Kapitola 1

Úvodní kurs

1.1 Výroky a kvantifikátory

Univerzitní matematika se od středoškolské matematiky odlišuje především důrazem na *abstrakci* a na *přesnost uvažování*.

Abstrakcí rozumíme to, že se většinou nebudeme zabývat konkrétními čísly nebo funkcemi, ale budeme zkoumat celé třídy matematických objektů, jako jsou čísla, rovnice, funkce, algoritmy, pravidla počítání. Výpočty budeme většinou provádět se symboly jako x, f, A, $\mathbf{v}$, atd.

Význam abstrakce spočívá v tom, že se snažíme formulovat matematické výsledky tak, aby je bylo možné použít v nejrůznějších situacích. Typickou a dobře známou ukázkou abstrakce je vzorec pro kořeny kvadratické rovnice s reálnými koeficienty

$$ax^2 + bx + c = 0,$$

kde $a \neq 0$. Říká, že kořeny této rovnice jsou čísla

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Tento vzorec vyjadřuje kořeny *libovolné* kvadratické rovnice s reálnými koeficienty. Potřebujeme-li vyřešit konkrétní rovnici, např. $2x^2 + 5x - 10 = 0$, stačí pouze dosadit do vzorce za symboly a, b, c konkrétní čísla, v našem případě $a = 2, b = 5, c = -10$.

Požadavek přesnosti uvažování vede k tomu, že matematika si vytváří vlastní jazyk, ve kterém se snaží odstranit jakékoliv nejednoznačnosti. Těm se přirozený jazyk nikdy nemůže vyhnout, ve skutečnosti jsou zdrojem mnohé zábavy, vtipů, básní, a také nedorozumění. Přesnost uvažování nám také pomáhá ujistit se, že naše matematické výsledky jsou správné. Prakticky vše, co budeme tvrdit, budeme také dokazovat. Důkazy nám dávají možnost pochopit, proč jsou matematická tvrzení správná, abychom je mohli případně adaptovat na jiné situace. A studiem důkazů se také učíme jak dokazovat nové matematické výsledky.

Pro úspěšné studium matematiky je třeba dobře zvládnout matematický jazyk.

Základním stavebním kamenem matematického jazyka jsou *výroky*. Výroky jsou věty, o kterých má smysl rozhodnout, jsou-li pravdivé nebo ne.

Příklady.

- Číslo π je kladné reálné číslo. (Je výrok.)
- Nový Bydžov je hlavní město Kanady. (Je výrok.)
- Císař pán je korunovanej. (Je výrok.)
- Ahoj! (Není výrok.)
- Miluji tě. (Je výrok.)
- 2^π je iracionální číslo. (Je výrok. Není ale známo, je-li pravdivý nebo ne.)

Výroky můžeme kombinovat do složitějších výroků pomocí *logických spojek a* a *nebo*. Spojky *a* a *nebo* jsou používámy také v přirozeném jazyce. V matematice je používáme v přesně definovaném významu, který zdůrazňujeme tím, že mluvíme o *logických spojkách*.

Definice 1.1.1. Jsou-li P, Q výroky, pak *konjunkce výroků* P, Q je výrok P a Q. *Disjunkce výroků* P, Q je výrok P nebo Q.

Konjunkci výroků P, Q zapisujeme také jako $P\&Q$ nebo $P \wedge Q$. Disjunkci výroků P, Q zapisujeme rovněž jako $P \vee Q$.

Pravdivost konjunkce a disjunkce výroků P, Q je definována pomocí pravdivosti výroků P, Q. Zdůrazněme ještě, že logickou spojku *a* používáme ve smyslu *a zároveň*. Logickou spojku *nebo* nepoužíváme ve *vylučujícím smyslu*, jak se občas stává v běžném jazyce.

Definice 1.1.2. Konjunkce P a Q je pravdivá, pokud jsou pravdivé oba výroky P, Q. Disjunkce P nebo Q je pravdivá, pokud je pravdivý aspoň jeden z výroků P, Q.

Výrok *číslo π je kladné reálné číslo a (zároveň) Nový Bydžov je hlavní město Kanady* tedy není pravdivý, zatímco výrok *číslo π je kladné reálné číslo nebo tě miluji* pravdivý je. Uspějete s ním ovšem pouze tehdy, pokud objekt vašeho zájmu nechápe spojku *nebo* ve vylučujícím smyslu, tj. že platí jedno nebo druhé, nikoliv obé současně.

Matematické výroky se narozdíl od výroků běžného jazyka (*Císař pán je korunovanej.*) vyznačují tím, že pojmy, které v nich používáme, jsou přesně definované. V této chvíli sice neumíme definovat reálné číslo, můžeme ale přesně definovat, co je to druhá odmocnina z kladného reálného čísla.

Definice 1.1.3. *Druhá odmocnina* z kladného reálného čísla x je takové kladné reálné číslo y, pro které platí $y^2 = x$.

Matematické definice dávají přesný matematický význam výrazům běžného jazyka, jako třeba vektor, matice, spojitost, podíl, grupa, které budeme v matematických formulacích používat. První součástí matematických textů jsou tedy *definice* používaných matematických pojmů. Definice tvoří slovník matematického jazyka, ve kterém jsou nové matematické pojmy definovány pomocí jiných matematických

pojmů, které považujeme za známé. Tak například v definici druhé odmocniny z kladného reálného čísla považujeme za známou operaci násobení (druhou mocninu) reálných čísel.

