

Seriál III. – Jak vyžrát na diofantické rovnice?

V dalším díle našeho oblíbeného seriálu si povíme, jak řešit nejrůznější zašmodrchané diofantické rovnice. Co to ale taková diofantická rovnice je? Jde prostě o nějakou rovnici, která je zvláštní tím, že se zajímáme jenom o její celočíselná řešení.¹ Jak už to tak bývá, „diofantické“ se takovýmto rovnicím říká podle Řeka Diofanta z Alexandrie. Ten žil někdy kolem roku 250 před Kristem, a přestože nebyl první, kdo takovéto rovnice řešil, jmenují se po něm.

My si postupně ukážeme finty a postupy, které zaberou na všemožné rovnice. Tento díl seriálu je tedy zčásti pojatý jako jakýsi přehled nejznámějších metod řešení diofantických rovnic. Zvlášť na jeho začátku se tedy může snadno stát, že leccos z toho, o čem tady píšeme, už znáš. Ani v takovém případě však ještě není vše ztraceno a nemusíš zoufat! (: Ke konci seriálu bys měl najít věci, které jsi ještě nepotkal a nad jejichž pozoruhodností Ti srdce zaplesá (:²

Mocniny a kongruence

Než se budeme moci pustit do řešení rovnic, bude se nám hodit si připomenout i něco o řešení kongruencí. Často totiž při řešení diofantické rovnice pomůže podívat se na zadanou rovnost modulo nějaké vhodně zvolené číslo.

Jedním ze základních nástrojů při práci s kongruencemi a mocninami je malá Fermatova věta (a případně Eulerova věta). I my je dnes občas využijeme, připomeňme si tedy, co říkají.

Malá Fermatova věta: Mějme prvočíslo p a celé číslo a , které není dělitelné p . Pak platí $a^{p-1} \equiv 1 \pmod{p}$.

Eulerova věta: Mějme $m \in \mathbb{N}$, $m \neq 1$ a celé číslo a , které je s m nesoudělné. Pak $a^{\varphi(m)} \equiv 1 \pmod{m}$, kde $\varphi(m)$ je Eulerova funkce. Pokud je $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, kde $p_1, \dots, p_k$ jsou po dvou různá prvočísla, $k \in \mathbb{N}$ a $\alpha_1, \dots, \alpha_k \in \mathbb{N}$, je $\varphi(m) = m(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$.

Ačkoli na řešení kongruencí existují i sofistikovanější metody (které jsou ale bohužel většinou neelementární), pro naše účely bude stačit, když si ukážeme, jak řešit kongruence zkoušením. K tomu se nám bude hodit následující jednoduchá věta.

Věta. (o polynomech a kongruencích) Mějme polynom $P(x)$ s celočíselnými koeficienty,³ přirozené číslo m a celá čísla a a b . Pokud $a \equiv b \pmod{m}$, pak také $P(a) \equiv P(b) \pmod{m}$.

Důkaz. Ač se může zdát, že je tento důkaz nepříjemně přeplněn nejrůznějšími písmenky, není na něm nic těžkého. Prostě jenom dosadíme čísla a, b do polynomu a hodnoty porovnáme. Pustíme se tedy do toho. (:

Označme $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ pro nějaké $n \in \mathbb{N}$ a $a_n, \dots, a_1, a_0 \in \mathbb{Z}$. Víme, že $a \equiv b \pmod{m}$, a tedy také $a^k \equiv b^k \pmod{m}$ pro všechna k (využíváme jednu ze základních vlastností kongruencí – to, že kongruenci můžeme umocnit na jakékoli přirozené číslo). Vynásobením číslem a_k dostáváme, že platí $a_k a^k \equiv a_k b^k \pmod{m}$. Sečteme-li všechny tyto kongruence pro $k = 0, 1, \dots, n$, dostaneme $a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0 \equiv a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 \pmod{m}$, neboli $P(a) \equiv P(b) \pmod{m}$.

Tato věta se nám velice hodí v situaci, kdy nás zajímá, jakých hodnot nabývá daný polynom modulo nějaké číslo. A to se nám může hodit při řešení rovnic, často to totiž dopadne tak, že polynom všech možných hodnot nenabývá.

¹Aspoň většinou. Často také budeme studovat řešení v přirozených číslech a občas dokonce i mezi čísly racionálními.

²Aspoň v to teda doufám. (:

³To znamená, že $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ pro nějaké $n \in \mathbb{N}$ a $a_n, \dots, a_1, a_0 \in \mathbb{Z}$.



Příklad. Urči všechny možné hodnoty $x^2 \bmod 5$.

Řešení. Každé celé číslo x je modulo 5 kongruentní s jedním z čísel 0, 1, 2, 3, 4, označme je na chvíli třeba a . Nás zajímá, kolik je $x^2 \bmod 5$, podle výše uvedené věty je $x^2 \equiv a^2 \pmod{5}$. Abychom tedy našli všechny možné hodnoty $x^2 \bmod 5$, stačí, když spočteme hodnoty $a^2 \bmod 5$ pro $a = 0, 1, 2, 3, 4$. To je ale jenom 5 čísel, můžeme je tedy jedno po druhém zkusit dosadit. Zjistíme, že $a^2 \pmod{5}$ může být jen 0, 1 nebo 4.

Příklad. Dokaž, že pokud 7 dělí $x^2 + y^2$, pak 7 dělí jak x tak y .

Řešení. Zkusme zjistit, kdy se může stát, že $7 \mid x^2 + y^2$. Jde nám tedy o to, kdy je $x^2 + y^2 \equiv 0 \pmod{7}$. Podobně jako v předchozím příkladě můžeme spočítat, že $x^2 \pmod{7}$ může být jen 0, 1, 2 a 4, stejně tak samozřejmě i pro y^2 . Máme tedy dvě čísla (x^2 a y^2) z množiny $\{0, 1, 2, 4\}$, taková, že jejich součet je 0 modulo 7. Po chvilce zkoušení (nebo bychom si třeba mohli udělat tabulku všech možných součtů) zjistíme, že se to může stát jenom tehdy, když jsou obě čísla 0. Máme tedy $x^2 \equiv 0 \equiv y^2 \pmod{7}$, a proto také $x \equiv 0 \equiv y \pmod{7}$, což je to, co jsme chtěli dokázat.

Občas se nám také může hodit určit, jakých hodnot nabývá nějaká exponenciální funkce – třeba $2^a \pmod{5}$. V takovémto případě má člověk často tendenci si říct: „Nu, počítáme modulo 5, tak tedy vyzkouším dosadit všechny možné hodnoty $a \bmod 5$, tedy čísla 0, 1, 2, 3, 4.“ To je ale špatně! Vždy musíme být schopni nějak zdůvodnit, že stačí dosadit ty hodnoty, které dosazujeme. A v tomto případě ale (na rozdíl od dosazování do polynomu) neplatí, že pokud $a \equiv b \pmod{5}$, pak také $2^a \equiv 2^b \pmod{5}$.

Může nám pomoci třeba malá Fermatova věta, která v tomto případě říká, že $2^4 \equiv 1 \pmod{5}$. Pokud tedy $a \equiv b \pmod{4}$, je $a = b + 4k$ pro nějaké $k \in \mathbb{Z}$. Pak $2^a = 2^{b+4k} = 2^b 2^{4k} = 2^b (2^4)^k \equiv 2^b 1^k = 2^b \pmod{5}$, neboli $2^a \equiv 2^b \pmod{5}$. Protože je každé celé číslo a kongruentní s nějakým z čísel $b = 0, 1, 2, 3$ modulo 4, stačí vyzkoušet dosadit tyto hodnoty.

