Matematická indukce I – Padající domina

Milý příteli,
v rukou držíš zbrusu nový PraSečí seriál, ve kterém se dozvíš něco o matematické indukci. Jedná se o jednu ze základních důkazových technik, hned vedle přímého důkazu nebo důkazu sporem. Důkaz, to je gró matematiky. A proto je to samozřejmě i základ úloh matematického semináře. Bez správného dokazování matematických tvrzení by se nám celá teorie rozpadla – jak bychom jinak zajistili, aby bylo dané tvrzení pravdivé? Možnost dokazování je zároveň i krásná vlastnost matematiky, protože co jednou dokážeme, to je pak pravdivé a jasné a experimentem to nevyvrátíme, jako je tomu u méně exaktních věd.

Seriál pro Tebe letos píší Káťa Panešová a Ittihad. V případě zvídavých dotazů či jakýchkoli nejasností se na nás neváhej obrátit na *kacka.panesova@gmail.com* a *ahmedittihad@hotmail.com*.

Jak číst seriál

Jednotlivá témata jsme se snažili seřadit podle obtížnosti. Nicméně pokud se místy budeš ztrácet, klidně nějakou tu část přeskoč a vrať se k ní později – části na sobě nejsou nijak výrazně závislé.

V rámci tohoto textu najdeš i příklady k procvičení. Ty jsou nadepsané jako **Cvičení** nebo **Úloha**. Cvičení jsou jednodušší, jejich řešení Ti zabere pár minut a slouží k osvěžení právě zažité teorie. Naproti tomu úlohy mohou být složitější, jsou podobné soutěžním úlohám v semináři a jejich řešení může trvat déle. Na cvičeních ani úlohách další obsah seriálu nijak nestaví, a proto můžeš číst dál, i když je nevyřešíš všechny. Cvičení i úlohy mají na konci dílu nápovědy a řešení.

Na závěr jsme připojili dvě trochu náročnější kapitoly. První je ukázka řešení úlohy Mezinárodní matematické olympiády (fajnšmekři ji můžou zkusit vyřešit sami – napovíme: zapotřebí je indukce). Ta úloha není jednoduchá a uvádíme ji proto, abychom ukázali, že i velmi složitá úloha může vyžadovat překvapivě málo složité teorie, ovšem hodně důvtipu! Pokud řešení úplně neporozumíš, nevěš hlavu, tato část není zásadní – je to spíše takový bonus. Druhým bonusovým pokročilým tématem je pak Cauchyho funkcionální rovnice.

Ke každé sérii přísluší tři soutěžní úlohy, na základě tohoto dílu se tedy můžeš pustit do úloh 1. seriálové série. Těšíme se na Tvoje řešení!

Úvod

Jednoho obzvlášť nezáživného odpoledne sedíš ve svém pokoji a snažíš se nějak zabít čas. Všimneš si krabice s dominovými kostkami, o kterou jsi léta nezavadil(a). A začneš je stavět do řady. Se zvláštní pečlivostí dbáš na to, aby rozestupy mezi dominy nebyly příliš široké. A po chvíli jsou všechna domina dokonale seřazená a tvoří dlouhého hada. Pohlédneš na svůj výtvor a jemně cvrnkneš do prvního domina. A další následují ...

Jak tento dominový princip souvisí s naším seriálem? Nejlépe si to ukážeme na motivační úloze.

Příklad. Ukaž, že pro všechna přirozená čísla n platí

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Vyzkoušejme nejprve, zda to vůbec platí pro několik nízkých čísel. Snadno vypočteme, že pro 1, 2 i 3 rovnost platí. Navíc nemusíme pokaždé sčítat znovu od 1 do n na levé straně – například pro $n = 4$ využijeme znalosti součtu pro $n = 3$, tedy pouze sečteme 6 a 4. Obdobně pokračujeme pro 5, pak 6 atd. Takto bychom mohli postupně ověřit hypotézu pro všechna čísla až do 100, do 1000, ..., nikdy ovšem nevyjmenujeme všechna přirozená čísla!

Klíčem je provést krok, ve kterém ověříme, že hypotéza platí i pro číslo o 1 vyšší (jako jsme to udělali pro 4, 5 a 6), jen jednou pro obecné přirozené číslo.

Řešení. Předpokládejme, že rovnost platí pro nějaké přirozené číslo k. Tedy

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Potom pro $k + 1$ máme

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Což je přesně daná rovnost pro $k + 1$. Ukázali jsme, že pokud rovnost platí pro k, platí i pro $k + 1$. Dohromady s ověřením, že vztah platí pro 1, dostáváme, že je platný i pro každé následující číslo, a tedy postupně pro všechna přirozená čísla.

To, co jsme právě předvedli, se nazývá vznešeně *důkaz matematickou indukcí*. Proč přesně to funguje? Teď přichází do hry náš příměr s dominem. *Indukční krok* aneb to, jak jsme ukázali, že pokud rovnost platí pro k, platí i pro $k + 1$, vlastně odpovídá pečlivému rozestavění domin, aby nebyla moc daleko od sebe. Potom stačí jedno cvrnknutí do počátečního domina neboli *základní krok*, ve kterém jsme ověřili rovnost pro $n = 1$, a každé další domino už zcela jistě spadne. A naše tvrzení tak platí pro každé přirozené číslo.

Shrňme si postup důkazu: Chceme ukázat, že tvrzení $T(n)$ platí pro všechna přirozená čísla n. Důkaz matematickou indukcí probíhá ve třech krocích.

(1) Ukážeme, že tvrzení platí pro $n = 1$.
(2) Předpokládáme, že $T(k)$ je pravdivé. S tímto *indukčním předpokladem* ukážeme, že potom je i $T(k + 1)$ pravdivé.
(3) Potom tvrzení induktivně platí pro všechna přirozená čísla.

Počítáme aneb co všechno lze vyřešit indukcí

> *Mathematics presented with rigor is a systematic deductive science but mathematics in the making is an experimental inductive science.*
>
> – *G. Pólya*

Když z pozorovaného konkrétního jevu vyvodíme obecný závěr, říkáme tomu induktivní myšlení. Naproti tomu pomocí deduktivního myšlení jsme schopni dát dohromady obecné předpoklady a z nich usoudit na konkrétní logický důsledek. Ačkoli v matematických důkazech nejčastěji narazíte právě na dedukci, pravděpodobně jí předcházely hodiny zkoušení, pozorování a pokusů zobecnit pozorovanou skutečnost. Podobného procesu si všimni i u následujících problémů. K odhalení vztahu bylo zapotřebí induktivního myšlení a posléze k důkazu hypotézy použijeme dedukci ve

formě důkazu matematickou indukcí. Zde je nutné poznamenat, že i přes poněkud nešťastný název matematické indukce se jedná o důkazovou techniku, a tedy přesný opak induktivního myšlení.

Součty

Už jsme si ukázali, že součet prvních n přirozených čísel lze vyjádřit jako $\frac{n(n+1)}{2}$. Podívejme se na další zajímavé součty.

Příklad. Ukaž, že

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Řešení. Nejprve ověříme hypotézu pro $n = 1$. Levá strana je prostě 1, pravá strana je rovna $\frac{1\cdot 2\cdot 3}{6}$. Rovnost tedy platí.

Nyní předpokládejme, že rovnost platí pro přirozené číslo k. Potom

$$\begin{aligned} 1 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= (k+1) \cdot \frac{k(2k+1) + 6(k+1)}{6} \\ &= (k+1) \cdot \frac{2k^2 + 7k + 6}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6}, \end{aligned}$$

což je přesně výraz na pravé straně pro $n = k + 1$. Z matematické indukce pak plyne, že rovnost platí pro všechna přirozená čísla.

Cvičení 1. Dokaž, že pro všechna přirozená čísla n platí

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

Cvičení 2. Zjednoduš výraz

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)}.$$

Ukaž, že nalezená rovnost platí pro všechna přirozená čísla.

Cvičení 3. Zjednoduš součet

$$1\cdot 2\cdot 3 + 2\cdot 3\cdot 4 + \cdots + (n-1)n(n+1).$$

Matematickou indukcí nebo jiným způsobem ověř pravdivost svého řešení.

Cvičení 4. Zjednoduš výraz

$$1\cdot 2^0 + 2\cdot 2^1 + 3\cdot 2^2 + \cdots + n\cdot 2^{n-1}$$

a ověř jeho platnost pomocí indukce nebo jinak.

Dělitelnost

Definice. Mějme celá čísla m a n. Potom říkáme, že m *dělí* n, pokud existuje celé číslo k takové, že $n = mk$. Tuto skutečnost zapisujeme $m \mid n$.

Příklad. Ukaž, že pro každé přirozené číslo n platí $6 \mid 2n^3 + 3n^2 + n$.

Důkaz. Pro $n = 1$ dostáváme $2n^3 + 3n^2 + n = 2 + 3 + 1 = 6$, což je dělitelné šesti.

Předpokládejme nyní, že hypotéza platí pro $n = k$. Potom

$$\begin{aligned} 2(k+1)^3 + 3(k+1)^2 + (k+1) &= 2(k^3 + 3k^2 + 3k + 1) + 3(k^2 + 2k + 1) + (k+1) \\ &= (2k^3 + 3k^2 + k) + 6(k^2 + 2k + 1), \end{aligned}$$

což je dle indukčního předpokladu dělitelné šesti.

Podle matematické indukce pak tvrzení platí pro všechna přirozená čísla. □

Poznámka. Alternativně bychom mohli příklad řešit rozkladem na součin $n(n+1)(2n+1)$ a pozorováním, že právě jedno z těchto čísel je sudé a právě jedno je dělitelné třemi, jelikož pokud ani jedno z n, $n+1$ není dělitelné třemi, pak jejich součet jistě je.

Úloha 1. Ukaž, že mezi libovolnými 3^{k+1} čísly lze najít 3^k čísel, jejichž součet je dělitelný 3^k.

Úloha 2. Ukaž, že pro každé přirozené číslo n existuje číslo, jehož dekadický zápis obsahuje pouze cifry 1 a 2 a které je dělitelné 2^n.

Úloha 3. Nechť x je nenulové reálné číslo a $x + \frac{1}{x}$ je celé číslo. Ukažte, že potom $x^n + x^{-n}$ je celé číslo.

Nerovnosti

Pomocí matematické indukce umíme dokázat celou řadu zajímavých nerovností. Na jednu z nejznámějších nerovností si však počkáme až do kapitoly o Cauchyho indukci.

Příklad. Ukaž, že pro všechna přirozená čísla n platí nerovnost

$$V(n) = \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \geq \frac{1}{2}.$$

Důkaz. Pro $n = 1$ nerovnost zřejmě platí, resp. nastane rovnost.

V rámci indukčního kroku ukážeme, že součet na levé straně roste s rostoucím n, a tedy je stále větší než $\frac{1}{2}$. Rozdíl

$$\begin{aligned} V(n+1) - V(n) &= \left(\frac{1}{n+2} + \frac{1}{n+3} + \cdots + \frac{1}{2(n+1)}\right) - \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}\right) \\ &= \frac{1}{2n+1} + \frac{1}{2n+2} - \frac{1}{n+1} \\ &= \frac{1}{2n+1} - \frac{1}{2n+2} \end{aligned}$$

je kladný, což znamená, že každý další člen je o trochu větší.

Proto je-li $V(n)$ větší nebo roven $\frac{1}{2}$, tak i $V(n+1)$ je větší nebo roven $\frac{1}{2}$. Dle matematické indukce tvrzení platí pro všechna $n \in \mathbb{N}$. □

Příklad. Ukaž, že[1]

$$n! \geq 2^n$$

pro všechna přirozená čísla n větší nebo rovná 4.

Řešení. V tomto případě potřebujeme základní krok provést až pro $n = 4$. To jest $4! = 24 \geq 16 = 2^4$. Dalším krokem je předpokládat, že nerovnost platí pro $n = k$. Potom však

$$(k+1)! = (k+1)(k!) \geq (k+1) \cdot 2^k \geq 2 \cdot 2^k = 2^{k+1}.$$

Důkaz pak vyplývá z matematické indukce.

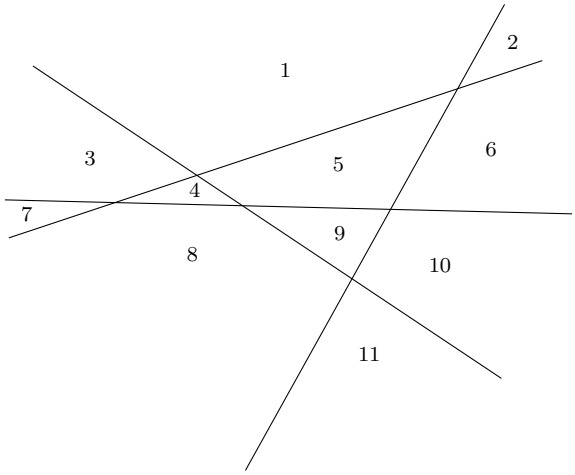
[1] Faktoriál přirozeného čísla n je součin přirozených čísel menších nebo rovných n, tedy $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$.

Úloha 4. Ukaž, že pro každé přirozené n větší nebo rovno 3 platí nerovnost

$$\sqrt{3}+\sqrt{4}+\cdots+\sqrt{n}<\frac{n^2}{4}.$$

Geometrie

Příklad. Mějme v rovině n přímek, z nichž žádné dvě nejsou rovnoběžné a žádné tři se neprotínají v jednom bodě. Na kolik oblastí přímky dělí rovinu?



Řešení. Tvrdíme, že odpověď je $1+\frac{n(n+1)}{2}$. Pro nula přímek tvrzení zřejmě platí.

Předpokládejme, že n přímek rozdělí rovinu na $1+\frac{n(n+1)}{2}$ částí. Zjistíme, kolik oblastí přibyde nakreslením další přímky. Protože nová přímka nesmí být rovnoběžná s žádnou z předchozích přímek a nesmí procházet žádným již nakresleným průsečíkem, jistě protne každou stávající přímku v právě jednom bodě a celkem přibyde n průsečíků. To znamená, že přibylo $n+1$ úseků mezi průsečíky, které rozdělily $n+1$ oblastí na dvě, celkem tedy přibylo $n+1$ oblastí. S použitím indukčního předpokladu je nyní oblastí celkem

$$1+\frac{n(n+1)}{2}+(n+1)=1+\frac{(n+1)(n+2)}{2}$$

a důkaz poté platí podle matematické indukce.

Cvičení 5. Mějme v rovině n kružnic, které ji dělí na několik oblastí. Ukaž, že lze jednotlivé oblasti obarvit dvěma barvami tak, aby spolu nesousedily žádné dvě oblasti stejné barvy.

Úloha 5. Mějme $2n$ bodů v rovině, kde n je větší než 1. Některé body spojíme úsečkami, nakreslíme celkem n^2+1 úseček. Ukaž, že jsme nakreslili alespoň jeden trojúhelník.

Úloha 6. Ukaž, že každý mnohoúhelník (ne nutně konvexní) lze rozdělit na trojúhelníky pomocí úhlopříček, které leží uvnitř mnohoúhelníku.

Tradiční úlohy

Příklad. Mějme n kanystrů s benzinem, rozmístěných po kruhové dráze. Rádi bychom si jeden okruh objeli, bohužel však máme prázdnou nádrž. Naštěstí víme, že v kanystrech je dohromady

právě takové množství pohonné hmoty, kolik potřebujeme na jedno kolo a kolik se vejde do nádrže. Auto můžeme umístit kamkoli na okruhu a doufat, že nám benzin z jednoho kanystru vydrží, než doplníme benzin z kanystru následujícího. Nebo doufat nemusíme? Ukaž, že lze pokaždé, ať je rozmístění kanystrů po dráze jakékoli a ať jsou jakákoli i množství benzinu v jednotlivých kanystrech (v součtu dávající plnou nádrž), vybrat startovací místo tak, abychom objeli celý okruh.

Řešení. Nejprve poznamenejme, že startovací místo musí být vždy u nějakého z kanystrů, protože na začátku je naše nádrž prázdná a potřebujeme doplnit benzin.

Pro $n = 1$ máme na dráze pouze jeden kanystr, a ten tedy musí obsahovat benzin na celé jedno kolo. Proto stačí umístit auto k tomuto kanystru a okruh pak hravě objedeme. Našli jsme tedy startovací místo pro $n = 1$.

Nyní předpokládejme, že pro $n = k$ jsme pokaždé schopni najít vhodné startovací místo. Je-li na dráze $k + 1$ kanystrů, ukážeme sporem, že vždy se najde takový, že benzin z něj vystačí na dojezd k dalšímu kanystru. Kdyby to totiž nešlo, pak by zcela jistě nevystačil benzin ze všech kanystrů dohromady na objetí celého okruhu, což je požadovaný spor.

Pojmenujme tento kanystr K_1 a kanystr po něm následující K_2. Představme si, že bychom odebrali kanystr K_2 a benzin z něj bychom přelili do kanystru K_1. Potom by na trati bylo k kanystrů a dle indukčního předpokladu bychom našli vhodné startovací místo.

Rozmysli si, že toto startovací místo funguje i pro předchozí uspořádání s $k+1$ kanystry. A jsme hotovi.

Cvičení 6. Adam a Berta hrají hru podle následujících pravidel. Mají n sirek a v každém tahu lze ubrat 1 až 4 sirky. Prohrává ten hráč, který už nemůže táhnout. Začíná Adam. Pro která n má Berta vyhrávací strategii?[2] Dokaž.

Úloha 7. V jisté zemi je každá cesta jednosměrná. Každá dvě města jsou propojena právě jednou přímou cestou. Ukaž, že můžeme nalézt město, do kterého se lze dostat z každého města buď přímo, nebo přes jedno jiné město.

Selhání indukce?

> *If we have no idea why a statement is true, we can still prove it by induction.* – *Gian-Carlo Rota*

Uvažme toto nepravdivé tvrzení a jeho falešný důkaz.