Naprostá většina matematických tvrzení je formulována tak, že z pravdivosti nějakého výroku, kterému říkáme *předpoklad*, plyne pravdivost jiného výroku, kterému říkáme *závěr*. Vždy je velmi důležité uvědomit si, co je předpoklad matematického tvrzení a co je závěr. V tvrzení

(T1a) Je-li $x > 0$ reálné číslo, pak existuje reálné číslo $y > 0$ takové, že $y^2 = x$.

je předpokladem výrok $x > 0$ *je reálné číslo* a závěrem je výrok *existuje reálné číslo* $y > 0$ *takové, že* $y^2 = x$. Můžeme jej také formulovat následujícím způsobem.

(T1b) Pro každé kladné reálné číslo x existuje kladné reálné číslo y takové, že $y^2 = x$.

Také tvrzení

(T1c) ke každému kladnému reálnému číslu existuje druhá odmocnina,

říká totéž, co tvrzení (T1a), vezmeme-li v úvahu Definici 1.1.3. Matematické definice tedy zjednodušují formulace, nemusíme vždy znovu vysvětlovat, co myslíme druhou odmocninou. Definice fixuje, co matematický termín znamená.

Vytváříme-li složitější výroky pomocí logických spojek *a* a *nebo*, musíme dávat pozor na jednoznačnost takto utvářených výroků. Např. výrok

(T2) miluji tě a číslo π je kladné reálné číslo nebo císař pán je korunovanej,

lze interpretovat dvěma různými způsoby. Buď jako

(T3) (miluji tě a číslo π je kladné reálné číslo) nebo císař pán je korunovanej,

tj. jako disjunkci dvou výroků, z nichž ten první je konjunkcí jiných dvou výroků, nebo jako

(T4) miluji tě a (číslo π je kladné reálné číslo nebo císař pán je korunovanej),

tj. jako konjunkci dvou výroků, z nichž ten druhý je disjunkcí jiných dvou výroků. Jde skutečně o dva různé výroky, protože výrok (T3) je pravdivý, je-li císař pán korunovanej, bez ohledu na to, jsem-li zamilovaný nebo ne. Oproti tomu k pravdivosti výroku (T4) stačí, abych byl zamilovaný a na císař pánovi nezáleží.

Podobných nejednoznačností je přirozený jazyk plný. Pokud jej používáme pro vyjádření matematických poznatků nebo úloh, musíme si být vědomi možných nejednoznačností. Tak například výraz z učebnice pro základní školy *součet trojnásobku neznámého čísla zvětšeného o dva a dvojnásobku téhož neznámého čísla zmenšeného o tři* můžeme matematicky vyjdřit jako $3(x + 2) + 2(x - 3)$ nebo jako $3x + 2 + 2x - 3$. První formulace je správná, druhá je také možná. Záleží na tom, co podle nás rozvíjí přívlastek *zvětšeného*. Jestli podstatné jméno *čísla* nebo celý větný člen *trojnásobek neznámého čísla*.

Typické matematické tvrzení je implikace ve smyslu následující definice.

Definice 1.1.4. Jsou-li P, Q výroky, pak výrok *z* P *plyne* Q nazýváme *implikace*.

Vzhledem k tomu, jak často se implikace v matematických textech vyskytují, existuje mnoho různých způsobů, jak je formulovat. Řadu z nich uvádíme v následujícím příkladu, v závorkách jsou pak jejich anglické verze.

Příklady.
- Je-li P, pak Q. (If P, then Q.)
- Platí-li P, pak platí Q. (If P holds, then Q holds.)
- P implikuje Q. (P implies Q.)
- Nechť platí P. Pak platí Q. (Let P hold. Then Q holds.)
- P je postačující podmínka pro Q. (P is a sufficient condition for Q.)
- Q je nutná podmínka pro P. (Q is a necessary condition for P.)
- P platí pouze platí-li Q. (P holds only if Q holds.)
- Pokud Q neplatí, pak neplatí P. (If Q does not hold, then P does not hold.)

Je věcí vkusu a jazykového citu, kterou z variant autor zvolí v závislosti na konkrétní podobě výroků P a Q.

Také pravdivost implikace můžeme rozhodnout na základě pravdivosti výroků P a Q.

Definice 1.1.5. Jsou-li P, Q výroky, pak implikace *z P plyne Q* je pravdivá, jestliže jsou pravdivé současně oba výroky P, Q, nebo výrok P není pravdivý.

Druhá z podmínek pravdivosti implikace *z P plyne Q* říká jinými slovy, že z nepravdivého výroku plyne cokoliv.

Implikace *z P plyne Q* se v matematických textech často zapisuje jako

$$P \Rightarrow Q.$$

Také my budeme toto označení používat.

V matematických formulacích záleží na každém slově. Tak například tvrzení

(T5) je-li $x > 0$ reálné číslo, pak existuje právě jedno reálné číslo $y > 0$ takové, že $y^2 = x$.

se od tvrzení (T1a) liší pouze dvěma slovy *právě jedno*.

Závěr této implikace *existuje právě jedno reálné číslo $y > 0$ takové, že $y^2 = x$* je ve skutečnosti konjunkcí dvou výroků, výroku *existuje aspoň jedno reálné číslo $y > 0$ takové, že $y^2 = x$* a výroku *existuje nejvýše jedno reálné číslo $y > 0$ takové, že $y^2 = x$*. Máme-li dokázat tvrzení (T5), musíme dokázat, že z předpokladu $x > 0$ *reálné číslo* plynou oba výroky, jejichž konjunkcí je závěr tvrzení (T5). Musíme tedy dokázat obě následující tvrzení.

(T6) Je-li $x > 0$ reálné číslo, pak existuje aspoň jedno reálné číslo $y > 0$ takové, že $y^2 = x$,

které říká totéž, co tvrzení (T1a), a tvrzení

(T7) je-li $x > 0$ reálné číslo, pak existuje nejvýše jedno reálné číslo $y > 0$ takové, že $y^2 = x$.

