1. Dělitelnost

Když jsme byli malí, naučili jsme se dělit celá čísla. Brzy jsme si všimli, že některé dvojice čísel se spolu dělí lépe (třeba číslo 12 se dělí třemi skvěle), jiná už si tak nesednou (pětku třemi tak snadno nevydělíme). V této kapitole tento vztah matematicky zavedeme a prozkoumáme. Dostaneme se k výsledkům, které jsou vysoce užitečné v oblasti výpočetní techniky, tato kapitola také tvoří základ pro počítání modulo (kapitola 2) a řešení diofantických rovnic (kapitola 3).

M **Poznámka:** Čtenář jistě ví, že množinu celých čísel značíme písmenem $\mathbb{Z}$. Zajímavá otázka zní, proč $\mathbb{Z}$ a ne Z. Máme přece úmluvu, že prvky množin značíme malými písmeny a množiny samotné velkými písmeny. Důvod je následující. Když napíšeme Z, tak bychom tím mysleli „jen“ množinu celých čísel $\{0, 1, -1, 2, -2, \dots\}$. Jenže my zde nemluvíme jen o nějaké množině čísel, ta naše je speciální. Máme k ní totiž také operace a k nim zase velice užitečná pravidla. Takovéto komplikovanější struktury se studují například v oboru zvaném algebra a existují pro ně značení jako $(Z, +, \cdot)$. Zdvojené písmeno $\mathbb{Z}$ nám říká, že pracujeme s touto velice speciální množinou. Podobně máme značení $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ pro další populární množiny.

Což nás přivádí k důležité poznámce. V této knize se jako přirozená čísla bere množina

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

Bohužel se matematici nedokázali shodnout a řada z nich si myslí, že přirozená čísla zahrnují i nulu. Autor této knihy si to nemyslí. Poučení je, že když čtenář začne číst pojednání, ve kterém přirozená čísla hrají roli, tak by se měl podívat, co tím autor míní.

Zde tedy nula přirozená není. Pokud ji budeme chtít zahrnout, tak na to máme šikovné značení

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}.$$

△

1a. Dělitelnost

Dvě čísla a, b spolu mají speciální pouto, pokud pokus o vydělení čísla b číslem a ve světě celých čísel dopadne příznivě, tedy $\frac{b}{a} \in \mathbb{Z}$. V definici ale dělení použít nechceme, protože jde o operaci choulostivou (vadí jí nula) a navíc jí chybí některé užitečné vlastností. Proto v následující definici použijeme násobení.

Definice.
Nechť $a, b \in \mathbb{Z}$. Řekneme, že a **dělí** b, značeno $a \,|\, b$, jestliže existuje $k \in \mathbb{Z}$ takové, že $b = a \cdot k$.
V takovém případě říkáme, že a je **dělitel** b, popřípadě **faktor** b, a že b je **násobek** a.
Také říkáme, že b je **dělitelné** číslem a.

Let $a, b \in \mathbb{Z}$. We say that a **divides** b, denoted $a \,|\, b$, if $b = a \cdot k$ for some $k \in \mathbb{Z}$.
Then we say that a is a **divisor** of b or a **factor** of b and that b is a **multiple** of a.

M **Poznámka:** Definice slouží k zavedení nového pojmu (pojmenování, typu objektu). Matematická oficiální prohlášení obvykle začínají preambulí (úvodní větou), kde se čtenář dozví, s jakými objekty se bude pracovat. Zde jsou to nějaká dvě celá čísla nazvaná a, b. Podstatné je i to, co napsáno není. Matematici takovouto úvodní větu chápou tak, že a, b jsou zvoleny libovolně, tedy následující text se vztahuje na **všechna** celá čísla a, b. Formálně řečeno, v matematičtině slovo „nechť“ v sobě zahrnuje univerzální kvantifikátor $\forall$ neboli prokaždítko.

Pak už následuje definice samotná, v tomto případě nový vztah pojmenovaný dělitelnost. Zhruba řečeno existují dva druhy definic. Asi méně časté jsou definice výčtové, třeba „pěknými čísly nazýváme čísla 13 a 23“. Častější je typ definice, který vidíme zde: K novému pojmu specifikujeme test, který jednoznačně rozhodne, kdy daný pojem máme právo použít a kdy ne. Díky tomu se všichni shodnou, kdy ta věc platí (jedno číslo dělí druhé) a kdy ne. Tím je zaručena jednoznačnost matematiky.

Kde se definice berou? Z praxe. Při svém bádání si matematici občas všimnou, že určité objekty či určité vlastnosti jsou užitečné, tak jim přidělí jména. Zadefinovat si vlastně můžeme cokoliv (pokud je to logicky konzistentní), ale když naše definice nebude užitečná, tak ji matematici nebudou používat a bude zapomenuta. Současné definice jsou tedy výsledkem darwinovského výběru.

△

Příklad 1a.a: Dělí opravdu 3 číslo 12? Zkusíme test z definice. Dokážeme najít celé číslo k tak, aby $12 = 3k$? Ano, $k = 4$ vyhovuje. Máme tedy právo napsat, že $3 \,|\, 12$.

Platí, že $5 \mid 13$? Zkusíme najít k takové, že $13 = k \cdot 5$, a také jej najdeme, $k = \frac{13}{5}$. Má to ale háček, definice požaduje, aby k bylo celé číslo, což to naše k není. Protože jiné k splňující žádanou rovnost není, nejsme schopni splnit podmínku z definice a tudíž 5 nedělí 13 (což jsme asi tušili).

Tento příklad upozornil na jednu podstatnou věc: Ta specifikace „$k \in \mathbb{Z}$“ není jen formalita, jako že každá proměnná se má odněkud brát, ale je to zároveň klíčová část podmínky, stejně důležitá jako ten vzoreček. Budeme na to muset myslet, až budeme dokazovat dělitelnost. Aby byl takový důkaz kompletní, musíme čtenáře přesvědčit, že námi nalezená konstanta k má dvě vlastnosti: splňuje žádanou rovnost a je to celé číslo. To druhé je obvykle velmi snadné, ale to neznamená, že to lze opominout.

△

M **1a.1 Poznámka:** Podmínka z definice dělitelnosti by se formálně zapsala například takto: $\exists k \in \mathbb{Z}\colon b = a \cdot k$.

Je užitečné si s tímto formálním jazykem rozumět. Pokud je pro vás nový, popřípadě pokud narazíte na nějakou nejasnost, tak navštivte Dodatky k této knize.

Při práci s definicemi a tvrzeními je důležité si uvědomit, že konkrétní písmena použitá ve vzorcích jako proměnné nejsou podstatná a jsou volně nahraditelná jinými. Výjimkou jsou specializované konstanty. Například v tvrzení „Plocha kruhu o poloměru r je πr^2“ je evidentně π nutné, ale když všechna r zaměníme jiným písmenem, tak se obsah sdělení nezmění: „Plocha kruhu o poloměru w je πw^2“. Jméno proměnné není podstatné, je to jen ukazatel, jak se přesouvá informace: Když seženeme poloměr, tak se dotyčná hodnota dá do vzorce na odpovídající místo.

Stejně tak naše definice specifiuje, jak se objekty (celá čísla) přesouvají mezi sdělením „a dělí b“ a sdělením „máme jistou rovnost a info o celočíselnosti jednoho členu“. Symbolicky:

$$\forall a, b \in \mathbb{Z};\quad a \,|\, b \quad\longleftrightarrow\quad \exists k \in \mathbb{Z}\colon b = a \cdot k.$$

Je důležité nevázat se na písmena, ale podívat se, jak se jednotlivé objekty těmi písmeny označené přesouvají. Díky tomu pak můžeme tuto definici aplikovat i v situaci, kdy nás okolnosti donutí použít písmena jiným způsobem, například testovat, zda b dělí a. Možná je nejlepší místo písmen vidět symboly pro objekty:

$$\forall \heartsuit, \diamondsuit \in \mathbb{Z};\quad \heartsuit | \diamondsuit \quad\longleftrightarrow\quad \diamondsuit = \heartsuit \cdot \Theta \quad\wedge\quad \Theta \in \mathbb{Z}.$$

To nám říká, že pokud se nám podaří vytvořit algebraický vzorec, který formou (strukturou) souhlasí s tím napravo, a k tomu informaci o celočíselnosti, tak máme právo z příslušných komponent vytvořit informaci nalevo. Pokud například máme celá čísla $45, 9$ a k nim pravdivou rovnost $45 = 9 \cdot 5$ s poznámkou $5 \in \mathbb{Z}$, tak máme právo z těchto čísel vytvořit tvrzení „9 dělí 45“. Všimněte si, že formálně nemáme právo přejít k tvrzení $5 \,|\, 45$, protože ta pětka není na správném místě ve vzorci a tedy ji nelze přesunout na žádané místo. My ale samozřejmě můžeme tu rovnost přepsat na $45 = 5 \cdot 9$, $9 \in \mathbb{Z}$ a teď už můžeme psát $5 \,|\, 45$.

Symboly v definici mohou zastupovat celá čísla v libovolné formě, třeba i výrazy. Například je-li $a \in \mathbb{Z}$, pak jsou i výrazy $6a^4$ a $2a^3$ celá čísla. Můžeme aplikovat definici dělitelnosti a z informace $6a^4 = (2a^3) \cdot (3a)$, $3a \in \mathbb{Z}$ máme právo přejít ke tvrzení $(2a^3) \,|\, (6a^4)$.

Vztah samozřejmě funguje i při přechodu v opačném směru. Pokud máme odněkud informaci, že jedno číslo dělí jiné, pak z nich můžeme sestavit rovnost správného tvaru.

Tato poznámka je obecná a vztahuje se na všechny definice i tvrzení v matematice. Není dobré učit se vzorce nazpaměť jako doslovnou sekvenci písmen. Podstatné je podívat se, jakou strukturu pro přesouvání informace písmena vytvářejí.

△

→ Poznámka pro fajnšmekry: Podmínka z definice má jednoznačně rozhodnout, zda pro jistá dvě čísla dělitelnost máme nebo ne. To znamená, že bychom měli v definici použít ekvivalenci, formálně zapsáno

$$a \,|\, b \iff (\exists k \in \mathbb{Z}\colon b = a \cdot k).$$

Jenže v definici vidíme spojku „jestliže“, takže je tam vlastně implikace

$$(\exists k \in \mathbb{Z}\colon b = a \cdot k) \implies a \,|\, b.$$

To ovšem umí dělitelnost jen potvrdit, nikoliv vyvrátit. Ta definice je tedy chybně formulována! Nejen to, všechny definice v české literatuře jsou dělány takto, stejně jako v dalších světových jazycích. Matematici to tak dělají už pár set let a prostě vědí, že se v definicích sice říká „jestliže“, ale myslí se tím „tehdy a jen tehdy“. Teď už to víte taky. Člověk by to od matematiků, kteří mají být přesní a korektní, nečekal, ale i oni jsou jen ← lidé.

Dělitelnost je užitečný pojem. Svědčí to tom například fakt, že pro některá populární čísla a existují testy, jak snadno poznat, která čísla jsou tímto a dělitelná. Oblíbené je třeba kritérium pro dělitelnost desíti (číslo končí nulou). Některá připomeneme ve cvičení 1a.13, hlouběji se do tohoto tématu ponoříme s vhodnějšími nástroji v následující kapitole, jmenovitě v poznámce 2a.14 a cvičení 2a.13. Máme také populární název pro celá čísla dělitelná dvěma (sudá) a ta, která dělitelná dvěma nejsou (lichá).

Dělitelnost se také často používá při práci s polynomy, kde funguje obdobně. Lze třeba říct, že polynom $x - 1$ dělí polynom $x^2 - 1$, protože $x^2 - 1 = (x - 1)(x + 1)$. Zde $x + 1$ hraje roli k. Více viz kapitola 17.

Když matematici vymyslí nějaký pojem, tak se o něm snaží zjistit, jaké má vlastnosti a jak funguje. Své výsledky pak sdělují pomocí takzvaných tvrzení, která se ale mohou jmenovat různě. Když jde o něco snadného, můžeme tomu říkat Fakt.

Fakt 1a.2.
Pro každé $a \in \mathbb{Z}$ platí:
(i) a dělí a;
(ii) 1 dělí a;
(iii) a dělí 0.

Přeloženo do lidštiny, tvrdí se tady, že každé celé číslo dělí sebe sama, že číslo 1 dělí libovolné celé číslo, a že každé celé číslo dělí nulu neboli nula je násobkem libovolného čísla. Dalo by se říci, že jednička je univerzální dělitel a nula univerzální násobek.

M **Poznámka:** Máme zde naše první matematické tvrzení. I ono začíná preambulí, kde se dozvíme, s čím budeme pracovat, v tomto případě s nějakým celým číslem zvaným a. Zde se přímo řeklo, že se naše tvrzení vztahuje na všechna celá čísla, tedy formálně je tam vysloveno prokaždítko. Místo toho se dalo napsat „Nechť $a \in \mathbb{Z}$." a matematici by tomu rozuměli stejně.

Pak se o tom a coby zástupci všech celých čísel něco dozvíme. Zde se autor rozhodl, že v rámci jednoho Faktu řekne těch novinek víc, což se někdy dělá. Pak je tradicí tato jednotlivá tvrzení číslovat pomocí malých římských čísel v závorce.

Spolehlivost matematiky je založena nejen na jednoznačnosti pojmů (my už umíme zcela jednoznačně a spolehlivě rozhodnout, jestli jistá čísla mají nebo nemají mezi sebou vztah dělitelnosti), ale také na tom, že všechna tvrzení jsou dokázaná. Důkaz je slohový útvar, ve kterém čtenáři ukážeme, jak naše tvrzení vyplývá přesně kontrolovatelným (a tedy spolehlivým) postupem z něčeho, co už je známo. Pro účely této knihy budeme za známé považovat zhruba to, co se v matematice probere během prvních deseti let školní docházky.

Abychom mohli postup od známého k novému ověřit, musí být založen na pravidlech logiky, aritmetiky a dalších již ověřených matematických manipulacích. Naštěstí budeme používat praktickou logiku, která je vlastně formalizací selského rozumu, takže nebude třeba rozsáhlého studia oboru logika, stačí základy například na úrovni Dodatku 1.

Nejprve si rozebereme, jak by měl takový důkaz vypadat, jak se na něj dá přijít a posléze jej napsat.
△

M **1a.3 Poznámka:** Aby byl důkaz čitelný, je dobré zachovávat následující strukturu: Nejprve čtenáři řekneme, s jakými objekty budeme pracovat. Poté provedeme nějakou práci a pak shrneme, k čemu jsme se dostali.

Budeme dokazovat tvrzení (i), které lze formálně napsat například takto:

$$\forall a \in \mathbb{Z}\colon a \mid a.$$

Něco tady tvrdíme o **všech** celých číslech. Jak dokážeme, že máme pravdu? Určitě ne tak, že to vyzkoušíme na několika konkrétních číslech. Mohli jsme totiž mít štěstí a trefit se do těch, pro které tvrzení náhodou platí. Je pravda, že pokud bychom něco dokazovali pro objekty z konečné (a malé) množiny, tak by je šlo probrat jeden po druhém a pro každý ukázat, že pro něj dotyčná věc platí. To se ale vyskytne velmi zřídka, obvykle dokazujeme tvrzení pro objekty z velkých množin, například nekonečných (to nás čeká v této knize).

Jak tedy ověříme, že něco platí pro prvky velké množiny? Dělá se to metodou anonymního zástupce. Někdo nám vybere mezi kandidáty jednoho (v našem případě nějaké celé číslo), ale neřekne nám, který přesně to je. Dá nám ho v neprůhledné krabičce. My pak s tímto anonymním zástupcem zkusíme udělat to, co je třeba. Protože nevíme, jaké konkrétní číslo máme, jsme nuceni se omezit pouze na ty postupy, jejichž správnost máme potvrzenu pro všechna celá čísla (obecněji pro všechny kandidáty, pro které se něco dokazuje), takže nemůže dojít k tomu, že bychom si šťastnou volbou zástupce usnadnili práci. Pokud se nám tedy s tím anonymním zástupcem něco povede udělat, tak se to logicky musí povést s libovolným členem dotyčné skupiny (v našem případě s libovolným celým číslem), takže jsme prostřednictvím práce s anonymním zástupcem vlastně něco udělali pro všechny takové objekty.

Shrnuto, pokud dokazujeme něco pro všechny členy množiny M, tedy pokud námi dokazované tvrzení začíná „$\forall x \in M$", tak důkaz začneme volnou (vybírá někdo jiný) nám neznámého zástupce. Tradiční první věta důkazu pak vypadá například takto: „Nechť $x \in M$ je libovolné". Lze to vyjádřit i jinak, populární jsou „Dáno $x \in M$ libovolné" či „Mějme $x \in M$ libovolné". Podstatný je smysl: práce s anonymním zástupcem.

Pak následuje argument, pomocí kterého se od známého dostaneme k tomu, co chceme. V následující poznámce si rozmyslíme, jak správně odůvodnit, že $a \mid a$.

Kromě tvrzení univerzálních uvozených „prokaždítkem" $\forall$ jsou také výroky existenční uvedené „existítkem" $\exists$. Například pro potvrzení, že $a \mid a$, máme podle definice ukázat pravdivost výroku $\exists k \in \mathbb{Z}\colon a = a \cdot k$.

My už jsme se s existenčním důkazem setkali, když jsme potvrzovali, že $3 \mid 12$: dokazovali jsme tam tvrzení $\exists k \in \mathbb{Z}\colon 12 = 3k$. Jak jsme to udělali? Našli jsme $k = 4$. Toto je nejoblíbenější způsob, jak dokazovat existenci. Ne

vždy je takto snadné najít vhodný objekt, ale pokud se to povede, máme vyhráno. Obvykle tento objekt vytváříme pomocí nějakého výpočtu, což se často uvozuje slovem „zvolme“ či „označme“.

Shrneme si to:

Pravidlo pro práci s prvky: Pokud při dokazování reagujeme na text $\forall x \in M$, tak nám to x dá někdo jiný a my ukážeme, že tento anonymní zástupce splňuje žádané. Pokud reagujeme na text „$\exists x \in M$“, tak je na nás najít (vytvořit, zvolit) nějaké konkrétní x a ukázat, že opravdu dělá to, co se od něj chce.

