredukovat na jedinou diofantickou rovnici. Díky Wilesovi ovšem dnes víme, že $P = 0$ žádné řešení nemá a tak tento příklad poněkud ztrácí na lesku.

Tvrzení 76 (diofantičnost binomického koeficientu). *Binomický koeficient je binární diofantická funkce, protože pro $x, y \in \mathbf{N}_0$ platí*

$$z = \binom{x}{y} \iff \exists\, u\, [u > 2^x \;\&\; z = \mathrm{zby}(\mathrm{pod}((u+1)^x, u^y), u)]\ .$$

Důkaz. Už víme, že $2^x, (u+1)^x$ a u^y jsou diofantické funkce. Formule vpravo je tudíž diofantická. Nechť $u > 2^x$. Pomocí binomické věty máme

$$\frac{(u+1)^x}{u^y} = \sum_{i=y+1}^{x} \binom{x}{i} u^{i-y} + \binom{x}{y} + r\ ,$$

kde

$$r = \sum_{i=0}^{y-1} \binom{x}{i} u^{i-y} \le \frac{1}{u} \sum_{i=0}^{x} \binom{x}{i} \le \frac{2^x}{u} < 1\ .$$

Proto $\mathrm{pod}((u+1)^x, u^y) \equiv \binom{x}{y} \bmod u$. Vzhledem k $u > 2^x$ je binomický koeficient menší než modul u a platí dokazovaná rovnost. $\diamondsuit$

Tvrzení 77 (i faktoriál je diofantický). *Faktoriál je diofantická funkce, protože*

$$y = x! \iff \exists\, z\, [z > 2(x-1)^2 x^x + x - 1 \;\&\; y = \mathrm{pod}(z^x, \tbinom{z}{x})]\ .$$

Důkaz. Díky předchozím výsledkům je formule diofantická a stačí jenom ukázat, že definuje faktoriál. Nechť $z > 2(x-1)^2 x^x + x - 1$ je libovolné. Po snadných úpravách se vidí, že

$$x! \leq \frac{z^x}{\binom{z}{x}} = x! \prod_{i=1}^{x-1} \left(1 + \frac{i}{z-i}\right) < x! \mathrm{e}^{(x-1)^2/(z-x+1)} < x! \left(1 + \frac{2(x-1)^2}{z-x+1}\right) .$$

Užili jsme odhad $1 + u < \mathrm{e}^u < 1 + 2u$ platný v intervalu $(0, 1/2)$. Poslední výraz v hořejším odhadu je $< x! + 1$, protože $x^x > x!$. Po zaokrouhlení podílu dolů dostaneme $x!$. $\diamondsuit$

Máme už dost prostředků, abychom dokázali diofantičnost množiny prvočísel (úloha 19). Chceme-li však k tomu použít přirozenou definici prvočísla, musíme zdolat ještě jednu překážku.

3.5.3 Omezený $\forall$ zachovává diofantičnost

Obecný kvantifikátor $\forall$ diofantičnost nezachovává (úloha 20). Jeho omezená forma však ano. Značení $\forall\, y < a\ [\ldots]$ je zkratka pro $\forall\, y\ [y \geq a \vee \ldots]$ a říká se mu *omezený obecný kvantifikátor*.

Tvrzení 78 (diofantičnost omezeného $\forall$). *Nechť $R \subset \mathbf{N}_0^n$ je diofantická relace. Pak i relace $S \subset \mathbf{N}_0^n$,*

$$S(a_1, \ldots, a_n) \iff \forall\, y < a_n\ [R(a_1, \ldots, a_{n-1}, y)] ,$$

je diofantická.

Důkaz. Pro $n = 1$ tvrzení platí triviálně (proč?). Pro jednoduchost značení předpokládáme, že $n = 2$, obecný případ je velmi podobný (úloha 22). Nechť relaci R reprezentuje celočíselný polynom $D(a, y, x_1, \ldots, x_m)$ se dvěma parametry a, y a m neznámými x_i.

Jako $B(a, b, w)$ označíme polynom s nezápornými koeficienty, který vznikne z D změnou znamének záporných koeficientů a substitucí $y = b, x_1 = w, \ldots, x_m = w$. Dokážeme ekvivalenci

$$\begin{aligned}
&\forall\, y < b\ \exists\, x_1, \ldots, x_m\ [D(a, y, x_1, \ldots, x_m) = 0] \iff \\
&\exists\, w, z_0, \ldots, z_m\ [\tbinom{z_0}{b} \backslash D(a, z_0, \ldots, z_m)\ \& && (25)\\
&b!(b + w + B(a, b, w))! \backslash (z_0 + 1)\ \& && (26)\\
&\tbinom{z_0}{b} \backslash \tbinom{z_1}{w}\ \& \cdots \&\ \tbinom{z_0}{b} \backslash \tbinom{z_m}{w}] . && (27)
\end{aligned}$$

Vlevo od ekvivalence je formule definující relaci $S \subset \mathbf{N}_0$. Vpravo máme za existenčním kvantifikátorem konjunkci $m+2$ podmínek. Podle předešlých výsledků, zejména tvrzení 76 a 77, je každá z nich diofantická a tedy i relace S je diofantická. Zbývá dokázat ekvivalenci.

$\Longrightarrow$. Nechť $(a,b) \in \mathbf{N}_0^2$ je taková dvojice, že $D(a,y,x_1^y,\ldots,x_m^y)=0$ pro $y=0,1,\ldots,b-1$ pro nějaká $x_i^y \in \mathbf{N}_0$ (exponent y označuje v tomto důkazu závislost na y, ne umocnění). Zvolíme w libovolně, ale tak, že $w > x_i^y$ pro všechna y a i. Číslo z_0 zvolíme libovolně, ale tak, že platí podmínka (26). Pro $y=0,1,\ldots,b-1$ definujeme přirozená čísla

$$q_y = \frac{z_0+1}{y+1} - 1 \ .$$

Z volby z_0 plyne, že čísla q_y jsou po dvou nesoudělná. (Protože $q_y \perp b!$ a pro $y > z$ máme $(y+1)q_y - (z+1)q_z = y - z < b$.) Dále $z_0 \equiv y \bmod q_y$ a $q_y \perp w!$ pro každé y. Pro každé $i = 1,2,\ldots,m$ uvážíme soustavu b kongruencí $z_i \equiv x_i^y \bmod q_y$, $y=0,1,\ldots,b-1$. Podle čínské věty o zbytku (tvrzení 5) existuje řešení $z_i \in \mathbf{N}_0$. Pro $y = 0,1,\ldots,b-1$ tedy platí

$$z_i \equiv x_i^y \ \&\ z_0 \equiv y \bmod \prod_{y=0}^{b-1} q_y = \binom{z_0}{b} \ .$$

Odtud plyne, že platí (25). Z volby w a $z_1,\ldots,z_m$ plyne, že q_y dělí součin $(z_i-0)(z_i-1)\cdots(z_i-w+1)$. Tedy q_y dělí i $\binom{z_0}{w}$ (protože $q_y \perp w!$). Proto (nesoudělnost čísel q_y) platí (27).