Kdybychom určovali hodnoty $2^k \pmod{m}$ pro složené m , nemohli bychom použít malou Fermatovu větu. V takovém případě se hodí Eulerova věta, nesmíme jen zapomenout ověřit předpoklad, zda je (v tomto případě) umocňované číslo 2 nesoudělné s m . Obecně tedy můžeme víceméně říci, že při počítání modulo m „dole“⁴ zkoušíme všechny možné zbytky modulo m , zatímco „nahore“⁵ dosazujeme všechny hodnoty modulo $\varphi(m)$. A kdyby nás zajímalo to, jakých hodnot nabývá funkce 5^{7^x} modulo m , zkoušeli bychom hodnoty x modulo $\varphi(\varphi(m))$ – samozřejmě jen pokud by byly splněné předpoklady obou Eulerových vět, které bychom potřebovali použít. (Pokud Ti to není jasné, zkus si to rozmyslet. (:)

Ještě složitější může být situace v případě komplikovanější funkce – zkus si třeba rozmyslet, jaké hodnoty by bylo potřeba dosazovat, kdybychom chtěli určit všechny možné hodnoty $x^x \pmod{7}$ nebo $x^x \pmod{10}$.

Na závěr této sekce se zmiňme o tom, že se věta o polynomech a kongruencích může hodit i k řešení úloh o polynomech. Opět si to předvedeme na příkladu.

Příklad. Najdi všechny polynomy $P(x)$ s celočíselnými koeficienty takové, že $P(5) = 7$ a přitom $P(8) = 8$.

Řešení. Nuže, zkusme nějak použít uvedenou větu. Můžeme si třeba všimnout, že platí $5 \equiv 8 \pmod{3}$ (s 5 a 8 počítáme proto, že se vyskytují v zadání, 3 jsme zvolili třeba proto, že je to

⁴Tím myslíme například ve funkcích $x, x^2, 3x^{18} + x^{23}, \dots$ – jde o to, že neznámá x je tu umocňovaná.

⁵Tedy v exponentu, třeba u funkcí $5^x, 13^x, \dots$

rozdíl těchto čísel). Podle věty by tedy mělo být $P(5) \equiv P(8) \pmod{3}$. Ovšem podle zadání by mělo být $7 = P(5) \equiv P(8) = 8 \pmod{3}$. To ale zjevně neplatí, žádný celočíselný polynom tedy zadání nemůže vyhovovat.

Cvičení.

- (1) Najdi všechna řešení kongruence $x^2 \equiv 3 \pmod{7}$.
- (2) Urči všechny možné hodnoty $x^2 \pmod{4}$.
- (3) Najdi všechna celá čísla x taková, že $7 \mid x^3 + 1$.
- (4) Urči všechny možné hodnoty $2^a \pmod{7}$.
- (5) Najdi všechny polynomy $P(x)$ s celočíselnými koeficienty takové, že $P(7) = 22$ a $P(19) = 42$.
- (6) Najdi všechna celá čísla x taková, že $x^{12} \equiv 3 \pmod{11}$.
- (7) Urči všechny možné hodnoty $x^x \pmod{7}$.

Lineární rovnice

Příklad. Najděte všechna celočíselná řešení rovnice $4x + 14y + 21z = 5$.

Řešení. Vezměme si nějaké řešení (x, y, z) . Zkusme nejprve zjistit, co můžeme říct třeba o x . Abychom si ho mohli z rovnice „vyjádřit“, bylo by nejlepší se zbavit protivných neznámých y a z . To se nám povede třeba tak, že budeme počítat modulo 7 (všimni si, že jsme zvolili 7 coby největší společný dělitel čísel 14 a 21, koeficientů u y a z). Musí platit $4x \equiv 5 \pmod{7}$, (jediným) řešením této kongruence je $x \equiv 3 \pmod{7}$ (pokud Tě to překvapuje, zkus si pročíst minulý díl seriálu). To znamená, že $x = 3 + 7k$ pro nějaké celé číslo k .

Po dosazení do zadání zjistíme, že celou rovnici můžeme vydělit 7, po úpravě dostaneme $2y + 3z = 4k - 1$. Považujme odteď k za parametr a zkusme nyní vyjádřit neznámou y . Počítáním modulo 3 se zbavíme z a dostaneme kongruenci $2y \equiv 4k - 1 \pmod{3}$, jejímž řešením je $y \equiv 2k + 2 \pmod{3}$. Tedy $y = 3l + 2k + 2$ pro nějaké celé číslo k . Dosadíme-li i toto do zadání, po úpravě (tentokrát půjde dělit i 3) dostaneme, že $z = 2l + 1$.

Zjistili jsme tedy, že každé řešení musí být tvaru $x = 7k + 3, y = 2k + 3l + 2, z = 2l + 1$, kde $k, l \in \mathbb{Z}$. Zkouškou (nebo úvahou, že tomu ani jinak být nemůže) zjistíme, že všechny tyto trojice zadanou rovnici vskutku řeší.

A podobně bychom mohli postupovat, i kdybychom potřebovali vyřešit nějakou složitější rovnici. Obecně není těžké dokázat toto tvrzení:

Tvrzení. Mějme nenulová celá čísla $a_1, a_2, \dots, a_n$ pro nějaké $n \in \mathbb{N}$ a celé číslo b . Rovnice $a_1x_1 + a_2x_2 + \dots + a_nx_n = b$ s neznámými $x_1, x_2, \dots, x_n$ má řešení, právě když $\mathcal{NSD}(a_1, \dots, a_n)$ dělí číslo b .

Při řešení takové rovnice bychom si napřed vybrali nějakou neznámou, kterou bychom chtěli vyjádřit – třeba x_n . Abychom se zbavili ostatních neznámých, počítali bychom modulo $D = \mathcal{NSD}(a_1, a_2, \dots, a_{n-1})$. Získanou hodnotu $x_n \pmod{D}$ bychom pak dosadili do zadané rovnice. Potom bychom si vybrali nějakou další neznámou, podobně ji vyjádřili, dosadili ... A takto pořád dál a dál, až bychom znali všechny neznámé. Pak bychom už jen pro jistotu udělali zkoušku, jestli jsme opravdu našli řešení.

A určitě by nás nezaskočila ani o chloupek komplikovanější situace, kdy bychom měli soustavu takovýchto rovnic, jako třeba ve 3. cvičení:⁶

⁶Podobné rovnice a soustavy právě řešil již zmiňovaný Diofantos.

**Cvičení.**

- (1) Najdi všechna celočíselná řešení rovnice $2x + 3y = 5$.
- (2) Najdi všechna celočíselná řešení rovnice $105x + 70y + 42z = 67$.
- (3) Po dvorku pobíhá několik slepic, psů a bezhlavých trojnožců.⁷ Dohromady mají 43 nohou a 10 hlav. Urči, kolik je zvířat od každého druhu.
- (4) Najdi všechna celočíselná řešení rovnice $10x + 28y + 60z + 63t = 41$.