K důkazu tvrzení (T6) musíme přesně definovat, co je to reálné číslo a to je v současnosti mimo naše možnosti. Důkaz tvrzení (T7) je naopak jednoduchý a stačí k němu znát základní pravidla počítání s reálnými čísly.

Uvedeme si ještě definici negace výroku.

Definice 1.1.6. Je-li P výrok, pak *negace výroku* P je výrok $\neg P$.

Negaci výroku P můžeme také formulovat různými způsoby:

Příklady.
- P není pravdivý. (P is not true.)
- P neplatí. (P does not hold.)
- Není pravda, že P. (It is not true that P.)

Definice 1.1.7. Negace $\neg P$ je pravdivá, pokud výrok P není pravdivý.

Dalším běžným typem matematického tvrzení je ekvivalence dvou výroků.

Definice 1.1.8. Jsou-li P, Q výroky, pak říkáme že P *je ekvivalentní s* Q, pokud je pravdivá konjunkce dvou implikací $(P \Rightarrow Q)$ *a* $(Q \Rightarrow P)$.

Také výrok P *je ekvivalentní s* Q můžeme formulovat různými způsoby. Dvě nejčastější varianty jsou uvedené v následujícím příkladu.

Příklady.
- P platí právě tehdy, když platí Q. (P holds if an only if Q holds.)
- P právě když Q. (P if and only if Q.)

Výrok P *je ekvivalentní s* Q také zapisujeme jako

$$P \Leftrightarrow Q.$$

Tento zápis budeme často používat.

Pomocí pravdivostní tabulky můžeme dokázat následující tvrzení.

(T9) Pro libovolné dva výroky P, Q platí, že P je ekvivalentní s Q právě tehdy, když jsou výroky P, Q současně pravdivé nebo jsou současně nepravdivé.

Každý matematik používá zcela automaticky ekvivalence mezi různými dvojicemi výroků. Neúplný výčet těchto zautomatizovaných ekvivalencí následuje. První z nich je jinou formulací tvrzení (T9). Všechny můžeme dokázat pomocí pravdivostních tabulek.

Příklady. Nechť P, Q jsou libovolné výroky. Pak platí

- $P \Leftrightarrow Q$ právě když (P a Q) nebo ($\neg\ P$ a $\neg\ Q$),
- $P \Rightarrow Q$ právě když $\neg\ Q \Rightarrow \neg\ P$,
- $\neg(P$ a $Q)$ právě když $(\neg\ P)$ nebo $(\neg\ Q)$, (negace konjunkce je disjunkce negací)
- $\neg(P$ nebo $Q)$ právě když $(\neg\ P)$ a $(\neg\ Q)$, (negace disjunkce je konjunkce negací)
- $\neg(P \Rightarrow Q)$ právě když P a $\neg\ Q$.

Snaha o obecnost a abstrakci vede k častému používání jiných dvou výrazů: *pro každý* a *existuje*. Setkali jsme se s nimi už v tvrzení (T1b). Přeformulujeme si toto tvrzení ještě jedním způsobem.

(T10) Pro každé reálné číslo $x > 0$ existuje reálné číslo $y > 0$ takové, že $y^2 = x$.

Vezměme si ještě jednodušší tvrzení:

(T11) pro každé nenulové reálné číslo y platí $y^2 > 0$.

V něm se říká, že výrok y^2 *je kladné číslo* je pravdivý (platí) pro každé nenulové reálné číslo. O pravdivosti tohoto výroku můžeme rozhodnout teprve tehdy, víme-li konkrétní hodnotu čísla y. Pokud by y bylo rovné komplexní jednotce i, výrok y^2 *je kladné číslo* by pravdivý nebyl. Výrok y^2 *je kladné číslo* závisí na parametru y. Protože je tento výrok pravdivý pro velkou spoustu parametrů y, formulujeme naše tvrzení tak, že uvedeme, pro jaké hodnoty parametru y tvrdíme, že je výrok y^2 *je kladné číslo* pravdivý. Přesně to říká výraz *pro každé nenulové reálné číslo* y.

Častá podoba matematického tvrzení je

(T12a) pro každé $y \in S$ platí $P(y)$.

V našem případě je S množina všech nenulových reálných čísel a $P(y)$ je výrok $y^2 > 0$.
Pro výraz *pro každé* $y \in S$ používáme speciální značení

$$\forall\, y \in S.$$

Této formulaci říkáme *obecný kvantifikátor*, y je *kvantifikovaná proměnná*.
Tvrzení (T12a) pomocí obecného kvantifikátoru můžeme formulovat také následovně

(T12b) $(\forall\, y \in S)P(y)$.

Druhým typem kvantifikátoru je *existenční kvantifikátor*. Také s ním jsme se už setkali ve výroku *existuje reálné číslo* $y > 0$ *takové, že* $y^2 = x$. Pro větší jednoduchost si ještě zvolíme $x = 2$ a budeme uvažovat výrok *existuje reálné číslo* $y > 0$ *takové, že* $y^2 = 2$. V něm tvrdíme, že v množině všech kladných reálných čísel existuje prvek y, pro který platí (je pravdivý) výrok $y^2 = 2$. Poslední výrok $y^2 = 2$ závisí na parametru y, označíme si jej tedy $Q(y)$. A protože množinu všech kladných reálných čísel jsme označili S, můžeme náš výrok formulovat takto:

(T13a) existuje $y \in S$ takové, že platí $Q(y)$.

Také pro výraz *existuje* $y \in S$ používáme speciální značení

$$\exists\, y \in S,$$

pomocí kterého tvrzení (T13a) formulujeme následovně.

(T13b) $(\exists\, y \in T)Q(y)$.