$\Longleftarrow$. Máme $(a,b) \in \mathbf{N}_0^2$ a $w, z_0, \ldots, z_m \in \mathbf{N}_0$, že platí (25), (26) a (27) a máme zadáno $y, 0 \le y \le b-1$. Definujeme q_y jako výše. Opět $q_y \perp w!$. Nechť p_y je libovolný prvočinitel q_y. Z (27) vyplývá, že q_y a tedy i p_y dělí součin $(z_i-0)(z_i-1)\cdots(z_i-w+1)$, $i=1,\ldots,m$. Proto existují čísla $x_1^y,\ldots,x_m^y$, že $p_y \backslash (z_i - x_i^y)$. Opět $z_0 \equiv y \bmod q_y$, takže $p_y \backslash (z_0 - y)$. Podle (26) a definice q_y platí $p_y > B(a,b,w)$. Tudíž $|D(a,y,x_1^y,\ldots,x_m^y)| < p_y$ (definice B). To spolu s (25) dává $D(a,y,x_1^y,\ldots,x_m^y)=0$. Pro dané y jsme nalezli $x_1^y,\ldots,x_m^y$ s vlastností požadovanou vlevo: $D(a,y,x_1^y,\ldots,x_m^y)=0$. $\diamondsuit$

Přirozená definice prvočísla je prostřednictvím omezeného $\forall$:

$$x \text{ je prvočíslo} \iff x > 1 \ \&\ \forall y < x \ [y \le 1 \vee \mathrm{zby}(x,y) > 0] \ .$$

Podle právě dokázaného tvrzení je formule vpravo diofantická. Dokázali jsme

Tvrzení 79. *Množina prvočísel je diofantická.*

3.5.4 Rekurzivní funkce jsou diofantické

Velmi jsme pokročili. Zatímco na počátku jsme o mnohých jednoduchých aritmetických funkcích, jako třeba 2^x, nevěděli, zda jsou diofantické, nyní naopak není jasné, jak by mohla funkce daná jednoduchým aritmetickým předpisem nebýt diofantická. V tvrzení 81 dokážeme, že každá rekurzivní funkce je diofantická, což znamená, že v jistém smyslu „vše“ je diofantické. V tvrzení 82 sestrojíme binární diofantickou relaci, jejíž projekce probíhají všechny diofantické množiny. Standardní selfreferenční a diagonalizační argument teorie rekurze pak už vede přímo k důkazu Matijasevičovy věty.

Rekurzivní funkce tvoří třídu funkcí definovaných na $\mathbf{N}_0^n$ (n je obecně různé pro různé funkce), s hodnotami v $\mathbf{N}_0$. Jsou to ty funkce, které lze vytvořit z *konstantní funkce* $c : \mathbf{N}_0 \to \mathbf{N}_0$, $c(x) = 0$, z *funkce následníka* $s : \mathbf{N}_0 \to \mathbf{N}_0$, $s(x) = x + 1$, a z *projekcí* $U_i^n : \mathbf{N}_0^n \to \mathbf{N}_0$, $U_i^n(x_1, \ldots, x_n) = x_i$, konečným počtem aplikací tří níže definovaných operátorů skládání, primitivní rekurze a minimalizace.

Skládání složí m funkcí f_i arity n pomocí m-ární funkce f v novou n-ární funkci g,

$$g(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) \ .$$

Primitivní rekurze definuje z n-ární funkce f a $(n+2)$-ární funkce g novou $(n+1)$-ární funkci h,

$$\begin{aligned} h(x_1, \ldots, x_n, 0) &= f(x_1, \ldots, x_n) \ \text{ a} \\ h(x_1, \ldots, x_n, y+1) &= g(y, h(x_1, \ldots, x_n, y), x_1, \ldots, x_n) \ . \end{aligned}$$

Minimalizace definuje ze dvou $(n+1)$-árních funkcí f a g novou n-ární funkci h,

$$h(x_1, \ldots, x_n) = \mathrm{MIN}_y(f; g) = \min\{y : \ f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)\} \ ,$$

přičemž musí být splněna podmínka, že pro každou n-tici $x_1, \ldots, x_n$ má rovnice $f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)$ řešení y, to jest h je všude definovaná.

Jako příklad dokážeme, že binární aritmetické funkce $+$ a $\cdot$ jsou rekurzivní. Sčítání je rekurzivní, protože

$$x + 0 = U_1^1(x) \ \text{ a } \ x + (y+1) = g(y, x+y, x) \ ,$$

kde $g(u,v,w) = s(U_2^3(u,v,w))$. Funkce $+$ je definována aplikací primitivní rekurze a skládání na funkce U_1^1, s a U_2^3. Podobně je násobení rekurzivní, protože

$$x \cdot 0 = c(x) = 0 \ \text{ a } \ x \cdot (y+1) = g(y, x \cdot y, x) \ ,$$

kde $g(u,v,w) = U_2^3(u,v,w) + U_3^3(u,v,w)$ a rekurzivita $+$ je už dokázána. Rovněž každá konstantní funkce $c_k(x) = k, k \in \mathbf{N}_0$, je rekurzivní, neboť $c_0(x) = c(x)$ a $c_{k+1}(x) = c_k(x) + 1$. Každý polynom s kladnými celými koeficienty je rekurzivní funkce, protože vznikne opakovaným skládáním funkcí $+, \cdot$ a konstant.

Třída rekurzivních funkcí je mnohem obsáhlejší, než naznačují předchozí příklady. Představuje jednu z formálních specifikací pojmu algoritmu. Jiné specifikace jsou například Turingovy stroje nebo Markovovy normální algoritmy. O všech známých specifikacích se dá simulací jednoho modelu druhým ukázat, že definují tutéž třídu vyčíslitelných funkcí. Podle filozofické *Churchovy teze*, což je mimomatematické tvrzení, se tato třída shoduje s třídou funkcí vyčíslitelných jakýmkoli algoritmem (chápaným v intuitivním smyslu).

Pro důkaz následujících tvrzení se nám budou hodit funkce $p, q : \mathbf{N} \to \mathbf{N}_0$ definované vztahem

$$n = 2^{p(n)}(2q(n) + 1) \ .$$

Patrně $p(n), q(n) < n$. Zobrazení $n \to (p(n), q(n))$ je bijekce mezi $\mathbf{N}$ a $\mathbf{N}_0^2$. Lehce se vidí, že obě funkce jsou diofantické a rekurzivní. Totéž platí i pro funkci $F(i) = 2^{2^i} + 1$.