△

S **Rozbor:** Nyní už víme, že důkaz faktu, části (i) začneme tím, že si vezmeme libovolné $a \in \mathbb{Z}$ coby reprezentanta všech celých čísel. Potřebujeme pak ukázat, že toto a dělí samo sebe. Cílem důkazu je dojít k novému poznatku pomocí toho, co už známe, ale v této chvíli není jasné, odkud vlastně začít. Obvykle velmi pomůže, pokud se nejprve zamyslíme nad tím, kam chceme dojít.

Náš konečný cíl je ověřit, že $a \mid a$. To nám zatím moc nepomohlo, tak se zeptejme, co by tomuto závěru mělo předcházet. Co bychom měli čtenáři říct, aby pak už akceptoval, že $a \mid a$? Odpověď najdeme v definici. Máme ukázat, že dokážeme vytvořit rovnost vhodné formy, v tomto případě $a = a \cdot k$, přičemž to k musí být celé. Nás přitom konkrétní hodnota k vlastně nezajímá, podstatné je, že musí existovat. Potřebujeme tedy ukázat pravdivost existenčního tvrzení. Svůj nezájem o konkrétní podobu k můžeme ještě zdůraznit tím, že namísto písmene pro tuto komponentu rovnosti použijeme obrázek. Tím jsme získali náhradní cíl a ze situace „Chceme: $a \mid a$“ jsme se tedy posunuli do situace, kterou lze symbolicky zachytit třeba takto:

• Chceme:

$\exists \diamondsuit \in \mathbb{Z}\colon a = a \cdot \diamondsuit \qquad \longrightarrow \qquad a \mid a.$

Dá se říci, že takto důkaz vytváříme od konce.

Shodou okolností jsme si před chvílí rozmysleli, že důkaz existenčního tvrzení se nejlépe dělá předvedením doličného předmětu. Položíme si tedy klíčovou otázku: Jsme schopni takové k či $\diamondsuit$ najít? Ano, protože platí $a = a \cdot 1$. Tím máme vymyšlený důkaz, ale ještě jej musíme napsat. Správný důkaz začne s něčím, co je známé, a dovede nás k tomu, co chceme. My víme, co chceme (že $a \mid a$), a zjistili jsme, že se k tomu dostaneme od rovnosti $a = a \cdot 1$, která je považována za známou a je to tedy legitimní začátek argumentu. Máme už dobrou představu, jak důkaz směřovat.

Mimochodem, pokud bychom neviděli, jak náš náhradní cíl splnit, tak bychom se mohli zkusit podívat na krok, který by nás k tomuto náhradnímu cíli mohl dovést, takže bychom vlastně přidali předpředposlední etapu vznikajícího důkazu. Je důležité vědět, že takto jdeme pozpátku, takže pokud bychom naši úvahu zapsali v pořadí, v jakém vzniká, například

$a \mid a \qquad \longrightarrow \qquad \exists k \in \mathbb{Z}\colon a = ak \qquad \longrightarrow \qquad a = a \cdot 1,$

tak tím nezískáme platný důkaz, protože to jde špatným směrem (začíná cílem). Je to jen nápověda, jaké kroky pak napsat ve správném směru, aby důkaz vznikl. Proto si tyto úvahy děláme někde bokem a teprve pak napíšeme důkaz samotný.

Důkaz: (i): Dáno $a \in \mathbb{Z}$ libovolné. Víme, že $a = a \cdot 1$. Označíme-li $k = 1$, dostáváme $a = a \cdot k$ a $k \in \mathbb{Z}$, tedy podle definice dělitelnosti $a \mid a$.

Důkazy (ii) a (iii) jsou obdobné a tak snadné, že je s důvěrou necháme jako cvičení 1a.2.

□

To k není nutné zavádět, mohli bychom argumentovat takto: Platí $a = a \cdot 1$ a $1 \in \mathbb{Z}$, tedy $a \mid a$.

1a.4 Poznámka: Ta zmínka o $1 \in \mathbb{Z}$ vypadá směšně, ale je podstatná. Pro platnost vztahu dělitelnosti je třeba mít podle definice splněny dvě podmínky: vzoreček vhodného typu a v něm na klíčovém místě celé číslo. Obojí tedy musíme čtenáři předložit, abychom byli oprávněni dojít k dělitelnosti. Má to i smysl pedagogický, připomínáme tím čtenáři i sobě, že bychom tyto triviální ale klíčové podmínky neměli opomíjet, ale krátce se zamyslet, jak víme, že jsou splněny.

△

S **1a.5 Poznámka:** Vraťme se ještě k důkazu části (i). Rozmysleli jsme si, že vlastně potřebujeme dokázat toto formální tvrzení:

$$\forall a \in \mathbb{Z}\ \exists k \in \mathbb{Z}\colon a = ak.$$

Náš důkaz (bez konečného závěru) by se dal zapsat takto:

Dáno $\underline{a \in \mathbb{Z} \text{ lib.}}$ $\underline{\text{Zvolme}}$ $k = 1$. Pak $\underline{k \in \mathbb{Z}}$ a $\underline{a = ak}$.

Všimněte si, jak jednotlivé podtržené sekce důkazu odpovídají jednotlivým částem toho formálního tvrzení, zejména u kvantifikátorů reagujeme způsobem popsaným výše. To je známkou, že náš důkaz má správnou strukturu. Jak ještě opakovaně uvidíme, prakticky všechny (přímočaré) důkazy budou takto fungovat, čtení dokazovaného tvrzení zleva doprava vytýčí milníky našeho důkazu. To je významná nápověda pro toho, kdo se snaží

takové jednodušší důkazy vymýšlet. Existují výjimky z tohoto pravidla (specializované typy důkazů), ale ty teprve přijdou.

Co si má tedy hlídat začátečník, který se učí psát důkazy:

• Struktura důkazu musí odpovídat tomu, co se dokazuje. Je možno si strukturu sestavit předem a pak doplnit technické kroky.

• Argument vždy vede od známého k tomu, co chceme. Nesmíme používat jako nástroje věci, které teprve chceme dokázat.

△

S 1a.6 Poznámka o psaní důkazů:

V důkazech volíme úroveň vysvětlování podle předpokládané vyspělosti čtenáře a kontextu. Například poznámku, že poslední krok děláme podle definice, bychom obvykle vynechali. V méně formálním kontextu (například když na konci sekce píšeme řešení dokazovacích cvičení) mnohdy vynecháme prakticky vše kromě samotné matematičtiny. Extrémní podoba by mohla vypadat takto:

$a \in \mathbb{Z}$ lib.;
$a = a \cdot 1$, $1 \in \mathbb{Z}$
$a \,|\, a$.

Interpretace takového textu je založena na dvou konvencích. Pokud se na začátku textu objeví nějaká informace, tak se to bere tak, že autor textu se odkazuje na něco obecně platného. Zde se odkazujeme na to, že $a = a \cdot 1$.

Pokud nějaký řádek následuje předchozí s nějakým faktem, tak se to chápe tak, že z toho předchozího vyplývá. Tuto konvenci již čtenář zná ze situace, kdy dostane rovnici a postupně ji upravuje. Zde tedy vidíme jeden uvozovací krok, kdy z algebry a informace o jedničce pomocí definice přecházíme k závěru.

Z hlediska čitelnosti bývá dobré tyto uvozovací kroky nějak vyznačit, například slovy „Pak“, „Odtud“, „Proto“, „Tudíž“ a podobně. V méně formálním kontextu je možné použít uvozovací značku, což je v českém kontextu trochu problém, protože není nějaká obecně uznávaná. Formální logika používá uvozovací symboly $\vdash$ a $\models$, které by se pro uvozování v důkazu hodily, ale nejsou mimo tento obor příliš používané a tudíž by pro běžné čtenáře nebyly srozumitelné. Rozhodně není dobré použít symbol $\Longrightarrow$, protože značí logickou implikaci a ta je něco velmi odlišného od „z toho vlevo vyplývá to vpravo“, například už proto, že implikace nelze řetězit, zatímco v důkazech se uvozování řetězí běžně. Osobně nemám problém akceptovat standardní anglosaský symbol $\therefore$, jehož význam je „z toho předtím vyplývá to potom“, ale asi nejčastěji (například ve stručných řešeních) používám vcelku srozumitelný symbol $\longrightarrow$.

Čitelnější verze tohoto důkazu by tedy mohla vypadat takto:

$a \in \mathbb{Z}$ lib. $a = a \cdot 1 \wedge 1 \in \mathbb{Z} \quad \longrightarrow \quad a \,|\, a$.

Pokud by mi toto napsal student do písemky, bral bych to, ale čtenář ocení občasné hřejivé lidské slovo, navíc ten symbol šipky přeci jen není kodifikován, takže bych spíše doporučil verzi

$a \in \mathbb{Z}$ lib. Platí $a = a \cdot 1 \wedge 1 \in \mathbb{Z}$, proto $a \,|\, a$.

Stručná verze svádí k logické chybě. Začátečníci mají sklon napsat toto:

$a \in \mathbb{Z}$ lib. $a \,|\, a \quad \longrightarrow \quad a = a \cdot 1 \wedge 1 \in \mathbb{Z}$.

Tento důkaz je špatně, protože začíná tím, co chceme dokázat, a pak jde k něčemu, co dávno víme. Vzniká nešikovným zápisem běžného lidského zvyku něco říct a pak to dovysvětlit: a dělí a, protože platí … To by se ale symbolicky zapsalo

$$a \,|\, a \quad \longleftarrow \quad a = a \cdot 1 \wedge 1 \in \mathbb{Z}$$

a v logice zpětný chod nefunguje, argument má plynout od známého začátku k novému konci zleva doprava.

△

Možná jste si všimli, že se ve faktu nijak neomezujeme a připouštíme všechna celá čísla. To znamená, že tvrzení (i) a (iii) lze aplikovat i na $a = 0$. Dostáváme tak $0 \,|\, 0$. Nepřehlédli jsme nějakou výjimku v důkazu?

Tvrzení, že 0 dělí 0, se podle definice testuje splněním rovnosti $0 = 0 \cdot k$, což snadno zajistíme například volbou $k = 13 \in \mathbb{Z}$. Takže podle definice to je správně a důkaz nic nepřehlédl. Nabízí se otázka, jestli jsme tedy tu definici neudělali omylem jinak, než jsme zamýšleli. Zkušenost ukazuje, že je udělaná rozumně a nulu je třeba zahrnout, tak se s tím prostě smíříme. Ostatně definice krome slova dělitel nabízí i slovo násobek. Tvrzení „nula je násobkem nuly“ zní přijatelně.

To nás přivádí k podstatné poznámce. Existuje dělení a existuje dělitelnost a formálně jsou to velmi rozdílné věci. Dělení je operace, která má výsledek a ten nás zajímá. Dělitelnost čísla číslem je naopak vztah a může platit či neplatit. Hodnota toho k nás vůbec nezajímá, jen při potvrzování dělitelnosti potřebujeme vědět, jestli existuje. Právě nula ten rozdíl ilustruje velmi pěkně. Spočítat nula děleno nulou nelze (operace), ale jak jsme právě viděli, nula dělí nulu (vztah).

Na druhou stranu čtenář asi cítí, že pojem dělitelnosti má něco společného s dělením. Například tu konstantu $k = 4$ v příkladě $3 \mid 12$ jsme mohli uhodnout, ale asi jsme spíš jen vydělili $\frac{12}{3}$. Tato podobnost svádí k tomu, abychom vztah, že a dělí b, v praxi nahrazovali podmínkou, že $\frac{b}{a}$ je celé číslo. Není to ale totéž.

Výmluvně to ukazuje právě možnost, že by a mohlo být nula. Pak dělitelnost přes rovnost funguje, ale ten podíl ne. Už to by mělo stačit k tomu, abychom se při práci s dělitelností vyhýbali dělení. Je tu ale i aspekt praktický. Pro nenulová čísla sice lze najít pojítko mezi dělitelností a celočíselným podílem, ale zatímco pro práci s rovnostmi existuje řada nástrojů, s tvrzením „podíl je v $\mathbb{Z}$“ se pracuje významně hůře.

Proto čtenáři doporučujeme, aby při práci s dělitelností a zejména při psaní důkazů s dělením nepracoval. I my se mu zde budeme (až na pár nutných výjimek) vyhýbat.

M Poznámka: Jedna ze silných stránek matematičtiny je schopnost zachytit pravidelnosti, vzory či pravidla. Při přemýšlení o dělitelnosti si například všimneme, že $3 \mid 3^2$, $5 \mid 5^2$, $(-7) \mid (-7)^2$ a podobně. Matematicky to vyjádříme tvrzením $a \mid a^2$. Ale lze také tvrdit $a \mid a^n$ pro $n \in \mathbb{N}$. O tomto tvrzení by matematici řekli, že je **obecnější**, protože zahrnuje předchozí případ (volbou $n = 2$) a ještě přidá informaci navíc. Naopak $a \mid a^2$ by se označilo za speciální případ toho obecnějšího vzorce.

Ale ani tvrzení $a \mid a^n$ není nejlepší možné, dá se dále zobecnit.
△

Fakt 1a.7.
Nechť $a \in \mathbb{Z}$, $m, n \in \mathbb{N}$ a $m \leq n$. Pak $a^m \mid a^n$.

S Rozbor: V tomto tvrzení se objevuje „nechť“ coby indikátor kvantifikátoru $\forall$. Tvrzení se tedy vztahuje na všechna celá čísla a a všechny dvojice $m \leq n$ přirozených čísel. Pro ně máme dokázat tvrzení o dělitelnosti. Poučeni předchozím důkazem si tento cíl nahradíme cílem náhradním z definice: Potřebujeme rovnost ve tvaru

$$a^n = a^m \cdot \diamondsuit \text{ pro nějaké } \diamondsuit \in \mathbb{Z}.$$

Snadno ji vyrobíme pomocí identity pro mocniny, což coby známý fakt bude vhodným východiskem pro důkaz.
△

Důkaz (rutinní, poučný)**:** Dány $a \in \mathbb{Z}$ a $m, n \in \mathbb{N}$ splňující $m \leq n$.

Víme, že $a^n = a^m a^{n-m}$. Označme $k = a^{n-m}$. Pak díky $m, n \in \mathbb{N}$ a $m \leq n$ je $n - m$ celé nezáporné číslo a tedy $k = a^{n-m} \in \mathbb{Z}$ a také $a^n = a^n \cdot k$. Proto podle definice dělitelnosti $a^m \mid a^n$.

□

I tento důkaz byl povídavější, než by bylo pro zkušenějšího čtenáře třeba, například u posledního kroku by si domyslel, že jsme použili definici dělitelnosti. Jesliže jsme u odvozovacích spojek typu „proto“ jen doporučovali, aby čtenář ve svých důkazech čtenáře občas potěšil, tak to slovo „označme“ doporučujeme silně. Kdyby tam chybělo, tak by se čtenář divil, kde se to m vzalo. Vyplývá snad z nějakého matematického poznatku? My ovšem čtenáři vyjasníme situaci, když napíšeme „Označme $m = a^{n-m}$“. Tím mu říkáme, že jsme se sami o své vůli rozhodli vzít číslo a^{n-m} a pojmenovat jej m, například proto, že chceme (potřebujeme) dokázat existenci takového čísla.

Je ovšem možné se tomu m zcela vyhnout. Klíčovým krokem důkazu je ukázat existenci jistého čísla, které jsme značili m nebo třeba $\diamondsuit$. Jestliže na značení nezáleží, proč by se nemohlo jmenovat a^{n-m}? Ušetříme si tak práci. Následující stručná verze důkazu je postačující a srozumitelná:

Důkaz: Dány $a \in \mathbb{Z}$ a $m, n \in \mathbb{N}$ splňující $m \leq n$.

Pak je $n - m$ nezáporné celé číslo, takže $a^{n-m} \in \mathbb{Z}$ a také $a^n = a^m a^{n-m}$. Proto $a^m \mid a^n$.

□

Někteří lidé si název pro a^{n-m} zavádějí, protože jim to pomáhá při přemýšlení nad důkazem, popřípadě chtějí potěšit čtenáře, jiným to přijde zbytečné. Obojí je v pořádku.

S 1a.8 Poznámka: Uvažujme následující verzi důkazu.

Dány $a \in \mathbb{Z}$ a $m, n \in \mathbb{N}$ splňující $m \leq n$. Platí $a^n = a^m a^{n-m}$, proto $a^m \mid a^n$.

Tento důkaz není dobře, ačkoliv jsme v něm nenapsali nic nesprávného. Jeho chybnost spočívá v tom, že v něm chybí něco podstatného. Zapomněli jsme v něm ověřit, že $a^{n-m} \in \mathbb{Z}$. Podezření vzbuzuje už to, že se v tomto pokusu o důkaz nikde nevyužila informace $m \leq n$. O tom, že není správně, nás jednoznačně přesvědčí fakt, že tak jak je napsán jej lze aplikovat i na neplatnou situaci. Podle tohoto textu by totiž platilo $5^2 \mid 5$. Schválně:

Dány $5 \in \mathbb{Z}$ a $2, 1 \in \mathbb{N}$. Platí $5^1 = 5^2 5^{1-2}$, proto $5^2 \mid 5^1$.

Nesprávnému pokusu o důkaz to přesně vyhovuje.

Poučení tedy je, že správnost důkazu lze pokazit nejen chybou v jeho struktuře či logické návaznosti, ale i tím, že něco podstatného vynecháme.
△

M Naše první fakty nebyl zcela typické. Prostě se tam o libovolném čísle něco natvrdo řeklo. Ovšem většina matematických tvrzení spíše spojuje dva různé poznatky ve smyslu, že když máme jeden, tak automaticky máme i druhý. Tuto vazbu zachycuje logická spojka implikace. Je velmi důležité ji správně chápat, proto si připomene to nejdůležitější pomocí jednoduchého příkladu. Podrobnější informace se najdou v Dodatku 1.

Příklad 1a.b: Uvažujme následující tvrzení:

- Nechť $a \in \mathbb{Z}$. Jestliže je a dělitelné čtyřmi, pak je také dělitelné dvěma.