Příklad. Všichni koně na světě mají stejnou barvu.

Řešení. Indukcí podle n dokážeme tvrzení „Ve skupině n koní jsou všichni stejné barvy."

Základní krok je triviální – ve skupině o jednom koni mají nutně všichni koně stejnou barvu. Nyní předpokládejme, že tvrzení platí pro $n = k$, a uvažme skupinu $k+1$ koní $\{H_1, H_2, \ldots, H_{k+1}\}$. Podskupina $\{H_1, H_2, \ldots, H_k\}$ čítá k koní, a proto podle indukčního předpokladu mají všichni stejnou barvu. Stejně tak podskupina $\{H_2, H_3, \ldots, H_{k+1}\}$ obsahuje právě k koní, a tedy jsou všichni téže barvy. Obě podskupiny přitom mají společný průnik, proto jsou nutně obě podskupiny stejné barvy. A tedy i výsledná skupina je jednobarevná! Tím jsme dokázali indukční krok a z matematické indukce vyplývá dokazované tvrzení.

Toto je zcela jistě chybný závěr. Takže s důkazem musí být něco špatně. Najdeš co? Podívejme se na jiný problém.

[2] Vyhrávací strategie znamená, že hráč je schopen vyhrát, ať jeho protihráč táhne jakkoli.

Příklad. Účastníš se intenzivní letní školy, která se koná celý červenec. Těsně před začátkem školy vám profesor oznámí, že někdy během pobytu vás čeká zvláštní přepadový kvíz. Den kvízu bude vybrán tak, že až přijde, nebudete to čekat. Dokážeš přijít na to, kdy se test uskuteční?

Chvíli o tom přemýšlíš a dojde Ti, že kvíz nemůže být 31. července, protože je to poslední den pobytu. Kdyby do té doby nepřišel, všichni by čekali, že to musí přijít právě poslední den. Ale to znamená, že test nemůže být ani 30. července, protože jsme se již dopátrali toho, že 31. nebude, a tedy 30. je nyní poslední možný den. Obecně pokud se nemůže konat od n-tého dne dál, můžeš $(n-1)$-ního dne očekávat, že test přijde, a tedy test přijít nemůže. Induktivně dojdeme k závěru, že test se nemůže konat žádný den.

A přece, něco na tomto argumentu nehraje. Například předpokládejme, že kvíz dostanete 13. července. Tento výběr by Tě dozajista překvapil, neboť jsi právě usoudil(a), že žádný kvíz nebude. Tedy to nakonec přece jen byl přepadový test!

Tomuto paradoxu se též říká „paradox nečekané popravy“, kdy je příběh vyprávěn z pohledu vězně, který se dozví o „nečekané“ popravě. Je to vskutku zneklidňující paradox! Tady se ovšem do jeho rozboru nebudeme nořit příliš hluboko. Jen poznamenáme, že profesorův výrok je velmi vágní – abychom o problému mohli logicky uvažovat, potřebovali bychom přesně stanovit, co znamená být „překvapený“ a „vědět“, že se test musí daný den uskutečnit. Dostali bychom se do oblasti filosofie, které se říká epistemologie.

Naštěstí pro nás, úlohy, kterými se zde budeme zabývat, spadají čistě do matematiky a její přesnost zabraňuje vzniku induktivních paradoxů.

Výstražný případ

Zatím se mohlo zdát, že ta skutečná práce při důkazu indukcí spočívá v dokázání indukčního kroku. Až by se jeden mohl troufale domnívat, že stačí dokázat indukční krok, protože první krok je přece jasný. Ukážeme si, že bez základního kroku to nejde.

Tvrzení. *Všechna kladná lichá čísla jsou dělitelná dvěma.*

Důkaz. Předpokládejme, že tvrzení platí pro všechna lichá čísla až do $n = k$. Následující liché číslo je $k + 2$. Dle indukčního předpokladu je k dělitelné dvěma, a proto i $k + 2$ musí být násobek dvou. Dle matematické indukce tvrzení platí pro všechna kladná lichá čísla. □

Tvrzení. *Pro všechna přirozená čísla n platí, že* $23 \mid 7^{2n+1} + 3^{n+2}$.

Důkaz. Základní krok je jasný, takže jej přeskočíme. Předpokládejme, že tvrzení platí pro $n = k$. Potom

$$7^{2(k+1)+1} + 3^{(k+1)+2} = 49 \cdot 7^{2k+1} + 3 \cdot 3^{k+2} = 3 \cdot \left(7^{2k+1} + 3^{k+2}\right) + 46 \cdot 7^{2k+1}.$$

Oba sčítance jsou dle indukčního předpokladu dělitelné 23, a proto je i konečný součet násobkem 23. Dle matematické indukce tvrzení tedy platí pro všechna přirozená čísla. □

Snadno ověříme, že ani jedno z předchozích tvrzení není pravdivé. Proto nepodceňujme základní krok.

Indukce a její aplikace

Bernoulliho nerovnost

Věta. *Mějme reálné číslo x větší než -1 a přirozené číslo n. Potom*

$$(1 + x)^n \geq 1 + nx.$$

Důkaz. Zvolme pevně reálné číslo $x > -1$. Použijeme indukci podle n. Nejprve ověříme nerovnost pro $n = 1$. Zjevně $1 + x \geq 1 + x$.

Nyní předpokládejme, že nerovnost platí pro $n \geq 1$. Potom

$$(1 + x)^{n+1} = (1 + x)^n(1 + x) \geq (1 + nx)(1 + x).$$

Použili jsme indukční předpoklad a také fakt, že $1 + x > 0$. Po roznásobení dostaneme

$$1 + (n + 1)x + nx^2,$$

což je větší než $1 + (n + 1)x$.

Matematickou indukcí dostáváme Bernoulliho nerovnost pro všechna přirozená čísla. □

Cvičení 7. Ukaž, že pro přirozené číslo n platí

$$\left(1 + \frac{1}{n}\right)^n \geq 2.$$

Úloha 8. Ukaž, že posloupnost $\{a_n\}_{n\geq 1}$, kde $a_n = \left(1 + \frac{1}{n}\right)^n$, je rostoucí.

Binomický rozvoj

Věta. *Pro reálné číslo x a přirozené číslo n platí*

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

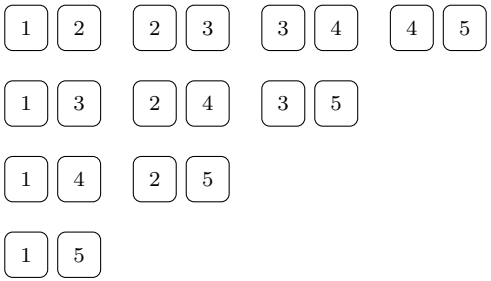
Nejprve si rozmysleme, co tato věta vlastně říká. Levá strana je prostě $(1 + x)$ umocněno na n-tou. Řecké písmeno *sigma* Σ na pravé straně je jen otázkou notace. Sumu můžeme rozepsat:

$$\sum_{k=0}^{n} \binom{n}{k} x^k = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \cdots + \binom{n}{n-1} x^{n-1} + \binom{n}{n} x^n.$$

$$\begin{array}{rl} \text{... až do } n\text{ \{} & \\ & \sum_{k=0}^{n} \binom{n}{k} x^k \\ k \text{ jde od } 0 \text{ ... \{} & \end{array}$$

$$\underbrace{\qquad\qquad}_{\text{tyto členy sčítáme}}$$

Dále je třeba objasnit, co znamená to záhadné $\binom{n}{k}$. Jedná se *kombinační číslo*, které vyjadřuje, kolika způsoby můžeme vybrat k objektů z množiny n objektů. Například $\binom{5}{2}$ je počet způsobů, jak z pěti objektů vybrat neuspořádanou dvojici. Těch je (jak ukazuje obrázek níže) deset, tedy $\binom{5}{2} = 10$.



Představme si, že vybíráme k karet z balíčku s n kartami a taháme je po jedné. Pro první kartu máme n možností, potom pro druhou zbývá už jen $n-1$ možností výběru a tak dále, až vybereme k-tou kartu ze zbývajících $n+1-k$ karet. To dává

$$n(n-1)(n-2)\cdots(n+1-k)$$

možností. Musíme si ovšem uvědomit, že některé skupinky po k kartách se opakují – stejnou skupinu určitých k karet lze totiž vybrat v několika různých pořadích. Kolik je těchto pořadí neboli kolika způsoby umíme seřadit k různých karet? Na první místo můžeme vybírat ze všech k karet, na druhé místo v pořadí nám jich zbývá jen $k-1$ a tak dále, až se dostaneme na poslední místo, na které už vyzbyla jediná karta. Máme tedy

$$k(k-1)(k-2)\cdots 3\cdot 2\cdot 1$$

seřazení k karet. Každou skupinku k karet z pytlíku jsme tedy vybrali přesně tolikanásobně! Proto je počet různých k-skupinek z n karet právě

$$\frac{n(n-1)(n-2)\cdots(n-(k-1))}{k(k-1)(k-2)\cdots 3\cdot 2\cdot 1}.$$

Pro ulehčení používáme zkrácený zápis pomocí *faktoriálu*[3], kdy

$$k! = k(k-1)\cdots 2\cdot 1.$$

Konečně tedy můžeme psát

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-(k-1))}{k(k-1)(k-2)\cdots 3\cdot 2\cdot 1} = \frac{n!}{(n-k)!k!}.$$

Nyní už chápeme, co binomická věta říká, pojďme se tedy podívat na pár příkladů.

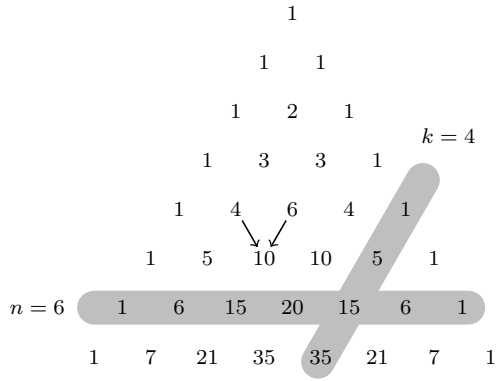
Pro $n=2$ dostáváme známý vzorec

$$(1+x)^2 = 1+2x+x^2.$$

Někteří možná ze školy znáte vzorec pro třetí mocninu

$$(1+x)^3 = 1+3x+3x^2+x^3.$$

Koeficientům jednotlivých mocnin x se říká *binomické koeficienty*. Binomické koeficienty tvoří řádky *Pascalova trojúhelníku*. Ten vzniká tak, že do horního vrcholu napíšeme 1 a potom každé další číslo je součtem dvou čísel nad sebou, jak ukazuje obrázek.



[3] Z kombinatorických důvodů máme $0! = 1$.

Pojďme si nyní binomickou větu dokázat jak jinak než pomocí matematické indukce!

Důkaz. Postupujme indukcí podle n. Ověříme hypotézu pro $n = 1$, máme

$$(1+x)^1 = \binom{1}{0} + \binom{1}{1} x.$$

Nyní předpokládejme, že rovnost platí pro nějaké n. Potom

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)(1+x)^n \\
&= (1+x) \sum_{k=0}^{n} \binom{n}{k} x^k \\
&= \sum_{k=0}^{n} \left(\binom{n}{k} x^k + \binom{n}{k} x^{k+1} \right) \\
&= \binom{n}{0} + \sum_{k=0}^{n-1} \left(\binom{n}{k} + \binom{n}{k+1} \right) x^{k+1} + \binom{n}{n} x^{n+1} \\
&= \binom{n}{0} + \sum_{k=0}^{n-1} \binom{n+1}{k+1} x^{k+1} + \binom{n}{n} x^{n+1} \\
&= \binom{n}{0} + \sum_{k=1}^{n} \binom{n+1}{k} x^{k} + \binom{n+1}{n+1} x^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k,
\end{aligned}$$

takže rovnost platí i pro $n+1$. V pátém řádku jsme použili rovnost $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$, která je znázorněna i v Pascalově trojúhelníku.

Důkaz poté vyplývá z matematické indukce. □

Cvičení 8. Ukaž, že platí

$$\sum_{j=k}^{n} \binom{j}{k} = \binom{n+1}{k+1}.$$

Trigonometrie

Trigonometrické funkce *sinus* a *cosinus* znáš ze školy. Tyto funkce jsou neskutečně zajímavé a byla by škoda, kdybychom se aspoň lehce nepodívali na některé z jejich vlastností, které lze dokázat indukcí.

Příklad. Dokaž rovnost

$$\sin x + \sin 2x + \cdots + \sin nx = \frac{\sin\left(\frac{n+1}{2}x\right) \sin\left(\frac{n}{2}x\right)}{\sin \frac{x}{2}},$$

kde $x \neq 2k\pi$ pro žádné $k \in \mathbb{Z}$.

Důkaz. Pro $n = 1$ máme platnou rovnost

$$\sin x = \frac{\sin x \sin \frac{x}{2}}{\sin \frac{x}{2}}.$$

V průběhu indukčního kroku budeme používat známé vztahy

$$\sin(A+B) = \sin A \cos B + \sin B \cos A,$$
$$\cos(A+B) = \cos A \cos B - \sin A \sin B.$$

Zvláště pak platí

$$\sin 2A = 2 \sin A \cos A,$$
$$\cos 2A = \cos^2 A - \sin^2 A.$$

V indukčním kroku předpokládejme, že rovnost platí pro $n = k$. Potom

$$\begin{aligned}
\sin x + \sin 2x + \cdots + \sin kx + \sin(k+1)x &= \frac{\sin\left(\frac{k+1}{2}x\right)\sin\left(\frac{k}{2}x\right)}{\sin\frac{x}{2}} + \sin(k+1)x \\
&= \frac{\sin\left(\frac{k+1}{2}x\right)\sin\left(\frac{k}{2}x\right)}{\sin\frac{x}{2}} + 2\sin\left(\frac{k+1}{2}x\right)\cos\left(\frac{k+1}{2}x\right) \\
&= \frac{\sin\left(\frac{k+1}{2}x\right)}{\sin\frac{x}{2}} \cdot \underbrace{\left(\sin\left(\frac{k}{2}x\right) + 2\cos\left(\frac{k+1}{2}x\right)\sin\left(\frac{x}{2}\right)\right)}_{=V}.
\end{aligned}$$

Nyní se zblízka podívejme na výraz V v závorkách. Dostaneme

$$\begin{aligned}
V &= \sin\left(\frac{k}{2}x\right) + 2\cos\left(\frac{k+1}{2}x\right)\sin\left(\frac{x}{2}\right) \\
&= \sin\left(\frac{k}{2}x\right) + 2\sin\frac{x}{2}\left(\cos\left(\frac{k}{2}x\right)\cos\frac{x}{2} - \sin\left(\frac{k}{2}x\right)\sin\frac{x}{2}\right) \\
&= \sin\left(\frac{k}{2}x\right)\cdot\left(1-\sin^2\frac{x}{2}\right) - \sin\left(\frac{k}{2}x\right)\sin^2\frac{x}{2} + 2\cos\left(\frac{k}{2}x\right)\sin\frac{x}{2}\cos\frac{x}{2} \\
&= \sin\left(\frac{k}{2}x\right)\cdot\left(\cos^2\frac{x}{2} - \sin^2\frac{x}{2}\right) + 2\sin\frac{x}{2}\cos\frac{x}{2}\cos\left(\frac{k}{2}x\right) \\
&= \sin\left(\frac{k}{2}x\right)\cos x + \sin x\cos\left(\frac{k}{2}x\right) \\
&= \sin\left(\frac{k}{2}x + x\right).
\end{aligned}$$

Konečně tedy můžeme dát dohromady rovnost

$$\sin x + \sin 2x + \cdots + \sin kx + \sin(k+1)x = \frac{\sin\left(\frac{k+2}{2}x\right)\sin\left(\frac{k+1}{2}x\right)}{\sin\frac{x}{2}},$$

jak jsme chtěli ukázat.

Podle matematické indukce pak rovnost platí pro všechna $n \in \mathbb{N}$. □

Příklad. Pro všechna reálná čísla x a přirozená čísla n platí nerovnost

$$|\sin nx| \leq n\,|\sin x|.$$

Důkaz. Pro $n = 1$ tvrzení zřejmě platí.

Podrobnosti následujícího postupu si rozmysli v rámci cvičení níže. Předpokládejme, že hypotéza platí pro všechna $x \in \mathbb{R}$ a $n = k$. Potom

$$\begin{aligned} |\sin(k+1)x| &= |\sin kx \cos x + \sin x \cos kx| \\ &\leq |\sin kx| \cdot |\cos x| + |\sin x| \cdot |\cos kx| \\ &\leq |\sin kx| + |\sin x| \\ &\leq k\,|\sin x| + |\sin x| \\ &= (k+1)\,|\sin x| \end{aligned}$$

a dle principu matematické indukce nerovnost platí pro všechna $n \in \mathbb{N}$. □

Cvičení 9. Tato nerovnost neplatí obecně pro jakékoli n. Je důležité, že n je přirozené číslo. Najdi protipříklad, kdy nerovnost pro nějaké $n \in \mathbb{R}$ neplatí. Kde v důkazu využíváme fakt, že n je přirozené číslo?

Cvičení 10. Rozmysli si, z čeho vyplývají jednotlivé nerovnosti v důkazu předchozího tvrzení.

Cvičení 11. Ukaž, že pro všechna reálná čísla x různá od $2k\pi$ a všechna přirozená čísla n platí identita

$$\frac{1}{2} + \cos x + \cos 2x + \cdots + \cos nx = \frac{\sin\left(\frac{2n+1}{2}x\right)}{2\sin\frac{x}{2}}.$$

V hlavní roli silná indukce

Doteď jsme se zabývali pouze relativně přímočarou indukcí. Avšak některé problémy nelze rozlousknout tak jednoduše! Potřebujeme na ně o trochu *silnější* louskáček. Proto v této sekci objevíme „tu pravou sílu“ matematické indukce s přiléhavým názvem *silná indukce*. V čem spočívá její síla? Odpověď zní: v indukčním kroku. Pojďme se na to podívat podrobněji.