Tvrzení 80 (kódování n-tic). *Existuje binární diofantická a rekurzivní funkce $S(i,u)$ s následující vlastností. Pro každé $n \in \mathbf{N}$ a každou n-tici $(a_1, \ldots, a_n) \in \mathbf{N}_0^n$ existuje $u \in \mathbf{N}_0$ takové, že*

$$S(0,u) = a_1 \ , \ S(1,u) = a_2 \ , \ \ldots \ , \ S(n-1,u) = a_n \ .$$

Důkaz. Položíme $S(i,u) = \mathrm{zby}(q(u), F(i + p(u))$. Nechť $(a_1, \ldots, a_n) \in \mathbf{N}_0^n$ je libovolná n-tice. Vezmeme dostatečně velké číslo $v \in \mathbf{N}_0$, aby pro $i = 1, \ldots n$ platilo $F(v) > a_i$. Tím spíše pak platí $F(i-1+v) > a_i$. Uvážíme systém kongruencí

$$w \equiv a_i \bmod F(i-1+v) \ , \ i = 1, \ldots, n \ .$$

Jeho moduly jsou po dvou nesoudělné, protože čísla $F(n), n \in \mathbf{N}_0$, jsou vzájemně nesoudělná. (To je snadné cvičení. Nebo viz oddíl 5.1.) Podle věty 5 z kapitoly 1 má systém řešení $w \in \mathbf{N}$. Položíme $u = 2^v(2w+1)$. Je jasné, že $S(i,u)$ pro $i = 0,\dots,n-1$ probíhá naši n-tici. Funkce zby, p, q a F jsou diofantické i rekurzivní, diofantická i rekurzivní je proto i S. $\diamondsuit$

Tvrzení 81 (hlavní výsledek). *Funkce je rekurzivní, právě když je diofantická.*

DŮKAZ. Nechť je funkce f diofantická, pak

$$\begin{aligned}&y = f(x_1,\dots,x_n) \iff \\ &\exists\, z_1,\dots,z_m\, [P(x_1,\dots,x_n,y,z_1,\dots,z_m) = Q(x_1,\dots,x_n,y,z_1,\dots,z_m)]\ ,\end{aligned}$$

kde P a Q jsou polynomy s koeficienty v $\mathbf{N}_0$. S použitím funkce S z předchozího tvrzení můžeme tuto definici přepsat ve tvaru

$$\begin{aligned}f(x_1,\dots,x_n) &= S(0, \mathrm{MIN}_u(P(x_1,\dots,x_n,S(0,u),S(1,u),\dots,S(m,u));\\ &\quad Q(x_1,\dots,x_n,S(0,u),S(1,u),\dots,S(m,u))))\ .\end{aligned}$$

Protože P, Q a S jsou rekurzivní funkce, je (minimalizace a skládání) rekurzivní i f.

Naopak dokážeme, že rekurzivní funkce jsou diofantické. Konstanta, následník a projekce jsou triviálně diofantické. Stačí dokázat uzavřenost třídy diofantických funkcí na skládání, primitivní rekurzi a minimalizaci.

Nechť f a f_i jsou diofantické funkce a funkce g z nich vznikla složením. Pak i g je diofantická díky zachování diofantičnosti substitucí diofantických termů do diofantické formule.

Nechť funkce h vznikla z diofantických funkcí f a g primitivní rekurzí. Pak (hodnoty $h(x_1,\dots,x_n,0),\dots,h(x_1,\dots,x_n,y)$ zakódujeme do u)

$$\begin{aligned}z = h(x_1,\dots,x_n,y) &\iff \exists\, u\, [S(0,u) = f(x_1,\dots,x_n)\\ \&\ \forall t < y\, [S(t+1,u) &= g(t, S(t,u), x_1,\dots,x_n)]\ \&\ z = S(y,u)]\ .\end{aligned}$$

Podle tvrzení 78 a 80 je h diofantická.

Podobně se nahlédne, že i minimalizace zachovává diofantičnost. Vznikla-li funkce h z diofantických funkcí f a g minimalizací, je též diofantická, protože

$$\begin{aligned}y = h(x_1,\dots,x_n) \iff &f(x_1\dots,x_n,y) = g(x_1,\dots,x_n,y)\\ &\&\ \forall t < y\, [f(x_1\dots,x_n,t) \neq g(x_1,\dots,x_n,t)]\ .\end{aligned}$$

$\diamondsuit$

Sestrojíme univerzální binární diofantickou relaci. Zafixujeme abecedu proměnných $x_0, x_1, \ldots$ a pomocí funkcí p a q, které byly definovány před tvrzením 80, definujeme následující enumeraci všech polynomů s koeficienty v $\mathbf{N}_0$.

$$\begin{aligned} P_0 &= 1 \\ P_{3i-2} &= x_{i-1} \\ P_{3i-1} &= P_{p(i)} + P_{q(i)} \\ P_{3i} &= P_{p(i)} P_{q(i)} \ . \end{aligned}$$

Posloupnost $P_0, P_1, \ldots$ obsahuje všechny celočíselné polynomy s kladnými koeficienty a $P_n = P_n(x_0, \ldots, x_n)$ závisí jen na proměnných $x_0, \ldots, x_n$. Pro $n \in \mathbf{N}$ položíme

$$D_n = \{x_0 : \ \exists\, x_1, \ldots, x_n \, [P_{p(n)}(x_0, \ldots, x_n) = P_{q(n)}(x_0, \ldots, x_n)]\} \ .$$

Posloupnost $D_1, D_2, \ldots$ obsahuje všechny diofantické množiny.

Tvrzení 82 (univerzální diofantická relace). *Binární relace*

$$U = \{(m, n) : \ m \in D_n\}$$

je diofantická.

Důkaz. S pomocí funkce S z tvrzení 80 prostě přepíšeme definici enumerace:

$$\begin{aligned} & m \in D_n \iff \exists\, u\, [S(0, u) = 1 \ \&\ S(1, u) = m \\ & \ \&\ \forall i < n\, [S(3i-1, u) = S(p(i), u) + S(q(i), u)] \\ & \ \&\ \forall i < n\, [S(3i, u) = S(p(i), u) S(q(i), u)] \\ & \ \&\ S(p(n), u) = S(q(n), u)] \ . \end{aligned}$$

Formule vpravo je diofantická díky diofantičnosti funkcí p, q a S a díky předchozím výsledkům, zejména tvrzení 78. Ukážeme, že definuje predikát $m \in D_n$.

Pokud $m \in D_n$, platí $P_{p(n)}(m, t_1 \ldots, t_n) = P_{q(n)}(m, t_1, \ldots, t_n)$ pro nějaká $t_i \in \mathbf{N}_0$. Zvolíme u tak, že pro $i = 0, 1, \ldots, n$ máme $S(i, u) = P_i(m, t_1, \ldots, t_n)$. S tímto u je pravá strana jistě splněna.

Naopak, nechť platí pro dané m a n pravá strana. Položíme

$$t_1 = S(4,u), t_2 = S(7,u), \ldots, t_n = S(3n+1,u) \ .$$

Pak $S(i,u) = P_i(m, t_1, \ldots, t_n)$ pro $i = 0, 1, \ldots, n$ a

$$P_{p(n)}(m, t_1 \ldots, t_n) = P_{q(n)}(m, t_1, \ldots, t_n) \ ,$$

takže $m \in D_n$. ♢

Věta 83 (Matijasevič, 1970). *Řešitelnost diofantických rovnic je algoritmicky nerozhodnutelná úloha.*

Důkaz. Množina

$$V = \{n \in \mathbf{N} : \ n \notin D_n\}$$

není diofantická. Kdyby byla, $V = D_N$ pro nějaké $N \in \mathbf{N}$ a dostáváme spor

$$N \in V \iff N \notin D_N = V \ .$$

Funkce $g : \mathbf{N}_0^2 \to \{0,1\}$ s hodnotou 1 na U a hodnotou 0 mimo U, kde U je univerzální diofantická relace z tvrzení 82, není rekurzivní. Kdyby byla, byla by diofantická (tvrzení 81) a její graf $z = g(m,n)$ by byl reprezentován polynomem P s parametry z, m a n a neznámými $x_1, \ldots, x_p$. Pak by ale V byla diofantická,

$$V = \{x : \ \exists\, x_1, \ldots, x_p \, [P(0, x, x, x_1, \ldots, x_p) = 0] \ ,$$

což je spor.