Kvantifikátory obou typů můžeme kombinovat a formulovat tak složitější tvrzení. Ukázku jsme už formulovali v tvrzení (T1b). Pomocí kvantifikátorů je můžeme formulovat takto

$$(\forall\, x > 0)(\exists\, y > 0)(y^2 = x).$$

Tento výrok říká přesně totéž jako výrok (T2), pokud víme, že x, y jsou reálná čísla. A pokud použijeme označení S pro množinu všech kladných reálných čísel, můžeme jej formulovat také jako

$$(\forall\, x \in S)(\exists\, y \in S)(y^2 = x).$$

Na pořadí kvantifikátorů stejného typu nezáleží, naopak pořadí kvantifikátorů různého typu měnit nemůžeme.

Všechny matematické texty mají nějaký *kontext*. Ten říká, s jakými objekty pracujeme. Poslední dvě formulace říkají totéž jako výrok (T1b), pokud víme, že *pracujeme v kontextu reálných čísel*. Kontext umožňuje neopakovat stále v každém tvrzení, že se zabýváme reálnými čísly. Stačí říct v úvodu knihy, kapitoly, odstavce, že v následujícím textu budeme pracovat s reálnými čísly. Kontext tak může být vyjádřený mnoho stránek před tím, než je třeba jej v nějakém tvrzení použít jako jeden z předpokladů.

Pokud v nějakém tvrzení používáme výraz *existuje právě jedno* $y \in S$, používáme pro takto formulovaný existenční kvantifikátor označení $\exists\,!\, y \in S$. Tvrzení (T5) pak pomocí kvantifikátorů zapíšeme jako

$$(\forall\, x \in S)(\exists\,!\, y \in S)(y^2 = x).$$

Také obecný kvantifikátor *pro každé* $x \in S$ můžeme vyjádřit mnoha různými způsoby. Neúplný přehled následuje.

Příklady.
- Nechť $x \in S$,
- nechť je dáno $x \in S$,
- kdykoliv $x \in S$,
- ať $x \in S$,
- každé $x \in S$,
- ka každému $x \in S$,
- pro každé $x \in S$.

Podobně rovněž existenční kvantifikátor *existuje* $x \in S$ formulujeme také jako

Příklady.
- pro nějaké $x \in S$,
- existuje aspoň jedno $x \in S$,
- lze nalézt $x \in S$.

Zápis výroků pomocí kvantifikátorů usnadňuje formulaci negace libovolně složitého výroku. To v běžném jazyce může občas působit problémy.

Jestliže výrok $(\forall\, x \in S)(P(x))$ neplatí, existuje nějaké $x \in S$, pro které výrok $P(x)$ neplatí, tj. platí jeho negace $\neg\, P(x)$. Negace výroku $(\forall\, x \in S)(P(x))$ je tedy ekvivalentní s výrokem

$$(\exists\, x \in S)(\neg\, P(x)).$$

Naopak, pokud neplatí výrok $(\exists\, y \in T)(Q(y))$, znamená to, že pro každé $y \in T$ platí negace výroku $Q(y)$, tj. platí výrok $\neg\, Q(y)$. Negace výroku $(\exists\, y \in T)(Q(y))$ je tak ekvivalentní s výrokem

$$(\forall\, y \in T)(\neg\, Q(y)).$$

Takto můžeme zcela mechanicky najít negaci každého kvantifikovaného výroku P. Každý obecný kvantifikátor nahradíme existenčním, každý existenční kvantifikátor nahradíme obecným kvantifikátorem a výrok P nahradíme jeho negací $\neg\, P$.

Negace výroku

$$(\forall\, x > 0)(\exists\, y > 0)(y^2 = x).$$

je tak ekvivalentní s výrokem

$$(\exists\, x > 0)(\forall\, y > 0)\, \neg\, (y^2 = x).$$

A protože negací výroku $y^2 = x$ je výrok $y^2 \neq x$, je negace výroku o existenci reálné druhé odmocniny z kladného reálného čísla ekvivalentní s výrokem

$$(\exists\, x > 0\, \forall\, y > 0)(y^2 \neq x).$$

Už z první přednášky víme, že

Příklady.

- výrok $\neg\, (P \wedge Q)$ je ekvivalentní s výrokem $\neg\, P \vee \neg\, Q$,
- výrok $\neg\, (P \vee Q)$ je ekvivalentní s výrokem $\neg\, P \wedge \neg\, Q$,
- výrok $\neg\, (P \Rightarrow Q)$ je ekvivalentní s výrokem $P \wedge \neg\, Q$.

Nyní můžeme zkusit formulovat nějakou složitější negaci.

Příklady. Negujte výrok *Každý je někdy na někoho naštvaný, ale ne vždy a ne na každého.*

1.2 Kongruence celých čísel

V dalším textu se budeme zabývat výhradně celými čísly. Množinu všech celých čísel budeme označovat $\mathbb{Z}$. Množinu všech přirozených čísel budeme označovat $\mathbb{N}$. Číslo 0 za přirozené číslo *nepovažujeme*. To je věcí dohody, někteří autoři 0 mezi přirozená čísla řadí.

Začneme s větou o dělení se zbytkem.

thm:deleni **Věta 1.2.1.** *Je-li $a \in \mathbb{Z}$ celé číslo a $n \in \mathbb{N}$ přirozené číslo, pak existují jednoznačně určená čísla $q \in \mathbb{Z}$ a $r \in \{0, 1, \ldots, n-1\}$ taková, že*

$$a = nq + r.$$

Důkaz. Existenci lze dokázat tak, že dokážeme správnost školského algoritmu pro dělení se zbytkem. Ukážeme jiný postup. Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$ jsou libovolná. Potřebujeme nalézt $q, r \in \mathbb{Z}$ tak, aby $0 \leq r \leq n-1$ a $a = nq + r$. Nechť q je největší celé číslo takové, že $a - nq \geq 0$[1] a položme $r = a - nq$. Nyní $a = nq + r$ a $r \geq 0$, takže stačí ověřit, že $r \leq n-1$. To plyne z volby q: Platí $a - n(q+1) < 0$ a po úpravě $r < n$.

