Seriál – Teorie čísel

Vítej u prvního dílu seriálu o teorii čísel. Co to vlastně ta teorie čísel je? Vždyť se přece skoro celá matematika zabývá čísly, nebo ne? Ne tak docela (máme tu třeba takovou geometrii; na vysoké pak zjistíš, že ta matematika nemá s čísly společného skoro nic), ale teorie čísel (překvapivě) opravdu čísla zkoumá. A to ne tak úplně ledajaká čísla, ale hlavně celá nebo racionální (a občas třeba taky komplexní, ale o tom se v tomto seriálu nanejvýš krátce zmíníme).

Co se dá o takových celých číslech zjišťovat? Základním pojmem, se kterým teorie čísel pracuje, je dělitelnost. A s tou souvisí třeba prvočísla. I kdyby se mohlo zdát, že skoro není nic jednoduššího než prvočísla (vždyť se přece učí tak někdy v 5. třídě základní školy), moc toho o nich nevíme. Prvočísla jsou totiž mezi přirozenými čísly dost nepravidelně rozmístěna a vůbec není lehké v jejich rozmístění objevit nějakou zákonitost nebo funkci, jejímiž všemi hodnotami by byla prvočísla. Matematici věnovali velké úsilí řešení takovýchto problémů; i ty se nad nimi můžeš zamyslet, ať už předtím, než se dál v seriálu dočteš, co je už známo a co ještě ne, nebo i potom.

Cvičení. Zkus najít nějaký řád v rozmístění prvočísel nebo třeba vzorec, který je bude (nejlépe všechna) generovat.[1]

Cvičení. Dokaž, že $n^2 + n + 41$ není prvočíselný vzorec. Zkus najít nejmenší n takové, že $n^2 + n + 41$ není prvočíslo.[2]

Prvočísla se k lecčemu hodí (v poslední době to je třeba šifrování), a tak se matematici dlouho předháněli (a pořád ještě předhánějí), kdo najde větší prvočíslo. Pěkná prvočísla jsou třeba $101, 2011, 1111211111, 56789012345678901234567890123$ a $2^{43\,112\,609} - 1$ (což je aktuálně největší známé prvočíslo a má 12 978 189 cifer). Samozřejmě kdyby se někomu podařilo najít nějaký prvočíselný vzorec, rovnou by toto soutěžení vyhrál, protože by mohl dosadit jakkoli velké přirozené číslo a tím dostat libovolně velké prvočíslo. Takový Fermat si třeba v 17. století myslel, že $2^{2^n} + 1$ je prvočíslo pro všechna n, Eulerovi se zase líbil vzorec z předchozího cvičení (ačkoli věděl, že ne všechny jeho hodnoty jsou prvočísla). Přesto se ale nedařilo[3] najít nějaký jednoduchý prvočíselný vzorec.

Cvičení. Měl Fermat pravdu?

A tak matematici aspoň zkoušeli zjišťovat, kolik těch prvočísel vlastně je. Už Euklides někdy kolem roku 300 před Kristem dokázal, že prvočísel je nekonečně mnoho, a my si to za chvíli taky zdůvodníme. O dost složitější je otázka, kolik prvočísel dostaneme jako hodnoty nějaké funkce. Dirichlet roku 1837 dokázal, že pokud jsou a a b nesoudělná přirozená čísla, je číslo $an + b$ prvočíslo pro nekonečně mnoho přirozených čísel n.[4]

Horší situace je, když uvažujeme mnohočleny vyšších stupňů. Ačkoli snad všichni matematici věří tomu, že každý „hezký“ polynom nabývá nekonečně mnoha prvočíselných hodnot, neumíme

---

[1] Na rozdíl od soutěžních úloh semináře, při řešení některých ze cvičení může být zajímavé zkusit použít i počítač, takže se toho klidně neboj. Není to ale samozřejmě vůbec nutné. Některá ze cvičení mohou být celkem dost těžká nebo ne úplně přesně zadaná (třeba toto :)), takže si nic nedělej z toho, když se ti nepodaří vyřešit.

[2] Prvočíselným vzorcem rozumíme takovou funkci, že po dosazení jakéhokoli přirozeného čísla dostaneme prvočíslo.

[3] A pořád ještě se nepodařilo, takže můžeš uspět ty a stát se slavným :)

[4] Toto tvrzení se občas může hodit v PraSátku nebo v Matematické olympiádě, zkus si ho tedy zapamatovat a používat ho.

to dokázat pro žádný polynom stupně aspoň 2 (tedy ani třeba pro n^2+1). A neznáme ani žádnou jinou jednoduchou funkci, pro kterou bychom to uměli dokázat.

Cvičení. Zjisti, jaký musí být „hezký“ polynom, aby mohl nabývat nekonečně mnoha prvočíselných hodnot.

Když už víme, že prvočísel je nekonečně mnoho, můžeme se také ptát, kolik je prvočísel menších než nějaké číslo x. Na konci 19. století Hadamard a de la Vallée Poussin dokázali, že jich je přibližně $x/\ln x$.[5] Jiné zajímavé tvrzení z podobného soudku, které dokázal Čebyšev kolem roku 1850, říká, že pro každé přirozené číslo n existuje prvočíslo p takové, že $n \leq p \leq 2n$.

Další typ problému, který číselné teoretiky zajímal a pořád ještě zajímá, je hledání celočíselných řešení rovnic. Jedním z prvních, kteří se tímto zabývali, byl řecký matematik Diofantos (žil ve 3. století před Kristem). Diofantos zkoumal řešení speciálního druhu rovnic „ze života“. Po něm se rovnicím, které řešíme v celých číslech, říká diofantické rovnice.

Řadu diofantických rovnic je velice těžké vyřešit. Známá velká Fermatova věta říká, že rovnice $x^n + y^n = z^n$ nemá pro $n \geq 3$ řešení v přirozených číslech. Ačkoli si už Fermat myslel, že ji umí dokázat, podařilo se to až Andrewu Wilesovi v roce 1995 za použití nechutně složitých metod a postupů. O jiné zajímavé rovnici hovoří Catalanova domněnka (v roce 2002 ji dokázal Mihăilescu): jediné řešení rovnice $x^a - y^b = 1; a, b > 1$ je $3^2 - 2^3 = 1$.

Zajímavých problémů a tvrzení je v teorii čísel přehršel (mohli bychom se zmínit třeba o prvočíselných dvojčatech, Goldbachově hypotéze, ...), prozatím by to ale snad mohlo stačit k tomu, abychom tě přesvědčili, že teorie čísel je zajímavá disciplína, o které má cenu se chtít dozvědět něco dalšího.

Ve zbytku dnešního seriálu najdeš pořádné definice některých základních pojmů (dělitelnost, prvočísla, Euklidův algoritmus a Bézoutova věta, kongruence, malá Fermatova a Eulerova věta) a tvrzení, která se jich týkají. Je pravděpodobné, že aspoň něco z toho budeš znát; určitě se tím nenech odradit, v příštích dílech už přijdou na řadu zajímavější věci.