Počítání modulo při řešení rovnic

Pokud jsi nepřeskočil minulou sekci, jistě sis všiml, že jsme k řešení uvedených rovnic přímo zásadním způsobem použili kongruence. Ty se často hodí i při řešení trochu složitějších rovnic. Zvláště když máme podezření,⁸ že zadaná rovnice nemá žádné řešení, není nic krásnějšího, než když se nám povede najít nějaké číslo takové, že modulo toto číslo nemá vzniklá kongruence řešení. Zkusit počítat modulo nějaké číslo se ale hodí i jindy – asi v podstatě vždycky, když nás při řešení diofantické rovnice nenapadá, jak postupovat, se vyplatí zkusit, co se stane, když budeme počítat modulo nějaká malá čísla. Zvláště třeba ta, která se v zadané rovnici přímo vyskytují. Počítáním modulo ně se totiž „zbavíme“ příslušných členů a rovnice se zjednoduší.

Dost už ale teoretických řečí, radši si postup ukažme na několika příkladech.

Příklad. Dokaž, že rovnice $7x^2 + 5y^3 + 14 = 0$ nemá celočíselné řešení.

Řešení. Předpokládejme, že máme nějaké řešení (x, y) . Zkusme se zbavit ošklivého členu $5y^3$. To se nám povede třeba, když budeme počítat modulo 5. Dostáváme $2x^2 + 4 \equiv 0 \pmod{5}$, neboli $x^2 \equiv 3 \pmod{5}$. Jak ale už víme (nebo rychle zjistíme vyzkoušením hodnot 0, 1, 2, 3, 4), vždy platí $x^2 \equiv 0, 1, 4 \pmod{5}$. Kongruence tedy nemůže mít řešení, a tedy řešení nemůže mít ani původní rovnice.

Příklad. Najdi všechna celočíselná řešení rovnice $2^x = 11 + 7y$.

Řešení. Nejprve si všimněme, že pokud je $x < 0$, není 2^x celé číslo. Pravá strana rovnice je ale celé číslo vždy, tato situace tedy nemůže nastat. Dále předpokládejme, že $x \geq 0$.

Z rovnice můžeme přímo vyjádřit $y = \frac{2^x - 11}{7}$. Zajímá nás tedy jen to, kdy je tento zlomek celé číslo. A to odpovídá tomu, kdy je $2^x \equiv 11 \pmod{7}$. Abychom toto zjistili, můžeme použít malou Fermatovu větu – podle ní je totiž $2^6 \equiv 1 \pmod{7}$, stačí tedy vyzkoušet hodnoty $x = 0, 1, 2, \dots, 5$. Dostáváme $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$. Mohli bychom samozřejmě počítat dál a dosadit ještě zbylé hodnoty x , není to ale potřeba. Protože nám vyšla 1 (coby $2^3 \pmod{7}$), vidíme, že dokonce $2^{a+3k} \equiv 2^a \pmod{7}$, a tedy stačí zkoušet jen hodnoty exponentu modulo 3 (jinak řečeno, hodnoty funkce $2^x \pmod{7}$ jsou periodické s periodou 3 – zatímco z malé Fermatovy věty jsme se dozvěděli jen o periodě 6).

Můžeme tedy uzavřít, že $2^x \equiv 11 \pmod{6}$, právě když $x \equiv 2 \pmod{3}$. Zadaná rovnice má tudíž řešení jen pro $x = 3k + 2$, $k \in \mathbb{N}_0$,⁹ potom dopočteme, že $y = \frac{2^{3k+2} - 11}{7}$. Z předchozího víme, že y je opravdu celé číslo, i když to tak nevypadá.

Příklad. Najdi všechna přirozená čísla m, n taková, že $1! + 2! + 3! + \dots + n! = m^2$.

⁷Jak jeho jméno napovídá, takový *bezhlavý trojnožec* nemá chudák žádnou hlavu, ale zato hned 3 nohy.

⁸Nejlépe na základě toho, že to po nás přímo chce zadání. (:

⁹Nesmíme zapomenout, že jsme na začátku zjistili, že x musí být nezáporné. Proto musí být i k nezáporné.

Řešení. Tato rovnice vypadá dost divně, na první pohled není moc jasné, co by s ní šlo dělat. Když nevíme, hodí se zkusit, co se stane, když budeme počítat modulo nějaké (zatím obecné) přirozené číslo k . Dobré je všimnout si toho, že je-li $l \geq k$, je $l! = l \cdot (l-1) \cdots (k+1)k(k-1) \cdots 3 \cdot 2 \cdot 1 \equiv 0 \pmod{k}$. Pokud je tedy $n \geq k$, máme $1! + 2! + 3! + \cdots + (k-1)! \equiv m^2 \pmod{k}$. Hodnota levé strany se tudíž modulo k pro velká n již nemění! Když si ještě vzpomeneme, že $m^2 \pmod{k}$ nikdy nenabývá všech možných hodnot, máme skoro vyhráno – stačí totiž najít k takové, že $1! + 2! + 3! + \cdots + (k-1)!$ nebude modulo k druhou mocninou. Pustíme se tedy systematicky do hledání:

$k = 2$: $1! = 1$ může být druhou mocninou modulo 2.

$k = 3$: $1! + 2! = 3 \equiv 0 \pmod{3}$ je druhou mocninou.

$k = 4$: $1! + 2! + 3! = 9 \equiv 1 \pmod{4}$ zase může být druhou mocninou.): Už by se nám chtělo začít zoufat, že to nikam nepovede, zkusme ale ještě chvilku vydržet!

$k = 5$: $1! + 2! + 3! + 4! = 33 \equiv 3 \pmod{5}$. Přitom ale $x^2 \equiv 0, 1, 4 \pmod{5}$, takže toto není možné!

Zjistili jsme tedy, že pokud $n \geq 5$, rovnice nemá řešení. Teď už jenom vyzkoušíme 4 zbývající hodnoty n . Pro $n = 1$ dostáváme řešení $m = 1$, pro $n = 2, 4$ rovnice žádné řešení nemá, ale pro $n = 3$ máme ještě jedno řešení $m = 3$. A je to! (:

Cvičení.

- (1) Najdi všechna celočíselná řešení rovnice $7x^2 + 5y = 13$.
- (2) Najdi všechna celočíselná řešení rovnice $x(x+3) = 4y - 1$.
- (3) Najdi všechna celočíselná řešení rovnice $3x^2 - 4y^2 = 13$.
- (4) Najdi všechna celočíselná řešení rovnice $2^a = 8 - 5b$.

Což takhle použít nějakou nerovnost?

Užitečným trikem pro řešení rovnic může být použití nerovností. Jednou takovou nerovností je třeba $x^2 \geq 0$ pro všechna celá čísla x :

Příklad. Najděte všechna celočíselná řešení rovnice $a^2 + 3b^2 = 13$.

Řešení. Víme, že musí platit $a^2 \geq 0$, a tedy dostáváme $13 = a^2 + 3b^2 \geq 3b^2$. Tuto nerovnost ale splňují jen $b \in \{-2, -1, 0, 1, 2\}$. Vidíme, že b může nabývat jen konečně mnoha různých hodnot. Není tedy žádný problém každou z nich zkusit dosadit do zadané rovnice a zjistit, pro které z nich dostaneme nějaké řešení. Vyjde nám, že rovnice má čtyři řešení $(1, 2)$, $(-1, 2)$, $(1, -2)$, $(-1, -2)$.