Řekněme, že máme algoritmus, který umí rozhodnout existenci řešení jakékoli diofantické rovnice. Pak umíme algoritmicky rozhodnout platnost univerzálního diofantického predikátu $m \in D_n$: Vezmeme polynom $Q(m, n, x_1 \ldots, x_q)$ reprezentující U (tvrzení 82) a pro $(m,n) \in \mathbf{N}_0^2$ prostě testujeme, zda $Q(m, n, x_1 \ldots, x_q) = 0$ má či nemá řešení $x_i \in \mathbf{N}_0$. To je fakticky algoritmus, který počítá funkci g. Funkce g je rekurzivní, dostali jsme spor. ♢

Přesně řečeno, dokázali jsme, že neexistuje rekurzivní funkce, která by rozhodovala řešitelnost diofantických rovnic. Churchova teze rozšiřuje tento negativní výsledek na všechny myslitelné algoritmy.

Vlastně bylo dokázáno následující. Neexistuje algoritmus, který by rozhodoval existenci řešení $x_1, \ldots, x_q \in \mathbf{Z}$ pro vstupy

$$\{Q(n, n, x_1, \ldots, x_q) = 0 : \ n \in \mathbf{N}\} ,$$

kde Q je polynom reprezentující U. (Jinak by charakteristická funkce množiny V byla rekurzivní a V by byla diofantická.) Polynom Q se dá efektivně sestrojit.

Uvedeme slíbený paradoxní(?) důsledek existence univerzální diofantické relace U. Existuje *absolutní* konstanta $q \in \mathbf{N}$ taková, že *každá* diofantická množina $X \subset \mathbf{N}_0$ má reprezentaci celočíselným polynomem s jedním parametrem a q neznámými. Je to polynom $Q(x, r, x_1 \ldots, x_q)$, kde Q reprezentuje U a $X = D_r$ (X je r-tá množina v enumeraci diofantických množin). Jako příklad uvažme diofantické množiny M_n,

$$x \in M_n \iff \exists\, y_1, \ldots, y_n \, [x = (y_1 + 2)(y_2 + 2) \cdots (y_n + 2)] \ .$$

$M_1 = \mathbf{N} \backslash \{1\}$, M_2 je množina všech složených přirozených čísel a obecně je M_n množina všech „n-násobně složených“ čísel. Jak víme, kromě této „přirozené“ diofantické definice M_n existuje i taková, která používá (pro $n > q$) méně než n proměnných, dokonce omezeně mnoho!

3.6 Poznámky

Termín „diofantický“ je odvozen od jména antického matematika Diofanta, který ve své *Aritmetice* zkoumal řešení rovnic v racionálních číslech. Měli bychom asi hovořit o „fermatických“ rovnicích a problémech, protože to byl Fermat, kdo jako první zdůrazňoval řešení v oboru celých čísel.

O rozmanitosti diofantických problémů a metod pro jejich řešení si lze udělat dobrý obraz třeba z Mordellovy [27], Ribenboimovy [36] nebo Sprindžukovy [43] monografie. Nepatrná změna parametru může proměnit triviální úlohu ve velmi obtížně, pokud vůbec, řešitelný problém a naopak. Snadno lze přehlédnout jednoduchou cestu k řešení. Roberts [38] uvádí v kapitole o čísle 117 následující epizodu.

> In the chapter “Diophantine Equations: p-adic Methods” in *Studies in Number Theory* (edited by W. J. LeVeque), D. J. Lewis states on page 26: "The equation $x^3 - 117y^3 = 5$ is known to have at most 18 integral solutions but the exact number is unknown.”

Finkelstein and London (1971) made use of the field $\mathbf{Q}(117^{1/3})$, where the cube root is real, to show that, in fact, the equation has no solutions in integers.

Halter-Koch (1973) and Udrescu (1973) independently observed that by considering the equation modulo 9 we get $x^3 \equiv 5 \pmod 9$ and this congruence clearly has no solutions. Consequently we immediately see that the equation has no solutions.

3.1 O Fermatově poslední větě. Literatura: Edwards [8]. Eulerův důkaz FPV pro $n = 3$ byl neúplný, viz [8]. Edwardsova zajímavá kniha obsahuje historii FPV od počátků až do Kummera. Důkaz FPV, která dlouho fascinovala profesionály i amatéry (viz třeba [5]), v roce 1993 oznámil a v roce 1995 publikoval, s pomocí Taylora, Wiles, viz [47] a [45]. Čtenářka nalezne další zajímavosti a odkazy v Ribenboimových knihách [34] a [35]. Zde zmíníme pouze slavný klasický Kummerův výsledek, v němž se znovu záhadně objevují Bernoulliova čísla.

Zhruba v roce 1850 Kummer dokázal, že FPV platí pro každý prvočíselný exponent $n = p > 2$, který je *regulárním* prvočíslem. Regularita prvočísla se definuje pojmy algebraické teorie čísel a je ekvivalentní, jak Kummer rovněž dokázal, s tím, že p nedělí žádného čitatele Bernoulliových čísel $B_0, B_2, B_4, \ldots, B_{p-3}$. (Bernoulliova čísla jsou definována v úloze 22 v 1. kapitole.) Čitatele $B_0, B_2, \ldots, B_8$ jsou 1. Prvočíselné rozklady čitatelů $B_{10}, B_{12}, \ldots, B_{22}$ jsou:

$$\begin{array}{ll}
B_{10} = 5/\cdots & B_{12} = -691/\cdots \\
B_{14} = 7/\cdots & B_{16} = -3617/\cdots \\
B_{18} = 43867/\cdots & B_{20} = -(283 \cdot 617)/\cdots \\
B_{22} = (11 \cdot 131 \cdot 593)/\cdots & B_{24} = -(103 \cdot 2294797)/\cdots \\
B_{26} = (13 \cdot 657931)/\cdots\ . &
\end{array}$$

Odtud vidíme, že všechna prvočísla ≤ 29 jsou regulární a FPV pro ně platí. Neregulární prvočísla se nazývají *singulární*. Naše minitabulka ukazuje na druhé straně, že prvočísla $103, 131, 283, 593, 617, 691, 3617, 43867, 657931$ a 2294797 jsou singulární. Kummerovu větu pro ně nelze použít. (Lze pro ně použít jiná kritéria, která byla Kummerovou metodou odvozena později.) Mezi prvočísly nepřesahujícími 100 jsou singulární pouze $37, 59$ a 67 (dělí čitatele B_{32}, B_{44} a B_{58}). Je známo, že jak regulárních tak singulárních prvočísel je nekonečně mnoho.

3.2 Čtyři čtverce stačí. Literatura: Ireland a Rosen [13] a Nathanson [30]. Lagrangeova věta je „nejdůležitější výsledek v aditivní teorii čísel" (Nathanson [30]). Zobecňuje ji *Waringův problém*: Dokažte, že pro každé $r \in \mathbf{N}$ existuje počet $k = k(r)$ takový, že rovnice

$$x_1^r + x_2^r + \cdots + x_k^r = n$$

má pro každé $n \in \mathbf{N}_0$ řešení $x_i \in \mathbf{N}_0$. Podle Lagrangeovy věty lze pro $r = 2$ položit $k = 4$ (a víme, že nelze položit $k = 3$). Waring svůj problém publikoval v r. 1770. První důkaz nalezl v r. 1909 Hilbert, viz [30] nebo přímo [10].