Chceme dokázat, že tvrzení $S(n)$ platí pro všechna přirozená čísla n.

(1) Ukážeme, že $S(0)$ je pravdivé.
(2) Zde přijde obměna! Předpokládáme totiž nejen to, že $S(k)$ platí, nýbrž že platí všechna tvrzení $S(0)$, $S(1)$, …, $S(k)$. S tímto silnějším předpokladem prokážeme pravdivost $S(k+1)$.
(3) A odměnou nám je, že dle principu silné matematické indukce platí tvrzení pro všechna přirozená čísla.

Rozmysleme si nyní, proč to funguje. Můžeme vůbec něco takového předpokládat? Jistěže ano – vrátíme-li se k analogii s dominem, tak využijeme faktu, že prvních n domin spadlo, abychom dokázali, že spadne i $(n+1)$-ní. Důkaz silnou indukcí je dokonce ekvivalentní důkazu běžnou indukcí!

Cvičení 12. Rozmysli si to jako cvičení.

Pro následující část se nám budou hodit Fibonacciho čísla.

Definice. Fibonacciho posloupnost $F(0)$, $F(1)$, $F(2)$, … je definovaná následujícím způsobem:

(1) $F(0) = 0$ a $F(1) = 1$.
(2) Pro přirozené číslo n platí $F(n+1) = F(n) + F(n-1)$.

Prvních několik členů Fibonacciho posloupnosti je tedy 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, …

Pojďme se nyní na silnou indukci podívat v akci.

Věta. (Zeckendorfova) *Každé přirozené číslo lze zapsat jako součet různých Fibonacciho čísel, z nichž žádná dvě nejsou ve Fibonacciho posloupnosti po sobě jdoucí.*

Podívejme se na několik zajímavých[4] čísel a zkusme je vyjádřit jako součet Fibonacciho čísel, která po sobě nenásledují:

$$\begin{aligned}
6 &= 5 + 1 \\
&= F(5) + F(2), \\
28 &= 21 + 5 + 2 \\
&= F(8) + F(5) + F(3), \\
496 &= 377 + 89 + 21 + 8 + 1 \\
&= F(14) + F(11) + F(8) + F(6) + F(2), \\
8128 &= 6765 + 987 + 233 + 89 + 34 + 13 + 5 + 2 \\
&= F(20) + F(16) + F(13) + F(11) + F(9) + F(7) + F(5) + F(3).
\end{aligned}$$

Všimni si, že žádná dvě čísla v součtu po sobě v posloupnosti nenásledují.

Důkaz. Důkaz povedeme silnou indukcí. Nechť $S(n)$ je tvrzení, že přirozené číslo n lze zapsat jako součet Fibonacciho čísel, která nejsou po sobě jdoucí:

První krok je snadný, číslo 1 je samo o sobě Fibonacciho číslo. Dále předpokládejme, že tvrzení platí pro $1, \ldots, k$ neboli že každé přirozené číslo až do k lze zapsat jako součet Fibonacciho čísel, z nichž žádná dvě nejdou po sobě. Uvažme číslo $k+1$. Pak existuje Fibonacciho číslo $F(x)$ pro nějaké $x \in \mathbb{N}$ takové, že

$$0 < F(x) \leq k + 1 < F(x+1),$$

tedy že číslo $k+1$ leží mezi dvěma Fibonacciho čísly nebo je rovno nižšímu z nich. Pokud nastane rovnost, jsme hotovi, jelikož $k+1$ lze zapsat jako $F(x)$. Pokud je $k+1$ ostře větší než $F(x)$, potom $\ell = k + 1 - F(x)$ je přirozené číslo nižší než $k+1$, a tedy dle indukčního předpokladu jej lze zapsat jako

$$\ell = F(i_1) + F(i_2) + \cdots + F(i_j),$$

kde indexy $i_1, i_2, \ldots, i_j$ jsou různé a nejsou po sobě jdoucí. Potom

$$k + 1 = F(i_1) + F(i_2) + \cdots + F(i_j) + F(x).$$

Tvrdíme, že Fibonacciho čísla v součtu jsou různá a nenásledují po sobě. Dokážeme to sporem. Bez újmy na obecnosti můžeme předpokládat, že $i_1 < i_2 < \cdots < i_j$. Protože $F(x)$ je největší Fibonacciho číslo, které je nižší než $k+1$, tak je $F(i_j)$ jistě menší nebo rovno $F(x)$. Proto nám stačí ukázat, že i_j a x nejsou po sobě jdoucí. Pro spor připusťme, že $F(x-1) \leq F(i_j)$. Potom však

$$\begin{aligned}
k + 1 &= F(i_1) + F(i_2) + \cdots + F(i_j) + F(x) \\
&\geq F(i_1) + F(i_2) + \cdots + F(x-1) + F(x) \\
&\geq F(x-1) + F(x) \\
&= F(x+1),
\end{aligned}$$

což je požadovaný spor. Takže jsme našli vhodná Fibonacciho čísla pro $k+1$, a tím jsme dle principu silné indukce hotovi. □

Poznámka. Všimni si, že k důkazu by nám nestačilo, že $S(k)$ platí. O číslu ℓ totiž nic moc nevíme, jen to, že je menší než $k+1$.

[4] Přijdeš na to, čím jsou tato čísla zajímavá?

Ještě více Fibonacciho čísel

Fibonacciho posloupnost má mnoho krásných vlastností. Zkus si některé z nich dokázat!

Cvičení 13. Ukaž, že pro všechna pro všechna přirozená čísla n platí

$$F(n-1)F(n+1) = F(n)^2 + (-1)^n.$$

Cvičení 14. Nechť $t_1 = 1$, $t_2 = 1 + \frac{1}{1}$, $t_3 = 1 + \frac{1}{1+\frac{1}{1}}$, ... Ukaž, že $t_n = \frac{F(n+1)}{F(n)}$.

Poznámka. Posloupnost $t_1, t_2, \ldots$ se postupně „přibližuje“ řešení rovnice $t = 1 + \frac{1}{t}$. Tu můžeme upravit na rovnici $t^2 - t - 1 = 0$, jejímž kladným kořenem je *zlatý řez* $\varphi = \frac{1+\sqrt{5}}{2}$. Proto se poměr dvou po sobě jdoucích Fibonacciho čísel postupně blíží zlatému řezu.

Úloha 9. Ukaž, že pokud $m \mid n$, tak $F(m) \mid F(n)$.

Cauchyho indukce aneb cesta tam a zase zpátky

Ačkoli není nijak závratně používaná, tato varianta matematické indukce ukazuje, jak flexibilní a silná dokáže indukce být. Tuto metodu posléze použijeme pro dokázání známé AG-nerovnosti. Bez většího otálení pojďme na to!

Chceme dokázat, že tvrzení $C(n)$ platí pro všechna přirozená čísla n.

(1) Provedeme základní krok: dokážeme $C(1)$.
(2) Následuje indukční krok, který tu má *dvě* části.
    Tam: Ukážeme implikaci „pokud platí $C(k)$, tak platí i $C(2k)$“.
    Zpátky: Ukážeme implikaci „pokud platí $C(m)$, tak platí i $C(m-1)$“.
(3) Potom tvrzení $C(n)$ platí pro všechna přirozená čísla n podle Cauchyho indukce.

Indukční krok **tam** zajišťuje, že tvrzení je pravdivé pro stále větší n, zanechává však značné mezery uprostřed. O ty se postará indukční krok **zpátky**.

AG-nerovnost

Známá a v olympiádách hojně využívaná nerovnost mezi aritmetickým a geometrickým průměrem přímo vybízí k důkazu matematickou indukcí. Běžným způsobem to ovšem nepůjde!

Věta. (AG-nerovnost) *Nechť $x_1, x_2, \ldots, x_n$ jsou nezáporná reálná čísla. Potom platí, že jejich aritmetický průměr je větší nebo roven jejich průměru geometrickému:*

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n}.$$

Důkaz. Všimněme si, že pokud jsou všechna čísla rovna 0, nerovnost automaticky platí. Proto můžeme dále předpokládat, že alespoň jedno číslo je nenulové (a jejich součet je tudíž nenulový, což se hodí, až tímto součtem budeme dělit).

Nejprve uvažme základní kámen $n = 2$:

$$\begin{aligned} \frac{x_1 + x_2}{2} \geq \sqrt{x_1 x_2} &\iff (x_1 + x_2)^2 \geq 4x_1 x_2 \\ &\iff x_1^2 - 2x_1 x_2 + x_2^2 \geq 0 \\ &\iff (x_1 - x_2)^2 \geq 0, \end{aligned}$$

což platí vždy, jelikož druhá mocnina reálného čísla je vždy nezáporná. Všimněme si také, že rovnost nastane právě tehdy, když $x_1 = x_2$.

Nyní se pusťme do indukčního kroku **tam**. Předpokládejme, že nerovnost platí pro k proměnných. Nechť $x_1, x_2, \ldots, x_{2k}$ je $2k$ nezáporných reálných čísel. Máme

$$\begin{aligned}\frac{x_1 + x_2 + \cdots + x_{2k}}{2k} &= \frac{\frac{x_1+x_2+\cdots+x_k}{k} + \frac{x_{k+1}+x_{k+2}+\cdots+x_{2k}}{k}}{2} \\ &\geq \frac{\sqrt[k]{x_1 x_2 \cdots x_k} + \sqrt[k]{x_{k+1} x_{k+2} \cdots x_{2k}}}{2} \\ &\geq \sqrt{\sqrt[k]{x_1 x_2 \cdots x_k}\,\sqrt[k]{x_{k+1} x_{k+2} \cdots x_{2k}}} \\ &= \sqrt[2k]{x_1 x_2 \cdots x_{2k}}.\end{aligned}$$

Nerovnosti výše vyplývají postupně z AG-nerovnosti pro k (indukčního předpokladu) a AG-nerovnosti pro 2 (kterou jsme již ukázali).

Tedy platí-li AG-nerovnost pro k, pak platí i pro $2k$. Zatím jsme tedy ukázali pravdivost nerovnosti pro $n = 2, 4, 8, 16, \ldots$ a zbývá nám vyplnit mezery. K tomu poslouží indukční krok **zpátky**.

Podle AG-nerovnosti pro m proměnných máme

$$\frac{x_1 + x_2 + \cdots + x_m}{m} \geq \sqrt[m]{x_1 x_2 \cdots x_m}.$$

Chceme ukázat AG-nerovnost pro $x_1, x_2, \ldots, x_{m-1}$. Dosaďme je do AG-nerovnosti pro m spolu s $x_m = \frac{x_1+x_2+\cdots+x_{m-1}}{m-1}$. Potom

$$\frac{x_1 + x_2 + \cdots + x_{m-1} + \frac{x_1+x_2+\cdots+x_{m-1}}{m-1}}{m} = \frac{x_1 + x_2 + \cdots + x_{m-1}}{m-1}.$$

AG-nerovnost pro m pak říká

$$\frac{x_1 + x_2 + \cdots + x_{m-1}}{m-1} \geq \sqrt[m]{x_1 x_2 \cdots x_{m-1} \cdot \frac{x_1 + \cdots + x_{m-1}}{m-1}}.$$

Můžeme obě strany umocnit na m, protože všechny proměnné jsou nezáporné. Dostáváme

$$\left(\frac{x_1 + x_2 + \cdots + x_{m-1}}{m-1}\right)^m \geq x_1 x_2 \cdots x_{m-1} \cdot \frac{x_1 + x_2 + \cdots + x_{m-1}}{m-1}.$$

Vydělíme kladným[5] $\frac{x_1+x_2+\cdots+x_{m-1}}{m-1}$, čímž dostaneme

$$\left(\frac{x_1 + x_2 + \cdots + x_{m-1}}{m-1}\right)^{m-1} \geq x_1 x_2 \cdots x_{m-1},$$

což následně odmocníme na požadovanou nerovnost

$$\frac{x_1 + x_2 + \cdots + x_{m-1}}{m-1} \geq \sqrt[m-1]{x_1 x_2 \cdots x_{m-1}}.$$

Dle principu Cauchyho indukce jsme hotovi. □

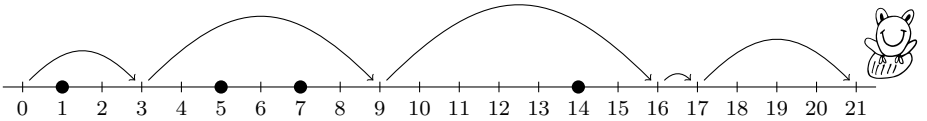
[5]Předpokládali jsme, že součet je nenulový.

IMO 2009/6

Indukce je přítelem chudého.
– staré bangladéšské pořekadlo

V této části si ukážeme rafinované použití indukce na úloze z Mezinárodní matematické olympiády.

Úloha 10. Nechť a_1, a_2, …, a_{n+1} jsou po dvou různá přirozená čísla. Nechť M je množina n přirozených čísel v intervalu $(0, s)$, kde $s = a_1 + a_2 + \cdots + a_{n+1}$. Žába skáče po číselné ose, začíná na bodu 0 a poté udělá $n+1$ skoků doprava o délkách a_1, a_2, …, a_{n+1} v nějakém pořadí. Dokaž, že může zvolit takové pořadí, že nikdy neskočí na žádné číslo z množiny M.



Řešení. Budeme postupovat indukcí podle n.

Základním krokem je ověřit, že tvrzení platí pro $n = 1$. Máme čísla a_1, a_2 a jedno číslo $m \in M$ z intervalu $(0, a_1 + a_2)$, kterému se chceme vyhnout. Jelikož jde jen o jedno číslo a čísla a_1, a_2 jsou různá, tak m může být nanejvýš jedno z těchto čísel. Pokud je různé od obou, jsme hotovi, a pokud je rovno jednomu z nich, zvolíme jako první skok to druhé číslo, čímž se číslu m hravě vyhneme. Tedy tvrzení pro $n = 1$ platí.

Pro indukční krok předpokládejme, že $n \geq 1$ a že tvrzení platí pro 1, 2, …, $n-1$. Bez újmy na obecnosti můžeme předpokládat, že $a_1 < \cdots < a_{n+1}$. Nechť m je nejmenší prvek M. Situaci rozdělíme na dva případy.

Případ 1: $m < a_{n+1}$

Nejprve předpokládejme, že $a_{n+1} \notin M$. Potom můžeme pro začátek poskočit o a_{n+1}. Přeskočili jsme m a použili jsme jeden skok, zbývají tedy $a_1, \ldots, a_n$ a nanejvýš $n-1$ čísel v M. Dle indukčního předpokladu toto již přeskákat lze.

Nyní nechť tedy $a_{n+1} \in M$. Uvažme následujících n dvojic: $(a_1, a_1 + a_{n+1}), \ldots, (a_n, a_n + a_{n+1})$. Je-li nějaké z čísel ve dvojicích v M, pak je i v $M \setminus \{a_{n+1}\}$, protože $a_i < a_{n+1} < a_i + a_{n+1}$ pro všechna $1 \leq i \leq n$. V $M \setminus \{a_{n+1}\}$ je ovšem jen $n-1$ členů, a proto existuje aspoň jedna dvojice, z níž ani jedno číslo není v $M \setminus \{a_{n+1}\}$. Označme ji $(a_k, a_k + a_{n+1})$. Pokud žabka udělá první dva skoky o délkách a_k a a_{n+1}, přeskočí jednak m, jednak a_{n+1}, což jsou obě čísla z množiny M. A před žabkou nyní stojí úkol vyhnout se $n-2$ číslům množiny $M \setminus \{m, a_{n+1}\}$ pomocí $n-1$ skoků délek $a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n$, což má řešení podle indukčního předpokladu.

Případ 2: $m \geq a_{n+1}$

Tento případ vyřešíme obráceně. Představíme si, že žába musí přeskákat z čísla $s = a_1 + a_2 + \cdots + a_{n+1}$ k nule. Pokud najdeme takovou cestu, můžeme ji vzít i pozpátku a jsme hotovi.

Podle indukčního předpokladu dokáže žabka udělat n skoků o délkách $a_1, \ldots, a_n$, aniž by skočila na nějaké číslo z množiny $M \setminus \{m\}$. Jestliže se navíc přitom vyhnula i číslu m, tak jednoduše doskočí poslední skok a jsme hotovi. Pokud nějakým skokem doskočila na číslo m, postupujme následovně: dejme tomu, že na m doskočila skokem délky a_k. Potom prohoďme v posloupnosti skoků a_k a a_{n+1}, pak žabka dopadne až za číslo m, to znamená blíže k nule. Díky tomu, že m je nejmenší

prvek M, víme, že žádné další nebezpečné číslo už před žabkou neleží a zbylé skoky už můžou být v libovolném pořadí. Tím jsme vyřešili i tento případ.

Matematickou indukcí pak dostáváme, že tvrzení platí pro všechna přirozená čísla.

Cauchyho funkcionální rovnice

Naši pouť zákoutími matematické indukce završíme důkazem světoznámé Cauchyho funkcionální rovnice. Funkcionální rovnice je rovnice, ve které je neznámou přímo funkce, tedy nějaký zobrazení z jedné množiny čísel do druhé.

Příklad. (Cauchyho funkcionální rovnice) Nechť $f : \mathbb{Q} \to \mathbb{R}$ je funkce, která pro všechna $x, y \in \mathbb{Q}$ splňuje

$$f(x + y) = f(x) + f(y).$$

Nalezni všechny takové funkce.

Řešení. Nejprve si všimněme, že všechny funkce tvaru $f(x) = cx$, kde $c \in \mathbb{R}$, splňují Cauchyho rovnici. Odvážně tvrdíme, že tohoto tvaru jsou všechna řešení Cauchyho rovnice.