Dělitelnost a prvočíselnost

Definice. *Číslo a dělí číslo b, právě když existuje číslo c, že $ac = b$. Tento fakt zapisujeme $a \mid b$. Číslo a nazýváme* dělitelem *čísla b* a *b* násobkem *čísla a.*

Teď, když už víme, co je to dělitel a násobek, definujme si ještě *největší společný dělitel* a *nejmenší společný násobek* několika čísel. Nejdříve společný dělitel čísel $a_1, a_2, \ldots, a_n$ je takové číslo d, že dělí všechna a_i (pro $i = 1, 2, \ldots, n$). Obdobně společný násobek je takové číslo n, že n je násobkem každého a_i (pro $i = 1, 2, \ldots, n$). Největší společný dělitel se pak definuje jako takový společný dělitel d, že pro každého jiného společného dělitele d' platí $d' \mid d$, nejmenší společný násobek je pak takový společný násobek n, že každý jiný společný násobek n' je jeho násobkem, tj. $n \mid n'$.

Všimni si, že vlastní definice neříká, že je to *největší* společný dělitel, ale přitom to (skoro) platí (kromě toho největšího d definujeme jako největšího společného dělitele i $-d$ z čistě formálních důvodů). Budeme-li se pohybovat v přirozených číslech, tak nejmenší společný násobek i největší společný dělitel je určen jednoznačně. Pak si můžeme dovolit označit (a, b) největší společný dělitel čísel a a b. (Podobně $(a_1, a_2, \ldots, a_n)$ je největší společný dělitel $a_1, a_2, \ldots, a_n$).

[5] $\ln x$ je přirozený logaritmus čísla x, tedy logaritmus o základu e. Pokud nevíš, o co jde, vůbec se tím netrap, nebudeme to k ničemu potřebovat.

Co nám ještě zbývá, je definovat nesoudělnost. Čísla a a b nazveme nesoudělná, pokud $(a, b) = 1$, tedy pokud jejich největší společný dělitel je 1 (ten je vždy společným dělitelem a přitom největším společným, pouze pokud a a b nemají žádné jiné společné dělitele).

Cvičení. Dokaž, že je-li d největší společný dělitel a n nejmenší společný násobek čísel a a b, tak platí $nd = ab$.

Definice. *Číslo $p \in \mathbb{N}$ nazveme* prvočíslem, *jestliže pro každá $a, b \in \mathbb{Z}$ platí, že pokud $p \mid ab$, tak $p \mid a$ nebo $p \mid b$.*

Můžeš si rozmyslet, že toto tvrzení je ekvivalentní s tím, že jediní dělitelé čísla p jsou 1 a p (tady uvažujeme pouze ty přirozené). Užitečnější je však naše definice, tak si ji, pokud ji ještě neznáš, dobře zapamatuj.

Známé je tvrzení o jednoznačném rozkladu na prvočinitele:

Tvrzení. *Každé přirozené číslo n lze jednoznačně (až na pořadí) zapsat jako součin $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, kde $p_1, p_2, \dots, p_n$ jsou po dvou různá prvočísla a $\alpha_i \in \mathbb{N}$ pro $i = 1, 2, \dots, n$.*

Důkaz. Nejprve dokážeme, že takový rozklad existuje, a teprve potom budeme dokazovat jednoznačnost. Existenci dokážeme matematickou indukcí. Začneme číslem 2, které je prvočíslo, a tedy ho lze zapsat jako součin.

Za indukční předpoklad si vezmeme tvrzení, že každé číslo $k \in \mathbb{N}, k < n$ lze zapsat jako součin prvočinitelů. Dokážeme tvrzení pro n. Buď n nemá žádné netriviální dělitele a pak je prvočíslo, tedy má rozklad triviálně, nebo existuje $d, c < n$, že $n = dc$. Pak jak d, tak c má rozklad na prvočinitele.

Jednoznačnost dokážeme další indukcí, pro malá prvočísla 2 a 3 (ostatně jako pro všechna prvočísla) je zřejmá. Dále předpokládejme, že každé číslo ostře menší než n má jednoznačný rozklad. Pro spor nechť $n = p_1 p_2 \cdots p_n = s_1 s_2 \cdots s_m$, kde p_i a s_i jsou prvočísla. Bez újmy na obecnosti můžeme předpokládat, že jsou seřazena dle velikosti tj. $p_1 \leq p_2 \leq \ldots \leq p_n$ a $s_1 \leq s_2 \leq \ldots \leq s_m$.

Dokážeme, že $p_1 = s_1$, $p_2 = s_2$ atd. Nechť $p_1 < s_1$. Víme, že $p_1 \mid n = s_1 \leq s_2 \leq \ldots \leq s_m$, pak ale p_1 dělí jedno z prvočísel s_i $(0 < i \leq m)$, přitom $p_1 < s_1 \leq s_i$ pro každé i a s_i jsou prvočísla, tedy dostáváme spor a $p_1 \geq s_1$. Obdobně ale můžeme dokázat $s_1 \geq p_1$, tedy $p_1 = s_1$. Nakonec položme $n' = p_2 p_3 \cdots p_n = s_2 \cdots s_m$. Platí $n' < n$, tedy pro n' máme indukční předpoklad, který nám dává kýžené $(\forall i)\, p_i = s_i$ a $n - 1 = m - 1$, tedy i $n = m$.

Věta. *V celých číslech existuje nekonečně mnoho prvočísel.*

Důkaz. Postupujme sporem, nechť existuje jen konečně mnoho prvočísel $p_1, p_2, \dots, p_k$. Uvažme číslo $n = p_1 p_2 \cdots p_k + 1$, pak zřejmě p_i nedělí n pro žádné $i = 1, 2, \dots, k$. Ale $n > 1$, takže musí mít netriviální rozklad na prvočinitele, čímž dostáváme spor.

Cvičení. Najdi jiný důkaz, že existuje nekonečně mnoho prvočísel.

Euklidův algoritmus a Bézoutova věta

Tvrzení. (Dělení se zbytkem) *Pro každé $a, b \in \mathbb{Z}$ existují jediná $r, q \in \mathbb{Z}$, $0 \leq r < |b|$, že $a = bq + r$. Číslu q říkáme (celočíselný) podíl a a b a číslu r zbytek po dělení čísla a číslem b.*

Nyní si popíšeme způsob, jak najít největšího společného dělitele nějakých dvou čísel. Následujícímu postupu se říká *Euklidův algoritmus*, a přestože je relativně jednoduchý, tak má dodnes široké využití a je to asi nejefektivnější způsob, jak najít největšího společného dělitele. Mimo to má i využití v teoretické matematice.