3.3 Pelliána. Literatura: Hlawka, Schoißengaier a Taschner [12], Mordell [27] a [18]. Pellova rovnice ke svému jménu přišla omylem a Pell s ní neměl nic společného, viz Edwards [8]. Tabulka generátorů $\varepsilon_d = a_d^* + b_d^*\sqrt{d}$ grupy $(U, \cdot)$ ukazuje, že již pro malé d mohou být čísla a_d^* a b_d^* dosti velká, například pro $d = 13$ a $d = 29$. Z dvouciferných d je nejzapeklitější 61: $a_{61}^* = 1766319049$ a $b_{61}^* = 226153980$. Hodnota $d = 1621$ je ještě horší. Zatímco $a_{1620}^* = 161$ a $b_{1620}^* = 4$, pro d o 1 větší

$$\begin{aligned} a_{1621}^* &= 6298101812493732343034974500091457815529942308667051412857352310169665125001 \end{aligned}$$

a

$$\begin{aligned} b_{1621}^* &= 1564293243699791121284455833450983386275520438748241083991779224427510505 00\,. \end{aligned}$$

Tvrzení 61 o diofantické rovnici $x^2 - y^3 = 1$ je částečnou odpovědí na *Catalanovu domněnku*, podle níž má rovnice $x^a - y^b = 1$ jen jediné řešení $x, y, a, b > 1$, totiž $3^2 - 2^3 = 1$. Domněnka, předložená Catalanem v roce 1844, je dosud (v roce 2000) nedokázaná a nevyvrácená. V r. 1976 Tijdeman [46] dokázal, že všechny složky všech řešení Catalanovy rovnice nepřesahují jistou efektivně vyčíslitelnou konstantu. Případných protipříkladů je tedy efektivně konečně mnoho. Langevin z Tijdemanova důkazu odvodil v r. 1976 konkrétní odhady $a, b < \mathrm{e}^{245}$ a $x, y < \exp(\exp(\exp(\exp(730))))$. Zejména první odhad byl od té doby výrazně zlepšen, viz Ribenboimova kniha [36]. V ní lze nalézt důkaz zesílení tvrzení 61, které dokázal v r. 1738 Euler: $x^2 - y^3 = \pm 1$ má v oboru kladných *racionálních* čísel jediné řešení $3, 2$.

Z jiného hlediska je $x^2 - y^3 = 1$ zvláštním případem *Mordellovy rovnice* $x^2 - y^3 = k$, $k \in \mathbf{Z}$ je parametr. Viz Mordell [27] a Ireland a Rosen [13]. Konečnost počtu řešení $x, y \in \mathbf{Z}$ pro každé k dokázal v r. 1914 v [28] Mordell.

Použil redukci na Thueho rovnici a získaný odhad byl proto neefiktivní. V r. 1968 Baker [2] dokázal efektivní odhad: $|x|, |y| < \exp(10^{10}|k|^{10000})$. Mnohem lepší odhady uvádí Sprindžuk [43]. Mordellova rovnice je speciálním případem eliptické křivky, kdy se zkoumají *racionální* řešení.

3.4 Thueho rovnice. Literatura: Ireland a Rosen [13]. Věty Fermata, Eulera, Lagrange, Kummera a dalších zahrnovaly pouze jednotlivé rovnice. První obecný výsledek o diofantických rovnicích odvodil jednoduchými úvahami algebraické geometrie v r. 1887 Runge [39]. (Jak píše v [41] Skolem, v r. 1922 nezávisle znovuobjevil Rungeho výsledky.) Runge dokázal: Je-li $f(x, y) \in \mathbf{Z}[x, y]$ ireducibilní polynom stupně n, jehož homogení složka stupně n je reducibilní, ale není násobkem mocniny ireducibilního polynomu, má diofantická rovnice $f(x, y) = 0$ jen konečně mnoho řešení. (Reducibilita a ireducibilita se míní v $\mathbf{Q}[x, y]$.) Rungeho metoda dává obvykle velmi silné *efektivní* odhady velikosti řešení, její nevýhodou jsou značně omezující předpoklady použití. Nelze ji například použít ani pro Mordellovu ani pro Thueho rovnici (pro ireducibilní $F(x, y)$). Viz Mordell [27], Sprindžuk [43] nebo Skolem [41].

Na počátku 20. století zazářila v diofantické analýze jako meteor Thueho věta. Metoda však nesla stín neefektivnosti a algoritmická rozhodnutelnost řešitelnosti Thueho rovnic zůstávala otevřená. Všechna zesílení Liouvilleovy nerovnosti, o nichž píšeme v poznámkách k oddílu 2.7, byla neefektivní. Ve třicátých letech vyvinul Skolem „snad nejkrásnější metodu teorie diofantických rovnic“ (Sprindžuk [43]), založenou na analytických funkcích v p-adických polích a teorii lokálních analytických variet, která umožňovala dokázat konečnost počtu řešení pro řadu diofantických rovnic, mezi nimi i pro Thueho rovnici (za dodatečného předpokladu, že $F(x, 1)$ má alespoň jeden komplexní kořen). Skolemova metoda však byla stále neefektivní a nevedla k algoritmu nalézajícímu celočíselná řešení (je efektivní pro p-adická řešení). Viz Sprindžuk [43], Borevič a Šafarevič [6] nebo přímo Skolem [41].

Průlom přišel v šedesátých letech, kdy Baker dokázal efektivní odhady velikosti řešení Thueho rovnic. Jeho metoda odhadů lineárních forem logaritmů algebraických čísel našla mnoho dalších uplatnění, je například základem výše zmíněného Tijdemanova výsledku o Catalanově rovnici. V roce 1970 vynesly Bakerovi jeho průkopnické práce Fieldsovu medaili. O metodě lineárních forem logaritmů se lze poučit v [3] a [4].

Populární vysvětlení hlubokých výsledků o konečnosti počtu řešení rozsáhlých tříd diofantických rovnic, jichž bylo dosaženo metodami diofantické algebraické geometrie, jako je Siegelův (1929) nebo Faltingsův (1983) (Fieldsova medaile v r. 1986), lze nalézt v přehledovém článku [37]. Podrobnější průzkum tohoto oceánu může začít třeba v Langových knihách [22] a [23]. Zajímavá debata o diofantické analýze proběhla v [29], [20] a [21]. Počítačové algoritmy pro hledání řešení diofantických rovnic popisuje Smart [42].

3.5 Desátý Hilbertův problém. Literatura: [7], [16] a Matijasevičova monografie [26]. Důkaz Matijasevičovy věty je v závěru poněkud šroubovaný proto, abychom se vyhnuli zavádění dalších pojmů z teorie rekurze. Správná formulace hlavního výsledku je ta, že množina (relace) je diofantická, právě když je rekurzivně spočetná. Lze sestrojit reprezentaci univerzální diofantické relace U s $q = 9$ neznámými, viz [25] a [15]. O dalších Hilbertových problémech se lze dočíst v [17] a o Hilbertovi samém v Reidové [33].

Hilbert v roce 1900 v proslulé přednášce na kongresu matematiků v Paříži ([11]) předložil přicházejícímu 20. století třiadvacet problémů, které byly podle jeho názoru klíčové pro rozvoj matematiky. V desátém z nich se tázal po obecné metodě pro hledání řešení diofantických rovnic. V jiné části přednášky uvažoval možnost, že některé problémy se mohou ve vhodné formulaci ukázat být neřešitelnými. Pak požadoval důkaz neřešitelnosti.