Spojky „Jestliže … pak“ jasně ukazují na implikaci. Lze se ale setkat i s jiným vyjádřením implikace, v našem případě například:

- Pro každé celé číslo a platí, že když čtyři dělí a, tak dvě dělí a.
- Pro všechna celá čísla platí, že když jsou dělitelná čtyřmi, pak jsou dělitelná i dvěma.
- Každé celé číslo, které je dělitelné čtyřmi, je také dělitelné dvěma.
- Celá čísla jsou dělitelná dvěma, pokud jsou dělitelná čtyřmi.
- Všechna celá čísla dělitelná čtyřmi jsou také dělitelná dvěma.

Formální zápis všech těchto vět vypadá takto:

$$\forall a \in \mathbb{Z}\colon (4 \,|\, a \implies 2 \,|\, a).$$

V méně formální situaci by se ta závorka kolem výroku mohla i vynechat.

Implikace spojuje dva samostatné výroky zvané předpoklad (zde $4 \mid a$) a závěr (zde $2 \mid a$). Mohli bychom ji symbolicky vyjádřit jako $P \implies Z$, popřípadě $P(a) \implies Z(a)$, pokud bychom chtěli zdůraznit, že předpoklad i závěr pracují s proměnnou a.

K čemu implikace slouží? Pokud víme, že je pravdivá, tak nám říká, že v situaci, kdy je splněn předpoklad, už musí automaticky být splněn i závěr. Pravdivá implikace tedy neříká nic o pravdivosti jednotlivých složek, jen o jejich vztahu. Podstatné je, že tento vztah není dokonalý. Můžeme si představit, že pokud implikaci $P(a) \implies Z(a)$ aplikujeme na prvky a z nějaké množiny M, tak se M rozdělí na dvě části podle platnosti $P(a)$.

V jedné části jsou ty a, pro které předpoklad $P(a)$ platí. O těch nám pravdivá implikace dá informaci, že také splňují závěr $Z(a)$. Tento přesun informace o pravdivosti z P na Z (zleva doprava) je hlavním účelem pravdivé implikace. V zásadě od ní nic víc ani neočekáváme, takže to, zda tento cíl plní, je vlastně ukazatelem, zda je naše implikace pravdivá. Získali jsme tak návod, jak implikace dokazovat: Ověříme, zda přenáší pravdivost z P na Z. Podrobně to probereme níže, zde tedy jen intuitivně na základě zkušenosti usoudíme, že čísla dělitelná čtyřmi jsou vždy sudá neboli dělitelná dvěma, takže naše ukázková implikace nejspíš bude pravdivá (a také je).

Z pohledu uživatele je důležité vědět nejen co pravdivá implikace dělá, ale také co neumí. Zatímco o těch prvcích z výchozí množiny M, které splňují předpoklad, nám něco řekne, tak o těch zbývajících nám neřekne nic ohledně závěru. Vyplývá to z definice implikace coby logické spojky: Je-li předpoklad nepravdivý, tak implikace jako celek je pravdivá bez ohledu na to, co se říká v závěru. A opravdu, pokud se u naší implikace podíváme na čísla, která nejsou dělitelná čtyřkou, tam mezi nimi najdeme sudá i lichá, takže se o jejich dělitelnosti dvěma nic nedozvíme.

Dá se tedy říct, že pravdivá implikace přesouvá zleva doprava pravdivost, ale neumí takto přesunout nepravdivost. Stejně tak neumí přesunout zprava doleva (v opačném směru) pravdivost. Opět to výmluvně ilustruje náš příklad. Pokud je číslo sudé, tak nic nevíme o jeho dělitelnosti čtyřmi. Značka $\implies$ je tedy výstižná. Podotkněme, že někdy se stane, že se pravdivost přenáší i v opačném směru (ze závěru na předpoklad). Pak vlastně máme jinou situaci, jde o logickou spojku ekvivalence značenou $\iff$, ke které se dostaneme časem.

Užitečnost pravdivé implikace je, že nám umožňuje dělat úvahy. Když zjistíme, že něco je pravda (předpoklad P), tak díky vhodné pravdivé implikaci usoudíme, že je pravda i něco dalšího (závěr Z). To může pomoci v situaci, kdy nás zajímá pravdivost Z, ale není snadné to zjistit. Pravdivá implikace $P \implies Z$ nám umožní místo toho zkoumat P a v případě úspěchu (platí) už máme informaci o Z. Jinak řečeno, pravdivost P je postačující pro pravdivost Z. Z toho vyplývá další alternativní slovní vyjádření **pravdivé** implikace:

- Nechť $a \in \mathbb{Z}$. Vlastnost $4 \,|\, a$ je postačující podmínka pro $2 \,|\, a$.

Pravdivá implikace nám také může posloužit jako filtr. Řekněme, že hledáme čísla dělitelná čtyřkou. Podle naší implikace musí být dělitelná i dvěma, což znamená, že je zbytečné hledat mezi lichými. Obecně, pokud hledáme objekty s vlastností P a máme nějakou pravdivou implikaci $P \implies Z$, tak stačí hledat jen mezi objekty splňujícími Z. V takové situaci je pak splněná vlastnost Z nutná pro to, aby mělo vůbec smysl zkoušet testovat P. To nám nabízí poslední alternativní způsob, jak vyjádřit **pravdivou** implikaci:

- Nechť $a \in \mathbb{Z}$. Dělitelnost a dvěma je nutná podmínka pro dělitelnost a čtyřmi.

Tím se dostáváme k poslednímu zajímavému pozorování. Pokud je platnost Z nutná pro to, aby měl předpoklad P šanci platit, tak při nesplnění Z nemůže P platit také. Jinak řečeno, u pravdivé implikace se nepravda přenáší v opačném směru, zprava doleva. Formálně se to dá zapsat následovně:

- $\forall a \in \mathbb{Z}$: $2 \,|\, a$ neplatí $\implies$ $4 \,|\, a$ neplatí.

Neboli symbolicky pomocí negace: $\neg Z \implies \neg P$. Tato nová implikace vyjadřuje přesně stejnou informaci jako ta původní $P \implies Z$, formálně řečeno má vždy stejnou pravdivostní hodnotu. Říká se jí obměna té původní implikace a ačkoliv jde z logického pohledu o totéž, ve slovním vyjádření mnohdy nabídne zajímavý vhled do zkoumané záležitosti.

Ukázali jsme si řadu způsobů, jak implikaci vyjádřit slovně. Jeden z nich (začíná slovy „Všechna celá…“) nás inspiruje k alternativnímu formálnímu vyjádření implikace. Nejprve si zavedeme pomocnou množinu M_P, která obsahuje všechna celá čísla, která jsou dělitelná číslem 4. Formálně: $M_P = \{a \in \mathbb{Z} : 4 \,|\, a\}$. Pomocí této množiny můžeme naši implikaci zapsat rovnocenně takto:

- $\forall a \in M_P$: $2 \,|\, a$.

Všimněte si, že tento výrok už není implikace. Podává ale stejnou informaci. Původní implikační forma se fakticky vyjadřovala jen k situaci, kdy a je dělitelné čtyřmi, o ostatních číslech nic neuměla říct. Tato nová forma dělá přesně totéž. Tento přechod mezi vyjádřením pomocí implikace a pomocí omezené množiny u kvantifikátoru se dá často dělat v obou směrech a podle kontextu může někdy být jeden či druhý výhodnější.

Tím jsme probrali to hlavní, co je třeba o implikacích vědět.

△

M **1a.9 Poznámka:** Shrňme si pravidla pro práci s implikacemi, které jsme si představili v příkladě výše.

Každá implikace $P \implies Z$ má **obměnu** $\neg Z \implies \neg P$, která má stejnou pravdivostní hodnotu a tedy dává stejnou informaci.

Pravdivost implikace $P \implies Z$ lze také vyjádřit slovy „P je postačující podmínka pro Z“ nebo „Z je nutná pdmínka pro P“.

Uvažujme nějakou množinu M a výroky $P(a)$, $Z(a)$, které mají pro prvky množiny M smysl. Uvažujme tvrzení

$$\forall a \in M\colon P(a) \implies Z(a).$$

Toto tvrzení se dá rovnocenně přepsat následovně:

$$\forall a \in \{a \in M : P(a)\}\colon Z(a).$$

Abychom dokázali pravdivost implikace na nějaké množině M, musíme ukázat, že pro všechna $a \in M$ splňující $P(a)$ musí také platit závěr $Z(a)$. Formálně tedy důkaz vypadá následovně:

Po vybrání anonymního zástupce (či zástupců) objektů, se kterými budeme pracovat, omezíme svou pozornost pouze na ty z nich, které splňují předpoklad. Vyjádříme to slovy „Předpokládejme, že…“. Tím zároveň získáme výchozí bod pro naši práci neboli fakta, pomocí kterých budeme chtít ukázat, že v námi zkoumané situaci platí rovněž závěr. Za tím účelem se z našich výchozích faktů (a možná pomocí dalších již známých poznatků) k tomuto závěru dostaneme korektními kroky.

Dá se říci, že při důkazu potřebujeme čtenáře dovést od faktu (faktů) vypsaných v předpokladu k faktu (faktům) vypsaným v závěru, a to tak malými kroky, aby bylo možné ověřit jejich správnost. Symbolicky (a s povolením využití dalších známých věcí značených f):

$$P \longrightarrow \xrightarrow{f} \cdots \longrightarrow\longrightarrow Z$$

Z praktického pohledu na začátku důkazu máme nějaké znalosti, především to, co jsme předpokládali, a možná další již známé matematické poznatky. Zároveň je dán cíl, to je ten závěr implikace. My potřebujeme pomocí toho, co máme, dojít k tomu, co chceme. Tomuto způsobu dokazování implikace se říká **přímý důkaz** a je to v zásadě univerzální způsob, jak implikace dokazovat.

Někdy potkáme tvrzení, o kterém rozpoznáme, že pravdivé není. I tuto nepravdivost je nutno dokázat: Říkáme, že tvrzení vyvracíme. Pokud tvrzení začíná „prokaždítkem“, tak selský rozum říká, že k vyvracení stačí najít konkrétní situaci, kdy tvrzení neplatí. Je to tak, té situaci se říká **protipříklad**.

Je například zjevné, že tvrzení $\forall a \in \mathbb{Z}$: $13 \,|\, a$ neplatí. Abychom jej vyvrátili, stačí napsat:

Důkaz neplatnosti: protipříklad $a = 1$.

Protože třináctka nedělí jedničku, tvrzení pro toto $a \in \mathbb{Z}$ neplatí a je vyvrácené.

Co když chceme vyvracet implikaci $P(a) \implies Z(a)$? Potřebujeme najít protipříklad, tedy prvek a, pro který tato implikace neplatí. Hledáme tedy prvek, pro který se pravdivost nepřenáší z P do Z. Náš protipříklad proto musí splňovat předpoklad a nesplňovat závěr. Například $a = 5$ coby protipříklad vyvrací implikaci, že jestliže je celé číslo dělitelné pěti, tak je dělitelné desíti.

△

Zopakovali jsme si vlastnosti implikace a jsme připraveni formulovat pravidla, která platí pro dělitelnost a mohou nám usnadnit práci s ní. Začneme něčím snadným.

Fakt 1a.10.
Nechť $a, b \in \mathbb{Z}$. Jestliže $a \,|\, b$, pak $a \,|\, b^2$.

Ve cvičení 1a.3 uvidíme, že z předpokladu $a \,|\, b$ se dá dokonce ukázat $a \,|\, b^n$ a $a^n \,|\, b^n$, ale pro začátek jsme zvolili jednoduchou verzi. Rozmyslíme si, jak bude vypadat důkaz.

S Rozbor: Víme už, že to úvodní „nechť“ zahrnuje univerzální kvantifikátor, takže má jít o obecné tvrzení platné pro všechna celá čísla a, b. Důkaz tedy začne náhodnou volbou anonymního zástupce, máme celá čísla a, b. Pro ně potřebujeme dokázat tvrzení, které má formu implikace, formálně $a \,|\, b \implies a \,|\, b^2$.

Jak jsme si rozmysleli výše, důkaz implikace spočívá v tom, že čtenáře dovedeme od předpokladu k závěru. Ten začátek musíme sdělit, takže důkaz začne například takto:

Dáno $a, b \in \mathbb{Z}$. Předpoklad: $a \,|\, b$.

Tyto věci tedy máme k dispozici, pomocí nich chceme dokázat platnost závěru. Výchozí situace je proto následující:

- Máme: a dělí b
- Chceme: a dělí b^2

Vidíme, jak se dostat od toho, co máme, k tomu, co chceme? Nejspíše ne, tak se v kolonce „chceme“ podíváme na ideální předchozí krok. Podobně jako v prvních důkazech nám definice poradí, odkud se k našemu cíli dostat.

- Máme: a dělí b
- Chceme: a dělí b^2
  $\uparrow$
  $b^2 = a \cdot \diamondsuit$ pro nějaké $\diamondsuit \in \mathbb{Z}$.

Asi ještě pořád nevidíme, jak se od toho, co máme, dostat k tomu, co nově chceme, což je teď dáno tím, že napravo máme nějakou algebru (rovnost) a nalevo ne, neboli kolonky „máme“ a „chceme“ nemluví stejným jazykem. To ale snadno napravíme, i náš předpoklad si můžeme podle definice přepsat na rovnost, která bude stále v kategorii „máme“.

- Máme: a dělí b
  $\downarrow$
  $b = a \cdot k$, kde $k \in \mathbb{Z}$
- Chceme: a dělí b^2
  $\uparrow$
  $b^2 = a \cdot \diamondsuit$ pro nějaké $\diamondsuit \in \mathbb{Z}$

Pokud by čtenáře iritoval ten obrázek napravo a chtěl by raději písmenko, tak samozřejmě může. Podstatné ovšem je, že nesmí zkopírovat to k z definice. Důvod je, že už jsme k jednou použili při přepisu předpokladu. Tím se mu přiřadila nějaká konkrétní hodnota (pro $a \neq 0$ by šlo o poměr mezi b a a). My tuto hodnotu neznáme, ale k už ji má a tudíž nemůže zároveň sloužit jako konstanta pro přechod mezi a a b^2. Poměr mezi b^2 a a může být jiný než poměr mezi b a a a my musíme umožnit, aby se tak opravdu stalo. Uděláme to tak, že použijeme jiné písmeno, tím dáme vzorečku napravo potřebnou svobodu. Naštěstí s tím není problém, protože už víme, že k je v definici jen zástupný symbol, který lze nahradit jiným.

Pro úplnost podotkněme, že kdybychom omylem napsali

- Máme: a dělí b
  $\downarrow$
  $b = a \cdot k$, kde $k \in \mathbb{Z}$
- Chceme: a dělí b^2
  $\uparrow$
  $b^2 = a \cdot k$ pro $k \in \mathbb{Z}$ (chyba!)

tak máme po důkazu, protože od vzorce $b = ak$ se ke vzorci $b^2 = ak$ dostat nelze. Problém by nebyl s platností tvrzení, ale s naší nešikovností. My ovšem nešikovní nejsme a víme, že máme použít jiné písmeno, například takto:

- Máme: a dělí b
  $\downarrow$
  $b = a \cdot k$, kde $k \in \mathbb{Z}$
- Chceme: a dělí b^2
  $\uparrow$
  $b^2 = a \cdot m$ pro $m \in \mathbb{Z}$

Umíme se pomocí vzorce nalevo dostat ke vzorci, který by měl strukturu toho napravo? Zkušenější čtenáři už vidí, že odpověď zní ano. Tím je hotov plán důkazu. Aby začal tím, co máme, a skončil tím, co chceme, tak začne v kolonce „máme“ nahoře, pojede dolů, pak přeskočí na poslední řádek kolonky „chceme“ a dojede do cíle nahoru. Musíme to ale celé napsat, protože kolonku „chceme“ si píšeme bokem, čtenář ji nevidí.

Důkaz (rutinní, poučný)**:** Dány $a, b \in \mathbb{Z}$ libovolné. Předpokládejme, že platí $a \,|\, b$. Z předpokladu $a \,|\, b$ víme, že $b = ak$ pro nějaké $k \in \mathbb{Z}$. Když tuto rovnost vynásobíme číslem b (povolená operace), dostaneme rovněž platnou rovnost $b^2 = bak$. To lze upravit jako $b^2 = a(kb)$. Když označíme $m = kb$, tak díky $k, b \in \mathbb{Z}$ platí i $m \in \mathbb{Z}$ a také $b^2 = am$, proto platí $a \,|\, b^2$.

Alternativa: … Když tuto rovnost umocníme na druhou (povolená operace), dostaneme rovněž platnou rovnost $b^2 = (ak)^2$. To lze upravit jako $b^2 = a(ak^2)$. Když označíme $m = ak^2$, tak díky $k, a \in \mathbb{Z}$ platí i $m \in \mathbb{Z}$ a také $b^2 = am$, proto …

□

V tomto důkazu jsme klíčovou konstantu nazvali jménem, abychom potěšili čtenáře, ale hlavně proto, že se ukázalo, že je pro ni více možností. Někdy se stane, že se z výchozích dat k cílové rovnosti dá dostat více způsoby. Vlastně tedy není jedna konkrétní cílová rovnost, do které je potřeba se trefit, podstatné jsou jen povinné části (b^2 nalevo, součin s členem a napravo), ale je určitá volnost v místě, kde jsme si obrázkem naznačili, že tam může být libovolné celé číslo. Právě proto není dobré se upínat na nějakou konkrétní podobu, je dobré nemít předem nějaká očekávání.

S 1a.11 Poznámka: V poznámce 1a.6 jsme diskutovali důkazy z logického i slohového pohledu. Obojí se vztahuje i na důkazy implikace.

Náš důkaz obsahuje výchozí informaci a následují odvozovací kroky. Již jsme doporučili, aby je pisatel čtenáři vhodným způsobem indikoval. Pak už nemusíme každý odvozovací krok psát na samostatný řádek, což ušetří místo. Nicméně z hlediska přehlednosti je dobré alespoň významné kroky udělat na novém řádku.

Je také dobré čtenáře upozornit, jakým trikem jsme z jedné etapy přešli do druhé. Zde zase záleží na vyspělosti čtenáře, možná by sám pochopil, že jsme rovnost vynásobili číslem b, ale raději to alespoň naznačíme. Velmi stručná verze by tedy mohla vypadat například takto:

$a, b \in \mathbb{Z}$ lib. Předp.: $a \mid b$.