K důkazu jednoznačnosti předpokládejme, že $a \in \mathbb{Z}, n \in \mathbb{N}$ a $a = nq_1 + r_1$, $a = nq_2 + r_2$, kde $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1, r_2 \leq n-1$. Potřebujeme ukázat, že $q_1 = q_2$ a $r_1 = r_2$. Ze vztahu $nq_1 + r_1 = nq_2 + r_2 (= a)$ dostáváme po úpravě

$$n(q_1 - q_2) = r_1 - r_2$$

a aplikací absolutní hodnoty na obě strany získáme

$$n|q_1 - q_2| = |r_1 - r_2|.$$

Z $r_1 \leq n-1$, $-r_2 \leq 0$ dostaneme sečtením $r_1 - r_2 \leq n-1$. Podobně dostaneme $-(n-1) \leq r_1 - r_2$ a dohromady $|r_1 - r_2| \leq n-1$. Na pravé straně tedy máme výraz ostře menší než n. Z levé strany nyní vidíme, že $|q_1 - q_2| = 0$, neboli $q_1 = q_2$. Teď už zřejmě $r_1 = r_2$ (protože např. $r_1 = a - nq_1 = a - nq_2 = r_2$). □

Definice 1.2.2. Číslo $q \in \mathbb{Z}$ (resp. $r \in \{0, 1, \ldots, n-1\}$) z předchozí věty nazýváme *podíl* (resp. *zbytek*) *při dělení a číslem n*. Zbytek při dělení a číslem n označujeme $a \bmod n$.

Příklady.
- *Podíl při dělení čísla* 17 *číslem* 5 *je* 3 *a zbytek je* 2, *protože* $17 = 5 \cdot 3 + 2$ *a* $0 \leq 2 \leq 5 - 1$.
- *Podíl při dělení čísla* -17 *číslem* 5 *je* -4 *a zbytek je* 3, *protože* $-17 = 5 \cdot (-4) + 3$ *a* $0 \leq 3 \leq 5 - 1$.

Pro daná dvě přirozená čísla můžeme jejich podíl a zbytek zjistit školským dělením. Rozmyslete si jak vydělit záporné číslo číslem přirozeným. Pokud se vám zdá definice v tomto případě nepřirozená, zamyslete se nad jinými možnými definicemi v kontextu následujících vět.

Nyní připomeneme definici dělitelnosti dvou celých čísel.

Definice 1.2.3. Jsou-li $a, b \in \mathbb{Z}$ celá čísla, pak říkáme, že a *dělí* b, jestliže existuje $c \in \mathbb{Z}$ takové, že $b = ac$. Skutečnost, že a dělí b zapisujeme také $a \mid b$. Pokud a nedělí b, píšeme $a \nmid b$.

Příklady.
- 5 *dělí* -15, *protože* $-15 = 5 \cdot (-3)$
- 4 *nedělí* 13, *protože* $4c = 13$ *neplatí pro žádné celé číslo* c
- *jakékoliv číslo* a *dělí* 0, *protože* $0 = a \cdot 0$
- 0 *nedělí žádné číslo, kromě* 0 *(proč?)*

Příklady. *Dokažte následující dvě tvrzení:*
- *Pokud* $n, a, b \in \mathbb{Z}$, $n \mid a$ *a* $n \mid b$, *pak* $n \mid a + b$.
- *Pokud* $n, a, b \in \mathbb{Z}$, $n \mid a$, *pak* $n \mid ab$. *Speciálně, pokud* $n \mid a$, *pak* $n \mid -a$.

Uvedená tvrzení budeme v dalším textu často používat, někdy vícekrát v jednom kroku důkazu. Například v úvaze „pokud $3 \mid a$ *a* $3 \mid b$, *pak* $3 \mid 17a - 45b$“ *používáme dvakrát druhé tvrzení a jednou první.*

Velice užitečným pojmem při studiu dělitelnosti je kongruence:

Definice 1.2.4. Jsou-li $a, b \in \mathbb{Z}$ celá čísla a $n \in \mathbb{N}$ přirozené číslo, pak říkáme, že a *je kongruentní s* b *modulo* n, jestliže n dělí $a - b$.

Skutečnost, že a je kongruentní s b modulo n zapisujeme jako $a \equiv b \pmod{n}$. Jestliže a není kongruentní s b modulo n, pak píšeme $a \not\equiv b \pmod{n}$.

Jinými slovy, a je kongruentní s b modulo n, pokud se a od b liší o celočíselný násobek čísla n.

Příklady. $3 \equiv 13 \pmod{5}$, $3 \equiv -2 \pmod{5}$, $3 \not\equiv -3 \pmod{5}$.

Následující věta dokládá, že $a \equiv b \pmod{n}$ právě tehdy, když a a b dávají po dělení n stejný zbytek.

[1] Vysvětlit, že existuje

Věta 1.2.5. *Pro libovolná dvě celá čísla $a, b \in \mathbb{Z}$ a pro libovolné přirozené číslo $n \in \mathbb{N}$ platí $a \equiv b \pmod{n}$ právě tehdy, když $a \bmod n = b \bmod n$.*

Důkaz. Nechť $a, b \in \mathbb{Z}$ a $n \in \mathbb{N}$ jsou libovolná. Označme q_1, r_1 (resp. q_2, r_2) podíl a zbytek po dělení čísla a (resp. b) číslem n. Tedy $a \bmod n = r_1$ a $b \bmod n = r_2$.