Zkusíme položit $k = f(1)$ a hledat řešení rovnice, které bude zahrnovat k. Začneme tím, že položíme $x = y = 0$ a Cauchyho rovnice pak říká, že $f(0+0) = 2f(0)$, tedy $f(0) = 0$. Dále můžeme položit $x = y = 1$ a získat tak $f(2) = f(1) + f(1) = 2k$. Obdobně můžeme pokračovat pro $x = 2$ a $y = 1$ a dostat $F(3) = 3k$. Matematickou indukcí lze dokázat, že $f(n) = kn$ pro všechna $n \in \mathbb{N}$.

Jak toto rozšířit na záporná celá čísla? Dosaďme do rovnice $x = -n$, $y = n$, kde $n \in \mathbb{N}$. Potom $f(0) = f(-n) + f(n)$, takže $f(-n) = -f(n) = k \cdot (-n)$. Dohromady tedy $f(n) = kn$ pro všechna celá čísla n.

Ovšem stále jsme ještě nevyčerpali celý definiční obor funkce f, kterým jsou racionální čísla $\mathbb{Q}$. Zkusme se odrazit od toho, jak bychom určili hodnotu $f\left(\frac{1}{2}\right)$. Z rovnice vyplývá, že

$$f\left(\frac{1}{2}\right) + f\left(\frac{1}{2}\right) = f(1) = k,$$

z čehož plyne $f\left(\frac{1}{2}\right) = \frac{k}{2}$.

Inspirováni tímto vidíme, že pro racionální číslo $\frac{p}{q}$, kde a p, q jsou celá čísla a $q > 0$, máme

$$q \cdot f\left(\frac{p}{q}\right) = \underbrace{f\left(\frac{p}{q}\right) + f\left(\frac{p}{q}\right) + \cdots + f\left(\frac{p}{q}\right)}_{q\text{-krát}} = f(p) = kp,$$

a tedy $f\left(\frac{p}{q}\right) = k \cdot \frac{p}{q}$.

Došli jsme k závěru, že všechny funkce $f : \mathbb{Q} \to \mathbb{R}$, které splňují Cauchyho rovnici, jsou tvaru $f(x) = kx$ pro nějaké $k \in \mathbb{R}$.

Je nezbytné podotknout, že výběr definičního oboru funkce f je extrémně důležitý a kritický pro řešení úlohy. Náš postup fungoval, jelikož jsme schopni použít indukci na $\mathbb{N}$ a poté ji rozšířit na celou množinu $\mathbb{Q}$. Kdybychom za definiční obor vzali $\mathbb{R}$, náš postup by se zbortil na tom, že nemůžeme indukovat přes celé $\mathbb{R}$. Ba co víc, Cauchyho funkcionální rovnice v $\mathbb{R}$ začne mít opravdu podivná patologická řešení!

Závěrem

Gratulujeme k přečtení celého dílu! Doufáme, že Tě první díl obohatil jak novými znalostmi, tak zkušenostmi v řešení matematických úloh. V příštím díle se můžeš těšit na rigorózní zdůvodnění, proč indukce funguje, na několik axiomů a především na odvození základních aritmetických pravidel pouze na základě těchto axiomů!

My se na oplátku těšíme na Tvoje řešení úloh 1. seriálové série a přejeme mnoho štěstí.

Návody ke cvičením

1. Začni od pravé strany.

2. Vyjde součet $\frac{n}{n+1}$.

3. Vyjde $\frac{(n-1)n(n+1)(n+2)}{4}$.

4. Vyjde $(n-1)2^n + 1$.

5. Po přidání nové kružnice přebarvi její vnitřek.

6. Pro násobky 5. Indukce na k, kde $n = 5k$.

8. Použij indukci podle n.

9. Např. pro $n = \frac{1}{2}$ a $x = \pi$ nerovnost neplatí. Fakt, že n je přirozené, využívá z principu samotná indukce!

10. (i) Trojúhelníková nerovnost,
(ii) pro všechna $x \in \mathbb{R}$ je $|\cos x| \leq 1$,
(iii) indukční předpoklad.

12. Představ si, že máš důkaz silnou indukcí, kde $S(n)$ je n-té tvrzení. Víš tedy, jak ukázat, že platí-li $S(0)$, $S(1)$, …, $S(n)$, pak platí i $S(n+1)$. Zvol vhodně tvrzení $T(n)$ tak, aby důkaz vypadal tak, že dokážeme $T(n+1)$ pouze s pomocí $T(n)$. Co musí být dané tvrzení $T(n)$?

13. Použij indukci podle n. Vzpomeň si na rekurentní definici Fibonacciho čísel.

14. Všimni si, že $t_{n+1} = 1 + \frac{1}{t_n}$.

Návody k úlohám

1. Pro základní krok se podívej na zbytky, které čísla dávají po dělení 3 a použij Dirichletův princip. Indukční krok aplikuj několikrát, dokud nedostaneš aspoň 5 skupin, jejichž součet je dělitelný 3^{k-1}. Z nich vyber tři vhodné, jejichž součet bude dělitelný 3^k.

2. Lépe se bude dokazovat silnější tvrzení, a to že hledané číslo je n-ciferné.

3. Někdy je třeba v indukčním kroku předpokládat, že tvrzení platí pro předchozí dvě čísla namísto jednoho, tedy pro n a $n-1$. Této úpravě však musíš přizpůsobit základní krok a ověřit hypotézu pro $n = 1$ i pro $n = 2$.

4. Pokus se o indukční krok $T(n-1) \to T(n)$, použij substituci $x = \sqrt{n}$. Pro která n indukční krok funguje? Potom ověř ručně pro zbývající malá n.

5. Ukaž ekvivalentní tvrzení, a to „pokud mezi $2n$ body není žádný trojúhelník, tak jsme použili nanejvýš n^2 úseček“. V jazyce grafů[6]: Graf s $2n$ vrcholy, ve kterém není žádný trojúhelník, má nejvýše n^2 hran. V induktivním kroku uvažte dva body spojené úsečkou a zkoumejte, jak mohou vypadat jejich vztahy ke zbylým $2n$ bodům.

6. Lze vždy nalézt úhlopříčku, která celá leží uvnitř n-úhelníka? Potom použij silnou indukci (viz kapitolu *Silná indukce*).

7. Podle předpokladu jde mezi n městy najít město A takové, že do něj vede z každého města přímá cesta nebo cesta přes jedno jiné město. Rozděl města do dvou skupin podle toho, zda z nich do A vede přímá nebo nepřímá cesta. Poté přidej město B a podívej se na cesty z něj/do něj.

8. Nerovnost $a_n \leq a_{n+1}$ uprav na $\left(1 - \frac{1}{(n+1)^2}\right)^{n+1} \geq \frac{n}{n+1}$ a použij Bernoulliho nerovnost.

9. Rozmysli si, že to znamená, že pro všechna $n \in \mathbb{N}$ platí $F(k) \mid F(kn)$, kde k je libovolné přirozené číslo. Toto tvrzení pak už určitě rozlouskneš indukcí podle n.

[6] O grafech si můžeš přečíst v seriálu 34. ročníku Letem grafovým světem. *https://prase.cz/archive/34/serial.pdf*

Matematická indukce II – Recept na přirozená čísla

Milý příteli,

vítáme Tě u druhého dílu seriálu o matematické indukci! Možná sis všiml(a), že většina cvičení z minulého dílu počítá s přirozenými čísly. Často jsme chtěli dokázat, že nějaké tvrzení platí pro všechna přirozená čísla. Už samotný princip indukce je definovaný na přirozených číslech. Proto si v tomto díle položíme otázku, co jsou to vlastně ta přirozená čísla, a podíváme se na ně úplně od základů! Začneme axiomy, které definují přirozená čísla, a pouze na jejich základě odvodíme operace na přirozených číslech, jako je sčítání či násobení.

Tento díl se od prvního dílu liší tím, že při čtení je třeba mnohem víc abstraktního myšlení a pochopení některých zcela nových konceptů. V textu najdeš jednu velmi důležitou větu, nazvanou věta o rekurzi, kterou posléze využijeme k definování operací na přirozených číslech. Její důkaz je poměrně technický a nevadí, pokud se budeš místy ztrácet, pro pochopení dalšího textu nutný není.

Podnětné čtení Ti přejí

Káťa a Ittihad

Úvod

Bůh stvořil přirozená čísla, všechno ostatní je lidské dílo.
– Leopold Kronecker (1823–1891)

Odbočme nyní zdánlivě od tématu indukce a položme si otázku: Co jsou to přirozená čísla?

Můžeme je vyjmenovat: 1, 2, 3 a tak dále, každé další číslo je o 1 větší než to předchozí. Jenže tento seznam nám nic neřekne o jejich vlastnostech – jak funguje sčítání či násobení přirozených čísel? Máme-li dvě přirozená čísla, umíme je porovnat? Co víc, nelze vypsat všechna přirozená čísla – víme tedy, jak vypadají a jak se chovají velmi vysoká čísla? Je tento seznam opravdu nekonečný?

K samotnému vyjmenování přirozených čísel jsme potřebovali frázi „a tak dále“. V minulém díle jsme zjistili, že na argumentu „a tak dále“ vlastně stojí celý důkaz matematickou indukcí. Celou dobu jsme ovšem mlčky předpokládali, že všechna přirozená čísla lze takto induktivně pokrýt, žádnou záruku, že to jde, jsme však nedostali!

Aby naše důkazy nestály na zavádějícím a nejasném „a tak dále“, zahrneme matematickou indukci *přímo do definice* přirozených čísel.

Nejprve však zavedeme několik užitečných pojmů.

Funkce

If you are wandering down in Cornmarket and you bump into a second-hand function dealer and they try to sell you a function with only the rule part and not the domain or the codomain, please walk away! They're a dodgy, unscrupulous function dealer and you should not trade with them.
– Vicky Neale (University of Oxford)

Definice. *Zobrazení* f množiny A do množiny B je cokoli, co každému prvku a množiny A přiřadí právě jeden prvek množiny B. Ten pak značíme $f(a)$.

Zobrazení může být zadáno nějakým pravidlem, například zobrazení, které každému reálnému číslu x přiřadí jeho obraz x^2. Můžeme ale narazit i na zobrazení z množiny $\{1, 3, 7\}$ do množiny $\{2, 3, 4, 10\}$, které jedničce přiřadí 10, trojce přiřadí 4 a sedmičce přiřadí 10. Navíc množiny A a B ani nemusí být množiny čísel, ale např. množiny trojúhelníků v rovině, zvířat v zoo, žáků 3.B atd.

Termín *cokoli* v předchozí definici se může zdát poněkud vágní. Zobrazení neboli funkci můžeme přesněji definovat pomocí množin – představme si, že naše funkce páruje prvky množiny A s prvky z B. Výčtem uspořádaných dvojic $(a, f(a))$ pak funkci f jasně popíšeme. Množinu všech uspořádaných dvojic (a, b), kde $a \in A$ a $b \in B$ nazýváme kartézským součinem a značíme ji $A \times B$. To inspiruje následující definici:

Definice. Nechť jsou A a B množiny. *Funkce* $f\colon A \to B$ je taková *podmnožina* f množiny $A \times B$, pro kterou platí

(i) pro všechna $a \in A$ existuje $b \in B$ takové, že $(a, b) \in f$,
(ii) tento prvek b je právě jeden, tedy pokud $(a, b) \in f$ a současně $(a, c) \in f$, potom $b = c$.

Poznámka. Důležité je, že funkce f vždy „chodí společně“ s množinami A a B! Je důležité uvést, odkud a kam funkce posílá prvky.[1]

Ukážeme si to na příkladu funkce $f\colon \mathbb{R} \to \mathbb{R}$ dané předpisem $f(x) = x^2$. Zde bychom funkci popsali pomocí uspořádaných dvojic (x, x^2) pro každé $x \in \mathbb{R}$. Tyto dvojice můžeme znázornit grafem funkce, který znáte ze školy – každý bod paraboly odpovídá jedné z dvojic. Mezi dvojicemi, které popisují naši funkci, by byly například $(0, 0)$, $(1, 1)$, $(2, 4)$, ale i $(-1, 1)$ nebo $(-5, 25)$.

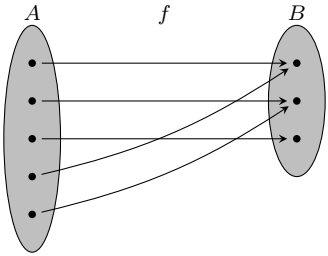
Cvičení 1. Kolik existuje funkcí z množiny $A = \{1, 2, 3\}$ do množiny $B = \{0, 1\}$?

Podotkněme, že není nutné, aby všechny prvky množiny B byly použity. Stejně tak není nutné, aby byly prvkům množiny A přiřazeny různé prvky množiny B. To vede k následujícím definicím:

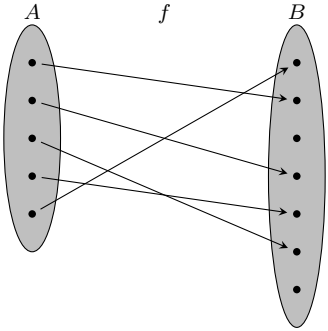
[1] Viz citát výše.

Definice. Nechť $f\colon A \to B$ je funkce. Potom:

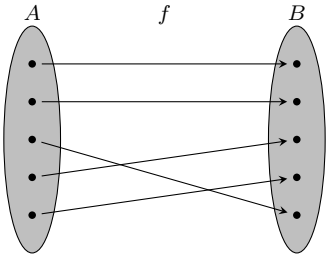
(i) f je *na*, pokud pro každé $b \in B$ existuje $a \in A$ takové, že $f(a) = b$.



(ii) f je *prostá*, jestliže pro všechna $x, y \in A$ platí, že pokud $f(x) = f(y)$, tak nutně $x = y$.



(iii) f je *bijekce*, pokud je zároveň prostá a na.



Peanovy axiomy

Mathematical induction is a definition, not a principle.
– Bertrand Russell (1872–1970)

Naším cílem v této kapitole bude definovat přirozená čísla. Velmi zajímavé a možná na první pohled zarážející je to, že přirozená čísla definuje právě možnost dělat na nich indukci. Všechny další

vlastnosti, jako je způsob počítání s přirozenými čísly nebo jejich pořadí, potom z této vlastnosti vyplývají.

Bude se nám hodit pracovat i s nulou jako přirozeným číslem, proto rozšiřme množinu $\mathbb{N}$ na množinu přirozených čísel s nulou, kterou označíme $\mathbb{N}_0$. Ve zbytku textu budeme nulu považovat za přirozené číslo.

Přirozená čísla po sobě následují. Začneme nulou, pokaždé přičteme 1 a opakujeme. Tuto vlastnost chceme zahrnout do definice.

Zavedeme proto funkci $s\colon \mathbb{N}_0 \to \mathbb{N}_0$, kterou nazveme *následník*[2], jež bude vystihovat to, že jedno číslo následuje po jiném, tedy $s(1) = 2$, $s(2) = 3$ a podobně.

Zamysleme se nad tím, co bychom od této funkce chtěli, aby nám definovala přirozená čísla. Zaprvé, číslo 0 není následníkem žádného čísla. Zadruhé, známe-li následníka nějakého čísla, je toto číslo už jednoznačně určeno (neboli dvě různá čísla nemohou mít stejného následníka). Zatřetí, tato funkce musí mít určitou vlastnost, kterou využijeme při indukci. Při důkazu matematickou indukcí jsme nejprve ukázali, že tvrzení platí pro 0 a poté jsme dokázali, že platí-li pro n, tak platí i pro $n+1$. Tím byl důkaz završen – tvrzení platí pro všechna přirozená čísla. Něco podobného vyslovme v jazyce množin, vždyť přirozená čísla jsou také množina:

„Předpokládejme, že S je podmnožina $\mathbb{N}_0$, která obsahuje nulu a pro kterou platí, že pokud $n \in S$, tak i $s(n) \in S$. Potom $S = \mathbb{N}_0$."

Ukáže se, že pouhé tyto tři vlastnosti naprosto stačí k jednoznačné definici přirozených čísel!

Představíme *Peanovy axiomy*, které pro definování množiny přirozených čísel zavedl italský matematik konce 19. století Giuseppe Peano.

Peanovy axiomy. *Předpokládejme, že existuje množina $\mathbb{N}_0$ a funkce $s\colon \mathbb{N}_0 \to \mathbb{N}_0$ taková, že:*

(1) *Funkce s není na: existuje prvek $0 \in \mathbb{N}_0$ takový, že pro žádné $n \in \mathbb{N}_0$ neplatí $s(n) = 0$.*
(2) *Funkce s je prostá: je-li $s(m) = s(n)$, potom $m = n$.*
(3) *Je-li S podmnožina $\mathbb{N}_0$ taková, že $0 \in S$ a pro všechna $n \in \mathbb{N}_0$ platí $n \in S \implies s(n) \in S$, potom $S = \mathbb{N}_0$.*

Poznámka. Všimněme si, že $s\colon \mathbb{N}_0 \to \mathbb{N}_0$ znamená, že pro přirozené číslo n platí, že jeho následník $s(n)$ je také přirozené číslo, tedy množina $\mathbb{N}_0$ je *uzavřená na operaci s*.

Nic nám nezaručuje, že daná množina skutečně existuje, proto vezmeme její existenci jako axiom neboli tvrzení, které považujeme za pravdivé a nedokazujeme jej. Je to jako můstek, od kterého se musíme odrazit, chceme-li vůbec nějak dál v matematice pracovat.

Axiom. (existence přirozených čísel) *Existuje množina $\mathbb{N}_0$ a funkce $s\colon \mathbb{N}_0 \to \mathbb{N}_0$, které splňují Peanovy axiomy výše.*

Z 2. axiomu plyne, že různá čísla mají různé následníky. Proto pokud číslo má předchůdce, pak je jen jeden. Která čísla ovšem mají předchůdce mají?