Celý algoritmus se opírá o několik jednoduchých tvrzení, která Ti necháme na rozmyšlení. (Ještě naposled připomenu, že symbolem (a, b) rozumíme největšího společného dělitele a a b.) Rozmysli si tedy, že platí: $(a, b) = (a - b, b)$, $(a, b) = (a - rb, b)$ pro $r \in \mathbb{Z}$ a $(a, 0) = a$. Možná už víš, jak budeme postupovat dále. Podívej se na následující posloupnost dělení se zbytkem (pro jednoduchost předpokládejme, že $a > b$):

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1} \end{aligned}$$

Tato posloupnost dělení se zbytkem musí jednou skončit, neboť kdyby ne, tak $a, b, r_1, r_2, \ldots$ je ostře klesající nekonečná posloupnost přirozených čísel a ta neexistuje.[6] Dále z vlastností, jež sis už zajisté rozmyslel, plyne, že $(a, b) = (b, r_1) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, 0) = r_{n-1}$. Tedy největší společný dělitel a a b je právě poslední nenulový zbytek v této posloupnosti dělení se zbytkem.

Cvičení. Najdi největší společné dělitele $(610, 377)$, $(2^{2^n} + 2^{n+1} + 1, 2^{2^n} - 2^{n+1} + 1)$ a $(n! + 1, (n+1)! + 1)$.

Budeme ještě chvíli zkoumat Euklidův algoritmus. Víme, že $d = (a, b) = r_{n-1}$, přitom z $(n-1)$. rovnosti máme $d = -q_{n-1} r_{n-2} + r_{n-3}$, r_{n-2} umíme zase vyjádřit z $(n-2)$. rovnosti pomocí r_{n-3} a r_{n-4}, obdobně r_{n-3} atd. Rozmysli si, že postupným dosazováním umíme dostat d jako součet nějakých násobků čísel a a b. Tímto rovnou popisujeme postup, jak získat čísla x a y z následující věty.

Věta. (Bézoutova) *Jsou-li a a b celá čísla, pak existují celá čísla x, y, že*

$$xa + yb = (a, b).$$

Cvičení. Vyzkoušej si tento postup na některých (třeba na svých oblíbených) dvojicích čísel.

Kongruence

Definice. *Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Pokud platí $m \mid (b-a)$, zapisujeme tuto skutečnost symbolem $a \equiv b \pmod{m}$ a čteme a je* kongruentní *s b modulo m.*

Uvedený výraz se nazývá *kongruence*. Sám si rozmyslíš, že tato definice vlastně říká, že a i b dávají stejné zbytky při dělení m.

Příklad. Uvědomíme si, že platí $20 \equiv 11 \pmod{9}$, $-12 \equiv 2 \pmod{7}$, ...

Práce s kongruencemi je vcelku příjemná díky tomu, že s nimi můžeme zacházet skoro jako s rovnicemi. Více už napoví následující tvrzení.

---

[6] Tato vlastnost přirozených čísel je v teorii čísel velmi užitečná. Třeba jsi už slyšel o metodě „nekonečného sestupu“, která ji využívá.

Tvrzení. *Pokud* $a \equiv b \pmod m$ *a* $c \equiv d \pmod m$ *pro* a, b, c, d *celá čísla a* m *číslo přirozené. Pak platí*

(i) $a + c \equiv b + d \pmod m$ *Kongruence tedy můžeme sčítat při stejném modulu ...*
(ii) $ac \equiv bd \pmod m$ *... stejně tak násobit*
(iii) *Pokud navíc* $d \mid m$*, pak i* $a \equiv b \pmod d$ *... a přecházet k jiným modulům.*

Důkaz. Dokážeme nyní první tvrzení. Podle definice víme, že $m \mid (a - b)$ a též $m \mid (c - d)$, a potřebujeme dokázat, že $m \mid (a + c - b - d)$. K tomu ovšem stačí si uvědomit, že pokud m dělí nějaká dvě čísla, pak dělí i jejich součet, a výraz $(a + c - b - d)$ není nic jiného než součet $(a - b) + (c - d)$.

Cvičení. Zkus si dokázat zbylá dvě tvrzení. Neboj se, že by to bylo nějak těžké, stačí si vše rozepsat podle definice.

Záludnost se objeví teprve ve chvíli, kdy chceme kongruence dělit. Platí totiž pouze

Tvrzení. *Pokud je* n *nesoudělné s* m *a platí* $na \equiv nb \pmod m$*, pak už platí* $a \equiv b \pmod m$.

Toto opět snadno dokážeme. První kongruence nám říká, že $m \mid na - nb$, tedy $m \mid n(a - b)$. Takže jsou-li m a n nesoudělná, musí platit $m \mid (a - b)$.

Důležité je, že podmínku nesoudělnosti nemůžeme vypustit. Například $2 \equiv 6 \pmod 4$, ovšem $1 \not\equiv 3 \pmod 4$. Takže vždycky když chceme kongruenci pokrátit, musíme ověřit, zda dělíme nesoudělným číslem.

Všimněte si, že kongruence vlastně neříkají nic, co bychom dříve neznali. Je to jen jiný způsob zápisu. Jeho výhodnost by měl ilustrovat následující příklad.

Příklad. Najdi všechna celá čísla k splňující $7 \mid k^2 - 2k - 1$.

Řešení. Požadavek úlohy si přepíšeme jako kongruenci a tu pak, díky předchozím tvrzením, můžeme upravovat jako rovnici. Například přičítání násobků sedmi na levou stranu je jistě ekvivalentní úprava.

$$k^2 - 2k - 1 \equiv 0 \pmod 7$$
$$k^2 + 5k + 6 \equiv 0 \pmod 7$$
$$(k + 2)(k + 3) \equiv 0 \pmod 7$$

Odtud vyčteme, že $7 \mid (k + 2)(k + 3)$. Díky tomu, že 7 je prvočíslo, dostáváme $7 \mid k + 2$ nebo $7 \mid k + 3$. Úpravy byly ekvivalentní, takže stačí splnit jednu z těchto podmínek a řešením tedy jsou všechna k ve tvaru $k = 7t - 2$ a $k = 7t - 3$ pro jakékoliv $t \in \mathbb{Z}$.

Cvičení. Zkuste si pomocí kongruencí odvodit, že vynásobíme-li dvě čísla tvaru $3k+1$, získáme opět číslo tvaru $3k + 1$. Zkuste postupovat za pomoci kongruencí i bez nich a oba postupy porovnejte.

Pokud jste minulé cvičení řešili pomocí násobení kongruencí, jistě vás nepřekvapí, že platí i toto.

Tvrzení. *Pokud* $a \equiv b \pmod n$*, pak platí i* $a^k \equiv b^k \pmod n$*, pro* $a, b \in \mathbb{Z}$ *a* $k, n \in \mathbb{N}$.

K důkazu stačí tuto kongruenci k-krát vynásobit samu se sebou.

Příklad. Ukažte, že $4^n \equiv 1 \pmod 3$ pro každé $n \in \mathbb{N}$.

Řešení. Z předchozího tvrzení víme, že $4^n \equiv 1^n \pmod 3$, neboť jistě platí $4 \equiv 1 \pmod 3$. Ovšem $1^n = 1$ a jsme hotovi.

Cvičení. Dokažte, že $11 \mid 10^{2n+1} + 12^n$ pro každé $n \in \mathbb{N}$.