Dalším užitečným faktem, který souvisí s nerovnostmi, je tento:

Tvrzení. (o po sobě jdoucích mocninách) *Mějme přirozené číslo n . Neexistují celá čísla a, b taková, že $a^n < b^n < (a+1)^n$.*

Není vůbec těžké si rozmyslet, proč toto tvrzení platí. Necháme to tedy jako cvičení a radši si ukážeme, jak se toto tvrzení hodí při řešení rovnic.

Příklad. Najdi všechna celočíselná řešení rovnice $x^2 = y(y+2)$.

Řešení. Předpokládejme, že x, y řeší zadanou rovnici a rozlišíme dva případy podle toho, jestli je y záporné.

(a) $y \geq 0$: Pak zřejmě platí $y^2 \leq y^2 + 2y = y(y+2) < y^2 + 2y + 1 = (y+1)^2$. Protože $x^2 = y(y+2)$, nemůže být první z nerovností ostrá, a tedy musí být $y^2 = y^2 + 2y$ a $y = 0$. Pak dostáváme $x = 0$, dvojice $(0, 0)$ je zjevně řešením dané rovnice.



(b) $y < 0$: Označme $z = -y > 0$. Zadaná rovnice pak je tvaru $x^2 = z^2 - 2z$. Vidíme, že $z^2 - 2z < z^2 - 2z + 1 = (z - 1)^2$. Chceme opět dostat, že by x^2 mělo ležet mezi dvěma po sobě jdoucími druhými mocninami, zkusme tedy zjistit, pro která z platí $(z - 2)^2 < z^2 - 2z$. Roznásobením zjistíme, že to nastane, právě když $z > 2$. Kdyby tedy bylo $z > 2$, platilo by $(z - 2)^2 < z^2 - 2z = y(y + 2) = x^2 < (z - 1)^2$, což ale odporuje tvrzení o po sobě jdoucích mocninách. Zbývají nám tedy jen možnosti $-y = z = 1$ a $-y = z = 2$. Pro $y = -1$ zadaná rovnice řešení nemá; pro $y = -2$ dostáváme řešení $(0, -2)$.

Cvičení.

- (1) Najdi všechna celočíselná řešení rovnice $6x^2 + 5y^2 = 74$.
- (2) Najdi všechna celočíselná řešení rovnice $(x + 3)^3 - x^3 = y^2$ taková, že $x \geq 0$.
- (3) Najdi všechna celočíselná řešení rovnice $(x + 2)^4 - x^4 = y^3$ taková, že $x \geq 0$.

Rozlož to!

Věta. Každé celé číslo jde jednoznačně (až na pořadí) rozložit na součin prvočísel.

Toto známé tvrzení má spoustu různých využití v teorii čísel, mimo jiné se také může hodit při řešení diofantických rovnic.

Příklad. Najdi všechna celočíselná řešení rovnice $x^2 = y^2 + p$, kde p je prvočíslo.

Řešení. Jednoduchou úpravou převedeme rovnici do tvaru $(x - y)(x + y) = p$. Protože je p prvočíslo, dá se vyjádřit jako součin jen čtyřmi způsoby: $p = 1 \cdot p$, $p = (-1) \cdot (-p)$, $p = (-p) \cdot (-1)$ a $p = p \cdot 1$. Máme tedy jen čtyři možnosti:

- (a) $x - y = 1, x + y = p$. Vyřešením soustavy lineárních rovnic dostaneme $x = \frac{p+1}{2}, y = \frac{p-1}{2}$.
- (b) $x - y = -1, x + y = -p$. Dostáváme $x = -\frac{p+1}{2}, y = -\frac{p-1}{2}$.
- (c) $x - y = -p, x + y = -1$. Dostáváme $x = -\frac{p-1}{2}, y = -\frac{p+1}{2}$.
- (d) $x - y = p, x + y = 1$. Dostáváme $x = \frac{p-1}{2}, y = \frac{p+1}{2}$.

Teď už si jen nesmíme zapomenout ověřit, jestli jsou opravdu x, y celá čísla. Pokud je p liché, tak ano, pro $p = 2$ ale ne. Můžeme tedy uzavřít, že pro $p = 2$ nemá rovnice žádné řešení a pro $p \neq 2$ má čtyři řešení uvedená výše.

Podobně můžeme vyřešit řadu rovnic, když se nám povede je převést do tvaru, kdy na obou stranách rovnice je součin. Trikem, který nám k tomu někdy může pomoci, je identita $(x - 1)(y - 1) = xy - x - y + 1$.

Ale je potřeba dávat pozor! Když třeba dostaneme rovnici do tvaru $ab = cd$, svádí to k omylu, že $a = c$ a $b = d$ nebo $a = d, b = c$ (a ještě případně možnosti s opačnými znaménky). Tak to ale vůbec nemusí být – například $a = 10, b = 21, c = 6, d = 30$ je také řešení dané rovnice. Pokud ale víme, že aspoň některé součinitele jsou nesoudělné, můžeme toho s výhodou využít, třeba za pomoci následujícího tvrzení.

Tvrzení. Mějme nesoudělná celá čísla a, b a přirozené číslo n . Pokud je součin ab n -tá mocnina nějakého celého čísla, je $a = eu^n$, $b = ev^n$ pro nějaká celá čísla u, v a $e = \pm 1$ (čísla a, b tedy jsou, až na znaménko, také n -té mocniny).

Důkaz. Dokázat toto tvrzení není vůbec složité. Jen si napíšeme prvočíselné rozklady čísel a a b a zjistíme, že exponent u každého prvočísla musí být násobkem n :

Nechť tedy $a = xp_1^{\alpha_1} \cdots p_k^{\alpha_k}$ a $b = yq_1^{\beta_1} \cdots q_l^{\beta_l}$, kde $p_1, \dots, p_k$ jsou po dvou různá prvočísla, $q_1, \dots, q_l$ jsou po dvou různá prvočísla, $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l \in \mathbb{N}$ a $x, y = \pm 1$. Protože jsou čísla a, b nesoudělná, musí být $p_i \neq q_j$ pro všechna i, j , takže $ab = (xy)p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$ je rozklad čísla ab na součin (po dvou různých) prvočísel.

Podle předpokladu víme, že $ab = w^n$ pro nějaké $w \in \mathbb{Z}$. Označme ještě $w = zr_1^{\gamma_1} \cdots r_m^{\gamma_m}$ rozklad čísla w na součin prvočísel (r_i jsou po dvou různá prvočísla, $\gamma_i \in \mathbb{N}$, $z = \pm 1$). Pak $(xy)p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l} = ab = w^n = z^n r_1^{n\gamma_1} \cdots r_m^{n\gamma_m}$. Protože je rozklad čísla na součin prvočísel jednoznačný, mohou se tyto dva rozklady čísla ab od sebe lišit jen pořadím prvočísel. Je tedy $xy = z^n$, $m = k + l$. Bez újmy na obecnosti můžeme předpokládat, že $r_1 = p_1, r_2 = p_2, \dots, r_k = p_k, r_{k+1} = q_1, r_{k+2} = q_2, \dots, r_m = q_l$, potom $\alpha_i = n\gamma_i, \beta_j = n\gamma_{j+k}$ pro všechna i, j . Je tedy $a = x(p_1^{\gamma_1} \cdots p_k^{\gamma_k})^n, b = y(q_1^{\gamma_{k+1}} \cdots q_l^{\gamma_m})^n$, obě čísla jsou tudíž až na znaménko n -té mocniny. Dořešit situaci se znaménky už není těžké.