Důkaz implikace $\Rightarrow$. Předpokládejme, že $a \equiv b \pmod{n}$, neboli $n \mid a - b$. Potřebujeme dokázat, že $r_1 = r_2$. Ze vztahů $a = nq_1 + r_1$, $b = nq_2 + r_2$ dostaneme po úpravě

$$(a - b) + n(q_1 - q_2) = r_1 - r_2.$$

Oba sčítanci na levé straně jsou dělitelní n, takže n dělí levou stranu, tedy také $n | r_1 - r_2$. Protože $-(n-1) \leq r_1 - r_2 \leq n - 1$ (viz důkaz tvrzení 1.3.1), máme $r_1 - r_2 = 0$, tedy $r_1 = r_2$ a jsme hotovi.

Důkaz implikace $\Leftarrow$. Předpokládáme, že $r_1 = r_2$, a snažíme se dokázat $n \mid a - b$. Úpravou $a = nq_1 + r_1$, $b = nq_2 + r_2$ získáme

$$a - b = n(q_2 - q_1) + (r_2 - r_1) = n(q_2 - q_1).$$

Výraz na pravé straně je dělitelný n tedy i $n \mid a - b$, což jsme chtěli. □

Následující tvrzení ukazuje, že relace „být kongruentní modulo n“ je *reflexivní*, *symetrická* a *tranzitivní*, takže je to *ekvivalence*. Tyto pojmy potkáte později v úvodním kurzu.

Věta 1.2.6. *Buď $a, b, c \in \mathbb{Z}$ a $n \in \mathbb{N}$. Pak platí*

1. *$a \equiv a \pmod{n}$ (reflexivita),*
2. *jestliže $a \equiv b \pmod{n}$, pak $b \equiv a \pmod{n}$ (symetričnost),*
3. *jestliže $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, pak $a \equiv c \pmod{n}$ (tranzitivita).*

Důkaz.

1. $n | a - a$, tedy $a \equiv a \pmod{n}$.
2. Pokud $a \equiv b \pmod{n}$, čili $n \mid a - b$, pak $n \mid -(a - b) = b - a$, čili $b \equiv a \pmod{n}$.
3. Pokud $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, neboli $n \mid a - b$ a $n \mid b - c$, pak $n \mid (a - b) + (b - c) = a - c$, neboli $a \equiv c \pmod{n}$.

□

Obecnou vlastností ekvivalencí je, že se příslušná množina rozpadá na disjunktní třídy navzájem ekvivalentních prvků. V našem případě, např. pro $n = 5$, lze množinu celých čísel rozložit na 5 podmnožin $A_0, A_1, \ldots, A_4$:

$$\begin{aligned} A_0 &= \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\} \\ A_1 &= \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\} \\ &\ldots \\ A_4 &= \{\ldots, -6, -1, 4, 9, 14, 19, \ldots,\} \end{aligned}$$

(A_i je tvořená čísly, která dávají po dělení pěti zbytek i.) Dvě celá čísla jsou kongruentní modulo 5 právě tehdy, když náleží do stejné podmnožiny.

Tranzitivita také ospravedlňuje řetězové zápisy kongruencí typu

$$a_1 \equiv a_2 \equiv \cdots \equiv a_k \pmod{n}.$$

Pokud totiž kongruence platí vždy pro sousední prvky, pak je libovolná dvojice a_i a a_j kongruentní modulo n.

Další tvrzení ukazuje, že dvě kongruence modulo n lze sečíst i vynásobit.

thm:operace

Věta 1.2.7. *Buď $a, b, c, d \in \mathbb{Z}$ a $n \in \mathbb{N}$. Pak platí*

1. *jestliže $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, pak $a + c \equiv b + d \pmod{n}$,*
2. *jestliže $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, pak $ac \equiv bd \pmod{n}$.*

Důkaz.

1. Pokud $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, pak $n \mid a-b$ a $n \mid c-d$, takže $n \mid (a-b)+(c-d) = (a+c)-(b+d)$ a tím pádem $a+c \equiv b+d \pmod{n}$.
2. Máme-li $n \mid a-b$, pak $n \mid (a-b)c = ac-bc$, tedy $ac \equiv bc \pmod{n}$. Podobně ukážeme, že $bc \equiv bd \pmod{n}$. Nyní $ac \equiv bc \equiv bd \pmod{n}$ a jsme hotovi (užíváme tranzitivitu).

□

Příklady.

- Je-li $a \equiv b \pmod{n}$ a $c \in \mathbb{N}$, pak také $a^c \equiv b^c \pmod{n}$. Lze totiž c-krát vynásobit kongruenci $a \equiv b \pmod{n}$.
- Na druhou stranu obecně neplatí, že pokud $a, b, c \in \mathbb{N}$ a $a \equiv b \pmod{n}$, pak $c^a \equiv c^b \pmod{n}$. Například $1 \equiv 4 \pmod{3}$, ale $2^1 \not\equiv 2^4 \pmod{3}$.

Z věty thm:operace 1.3.7 a předchozího příkladu vyplývá, že ve výrazu můžeme nahradit sčítanec, součinitel a mocněnec kongruentním číslem (modulo n) a výsledek bude kongruentní s původním výrazem modulo n. Pozor ale na exponenty, kde toto provést nelze.

Příklad. *Chceme-li zjistit zbytek po dělení čísla* $33^{159951} \cdot 19 - 16$ *číslem* 17*, můžeme upravovat*

$$33^{159951} \cdot 19 - 16 \equiv (-1)^{159951} \cdot 2 + 1 = -2 + 1 = -1 \equiv 16 \pmod{17},$$

tedy hledaný zbytek je 16*. (Při výpočtu jsme užili kongruencí* $33 \equiv -1 \pmod{17}$*,* $19 \equiv 2 \pmod{17}$*,* $-16 \equiv 1 \pmod{17}$ *a* $-1 \equiv 16 \pmod{17}$*.)*

Nyní budeme směřovat k řešení některých typů lineárních kongruencí, tj. rovnic tvaru $ax \equiv b \pmod{n}$. K tomu připomeneme pojem největšího společného dělitele a Euklidův algoritmus na jeho hledání.