Kongruence mohou být také užitečné při řešení diofantických rovnic. Můžeme například s jejich pomocí snadno ukázat, že rovnice nemá žádná řešení.

Příklad. Najděte všechny dvojice celých čísel k, l, m takových, že platí $k^2 + l^2 = 4m + 3$.

Řešení. Mají-li se obě strany rovnice rovnat, musí se rovnat i modulo 4. Můžeme tedy psát

$$k^2 + l^2 \equiv 4m + 3 \pmod 4,$$
$$k^2 + l^2 \equiv 3 \pmod 4.$$

Jenomže poslední kongruence už sama o sobě nemá žádné řešení. Zkus si rozmyslet, že ať umocníš jakékoliv číslo na druhou, vždy bude dávat po dělení čtyřmi zbytek 0 nebo 1. Nyní už je zřejmé, že levá strana může nabývat pouze hodnot 0,1 a 2 ovšem nikoliv 3. Takže ani původní rovnice nemá žádné řešení.

Seriál II. – Prvočísla a jiná zvířata

Již od objevení pojmu prvočíslo někdy ve starověkém Řecku se matematici snaží najít způsob, jak poznat, že nějaké dané číslo je prvočíslo, a předhání se v tom, kdo najde největší. Dnes už většinu z té práce necháváme počítačům, největší prvočísla sotva zvládneme napsat na papír a těch menších jsou miliardy tabulek.

A to, že to není problém jednoduchý, ukazují staletí výzkumu. Naproti tomu když se podíváš na opačný problém, najít číslo, které je složené, tak zjistíš, že je velmi jednoduchý – třeba číslo $2^{372539082} - 8$ je složené a dokonce větší, než největší známé prvočíslo. Vidíš, v čem je ten trik? Dokonce jde i velmi snadno dokázat, že existuje libovolně dlouhá posloupnost po sobě jdoucích složených čísel.

Cvičení. Nechť $n \in \mathbb{N}$ libovolné (a zvláště libovolně velké). Dokaž, že čísla $n!+2, n!+3, \ldots, n!+n$ jsou složená.

V tomto díle se tedy můžeš těšit na to, že se dozvíš, jak se dnes zjišťuje, zda nějaká (velká) čísla jsou prvočísla. Následně si pak povíme o aplikaci v šifrování a popíšeme si algoritmus RSA. Nejdříve však budeme muset trochu zpomalit a podíváme se ještě na tři ze základních vět teorie čísel.

Čínská zbytková věta

Uvažme jednu soustavu kongruencí – můžeš se hned zamyslet nad tím, jak bys ji řešil. Mějme daná $a, b \in \mathbb{N}$ a moduly $m, n \in \mathbb{N}$ a pro jednoduchost budeme předpokládat, že m a n jsou nesoudělná. Hledejme x takové, že:

$$x \equiv a \pmod n$$
$$x \equiv b \pmod m$$

Nejdříve si ověříme, jestli tato soustava vůbec nějaké řešení má. Z Bezoutovy věty existují $x, y \in \mathbb{Z}$, že $xn + ym = 1$, tj. $xn \equiv 1 \pmod m$ a obdobně $ym \equiv 1 \pmod n$, pak ale číslo $r = axn + bym$ dává zbytek a modulo n a zbytek b modulo m a našli jsme jedno řešení.

Je toto jediné řešení? Mnozí z vás již tuší, že i čísla $knm + r$ budou řešení pro každé $k \in \mathbb{Z}$. Další řešení už soustava nemá, protože kdykoliv x a y jsou dvě řešení, tak $m \mid x - y$ i $n \mid x - y$ (jeden zbytek je a a druhý b) a z nesoudělnosti m, n máme $mn \mid x - y$ a $x \equiv y \pmod{mn}$. Celkem

jsme tedy ukázali, že soustavu řeší čísla $kmn + r$ pro libovolné $k \in \mathbb{Z}$ a jediné $r \equiv axn + bym$ modulo mn.

Cvičení. Honza, který žil v království Za sedmero horami, měl stádo ovcí. Nebylo to jen tak stádečko jen tak obyčejných ovcí, poslouchaly ho na slovo a on je vždy přepočítával tak, že jim vždycky řekl, ať se seřadí nejdříve do sedmistupu, pak do jedenáctistupu a nakonec do desetistupu. Nikdy žádná ovečka nevyčuhovala z řady a všechny řady byly úplné a tak Honza věděl, že mu žádná nechybí a že jich má právě 770. Jednoho dne se nad Honzovou chaloupkou prohnal drak a rozehnal stádo do všech koutů země (některé z chytrých oveček můžete potkat i u nás). Domů se vrátily jen některé, a když jim Honza přikázal, ať se srovnají, tak nejdříve v sedmistupu v poslední řadě stály pouze čtyři, v jedenáctistupu jich v poslední řadě stálo sedm a v desetistupu jen jediná ovečka. Kolik Honzovi zbylo oveček po drakově útoku?

Když se podíváš na předchozí cvičení o Honzovi, všimni si, že v něm jsi řešil (pokud jsi pilný řešitel) soustavu dokonce tří kongruencí. Taky platí, že každá „taková“ (libovolně velká[7]) soustava kongruencí má jednoznačné řešení modulo součin modulů. A co znamená taková? Formálně:

Věta. (Čínská zbytková) *Nechť $n \in \mathbb{N}$, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ a $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ jsou po dvou nesoudělná čísla. Pak soustava kongruencí*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

má řešení x a navíc pro libovolná dvě řešení x_1, x_2 soustavy platí $x_1 \equiv x_2 \pmod{m_1 m_2 \cdots m_n}$.

Důkaz. Už víme, že soustava jedné a dvou rovnic má řešení, a dokonce jednoznačné. Indukcí budeme postupovat dále, mějme tedy $n+1$ rovnic, pak soustava prvních n kongruencí má jednoznačné řešení r modulo $m_1 m_2 \cdots m_n$. A uvažme novou soustavu dvou kongruencí

$$\begin{aligned} x &\equiv r \pmod{m_1 m_2 \cdots m_n}, \\ x &\equiv a_{n+1} \pmod{m_{n+1}}. \end{aligned}$$

Každé řešení této soustavy je i řešení původní a naopak. Navíc platí $(m_1 m_2 \cdots m_n, m_{n+1}) = 1$ (z nesoudělnosti m_i, m_j). Tím jsme získali soustavu dvou rovnic a o ní už víme, že má jednoznačné řešení.

Jiný, možná názornější způsob, jak najít nějaké řešení soustavy kongruencí ze znění čínské zbytkové věty, vypadá zhruba takto: zkusíme x vyjádřit z první kongruence, výsledek dosadíme do druhé kongruence, odkud znovu vyjádříme a dosadíme do třetí kongruence, ... Postup budeme psát pro obecnou soustavu, názornější ale nejspíš bude, když ho hned zkusíš aplikovat na nějakou konkrétní soustavu kongruencí.