Tvrzení. *Pro každé $n \in \mathbb{N}_0$ různé od 0 existuje právě jedno $m \in \mathbb{N}_0$ takové, že $n = s(m)$.*

Důkaz. Chceme ukázat, že pro libovolné $n \in \mathbb{N}_0$ je buď $n = 0$, nebo $n = s(m)$ pro nějaké $m \in \mathbb{N}_0$. Využijeme k tomu třetí Peanův axiom a indukci, a to tak, že sestrojíme množinu S obsahující ta čísla n, pro která to platí, a pak ukážeme, že $S = \mathbb{N}_0$.

Nechť $S = \{n \in \mathbb{N}_0;\ n = 0 \text{ nebo } n = s(m) \text{ pro nějaké } m \in \mathbb{N}_0\}$. Jistě platí, že $0 \in S$. Nyní předpokládejme, že číslo n je v S, a pokusme se ukázat, že potom je i $s(n)$ v S. Co lze říct o číslu $s(n)$? Jistě $s(n) = s(m)$ pro nějaké $m \in \mathbb{N}_0$, konkrétně pro $m = n$. Tedy $s(n) \in S$. Podle třetího Peanova axiomu pak platí, že $S = \mathbb{N}_0$, což jsme chtěli ukázat. □

[2] Anglicky je to *successor*, a proto ji značíme s.

Aritmetika

Označení *přirozená čísla* zřejmě pochází z lidské zkušenosti – již starověké civilizace používaly právě čísla 1, 2, ... k počítání každodenních věcí, měření délek a porovnávání množství. Tato čísla se prostě používala k zacházení s přirozeně se vyskytujícími jevy. Např. záporná čísla do tohoto konceptu nepatřila, neboť nelze mít méně než nic (záporné množství lidé ještě neuvažovali), o racionálních, iracionálních či komplexních číslech ani nemluvě.

Přirozená čísla se tedy vyvinula jako čísla používaná k počítání. K tomu budeme potřebovat dvě základní operace, sčítání a násobení.

Uvažme nejprve sčítání. Mějme dva košíky jablek, v jednom 10 a ve druhém 7 kusů ovoce. Představme si, že zatím neumíme sčítat z paměti. Jak zjistíme, kolik jablek máme dohromady? Nejprve spočítáme jablka v prvním košíku, 1, 2, ..., 10, poté bereme do ruky jedno jablku z druhého košíku po druhém a pokračujeme přitom s vyjmenováváním čísel 11, 12, ..., 17. Navíc víme-li, jak přičíst číslo 7, potom umíme přičíst i číslo 8 – prostě přidáme jedno jablko. Na základě této zkušenosti bychom rádi definovali sčítání takto:

$$m + (n + 1) = (m + n) + 1.$$

Jedná se o rekurzivní definici – víme-li, jak přičíst n, tak víme i to, jak přičíst $n + 1$.

Potřebujeme ovšem ještě nějaký základní kámen, od kterého se odrazíme. Tím pro nás bude přičítání nuly, tedy vlastnost, že nepřidáme-li žádné jablko, počet jablek se nezmění.

$$m + 0 = m.$$

Je tu ovšem jistý zádrhel: Zaprvé, abychom k číslu m přičetli $n+1$, potřebujeme již znát hodnotu $m + n$. Tu můžeme získat postupným přičítáním jednotek k číslu m, dokud se nedostaneme na hodnotu n. To je intuitivní přístup, v naší definici podle Peanových axiomů ovšem není řečeno, zda se takto vůbec někdy dobereme čísla n.

Abychom dali rekurzivní definici pevný rámec a zároveň se vyhnuli slovnímu spojení „a tak dále, dokud nenarazíme na n“, dokážeme si následující větu pro obecný případ, kterou poté aplikujeme ve vhodných podmínkách.

Věta. (o rekurzi) *Mějme množinu X a funkci $f\colon X \to X$. Nechť $c \in X$. Potom existuje právě jedna funkce $\varphi\colon \mathbb{N}_0 \to X$ taková, že*

(1) $\varphi(0) = c$,
(2) $\varphi(s(n)) = f(\varphi(n))$ *pro každé* $n \in \mathbb{N}_0$.

Poznámka. Funkce φ nám tedy říká, kolikrát jsme aplikovali funkci f na prvek c, jedná se o opakovanou kompozici funkce f. Máme

$$\varphi(n) = f^n(c) = \underbrace{f(f(\cdots f(}_{n\text{-krát}} c)\cdots)).$$

Chceme ukázat to, že taková funkce existuje a že je jen jedna (pro dané f a c). Když později nahradíme f funkcí s, potvrdíme tak, že rekurzivní definice sčítání dává smysl neboli že je *dobře definovaná*.

Důkaz. Nejprve se ohlédněme a vzpomeňme si, co je to funkce. Funkci jsme si zadefinovali jako množinu uspořádaných dvojic, která splňuje dva požadavky: každý prvek vstupní množiny je v nějaké dvojici a tato dvojice je jedinečná.

My navíc potřebujeme, aby funkce φ splňovala body (1) a (2), tedy aby byla takovou podmnožinou $\mathbb{N}_0 \times X$, že

(1) $(0, c) \in \varphi$,
(2) pokud $(n, x) \in \varphi$, tak také $(s(n), f(x)) \in \varphi$.

Podmnožin splňujících body (1) a (2) (které však nemusí být funkce) je mnoho, např. i celá množina $\mathbb{N}_0 \times X$. My ukážeme, že ta, kterou hledáme (tj. která bude zároveň funkcí), je průnikem všech podmnožin splňujících body (1) a (2). Jinými slovy to znamená, že naše hledaná podmnožina je nejmenší možná.

Nechť φ je průnikem všech podmnožin $U \subset \mathbb{N}_0 \times X$, pro které platí

(1) $(0, c) \in U$
(2) pokud $(n, x) \in U$, tak také $(s(n), f(x)) \in U$.

Nejprve ukážeme, že se jedná o funkci. To znamená ukázat, že pro každé $n \in \mathbb{N}_0$ existuje právě jedno $x \in X$ takové, že $(n, x) \in \varphi$. Ukážeme to pomocí indukce, tedy s využitím třetího Peanova axiomu.

Nechť $S = \{n \in \mathbb{N}_0;\ (n, x) \in \varphi$ pro nějaké $x \in X\}$ je množina všech přirozených čísel, pro která existuje nějaká funkční hodnota x. Podle první podmínky je $0 \in S$. Nyní pokud $n \in S$, tak existuje $x \in X$, pro které $(n, x) \in \varphi$, a proto podle druhé podmínky také $(s(n), f(x)) \in \varphi$. Jelikož $f(x) \in X$, získáváme $s(n) \in S$ a induktivně podle třetího axiomu pak $S = \mathbb{N}_0$.

Tedy pro každé $n \in \mathbb{N}_0$ existuje alespoň jedna dvojice (n, x). Chceme ukázat, že tato dvojice je jen jedna, což bude znamenat, že φ definuje funkci. K tomu využijeme podmínku, že φ je průnikem všech podmnožin $\mathbb{N}_0 \times X$, které splňují (1) a (2).

Nechť $T = \{n \in \mathbb{N}_0;\ (n, x) \in \varphi$ pro právě jedno $x \in X\}$ je množina všech přirozených čísel, pro něž existuje jedinečná funkční hodnota x. Ověříme, že $T = \mathbb{N}_0$.

Nejprve ukážeme, že $0 \in T$. Pro spor předpokládejme, že existuje $d \neq c$, pro které $(0, d) \in \varphi$. Uvažme množinu $\varphi^* = \varphi \setminus \{(0, d)\}$. Potom $(0, c) \in \varphi^*$, a pokud $(n, x) \in \varphi^*$, tak $(s(n), f(x)) \in \varphi^*$. To platí, protože $(s(n), f(x))$ rozhodně není odebranou dvojicí $(0, d)$, jelikož $0 \neq s(n)$ pro žádné $n \in \mathbb{N}_0$. Jenže $\varphi^* \subset \varphi$ splňuje podmínky (1) a (2), což je ve sporu s předpokladem, že φ je průnikem všech takových podmnožin. Tedy $0 \in T$.

Obdobně ukážeme, že pokud $n \in T$, tak také $s(n) \in T$. Předpokládejme tedy, že $(n, x) \in \varphi$ pro jedno jediné $x \in X$. Potom podle (2) platí $(s(n), f(x)) \in \varphi$. Pro spor nechť existuje $y \neq f(x)$ takové, že $(s(n), y) \in \varphi$. Sestrojme tentokrát $\varphi^* = \varphi \setminus \{(s(n), y)\}$. Potom $(0, c) \in \varphi^*$. Mějme $(m, z) \in \varphi^*$. Chceme ukázat, že potom $(s(m), f(z)) \in \varphi^*$. Buď $m = n$, potom $z = x$ a víme, že $(s(m), f(z))$ ve φ^* leží. Nebo platí $m \neq n$. V tom případě $(s(m), f(z)) \in \varphi^*$, protože $(s(m), f(z)) \in \varphi$ podle (2) a zároveň $s(m) \neq s(n)$ podle 2. axiomu, takže jsme tuto dvojici nemohli vyhodit jako $(s(n), y)$. V každém případě pro φ^* platí (2), což je spor s tím, že φ je nejmenší podmnožinou splňující body (1) a (2).

Z toho plyne, že pokud $n \in T$, tak také $s(n) \in T$. Potom podle třetího axiomu $T = \mathbb{N}_0$.

Dokázali jsme, že takto sestrojené φ je funkce, která splňuje podmínky věty o rekurzi. Navíc tato funkce je jen jedna. Předpokládejme totiž, že máme jinou funkci ψ, která také řeší naše zadání. Potom je z definice naše sestrojená funkce φ podmnožinou ψ. Ale z funkce nelze už nic škrtnout, jinak by nebyla definovaná na celém oboru, a proto $\varphi = \psi$. Tím jsme hotovi. □

K čemu nám věta o rekurzi bude? Už dříve jsme naťukli, že součet dvou čísel můžeme definovat pomocí opakovaného přičítání čísla 1. Dosaďme za f funkci následník s a za c nějaké počáteční číslo. Potom funkci φ můžeme chápat jako operaci „přičti to k danému číslu c“. Druhá část věty o rekurzi se pak přemění na tvrzení „nejprve vzít následníka čísla n a poté ho přičíst je stejné, jako nejprve přičíst číslo n a poté vzít následníka součtu“. Pokud tedy za f vezmeme funkci následník s, pak nám věta o rekurzi říká, že součet, kterého se takto dobereme, je právě jeden. To je důležité, protože když definujeme operaci, musíme se ujistit, že nám ta operace vyhodí právě jeden výsledek.

Poznámka. Pro lepší pochopení toho, co se myslí pojmem „dobře definovaná operace“, zabrousíme do počítání modulo 3. Nejde o nic jiného, než že číslo n nahradíme jeho zbytkem po dělení 3.

Toto číslo pak značíme n_3.[3] Např. $32_3 = 2_3$ a $4_3 = 1_3$. Představme si, že bychom rádi definovali mocnění modulo 3. Intuitivně zkusíme definovat

$$(m_3)^{n_3} = (m^n)_3,$$

tedy že vezmeme-li dvě čísla m a n, pak dostaneme stejný výsledek, když nejprve vezmeme zbytky těch čísel a umocníme, jako když nejprve umocníme a potom vezmeme zbytek. Ovšem potom

$$1_3 = 4_3 = (2^2)_3 = (2_3)^{2_3} = (2_3)^{5_3} = (2^5)_3 = 32_3 = 2_3,$$

což je zjevný nesmysl – umocněním čísla 2_3 postupně na čísla 2_3 a 5_3 jsme dostali různé výsledky, přitom však $2_3 = 5_3$, a tedy bychom měli získat stejný výsledek. Toto se stalo právě proto, že naše operace nebyla dobře definovaná.

Nyní můžeme definovat mnohé rekurzivní operace na přirozených číslech pro dané $m \in \mathbb{N}_0$.

(1) *Sčítání* $\alpha_m \colon \mathbb{N}_0 \to \mathbb{N}_0$.
Operace sčítání je definována rekurzivně takto:

$$\begin{aligned} \alpha_m(0) &= m, \\ \alpha_m(s(n)) &= s(\alpha_m(n)). \end{aligned}$$

Budeme používat běžné značení $\alpha_m(n) = m+n$, a proto předchozí dvě rovnosti lze přeložit jako $m + 0 = m$ a $m + (n + 1) = (m + n) + 1$.

K tomu, aby bylo sčítání dobře definované, jsme využili větu o rekurzi s $c = m$ a $f = s$.

(2) *Násobení* $\mu_m \colon \mathbb{N}_0 \to \mathbb{N}_0$.
Násobení rekurzivně definujeme pomocí

$$\begin{aligned} \mu_m(0) &= 0, \\ \mu_m(s(n)) &= \mu_m(n) + m. \end{aligned}$$

Tentokrát jsme ve větě o rekurzi položili $c = 0$ a $f(x) = x + m$.

Násobení zapisujeme jako obvykle $\mu_m(n) = mn$. Použitím tohoto zápisu na předchozí dvě rovnice dostaneme $m \cdot 0 = 0$ a $m(n + 1) = mn + m$.

Všimněme si, že k samotné definici násobení jsme potřebovali mít už zadefinované sčítání.

(3) *Mocnění* $\pi_m \colon \mathbb{N}_0 \to \mathbb{N}_0$.
Mocniny definujeme rekurzivně pomocí

$$\begin{aligned} \pi_m(0) &= 1, \\ \pi_m(s(n)) &= m\pi_m(n). \end{aligned}$$

Zde jsme položili $c = 1$ a $f(r) = rm$.

Běžně zapisujeme $\pi_m(n) = m^n$, a mocnění je tedy definováno podle $m^0 = 1$ a $m^{(n+1)} = m \cdot m^n$.

Opět si uvědomme, že v definici předpokládáme, že násobení je už definováno.

[3] Toto značení není obecně moc rozšířené.

Máme definované základní operace na přirozených číslech a je čas dokázat některá základní „pravidla“ pro jejich používání. Tyto zásady běžně používáme. A nyní nás vlastně čeká ukázat, že tato pravidla nejsou ve své podstatě pravidla, nýbrž důsledky Peanových axiomů!

Nejprve nahradíme zápis pomocí funkce následník $s(n)$ běžnějším značením $n+1$. Dostaneme tak rekurzivní definice sčítání a násobení

$$\begin{aligned} &(\alpha 1) \quad m+0=m, && (\alpha 2) \quad m+(n+1)=(m+n)+1,\\ &(\mu 1) \quad m0=0, && (\mu 2) \quad m(n+1)=mn+m. \end{aligned}$$

Důkazy základních pravidel využívají indukci neboli třetí Peanův axiom. Ukážeme si to nejprve na příkladu.

Tvrzení. *Platí*

$$\begin{aligned} &(a) \quad 0+m=m,\\ &(b) \quad 1+m=m+1,\\ &(c) \quad 0m=0,\\ &(d) \quad 1m=m. \end{aligned}$$

Důkaz. (a) Použijeme indukci podle m. Nechť $S=\{m\in\mathbb{N}_0;\ 0+m=m\}$.

Potom $0\in S$, neboť $0+0=0$ podle $(\alpha 1)$. Dále pokud $m\in S$, tak

$$0+(m+1)=(0+m)+1=m+1$$

podle $(\alpha 2)$, tedy $m+1\in S$. Z 3. axiomu potom plyne $S=\mathbb{N}_0$, a tedy $0+m=m$ pro všechna $m\in\mathbb{N}_0$.

(b) Buď $S=\{m\in\mathbb{N}_0;\ 1+m=m+1\}$. Potom

$$\begin{aligned} 1+0&=1 && \text{podle } (\alpha 1)\\ &=0+1 && \text{podle } (a), \end{aligned}$$

takže $0\in S$.

Předpokládejme, že $m\in S$. Potom

$$\begin{aligned} 1+(m+1)&=(1+m)+1 && \text{podle } (\alpha 2)\\ &=(m+1)+1 && \text{podle indukčního předpokladu,} \end{aligned}$$

a tedy i $m+1\in S$. Podle třetího axiomu pak dostáváme $S=\mathbb{N}_0$, neboli $1+m=m+1$ pro všechna $m\in\mathbb{N}_0$.

Cvičení 2. Dokaž si sám (sama) body (c) a (d). □

Asociativita

Tvrzení. *Pro všechna* $m,n,p\in\mathbb{N}_0$ *platí*

$$(m+n)+p=m+(n+p).$$

Ukážeme, že operace $+$ je asociativní, což ve volném překladu znamená „zapomeňte na závorky“. Díky této vlastnosti později budeme moct psát prostě $m+n+p$ a budeme vědět, že nezáleží na tom, zda nejprve sečteme m a n a potom přičteme p, nebo zda k m přičteme součet $n+p$.

Důkaz. Důkaz provedeme indukcí podle p. Mějme libovolná, avšak pevně stanovená čísla m a n. Nechť

$$S=\{p\in\mathbb{N}_0;\ (m+n)+p=m+(n+p)\}.$$

Potom $0 \in S$, protože

$$\begin{aligned}(m+n)+0 &= m+n && \text{podle } (\alpha 1)\\ &= m+(n+0) && \text{podle } (\alpha 1).\end{aligned}$$

Nyní jestliže $p \in S$, potom

$$\begin{aligned}(m+n)+(p+1) &= ((m+n)+p)+1 && \text{podle } (\alpha 2)\\ &= (m+(n+p))+1 && \text{podle indukčního předpokladu}\\ &= m+((n+p)+1) && \text{podle } (\alpha 2)\\ &= m+(n+(p+1)) && \text{podle } (\alpha 2),\end{aligned}$$

takže $p+1 \in S$.

Potom třetí axiom říká, že $S = \mathbb{N}_0$, a tedy $(m+n)+p = m+(n+p)$ pro všechna $m, n, p \in \mathbb{N}_0$, jak jsme chtěli ukázat. □

Poznámka. Všimněte si, že pro první část důkazu jsme potřebovali pouze $(\alpha 1)$, kdežto pro indukční krok jsme již využili $(\alpha 2)$.