Definice 1.2.8. Jsou-li $a, b \in \mathbb{Z}$ celá čísla, taková, že aspoň jedno je nenulové, pak *největší společný dělitel* čísel a, b je největší celé číslo d, které dělí obě čísla a, b.

Největšího společného dělitele čísel a, b budeme označovat $\gcd(a, b)$.

Existují rozumné důvody definovat definovat $\gcd(0, 0) = 0$, zde je ale uvádět nebudeme.

Poznámka 1.2.9.

1. Pro libovolná dvě celá čísla $a, b \in \mathbb{Z}$ platí $\gcd(a, b) = \gcd(|a|, |b|)$,
2. pro každé přirozené číslo $b \in \mathbb{N}$ platí $\gcd(b, 0) = b$.

Podle bodu 1. stačí umět počítat největšího společného dělitele pro dvojice přirozených čísel. K tomu nám pomůže následující pozorování.

Věta 1.2.10. *Pro libovolná dvě čísla* $a, b \in \mathbb{N}$ *platí* $\gcd(a, b) = \gcd(b, a \bmod b)$.

Důkaz. Ukážeme, že dvojice čísel a, b a $b, a \bmod b$ mají stejné společné dělitele, věta pak bude zřejmá. Dokážeme tedy následující tvrzení: Je-li c celé číslo, pak c dělí a a b právě tehdy, když c dělí b a $a \bmod b$.

Buď $c \in \mathbb{Z}$ libovolné. Je třeba dokázat dvě implikace.

Pokud c dělí a a b, pak c dělí b a $a \bmod b$. Předpokládáme, že $c \mid a, b$. Triviálně $c \mid b$, takže zbývá dokázat $c \mid a \bmod b$. Označme q podíl při dělení a číslem b. Máme $a = bq + (a \bmod b)$, čili $a \bmod b = a - bq$. Protože $c \mid a$ a $c \mid -bq$, skutečně platí $c \mid a - bq = a \bmod b$.

Pokud c dělí b a $a \bmod b$, pak c dělí a a b. Předpokládáme, že $c \mid b, a \bmod b$. Triviálně $c \mid b$, zbývá dokázat $c \mid a$. Označme opět q podíl při dělení a číslem b. Máme $a = bq + (a \bmod b)$. Oba členy na pravé straně jsou dělitelné c, takže opravdu $c \mid a$. □

Poslední věta vede k následujícímu algoritmu pro nalezení největšího společného dělitele $\gcd(a, b)$, $a > b$. Tento algoritmus se nazývá *Euklidův algoritmus.*

if $b = 0$
  return a
else

return $\gcd(b, a \bmod b)$

Euklidův algoritmus tedy převede výpočet $\gcd(a,b)$, $a > b$, na výpočet $\gcd(b, a \bmod b)$. Všimněte si, že $b > a \bmod b$, takže argumenty pro rekurzivní volání jsou správně uspořádány. Navíc první argument při každém rekurzivním volání klesá, z čehož vyplývá, že algoritmus skončí. Formálně bychom toto tvrzení dokazovali indukcí, ale dělat to nebudeme.

Příklad. *Pro výpočet* $\gcd(-16, 38)$ *si nejprve uvědomíme, že* $\gcd(-16, 38) = \gcd(16, 38)$*, pak čísla uspořádáme sestupně a použijeme předchozí algoritmus:*

$$\gcd(38, 16) = \gcd(16, 6) = \gcd(6, 4) = \gcd(4, 2) = \gcd(2, 0) = 2.$$

Takže $\gcd(-16, 38) = 2$.

Bez rekurze lze Euklidův algoritmus napsat například takto:
while $b \neq 0$ **do**
$c \leftarrow a \mod b$,
$a \leftarrow b$,
$a \leftarrow c$,
end
return a

Následující věta říká, že $gcd(a, b)$ lze napsat ve tvaru $sa+tb$ pro nějaká celá čísla s, t. Tato čísla se nám budou hodit k řešení lineárních kongruencí. Jejich nalezení nejprve předvedeme na příkladu $a = 38, b = 16$. Postup je takový, že provádíme Euklidův algoritmus na výpočet $\gcd(38, 16)$ a zapíšeme každé dělení se zbytkem (tučně je vyznačen dělenec a dělitel):

$$\begin{aligned} \mathbf{38} &= 2 \cdot \mathbf{16} + 6 \\ \mathbf{16} &= 2 \cdot \mathbf{6} + 4 \\ \mathbf{6} &= 1 \cdot \mathbf{4} + 2 \\ \mathbf{4} &= 2 \cdot \mathbf{2} \end{aligned}$$

Pak postupujeme od konce a vyjadřujeme největší společný dělitel ve tvaru $s'a' + t'b'$, kde a', b' jsou tučně vyznačená čísla. V prvním kroku je zápis zřejmý, v dalších pak vyjádříme z příslušné rovnosti zbytek, dosadíme do předchozího vztahu a vytkneme tučná čísla:

$$\begin{aligned} 2 &= 0 \cdot \mathbf{4} + 1 \cdot \mathbf{2} \\ 2 &= 0 \cdot \mathbf{4} + 1 \cdot (\mathbf{6} - 1 \cdot \mathbf{4}) = 1 \cdot \mathbf{6} + (-1) \cdot \mathbf{4} \\ 2 &= 1 \cdot \mathbf{6} + (-1) \cdot (\mathbf{16} - 2 \cdot \mathbf{6}) = (-1) \cdot \mathbf{16} + 3 \cdot \mathbf{6} \\ 2 &= (-1) \cdot \mathbf{16} + 3 \cdot (\mathbf{38} - 2 \cdot \mathbf{16}) = 3 \cdot \mathbf{38} + (-7) \cdot \mathbf{16}. \end{aligned}$$

Dostali jsme $s = 3$, $t = -7$ (řešení je více, např. $s = 3 + 16, t = -7 - 38$).