Podle první kogruence musí být $x = a_1 + ym_1$ pro nějaké celé číslo y (které neznáme). Když toto vyjádření dosadíme do druhé kogruence, dostaneme $a_1 + ym_1 \equiv a_2 \pmod{m_2}$, neboli $ym_1 \equiv a_2 - a_1 \pmod{m_2}$. Teď bychom chtěli vyjádřit y. Jak ale na to?

[7] Zase uplně libovolně velká být nemůže, ale řekněme konečná – i tak může obsahovat třeba dvacet miliard kongruencí.

Ukážeme si, jak obecně najít řešení kongruence $ta \equiv b \pmod m$ (a, b, m jsou „známá“ přirozená čísla, a a m jsou nesoudělná a hledáme t).[8] Chceme vlastně kongruenci upravit do tvaru $t \equiv c \pmod m$ pro nějaké číslo c, potřebujeme tedy obě strany vydělit číslem a. To je snadné, pokud a dělí b, jenže co když tomu tak není?

Vyberme si libovolné prvočíslo p, které dělí a. Pokud p dělí b, není co řešit. Pokud nedělí, vzpomeňme si na základní vlastnosti kongruencí – víme, že platí $ta \equiv b \equiv b + m \pmod m$, zkusme tedy číslem p vydělit $b + m$. Pokud ani toto není celé číslo, není potřeba zoufat –platí také $ta \equiv b \equiv b + 2m \pmod m$, a tedy můžeme zkusit, zda p dělí $b + 2m$, případně jestli $p \mid b + 3m, b + 4m, \ldots, b - m, b - 2m, \ldots$. Jakmile dělení vyjde beze zbytku, dostaneme novou kongruenci $ta' \equiv b' \pmod m$, kde $a' = a/p$ a $b' = (b + im)/p$ pro výše nalezené i. Abychom vyřešili tuto kongruenci, zase si vybereme nějaké prvočíslo, které dělí a' a zkusíme jím novou kongruenci vydělit. Časem takto kongruenci převedeme do kýženého tvaru $t \equiv c \pmod m$.[9]

Cvičení. Možná sis všiml, že jsme nijak nezdůvodnili, že p dělí nějaké z čísel $b + im$. Zkus to (s využitím nesoudělnosti čísel a a m) dokázat.

A už se můžeme vrátit k naší soustavě kongruencí! Potřebovali jsme vyřešit kongruenci $ym_1 \equiv a_2 - a_1 \pmod{m_2}$. To už pro nás není žádný problém, a tak můžeme napsat, že $y = c + zm_2$, kde c je řešení nalezené výše uvedeným postupem a z je nějaké neznámé celé číslo. Když to ještě dosadíme do $x = x = a_1 + ym_1$, dostaneme, že $x = a_1 + cm_1 + zm_1m_2$. Můžeš si (nejlépe na konkrétním příkladě) vyzkoušet, že každé takovéto x je řešením prvních dvou kongruencí.

Když máme víc než dvě kongruence, můžeme získané x zase dosadit do další kongruence a vyjádřit z ní z ve tvaru $d + tm_3$ (t neznáme). Tak dostaneme x, které už splňuje první 3 kongruence, a můžeme pokračovat, dokud nezískáme řešení celé soustavy.

Čínská zbytková věta je klíčové tvrzení teorie čísel, které lze vnímat i tak, že dává jednoznačnou souvislost mezi zbytkovými třídami modulo $m_1m_2 \cdots m_n$ a n-ticemi zbytkových tříd modulo postupně m_1, m_2 až m_n. Podívej se třeba na nejmenší rozumné moduly 2 a 3, jejich součin je 6 a opravdu zbytek 1 odpovídá dvojici zbytků $(1, 1)$, 2 pak $(0, 2)$, 3 odpovídá $(1, 0)$, zbytky $(0, 1)$ odpovídají číslu 4 atd.

Malá Fermatova a Eulerova věta

Věta. (malá Fermatova) *Nechť $a \in \mathbb{N}$ a p je prvočíslo, navíc platí $p \nmid a$, pak*

$$a^{p-1} \equiv 1 \pmod p.$$

Důkaz. Uvažme množinu čísel $\{a, 2a, \ldots, (p-1)a\}$. Tato čísla dávají po dvou různý zbytek po dělení p, neboť kdyby to tak nebylo, tj. $ka \equiv la \pmod p$) pro nějaká $k, l \in 1, 2, \ldots p-1$ a $k > l$,

[8] Uvedený postup je celkem dobrý pro počítání s rozumně malými čísly na papíře, rozhodně ale není jediný nebo nejlepší možný. Jiná možnost je třeba použít Eulerovu větu, uvedenou níže (zkus vynásobit obě strany řešené kongruence číslem $a^{\varphi(m)}$). A asi nejlepší je pomocí Euklidova algoritmu najít čísla u, v podle Bezoutovy věty, tedy taková, že platí $au + mv = (a, m) = 1$ a pak řešenou kongruenci vynásobit číslem u.

[9] Můžeš si všimnout, že jsme úplně stejně mohli rovnou vydělit celým a. Jen by to vzhledem k použitému postupu bylo pravděpodobně o dost pomalejší než dělit postupně jednotlivými prvočísly, která jsou menší, a máme tedy lepší šanci, že nebudeme muset zkoušet přičítat m moc dlouho.

tak dostáváme $p \mid (ka - la) = (k - l)a$. Tedy p dělí buď a, což je ve sporu s předpokladem věty, nebo $k - l$, což je číslo menší než p, každopádně dostáváme spor. Z toho je také vidět, že všechna dávají nenulový zbytek po dělení p. Tedy nabývají všech (nenulových) zbytků, proto platí:

$$(p-1)! = 1 \cdot 2 \cdots 3 \equiv a \cdot 2a \cdots (p-1)a = (p-1)! \cdot a^{p-1} \pmod{p}.$$

Protože $(p-1)!$ je nesoudělné s p, můžeme tuto kongruenci pokrátit a dostaneme tvrzení věty.

Věta. (Eulerova) *Nechť $a, n \in \mathbb{N}$ jsou dvě nesoudělná čísla a $\varphi(n)$ je počet čísel menších nebo rovných n, která jsou s n nesoudělná, pak platí:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Cvičení. Dokaž Eulerovu větu. (Neměj strach, důkaz je prakticky stejný jako důkaz Malé Fermatovy věty, takže to určitě zvládneš.)

Číslo $\varphi(n)$ se nazývá *Eulerova funkce* čísla n. Existuje mnoho způsobů, jak ji spočítat, všechny však předpokládají znalost rozkladu. Právě tohoto faktu se užívá v kryptologii v šifrovacím algoritmu RSA.