Formální upřesnění, co rozumět „metodou", byla v podobě modelů algoritmů zavedena ve třicátých a čtyřicátých letech. Tehdy se také objevily první algoritmicky nerozhodnutelné úlohy a důkazy nerozhodnutelnosti. Domněnka, že by mezi takové úlohy mohl patřit 10. HP byla zmíněna Postem a v r. 1949 ji publikoval Davis. V padesátých a šedesátých letech pracovali na 10. HP tři američtí logikové: Davis, Putnam a Robinsonová.

Davis v roce 1953 uveřejnil domněnku, že každá rekurzivně spočetná relace je diofantická. Ta okamžitě implikuje nerozhodnutelnost 10. HP, protože podle klasického výsledku teorie rekurze existují rekurzivně spočetné množiny, které nejsou rekurzivní. Davis tehdy také dokázal, že každá rekurzivně spočetná relace $R(a_1, \ldots, a_m)$ má reprezentaci ve tvaru

$$\exists\, y\, \forall\, z \leq y\, \exists\, x_1, \ldots, x_n\, [P(a_1, \ldots, a_m, y, z, x_1, \ldots, x_n = 0]\ ,$$

kde P je celočíselný polynom. Zbývalo se „pouze" zbavit jednoho omezeného obecného kvantifikátoru.

Robinsonová přistupovala k problému z opačné, „nelogické" strany. Motivována problémem, který zmínil její učitel Tarski — dokázat, že funkce 2^x *není* diofantická — dokazovala diofantičnost řady relací. Zavedla pojem *relace exponenciálního růstu*. Je to taková binární relace D, že $D(a, b)$ implikuje $b < a^a$, ale na druhou stranu pro každé $k \in \mathbf{N}$ existují čísla $a, b \in \mathbf{N}$

taková, že $D(a,b)$ & $b > a^k$. Robinsonová v roce 1952 dokázala, že z existence diofantické relace exponenciálního růstu plyne diofantičnost exponenciály, faktoriálu a binomických koeficientů. Domněnka, že diofantická relace exponenciálního růstu existuje, se stala známou jako *hypotéza Robinsonové*.

Davis a Putnam v roce 1959 dokázali, že každá rekurzivně spočetná relace $R(a_1, \dots, a_m)$ má *exponenciálně diofantickou* reprezentaci ve tvaru

$$\begin{aligned}&\exists\, u_1, \dots, u_n, v_1, \dots, v_n, w_1, \dots, w_n \\ &[P(a_1, \dots, a_m, u_1, \dots, u_n, v_1, \dots, v_n, w_1, \dots, w_n) = 0 \\ &\ \&\ u_1 = v_1^{w_1}\ \&\ \dots\ \&\ u_n = v_n^{w_n}]\ .\end{aligned}$$

(P je celočíselný polynom.) Jejich důkaz však byl založen na nedokázané hypotéze, že v množině prvočísel existují libovolně dlouhé aritmetické posloupnosti. To je dosud (v roce 2000) otevřený problém. Robinsonová ukázala, jak tuto hypotézu z důkazu odstranit a v roce 1961 trojice badatelů publikovala společně výsledek, že každá rekurzivně spočetná relace je exponenciálně diofantická.

V tomto okamžiku bylo jasné, že ústředním problémem je diofantičnost exponenciály, jež plyne z hypotézy Robinsonové. Kdokoli nalezne diofantickou relaci exponeciálního růstu, dokáže diofantičnost rekurzivně spočetných množin a tím nerozhodnutelnost 10. HP a ostatní důsledky, jako je diofantičnost prvočísel a redukce proměnných libovolného diofantického problému na omezený počet. Ne všichni sdíleli víru v takové rozuzlení. Například logik Kreisel v recenzi článku Davise, Putnama a Robinsonové v časopisu *Mathematical Reviews* v roce 1962 napsal:

> These results are superfitially related to Hilbert's tenth Problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors' results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. sets and so it is likely that the present result is not closely connected with Hilbert's tenth Problem. Also it is not altogether plausible that all (ordinary) Diophantine problems are uniformly reducible to those in a fixed number of variables of fixed degree, which would be the case if all r.e. sets were Diophantine.

V lednu 1970 dvaadvacetiletý leningradský student Matijasevič dokázal diofantičnost relace

$$\{(n, F_{2n}) :\ n \in \mathbf{N}\}\ ,$$

kde F_n je posloupnost Fibonacciových čísel ($F_1 = F_2 = 1, F_{n+1} = F_n + F_{n-1}$). Je exponenciálního růstu: $F_n \sim \frac{1}{\sqrt{5}}((1+\sqrt{5})/2)^n$. Hypotéza Robinsonové platí spolu se všemi důsledky.

Po vyřešení známého problému vystoupí do popředí úspěšná cesta a částečné výsledky, neřkuli slepé uličky, upadají v zapomnění. Slepou uličkou v řešení 10. HP byla redukce na rovnici mezi slovy ve volné pologrupě. Jedná se o následující problém. Rozhodněte, zda pro dvě slova Φ a Ψ nad abecedou $\{a_1, \ldots, a_n, x_1, \ldots, x_m\}$ má rovnice $\Phi = \Psi$ řešení, to jest zda existuje m slov $X_1, \ldots, X_m$ nad abecedou $\{a_1, \ldots, a_n\}$ tak, že po substituci X_i za všechny výskyty x_i v Φ a Ψ vzniknou dvě stejná slova. Tento problém se dá redukovat na diofantické rovnice. Z nerozhodnutelnosti řešitelnosti rovnic mezi slovy by plynula nerozhodnutelnost 10. HP (ale ne naopak). Proč nepracovat raději se slovy místo s polynomy, „odaritmetizování“ situace může být zjednodušením. Na radu učitele takto zpočátku k 10. HP přistupoval i Matijasevič. Cesta však nevede nikam. V roce 1977 Makanin nalezl algoritmus, který rozhoduje řešitelnost rovnic mezi slovy.

Zajímavým osobním pohledem na historii řešení 10. HP a vůbec do zákulisí matematiky je Matijasevičova vzpomínka [25].

O dalších nerozhodnutelných a nedokazatelných tvrzeních (paradoxy teorie množin, Gödelovy výsledky, hypotéza kontinua, Matijasevičova věta) píše Podnieks [32].

Pro příbuzné problémy byly dosaženy i pozoruhodné pozitivní výsledky. Siegel [40] v r. 1972 v pětasedmdesáti dokázal, že řešitelnost kvadratických diofantických rovnic je algoritmicky rozhodnutelná. Zda to platí i pro kubické rovnice či zda už ony jsou nerozhodnutelné není známo. (Jak víme z úvodu, bikvadratické diofantické rovnice jsou nerozhodnutelné.) Jednodušší rozhodovací algoritmus pro kvadratické diofantické rovnice našli Grunewald a Segal [9]. Kornhauser [19] v r. 1990 dokázal, že má-li binární kvadratická diofantická rovnice $f(x, y) = 0$ řešení, pak má řešení splňující

$$\max\{|x|, |y|\} \leq (14H)^{15H} ,$$

kde H je největší absolutní hodnota koeficientu polynomu f. Nerode [31] nalezl algoritmus, který rozhoduje řešitelnost diofantických rovnic v p-adických číslech pro pevné p, a Ax [1] algoritmus, který rozhoduje, zda má daná diofantická rovnice řešení v p-adických číslech pro každé p.