Příklad. Najdi všechna celočíselná řešení rovnice $x^2 + 3x = y^3 - 2$.

Řešení. Zkusme rovnici upravit tak, abychom na obou stranách dostali součin. Po chvilce snažení se nám třeba povede přijít na úpravu do tvaru $(x+1)(x+2) = y^3$. Pokud je $x = -1$ nebo -2 , dostáváme řešení pro $y = 0$. Dále předpokládáme, že x není -1 ani -2 .¹⁰

Obě čísla $x+1$ a $x+2$ jsou pak nenulová. Protože jde o dvě po sobě jdoucí celá čísla, jsou nesoudělná (každý jejich společný dělitel totiž musí dělit i jejich rozdíl, což je 1). Součin těchto dvou čísel je třetí mocnina, můžeme tedy použít tvrzení. Dostáváme, že $x+1 = eu^3$ a $x+2 = ev^3$ pro nějaká celá čísla u, v a $e = \pm 1$. Teď bychom mohli rozebrat dva případy podle toho, jestli je e 1 nebo -1 , není to ale potřeba. Kdyby totiž bylo $e = -1$, mohli bychom položit $u' = -u$ a $v' = -v$. Pak by platilo $x+1 = u'^3$ a $x+2 = v'^3$, takže bychom byli ve stejné situaci, jako když $e = 1$. V podstatě se tedy nemusíme znaménkem e zabývat, protože ho můžeme „schovat“ do třetí mocniny – to jde díky tomu, že 3 je liché číslo, a tedy $(-1)^3 = -1$.

Máme $x+1 = u^3$ a $x+2 = v^3$, odkud odečtením dostaneme, že $1 = v^3 - u^3 = (v-u)(v^2 + uv + u^2)$. Opět máme na obou stranách rovnice součin, tentokrát jsou jen dvě možnosti: buďto je $v-u = 1$ a $v^2 + uv + u^2 = 1$, nebo $v-u = -1$ a $v^2 + uv + u^2 = -1$. V prvním případě je $v = u+1$ a když dosadíme do druhé rovnice a vyřešíme kvadratickou rovnici, dostaneme dvě řešení $u = 0, v = 1$ a $u = -1, v = 0$. V druhém případě soustava řešení nemá. Ze dvou nalezených řešení ale dostaneme jen už známá řešení $x = -1$ nebo -2 , zadaná rovnice tedy žádná další řešení nemá.

Cvičení.

- (1) Najdi všechna celočíselná řešení rovnice $x^2 = y^2 + 13$.
- (2) Najdi všechna celočíselná řešení rovnice $xy = x + y$.
- (3) Najdi všechna celočíselná řešení rovnice $x(x+2y) = p + 3y^2$, kde p je prvočísl.
- (4) Najdi všechna celočíselná řešení rovnice $x(x+1)(x+2)(x+3) = y^2$.
- (5) Najdi všechna celočíselná řešení rovnice $1 + x + x^2 + x^3 = 2^y$.

Nekonečný sestup

Nekonečný sestup je jeden z pozoruhodných a možná i překvapivých způsobů, jak řešit diofantické rovnice. Ačkoli je totiž založený na zcela triviálním pozorování, a sice že neexistuje nekonečná

¹⁰Tento předpoklad děláme proto, abychom mohli bez problémů hovořit o nesoudělnosti čísel $x+1, x+2$. Záleží na tom, jak definujeme NSD, často ale právě nebývá definovaný, pokud je jedno z čísel 0.



ostře klesající posloupnost přirozených čísel, dají se s jeho pomocí dělat hotové divy. Někaký takový způsob nejspíš už Pythagorejci použili k důkazu, že $\sqrt{2}$ je iracionální číslo (a objevitele tohoto faktu pak ostatní za odměnu zabili). Tuto metodu ale proslavil hlavně Fermat, který s její pomocí vyřešil řadu diofantických rovnic. Jak už jsme naznačili, je založená na jednoduchém tvrzení, které ani nebudeme dokazovat.¹¹

Věta. *Neexistuje nekonečná posloupnost přirozených čísel $a_1, a_2, a_3, \dots$ taková, že $a_1 > a_2 > a_3 > \dots$.*

Jak se toho dá využít k řešení rovnic? Třeba takto:

Příklad. Najdi všechna celočíselná řešení rovnice $x^3 = 2y^3 + 4z^3$.

Řešení. $x = y = z = 0$ je jistě řešením zadané rovnice. Předpokládejme, že rovnice má nějaké řešení takové, že aspoň jedna z neznámých je nenulová. 2 dělí pravou stranu rovnice, takže 2 musí dělit x^3 , a tedy i x . Označme $x_1 = 2x$. Po dosazení dostáváme $4x_1^3 = y^3 + 2z^3$, odkud vidíme, že $2 \mid y^3$, a tedy $2 \mid y$. Můžeme tedy položit $y = 2y_1$, pak dostaneme $2x_1^3 = 4y_1^3 + z^3$. Tentokrát 2 musí dělit z , necht $z = 2z_1$. Po dosazení obdržíme rovnici $x_1^3 = 2y_1^3 + 4z_1^3$.

To je ale úplně stejná rovnice, jako na začátku! Jen teď každou z neznámých máme s indexem 1. Můžeme tedy postupovat úplně stejně jako v předchozím odstavci a postupně dostat $x_1 = 2x_2$, $y_1 = 2y_2$ a $z_1 = 2z_2$ a rovnici $x_2^3 = 2y_2^3 + 4z_2^3$. Teď zase máme $x_2 = 2x_3$, $y_2 = 2y_3$ a $z_2 = 2z_3 \dots$ a takto bychom mohli pokračovat pořád dál a dál. Máme tedy posloupnosti čísel $x, x_1, x_2, x_3, \dots$, $y, y_1, y_2, y_3, \dots$ a $z, z_1, z_2, z_3, \dots$, která odpovídají řešením naší rovnice. Na začátku jsme předpokládali, že aspoň jedna z neznámých je nenulová. Ať je to třeba x . Pak také $x_i \neq 0$ pro všechna i . Absolutní hodnota čísla x a všech x_i je tedy kladná, protože $x_{i+1} = x_i/2$, je $|x_{i+1}| < |x_i|$. Máme tedy posloupnost přirozených čísel $|x| > |x_1| > |x_2| > |x_3| > \dots$. Ta ale podle věty existovat nemůže! Dostali jsme spor, rovnice tedy má jediné řešení $x = y = z = 0$.

Už je Ti možná i jasné, proč se této metodě říká nekonečný sestup. Začneme totiž s nějakým řešením a z něj postupně vyrábíme menší a menší řešení, jejich hodnota „nekonečně sestupuje“. (: To ale není možné.

V uvedeném příkladu bylo úplně jasné, jak vyrábět menší řešení. Občas to může být trochu složitější – v 1. ze cvičení se třeba hodí použít předposledního příkladu z odstavce o mocninách a kongruencích.

Cvičení.