Komutativita

Tvrzení. *Pro všechna $m, n \in \mathbb{N}_0$ máme*

$$m+n = n+m.$$

To, že je operace $+$ komutativní, znamená, že můžeme prohodit pořadí sčítanců. Zdá se to jako jasná věc – jako výstraha, proč je potřeba to dokázat, nám poslouží příklad operace, která není komutativní, například odčítání nebo dělení, zde na pořadí záleží!

Důkaz. Použijeme indukci na n. Mějme $m \in \mathbb{N}_0$ a sestrojme množinu

$$S = \{n \in \mathbb{N}_0;\ m+n = n+m\}.$$

Nyní podle $(\alpha 1)$ a (a) víme, že $0 \in S$. Dále pokud platí $m+n = n+m$, tak

$$\begin{aligned}m+(n+1) &= (m+n)+1 && \text{podle } (\alpha 2)\\ &= (n+m)+1 && \text{podle indukčního předpokladu}\\ &= 1+(n+m) && \text{podle } (b)\\ &= (1+n)+m && \text{díky asociativitě sčítání}\\ &= (n+1)+m && \text{podle } (b),\end{aligned}$$

a proto $n+1 \in S$. Z třetího Peanova axiomu pak vyplývá, že $S = \mathbb{N}_0$, a tedy pro všechna $m, n \in \mathbb{N}_0$ platí $m+n = n+m$, čímž jsme hotovi. □

Poznámka. Znovu si všimněme, které předchozí vlastnosti jsme použili. Tentokrát jsme potřebovali také (a) a (b), na rozdíl od důkazu asociativity, a také byla zapotřebí asociativita samotná. Proto bývá výhodné najít vhodné pořadí pro dokazování tvrzení, na což ještě narazíme.

Distributivita

Tvrzení. *Pro všechna $m, n, p \in \mathbb{N}_0$ platí*

$$m(n+p) = mn+mp.$$

Distributivitě násobení přes sčítání často říkáme „roznásobení závorky“. I tato vlastnost je dokazatelná na základě tří Peanových axiomů.

Důkaz. Budeme postupovat indukcí podle p. Pro daná $m, n \in \mathbb{N}_0$ označme

$$S = \{p \in \mathbb{N}_0;\ m(n+p) = mn + mp\}.$$

Nejprve ukážeme, že $0 \in S$. Máme

$$\begin{aligned} m(n+0) &= mn && \text{podle } (\alpha 1)\\ &= mn + 0 && \text{podle } (\alpha 1)\\ &= mn + m0 && \text{podle } (\mu 1). \end{aligned}$$

Nyní předpokládejme, že $p \in S$. Potom

$$\begin{aligned} m(n+(p+1)) &= m((n+p)+1) && \text{podle } (\alpha 2)\\ &= m(n+p) + m && \text{podle } (\mu 2)\\ &= (mn + mp) + m && \text{podle indukčního předpokladu}\\ &= mn + (mp + m) && \text{díky asociativitě}\\ &= mn + m(p+1) && \text{podle } (\mu 2), \end{aligned}$$

a tedy $p + 1 \in S$. Podle třetího axiomu pak máme, že $S = \mathbb{N}_0$, a tedy pro všechna $m, n, p \in \mathbb{N}_0$ platí distributivní zákon. □

Poznámka. Poznamenejme, že k důkazu jsme kromě rekurzivních definic sčítání a násobení potřebovali také asociativitu, kterou již máme dokázanou.

Násobení

Zbývá nám ukázat asociativitu a komutativitu násobení.

Úloha 1. Ukaž, že pro všechna $m, n, p \in \mathbb{N}_0$ platí $m(np) = (mn)p$.

Důkaz následujícího tvrzení je o něco důvtipnější a zajímavější.

Tvrzení. *Pro všechna $m, n \in \mathbb{N}_0$ platí komutativní zákon $mn = nm$.*

Důkaz. Mějme pro dané $m \in \mathbb{N}_0$

$$S = \{n \in \mathbb{N}_0;\ mn = nm\}.$$

Podle (c) je 0 v S. Nyní jestliže $n \in S$, tak

$$\begin{aligned} m(n+1) &= mn + m && \text{podle } (\mu 2)\\ &= nm + m && \text{díky komutativitě.} \end{aligned}$$

Nyní přijde ta hustokrutopřísná část. Hodilo by se nám, kdybychom mohli vytknout m „dozadu“, to bohužel ještě nevíme. Ovšem vzhledem k tomu, že jsme už ukázali vytýkání „dopředu“ neboli distributivitu, můžeme se právem domnívat, že půjde něco obdobného i opačně. Klíčem k tomu je další indukce. Ať

$$T = \{m \in \mathbb{N}_0;\ nm + m = (n+1)m\}.$$

Zjevně $0 \in T$. Dále pokud $m \in T$, tak

$$\begin{aligned}
n(m+1)+(m+1) &= (nm+n)+(m+1) && \text{podle } (\mu 2)\\
&= nm+n+m+1 && \text{díky asociativitě můžeme rozpustit závorky}\\
&= nm+m+n+1 && \text{díky komutativitě sčítání lze přeuspořádat členy}\\
&= (nm+m)+(n+1) && \text{díky asociativitě můžeme závorkovat, jak chceme}\\
&= (n+1)m+(n+1) && \text{podle indukčního předpokladu}\\
&= (n+1)(m+1) && \text{podle } (\mu 2).
\end{aligned}$$

Tedy $m+1 \in T$ a podle třetího axiomu $T = \mathbb{N}_0$. Konečně tedy dostáváme, že $m(n+1) = (n+1)m$, a tedy $n+1 \in S$. Podle třetího Peanova axiomu potom $S = \mathbb{N}_0$ a $mn = nm$ pro všechna $m, n \in \mathbb{N}_0$, jak jsme chtěli ukázat. □

Porovnávání

Kromě sčítání a násobení můžeme přirozená čísla také porovnávat. Jak definujeme, že a je menší nebo rovno b? Můžeme se na to podívat tak, že seřadíme přirozená čísla do řady podle toho, jak po sobě *následují*, a řekneme, že a je menší nebo rovno b, pokud je a v řadě dříve (nebo nastejno) než b. Jenže pokud jsou čísla a nebo b velmi vysoká, tak bychom se k nim také nemuseli za lidský život dopracovat. Zkusme jiný pohled, řekněme, že $a \leq b$, pokud je rozdíl $b - a$ také přirozeným číslem. Avšak rozdíl jsme ještě nedefinovali, navíc se dostáváme k definici kruhem, kdy rozdíl $b - a$ dvou přirozených čísel můžeme vůbec definovat jen tehdy, když $a \leq b$, protože záporná čísla vlastně ještě neznáme. Tento zádrhel však můžeme snadno obejít tak, že definujeme $a \leq b$ právě tehdy, když existuje přirozené číslo r takové, že $b = a + r$. Číslo r je tu tím nezáporným rozdílem.

Definice. Definujme relaci $\leq$ na množině přirozených čísel $\mathbb{N}_0$ takto:

$$a \leq b \iff \text{existuje } r \in \mathbb{N}_0 \text{ splňující } b = a + r.$$

Tato definice nám umožňuje dokázat několik základních pravidel pro porovnávání přirozených čísel. Uvádíme je jako cvičení.

Cvičení 3. Ukaž, že pokud pro přirozená čísla a, b a c platí $a \leq b$ a $b \leq c$, potom $a \leq c$.

Cvičení 4. Ukaž, že pro všechna přirozená čísla n platí $n \leq n$.

Úloha 2. Ukaž, že pokud $a \leq b$ a současně $b \leq a$, pak nutně $a = b$.

V předchozích třech cvičeních a úloze jsme postupně ukázali tři vlastnosti porovnávání přirozených čísel, které definují *uspořádání*:

Definice. *Uspořádání* je relace R na nějaké množině, která je:

(1) *Tranzitivní*: pro všechna x, y, z z dané množiny platí: jestliže xRy a yRz, potom i xRz.
(2) *Reflexivní*: pro všechna x z dané množiny platí xRx neboli x je v relaci samo se sebou.
(3) *Antisymetrická*: pro všechna x, y z dané množiny platí „jestliže xRy a současně yRx, potom $x = y$“.

Tedy relace $\leq$ na přirozených číslech je relací uspořádání.

Navíc si všimněme dvou dalších zajímavých vlastností. Všechny prvky množiny přirozených čísel jsou vzájemně porovnatelné, to znamená, že pro každá dvě čísla a a b platí buď $a \leq b$, nebo $b \leq a$ (nebo obojí, viz vlastnost antisymetrie). Tuto vlastnost rozhodně nemají všechny množiny a relace: vezměme například relaci $\subset$ „být podmnožinou“.

Cvičení 5. Uvaž relaci „být podmnožinou“ $\subset$ na potenční množině $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ množiny $A = \{a, b\}$. Najdi dva prvky množiny $P(A)$, které mezi sebou nejsou porovnatelné, a dva prvky, které porovnatelné jsou.

Množina přirozených čísel je ještě k tomu takzvaně dobře uspořádaná, což znamená, že každá neprázdná podmnožina $\mathbb{N}_0$ má nejnižší prvek.

Definice. *Nejnižší prvek* je takový prvek x, že pro všechna y z dané množiny platí $x \leq y$.

Tvrzení. *Každá neprázdná podmnožina přirozených čísel má nejnižší prvek.*

Důkaz. Tvrzení dokážeme sporem. Pro spor předpokládejme, že $S \subset \mathbb{N}_0$ je neprázdná podmnožina, která nemá nejnižší prvek. Definujme $S^* = \{n \in \mathbb{N}_0;$ žádné z čísel $0, 1, \ldots, n$ není v $S\}$. Naším cílem bude ukázat, že $S^* = \mathbb{N}_0$, tedy že S je prázdná množina, což je spor.

Nejprve si všimněme, že $0 \in S^*$, neboť jinak by 0 byla v S a pak by S měla nejnižší prvek.

Nyní pokud $n \in S^*$, tak žádné z čísel $0, 1, \ldots, n$ není v S, a proto ani $n + 1$ nemůže být v S, jinak by $n + 1$ bylo nejnižším prvkem S. Tedy žádné z čísel od nuly po $n + 1$ není v S, a proto $(n + 1) \in S^*$.

Dle třetího Peanova axiomu máme $S^* = \mathbb{N}_0$, což je kýžený spor. □

Cvičení 6. Rozhodni a zdůvodni, zdali jsou následující množiny dobře uspořádané:

(1) množina celých čísel $\mathbb{Z}$,
(2) množina kladných racionálních čísel $\mathbb{Q}^+$,
(3) potenční množina[4] $P(A)$ množiny $A = \{a, b, c\}$.

Úloha 3. Ukaž, že každá ostře klesající posloupnost $x_1, x_2, x_3, \ldots$ přirozených čísel musí být konečná.

Je množina přirozených čísel jen jedna?

Zatím jsme v našem povídání hovořili o jedné množině přirozených čísel, která je definovaná Peanovými axiomy. Všechny vlastnosti aritmetiky a uspořádání přirozených čísel jsme dokázali pouze na základě těchto axiomů. Ale co když existuje ještě jiná množina, která splňuje tři Peanovy axiomy, která se od té naší liší?

Předpokládejme, že taková množina existuje, a nazvěme ji $\mathbb{N}_0^*$ spolu s funkcí následník s^*, která splňuje tři Peanovy axiomy. Potom můžeme stejným způsobem jako dříve odvodit pravidla aritmetiky a uspořádání. Předpokládali bychom, že tato množina bude „v podstatě stejná“ jako $\mathbb{N}_0$, až na to, že její prvky se mohou jinak jmenovat, ale chovat se budou stejně. To, jak se daný objekt chová, je ale právě to, o co nám v matematice jde! Vůbec nám nezáleží na tom, co daný objekt *je*, často to ani zjistit nemůžeme.

Proto zavedeme důležitý pojem, a to *izomorfismus*. Říkáme, že dvě množiny jsou izomorfní, pokud můžeme prvky jedné množiny přejmenovat, abychom dostali druhou množinu s tím, že všechny aritmetické vlastnosti zůstanou zachovány. V našem případě navíc potřebujeme izomorfismus, který zachovává i uspořádání.

Nebudeme zde zabíhat do detailů, pouze zmíníme, že bijekce mezi $\mathbb{N}_0$ a $\mathbb{N}_0^*$ zachovává sčítání, násobení i uspořádání. (Tedy například u sčítání nezáleží na tom, zda nejdřív dvě čísla sečteme a potom daný součet zobrazíme tou bijekcí (přejmenujeme), nebo zda nejdřív dvě čísla zobrazíme (přejmenujeme) a poté tyto obrazy sečteme.) To vše lze dokázat indukcí.

To znamená, že pouhé tři Peanovy axiomy definují přirozená čísla jednoznačně!

[4]Potenční množina je množina všech podmnožin dané množiny.

Závěr

Gratulujeme Ti k přečtení druhého dílu seriálu! Tento díl byl daleko více technický a rigorózní než díl předchozí. My doufáme, že si každý přišel aspoň v jednom díle na své. Axiomatický přístup, který jste měli možnost zažít v tomto povídání, je typický pro studium čisté matematiky na vysoké škole. Pokud Tě to zaujalo a chceš si o systémech čísel přečíst víc, vřele doporučujeme publikaci *The Foundations of Mathematics* (I. Stewart a D. Tall), ze které jsme jako autoři také čerpali.

Přejeme Ti hodně zdaru při řešení soutěžních úloh a těšíme se na Tebe u příštího dílu, tentokrát o algoritmech.

Návody ke cvičením

1. Podívej se na to, kolika způsoby lze spárovat prvky A s prvky B. Pozor na to, že musíš použít všechny prvky A právě jednou, ale prvky B se klidně můžou opakovat.

3. Rozepiš definice.

4. Použij $r = 0 \in \mathbb{N}_0$.

5. O $\{a\}$ a $\{b\}$ se nedá říct ani $\{a\} \subset \{b\}$, ani $\{b\} \subset \{a\}$. Naopak prvky $\emptyset$ a $\{a, b\}$ porovnatelné jsou, neboť $\emptyset \subset \{a, b\}$.

6. (1) Ne. (2) Ne. (3) Ne.

Návody k úlohám

2. Ukaž nejprve implikaci „jestliže $a + t = b + t$, pak $a = b$“.

3. Uvaž nejnižší prvek množiny $\{x_1, x_2, x_3, \dots\} \subset \mathbb{N}_0$. Pokračuj sporem.

Matematická indukce III – V rytmu algoritmů

Milý příteli,
vítáme Tě u třetího a posledního dílu seriálu o matematické indukci. Tentokrát se podíváme na algoritmy, které využívají indukci. Řeč bude o tom, jak najít nejvyššího společného dělitele dvou čísel, jak najít společné kořeny polynomů, ale zabrousíme i do oblasti diofantických rovnic. Poté se podíváme na příklad z trochu jiného soudku, neboť prozkoumáme způsoby seřazení balíčku karet podle jejich hodnoty. Závěrečná kapitola je spíše k zamyšlení nad tím, jak určit, zda algoritmus po nějakém čase doběhne.

Podnětné čtení Ti přejí

autoři

O smyslu algoritmizace

Algoritmus je proces nebo postup, který po konečně mnoha krocích dospěje k nějakému závěru, nejčastěji k vyřešení zadané úlohy. Jednotlivé kroky jsou jednoznačně zadané a často jednoduché na provedení. Zároveň je daný algoritmus v jistém smyslu univerzální, tedy dokáže vyřešit více úloh podobného druhu.

Etymologické okénko. Původ slova algoritmus sahá do 9. století. Název je odvozen od jména perského matematika Al-Chorezmího, který zavedl počítání s arabskými číslicemi (tehdy nazývané indickými) a položil základy algebry. Původní slovo *algorismus* znamenalo pouze počítání v desítkové soustavě. Později se pod vlivem řeckého slova *arithmos* začala používat zkomolenina *algoritmus*. Význam, pod kterým jej známe dnes, však slovo získalo až v 19. století.

Algoritmy však byly známé již starým Babyloňanům 2500 let před naším letopočtem. Staří Řekové zas používali například Eratosthenovo síto pro hledání prvočísel nebo Eukleidův algoritmus, který si představíme i v tomto dílu.

Proč jsou algoritmy užitečné? Ve statistice slouží k analýze dat a také k rozpoznání těch dat, která mají nějaký reprezentativní význam, například při jejich roztřídění do takzvaných clusterů. V aplikované matematice jsou algoritmy používány pro hledání přibližných řešení matematických modelů skutečného světa. Nicméně i v čisté matematice mají algoritmy svůj význam – například pro důkaz existence řešení. Síla algoritmů spočívá také v jejich jednoduchosti a repetitivní podstatě, čehož dokáží počítače využít pro extra rychlé nalezení řešení. Lidé oproti tomu nejsou tak efektivní v provádění ručních opakovaných výpočtů, ale umí napsat program, který to za ně udělá v řádu milisekund!

Dělicí algoritmus

Úmluva. V průběhu budeme pracovat s přirozenými čísly $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ jako jsme je definovali v předchozím díle. Podotkněme, že nulu zde považujeme za přirozené číslo.