Vzorem posledním algoritmům sloužil průkopnický výsledek polsko-amerického logika Tarskiho, který Tarski oznámil v r. 1931, ale publikoval, kvůli válce, až v r. 1948 v [44]: Elementární Euklidova geometrie je algoritmicky rozhodnutelná. Tarski sestrojil algoritmus, který pro každou uzavřenou formuli φ jazyka uspořádaných okruhů (to jest formuli predikátové logiky prvního řádu se symboly konstant 0 a 1, funkčními symboly $+, -$ a $\cdot$ a predikátovými symboly $=$ a $<$) rozhodne, zda v tělese $\mathbf{R}$ reálných čísel φ platí nebo ne. Tarského algoritmus rozhodne řešitelnost jakékoli soustavy polynomiálních rovnic a nerovnic v reálných číslech, a umí mnohem víc než to. Viz třeba Jacobsonova kniha [14]. Pro další fascinující otázky a výsledky ležící na hranici mezi teorií modelů, algebrou a teorií čísel viz [24].

3.7 Úlohy

1. (**2**) Dokažte, že kromě $(x, y, z) = (1, 1, 1)$ a $(4, 2, 2)$ nemá rovnice
$$2^x + 3^y = 5^z$$
v $\mathbf{N}$ jiné řešení.

2. (**3**) Jsou-li $f, g, h \in \mathbf{C}[x]$ vesměs nesoudělné polynomy, ne všechny konstantní, a platí-li
$$f + g = h\ ,$$
platí nutně nerovnost
$$\max\{\deg(f), \deg(g), \deg(h)\} \leq K - 1\ ,$$
kde K je počet *různých* kořenů polynomu fgh.

3. (**1**) Pomocí předchozí úlohy odvoďte polynomiální verzi FPV: Pokud $n \geq 3$ a platí
$$f^n + g^n = h^n\ ,$$
kde $f, g, h \in \mathbf{C}[x]$ jsou vesměs nesoudělné polynomy, pak f, g, h mají stupeň nula.

4. Tato kaskáda tří úloh se zabývá modulární verzí FPV.

   (a) (**2**) Dokažte, že pro každé $r \in \mathbf{N}$ existuje číslo $s \in \mathbf{N}$ takové, že pro každý rozklad množiny $X = \{A:\ A \subset \{1, 2, \ldots, s\}\ \&\ |A| = 2\}$ na r množin $X = X_1 \cup X_2 \cup \ldots \cup X_r$ existuje $i, 1 \leq i \leq r$, a tříprvková množina $S, S \subset \{1, 2, \ldots, s\}$, tak, že
$$\{A:\ A \subset S\ \&\ |A| = 2\} \subset X_i\ .$$

(b) (**1**) Dokažte, že pro každé $r \in \mathbf{N}$ existuje číslo $n \in \mathbf{N}$ tak, že pro libovolné rozdělení čísel $1, 2, \ldots, n$ do (nejvýše) r tříd se v jedné třídě najdou tři čísla $1 \leq x < y < z \leq n$ taková, že $z = x + y$.

(c) (**3**) Pomocí b dokažte, že pro každé $n \in \mathbf{N}$ existuje $m \in \mathbf{N}$ tak, že pro každé prvočíslo $p, p > m$, má kongruence

$$x^n + y^n \equiv z^n \bmod p$$

řešení $x, y, z \in \mathbf{Z}$, $xyz \not\equiv 0 \bmod p$.

5. (**2**) Dokažte první případ FPV pro exponenty $p = 13, 17, 19$.

6. (**1**) Nalezněte polynomiální identitu, která dokazuje, že součin dvou přirozených čísel, z nichž každé je součtem dvou čtverců, je opět součtem dvou čtverců.

7. (**2**) Existuje nekonečně mnoho dvojic po sobě jdoucích přirozených čísel, z nichž každé je součtem dvou čtverců? Trojic? Čtveřic?

8. (**2**) Projděte důkaz Lagrangeovy věty 57 o Pellově rovnici a rozhodněte, zda je efektivní. Pokud ano, jaký odhad nám poskytne, v závislosti na d, pro velikost nejmenšího netriviálního řešení Pelliány $x^2 - dy^2 = 1$?

9. (**3**) Nechť p je prvočíslo, $p \equiv 1 \bmod 4$. Dokažte, že

$$x^2 - py^2 = -1$$

má řešení. (Rovnice má tedy nekonečně mnoho řešení.)

10. (**2**) Ukažte, jak lze ze znalosti řešení rovnice $x^2 - y^3 = 1$ spočítat řešení rovnice $x^3 - 2y^3 = \pm 1$ a naopak. Nalezněte všechna řešení poslední rovnice.

11. (**2**) Dokažte, že $x^2 - y^3 = -1$ má v $\mathbf{Z}$ pouze triviální řešení $(0, 1)$. (Modifikujte důkaz tvrzení 61.)

12. (**2**) Dokažte, že $x^2 - y^n = -1$ má pro $n > 1$ pouze triviální celočíselné řešení $(0, 1)$. (Užijte faktorizaci $x^2 + 1 = (x + i)(x - i)$.)

13. (**2**) Dokažte, že $x^y - y^x = 1$ má v $\mathbf{N}$ jediné řešení $x = 3, y = 2$.

14. Nechť čísla $x, y \in \mathbf{N}$ jsou větší než 1, čísla $p, q \in \mathbf{N}$ jsou prvočísla, přičemž $p > q$, a platí $x^p - y^q = \pm 1$. (Každé netriviální řešení Catalanovy rovnice lze takto vyjádřit.)

    (a) (**2**) Dokažte, že q dělí x.

    (b) (**4**) Dokažte, že p dělí y.

15. (**1**) Číslo $n \in \mathbf{N}$ se nazývá *mocné*, pokud exponenty a_i v jeho prvočíselném rozkladu $n = p_1^{a_1} \dots p_r^{a_r}$ splňují nerovnost $a_i \geq 2$. Dokažte, že existuje nekonečně mnoho dvojic $n, n+1$ po sobě jdoucích mocných čísel.

16. (**1**) Co se dá říci o počtu řešení Thueho rovnice, vynecháme-li předpoklad ireducibility $F(x, y)$?

17. (**2**) Ukažte, jak libovolnou diofantickou rovnici redukovat na ekvivalentní soustavu rovnic typu $\alpha = \beta + 1$ a $\alpha = \beta \cdot \gamma$. ($\alpha, \beta, \gamma$ jsou neznámé nebo konstanty ze $\mathbf{Z}$.)

18. (**2**) Nalezněte diofantickou reprezentaci množiny přirozených čísel, která nejsou mocninou 2. Totéž pro čísla, která nejsou mocninou čísla $a \in \mathbf{N}$.

19. (**2**) Dokažte bez použití diofantičnosti omezeného obecného kvantifikátoru, že množina prvočísel je diofantická.

20. (**2**) Ukažte, že implikace $\Rightarrow$, negace $\neg$ a (neomezený) obecný kvantifikátor $\forall$ diofantičnost nezachovávají.