- (1) Najdi všechna celočíselná řešení rovnice $x^2 + y^2 = 7z^2$.
- (2) Dokaž, že $\sqrt{2}$ je iracionální číslo.
- (3) $x^3 + 2y^3 + 4y^3 = 6xyz$
- (4) $x^2 + y^2 = x^2y^2$
- (5) $x^2 + xy + y^2 = x^2y^2$

I geometrie se někdy hodí

A teď už přichází slibovaný zlatý hřeb celého dnešního seriálu. Je jím postup, jak vyřešit leccakou rovnici pomocí geometrických představ. To může být docela překvapivé a zajímavé – na první

¹¹Tato vlastnost přirozených čísel se totiž občas bere za jeden z axiomů – nejčastěji ve formulaci, že každá neprázdná podmnožina přirozených čísel má nejmenší prvek. Můžeš si rozmyslet, že je to ekvivalentní s naší větou a také s principem matematické indukce.

pohled totiž zdaleka není jasný, jak by nějaké geometrické čmáranice mohly souviset s čistě ne-geometrickým problémem – s řešením diofantických rovnic. Takovéto nečekané souvislosti a finty se v matematice občas objeví – a právě ty jsou pro leckoho tím, co ho na matematice zajímá a baví.

Aby se nám lépe vyjadřovalo, definujeme si nejprve několik užitečných pojmů (většinou ale nejde o nějaké všeobecně rozšířené názvy, takže kdybys je chtěl používat třeba v olympiádě, asi by stálo za to uvést v řešení i jejich definice). Mějme rovinu se souřadnicovým systémem s osami x a y . Každý bod tedy ztotožníme s dvojicí reálných čísel – jeho souřadnic.¹²

Definice. Bod (x, y) nazveme racionálním bodem, pokud $x, y \in \mathbb{Q}$.

Kromě bodů ale v rovině leží i přímky. Každá přímka jde vyjádřit jako množina bodů, které splňují $ax + by = c$ pro nějaká reálná čísla a, b, c (taková, že aspoň jedno z čísel a, b není 0). Uvědomme si ještě, že rovnici každé přímky můžeme upravit buď do tvaru $x = q, q \in \mathbb{R}$ (pokud $b = 0$, a přímka je tedy rovnoběžná s osou y) nebo $y = kx + l, k, l \in \mathbb{R}$ (to pokud $b \neq 0$).

Definice. Přímku s rovnicí $ax + by = c$ nazveme racionální přímkou, pokud $a, b, c \in \mathbb{Q}$.

Věta. (o spojnici) Spojnice dvou racionálních bodů je racionální přímka.

Důkaz. Označme souřadnice bodů $(k, l), (m, n)$. Rozmysli si, že spojnice těchto bodů má rovnici $(n - l)x + (k - m)y = kn - lm$, a tedy jde o racionální přímku (pokud se Ti zdá divné, že ta rovnice takto spadla z nebe a zajímalo by Tě, jak se na to dá přijít, není to těžké – stačí do obecné rovnice přímky postupně dosadit souřadnice našich dvou bodů a zjistit, pro která a, b, c vzniklé rovnice platí).

A ještě máme v rovině kuželosečky. Za kuželosečku budeme považovat množinu bodů, které splňují rovnici $ax^2 + bxy + cy^2 + dx + ey = f$ pro nějaká reálná a, b, c, d, e, f (taková, že aspoň jedno z čísel a, b, c, d, e není 0). Rozhodně se nenechej odstrašit zdánlivou složitostí této rovnice ani tím, že s kuželosečkách ještě neslyšel. Jediné, co je pro nás na rovnici důležité, je to, že každý ze sčítanců má celkový stupeň nejvýše 2 (neboli že tam není třeba člen x^2y , který má stupeň $2+1=3$).

Definice. Řekneme, že kuželosečka k je netriviální, pokud k není podmnožinou žádné přímky.

S kuželosečkami ses možná už setkal (nebo je ještě potkáš) ve škole. Tam se dozvíš, že netriviálními kuželosečkami jsou kružnice, elipsa, parabola a hyperbola. Není těžké dokázat, že se každá netriviální kuželosečka protíná s libovolnou přímkou nejvýš ve 2 bodech.

Definice. Kuželosečku s rovnicí $ax^2 + bxy + cy^2 + dx + ey = f$ nazveme racionální, pokud $a, b, c, d, e, f \in \mathbb{Q}$.

K tomu, abychom pomocí těchto pojmů mohli začít řešit příklady, budeme potřebovat větu o racionálních bodech na kuželosečkách. Její důkaz snad není příliš složitý, zkus ho tedy přecíst a pochopit. Ještě před tím ale potřebujeme dokázat větu o průsečících. Říká v podstatě to, že když protneme dvě racionální věci (přímku a kuželosečku), dostaneme racionální bod. Její důkaz je bohužel trochu delší – pokud se Ti ale nepodaří se jím prokousat, ničemu by to moc vadit nemělo.

¹²Pokud ses ještě nesetkal s analytickou geometrií, může Ti tato sekce dělat trochu problémy. Zkus se jí prokousat, pokud se Ti to ale nepovede, svět se taky nezboří. (:



Věta. (o průsečících) *Buď k kuželosečka a A racionální bod ležící na k . Pokud je p racionální přímka procházející bodem A taková, že protíná kuželosečku k právě ve dvou bodech A, B , pak je B racionální bod.*

Důkaz. Nechť $ax^2 + bxy + cy^2 + dx + ey = f$, kde $a, b, c, d, e, f \in \mathbb{Q}$, je rovnice kuželosečky k . Souřadnice bodu A označme (u, v) . Uvažujme obecnou přímku p a předpokládejme, že jsou splněny podmínky ze zadání. Rovnice přímky p je buďto tvaru $x = q$ pro $q \in \mathbb{Q}$ nebo tvaru $y = kx + l, k, l \in \mathbb{Q}$.

V prvním případě musí být $q = u$ (neboť bod A leží na p). Bod B je průsečík p a k , jeho souřadnice (r, s) tedy musí splňovat rovnice přímky p i kuželosečky k . Z rovnice p vidíme, že $r = u$. Po dosazení do rovnice k dostáváme, že $cy^2 + y(bu + e) + (au^2 + du - f) = 0$. To je rovnice stupně nejvýše 2, podle předpokladu víme, že má právě 2 kořeny (a to y -ové souřadnice bodů A, B , neboli čísla v, s), musí mít tedy stupeň právě 2 (neboli $c \neq 0$). Z Viětových vztahů¹³ pak vyplývá, že $v + s = -(bu + e)/c$, a tedy $s = v - (bu + e)/c \in \mathbb{Q}$. Protože $r = u$ je také racionální číslo, dokázali jsme, že B je racionální bod.

Druhý případ je obdobný: aby na p ležel bod A , musí platit $v = ku + l$, neboli $l = v - ku$. Přímka má tedy rovnici $y = kx + (v - ku)$. Je-li opět $B = (r, s)$, dostáváme $s = kr + (v - ku)$. x -ové souřadnice průsečíků p a k tedy splňují rovnici $ax^2 + bx(kx + (v - ku)) + c(kx + (v - ku))^2 + dx + e(kx + (v - ku)) = f$ (do rovnice k jsme dosadili y -ovou souřadnici vyjádřenou podle rovnice přímky p). To je opět rovnice stupně nejvýše 2 (s neznámou x). Podle předpokladu má právě dva kořeny u, r , její stupeň je tudíž právě dva a z Viětových vztahů stejně jako předtím dostaneme, že r je racionální. Pak je i $s = kr + (v - ku) \in \mathbb{Q}$, a tedy B je racionální bod.