$\longrightarrow \quad b = ak,\ k \in \mathbb{Z} \quad \xrightarrow{\cdot b} \quad b^2 = bak \quad \longrightarrow \quad b^2 = a(kb).$

Ozn. $m = kb \quad \longrightarrow \quad b^2 = am,\ m \in \mathbb{Z} \quad \longrightarrow \quad a \mid b^2.$

Všimněte si, že i přes extrémní stručnost některá slova zůstala. Slovo „předpoklad“ je klíčové, protože mění logický význam důkazu. Pokud by náš důkaz začínal slovy

$a, b \in \mathbb{Z}$ lib.; $a \mid b$,

tak by to vypadalo, že tvrdíme následující: Kdykoliv nám dá někdo dvě celá čísla, tak vždy to první dělí druhé. To ovšem říct nechceme, už proto, že to není pravda. Proto je důležité slovo „předpoklad“, které čtenáři říká: My víme, že se klidně může u náhodně zvolených čísel stát, že číslo a to b nedělí. Ale my dokazujeme implikaci, takže nás tyto případy nezajímají a omezíme se pouze na ty situace, kdy a opravdu dělí b. Protože je zásadní rozdíl mezi „je to tak“ a „omezme se na případ, kdy je to tak“, je slovo „předpoklad“ je u důkazů implikace nutné.

Ukážeme si trochu povídavější ale pořád stručnou verzi, která bude pro čtenáře příjemnější, tentokráte to zkusíme bez jména pro nalezenou konstantu.

$\underline{a, b \in \mathbb{Z}}$ lib. Předp.: $\underline{a \mid b}$.

Odtud $b = ak,\ k \in \mathbb{Z} \quad \xrightarrow{\cdot b} \quad b^2 = bak$ neboli $b^2 = a(kb)$, přitom $kb \in \mathbb{Z}$.

Proto $\underline{a \mid b^2}$.

Nyní se od slohu přeneseme k obsahu. Jak jsme již poznamenali, správný přímý důkaz implikace dovede čtenáře od předpokladu k závěru. Ten náš do dělá. Obecně se důkaz musí vypořádat se vším, co vidíme v tvrzení. My dokazujeme toto:

$$\forall a, b \in \mathbb{Z}\colon a \mid b \implies a \mid b^2.$$

Když se podíváme na podtržené části poslední verze důkazu výše, tak vidíme, že přesně a ve správném pořadí odpovídají jednotlivým částem (kvantifikátorové skupiny, předpoklad atd.) našeho tvrzení. To ukazuje, že náš důkaz má správnou základní strukturu (viz 1a.5). Až budete psát vlastní důkazy implikací, tak si vlastně dopředu můžete takto napsat začátek a konec důkazu. V jistém smyslu jsme to dělali výše, když jsme si psali „máme“ a „chceme“. Pomůže vám to ve správném směřování.

Což nás přivádí k oblíbeným chybám. S přehledem nejčastější chyba je důkaz pozpátku, obecněji logická chyba vzniklá tím, že jako nástroj použijeme něco, co je v kolonce „chci“. Oblíbený nefunkční důkaz může vypadat třeba takto:

Předpoklad: $a \mid b$. Odtud $b = ak$ pro $k \in \mathbb{Z}$. Chceme: $b^2 = am$. Dosadíme z předpokladu:

$(ak)^2 = am \quad \longrightarrow \quad m = ak^2$. Důkaz hotov.

Tento důkaz má na první pohled problém na svém konci. Produktem naší usilovné práce je $m = ak^2$. Opravdu jsme zrovna toto chtěli dokázat? Nic takového v tvrzení, které dokazujeme, není. To je jasný indikátor, že jsme v důkazu zabloudili. Ta hlavní chyba je nicméně v okamžiku, kdy jsme tu rovnost $b^2 = am$ k něčemu použili. Je v kategorii „chci“, takže ve chvíli, kdy důkaz píšeme, vůbec nevíme, jestli vlastně platí. My ale v důkazu můžeme používat jen to, co je pravda (nebo o čem to předpokládáme). Jakmile toto základní pravidlo porušíme, tak je důkaz špatně.

△

Poznámka: Všímavý čtenář si možná všiml, že jednu zamaskovanou implikaci jsme již měli. Fakt 1a.7 bylo možné formulovat také takto:

Nechť $a \in \mathbb{Z}$, $m, n \in \mathbb{N}$. Jestliže $m \leq n$, pak $a^m \mid a^n$.

V původní formulaci jsme omezili množinu, ke které se tvrzení vyjadřovalo, nyní to omezení máme jako předpoklad. Původní důkaz se dá snadno upravit, aby vyhovoval struktuře očekávané pro důkaz implikace:

Dány $a \in \mathbb{Z}$, $m, n \in \mathbb{N}$. Předpokládejme, že $m \leq n$. Pak $n - m$ je nezáporné celé číslo, proto $a^{n-m} \in \mathbb{Z}$ a také $a^n = a^m a^{m-n}$, tedy $a^m \,|\, a^n$.

Naopak fakt 1a.10 šlo formulovat takto:

Pro všechna $a, b \in \mathbb{Z}$ splňující $a \,|\, b$ platí $a \,|\, b^2$.

V tomto případě něco tvrdíme o dvojicích čísel z množiny $M = \{(a, b) \in \mathbb{Z}^2 : a \mid b\}$, a to něco je prostý fakt, nikoliv implikace. Důkaz se pak napíše tak, že se zvolí anonymní zástupci z množiny M a pro ně se uká6e platnost onoho tvrzení, což prakticky vzato znamená ukázat platnost rovnosti typu $b^2 = a \cdot \diamondsuit$. Začali bychom tedy takto:

Dány $a, b \in \mathbb{Z}$ splňující $a \,|\, b$. Pak $b = ak$ pro nějaké $k \in \mathbb{Z}$ ...

A důkaz by pokračoval zcela stejně jako předtím. Protože mají původní i nová formulace stejný význam (a z pohledu důkazu stejný cíl i stejné vstupní informace), musí se shodovat i jádro důkazu, přizpůsobí se jen formální nastavení na začátku.

△

M **1a.12 Poznámka:** Mnohem užitečnější než implikace je ekvivalence, což je logická operace, která obohacuje implikaci o možnost přenášet pravdivost také v opačném směru. Což nás přivádí k přirozené otázce. Dokázali jsme, že platí implikace $a \,|\, b \implies a \,|\, b^2$. Platí také implikace opačná? Zajímá nás tedy pravdivost tohoto tvrzení:

$$\forall a, b \in \mathbb{Z}\colon a \,|\, b^2 \overset{?}{\implies} a \,|\, b.$$

Jedna možnost je začít zkoušet různá čísla a sledovat, jestli to funguje. Optimisté se mohou rovnou pokusit napsat důkaz. Udělali bychom podobný rozbor jako předtím a dostali následující:

- Máme: $a \,|\, b^2$ $\downarrow$ $b^2 = a \cdot k$, kde $k \in \mathbb{Z}$
- Chceme: $a \,|\, b$ $\uparrow$ $b = a \cdot \diamondsuit$ pro nějaké $\diamondsuit \in \mathbb{Z}$

Abychom z rovnosti $b^2 = ak$ dostali nalevo b, mohli bychom odmocnit, ale to bychom si zkazili to a napravo, navíc nevíme, jestli náhodou a a k nejsou záporná. Nebo bychom ji mohli vydělit tím b (optimisticky na chvíli ignorujeme možnost $b = 0$). Dostaneme $b = a\frac{k}{b}$, což je rovnost správného typu, ale není vůbec jasné, proč by mělo $\frac{k}{b}$ být celé číslo, což nutně potřebujeme kvůli dělitelnosti. Máme tedy problém a možná je čas na pesimistický přístup, tedy hledání protipříkladu.

Ten se dá hledat metodou střelby (což nás vrátí k experimentování, kterým jsme mohli rovnou začít), ale nepovedený pokus o důkaz mnohdy napoví, kde je zádrhel. My bychom rádi našli čísla a, b, k taková, aby $b^2 = ak$, ale aby b nedělilo to k. To se snadno najde, například lze zařídit, aby v součinu $b^2 = ak$ bylo to k menší než b. Můžeme pak dotyčné tvrzení vyvrátit, tedy napsat

Důkaz (neplatnosti)**:** Protipříklad: $a = 9$, $b = 3$. 9 dělí 3^2, ale nedělí 3. □

To vysvětlení možná nebylo potřebné, opět záleží na očekávané matematické zralosti čtenáře.

Každopádně vidíme, že implikace ve faktu 1a.10 je to nejlepší možné, ekvivalence neplatí.

△

Poznámka: Dokázali jsme pro všechna $a, b \in \mathbb{Z}$ implikaci $a \mid b \implies a \mid b^2$. Tím také automaticky platí její obměna:

Jestliže a nedělí b^2, tak a nedělí ani b.

Ačkoliv obměna nabízí z pohledu logiky totožnou informaci, odlišné podání může být přínosné a také může být podstatný rozdíl v obtížnosti důkazu. Jak bychom postupovali, pokud bychom chtěli tuto obměnu dokázat? Rozbor by vedl na následující situaci:

- Máme: $\neg a \,|\, b^2$ $\downarrow$ neexistuje $k \in \mathbb{Z}$, aby platilo $b^2 = a \cdot k$
- Chceme: $\neg a \,|\, b$ $\uparrow$ nexistuje $\diamondsuit \in \mathbb{Z}$, aby platilo $b = a \cdot \diamondsuit$

Jak se pracuje s informací, že něco neexistuje? Rozhodně hůř než s informací, že máme rovnost. Pro rovnosti existují operace a známé postupy. Pro „neexistuje k“ nic takového nemáme. Pokud bychom si tedy mohli vybrat, určitě bychom raději dokazovali původní implikaci.

Není to ale takto vždycky.

△

M **1a.13 Poznámka:** V poznámce 1a.9 jsme napsali, že přímý důkaz je v zásadě univerzální typ důkazu pro implikace. Poučenějšího čtenáře mohlo napadnout, jestli nepřeháníme, protože existuje také například důkaz nepřímý. Ve skutečnosti v tom není rozpor.

Nepřímý důkaz implikace $P \implies Z$ spočívá v tom, že se namísto původní implikace dokazuje její obměna $\neg Z \implies \neg P$.

I toto je implikace a obvykle se dokazuje přímo, tedy provedeme čtenáře od $\neg Z$ k $\neg P$ způsobem, který zde běžně používáme. Při nepřímém důkazu se tedy nemění postup, ale tvrzení, které dokazujeme.

Například nepřímý důkaz implikace

Jestliže a nedělí b^2, tak a nedělí ani b

se provede tak, že se dokáže implikace

Jestliže a dělí b, tak a dělí b^2.

△

Tvrzení o dělitelnosti druhé mocniny je ve skutečnosti jen speciální případ obecnějšího faktu. V odborném textu bychom jej tedy neuváděli, ale tady plnil pedagogický účel. Podívejme se teď na plnou verzi.

Fakt 1a.14.
Nechť $a, b \in \mathbb{Z}$. Jestliže $a \,|\, b$, pak $a \,|\, (cb)$ pro všechna $c \in \mathbb{Z}$.

S **Rozbor:** Dokazujeme následující tvrzení:

$$a \,|\, b \implies \big[\forall c \in \mathbb{Z} : \; a \,|\, (cb)\big].$$

Víme už, že máme začít takto:

Dáno $a, b \in \mathbb{Z}$. Předpoklad: $a \,|\, b$.

Teď máme ukázat platnost závěru, přičemž závěr samotný zase začíná univerzálním kvantifikátorem. Náš imaginární přítel nám proto poskytne další celé číslo. Začátek důkazu tedy bude vypadat následovně:

Dáno $a, b \in \mathbb{Z}$. Předpoklad: $a \,|\, b$. Nechť $c \in \mathbb{Z}$.

Argument pak má následující východisko a cíl:

- Máme: $a \,|\, b$
- Chceme: $a \,|\, (cb)$

Opět si je přeložíme do řeči rovností.

- Máme: $a \,|\, b$ $\quad\downarrow\quad$ $b = a \cdot k$, kde $k \in \mathbb{Z}$
- Chceme: $a \,|\, (cb)$ $\quad\uparrow\quad$ $cb = a \cdot \diamondsuit$ pro nějaké $\diamondsuit \in \mathbb{Z}$

Čtenář už doufejme vidí, jak pomocí rovnosti vlevo dostat rovnost správného tvaru, zejména levá strana hodně napoví.

Důkaz (rutinní, poučný)**:** Dány $a, b \in \mathbb{Z}$ libovolné. Předpokládejme, že platí $a \,|\, b$, mějme $c \in \mathbb{Z}$. Z předpokladu víme, že $b = ak$ pro nějaké $k \in \mathbb{Z}$. Vynásobením rovnosti číslem c dostaneme $cb = cak$ neboli $cb = a(ck)$. Také $ck \in \mathbb{Z}$ a proto platí $a \,|\, (cb)$.

□

1a.15 Poznámka: Každé matematické tvrzení má základní myšlenku, kterou se snažíme vyjádřit matematičtinou. Zde jde o možnost přinásobení něčeho celého k b při dělitelnosti. Ve faktu 1a.14 jsme zvolili následující formalizaci:

(F) $\forall a, b \in \mathbb{Z}$: $a \,|\, b \implies \big[\forall c \in \mathbb{Z} : \; a \,|\, (cb)\big]$.

Ta podtrhuje centrální roli dvojice a, b s jejich vztahem; jakmile toto máme, pak už přidáme k b cokoliv (celého). V praxi ale mnohdy rovnou začínáme s třemi čísly. Tomu by odpovídala následující alternativní formalizace:

(A) $\forall a, b, c \in \mathbb{Z}$: $a \,|\, b \implies a \,|\, (cb)$.

Tento výrok je na pohled jednodušší a tedy pro čtenáře stravitelnější. Také platí, že pokud nás zajímá čistě tento směr úprav, tak tato alternativa dává přesně stejnou informaci jako ta původní verze. Je to vidět i na důkazu. Ten by musel začít kvůli formálně odlišnému tvrzení jinak:

Dáno $a, b, c \in \mathbb{Z}$. Předpoklad: $a \,|\, b$. Pak . . . .

Od našeho předchozího důkazu se to ale vlastně liší jen tím, že zde jsme si to c vzali hned na začátku, což neovlivní jeho podstatu a další kroky by byly shodné.

Rozdíl mezi formulacemi (F) z faktu a alternativní (A) ale je a projeví se, když se pokusíme směr implikace obrátit.

Případ (F):

Zajímá nás, zda pro $a, b \in \mathbb{Z}$ platí implikace $\big[\forall c \in \mathbb{Z} : \; a \,|\, (cb)\big] \implies a \,|\, c$.

Odpověď zní, že je pravdivá. Jestliže má dělitelnost $a \,|\, (cb)$ platit pro všechna $c \in \mathbb{Z}$, pak musí jistě platit také pro $c = 1$, což nám dá $a \mid b$. Ve skutečnosti jsme tedy mohli do faktu dát ekvivalenci, ale opačný směr není příliš užitečný. V praxi obvykle potkáváme spíše situace, kdy hned od začátku máme tři čísla. Což nás přivádí k alernativě.

Případ (A):

Zajímá nás, zda pro $a, b, c \in \mathbb{Z}$ platí implikace $a \,|\, (cb) \implies a \,|\, b$.

Když si zkusíte experimentovat, brzy zjistíte, že to nemusí platit. Například pokud nám někdo dá $a = 4$, $b = 6$, $c = 2$, tak jistě 4 dělí číslo $2 \cdot 6 = 12$, ale neplatí $4 \,|\, 6$. Obecně pokud a dělí součin dvou čísel, tak nemusí dělit ani jedno z nich.

Alternativní formalizace tvrzení tedy není ekvivalence, ale bohužel existují významné situace, kde bychom zrovna tento opačný směr velmi nutně potřebovali. Zařídí se to tak, že se ještě přidá další předpoklad, což uvidíme v lemma 1b.20. Na to se ale nejprve budeme muset naučit nějaké pokročilé nástroje, takže se zatím vrátíme k základním vlastnostem.

△

Použitím faktu 1a.14 s $c = b$ dostaneme fakt 1a.10. Když z dokázaného výsledku už prakticky okamžitě vyplyne další zajímavý poznatek, tak tomu matematici říkají důsledek. Volba $c = -1$ nám dá tento:

Důsledek 1a.16.
Nechť $a, b \in \mathbb{Z}$. Jestliže $a \,|\, b$, pak $a \,|\, (-b)$.

Tento důsledek vlastně říká, že při zkoumání dělitelnosti nám u b nezáleží na znaménku. Ve skutečnosti nám na něm nezáleží ani u a, prostě dělitelnost jako taková může znaménka ignorovat. Dá se to vyjádřit například takto:

Věta 1a.17.
Nechť $a, b \in \mathbb{Z}$. a dělí b právě tehdy, když $|a|$ dělí $|b|$.

M **1a.18 Poznámka:** Fráze „právě tehdy, když“ indikuje logickou spojku **ekvivalenci**. Formálně:

$$\forall a, b \in \mathbb{Z}\colon\ a \,|\, b \iff |a| \,|\, |b|.$$

Další populární slovní vyjádření je třeba toto:

- a dělí b tehdy a jen tehdy, když $|a|$ dělí $|b|$.
- Tvrzení $a \,|\, b$ a $|a| \,|\, |b|$ jsou ekvivalentní.

Ekvivalence říká, že výroky nalevo a napravo mají vždy stejnou pravdivost, tedy podávají přesně stejnou informaci. Z praktického pohledu můžeme přesouvat platnost i neplatnost v obou směrech. To naznačuje, že ekvivalence je vlastně totéž, jako mít implikaci v obou směrech, což je pravda (a značka tomu odpovídá). Je to také návod na důkaz. Ve snadných případech se dají oba směry přenosu pravdivosti potvrdit najednou, ale obvykle je lepší dokazovat zvlášť dvě implikace, jednu vedoucí zleva doprava a druhou vedoucí zprava doleva. Dokazujeme je obvyklým způsobem.

△

S **Rozbor:** Pro důkaz implikace zleva doprava je situace následující:

- Máme: a dělí b ↓ $b = a \cdot k$, kde $k \in \mathbb{Z}$
- Chceme: $|a|$ dělí $|b|$ ↑ $|b| = |a| \cdot \diamondsuit$ pro $\diamondsuit \in \mathbb{Z}$

Přechod od rovnosti nalevo k té napravo je snadný, takže tuto část důkazu máme vymyšlenu.