21. (**3**) Ukažte dvěma redukcemi algoritmickou ekvivalenci úloh U1 a U2. U1: Rozhodnout, zda diofantická rovnice má *racionální* řešení. U2: Rozhodnout, zda diofantická rovnice s homogením polynomem má *netriviální* (ne všechny složky jsou 0) celočíselné řešení.

22. (**3**) Promyslete si důkaz tvrzení 78 pro obecné $n \geq 2$.

Literatura

[1] J. Ax, The elementary theory of finite fields, *Ann. Math.,* **88** (1968), 239–271.

[2] A. Baker, The diophantine equation $y^2 = x^3 + k$, *Phil. Trans. Roy. Soc. London,* **263** (1968), 193–208.

[3] A. Baker, The theory of linear forms in logarithms, 1–27. In: A. Baker and D. W. Masser (ed.), *Transcendence Theory: Advances and Applications,* Academic Press, New York 1977.

[4] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. reine und angew. Math.,* **442** (1993), 19–62.

[5] K. Barner, Paul Wolfskehl and the Wolfskehl Prize, *Notices Amer. Math. Soc.,* **44** (1997), 1294–1303.

[6] Z. I. Borevič a I. R. Šafarevič, *Těorija Čisel,* Mir, Moskva 1985. [Anglický překlad: Z. I. Borevich and I. R. Shafarevich, *Number Theory,* Academic Press, New York 1966.]

[7] M. Davis, Hilbert's Tenth Problem is unsolvable, *Amer. Math. Monthly,* **80** (1973), 233–269.

[8] G. Edvards, *Posledňaja Těorema Ferma,* Mir, Moskva 1980. [Původně: H. M. Edwards, Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory, Springer, New York 1977.]

[9] F. J. Grunewald and D. Segal, How to solve a quadratic equation in integers, *Math. Proc. Cambridge Philos. Soc.,* **89** (1981), 1–5.

[10] D. Hilbert, Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem), *Math. Annalen,* **67** (1909), 281–300. [Viz též: *Gesammelte Abhandlungen. Erster Band. Zahlentheorie,* Springer, Berlin 1932.]

[11] D. Hilbert, Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongreß zu Paris 1900, *Nachrichten von der Königliche Gesellschaft der Wissenschaften zu Göttingen,* (1902), 253–297. [Viz *Gesammelte Abhandlungen,* Springer, Berlin 1932, strany 290–329.]

[12] E. Hlawka, J. Schoissengaier and R. Taschner, *Geometric and Analytic Number Theory,* Springer, Berlin 1991.

[13] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,* Springer, New York 1990.

[14] N. Jacobson, *Basic Algebra. I,* Freeman, San Francisko 1974.

[15] J. P. Jones, Universal diophantine equation, *J. Symbolic Logic,* **47** (1982), 549–571.

[16] J. P. Jones and Y. V. Matijasevič, Proof of recursive unsolvability of Hilbert's Tenth Problem, *Amer. Math. Monthly,* **98** (1991), 689–709.

[17] J.-M. Kantor, Hilbert's problems and their sequels, *Mathem. Intell.,* **18** (1996), 21–30.

[18] M. Klazar, O řešení diofantické rovnice $x^2 - y^3 = \pm 1$, *Matematické obzory,* **32** (1989), 47–53.

[19] D. Kornhauser, On the smallest solution to the general binary quadratic diophantine equation, *Acta Arith.,* **55** (1990), 83–94.

[20] S. Lang, Mordell's review, Siegel's letter to Mordell, Diophantine geometry, and 20th century mathematics, *Notices Amer. Math. Soc.,* **42,3** (1995), 339–350.

[21] S. Lang, Review of Mordell's Diophantine Equations, *Bull. Amer. Math. Soc.,* **76** (1970), 1230–1234.

[22] S. Lang, *Fundamentals of Diophantine Geometry,* Springer, Berlin 1983.

[23] S. Lang, *Number Theory III: Diophantine Geometry,* Springer, Berlin 1991. [Encyklopaedia of Mathematical Sciences, sv. 60.]

[24] D. Marker, Model theory and exponentiation, *Notices of the Amer. Math. Soc.,* **43,7** (1996), 753–759.

[25] Yu. Matijasevich, My collaboration with Julia Robinson, *Mathem. Intell.,* **14** (1992), 38–45. [Addendum ibidem 1993, 75.]

[26] Yu. V. Matiyasevich, *Hilbert's Tenth Problem,* The MIT Press, Cambridge, MA 1993.

[27] L. J. Mordell, *Diophantine Equations,* Academic Press, London 1969.

[28] L. J. Mordell, Indeterminate equations of the third and fourth degrees, *Quart. J. Pure and Appl. Math.,* **45** (1914), 170–186.

[29] L. J. Mordell, Review of Lang's Diophantine Geometry, *Bull. Amer. Math. Soc.,* **70** (1964), 491–498.

[30] M. Nathanson, *Additive Number Theory. The Classical Bases,* Springer, Berlin 1996.

[31] A. Nerode, A decision method for p-adic integral zeros for diophantine equations, *Bull. Amer. Math. Soc.,* **69** (1963), 513–517.

[32] K. M. Podnieks, *Vokrug Tĕoremy Gedĕlja,* Zinatnĕ, Riga 1992.

[33] C. Reid, *Hilbert,* Copernicus (Springer), New York 1996. [Druhé vydání, první v r. 1970.]

[34] P. Ribenboim, *Fermat's Last Theorem for Amateurs,* Springer, Berlin 2000.

[35] P. Ribenboim, *13 Lectures on Fermat's Last Theorem,* Springer, Berlin 1979.

[36] P. Ribenboim, *Catalan's Conjecture. Are 8 and 9 the Only Consecutive Powers?,* Academic Press, Boston 1994.

[37] P. Ribenboim, Some fundamental methods in the theory of diophantine equations, 635–663. In: J. A. Barroso (ed.), *Aspects of Mathematics and its Applications,* Elsevier, Amsterdam 1986.

[38] J. Roberts, *Lure of the Integers,* Mathematical Association of America, USA 1992.

[39] C. Runge, Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, *J. reine und angew. Math.,* **100** (1887), 425–435.

[40] C. L. Siegel, Zur Theorie der quadratischen Formen, *Nachrichten der Akademie der Wissenschaften in Göttingen. II. Matematisch-Physikalische Klasse,* **3** (1972), 21–46.

[41] T. Skolem, *Diophantische Gleichungen,* Springer, Berlin 1938.

[42] N. P. Smart, *The Algoritmic Resolution of Diophantine Equations,* Cambridge University Press, Cambridge, UK 1998.

[43] V. G. Sprindžuk, *Klassičeskije Diofantovy Uravněnija ot Dvuch Něizvěstnych,* Nauka, Moskva 1981. [Anglické vydání: V. G. Sprindzhuk, Classical Diophantine Equations. Lecture Notes in Mathematics 1559, Springer, Berlin 1993.]

[44] A. Tarski, *A Decision Method for Elementary Algebra and Geometry,* US Air Force Project Rand, Santa Monica, USA 1948. [K tisku připravil J. C. C. McKinsey, 60 stran.]

[45] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. Math., II,* **141** (1995), 553–572.

[46] R. Tijdeman, On the equation of Catalan, *Acta Arithm.,* **29** (1976), 197–209.

[47] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math., II,* **141** (1995), 443–551.