Věta. (o racionálních bodech na kuželosečkách) *Mějme racionální netriviální kuželosečku k a racionální bod A , který leží na k . Označme M množinu všech racionálních bodů ležících na k a N množinu všech průsečíků¹⁴ kuželosečky k s nějakou racionální přímkou p procházející bodem A . Pak $M = N$.*

Důkaz. Dokážeme, že $M \subseteq N$ a že $N \subseteq M$, z toho pak vyplývá, že $M = N$.

$M \subseteq N$: Potřebujeme dokázat, že každý racionální bod B ležící na k (neboli prvek M) leží také na nějaké racionální přímce p procházející bodem A . To je jednoduché – zvolíme-li za p spojnicu bodů A, B , je to podle věty o spojnici racionální přímka. Bod B tedy je prvkem množiny N .

$N \subseteq M$: Mějme nějaký průsečík B kuželosečky k s racionální přímkou p procházející bodem A . k je netriviální kuželosečka, protíná se tedy s p nejvýše ve 2 bodech, A a B jsou tedy jediné dva průsečíky k a p . Teď můžeme použít větu o průsečících – ta nám říká, že B je racionální bod. A to je přesně to, co jsme chtěli dokázat.

No to je sice všechno hrozně pěkný, ale na co nám to bude při řešení diofantických rovnic? Už se do toho můžeme pustit. (:

Příklad. Najdi všechna celočíselná řešení rovnice $a^2 + b^2 = c^2$ taková, že čísla a, b, c jsou po dvou nesoudělná.

Řešení. Pokud je $c = 0$, má rovnice jediné řešení $a = b = c = 0$ (i když v tomto případě asi nemůžeme mluvit o nesoudělnosti čísel a, b, c , ale to není až tak podstatné). Dále předpokládejme,

¹³Viětovy vztahy pro kvadratické rovnice říkají obecně toto: Máme-li kvadratickou rovnici $at^2 + bt + c = 0$ s neznámou t a kořeny t_1, t_2 , platí $t_1 + t_2 = -b/a, t_1 t_2 = c/a$.

¹⁴Průsečíkem zde, trochu neobvykle, rozumíme jakýkoli společný bod kuželosečky a přímky. Pokud je tedy například přímka tečnou dané kuželosečky, bod dotyku také považujeme za jejich průsečík.

že $c \neq 0$. Protože jsou čísla a, b nesoudělná, nemůžou být obě sudá. Kdyby byla naopak obě lichá, bylo by $a^2 \equiv b^2 \equiv 1 \pmod{4}$, a tedy $c^2 \equiv 1 + 1 = 2 \pmod{4}$, což není možné. Právě jedno z čísel a, b je tedy liché a jedno sudé. Bez újmy na obecnosti předpokládejme, že a je liché a b je sudé.

Označíme-li $x = a/c, y = b/c$, ze zadané rovnice dostaneme rovnici $x^2 + y^2 = 1$. Zajímají nás celočíselná řešení zadané rovnice, kterým odpovídají racionální řešení této nové rovnice. Představíme-li si x, y jako souřadnice bodů v rovině, jde o rovnici nějaké kružnice k (tedy netriviální racionální kuželosečky). Vidíme, že bod $A = (1, 0)$ je racionální bod, který leží na k . Podle věty o racionálních bodech na kuželosečkách tedy každý racionální bod ležící na k (neboli každé řešení naší rovnice) dostaneme jako průsečík k s nějakou racionální přímkou p procházející bodem A . Takto tedy můžeme najít všechna řešení naší rovnice.

Rovnice přímky p je tvaru $x = q, q \in \mathbb{Q}$ nebo $y = kx + l, k, l \in \mathbb{Q}$. V prvním případě je $q = 1$ (aby na p ležel bod A), tato přímka má s kružnicí jediný společný bod A (jde totiž o tečnu ke kružnici v bodě A).

Případ, kdy přímka má rovnici $y = kx + l, k, l \in \mathbb{Q}$, je zajímavější. Aby na p ležel bod A , musí být $l = -k$, rovnice přímky p je tedy $y = kx - k$. Nás zajímají průsečíky této přímky s kružnicí k , dosadíme tedy za y do rovnice kružnice. Dostaneme $x^2 + (kx - k)^2 = 1$, neboli $(k^2 + 1)x^2 - 2k^2x + (k^2 - 1) = 0$. Teď bychom mohli použít známého vzorce pro řešení kvadratické rovnice, jednodušší ale je vzpomenout si, že jeden z kořenů známe a použít Viětovy vztahy. Jedním z průsečíků totiž je bod $A, x = 1$ je tudíž kořenem této rovnice. Označíme-li druhý z kořenů r , dostáváme $1 + r = 2k^2/(k^2 + 1)$, a tedy $r = (k^2 - 1)/(k^2 + 1)$. Druhá souřadnice hledaného průsečíku je $s = kr - k = -2k/(k^2 + 1)$.

Zjistili jsme, že množina všech racionálních bodů na kružnici k je

$$M = \left\{ \left(\frac{k^2 - 1}{k^2 + 1}, \frac{-2k}{k^2 + 1} \right) : k \in \mathbb{Q} \right\} \cup \{(1, 0)\}.$$

Nás ale zajímají řešení zadané rovnice, musíme je tedy ještě z těchto řešení zpátky vydobýt. k je racionální číslo, můžeme ho tedy napsat ve tvaru zlomku $k = -u/v$, kde $u \in \mathbb{Z}, v \in \mathbb{N}, (u, v) = 1$.¹⁵

Pak $\frac{a}{c} = x = \frac{k^2 - 1}{k^2 + 1} = \frac{u^2 - v^2}{u^2 + v^2}$ a $\frac{b}{c} = \frac{-2k}{k^2 + 1} = \frac{2uv}{u^2 + v^2}$. Už už by se nám chtělo uzavřít, že tedy $a = u^2 - v^2, b = 2uv, c = u^2 + v^2$, ale to bychom se unáhli! Nesmíme totiž zapomenout na předpoklad, že čísla a, b, c mají být po dvou nesoudělná, a liché a b sudé.

Jak je to tedy s tou nesoudělností? K tomu nám pomůže následující lemma,¹⁶ které sice není těžké, když víš, jak na takovéto věci jít – ale jinak také může být nejtěžší částí celého příkladu. (:

Lemma. Jsou-li u, v nesoudělná celá čísla, pak:

- (a) pokud jsou obě čísla lichá, je $(u^2 - v^2, u^2 + v^2) = 2$ a také $(2uv, u^2 + v^2) = 2$,
- (b) pokud mají čísla u, v různou paritu,¹⁷ je $(u^2 - v^2, u^2 + v^2) = 1$ a $(2uv, u^2 + v^2) = 1$.

Důkaz. Zkusme určit, kolik je $(u^2 - v^2, u^2 + v^2)$. Ve znění lemmatu už sice máme napsané, jak to má vyjít, ale při řešení příkladu nám to většinou nikdo dopředu neporadí a musíme na

¹⁵Minus jsme si před u vložili proto, aby nám za chvíli vyšly trochu hezčí výrazy. Na věci se tím nic nezmění, jen místo kladného čitatele máme teď záporné u a naopak. Mohli bychom si ale normálně napsat $k = u'/v$ a počítat dál.

¹⁶Lemma v matematice obvykle znamená pomocné tvrzení. Toto slovo středního rodu se trochu zákeřně skloňuje – druhý pád je (bez) lemmatu, 1. pád množného čísla je lemmata, atd.