Pro opačnou implikaci je to zase takto:

- Máme: $|a|$ dělí $|b|$ ↓ $|b| = |a| \cdot k$, kde $k \in \mathbb{Z}$
- Chceme: a dělí b ↑ $b = a \cdot \diamondsuit$ pro $\diamondsuit \in \mathbb{Z}$

Tentokráte je přechod mezi rovnostmi trochu náročnější, ale to je technický problém. Struktura této části důkazu bude obdobná jako u první a čtenář by jej měl být schopen sledovat.

△

Důkaz (poučný)**:** Mějme $a, b \in \mathbb{Z}$ libovolné.

$\implies$: Předpokládejme, že $a \,|\, b$. Pak $b = ak$ pro nějaké $k \in \mathbb{Z}$. Odtud $|b| = |a| \cdot |k|$, také $|k| \in \mathbb{Z}$, tedy dle definice $|a|$ dělí $|b|$.

$\Longleftarrow$: Předpokládejme, že $|a|$ dělí $|b|$. Pak $|b| = |a| \cdot k$ pro nějaké $k \in \mathbb{Z}$. Víme, že $|b| = b$ nebo $|b| = -b$, můžeme tedy psát $|b| = b \cdot z_b$, kde z_b (znaménko) je buď 1 nebo -1, každopádně je to celé (a nenulové) číslo. Obdobně $|a| = a \cdot z_a$ pro jisté $z_a = \pm 1$. Dosadíme do vzorce z dělitelnosti: $bz_b = az_a \cdot k$ neboli $b = a \cdot \frac{kz_a}{z_b}$. Protože $kz_a \in \mathbb{Z}$ a $z_b = \pm 1$, je $\frac{kz_a}{z_b} \in \mathbb{Z}$ a máme $a \,|\, b$.

□

Toto tvrzení jsme označili jako Větu. Tím matematici naznačují, že tvrzení je významné, popřípadě že má náročnější důkaz. Než se na něj podíváme, rozebereme si, co nám tato věta říká. Přímá interpretace je, že když se ptáme na dělitelnost dvou čísel, tak můžeme ignorovat jejich znaménka. Má ale také hodnotu praktickou, kdy nám umožňuje znaménka měnit.

Mějme čísla $a, b \in \mathbb{Z}$ a představme si, že u některého či obou chceme změnit znaménko, tedy budeme chtít určit dělitelnost pro čísla $\pm a, \pm b$. Aplikujeme větu nejprve na tato čísla a pak na ta původní s využitím toho, že $|\pm a| = |a|$ a $|\pm b| = |b|$ a dostaneme další užitečné pravidlo:

• $\pm a \,|\, \pm b \iff |\pm a| \,|\, |\pm b| \iff |a| \,|\, |b| \iff a \,|\, b$.

Začátek a konec tohoto řetízku úprav nám říká, že modifikace znamének nemění dělitelnost. Dá se to také dokázat přímo, viz cvičení 1a.5. Tento pohled souvisí s alternativním důkazem věty, který nám ukáže další z užitečných dokazovacích triků.

M **1a.19 Poznámka:** Při řešení rovnic s absolutní hodnotou se s oblibou používá zajímavý trik: Pracovní svět si rozdělíme na případy tak, abychom se v každém z nich díky informaci navíc absolutní hodnoty zbavili.

V případě, kdy dokazujeme obecné tvrzení, tedy tvrzení uvedené kvantifikátorem „$\forall x \in M$“, můžeme udělat stejnou věc: Rozložit si M na podmnožiny (případy) a dokazovat tvrzení zvlášť pro každý z nich. Podmínkou úspěchu je, že ty podmnožiny musí dát dohromady celé M a že v každém z případů to tvrzení úspěšně dokážeme.

V našem případě bychom si svět dvojic celých čísel (tedy vlastně množinu $\mathbb{Z}^2$) rozdělili na čtyři části. Důkaz by vypadal takto:

Nechť $a, b \in \mathbb{Z}$.

1) Případ $a, b \geq 0$: Pak $|a| = a$, $|b| = b$, máme tedy dokázat ekvivalenci
$$a \,|\, b \iff a \,|\, b.$$
Ta je evidentně pravdivá.

2) Případ $a \geq 0, b < 0$: Pak $|a| = a$, $|b| = -b$, máme tedy dokázat ekvivalenci
$$a \,|\, b \iff a \,|\, (-b).$$
Směr $\Longrightarrow$ jsme dokázali výše (viz důsledek 1a.16). Opačný směr se dokáže obdobně, ale také je možné použít následující fintu, kdy se důsledek aplikuje na čísla $a, -b$: Jestliže $a \,|\, (-b)$, tak podle důsledku a dělí také číslo $-(-b) = b$.

To bylo moc hezké, matematici mají takové vtipné využití již existujících poznatků moc rádi.

3) Případ $a < 0, b \geq 0$: Pak $|a| = -a$, $|b| = b$, máme tedy dokázat ekvivalenci
$$a \,|\, b \iff (-a) \,|\, b.$$
4) Případ $a, b < 0$: Pak $|a| = -a$, $|b| = -b$, máme tedy dokázat ekvivalenci
$$a \,|\, b \iff (-a) \,|\, (-b).$$
Celkem čtyři implikace v případech 3 a 4 by se dokazovaly velmi podobně, minimální úpravou důkazu faktu 1a.14.

Intuitivně vzato se v důkazu snažíme dojet do jistého cíle. V určitém okamžiku se může stát, že se trať rozdvojí (roztrojí atd.). Pak je třeba projet všechny možnosti a pokaždé dojet do správného cíle.

Dokazování po částech může být velmi efektivní v případě, kdy nám takové rozdělení nabídne užitečnou informaci navíc. Někdy nemáme na výběr, když se v naší základní množině objeví výjimečné případy. Zde to bude docela často nula, viz například důkaz věty 1a.28 a další.

Zajímavé je, že důkaz po částech nám nabídne alternativní vysvětlení, proč implikace dokazujeme tak, jak je dokazujeme. Jako ukázku si dokážeme například tento směr v případě 3:
$$(-a) \,|\, b \implies a \,|\, b. \qquad \text{(I)}$$

Důkaz: Nechť $a, b \in \mathbb{Z}$. Uvažujme dva případy.

Případ T (true): Předpoklad $(-a) \,|\, b$ je splněn. Pak $b = (-a)k$ pro nějaké $k \in \mathbb{Z}$. Odtud $b = a(-k)$ a $(-k) \in \mathbb{Z}$, tedy $a \,|\, b$. Dokázali jsme implikaci (I).

Případ F (false): Předpoklad $(-a) \,|\, b$ není splněn. Pak podle definice implikace je implikace (I) automaticky pravdivá (bez ohledu na závěr).

Protože žádný jiný případ není, dokázali jsme, že implikace (I) platí vždy.

□

Všimněte si, že v případě F jsme vlastně nic nedělali. Protože je každá implikace pravdivá v případě nesplněného předpokladu, tak by tento případ F vypadal úplně stejně při jakémkoliv pokusu o důkaz nějaké implikace. To znamená, že pravdivost implikace se rozhoduje v případě T (když je splněný její předpoklad), takže je zbytečné se tím druhým případem zabývat. Stačí prozkoumat případ T, což je přesně to, co dělá naše doporučená forma důkazu.
△

Fakt 1a.20.
Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \,|\, b$ a $a \,|\, c$, pak $a \,|\, (b + c)$.

S Rozbor: Máme tři celá čísla a, b, c. Potřebujeme pro ně dokázat implikaci $(a \,|\, b \wedge a \,|\, c) \implies a \,|\, (b + c)$.
Máme tedy následující situaci:

- Máme: a dělí b, a dělí c
- Chceme: a dělí $b + c$

Přepis do rovností už čekáme, v tomto případě si zase musíme dát pozor. První předpoklad přepíšeme jako $b = ak$, $k \in \mathbb{Z}$. Tím má k přidělenou roli a už jej nesmíme použít k jinému účelu. Druhý předpoklad proto přepíšeme pomocí jiného písmene. A pokud bychom chtěli použít písmeno i v kolonce „chceme“, tak bychom museli použít ještě nějaké třetí. Máme následující situaci:

- Máme: a dělí b, a dělí c
  $\downarrow$
  $b = a \cdot k$, $c = a \cdot l$
  pro nějaké $k, l \in \mathbb{Z}$
- Chceme: a dělí $b + c$
  $\uparrow$
  $b + c = a \cdot \diamondsuit$ pro nějaké $\diamondsuit \in \mathbb{Z}$.

Dál už by to čtenář mohl zvládnout sám a důkaz tedy necháme jako cvičení 1a.4. Přechod od dvou rovností nalevo k jedné napravo nás ovšem navede na zajímavou úvahu.
△

S 1a.21 Poznámka: Všechny důkazy implikací, které jsme zatím viděli, měly společnou strukturu. Deklarovali jsme předpoklad P, přepsali jsme jej do praktičtějšího tvaru a pomocí algebraických triků jej upravovali, dokud jsme se nedostali k závěru Z.

U první implikace jsme rovnost $b = ak$ vynásobili číslem b a následně upravili do tvaru $b^2 = a(kb)$, ale také jsme ji mohli umocnit a pak upravit. U druhého důkazu jsme rovnost $b = ak$ vynásobili číslem c a následně upravili do tvaru $bc = a(kc)$. V dalším důkazu jsme na tuto rovnost aplikovali absolutní hodnotu a dostali $|b| = |a| \cdot |k|$. No a v důkazu výše můžeme rovnosti $b = ak$, $c = al$ sečíst a dostaneme $b + c = ak + al$. To pak upravíme na $b + c = a(k + l)$ a máme přesně ten tvar, který potřebujeme.

Tento typ důkazu by šlo nazvat „přímá cesta“ a dal by se vyjádřit symbolicky tímto obrázkem.

$$P \longrightarrow\longrightarrow \cdots \longrightarrow Z$$

Hlavní motivace, kterou při jeho vymýšlení sledujeme, je dána touto otázkou: Jak se z toho, co mám, umíchá to, co chci?

Výhodou tohoto důkazu je jeho jednoduchost. Nevýhodou je, že funguje hlavně u jednoduchých situací, zatímco u složitějších selhává.

Proto si ukážeme ještě další možnost, která se v takto jednoduchých případech příliš neliší, ale časem uvidíme, že opravdu jde o něco jiného. Dá se aplikovat v situacích, kdy závěr implikace (nebo jeho přepis, tedy to, co vidíme v kolonce „chci“) má podobu rovnosti, ale také třeba nerovnosti, implikace, ekvivalence a podobně. Intuitivně řečeno by to měl být zápis cesty (rovnost či nerovnost je cesta z levé strany na pravou). Všechny důkazy, které jsme podrobně rozebrali výše, do této kategorie spadají. Pokud se zaměříme na fázi, kdy jsme přešli od dělitelnosti k rovnostem, tak potřebujeme potvrdit platnost implikace ve tvaru

$$P \implies (Z_L = Z_R).$$

Nový přístup funguje následovně. Předpoklad P deklarujeme, případně mírně modifikujeme, aby byl praktičtější, ale pak z něj nikam nevyjdeme. Necháme si jej v záloze, aby nám pomohl ve správný okamžik, a místo toho čtenáři ukážeme, že je možno dojít od Z_L k Z_R (nebo naopak). Při té cestě nám v nějakém kritickém okamžiku pomůže ten předpoklad. Schéma tohoto nového důkazu tedy vypadá takto:

$$P; \quad Z_L = \cdots \overset{P}{=\!=} \cdots = Z_R.$$

Klíčová otázka u tohoto typu důkazu je následující: Co vím o Z_L?

Ukažme si to u prvního důkazu implikace. Předpoklad byl $b = ak$, $k \in \mathbb{Z}$. Chtěli jsme se dostat k rovnosti typu $b^2 = a \cdot \diamondsuit$. Původní otázka zněla: Jak rovnost cílového typu dostanu z té dané? Nová otázka zní: Co v dané situaci víme o b^2? Odpovíme si, že podle předpokladu je možno b nahradit něčím jiným. Dostáváme $b^2 = (ak)^2$. To ještě není ono, tak pokračujeme dále a výraz dále upravujeme prodloužením řetízku rovnítek: $b^2 = (ak)^2 = a(ak^2)$. Tím jsme se dostali k cílovému Z_R, tato pravá strana nám již vyhovuje.

Vidíme v akci hlavní výhodu tohoto přístupu. Zatímco u rovnic a rovností je to tak, že když chceme jednu ze stran upravit, tak musíme napsat celou novou rovnost či rovnici (tedy opisujeme i ty strany, se kterými jsme spokojeni), tak řetízek rovností (a nerovností) můžeme libovolně dlouho prodlužovat, dokud se nedostaneme k žádanému cíli, a každý výraz píšeme jen jednou. Výrazy na úplném začátku a konci se pak rovnají (popřípadě je mezi nimi žádaná nerovnost). Tento přístup je tedy nejen flexibilnější, ale také kratší. Ostatně porovnejme si původní stručný zápis v poznámce 1a.11 s tímto:

$\underline{a, b \in \mathbb{Z}}$ lib. Předp.: $\underline{a \,|\, b}$.

Odtud $b = ak$, $k \in \mathbb{Z}$ $\quad\longrightarrow\quad$ $b^2 \overset{P}{=} (ak)^2 = a(ak^2)$, přitom $ak^2 \in \mathbb{Z}$.

Proto $\underline{a \,|\, b^2}$.

Je to trochu kratší. U takto jednoduchého důkazu se nedá čekat významné zjednodušení, ale liší se to významně způsobem, jakým jsme přemýšeli. Neformálně tomuto typu důkazu říkám typ „závěr jako cesta“.

Ukažme si tento nový pohled také u důkazu faktu 1a.20. Máme předpoklad (po přepisu do tvaru rovností) $b = ak$, $c = al$ pro $k, l \in \mathbb{Z}$. Podíváme se do kolonky „chci“ a položíme si klíčovou otázku: Co víme o čísle $b + c$? A takto si odpovíme:

$$\begin{aligned} \underline{b + c} &= ak + al \qquad \text{(podle předpokladu)} \\ &= a(k + l). \qquad \text{(upravíme na potřebný tvar).} \end{aligned}$$

Přidáme povinnou poznámku, že $k + l \in \mathbb{Z}$, a jsme připraveni napsat závěr.

V situaci, kdy nemusíme dělat tyto podrobné komentáře, jde o velmi efektivní metodu.

Většinu jednodušších důkazů, které níže následují, lze dělat oběma přístupy. Je docela dobrý trénink si zkoušet oba.

△

I u faktu 1a.20 se nabízí otázka, jestli náhodou neplatí opačný směr, tedy zda lze z platnosti $a \,|\, (b + c)$ odvodit, že automaticky $a \,|\, b$ a $a \,|\, c$. Trocha experimentování rychle ukáže, že to obecně neplatí, například $3 \,|\, (2 + 4)$, ale neplatí $3 \,|\, 2$ ani $3 \,|\, 4$. Máme tedy smůlu a jako obvykle je k dispozici jen implikace, tedy jednosměrný vztah.

Trochu delší experimentování by mohlo naznačit zajímavou věc, že když platí $a \,|\, (b + c)$, tak buď dělitelnost u obou b a c funguje, nebo se u obou pokazí, nelze to zkazit jen u jednoho z čísel. To ukazuje, že situace není zcela náhodná, a občas se to hodí. Tak si to vyjádříme způsobem, který ještě později párkrát použijeme.

Fakt 1a.22.
Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \,|\, (b + c)$ a $a \,|\, b$, pak $a \,|\, c$.

Důkaz: Dáno $a, b, c \in \mathbb{Z}$. Předpoklad: $a \,|\, (b + c)$ a $a \,|\, b$. Podle důsledku 1a.16 pak také $a \,|\, (-b)$. Aplikováním faktu 1a.20 na první a třetí pozorování dostaneme, že a musí dělit číslo $(b + c) + (-b) = c$.

□

M **Poznámka:** Čtenář byl možná překvapen, že jsme v důkazu nepracovali s rovnostmi. Bylo by to možné a pro čtenáře může být užitečné si takový důkaz napsat. Důkazu, který je veden základními nástroji z definic, se někdy říká „elementární důkaz“.

My jsme zde předvedli jiný přístup, kdy používáme věci, které už jsme dokázali. Takovéto důkazy bývají obvykle kratší a také přehlednější, protože pozornost není rozptýlena upravováním výrazů a podobnou manuální prací. Matematici obvykle tento přístup preferují (jsou to nadšení a asi historicky první recyklátoři), ale jsou výjimky, protože elementární důkaz někdy napomůže našemu intuitivnímu pochopení situace.

△

Spojením faktu 1a.14 a 1a.20 vznikne následující tvrzení:

Důsledek 1a.23.
Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \,|\, b$ a $a \,|\, c$, pak pro všechny $\beta, \gamma \in \mathbb{Z}$ platí $a \,|\, (\beta b + \gamma c)$.

Ukážeme si chytrý důkaz používající již odvedenou práci, opět doporučujeme zkusit si elementární důkaz jako trénink.

Důkaz: Dány $a, b, c \in \mathbb{Z}$, $\beta, \gamma \in \mathbb{Z}$. Předp.: $a \,|\, b$ a $a \,|\, c$. Podle faktu 1a.14 pak také $a \,|\, (\beta b)$ a $a \,|\, (\gamma c)$, tyto dva poznatky pak pomocí faktu 1a.20 vedou na $a \,|\, (\beta b + \gamma c)$.

□

Toto nové tvrzení tedy kombinuje dva předchozí poznatky o násobení a sčítání v dělitelnosti, naopak pokud máme toto tvrzení, tak z něj automaticky vyplyne to o násobení (volba $\gamma = 0$) i to o sčítání (volba $\beta = \gamma = 1$). Jde tedy o jednu myšlenku, kterou lze rovnocenně vyjádřit buď dvěma fakty o každé operaci zvlášť nebo jedním tvrzením, které zahrne obojí. Obdobná situace se v matematické teorii objevuje na více místech a autoři obvykle volí variantu, která jim zrovna přijde pěknější. Viz také poznámka 1b.14.