Obecněji, pokud $a > b$, q a r jsou pořadě podíl a zbytek po dělení a číslem b a existují čísla s', t' taková, že $\gcd(a, b) = s'b + t'r$, pak existují čísla s, t taková, že $\gcd(a, b) = sa + tb$. To ukazuje následující výpočet:

$$\gcd(a, b) = s'b + t'r = s'b + t'(a - qb) = t'a + (s' - t'q)b,$$

takže stačí položit $s = t'$ a $t = s' - t'q$. Tímto způsobem bychom indukcí dokázali následující tvrzení.

thm:bezout **Věta 1.2.11.** *Jsou-li* $a, b \in \mathbb{Z}$ *libovolná celá čísla, pak existují celá čísla* $s, t \in \mathbb{Z}$ *taková, že*

$$\gcd(a, b) = sa + tb.$$

Poznámka 1.2.12. Číslům s, t z předchozí věty se říká *Bezoutovy koeficienty.*

Nyní již můžeme přistoupit k řešení jednoho důležitého typu lineární kongruence.

thm:inverz **Věta 1.2.13.** *Pro každé prvočíslo* p *a každé celé číslo* a*, které není násobkem* p*, existuje celé číslo* s *takové, že*

$$sa \equiv 1 \pmod{p}.$$

Důkaz. Nechť p je prvočíslo a $a \in \mathbb{Z}$ je celé číslo, které není násobkem p. Naším cílem je nalézt s takové, že $as \equiv 1 \pmod{p}$.

Protože $\gcd(a,p)$ dělí p a p je prvočíslo, tento největší společný dělitel je buď 1 nebo p. Ale p to být nemůže, protože, podle předpokladu, p nedělí a. Tedy $\gcd(a,p) = 1$. Podle věty 1.3.11 existují čísla $s,t \in \mathbb{Z}$ taková, že

$$1 = sa + tp.$$

Vezmeme nějaká taková čísla s,t a ukážeme, že opravdu $sa \equiv 1 \pmod{p}$. Skutečně, podle předchozího vztahu $sa = 1 - tp$, a protože $tp \equiv 0 \pmod{p}$, máme $sa = 1 - tp \equiv 1 \pmod{p}$ a jsme hotovi. □

Číslo s z předchozí věty je „inverzním prvek modulo p" a tak jej taky můžeme využít při řešení dalších lineárních kongruencí, viz cvičení. Důkaz dává zároveň návod jak takové s nalézt.

Příklad. *Najdeme $s \in \mathbb{Z}$ takové, že $8s \equiv 1 \pmod{19}$. Protože 19 je prvočíslo a 8 není jeho násobkem, můžeme použít postup z důkazu. Vypočítáme Bezoutovy koeficienty.*

$$\gcd(8,19) = 1 = (-7) \cdot 8 + 3 \cdot 19.$$

Takže můžeme položit $s = -7$. Všimněte si, že jakékoliv číslo s takové, že $s \equiv -7 \pmod{19}$ naší kongruenci řeší, tedy např. i $s = 12$ nebo $s = -45$, atd. Jako cvičení je přenechán důkaz, že žádná jiná s kongruenci neřeší.

Cvičení 1.2.14. *Jsou dána přirozená čísla x,a,b,c taková, že $x \equiv a \pmod{b}$ a $x \equiv a \pmod{c}$. Musí pak nutně platit $x \equiv a \pmod{bc}$? (V případě, že ne, zkuste přidat předpoklady, aby tvrzení platilo.)*

Cvičení 1.2.15. *Najděte poslední cifru čísla 3^{991}.*

Cvičení 1.2.16. *Dokažte, že číslo $16^{15} + 29^{14} + 42^{13}$ je dělitelné 13.*

Cvičení 1.2.17. *Dokažte, že pro libovolné přirozené číslo n platí $60 \mid n^6 - n^2$. (Nápověda: Zkoumejte daný výraz modulo 3, 4 a 5.)*

Cvičení 1.2.18. *Pro které dvojice čísel a,b bude v Euklidově algoritmu na výpočet $\gcd(a,b)$ vycházet stále podíl 1?*

Cvičení 1.2.19. *Najděte největší společný dělitel a Bezoutovy koeficienty pro čísla*

1. *1234 a 4321*
2. *650 a 702*
3. *$3^{45} - 1$ a $3^{65} - 1$*

Cvičení 1.2.20. *Dokažte, že s z věty 1.3.13, je určen „jednoznačně modulo p", tj. dokažte, že kdykoliv $sa \equiv 1 \pmod{p}$ a $s'a \equiv 1 \pmod{p}$, pak $s \equiv s' \pmod{p}$. Pomocí toho popište všechna řešení rovnice $xa \equiv 1 \pmod{p}$ (kde a,p jsou pevně zvolená).*

Cvičení 1.2.21. *Navrhněte postup jak pro daná celá čísla a,b a prvočíslo p nalézt celé číslo x takové, že $ax \equiv b \pmod{p}$.*

Cvičení 1.2.22. *Najděte všechna x, pro která $21x \equiv 6 \pmod{9}$. (Nápověda: nejprve nahlédněte, že obě strany a modul kongruence lze krátit společným dělitelem.)*