¹⁷Neboli jedno z nich je sudé a druhé liché.



to přijít sami. Využijeme základních vlastností největšího společného dělitele, zvláště toho, že $(\alpha, \beta) = (\alpha - \beta, \beta)$ pro všechna α, β . Máme tedy $(u^2 - v^2, u^2 + v^2) = (u^2 - v^2, (u^2 + v^2) - (u^2 - v^2)) = (u^2 - v^2, 2v^2)$.

Předpokládejme nyní, že tento NSD není 1, a tudíž existuje nějaké prvočíslo p , které dělí $u^2 - v^2$ i $2v^2$. Pokud p dělí v^2 , dělí také $(u^2 - v^2) + v^2 = u^2$. A protože je p prvočíslo, které dělí u^2 a v^2 , musí také dělit u a v . To je ale ve sporu s předpokladem, že u a v jsou nesoudělná.

Protože p dělí $2v^2$ a nedělí v^2 , musí dělit 2, a tedy $p = 2$. Jediným prvočíslem, které se vyskytuje v rozkladu $(u^2 - v^2, 2v^2)$ na součin prvočinitelů, je tedy 2. Tudíž $(u^2 - v^2, 2v^2) = 2^i$ pro nějaké $i \in \mathbb{N}$.

To, že $2 \mid u^2 - v^2$ nastane, právě když čísla u a v mají stejnou paritu. Obě sudá být nemůžou (nebyla by nesoudělná), musí tedy být obě lichá. Pak ale je i v^2 liché číslo, a proto i nemůže být větší než 1. Naopak 2 opravdu dělí obě čísla $u^2 - v^2$ a $2v^2$, takže $2 = (u^2 - v^2, 2v^2) = (u^2 - v^2, u^2 + v^2)$. Zjistili jsme tedy, že jsou-li u, v lichá čísla, je hledaný NSD roven 2. Jinak (tedy pokud u, v mají různou paritu), je NSD roven 1.

Výpočet $(2uv, u^2 + v^2)$ je podobný, zkus ho jako cvičení.

Kdyby nastal v lemmatu případ a), dostali bychom $a = (u^2 - v^2)/2, b = uv$ a $c = (u^2 + v^2)/2$. Ovšem v tomto případě by b bylo liché, což odporuje našemu BÚNO předpokladu učiněnému na začátku.

Čísla u, v tedy musí mít různou paritu a potom jsou vskutku čísla $a = u^2 - v^2, b = 2uv$ a $c = u^2 + v^2$ po dvou nesoudělná a dávají nám řešení zadané rovnice. Neměli bychom zapomenout ani na řešení odpovídající zbývajícimu racionálnímu bodu na kružnici, tedy bodu A . Pro něj máme $a = 1, b = 0, c = 1$ (což odpovídá výše uvedenému řešení pro $u = 1, v = 0$).

Všechna nesoudělná řešení dané rovnice pak získáme tak, že k už nalezeným řešením ještě přidáme ta, která odpovídají prohození a a b .

Kdyby nás zajímala úplně všechna řešení zadané rovnice, nejen ta nesoudělná, není nic snazšího než každé nesoudělné řešení vynásobit nějakým přirozeným číslem t . (To sice není úplně zřejmé, není ale těžké si rozmyslet, že takto vskutku dostaneme úplně všechna řešení.)

Dokázali jsme tak následující větu:

Věta. (o řešení pythagorejské rovnice¹⁸) *Rovnice $a^2 + b^2 = c^2$ má právě tato celočíselná řešení:*

(i) $a = t(u^2 - v^2), b = 2tuv, c = t(u^2 + v^2)$, kde $t \in \mathbb{N}, u \in \mathbb{Z}, v \in \mathbb{N}_0$ a čísla u, v jsou nesoudělná a mají různou paritu.

(ii) $a = 2tuv, b = t(u^2 - v^2), c = t(u^2 + v^2)$, kde $t \in \mathbb{N}, u \in \mathbb{Z}, v \in \mathbb{N}_0$ a čísla u, v jsou nesoudělná a mají různou paritu.

Výše uvedená řešení jsou po dvou různá.

Tato věta se občas hodí i při řešení jiných diofantických rovnic, stojí tedy za to si ji (aspoň zhruba) pamatovat.

Možná Tě překvapilo, odkud a proč jsme vzali na začátku BÚNO předpoklad o paritě čísel a, b . Bylo to hlavně z tradičních důvodů, řešení pythagorejské rovnice se většinou uvádí v takovém tvaru, jaký je ve větě. Vůbec to ale nebylo potřeba a mohli jsme (možná i jednodušeji) úlohu vyřešit bez něj. Podívejme se, jak na to:

Zjistili jsme, že $\frac{a}{c} = x = \frac{k^2 - 1}{k^2 + 1}$ a $\frac{b}{c} = \frac{-2k}{k^2 + 1} = \frac{2uv}{u^2 + v^2}$. Aby byla čísla a, b, c nesoudělná, musí být $a = (u^2 - v^2)/D, b = 2uv/D$ a $c = (u^2 + v^2)/D$, kde D je NSD $u^2 - v^2$

¹⁸ *Pythagorejská* se této rovnici říká proto, že má stejný tvar jako Pythagorova věta o pravoúhlém trojúhelníku.

a $u^2 + v^2$ – právě vydělením největším společným dělitelem totiž zajistíme nesoudělnost čísel, rozmysli si, že D je (obecně) i NSD čísel $2uv$ a $u^2 + v^2$. Zbývá jen určit hodnotu D v závislosti na u, v . A to uděláme stejně jako v lemmatu.

Uvedeným postupem dokážeme vyřešit leckterou homogenní¹⁹ rovnici stupně 2. Nemusíme se ani omezovat jen na dvojrozměrnou rovinu, vše se dá obdobně dělat i v případě, kdy je neznámých více (například z rovnice $a^2 + b^2 + c^2 = d^2$ můžeme dostat rovnici $x^2 + y^2 + z^2 = 1$, což je rovnice koule v prostoru). Je ale vždy lepší si rozmyslet, jestli vše opravdu funguje tak, jak má – v prostoru například už neplatí, že by netriviální kvadrika (tak se říká obdobám kuželoseček) musela mít nejvýše dvoubodový průnik s přímkou. A samozřejmě, tento postup nám pomůže jenom v situaci, kdy umíme najít aspoň jedno netriviální řešení zadané rovnice – pak zkonstruujeme všechna řešení. Může se ale snadno stát, že rovnice žádné řešení nemá, a pak takto nepochodíme.

Rovnice vyšších stupňů takto bohužel řešit nejde, přesto jsou ale podobné geometrické myšlenky užitečné třeba při studiu kubických rovnic. Tomuto tématu se věnuje (dosti neelementární) teorie eliptických křivek, s jejíž pomocí byla například dokázána slavná velká Fermatova věta.

Cvičení.

- (1) Najdi všechna celočíselná řešení rovnice $a^2 + b^2 = c^2 + 3ab + ac$.
- (2) Najdi všechna celočíselná řešení rovnice $a^2 + 2b^2 = 5c^2$.
- (3) Najdi všechna celočíselná řešení rovnice $a^2 + b^2 + c^2 = d^2$.

¹⁹Tím myslíme, že všechny členy v rovnici mají stejný stupeň.