Mějme dvě přirozená čísla m, n, kde n je různé od nuly. Již ze základní školy víme, jak se dělí se zbytkem. Při dělení se zbytkem hledáme přirozená čísla q a r, kde r je menší než n, pro která platí

$$m = qn + r.$$

Je tato operace dělení dobře definovaná? Existuje vždy právě jeden výsledek, tedy právě jedna dvojice čísel q a r? Není to na první pohled zřejmé[1], proto si to pojďme dokázat:

Věta. *Nechť m, n jsou dvě přirozená čísla, kde $n \neq 0$. Potom existuje právě jedna dvojice přirozených čísel q a r takových, že $m = qn + r$ a $r < n$.*

Důkaz. Nejprve ukážeme existenci. Postupujme indukcí podle m. Nechť

$$S = \{m \in \mathbb{N}_0;\ m = qn + r \text{ pro nějaká } q, r \in \mathbb{N}_0, r < n\}.$$

Všimněme si, že $0 \in S$, neboť $0 = 0n + 0$. Nyní předpokládejme, že $m \in S$. Potom $m = qn + r$ a $r < n$, tedy

$$m + 1 = qn + r + 1.$$

Jelikož $r < n$, tak $r + 1 \leq n$ (jsme v přirozených číslech). Tedy buď $r + 1 = n$ a dostáváme

$$m + 1 = (q + 1)n + 0,$$

nebo $r + 1 < n$ a potom

$$m + 1 = qn + (r + 1),$$

kde $r + 1 < n$. V obou případech platí $m + 1 \in S$, tedy dle principu indukce (třetího Peanova axiomu) máme $S = \mathbb{N}_0$.

Nyní ukážeme, že daná q a r jsou jednoznačná. Mějme

$$m = qn + r = q'n + r',$$

kde $r, r' < n$. Potom

$$qn \leq m < (q + 1)n,$$
$$q'n \leq m < (q' + 1)n.$$

Z toho dostáváme $qn < (q' + 1)n$, a jelikož $n > 0$, tak $q < q' + 1$, tedy $q \leq q'$, protože pracujeme s přirozenými čísly. Obdobně dostaneme $q' \leq q$, takže dohromady $q = q'$. A z předpokladu pak plyne rovnost zbytků $r = m - qn = m - q'n = r'$. Tedy dvojice čísel q a r je opravdu jednoznačná. □

Přirozeně se můžeme ptát, co se stane, když budeme dělicí algoritmus aplikovat opakovaně. Pojďme to společně probádat.

Nechť a, b jsou dvě přirozená čísla. Potom dle dělicího algoritmu existují q_1 a $r_1 < b$ taková, že

$$a = q_1 b + r_1.$$

Pokračujme dál a aplikujme dělicí algoritmus na čísla b a r_1.

$$\begin{aligned} b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ r_2 &= q_4 r_3 + r_4, \\ r_3 &= q_5 r_4 + r_5, \\ &\vdots \\ r_i &= q_{i+2} r_{i+1} + r_{i+2}. \end{aligned}$$

[1] Například při dělení se zbytkem v okruhu *Gaussových čísel* $\mathbb{Z}[i]$ není zbytek jednoznačný, takže to rozhodně není samozřejmost! O Gaussových číslech se můžeš dočíst v prvním díle minulého seriálu *Teorie nejen čísel 1.*

Napřed několik pozorování:

Pozorování první. V každém kroku máme dle dělicího algoritmu zaručená čísla q_{i+2} a $r_{i+2} < r_{i+1}$, dokud není nějaký zbytek roven nule, protože nulou dělit nemůžeme (viz dělicí algoritmus).

Pozorování druhé. Získali jsme klesající posloupnost $b > r_1 > r_2 > r_3 > \cdots$

Pozorování třetí. Proces se po nějakém čase vždy zastaví.

Cvičení 1. Rozmysli si, že třetí pozorování vyplývá z prvního a druhého pozorování a z Úlohy 3 v předchozím dílu.

V následující kapitole se k tomuto procesu vrátíme a prozkoumáme jeho další zajímavé vlastnosti!

Eukleidův algoritmus

Pamatuješ si, jak jste ve škole hledali nejvyššího společného dělitele dvou čísel? Postup byl následující: nejprve obě čísla rozložíme na součin prvočísel a poté hledáme, která prvočísla mají oba rozklady společná. Avšak to jsme to trochu uspěchali – jak například víme, že lze pokaždé prvočíselný rozklad najít, a pokud ho náhodou najdeme, jak víme, že je jen jeden? To nám náš postup trochu komplikuje, skoro to vypadá, že by dvě čísla mohla mít více různých největších společných dělitelů!

Abychom si tento problém vyjasnili, potřebujeme nejdřív přesně zadefinovat potřebné pojmy.

Definice. Nechť m, n jsou přirozená čísla, kde n je různé od nuly. Potom říkáme, že n *dělí* m, pokud existuje přirozené číslo k takové, že $m = nk$. Tuto skutečnost zapisujeme jako $n \mid m$.

Všimněme si, že každé číslo (kromě jedničky) má alespoň dva dělitele, jedničku a sebe sama. Některá čísla jsou výjimečná tím, že je už dál dělit nelze.

Definice. Nechť p je přirozené číslo. Potom p je *prvočíslo*, jestliže p má právě dva různé dělitele.

Poznámka. Poznamenejme, že číslo 1 podle definice není prvočíslo. Proč to tak je? Není za tím žádná magie, důvod je ten, že definice vymýšlí lidé tak, aby byly co nejužitečnější. A prostě se hodí, aby jednička prvočíslem nebyla.

Pokud číslo d dělí m a současně dělí i n, potom říkáme, že d je *společný dělitel* čísel m a n. Číslo 1 je tak pokaždé společným dělitelem. Pokud je to zároveň jediný společný dělitel, říkáme, že čísla m a n jsou *nesoudělná*.

Vraťme se nyní k nejvyššímu společnému děliteli.

Definice. Přirozené číslo d je *největším společným dělitelem* čísel m, n, pokud platí následující dvě podmínky:

(i) d je společný dělitel m a n,
(ii) pokud c je dalším společným dělitelem m a n, pak $c \mid d$.

Potom píšeme $d = \mathrm{NSD}(m, n)$.

Poznámka. Rozmysli si, že tato definice je ekvivalentní s tím, že d je největší ze společných dělitelů.

Poznámka. S naší novou definicí můžeme říct, že čísla m a n jsou nesoudělná právě tehdy, když $\mathrm{NSD}(m, n) = 1$.

Přišel čas vrátit se k opakovanému použití dělicího algoritmu, kterým jsme končili předchozí kapitolu. Vyzbrojeni novou terminologií můžeme učinit další pozorování:

Pozorování čtvrté. Pokud proces skončí u $r_{i+2} = 0$, dostáváme rovnost $r_i = q_{i+1}r_{i+1}$, z čehož plyne, že r_{i+1} dělí r_i. O řádek výš máme rovnost

$$r_{i-1} = q_{i+1}r_i + r_{i+1},$$

tedy pravá strana je dělitelná číslem r_{i+1}, protože r_{i+1} dělí r_i. Proto je i r_{i-1} na levé straně dělitelné r_{i+1}. Takto postupujeme pořád nahoru a iterativně dostáváme, že číslo r_{i+1} dělí jak b, tak a, a tudíž je společným dělitelem výchozích dvou čísel.

Za chvíli ukážeme ještě mnohem silnější tvrzení, a sice že r_{i+1} je největším společným dělitelem čísel a a b.

Toto opakované použití dělicího algoritmu má svůj vlastní název – *Eukleidův algoritmus*. Výsledkem Eukleidova algoritmu je právě číslo r_{i+1}, tedy poslední nenulový zbytek.

Věta. *Nechť a a $b \neq 0$ jsou přirozená čísla. Potom Eukleidův algoritmus generuje nejvyššího společného dělitele čísel a a b.*

Důkaz. Nejprve si připomeňme značení jednotlivých členů v algoritmu:

$$\begin{aligned}
a &= q_1 b + r_1,\\
b &= q_2 r_1 + r_2,\\
r_1 &= q_3 r_2 + r_3,\\
r_2 &= q_4 r_3 + r_4,\\
r_3 &= q_5 r_4 + r_5,\\
&\vdots\\
r_i &= q_{i+2} r_{i+1} + r_{i+2},\\
&\vdots
\end{aligned}$$

Když v důkazu používáme algoritmus, měli bychom si položit následující otázky:

(1) Doběhne algoritmus někdy, tedy zastaví se proces po nějakém čase?
(2) Pokud se zastaví, vyhodí nám požadovanou odpověď (v našem případě největšího společného dělitele)?
(3) Jak rychle algoritmus konverguje, tj. jak rychle se blíží ke správné odpovědi?

Prvním krokem důkazu je ukázat, že se algoritmus zastaví, což je součástí Cvičení 1. Nechť r_{i+2} je první zbytek roven nule. Chceme ukázat, že r_{i+1} neboli přecházející zbytek je nejvyšším společným dělitelem čísel a a b.

Druhý krok již máme téměř za sebou: ve čtvrtém pozorování jsme nahlédli, že r_{i+1} je společným dělitelem a a b.

Nyní bychom rádi dokázali, že se jedná o nejvyššího společného dělitele. Budeme postupovat podle naší definice. Nechť tedy d je dalším dělitelem a a b. To znamená, že existují přirozená čísla α a β taková, že

$$a = \alpha d \qquad \text{a} \qquad b = \beta d.$$

Jelikož $a = q_1 b + r_1$, tak $r_1 = (\alpha - q_1\beta)d$, takže d dělí r_1. Induktivně dostáváme, že d dělí i další zbytky včetně předposledního, tedy d dělí r_{i+1}. Potom dle definice r_{i+1} je nejvyšším společným dělitelem a a b. □

Cvičení 2. Najdi nejvyššího společného dělitele čísel 3570 a 323 nejprve pomocí rozkladu na součin prvočísel a poté použitím Eukleidova algoritmu.

Cvičení 3. Ukaž, že čísla 19891 a 2022 jsou nesoudělná.

Dělicí algoritmus a Eukleidův algoritmus lze použít i pro dva polynomy. Místo zmenšujících se zbytků však potřebujeme něco jiného, co se bude při každé iteraci snižovat, což zaručí, že algoritmus někdy doběhne. Toto „něco“ je pak stupeň polynomu.

Úloha 1. Vyslov tvrzení podobné dělicímu algoritmu pro polynomy s reálnými koeficienty a dokaž jej.

Eukleidův algoritmus pak funguje úplně stejně i pro dva polynomy. Vyzkoušejte si to na úloze!

Úloha 2. Najdi mnohočlen nejvyššího možného řádu, který dělí $x^3 - 9x^2 - x + 105$ a zároveň $x^2 - 9x + 14$.

Úloha 3. Najdi všechny společné kořeny polynomů $x^4 + x^3 - 21x^2 - x + 20$ a $x^3 - x^2 - 22x + 40$.

Nyní přichází na řadu otázka, jak efektivní Eukleidův algoritmus je. Kolikrát je obecně třeba iterovat dělicí algoritmus, než se dostaneme k výsledku? Počet operací můžeme shora odhadnout podle velikosti b: jelikož $b > r_1 > r_2 > \cdots$, tak zbytek nula dostaneme nanejvýš po b aplikacích dělicího algoritmu.

Avšak je možné dosáhnout i přesnějších odhadů!

Věta. *Nechť $a > b > 0$ jsou dvě přirozená čísla. Předpokládejme, že Eukleidův algoritmus pro a a b sestává z N kroků. Potom nejnižší hodnota, které může a (resp. b) nabývat, je Fibonacciho číslo*[2] *$a = F(N + 2)$ (resp. $b = F(N + 1)$).*

Věta. *Počet iterací v Eukleidově algoritmu nikdy nemůže překročit pět krát počet cifer čísla b.*

Tato věta ukazuje, že horní mez počtu iterací roste úměrně počtu cifer čísla b, což ukazuje na *logaritmický* růst. Růst je měřítkem toho, jaká je cena algoritmu, tedy kolik kroků proces potřebuje, než se zastaví, vzhledem ke vstupním hodnotám, v tomto případě hodnotě čísla b. Je zřejmé, že čím větší čísla do Eukleidova algoritmu vhodíme, tím déle může iterativní proces trvat. Růst potom vyjadřuje konkrétní vztah mezi velikostí vstupu a cenou.

Důkaz těchto vět přesahuje odbornost tohoto textu, přesto je zmiňujeme pro zajímavost. O těchto vlastnostech algoritmu pravděpodobně Eukleides nevěděl, protože například druhá z vět byla dokázána až v roce 1844.

Diofantické rovnice

Ukážeme si zajímavé použití Eukleidova algoritmu při řešení diofantických rovnic. Diofantické rovnice jsou rovnice, jejichž řešení hledáme pouze v oboru celých čísel $\mathbb{Z}$. Taková rovnice může například vypadat takto:

$$13x + 7y = 2,$$

kde $x, y \in \mathbb{Z}$. Zkuste dosadit $(x, y) = (5, -9)$. Jak ale na toto řešení přijít? Existuje obecný postup? Nejsou možná i jiná řešení? Jak najít všechna řešení?

Zkusme použít Eukleidův algoritmus na koeficienty proměnných:

$$\begin{aligned} 13 &= 1 \cdot 7 + 6, \\ 7 &= 1 \cdot 6 + 1. \end{aligned}$$

Dobrá, to nám řeklo jen to, co už jsme dávno věděli: že čísla 13 a 7 jsou nesoudělná. Bodejť, vždyť jsou to prvočísla. Avšak můžeme z toho získat víc ...

[2]Fibonacciho čísla jsou definována rekurzí $F(0) = 0$, $F(1) = 1$ a $F(n + 1) = F(n) + F(n - 1)$ pro $n \geq 1$. Více o Fibonacciho číslech najdeš v prvním dílu seriálu.

Postupujme pozpátku, z druhé rovnosti vyjádříme $1 = 7 - 1 \cdot 6$ a z první nerovnosti pak $6 = 13 - 1 \cdot 7$. Dohromady dostáváme

$$1 = 7 - 6 = 7 - (13 - 7) = (-1) \cdot 13 + 2 \cdot 7.$$

Stačí tuto rovnost vynásobit dvěma, abychom dostali

$$2 = (-2) \cdot 13 + 4 \cdot 7,$$

takže jsme zkonstruovali další řešení naší rovnice, a to $(x, y) = (-2, 4)$.

Cvičení 4. Pomocí Eukleidova algoritmu najdi jedno celočíselné řešení

$$27x - 15y = 21.$$

Umíme tedy generovat alespoň jedno řešení (pokud nějaké existuje). Dokonce platí i něco silnějšího: pokud existuje jedno řešení, tak jich už nutně existuje nekonečně mnoho. Než se však pustíme do jejich hledání, zkus si vyřešit následující cvičení, která tě nasměrují na cestu k nalezení odpovědí na otázky v úvodu kapitoly.

Cvičení 5. Ukaž, že rovnice

$$72x - 117y = 42$$

nemá celočíselná řešení.

Cvičení 6. Nechť a a b jsou nesoudělná přirozená čísla. Najdi všechna celočíselná řešení (x, y) rovnice

$$ax + by = 0$$

a ukaž, že jiná řešení nejsou.

Možná už na základě svých pozorování při řešení předchozích cvičení zvládneš sám (sama) dokázat následující větu:

Věta. *Předpokládejme, že (x_0, y_0) je řešení diofantické rovnice $ax + by = c$, kde $a, b, c \in \mathbb{Z}$ jsou dané konstanty. Potom (x, y) řeší tuto rovnici právě tehdy, když $x = x_0 + x_h$ a $y = y_0 + y_h$, kde (x_h, y_h) je (nějakým) řešením* **homogenní** *rovnice*

$$ax + by = 0.$$

Důkaz. Tvrzení, které chceme dokázat, je ekvivalence, takže musíme dokázat oba směry implikace.

Nejprve tedy předpokládejme, že (x, y) řeší (nehomogenní) rovnici $ax + by = c$. Jelikož (x_0, y_0) je také řešením, tak

$$\begin{aligned} 0 &= c - c \\ &= (ax + by) - (ax_0 + by_0) \\ &= a(x - x_0) + b(y - y_0). \end{aligned}$$

Pokud tedy položíme $x_h = x - x_0$ a $y_h = y - y_0$, tak (x_h, y_h) je řešením homogenní rovnice. Potom $(x, y) = (x_0 + x_h, y_0 + y_h)$ má požadovaný tvar.

Nyní ukážeme opačnou implikaci, a sice že $(x, y) = (x_0 + x_h, y_0 + y_h)$, kde (x_h, y_h) řeší homogenní rovnici, je řešením (nehomogenní) rovnice $ax + by = c$. Máme

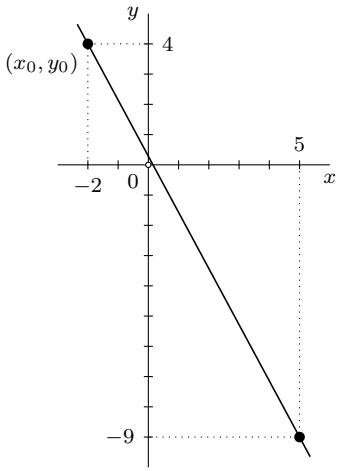
$$\begin{aligned} ax + by &= a(x_0 + x_h) + b(y_0 + y_h) \\ &= (ax_0 + by_0) + (ax_h + by_h) \\ &= c + 0 \\ &= c \end{aligned}$$

a jsme hotovi. □

Dobrá, víme tedy, že stačí najít jedno řešení (x_0, y_0), a pak nejenže $(x, y) = (x_0 + x_h, y_0 + y_h)$ je řešením, ale navíc všechna další řešení mají nutně tento tvar! To nám patřičně zužuje výběr a za chvíli nám to umožní ukázat, že jsme nalezli všechna řešení.

Nyní pojďme prozkoumat, co jsou zač ta řešení homogenní rovnice. Dobrá zpráva je, že jsi už většinu práce odvedl(a), protože jsi jistě poctivě vyřešil(a) Cvičení 6. Důležité je podotknout, že ve Cvičení 6 jsi vyřešil(a) homogenní rovnici pro a a b nesoudělná. Naštěstí je tu „easy fix“: Pokud jsou a a b soudělná, prostě vydělíme celou rovnici jejich největším společným dělitelem. A pokud jím není dělitelné číslo c, tak už díky Cvičení 5 víme, že potom rovnice nemá řešení (v oboru celých čísel) – stačí zobecnit tvrzení pro rovnici $ax + by = c$, která nemá řešení, pokud c není dělitelné největším společným dělitelem čísel a a b.