Zmínili jsme se o blahodárné vlastnosti rovnosti (a nerovnosti) spočívající v možnosti je řetězit a výsledný výpočet pak zkrátit na jednu rovnost (či nerovnost) spojující začátek a konec. Podstata je schována ve schopnosti zkracovat řetízek dvou rovností: Pokud $a = b$ a $b = c$ (neboli zkráceně $a = b = c$), pak $a = c$. Obdobně pokud $a \leq b$ a $b \leq c$ (neboli $a \leq b \leq c$), pak také $a \leq c$, čtenář si jistě vymyslí i verze pro nerovnosti ostré a v opačném směru. Tento typ chování je velmi užitečný a existuje pro něj odborná terminologie a teorie, což poznáme v kapitole 4. Je tedy potěšující, že takto významná vlastnost platí i pro dělitelnost.

Věta 1a.24.
Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \mid b$ a $b \mid c$, pak $a \mid c$.

S Rozbor: Důkaz je velmi podobný těm předchozím a s důvěrou jej necháme na čtenáři, viz cvičení 1a.4. Pro jistotu připomeneme, že když předpoklad a závěr přepisujeme do řeči rovností, tak nesmíme opakovat stejný název pro konstantu. Skončíme tak například v této situaci:

- Máme: $b = a \cdot k$, $c = b \cdot l$, kde $k, l \in \mathbb{Z}$
- Chceme: $c = a \cdot \diamondsuit$ pro nějaké $\diamondsuit \in \mathbb{Z}$.

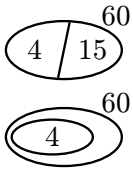
Při důkazu typu „přímá cesta“ si pak klademe následující otázku: Jakými rovnicovými operacemi vyrobíme z prvních dvou rovností rovnost třetího typu?

Při důkazu typu „závěr jako cesta“ si zase klademe tuto otázku: Co víme (například na základě předpokladu) o čísle c? Následně se snažíme, aby se objevil součin s a.

Můj pocit je, že v tomto případě je druhý přístup o něco snažší.
△

S 1a.25 Poznámka: Když pracujeme s matematickými pojmy, tak hodně pomůže, pokud si dokážeme vytvořit nějakou intuitivní představu, co se vlastně děje. Nejlepší je představa obrázková, protože mozek dobře pracuje s vizuálními podněty. U některých pojmů se představa nabízí, například při práci s funkcemi si přirozeně vybavujeme jejich grafy (i když jsou situace, kdy lépe funguje představa jiná, viz kapitola 8). U méně zřejmých pojmů se může možných představ nabízet více a každý máme svůj individuální pohled, já zde nabídnu představu, která u dělitelnosti funguje pro mě.

Základem je myšlenka jdoucí až ke starým Řekům: Velká čísla lze poskládat z menších pomocí násobení. Vrcholem této představy je rozklad čísla na prvočísla, což čtenář nejspíše zná, například $60 = 2 \cdot 2 \cdot 3 \cdot 5$. Dělitelnosti stačí méně a pracuje s možnými rozklady čísla na komponenty (faktory). Třeba rozklad $60 = 4 \cdot 15$ říká, že lze mít čtyřku jako komponentu šedesátky, zde tomu říkáme $4 \mid 60$. Když toto vidím, tak se mi v hlavě objeví obláčková představa, kterou vidíme napravo, nejprve podrobnější (ukazuje obě komponenty), pak ta zaostřená na čtyřku coby dělitele.



Protože se faktory spojují násobením, tak tato obláčková představa funguje dost dobře v situacích, kdy se násobí, což je příklad faktu 1a.14. Když číslo b vynásobíme číslem c, tak mu přidáme další faktor do rozkladu, ale existující komponentu a to nijak nezruší (obrázek níže vlevo). Pěkně to vystihuje i podstatu věty 1a.24 (obrázek níže vpravo).

Na druhou stranu ve faktu 1a.20 se sčítá, s tím si moje představa moc nerozumí.

Nebezpečí u intuitivních představ je, že nemusí být zcela přesné, takže v určitých situacích mohou napovídat špatně. Zde je potřeba dát si pozor na nulu. Intuitivně vidíme nulu jako velice malý obláček, možná jako tečku, ale ve skutečnosti nulu dělí všechna celá čísla, takže je vlastně obláčkem nekonečným, aby se do něj ta čísla vešla.

Jinak je ta obláčková představa docela dobrá a budeme se na ni občas odkazovat, nicméně je podstatné, abychom na různé intuitivní představy nespoléhali. Sice nám mohou pomoci v pochopení, co se děje, ale jistotu dát nemohou, tu dodá až důkaz.
△

Jaká je souvislost mezi dělitelností a velikostí čísel? Něco už jistě tušíme.

Věta 1a.26.
Nechť $a, b \in \mathbb{Z}$. Jestliže $a \mid b$ a $b \neq 0$, tak $|a| \leq |b|$.

Tento důkaz opět vyžaduje technický trik kvůli absolutní hodnotě, což zvyšuje jeho náročnost, ale ohledně struktury nečekáme žádné překvapení.

Důkaz (poučný)**:** Mějme $a, b \in \mathbb{Z}$ libovolné. Předpoklad $a \mid b$ dává $b = ak$ pro nějaké $k \in \mathbb{Z}$, což znamená $|b| = |a| \cdot |k|$. Jestliže $b \neq 0$, tak také $k \neq 0$, tudíž $|k| \in \mathbb{N}$. To znamená, že $|k| \geq 1$ a proto $|b| = |a| \cdot |k| \geq |a|$. □

Podstata tvrzení asi čtenáře nepřekvapila, ale je dost možné, že by přehlédnul nutnost podmínky $b \neq 0$. My ji tam ovšem potřebujeme, není problém najít a takové, že $a \mid 0$ a přitom $|a| > 0$. Je tedy důvod být opatrný. Obecně se dá říct, že nám nula komplikuje zkoumání dělitelnosti a často ji budeme muset brát v důkazech jako speciální případ. Svádí to k tomu, abychom tuto teorii budovali jen pro přirozená čísla. Ušetřili bychom si řadu starostí, ale pak by nám to chybělo v aplikacích, kde se objevují i záporná čísla a třeba i ta nula.
U tohoto tvrzení je docela užitečná také obměna, proto si ji uvedeme jako oficiální tvrzení.

Důsledek 1a.27.
Nechť $a, b \in \mathbb{Z}$. Jestliže $|a| > |b|$ a $b \neq 0$, tak a nedělí b.

Další užitečná vlastnost nerovnosti, na kterou se blíže podíváme v kapitolách 4 a 6, je tato: Pokud $a \leq b$ a $b \leq a$, tak $a = b$. Funguje něco takového i pro dělitelnost? Co si o tom myslí čtenář?
Pokud jsme při experimentování neomezovali svou fantazii, tak jsme možná přišli na příklad podobný tomuto: $13 \mid (-13)$ a $(-13) \mid 13$, ale neplatí $-13 = 13$. Takže obecně tu užitečnou vlastnost nemáme, ale začne platit, když se vhodně omezíme.

Věta 1a.28.
Nechť $a, b \in \mathbb{N}_0$. Jestliže $a \mid b$ a $b \mid a$, pak $a = b$.

Platnost tohoto tvrzení se nejlépe dokáže pomocí věty 1a.26, musíme si ale dát pozor, protože ta věta neplatí v případě $b = 0$. Případ nuly tedy budeme muset rozebrat zvlášť, takže uvidíme důkaz s rozkladem na případy, jak jsme o tom hovořili v poznámce 1a.19.

Důkaz (rutinní)**:** Nechť $a, b \in \mathbb{Z}$ lib. Jestliže $a = 0$, tak b coby násobek nuly musí být také 0, tedy platí $a = b$. Pokud $b = 0$, dostáváme symetricky $a = 0$ a zase máme $a = b$.
Zbývá případ, kdy jsou a, b nenulová čísla. Podle věty 1a.26 pak z předpokladu vzájemné dělitelnosti dostáváme $|a| \leq |b|$ a $|b| \leq |a|$ neboli $|a| = |b|$. Protože jsme brali $a, b \in \mathbb{N}_0$, je $|a| = a$ a $|b| = b$, tedy musí platit $a = b$. □

Tím končí naše přehlídka užitečných pravidel pro práci s dělitelností. Je také dobré umět rozpoznat, co naopak s dělitelností dělat nejde, a umět případně dokázat, že jistý nápad není obecně platný. Čtenář si to může vyzkoušet ve cvičení 1a.10. Tím také končí období snadných důkazů implikace s obtížností vhodnou pro začátečníka. Další důkazy tohoto typu přijdou v kapitole 2, zatím je možné si je procvičit například ve cvičení 1a.9.

Sice jsme na dělení celých čísel nechtěli moc myslet, ale brzy se nám bude velmi hodit zbytek po dělení, takže si jej pořádně matematicky zavedeme. Jako děti nás učili, že při dělení čísla a číslem d (nenulovým) nám může vzniknout zbytek r, a to pak zapisujeme jako $\frac{a}{d} = q + \frac{r}{d}$. Abychom si sem nezavlékali dělení, raději si to přepíšeme do ekvivalentního tvaru $a = qd + r$. Podle tohoto vzorečku ovšem zbytek ještě nepoznáme, protože podobných vyjádření pro daná čísla a, d je více. Například pro $a = 23$ a $d = 5$ máme $23 = 4 \cdot 5 + 3$, ale také $23 = 2 \cdot 5 + 13$. Jak poznáme, co je správně?

Definice.
Nechť $a, d \in \mathbb{Z}$, $d \neq 0$. Číslu r říkáme **zbytek** (**remainder**) při dělení čísla a číslem d, pokud existuje $q \in \mathbb{Z}$ takové, že $a = qd + r$ a $0 \leq r < |d|$.
Značíme jej $r = a \bmod d$, čteno „a modulo d“.
Číslu q pak říkáme **částečný podíl** (**quotient**) čísel a a d.

Takže 3 je správný zbytek po dělení 23 číslem 5, píšeme $23 \bmod 5 = 3$.

M Poznámka: Zase máme definici typu, kdy nám umožňuje nazvat nějaký objekt jménem, ale jen v případech, kdy je splněn specifikovaný test. Tato podmínka je velmi podobná té z dělitelnosti, zejména v tom, že nás u konstanty q nebude zajímat konkrétní hodnota, ale jen to, zda existuje. Podobně jako u dělitelnosti je dobré nevázat se

na konkrétní písmena ale na formy, struktury a přesuny objektů. Mějme tři celá čísla $\heartsuit, \diamondsuit, \triangle$, která mohou být konkrétní, ale také může jít o výrazy třeba i s proměnnými. Pokud se nám podaří vytvořit rovnost správné formy a splnit další dvě podmínky:

$$\diamondsuit = \Theta \cdot \heartsuit + \triangle \quad \wedge \quad \Theta \in \mathbb{Z} \quad \wedge \quad 0 \leq \triangle < |\heartsuit|,$$

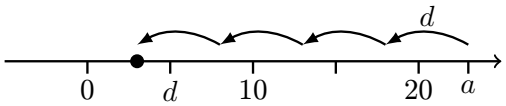
tak máme právo z těch tří objektů vytvořit obrázek $\triangle = \diamondsuit \bmod \heartsuit$. A také naopak.
△

Poučná poznámka se bude hodit v důkazech, ale jak zbytek hledáme prakticky? Ve škole jsme k tomu používali operaci, jejíž jméno zde nesmíme vyslovit, ale v praxi se tomu často snažíme vyhnout, protože je to operace relativně náročná na procesorový výkon, tudíž také relativně pomalá. Stejný pohled na věc máme i při ručním výpočtu. Naštěstí to jde i jinak. Podle definice je zbytek $r = a - qd$, což lze interpretovat tak, že jsme od čísla a odebrali číslo d určitý počet krát (popřípadě přidali, pokud je $q < 0$). Tato operace má jednoduchou geometrickou interpretaci. Na celočíselné ose jsme začali na pozici a a pak jsme se pomocí q kroků velikosti d přesunuli do pozice r. Znaménko čísla q určuje, zda jsme kroky o velikost d dělali doleva (když $q > 0$) nebo doprava.

Je ovšem dobré si uvědomit, že dělat krok velikosti $-d$ je totéž jako dělat krok o velikost d na opačnou stranu. Hledání zbytku po dělení lze tedy interpretovat tak, že se z pozice a přesouváme pomocí kroků o velikost $|d|$ směrem k počátku tak, abychom skončili na vhodném místě. Co je to vhodné místo? Definice říká, že máme skončit někde mezi nulou (včetně) a $|d|$. To je velikost kroku, takže to prakticky znamená, že máme skončit buď v nule, nebo napravo od ní a co nejblíže, co to jde.

Tento postup se dá snadno algoritmizovat cyklem s podmínkou a pro počítač je to v mnoha případech velice pohodlný způsob hledání zbytku. Pro člověka shodou okolností také.

Příklad 1a.c: Vyzkoušíme si to na příkladě $a = 23$ a $d = 5$, kde jsme už odhalili správný zbytkový zápis $23 = 4 \cdot 5 + 3$. Máme tedy $23 \bmod 5 = 3 = 23 - 4 \cdot 5$. Naše interpretace říká, že z pozice 23 na celočíselné ose jsme udělali čtyři skoky o velikosti 5 a dostali jsme se do lokace 3, což je nejblíže k nule, jak se dá pomocí těchto skoků legálně dostat. Další skok by nás dovedl do -2, což je sice k nule blíž, ale podmínka z definice nepovoluje záporné číslo jako zbytek.



Mimochodem, vidíme zde, proč je v definici podstatné, že počet skoků q je celé číslo. Pokud bychom si totiž povolili skákat i o půlkroky a podobně, tak bychom myšlenku hledání zbytku zcela pokazili.

Pro výpočty z hlavy je užitečné poznamenat, že nemusíme celou tu cestu dělat najednou. Pokud bych třeba hledal $150 \bmod 13$, tak bych si všimnul, že umím snadno skočit desetkrát a pořád zůstanu napravo od nuly. Dostanu tak výhodnější východisko $150 - 10 \cdot 13 = 20$. Z dvacítky už třináctkou snadno doskáčeme ke správné odpovědi $150 \bmod 13 = 7$.

Vraťme se k výsledku $23 \bmod 5 = 3$, který si teď modifikujeme.

Kolik je $23 \bmod (-5)$? Intuitivní odpověď založená na cestovací představě by byla, že zase 3, protože začínáme na stejném místě a skáčeme stejně velkými skoky. Jediný rozdíl je, že předtím jsme skákali čtyřikrát, zatímco teď budeme skákat -4 krát, protože směr skoku vede na opačnou stranu.

Máme pravdu? Algebraicky: $23 = (-4) \cdot (-5) + 3$, přičemž $-4 \in \mathbb{Z}$ a $0 \leq 3 \leq |-5|$. Číslo $r = 3$ tedy vyhovuje požadavkům z definice. Všimněte si souvislosti mezi těmito rovnostmi:

$$23 = 4 \cdot 5 + 3 \qquad 23 = (-4) \cdot (-5) + 3.$$

Pokud změníme znaménko u d, tak se q přizpůsobí a není třeba měnit r. Toto je srdcem důkazu tvrzení, že při hledání zbytku nezáleží na znaménku d, viz cvičení 1a.12.

Kolik je $(-23) \bmod 5$? Určitě nebude fungovat následující trik: Máme $23 = 4 \cdot 5 + 3$, prohodíme znaménka: $-23 = (-4) \cdot 5 + (-3)$, tedy $r = -3$. To by odpovídalo tomu, že náš obrázek překlopíme kolem svislé osy (horizontal flip). Jenže to nefunguje, definice nepřipouští záporná čísla jako zbytek.

Obrázek tedy překlápět nebudeme, místo toho změníme počátek cesty na $a = -23$ a tentokráte skáčeme po pětkách doprava, dokud se nedostaneme za nulu. Graficky tak odhalíme následující algebru: $-23 = (-5) \cdot 5 + 2$. Zde $-5 \in \mathbb{Z}$ a $0 \leq 2 \leq |-5|$, takže číslo $r = 2$ vyhovuje požadavkům z definice a máme $(-23) \bmod 5 = 2$.

Změna znaménka u a tedy výsledek počítání zbytku ovlivní. Možná i tušíte jak, viz cvičení 1a.12.

Na závěr konstatujme, že pokud by mělo být skoků hodně, tak může být pro počítač výhodnější najít r dělením. U člověka je to otázka vkusu. Jako příklad najdeme $4147 \bmod 37$. Jedna možnost je použít povědomý výpočet napravo. Zjistíme, že $4147 \bmod 37 = 3$.

```
4147 : 37 = 112
 44
 77
  3
```

Alternativa: Všimnu si, že mohu skočit stokrát a dostanu se na pozici $4147 - 100 \cdot 37 = 447$. Pak můžeme skočit desetkrát: $447 - 10 \cdot 37 = 77$. Nakonec to dorazíme: $77 - 3 \cdot 37 = 3$.

Dobrá zpráva je, že zde u teorie nebudeme řešit, jak se zbytky hledají, a v praktických příkladech budeme mít přátelská čísla, kde se zbytky najdou hned posunem. Pro úplnost čtenáři prozradíme, jak se to dělá pomocí dělení, v bonusové sekci 1a.33.

△

V našem praktickém okénku jsme podvědomě pracovali s dvěma představami, které ale (zatím) nejsou zaručeny. Definice specifikovala, jakým testem potvrdíme identitu zbytku, ale v této chvíli vůbec nevíme jistě, jestli se pro daná dvě čísla a, d s $d \neq 0$ dá uspět. U dělitelnosti nás to netrápilo: Když pro nějakou dvojici a, b test nevyšel, tak jsme prostě prohlásili, že a nedělí b. Ovšem u zbytku bychom velmi rádi, aby se dal najít vždy. To je oblíbená otázka existence.

S ní obvykle přichází další otázka, a to otázka jednoznačnosti. Když matematici zavedou značení pro nějaké číslo (třeba $\sqrt{13}$ nebo π), tak se očekává, že se bude používat ve výpočtech a tedy že bude mít jednoznačně určenou hodnotu. Bylo by nemilé, kdyby třeba π mělo tři možné hodnoty. Stejně tak jsme podvědomě očekávali, že když najdeme jeden zbytek, tak už je hotovo. Jak to tedy je, existují zbytky a jsou jednoznačné? Následující věta ukáže, že situace je nejlepší možná.