Podívejme se na nějaké vlastnosti funkce φ. Prvně $\varphi(p) = p - 1$ pro p prvočíslo, neboť všechna čísla menší než p jsou s ním nesoudělná. Tedy Eulerova věta je opravdu zobecněním Malé Fermatovy věty. Dále nahlédneme, že pro m, n nesoudělná platí $\varphi(nm) = \varphi(n)\varphi(m)$. To je důsledek Čínské zbytkové věty. Dále platí ještě $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$ pro p prvočíslo a $\alpha \in \mathbb{N}$ (soudělné jsou jen násobky p menší než p^α a těch je právě $p^{\alpha-1}$). Jako důsledek těchto dvou nahlédnutí dostáváme:

Tvrzení. *Nechť $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ je prvočíselný rozklad čísla n takový, že pro $i \neq j$ platí $p_i \neq p_j$. Pak platí*

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_n^{\alpha_n - 1}(p_n - 1) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right).$$

Prvočíselnost

V další části si povíme něco o prvočíselných testech. Všechny řeší základní problém: Máme dané přirozené číslo n a naším úkolem je zjistit, jestli je prvočíslem. Určitě jsi už některá čísla testoval a to u těch menších převážně zkoušením všech možných dělitelů čísla n. To je nejjednodušší prvočíselný test (a taky jeden z těch málo efektivních). K němu se váže i jednoduché tvrzeníčko: Je-li číslo n složené, tak má dělitele d, který je nejvýše $\sqrt{n}$. Ve zkratce uvedeme důkaz: je-li $n = de$, přičemž $d \leq e$, pak $d^2 \leq n$.

Fermatův test

Podíváme se na o něco lepší prvočíselné testy, které jsou založeny na malé Fermatově větě. Malá Fermatova věta říká, že je-li n prvočíslo a $(a, n) = 1$, pak

$$a^{n-1} \equiv 1 \pmod{n}$$

Na tomto tvrzení je založen Fermatův prvočíselný test, který se dá popsat následujícími slovy: Zvolme a libovolné, spočítejme $a^{n-1} \pmod{n}$, pokud je různé od jedné, tak n je složené. Už ve staré Číně se tento test používal striktně pro $a = 2$ (nejmenší rozumné číslo) a ukazuje se, že

první složené číslo, které není tímto testem odhaleno, je číslo 341. Snad jsem vás teď přesvědčil, že přece jen tento test k něčemu je. Komu by se taky chtělo u čísla asi 329 testovat jestli je dělitelné dvěma, třemi, pěti, sedmi, jedenácti, třinácti a sedmnácti, když místo toho může spočítat jenom výraz $2^{328} \bmod 329$ (a schválně, jak to vyjde?).[10]

Kromě toho se ukazuje, že tento test sice umí celkem rychle vyloučit hodně složených čísel, ale nemáme nic, o co bychom se mohli opřít, když chceme s naprostou jistotou tvrdit, že číslo je prvočíslo. Výsledek, ke kterému docházíme, je pouze: „Tohle číslo je s velkou pravděpodobností prvočíslo.“ A dokonce se i ukazuje, že tento test je špatný, protože existují čísla, kterým se říká Carmichaelovy:

Definice. *Číslo n nazveme* Carmichaelovým, *pokud pro každé $a \in \mathbb{Z}, (a,n) = 1$ platí $a^{n-1} \equiv 1 \pmod{n}$.*

Ještě než se pustíme do vypisování nějakých příkladů Carmichaelových čísel, tak si uvedeme jedno tvrzení, které nám trochu přiblíží, jak vypadají.

Tvrzení. *Nechť n je liché složené číslo. Pak platí:*

(1) *Je-li n Carmichaelovo, tak n není dělitelné žádnou druhou mocninou žádného prvočísla. (Takovým číslům n se říká bezčtvercová.)*
(2) *Jestliže n je bezčtvercové a $n = p_1 p_2 \cdots p_k$, pak n je Carmichaelovo, právě když $p_i - 1 \mid n - 1$ pro každé $i = 1, \ldots, k$.*

Důkaz. Důkazy první části tvrzení a jedné implikace z druhé časti neuvedeme, neboť jsou trochu obtížnější a vyžadují hlubší znalosti teorie čísel.

Podíváme se tedy na tu snadnou implikaci. Předpokládejme, že $(p_i - 1)d_i = n - 1$ pro každé $i = 1, 2, \ldots, k$. A nechť navíc máme b nesoudělné s n, tedy i s p_i a platí $b^{(p_i-1)d_i} \equiv 1^{d_i} \equiv 1 \pmod{p_i}$. To platí pro každé i a dostáváme $p_i \mid b^{n-1} - 1$, tedy i $n = p_1 p_2 \cdots p_k \mid b^{n-1} - 1$. A to jsme chtěli dokázat.

Teď je správný čas uvést si nějaké příklady. Číslo $n = 561 = 3 \cdot 11 \cdot 17$ je Carmichealovo. A opravdu 560 je dělitelné $3 - 1$, $11 - 1$ i $17 - 1$, a tedy je Carmichaelovo. Moje oblíbené číslo $1729 = 7 \cdot 13 \cdot 19$ je také Carmichaelovo (Je celkem vidět, že 1728 je dělitelné čtyřmi a devíti podle známých kritérií, tedy musí být nutně dělitelné 6, 12 a 18). Všimni si, že obě tato čísla jsou součinem tří prvočísel – dokonce platí, že každé Carmichaelovo číslo je součinem alespoň tří prvočísel.

Carmichaelových čísel očividně není mnoho. To, že jich je nekonečně mnoho, bylo třeba dokázáno až v roce 1992.

Cvičení. Dokaž, že Carmichaelovo číslo je součin alespoň tří různých prvočísel.

Miller-Rabinův test

Existence Carmichelových čísel, která velmi dobře procházejí Fermatovým testem, je největší slabina tohoto testu. Ukazuje se, že tato slabina se dá odstranit jednoduchou myšlenkou, která

[10] Co je to za blbost?! Jak by mohlo být počítání nějaké šílené mocniny rychlejší, než prostě jenom vyzkoušet dělitelnost pár malými čísly?! Zkus si to rozmyslet (a pokud jsi informatik, tak třeba i spočítat časovou složitost těchto algoritmů). Pár rad nebo námětů k zamyšlení: Počítáme modulo, takže se při umocňování můžeme velkých čísel zbavovat. Není potřeba postupně násobit a počítat (třeba) $2^1, 2^2, 2^3, \ldots, 2^{100}, 2^{101}, 2^{102}, \ldots, 2^{327}, 2^{328}$, ale můžeme umocňovat na druhou a počítat $2^1, 2^2, 2^4, 2^8, 2^16, \ldots$ – to jde o poznání rychleji.

je založena na tom, že pokud $b^2 \equiv 1 \pmod{p}$, kde p je prvočíslo, pak $p \mid b^2 - 1 = (b-1)(b+1)$, a protože p je prvočíslo, tak musí dělit první nebo druhou závorku a máme $b \equiv \pm 1$.