Řešení diofantické rovnice si můžeme představit i graficky. V rovině $\mathbb{R}^2$ s osami x a y jsou body s celočíselnými souřadnicemi právě mřížové body celočíselné mřížky. Nalezení jednoho konkrétního řešení (x_0, y_0) odpovídá jednomu bodu mřížky. Potom řešení homogenní rovnice určuje, kterým směrem se vydat z tohoto bodu. Všechna řešení pak leží na jedné přímce, která prochází některými mřížovými body, a tyto body jsou hledaná řešení rovnice.



Na obrázku je konkrétní řešení $(x_0, y_0) = (-2, 4)$ rovnice $13x + 7y = 2$, od kterého se vydáme směrem homogenního řešení. V tomto případě přičítáme násobky vektoru $(7, -13)$.

Úloha 4. Najdi všechna řešení diofantické rovnice

$$321x + 17y = 1.$$

Úloha 5. Najdi všechna celočíselná řešení rovnice

$$2022x + 312y = 18.$$

Úloha 6. Odvoď Bézoutovo lemma: Pokud a a b jsou nenulová přirozená čísla, potom existují celá čísla s a t taková, že

$$as + bt = \mathrm{NSD}(a, b).$$

Úloha 7. Nechť a, b a c jsou přirozená čísla taková, že c dělí ab. Ukaž, že pokud $\mathrm{NSD}(a, c) = 1$, tak c dělí b.

Úloha 8. Nechť a, b a c jsou taková přirozená čísla, že $\mathrm{NSD}(a, c) = 1 = \mathrm{NSD}(b, c)$. Dokaž, že potom $\mathrm{NSD}(ab, c) = 1$.

Jak co nejrychleji seřadit balíček karet?

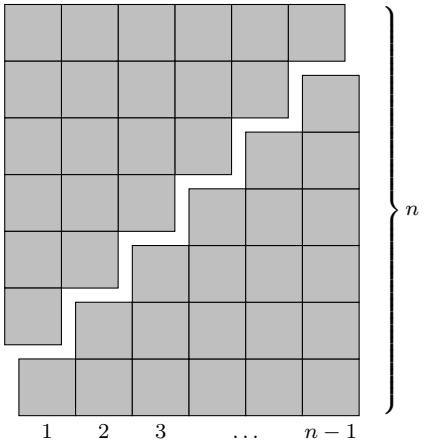
V této kapitole se zaměříme na ryze praktický problém: máme seřadit karty v balíčku vzestupně podle jejich hodnoty a chceme to provést co nejefektivněji.

Intuitivní přístup je brát postupně karty z balíčku a umístit je na správné místo do řady. Představme si, že v balíčku jsou karty s hodnotami 3, 7, 2, 4, 5 v tomto pořadí. Vytáhneme trojku, poté sedmičku položíme napravo od ní, pak vytáhneme dvojku a umístíme ji nalevo od trojky, potom čtyřku dáme mezi trojku a sedmičku a nakonec pětku vložíme mezi čtyřku a sedmičku. Tak jsme čísla seřadili jako 2, 3, 4, 5, 7.

Tomuto přístupu se říká *řazení vkládáním*. Pokud má tento algoritmus provést počítač na n prvcích, hodí se vědět, kolik jednotlivých operací musí v nejhorším možném případě provést. Operacemi myslíme jednotlivá porovnávání dvou prvků. V každém kroku vezmeme jednu kartu z neseřazeného balíčku a postupně ji porovnáváme s prvky v seřazené řadě. Začneme zprava (od největšího): pokud je vkládaná karta větší nebo stejná, umístíme ji napravo a jsme hotovi, je-li však nižší, pokračujeme porovnáním s kartou nalevo, a tak dále. V nejhorším případě musíme kartu porovnat se všemi již vyloženými kartami. Pro n karet tedy musíme provést nanejvýš

$$0 + 1 + 2 + 3 + 4 + \cdots + (n-1)$$

jednotlivých porovnání. Že to je v součtu $\frac{n(n-1)}{2}$, to si můžeš dokázat (např. indukcí[3]), pro stručnost to však zde nahlédneme jen pomocí obrázku:



Tedy v nejhorším možném případě musíme provést řádově n^2 operací – to je kvadratický růst, což je pro objemné balíčky karet opravdu hodně.

Řazení vkládáním, při kterém v každém kroku do $n-1$ již seřazených karet přidáme n-tou na správné místo, však není jediný přístup k řešení našeho problému.

Dalším možným způsobem je *řazení výběrem*. Proces probíhá tak, že z neseřazené řady vybereme nejnižší prvek a umístíme ho na první místo v seřazené řadě. Toto opakujeme s druhým nejnižším

[3]Viz první díl seriálu.

prvkem a tak dále. Kolik porovnání musíme provést? Nejnižší prvek můžeme najít následovně: porovnáme první dva prvky v řadě a z nich vezmeme ten nižší, který porovnáme s následujícím prvkem v řadě, a z těchto dvou opět vybereme ten nižší. Obdobně pokračujeme až na konec řady, kdy nám zbyde ten úplně nejnižší prvek. Hledáme-li tedy nejnižší prvek z řady o n prvcích, musíme provést $n-1$ porovnání. Celkem tedy řazení výběrem pracuje v

$$(n-1)+(n-2)+\cdots+2+1$$

krocích. To už víme, že je dohromady $\frac{n(n-1)}{2}$ kroků. Tedy řazení výběrem trvá stejně dlouho jako řazení vkládáním! Růst je opět kvadratický.

Pro zajímavost si představíme ještě jeden poměrně neefektivní způsob řazení, a tím je *bublinkové řazení*[4]. Nejprve porovnáme první a druhý prvek na začátku řady a případně je prohodíme, pokud je první prvek větší než druhý. Dále porovnáme druhý a třetí prvek a případně jejich pořadí prohodíme. Takto projdeme celou řadu, v každém kroku se soustředíme pouze na dvojici sousedních prvků. Pravděpodobně po tomto prvním projetí řadou nejsou prvky ve správném pořadí. Proto tento proces opakujeme znovu a znovu, dokud není řada seřazená.

Samozřejmě se nabízí otázka, zda nebudeme náhodou „probublávat“ naší řadou donekonečna. Zastaví se algoritmus někdy? Případně jak pozná, že se má zastavit?

Snadno nahlédneme, že nejvyšší číslo vždy probublá na konec řady. Můžeme tedy proces v každém procházení řadou o jeden krok snížit. Postupně tedy zafixujeme poslední číslo, pak předposlední a induktivně dojdeme k závěru, že potřebujeme projet řadou nanejvýš $(n-1)$-krát. Takže algoritmus se po nějakém čase zastaví. Navíc se může zastavit i dřív, pokud jej naprogramujeme tak, že se může zastavit už tehdy, když projede řadou a žádné dva prvky neprohodí. V nejhorším možném případě však musí postupně udělat $(n-1)$ probublání řadou, tedy celkem

$$(n-1)+(n-2)+\cdots+2+1$$

jednotlivých porovnání. Dostali jsme opět stejnou odpověď – kvadratický růst. Není to frustrující – vyzkoušeli jsme již tři různé způsoby řazení a nedostali jsme nic lepšího než kvadratický růst? Naštěstí existují i efektivnější řazení. Pojďme se na jedno podívat.

Představme si, že máme dvě hromádky karet, v nichž je dohromady n karet, které jsou již seřazené. Dokážeme je nyní spojit dohromady? Jistě, otázkou je spíš jak rychle, tedy v kolika krocích.

Cvičení 7. Vymysli způsob, jakým bys spojil(a) dva již seřazené balíčky do jednoho seřazeného. Z kolika kroků (porovnávání) se Tvůj algoritmus skládá?

Chceme seřadit celý balíček, místo toho si však představíme, že řadíme dva menší balíčky, které poté spojíme.

Poznámka. Všimněme si, že předchozí algoritmus řazení vkládáním je vlastně speciálním případem tohoto spojování dvou balíčků dohromady, kdy jeden balíček čítá $n-1$ karet a druhý jen jednu.

Toto jo základní myšlenka algoritmu typu *rozděl a panuj*. Daný problém rozdělíme na menší části, které lze vyřešit, a tyto části pak spojíme. Jak vyřešíme ty menší části? Znovu vyvoláme náš algoritmus – rozdělíme je na ještě menší části, které vyřešíme! Takto pokračujeme dál, dělíme na menší a menší části, až se dostaneme k těm, které lze nějak triviálně vyřešit (v našem případě je triviální jednotkou balíček o jedné kartě, který je rovnou srovnaný). Brzy zjistíme, že tento rekurzivní přístup je rychlejší než řazení vkládáním.

Definujme $P(n)$ jako počet kroků, kolik potřebuje algoritmus rozděl a panuj na seřazení n karet. Pro jednoduchost předpokládejme, že n je mocnina dvou, abychom mohli bez obav dělit balíček na

[4]To nejlepší video najdeš pod tímto odkazem: *https://youtu.be/lyZQPjUT5B4*.

půlky. V triviálním případě pro $n = 1$ máme $P(n) = 0$. Pro $n > 1$ pak dostáváme rekurzivní relaci

$$P(n) = 2 \cdot P\left(\frac{n}{2}\right) + n - 1,$$

což znázorňuje to, že balíček rozdělíme na půlky, které zvlášť vyřešíme v $P\left(\frac{n}{2}\right)$ krocích a poté je spojíme dohromady v $n - 1$ krocích[5]. Vyřešením této rekurzivní rovnice dostaneme počet kroků algoritmu v závislosti na n.

Úloha 9. Pomocí indukce (nebo jinak) ukaž, že $P(n) \leq n \log_2 n$ pro $n = 2^k$, kde k je přirozené číslo.

Tedy počet kroků v tomto algoritmu roste nanejvýš jako $n \log_2 n$, což je pro velká n o mnoho lepší než řazení vkládáním!

Úloha 10. Řazení vkládáním si lze také představit jako rekurenci. Napiš jaké vztahy splňuje příslušné $P(n)$ a indukcí ukaž, že řešením je opravdu $\frac{n(n-1)}{2}$.

Halting problem

Dostaneme-li nějaký algoritmus, vždy bychom si měli položit některé důležité otázky. Ku příkladu výše jsme zkoumali rychlost algoritmu, tedy kolik kroků potřebuje, než dospěje k výsledku. Avšak možná nejdůležitější otázkou je, zda se algoritmus vůbec někdy zastaví. U Eukleidova algoritmu a u bublinkového řazení jsme dokázali, že po nějakém čase se proces vždy zastaví. Existuje však obecný postup, kterým by šlo dokázat, že se algoritmus zastaví či nezastaví?

Problém zastavení zní takto: Máme před sebou algoritmus a nějakou jeho vstupní hodnotu (například dvě čísla, jejichž společného dělitele hledáme). Vložíme-li do algoritmu tuto vstupní hodnotu, zastaví se někdy nebo poběží donekonečna? A teď pojďme o úroveň výš – zkusme navrhnout obecný postup, který by pro daný algoritmus ukázal, zda se zastaví. To znamená navrhnout algoritmus, který toto rozhodne.

Bohužel (nebo naštěstí) se o to pokoušet nemusíme – nemělo by to cenu:

Věta. *Neexistuje žádný algoritmus, který by byl vždy schopen správně rozhodnout, zda se jiný algoritmus vůbec někdy zastaví při zadaném vstupu.*

Důkaz. Naznačíme jen základní myšlenku stojící za důkazem, nebudeme zde zabíhat do detailů. Důkaz využívá takzvanou *diagonální metodu*, která se často objevuje v teorii množin a můžeš ji znát třeba z Cantorova důkazu, že reálná čísla jsou nespočetná množina.

Pro spor připusťme, že existuje algoritmus $\text{Halt}(T, t)$, který pro daný vstup t rozhodne, zda se daný algoritmus T zastaví. Tedy $\text{Halt}(T, t) = 1$, pokud T zastaví při vstupu t, a $\text{Halt}(T, t) = 0$, pokud proces T při vstupu t poběží donekonečna.

Úmluva. Pokud do algoritmu vložíme vstup, který s ním není kompatibilní, předpokládáme, že algoritmus vyhodí chybovou hlášku a zastaví se.

Nyní definujme diagonální funkci $\text{Diagonal}(s)$ takto:

$$\text{Diagonal}(s) = 1, \quad \text{pokud } \text{Halt}(s, s) = 0,$$

zatímco v opačném případě, kdy $\text{Halt}(s, s) = 1$, se proces $\text{Diagonal}(s)$ zacyklí v nekonečné smyčce.

Poznámka. Podle naší úmluvy výše definice dává smysl. Existují algoritmy, které na vstupu přijímají jiný algoritmus. Proto je možné dát do Haltu jako vstup jiný algoritmus, a pokud jej Halt nezvládne zpracovat, prostě se zastaví.

[5] Viz Cvičení 7.

Je to vcelku zvláštní funkce, protože využívá algoritmu Halt pro rozhodnutí, zda algoritmus s zastaví „sám na sobě“. Nyní toto paradoxní odkazování na sebe sama pojďme pozvednout na vyšší úroveň – zeptejme se, co se stane, když do Diagonal vložíme jako vstupní hodnotu algoritmus Diagonal.

Jsou pouze dvě možnosti:

(1) Pokud Diagonal(Diagonal) = 1, znamená to, že Halt(Diagonal, Diagonal) = 0, tedy program Diagonal nikdy nezastaví, je-li vstupem Diagonal. To je ale ve sporu s tím, že Diagonal(Diagonal) = 1, tedy že Diagonal sám na sobě zastaví (a vyhodí hodnotu 1).

(2) Pokud Diagonal(Diagonal) nikdy nezastaví a zacyklí se v nekonečné smyčce, musí platit Halt(Diagonal, Diagonal) = 1. To znamená, že algoritmus Diagonal po nějakém čase zastaví, je-li na vstupu sám Diagonal. To je však spor s předchozím předpokladem, že se Diagonal(Diagonal) zacyklí v nekonečné smyčce.

V obou případech dojdeme ke sporu. Nějaký předpoklad, který jsme v průběhu použili, tedy nebyl pravdivý. A protože jediné tvrzení, jehož pravdivost jsme předpokládali, je to, že existuje algoritmus Halt, tak nutně žádný takový algoritmus neexistuje. Tím je důkaz hotov. □

Tuto větu dokázal v roce 1936 anglický matematik Alan Turing. O Turingově práci na rozluštění Enigmy (přístroje, kterým Němci za druhé světové války šifrovali tajné zprávy) se můžeš dozvědět například ve filmu Kód Enigmy (The Imitation Game) z roku 2014.

Ne vždy lze rozhodnout, zda se algoritmus zastaví, případně sice víme, že se zastaví, ale až po nepřiměřeně dlouhé době, přičemž přibližný výsledek dostaneme už za kratší čas. V praxi proto na vstupu často zadáváme, kolik iterací má algoritmus provést, či jak přesný výsledek potřebujeme (například přesnost na čtyři desetinná místa).

Poděkování a rozloučení

Gratulujeme, že ses dočetl(a) až sem! Věříme, že ses při čtení dozvěděl(a) něco nového a hlavně že Tě některá část seriálu podnítila k zamyšlení a hledání odpovědí na otázky, které Ti vyvstaly na mysli. Přejeme mnoho zdaru při řešení seriálových úloh!

Zároveň bychom rádi poděkovali všem orgům, kteří se na seriálu podíleli, a že jich nebylo poskrovnu. Zejména děkujeme Hedvice za jazykové korektury a užitečné postřehy, Matějovi za TEXnickou podporu, krásné obrázky a další nápady a Radovi za odborné korektury. Poděkování patří také Lence a Radkovi, kteří pro vás připravili čokoLeanovou výzvu. A samozřejmě děkujeme všem orgům, kteří pomáhali s výběrem a opravováním úloh.

Návody ke cvičením

2. Největším společným dělitelem je číslo 17. Který způsob byl v tomto případě rychlejší?

3. Použij Eukleidův algoritmus k zjištění, že jejich nejvyšší společný dělitel je 1.

4. $(x, y) = (-7, -14)$.

5. Jaký je největší společný dělitel čísel 72 a 117?

6. Uprav rovnost na $ax = -by$ a podívej se na to, čím jsou jednotlivé strany dělitelné. Jakého tvaru jsou pak x a y?

Odpověď je $x = nb$ a $y = -na$, kde n je celé číslo.

7. Dává smysl vždy porovnat nejmenší dvě karty, z každé hromádky jednu, a tu nižší umístit na následující místo v nové řadě. V nové řadě je potom n karet, tedy proběhlo $n - 1$ porovnávání.

Návody k úlohám

1. Tvrzení: Nechť $a(x)$ a $b(x)$ jsou dva polynomy. Potom existuje právě jedna dvojice polynomů $q(x)$ a $r(x)$ taková, že $a(x) = q(x)b(x) + r(x)$, přičemž stupeň $r(x)$ je ostře nižší než řád $b(x)$.

Důkaz je obdobou důkazu dělicího algoritmu pro přirozená čísla.

2. Nejprve vyděl první mnohočlen druhým, poté pokračuj v duchu Eukleidova algoritmu.

3. Pomocí Eukleidova algoritmu najdi největšího společného dělitele $x^2 + x - 20$. Kořeny tohoto kvadratického polynomu již snadno spočítáš.

4. $(x, y) = (8 - 17n, -151 + 321n)$, kde $n \in \mathbb{Z}$.

5. $(x, y) = (75 - 52n, 486 + 337n)$, kde $n \in \mathbb{Z}$.

6. Použij Eukleidův algoritmus pozpátku.

7. Použij Bézoutovo lemma.

8. Použij Bézoutovo lemma, rovnosti vynásob a uvaž, co musí splňovat jakýkoli společný dělitel ab a c.

9. Použij indukci podle k.

10. $P(1) = 0$ a $P(n) = P(n-1) + n$.