Věta 1a.29. (o dělení se zbytkem, division theorem, division algorithm)
Nechť $a, d \in \mathbb{Z}$, $d \neq 0$. Pak existují $q, r \in \mathbb{Z}$ takové, že $a = qd + r$ a $0 \leq r < |d|$.
Čísla q a r jsou jednoznačně určena.

S **Rozbor:** Věta má dvě části. První je existenční. Již víme, že důkaz existenčního tvrzení typicky spočívá v předvedení konkrétního exempláře. I my zde zbytek najdeme, a to metodou popsanou výše: Z a se posuneme pomocí d tak, abychom skončili na vhodném místě. Musíme to ale zapsat správně matematicky. Poté, co najdeme kandidáta na zbytek (a q), tak dokážeme, že jsme opravdu našli ty správné objekty, tedy ukážeme, že splňují podmínky z definice. To dá trochu práce a ověření jednoho z požadavků vyžaduje nápad (neboli trik), který se nenabízí, jak jsme byli zvyklí u jednodušších důkazů. Pokročilé matematické důkazy vyžadují zásah inspirace, které velmi pomáhá zkušenost. Tuto pasáž je možno provést více způsoby, jako nejpřirozenější se jeví důkaz sporem. Protože jej zde používáme poprvé, uděláme si níže matematickou poznámku o tom, jak důkaz sporem funguje.

Abychom si ušetřili určité technické komplikace. dokážeme existenci nejprve pro případ $d > 0$ a pak pomocí něj uděláme případ $d < 0$. Připomeňme, že varianta $d = 0$ je v tvrzení vyloučena.

Druhá část potvrzuje jednoznačnost. Jednoznačnost nějakého objektu x se typicky dokazuje takto. Předpokládáme, že máme dva kandidáty x_1, x_2. Můžeme si představit, že dva lidé nezávisle na sobě zkusili takový objekt x najít. My pak ukážeme, že nutně musí platit $x_1 = x_2$, tedy nemůže se stát, že by se nalezly dva různé objekty x.

△

M **1a.30 Poznámka:** Důkaz sporem je obecný nástroj na dokazování výroků, s oblibou se používá například na důkaz neexistence nějakého objektu. Funguje následovně.

Mějme nějaké tvrzení V. Důkaz V sporem spočívá v důkazu implikace $\neg V \implies F$, kde F označuje libovolný nepravdivý výrok. Existuje jen jediná možnost, kdy může být pravdivá implikace, jejíž závěr je neplatný: Když neplatí její předpoklad. Náš důkaz implikace $\neg V \implies F$ tedy ukazuje, že $\neg V$ neplatí, a tedy že V platí.

Dotyčnou implikaci $\neg V \implies F$ dokazujeme obvykle přímým důkazem, jak jsme zde již zvyklí. Prakticky tedy důkaz sporem sestává z následujících kroků:

0) Je dobré čtenáři na začátku říct, že V budeme dokazovat sporem.
1) Předpokládáme, že V neplatí.
2) Z tohoto předpokladu běžným způsobem odvodíme standardním postupem nějaký nesmyslný fakt, třeba že $0 < 1$. Tradičně se na to reaguje slovem „spor“.
3) Konstatujeme, že jsme došli ke sporu, tudíž platí původní tvrzení V.

Příklad: Dokážeme sporem, že neexistuje reálné číslo x splňující $x = x + 1$.

Předpokládejme, že existuje. Pak rovnost $x = x + 1$ upravíme na $0 = 1$ a máme spor. To dokazuje neexistenci takového čísla.

△

Důkaz (dobrý, poučný)**:** Mějme $a, d \in \mathbb{Z}$, $d \neq 0$.

1) Existence.

a) Případ $d > 0$, tedy vlastně $d \geq 1$. Uvažujme množinu

$$M = \{a - qd : q \in \mathbb{Z} \wedge a - qd \geq 0\}$$

čísel získaných z a posuny o d a vyhovujících první podmínce na zbytek, tedy nezáporných. Tato množina je neprázdná: Jestliže je $a \geq 0$, tak volba $q = 0$ dává $a \in M$. Jestliže $a < 0$, pak stačí zvolit $q = a$ a máme $a - qd = a(1 - d) \in M$, neboť díky $d \geq 1$ máme $(1 - d) \leq 0$ a tedy $a(1 - d) \geq 0$.

Už z definice jsou všechny prvky M nezáporné, jsou to samozřejmě celá čísla. Máme tedy neprázdnou podmnožinu $\mathbb{N}_0$, vezmeme její nejmenší prvek r. Musel vzniknout jako $r = a - q_0 d$ pro nějaké $q_0 \in \mathbb{Z}$, takže $a = q_0 d + r$ a máme potvrzenu platnost rovnosti z definice zbytku.

Protože M obsahuje jen nezáporná čísla, musí platit $0 \leq r$ a máme první z odhadů z definice. Dokážeme sporem, že platí i druhý, tedy $r < |d| = d$, což je třetí a poslední z podmínek definice zbytku.

Předpokládejme opak, tedy že $r \geq d$. Uvažujme číslo $r_1 = r - d$. Zjevně $r_1 < r$. Ovšem také $r_1 \geq 0$ a toto celé číslo lze navíc vyjádřit jako $r_1 = a - (q_0 + 1)d$, kde $q_0 + 1 \in \mathbb{Z}$, a proto $r_1 \in M$. Protože jsme zvolili r jako nejmenší číslo této množiny, musí platit $r \leq r_1$. Máme tedy zároveň $r_1 < r$ a $r \leq r_1$, což je spor.

Tím jsme potvrdili, že $r < |d|$ a tedy $r = a \bmod d$ existuje spolu s příslušným $q_0 \in \mathbb{Z}$.

b) Případ $d < 0$: Aplikujeme právě dokázané na $-d = |d| > 0$ a najdeme q, r tak, aby $a = q(-d) + r$ a $0 \leq r < |d|$. Pak $a = (-q)d + r$ a pořád platí $0 \leq r < |d|$, tedy čísla $-q$ a r vyhovují požadavkům.

2) Jednoznačnost: Předpokládejme, že $a = q_1 d + r_1$ a $a = q_2 d + r_2$, kde $q_1, q_2 \in \mathbb{Z}$, $0 \leq r_1 < |d|$ a $0 \leq r_2 < |d|$. Pak $q_1 d + r_1 = q_2 d + r_2$, proto $(q_1 - q_2)d = r_1 - r_2$. Díky $r_1, r_2 \geq 0$ lze odhadovat $-|d| < -r_2 \leq r_1 - r_2 \leq r_1 < |d|$ neboli $|r_1 - r_2| < |d|$. Takže $|q_1 - q_2| \cdot |d| < |d|$, což znamená $|q_1 - q_2| < 1$. Ale $(q_1 - q_2) \in \mathbb{Z}$, proto $q_1 - q_2 = 0$ a tedy $q_1 = q_2$. Pak také $r_1 = r_2$.

□

V průběhu důkazu jsme vlastně ukázali, že $a \bmod d = a \bmod |d|$. V praxi se proto můžeme omezit na (příjemná) kladná d.

Pro korektnost důkazu je klíčové, že všechny kroky musejí být správně odůvodněny. Obvykle se ovšem zmiňujeme jen o významnějších věcech, ty zcela jasné necháváme na čtenáři. Někdy ale takto dojde k průšvihu, když přehlédneme, že něco „jasného“ ve skutečnosti tak jasné není. V tomto důkazu takový okamžik najdeme. Jen tak mimochodem jsme řekli, že jako r vezmeme nejmenší číslo jisté množiny. Kde ale bereme jistotu, že existuje?

Teď se čtenář možná zarazil, sám jistě nejmenší a největší čísla mnohdy hledal a nacházel. Jenže ono to kupodivu není tak jednoduché, narážíme zde na samotné základy matematiky. O těch se čtenář dočte více v kapitole 6, náš konkrétní problém pak řeší tzv. Princip dobrého uspořádání (viz 6b.14).

Teď jsme ovšem provedli něco nebezpečného. Náš důkaz využívá něco z budoucí kapitoly, ale co když ta věc bude dokázaná pomocí věty o dělení? Tím by vznikl takzvaný důkaz kruhem, který ovšem důkazem není, je to logická chyba. Takovému zacyklení je třeba se vyhýbat a v odborné knize bychom se nikdy neodvolali na něco, co ještě nebylo dokázáno. Toto je ale úvodní učebnice a autor soudí, že na záležitosti spojené s existencí minima je třeba čtenáře nejprve trochu připravit. Zatím se tedy musí spokojit s autorovým ujištěním, že k žádnému zacyklení nedojde a důkaz je v pořádku.

Příznivci indukce ocení, že větu o dělení lze dokázat i pomocí tohoto nástroje, viz poznámky 7b.xx a 7b.yy. Ostatně v kapitole 7 uvidíme, že existence minim a funkčnost indukce spolu úzce souvisejí.

M **1a.31 Poznámka:** Vraťme se ještě k důkazu sporem. V některých středoškolských učebnicích se lze dočíst, že důkaz sporem slouží k dokazování implikací $P \implies Z$ a že funguje takto: Předpokládáme platnost P. Deklarujeme důkaz sporem a předpokládáme neplatnost Z, z čehož odvodíme neplatnost P. Protože P nemůže zároveň platit i neplatit, máme spor a tedy Z platí.

Tato představa není správná ze dvou důvodů. Za prvné, důkaz sporem lze použít i na jiná tvrzení než implikace, jak jsme viděli výše. Za druhé, podívejme se, co vlastně dělá doporučovaný postup:

1) Deklarujeme předpoklad P.

2) Dokážeme platnost implikace $\neg Z \implies \neg P$.

3) Konstatujeme spor mezi $\neg P$ a P, dokončíme důkaz.

Bod 2) by měl být čtenáři povědomý. Jde o důkaz obměny implikace $P \implies Z$. Stačilo tedy dokázat krok 2) a prohlásit, že jsme nepřímým důkazem dokázali danou implikaci $P \implies Z$. Kroky 1) a 3) jsou navíc.

Doporučený postup tedy bere korektní nepřímý důkaz a z nějakého důvodu jej zabalí do další vrstvy, aby uměle vyrobil důkaz sporem. Je to zbytečná komplikace a navíc to zakrývá podstatu toho, co se dělá. Proto obecně doporučuji se důkazům sporem spíše vyhýbat a místo toho při hledání alternativy nejprve pomýšlet na důkaz nepřímý.

Pro některé implikace $P \implies Z$ ovšem důkaz sporem je přirozenou cestou. Jak to má potom správně vypadat?

Podle obecného mustru bychom měli dokázat implikaci $\neg(P \implies Z) \implies F$. Podle pravidel logiky to dává $(P \wedge \neg Z) \implies F$. Postupujeme tedy následovně:

1) Deklarujeme důkaz sporem a uděláme předpoklad, že P platí a Z neplatí.

2) Standardním postupem odvodíme nějaké tvrzení, které je nemožné, tedy F.

3) Konstatujeme, že díky sporu jsme prokázali platnost implikace $P \implies Z$.

V praxi ten spor mnohdy nabývá podoby $P \wedge \neg P$, ale nemusíme se do toho nutit, důkaz sporem je mnohem flexibilnější. Ukážeme si to na jednoduchém příkladě.

Dokážeme pravdivost implikace $x > 23 \implies x > 13$ pro všechna $x \in \mathbb{R}$.

Důkaz sporem: Předpokládejme, že $x > 23$ ale neplatí $x > 13$. Pak máme nerovnosti $13 \geq x$ a také $x > 23$, spojením dostaneme $13 > 23$, spor. Dokazovaná implikace tedy platí.

△

Dělení se zbytkem je myšlenka, kterou lze aplikovat i na jiné objekty než celá čísla, například je užitečná při práci s polynomy. Dokonce na to existuje speciální matematický obor. Nás ale budou zajímat jen jednodušší věci, které jsou nicméně velmi důležité pro diskrétní matematiku a computer science.

Následující tvrzení je snadné a představuje dobrou příležitost procvičit si překládání z matematiky do lidštiny a také dokazování.

Fakt 1a.32.
Nechť $a, b \in \mathbb{Z}$, $a \neq 0$. Pak $a \,|\, b$ právě tehdy, když $b \bmod a = 0$.

Prostě a dělí b právě tehdy, když a vydělí b beze zbytku. To zní naprosto samozřejmě a člověka napadá, co na takovém tvrzení ještě dokazovat, ale každý z obou pojmů má svou vlastní definici, takže bychom to správně ověřit měli. Je to velmi snadné, důkaz necháme jako cvičení 1a.11. Stojí také za rozmyšlení, že bychom tam mohli dát podmínku $b \bmod |a| = 0$, v praxi většinou preferujeme pracovat s kladnými děliteli. Mimochodem, kdyby tento fakt pravdivý nebyl, tak by to bylo jasné pobídnutí k zamyšlení, zda jsou naše definice rozumné.

Teď se podíváme na některé populární aplikace dělitelnosti a modula.

Příklad 1a.d:

1. Knižní kód ISBN je navržen tak, aby částečně fungoval jako opravný kód, přesněji řečeno tak, abychom snadno a s vysokou pravděpodobností poznali, že nám při jeho předávání vznikla chyba. Jeho starší verze měla 10 cifer. Prvních 9 cifer identifikuje jazyk, nakladatele a číslo knihy dle katalogu nakladatele. Jako poslední číslo se vždy dává zbytek po dělení počátečního devítimístného čísla jedenácti, je samozřejmě třeba vyřešit problém zbytku 10, to se pak dává znak X. Tvrdíme, že výsledné číslo je pak již vždy dělitelné jedenácti.

Označíme-li jako a to počáteční devítimístné číslo, pak poslední cifra je $r = a \bmod 11$. Platí tedy $a = 11k + r$ pro nějaké $k \in \mathbb{Z}$, Výsledný ISBN kód je pak $n = 10a + r$. Dosadíme: $n = 110k + 10r + r = 11(10k + r)$, také $10k + r \in \mathbb{Z}$ a proto je n dělitelné jedenácti. Jiný důkaz, možná rychlejší (viz příští kapitola): Podle definice máme $a \equiv r \pmod{11}$, také $10 \equiv (-1) \pmod{11}$, proto $10a + r \equiv (-1)r + r = 0 \pmod{11}$.

To znamená, že když nám někdo dá ISBN číslo, my jej zkusíme vydělit 11 a nevyjde to, tak už víme, že se někde stala chyba. Tento test není dokonalý, neodhalí všechny překlepy při psaní čísla, ale platí následující: Pokud v čísle dělitelném jedenáctkou změníme jednu cifru, tak nové číslo zaručeně nebude dělitelné jedenácti. Tento bezpečnostní kód tedy umí odhalit chybu v jedné cifře, ale v případě více chyb už si jich všimnout nemusí.

Mimochodem, proč jsme použili zrovna jedenáctku? Uvažujme kandidáta $d \in \mathbb{N}$. Potřebujeme zajistit následující: Pokud v nějakém čísle změníme jednu cifru, tak se nutně musí změnit zbytek po dělení číslem d. Dá se ukázat, že čísla $d < 11$ toto neumí zajistit. Například číslo 5273 vzniklo chybným přepisem čísla 1273, ale má stejný zbytek při dělení desíti, osmi, šesti, pěti, čtyřmi, třemi a dvěma jako původní číslo. Nic menšího než $d = 11$ tedy fungovat nebude. Jedenáctka funguje a větší čísla s obdobnou vlastností by nám to zbytečně komplikovala.

2. Hashovací funkce. Představte si, že chceme ukládat data o lidech, kteří jsou kódováni rodnými čísly, ale máme jen n paměťových adres. Hledáme funkci h, která nám řekne, že data člověka s rodným číslem a se mají dát na adresu $h(a)$. Jedním z možných řešení je použít funkci $h(a) = a \bmod n$.

Výhody: h je na, rychle se počítá.

Nevýhoda: h není prostá, vznikají tzv. kolize. Jsou nutné strategie, co pak, což se probírá jinde než v diskrétní matematice.

3. Když už mluvíme o rodných číslech: Rodná čísla se dělají následovně: První dvoučíslí je rok narození, druhé měsíc narození zvýšený u žen o 50, třetí dvoučíslí je den narození, další tři pak identifikují oblast a pořadové číslo dítěte v rámci této oblasti. Jako poslední cifra rodného čísla se dá buď zbytek po dělení počátečního devítimístného čísla jedenácti, pokud vyjde menší než 10, nebo 0, pokud ten zbytek vyjde 10.

Co to znamená? Že každé rodné číslo nekončící nulou musí být dělitelné jedenácti, u čísel nulou končících už to ale nemusí být pravda. Moc jich nebývá: statisticky každé jedenácté, ale zejména v posledních desetiletích se takovým číslům při přidělování snaží vyhýbat, takže jich je výrazně méně než jedenáctina. Málokdo se s nimi potká, díky tomu přežívá fáma, že se dělitelností jedenáctkou dají kontrolovat správná rodná čísla.

4. Od rodných čísel přejdeme k náhodným. Pro různé simulace a samozřejmě také hry je potřeba mít zdroj náhodných čísel. To ale není tak snadné zařídit, protože tento zdroj musí být algoritmický (počítač má naprogramovánu metodu, jak to dělat). Nevznikají tak čísla náhodná, ale pseudonáhodná, jejich zdroji se říká generátor.

Když už se tedy smíříme s tím, že máme generátor jen pseudonáhodných čísel, tak bychom alespoň chtěli, aby ten algoritmus z dlouhodobého hlediska nezvýhodňoval žádná čísla ani nevykazoval pravidelnosti. To je velice náročný úkol, u méně náročných aplikací (třeba her) se dá od striktních nároků částečně ustoupit a pak přichází vhod tzv. **lineární kongruentní generátor**.

Funguje to následovně. Zvolíme modulus $n \in \mathbb{N}$. Pak zvolíme multiplikátor $a \in \mathbb{N}$ splňující $2 \leq a < n$ a posun $c \in \mathbb{N}$ splňující $0 \leq c < n$. Jako náhodná čísla používáme posloupnost $x_{k+1} = (a \cdot x_k + c) \bmod n$. Je nutno ji nastartovat pomocí zdrojové hodnoty $x_0 \in \mathbb{N}$. Vychází pak z toho čísla z rozmezí 0 až $n-1$, která se tváří náhodně (ale nejsou, protože se opakují, nejdelší možný řetězec má délku n, ale může se zacyklit dříve, zabráníme tomu tak, že zvolíme jako n prvočíslo).