Začneme s Fermatovým testem a uplatníme na něj předchozí pozorování. Nechť n je liché číslo, které budeme testovat. Aby n bylo prvočíslo, tak $a^{n-1} \equiv 1 \pmod{n}$, ale $n-1$ je sudé. Pokud tedy $a^{n-1} \equiv 1$, tak $a^{(n-1)/2} \equiv \pm 1$. A kdyby nám náhodou vyšlo 1 a exponent by byl pořád sudý, tak můžeme postup opakovat a dostáváme $a^{(n-1)/4} \equiv \pm 1$. Dále pokud vyjde -1 a navíc i $(n-1)/4$ je sudé, tak znovu $a^{(n-1)/8} \equiv \pm 1$ atd., až dokud exponent není lichý nebo nám nevyjde -1. Pro shrnutí je-li $n - 1 = 2^r m$, kde m je liché (ekvivalentně 2^r je nejvyšší mocnina dvojky, která dělí $n-1$), pak musí nastat jeden z následujících případů:

$$a^m \equiv \pm 1 \pmod{n},$$

$$
\begin{aligned}
a^{2m} &\equiv -1 \pmod{n},\\
a^{2^2 m} &\equiv -1 \pmod{n},\\
&\vdots\\
a^{2^{r-1} m} &\equiv -1 \pmod{n}.
\end{aligned}
$$

Protože víme, že nás postup se může zastavit, pouze pokud nám vyjde -1 (to jsou druhá až poslední kongruence) nebo budeme mít lichý exponent (tedy první kongruence). Tím dostáváme Miller-Rabinův test. V praxi se pak právě testuje v tomto pořadí, protože jakmile spočítáme a^m, tak každá další mocnina a, kterou potřebujeme, je druhou mocninou předchozí modulo n.

Ukazuje se, že tento algoritmus už je mnohem lepší. Je dokázáno, že pokud je n složené, tak test selže pro alespoň tři čtvrtiny možných voleb a. To mj. znamená, že pokud ho provedeme třeba třikrát s úspěšným výsledkem, tak naše číslo je s pravděpodobností $1 - \left(\frac{1}{4}\right)^3 = 98{,}4375\%$ prvočíslo! (Pořád k tomu, abychom si mohli být naprosto jistí, stejně potřebujeme otestovat více než čtvrtinu možných a, holt nemůžeme mít všechno.)

Všimni si, že tento test je oproti Fermatovu lepší „jen“ tím, že používá navíc definici prvočísla, tj. p je prvočíslo, právě když pro každé a, b, pokud $p \mid ab$, tak $p \mid a$ nebo $p \mid b$, která vede k jednoznačnému rozkladu polynomu (v našem případě rozkladu $x^2 - 1$) na kořenové činitele a nerozložitelné polynomy. Všimni si, že třeba pro osmičku tohle neplatí – kongruenci $x^2 \equiv 1 \pmod 8$ řeší libovolné liché číslo a ta dávají celkem čtyři různé zbytky modulo 8.

Šifrovací algoritmus RSA

Algoritmus RSA (pojmenován podle matematiků Rivesta, Shamira a Adlemana) je v současnosti jeden z nejpoužívanějších šifrovacích algoritmů. Patří mezi asymetrické šifry, to znamená, že je použit jiný algoritmus na zašifrování a jiný na dešifrování. Díky tomu může být šifrovací algoritmus veřejně znám, aby kdokoliv mohl poslat komukoliv zprávu. K dešifrování je pak potřeba soukromý klíč příjemce, který je naopak přísně utajen a zná ho jen příjemce sám. Tím je zařízeno, že zprávu si přečte jen a jen on.

Celý algoritmus je založen na Eulerově větě, z ní víme, že pro libovolné m platí $m^{\varphi(n)+1} \equiv m \pmod n$. Snadno matematickou indukcí dokážeme dokonce: pokud $a \equiv 1 \pmod{\varphi(n)}$, tak $m^a \equiv m \pmod n$. Přitom k získání $\varphi(n)$ je potřeba znát rozklad čísla n na prvočinitele a to je úloha, kterou v současné době neumíme rychle řešit. Pokud by tedy náhodou někdo objevil rychlý algoritmus na rozklad čísla na prvočinitele, tak by si nejen vydobil slávu a uznání celé matematické obce, ale tento objev by dokonce ovlivnil běžný život, protože by se okamžitě zhroutil veškerý systém elektronického bankovnictví, kde se dnes převážně používá RSA. Je pravda, že už existují alternativní algoritmy, ale ty nejsou globálně používány. Každopádně by to znamenalo nemalé změny a v dnešní ekonomické krizi by to bylo určitě zajímavé, takže vzhůru do toho!

Vraťme se zas od ekonomie k matematice. Jak tedy funguje RSA? veřejný klíč je dvojice čísel, první je modul n a druhý exponent e, který je nesoudělný s $\varphi(n)$. Zprávu m pak zašifrujeme tak, že ji umocníme na e modulo m, tedy pro zašifrovanou zprávu $š$ platí $š \equiv m^e \pmod n$. Soukromý klíč pak je dvojice n a d, kde d je zvoleno tak, aby $de \equiv 1 \pmod{\varphi(n)}$. Pak budeme dešifrovat umocněním na d modulo n tj. $š^d \equiv m^{ed} \equiv m \pmod n$.

A jak takové d dostaneme? Odpověď je v Bézoutově větě a Euklidově algoritmu. Z nich umíme zjistit pro čísla d a $\varphi(n)$ hodnoty e a f, aby $de + f\varphi(n) = 1$, pak bude platit i kýžené $de \equiv 1 \pmod{\varphi(n)}$.

Nakonec se ještě podíváme přesně na generování klíčů. V praxi se za n volí součin dvou dostatečně velkých prvočísel p a q. Pak víme, že $\varphi(n) = (p-1)(q-1)$. A postup vypadá:

(1) Zvolme dvě různá dostatečně velká a náhodná prvočísla p a q.
(2) Spočtěme $n = pq$ a $\varphi(n) = (p-1)(q-1)$.
(3) Zvolme libovolné e, aby $(e, \varphi(n)) = 1$.
(4) Spočtěme d z Euklidova algoritmu, aby $de \equiv 1 \pmod{\varphi(n)}$.
(5) Zvěřejníme n a e jako věřejný klíč, n a d si schováme jako soukromý klíč a mezivýsledky raději zapomeneme.

Na závěr se podíváme na ukázku, jak to všechno funguje. Běžně se používají oprvadu velká prvočísla, avšak abychom ukázali funkčnost RSA, tak nám budou stačit mnohem menší, řekněme 11 a 19. Spočteme si nejdříve modul $n = 11 \cdot 19 = 209$, $\varphi(n) = 10 \cdot 18 = 180$. Za exponent e zvolme třeba 37, ověřme, že je opravdu nesoudělný s $\varphi(n) = 180$ euklidovým algoritmem:

$$\begin{aligned} 180 &= 4 \cdot 37 + 32 \\ 37 &= 1 \cdot 32 + 5 \\ 32 &= 6 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Takže vidíme, že opravdu je. Teď zpětných chodem spočítáme d, chceme, aby $37d + 180k = 1$. Víme $1 = 5 - 2 \cdot 2 = 13 \cdot 5 - 2 \cdot 32 = 13 \cdot 37 - 15 \cdot 32 = 13 \cdot 37 - 15(180 - 4 \cdot 37) = 73 \cdot 37 - 15 \cdot 180$. Tedy $d = 73$ (potřebujeme d kladné, neboť na něj budeme umocňovat). Máme tak věřejný klíč $(209, 37)$ a soukromý $(209, 73)$.

Teď zašifrujme nějakou zprávu. Zpráva musí být číslo menší než modul, tedy 209. Budeme-li chtít tedy zakódovat třeba písmeno „a“, v ASCII mu odpovídá číslo 97. Zašifrujeme umocněním na exponent $e = 37$ modulo $n = 209$ (tady asi budeme potřebovat kalkulačku na pomoc):

$$\begin{gathered} 97^2 \equiv 4 \qquad 97^4 \equiv 4^2 \equiv 16 \qquad 97^8 \equiv 16^2 \equiv 47 \\ 97^{16} \equiv 47^2 \equiv 119 \qquad 97^{32} \equiv 119^2 \equiv 158 \pmod{209} \\ 97^{37} = 97^{32+4+1} \equiv 158 \cdot 16 \cdot 1 \equiv 59 \pmod{209} \end{gathered}$$

Takže zašifrovaná zpráva je 59. Tuto zprávu můžeme věřejně vyřvávat a nikdo jí nebude rozumět. Jakmile ji však dostane někdo, kdo zná soukromý klíč, tak může zprávu dešifrovat podobně jako byla zašifrovaná, jen použije klíč $(209, 73)$. Počítejme tedy:

$$\begin{gathered} 59^2 \equiv 137 \qquad 59^4 \equiv 137^2 \equiv 168 \qquad 59^8 \equiv 168^2 \equiv 9 \\ 59^{16} \equiv 9^2 \equiv 81 \qquad 59^{32} \equiv 81^2 \equiv 82 \qquad 59^{64} \equiv 82^2 \equiv 36 \pmod{209} \\ 59^{73} \equiv 59^{64+8+1} = 36 \cdot 9 \cdot 59 = 97 \pmod{209} \end{gathered}$$

Jestli jste mě zvládli sledovat, tak vidíte, že $59^{73} \equiv 97 \pmod{209}$. A tím tedy nakonec dostáváme opět původní zprávu, tedy písmeno „a“ v ASCII kódu. A je už jen na nás, jak takovou zprávu pochopíme.

Seriál III. – Jak vyzrát 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.[11] 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 (:[12]

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 $a^{\varphi(n)} \equiv 1 \pmod{m}$, kde $\varphi(m)$ je Eulerova funkce. Pokud je $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, kde $p_1, \ldots, p_k$ jsou po dvou různá prvočísla, $k \in \mathbb{N}$ a $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, 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,*[13] *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. Pusťme 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 $a_n, \ldots, a_1, a_0 \in \mathbb{Z}$. 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 $k = 0, 1, \ldots, n$, 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.

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

---

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

[12] Aspoň v to teda doufám. (:

[13] To 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 $a_n, \ldots, a_1, a_0 \in \mathbb{Z}$.

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 mod 5, tedy čísla 0, 1, 2, 3, 4." To je ale špatně! Vždy musíme být schopní 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"[14] zkoušíme všechny možné zbytky modulo m, zatímco „nahoře"[15] 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 rozdíl těchto čísel). Podle věty by tedy mělo být $P(5) \equiv P(8) \pmod 3$. Ovšem podle zadání by

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

[15] Tedy v exponentu, třeba u funkcí $5^x, 13^x, \ldots$.

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 $a_1, a_2, \ldots, a_n$ pro nějaké $n \in \mathbb{N}$ a celé číslo b. Rovnice $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ s neznámými $x_1, x_2, \ldots, x_n$ má řešení, právě když $\mathcal{NSD}(a_1, \ldots, a_n)$ 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 $D = \mathcal{NSD}(a_1, a_2, \ldots, a_{n-1})$. 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:[16]

[16] Podobné 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.[17] 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,[18] 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 $x = 0, 1, 2, \ldots, 5$. Dostáváme $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4 (\equiv 11)$, $2^3 \equiv 1 \pmod 7$. 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 $x = 3k + 2, k \in \mathbb{N}_0$,[19] 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 $1! + 2! + 3! + \cdots + n! = m^2$.

---

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

[18] Nejlépe na základě toho, že to po nás přímo chce zadání. (:

[19] Nesmíme 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 mod 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. Pusťme 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 rozlišme 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 pořadní) 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 $p_1, \ldots, p_k$ jsou po dvou různá prvočísla, $q_1, \ldots, q_l$ jsou po dvou různá prvočísla, $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l \in \mathbb{N}$ 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 $r_1 = p_1, r_2 = p_2, \ldots, r_k = p_k, r_{k+1} = q_1, r_{k+2} = q_2, \ldots r_m = q_l$, 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 předpokládejme, že x není -1 ani -2.[20]

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, tentokráte 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 prvočíslo.
(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

[20] Tento 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. Nějaký takovýto 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.[21]

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

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, nechť $z = 2z_1$. 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 $z_2 = 2z_3$ ... a takto bychom mohli pokračovat pořád dál a dál. Máme tedy posloupnosti čísel $x, x_1, x_2, x_3, \ldots$, $y, y_1, y_2, y_3, \ldots$ a $z, z_1, z_2, z_3, \ldots$, 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 $|x| > |x_1| > |x_2| > |x_3| > \ldots$. 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 lecjakou rovnici pomocí geometrických představ. To může být docela překvapivé a zajímavé – na první

[21] Tato 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 jasné, jak by nějaké geometrické čmáranice mohly souviset s čistě negeometrickým 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 ztotožněme s dvojicí reálných čísel – jeho souřadnic.[22]

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, žes o 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 přečíst 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 trošku delší – pokud se Ti ale nepodaří se jím prokousat, ničemu by to moc vadit nemělo.

---

[22] Pokud 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 Viètových vztahů[23] 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 Viètových 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 průsečíků[24] 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 spojnici 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,

[23] Viètovy 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 $t_1 + t_2 = -b/a, t_1 t_2 = c/a$.

[24] Průsečíkem 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, dosaďme 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 Viètovy 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 $u \in \mathbb{Z}, v \in \mathbb{N}, (u, v) = 1$.[25]

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 $a = u^2 - v^2, b = 2uv$ a $c = u^2 + v^2$, ale to bychom se unáhlili! 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,[26] 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,[27] 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

[25] Minus 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.

[26] Lemma 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.

[27] Neboli jedno z nich je sudé a druhé liché.

to přijít sami. Využijeme základních vlastností největšího společného dělitele, zvlášť 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 zbývajícímu 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 rovnice[28]) *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 $\frac{a}{c} = x = \frac{k^2-1}{k^2+1} = \frac{u^2-v^2}{u^2+v^2}$ 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 $u^2 - v^2$

[28] *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 homogenní[29] 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 $a^2 + b^2 + c^2 = d^2$.

[29] Tím myslíme, že všechny členy v rovnici mají stejný stupeň.