Například pokud zvolíme $n = 6$, $a = 4$, $c = 1$, dostáváme vzorec $x_{k+1} = (4x_k + 1) \bmod 6$. Když se rozhodneme začít dvojkou, dostaneme posloupnost $2, 3, 1, 5, 3, 1, 5, 3, \ldots$, délka cyklu je 3.

Když si zvolíme $n = 9$, $a = 7$, $c = 4$, pak ze vzorce $x_{k+1} = (7x_k + 4) \bmod 9$ už vyjde řetězec délky 9.

Často chceme čísla z intervalu $(0, 1)$, pak bereme x_k/n. Při volbě hodně velkého n a a to vychází docela dobře.

Často se volí $c = 0$, tzv. čistě multiplikativní generátor, pak nechceme $x_k = 0$ a je snaha volit n, a tak, aby vznikl právě řetězec délky $n - 1$. Typická volba je třeba $n = 2^{31} - 1$ a $a = 7^5 = 16807$, kdy pak opravdu dostaneme $2^{31} - 2 = 4294967294$ hodnot. To už je pro praktické účely docela dost.

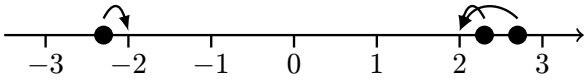
△

Jedna užitečná aplikace se ještě najde v příkladě 15.d v bonusové sekci.

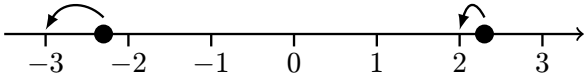
1a.33 Částečný podíl a zaokrouhlování

Na závěr se jako bonus vrátíme k problematice nalezení zbytku tak, že nejprve najdeme pomocí dělení $\frac{a}{d}$ částečný podíl q. Jakým vzorcem se to q najde? Dělá se to zaokrouhlením, ale správná otázka zní, jakým?

V inženýrské praxi se obvykle zaokrouhluje na nejbližší celé číslo, třeba $2.7 \doteq 3$ a $2.3 \doteq 2$, ale to zde nepomůže. Ve světě počítačů se často používá funkce $\mathrm{Int}(x)$, která z čísla odebere desetinnou část, takže třeba $\mathrm{Int}(2.7) = 2$, $\mathrm{Int}(2.3) = 2$, $\mathrm{Int}(-2.3) = -2$. Samozřejmě $\mathrm{Int}(2) = 2$. Tuto funkci nabízí řada programovacích jazyků i mnohá kalkulačka a dalo by se říci, že zaokrouhluje směrem k nule:



Toto zaokrouhlování opravdu nachází správné q v případě, kdy $a, d > 0$, což v mnoha aplikacích postačuje. My ale chceme vzorec obecný a tím správným zaokrouhlením pro naše účely je zaokrouhlení stále na stejnou stranu. Taková zaokrouhlení jsou dvě. Jedno z nich je zaokrouhlení dolů, tedy doleva na číselné ose, což souhlasí s $\mathrm{Int}(x)$ u kladných čísel.



Očekáváme tedy, že -2.3 se zaokrouhlí na -3. Na druhou stranu na číselné ose se posouvá zaokrouhlení nahoru.

Definice.
Definujme následující funkce na $\mathbb{R}$:

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}; \qquad \text{(zaokrouhlení dolů, floor)}$$
$$\lceil x \rceil = \min\{n \in \mathbb{Z} : n \geq x\}. \qquad \text{(zaokrouhlení nahoru, ceiling)}$$

Přeloženo z matematičtiny do lidštiny, $\lfloor x \rfloor$ je největší celé číslo, které „nepřeleze“ x. Tím je dán význam definice. Podíváme se na příklady.

Příklad 1a.e: Podle definice

$$\lfloor 13 \rfloor = \max\{n \in \mathbb{Z} : n \leq 13\} = \max\{\ldots, -1, 0, 1, \ldots, 11, 12, 13\} = 13.$$

Obdobně (rozmyslete si to) $\lceil 13 \rceil = 13$, $\lfloor -13 \rfloor = -13$ a $\lceil -13 \rceil = -13$.

Snadno také nahlédneme, že

$$\begin{aligned}\lfloor 2.3\rfloor &= \max\{\dots,-1,0,1,2\} = 2,\\ \lceil 2.3\rceil &= \min\{3,4,5,\dots\} = 3,\\ \lfloor -2.3\rfloor &= \max\{\dots,-5,-4,-3\} = -3,\\ \lceil -2.3\rceil &= \min\{-2,-1,0,1,\dots\} = -2.\end{aligned}$$

Vypadá to, že definice dělá to, co od ní čekáme.
△

Podotkněme, že s maximy a minimy zde opět pracujeme intuitivně a do probrání kapitoly 6b zatím jen věříme autorovi, že u množin v definici vždy existují a lze tedy spolehlivě zaokrouhlovat.

Zájemce o další vlastnosti těchto funkcí odkážeme na bonusovou kapitolu 15. Tam také čtenář najde několik užitečných aplikací včetně převodu mezi číselnými soustavami a zejména důkaz následujícího tvrzení, viz fakt 15.5:

Fakt 1a.34.
Nechť $a, d \in \mathbb{Z}$, $d \neq 0$, nechť je q částečný podíl a a d.
Pak $q = \left\lfloor \frac{a}{d} \right\rfloor$ pro $d > 0$ a $q = \left\lceil \frac{a}{d} \right\rceil$ pro $d < 0$.

Cvičení

Cvičení 1a.1 (rutinní)**:** Najděte následující:
(i) 218 mod 87,
(ii) 60 mod 15,
(iii) -13 mod 7,
(iv) 2 mod 17,
(v) 0 mod 7,
(vi) -1030 mod 13.

Cvičení 1a.2 (rutinní)**:** Dokažte, že pro každé $a \in \mathbb{Z}$ platí $a \mid a$, $1 \mid a$ a $a \mid 0$ (viz fakt 1a.2).

Cvičení 1a.3 (rutinní)**:** Dokažte, že jestliže $a, b \in \mathbb{Z}$ splňují $a \mid b$, pak pro každé $n \in \mathbb{N}$ platí:
(i) $a \mid b^n$.
(ii) $a^n \mid b^n$.

Cvičení 1a.4 (rutinní)**:** Nechť $a, b, c \in \mathbb{Z}$.
(i) Dokažte, že jestliže $a \mid b$ a $a \mid c$, pak $a \mid (b + c)$. Viz fakt 1a.20.
(ii) Dokažte, že jestliže $a \mid b$ a $b \mid c$, pak $a \mid c$. Viz věta 1a.24.

Cvičení 1a.5 (rutinní, poučné)**:** Nechť $a, b \in \mathbb{Z}$. Dokažte, že následující podmínky jsou ekvivalentní:
(i) $a \mid b$,
(ii) $(-a) \mid b$,
(iii) $a \mid (-b)$,
(iv) $(-a) \mid (-b)$,
Tím se ukáže, že při dělitelnosti na znaménku nezáleží, viz věta 1a.17
Nápověda: Vytvořte z implikací nějaký uzavřený cyklus zahrnující (i) až (iv), třeba (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) $\implies$ (i), a dokažte jej. Rozmyslete si, že pak už z toho plyne libovolná implikace mezi nějakými dvěma podmínkami z těchto čtyř, jsou tedy všechny ekvivalentní.

Cvičení 1a.6 (rutinní)**:** Nechť $a, b, c, d \in \mathbb{Z}$. Dokažte, že jestliže $a \mid b$ a $c \mid d$, pak $(ac) \mid (bd)$.

Cvičení 1a.7 (rutinní)**:** Nechť $a, b, c \in \mathbb{Z}$. Dokažte:
(i) Jestliže $a \mid b$, pak $(ac) \mid (bc)$.
(ii) Jestliže $(ac) \mid (bc)$ a $c \neq 0$, pak $a \mid b$.
Co by se stalo, kdyby $c = 0$?

Cvičení 1a.8 (poučné)**:** Nechť $a, b, c \in \mathbb{Z}$. Dokažte/vyvraťte, že jestliže $a \mid bc$, pak $a \mid b$ nebo $a \mid c$.

Cvičení 1a.9 (rutinní, poučné)**:** Dokažte přímo (elementárním důkazem) následující:
(i) Pro $a \in \mathbb{Z}$ platí $a \mid a^3$.
(ii) Pro $a \in \mathbb{Z}$ platí $(3a) \mid (6a^2)$.
(iii) Pro $a, b \in \mathbb{Z}$ platí: Jestliže $a \mid b$, pak $ab \mid b^2$.
(iv) $\forall a, b \in \mathbb{Z}$: $a \mid b \implies a \mid (b - a)$.

Cvičení 1a.10 (rutinní)**:** Vyvraťte následující tvrzení (neboli dokažte jejich nepravdivost):
(i) Nechť $a, b \in \mathbb{Z}$. Jestliže $a \,|\, b$, pak $a^2 \,|\, b$.
(ii) Nechť $a, b \in \mathbb{Z}$. Jestliže $a \,|\, b$, pak $(b-a) \,|\, b$.
(iii) Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \,|\, c$ a $b \,|\, c$, pak $(ab) \,|\, c$.
(iv) Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \,|\, c$ a $b \,|\, c$, pak $(a+b) \,|\, c$.
(v) Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \,|\, b$, pak $(a+c) \,|\, (b+c)$.

Cvičení 1a.11 (rutinní)**:** Nechť $a, b \in \mathbb{Z}$, $a > 0$. Dokažte, že $a \,|\, b$ právě tehdy, když $b \bmod a = 0$.

Cvičení 1a.12 (poučné)**:** Nechť $a, d \in \mathbb{N}$, položme $r = a \bmod d$.
(i) Dokažte, že $a \bmod (-d) = r$.
(ii) Dokažte, že když $r \neq 0$, tak platí $(-a) \bmod d = d - r$ a $(-a) \bmod (-d) = d - r$.
Jak to funguje pro případ $a \bmod d = 0$?

Cvičení 1a.13 (poučné)**:** Nechť $n \in \mathbb{N}_0$.
(i) Dokažte, že n je dělitelné pěti právě tehdy, je-li jeho poslední cifra rovna 0 nebo 5.
(ii) Dokažte, že n je dělitelné čtyřmi právě tehdy, je-li jeho poslední dvoučíslí dělitelné 4.
Nápověda: Poslední cifra r čísla n se dá algebraicky zjistit pomocí $n = 10k + r$, poslední dvojčíslí dá $n = 100k + r$.

Řešení:
1a.1: (i) 44, (ii) 0, (iii) 1, (iv) 2, (v) 0, (vi) 10.
1a.2: Dáno $a \in \mathbb{Z}$. $a = a \cdot 1$ a $1 \in \mathbb{Z}$, $a = 1 \cdot a$ a $a \in \mathbb{Z}$, $0 = a \cdot 0$ a $0 \in \mathbb{Z}$.
1a.3: (i): $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ lib. Předp: $a \,|\, b$ neboli $b = ak$, $k \in \mathbb{Z} \implies b^n = b \cdot b^{n-1} \overset{P}{=} (ak)b^{n-1} = a(kb^{n-1})$, také $kb^{n-1} \in \mathbb{Z}$, tedy $a \,|\, b^n$.
Alternativa: $b^n \overset{P}{=} (ak)^n = a(a^{n-1}k^n)$, také $a^{n-1}k^n \in \mathbb{Z}$, tedy $a \,|\, b^n$.
(ii): $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ lib. Předp: $a \,|\, b \implies b = ak$, $k \in \mathbb{Z} \implies b^n \overset{P}{=} (ak)^n = a^n k^n$, také $k^n \in \mathbb{Z}$, tedy $a^n \,|\, b^n$.
1a.4: (i): $a, b, c \in \mathbb{Z}$ lib. Předp: $a \mid b$, $a \mid c \implies b = ak, c = al \wedge k, l \in \mathbb{Z} \implies b + c \overset{P}{=} ak + al = a(k+l)$ a $k + l \in \mathbb{Z} \implies a \,|\, (b+c)$.
(ii): $a, b, c \in \mathbb{Z}$ lib. Předp: $a \,|\, b$ a $b \,|\, c \implies b = ak, c = bl \wedge k, l \in \mathbb{Z} \implies c \overset{P}{=} (ak)l = a(kl)$ a $kl \in \mathbb{Z} \implies a \,|\, c$.
1a.5: $a, b \in \mathbb{Z}$ lib. (i) $\implies$ (ii): $a \,|\, b \implies b = ak, k \in \mathbb{Z} \implies b = (-a) \cdot (-k) \wedge -k \in \mathbb{Z} \implies (-a) \,|\, b$.
(ii) $\implies$ (iii), (iii) $\implies$ (iv), (iv) $\implies$ (i) obdobně.
1a.6: $a, b, c, d \in \mathbb{Z}$ lib. Předp: $a \,|\, b$, $c \,|\, d$ neboli $b = ak$, $d = cl$, $k, l \in \mathbb{Z} \implies bd \overset{P}{=} (ak)(cl) = (ac)(kl)$, také $kl \in \mathbb{Z}$, tedy $(ac) \,|\, (bd)$.
1a.7: $a, b, c \in \mathbb{Z}$ lib. (i): Předp: $a \,|\, b \implies b = ak$, $k \in \mathbb{Z} \implies bc = (ac)k \wedge k \in \mathbb{Z} \implies (ac) \,|\, (bc)$.
(ii): Předp: $c \neq 0$, $(ac) \,|\, (bc) \implies bc = ack \wedge k \in \mathbb{Z} \implies b = ka \wedge k \in \mathbb{Z} \implies a \,|\, b$.
Kdyby $c = 0$, tak nelze zkrátit a důkaz je neplatný. Jiný důkaz vymyslet nelze, tvrzení s $c = 0$ neplatí, viz $a = 13$, $b = 23$, $c = 0$.
1a.8: Neplatí, $6 \,|\, (4 \cdot 9)$, ale není $6 \,|\, 4$ ani $6 \,|\, 9$.
1a.9: (i): $a \in \mathbb{Z}$ lib. Víme $a^3 = a \cdot a^2$, také $a^2 \in \mathbb{Z}$, tedy $a \,|\, a^3$.
(ii): $a \in \mathbb{Z}$ lib. Víme $6a^2 = (3a) \cdot (2a)$, také $2a \in \mathbb{Z}$, tedy $(3a) \,|\, (6a^2)$.
(iii): $a, b \in \mathbb{Z}$ lib. Předp: $a \,|\, b$ neboli $b = ak$, $k \in \mathbb{Z} \implies b^2 = b \cdot b \overset{P}{=} akb = (ab)k$, také $k \in \mathbb{Z}$, tedy $(ab) \,|\, b^2$.
(iv): $a, b \in \mathbb{Z}$ lib. Předp: $a \,|\, b$ neboli $b = ak$, $k \in \mathbb{Z} \implies b - a \overset{P}{=} ak - a = a(k-1)$, také $k - 1 \in \mathbb{Z}$, tedy $a \,|\, (b-a)$.
1a.10: (i): Protipříklad $a = 4$, $b = 20$. (ii): Protipříklad $a = 2$, $b = 6$. (iii): Protipříklad $a = 4$, $b = 6$, $c = 12$. (iv): Protipříklad $a = 4$, $b = 6$, $c = 12$. (v): Protipříklad $a = 2$, $b = 4$, $c = 1$.
1a.11: $a, b \in \mathbb{Z}$, $a \neq 0$ lib.
Jestliže $a \,|\, b$, pak $b = ak = ka + 0$, kde $k \in \mathbb{Z}$ a $0 \leq 0 < |a|$, tedy $r = 0$.
Jestliže $b \bmod a = 0$, pak $\exists q \in \mathbb{Z}$ aby $b = qa + 0 = aq \longrightarrow a \,|\, b$.
1a.12: Jestliže $r = a \bmod d$, pak $a = qd + r$ pro nějaké $q \in \mathbb{Z}$ a $0 \leq r < d$. Protože $d > 0$, je $d = |-d|$.
(i): Pak také $a = (-q)(-d) + r$, $-q \in \mathbb{Z}$ a $0 \leq r < |-d|$, tedy číslo r splňuje požadavek na zbytek.
(ii): Přepis: $(-a) = (-q)d - r = (-q)d - d + d - r = (-q-1)d + (d-r)$, přičemž $-q - 1 \in \mathbb{Z}$ a díky $0 < r < d$ je $-d < -r < 0$, tedy $0 < d - r < d$. Číslo $d - r$ proto splňuje podmínku z definice $(-a) \bmod d$.
Obdobně se použije $(-a) = q(-d) - r$.
Jestliže $r = 0$ neboli $d \,|\, a$, pak už víme, že u dělitelnosti na znaménku nezáleží, tedy vždy $\pm a \bmod \pm d = 0$.
1a.13: (i) Označme $n = 10a + b$, tedy b je poslední cifra. Protože 5 dělí 10, tak podle faktu 1a.14 dělí i $10a$. Podle faktu 1a.20, popřípadě faktu 1a.22 $5 \mid n$ právě tehdy, když $5 \mid b$. Pro jednociferné číslo b ale $5 \mid b$ jen pro $b = 0$ a $b = 5$.
(ii): Označte $n = 100a + b$, kde b je dvouciferné. Protože 4 dělí 100, tak ...

1b. Nejmenší společný dělitel, Bezoutova identita

Víme, že pro každé číslo a platí $a = 1 \cdot a$. Pro celá čísla nám to ukazuje, že vždy existuje jejich faktorizace na dva faktory. Je to ale faktorizace poněkud nudná (matematici raději říkají „triviální“) a hlavně extrémní, celá hodnota čísla a je soustředěna do jednoho faktoru. Stejně extrémní je faktorizace $a = (-1) \cdot (-a)$. Existují čísla, která už jinou faktorizaci nemají. Ta jsou velmi speciální. Ostatní čísla nabízejí navíc i jiné faktorizace (netriviální), kde se a rozdělí rovnoměrněji mezi faktory, například $12 = 3 \cdot 4$. Těmto dvěma typům čísel přiřadíme jména, ale je zvykem tato jména používat pouze pro kladná čísla.

Definice.
Nechť $a \in \mathbb{N}$, $a \neq 1$.
Řekneme, že a je **prvočíslo** (**prime**), jestliže jediná přirozená čísla, která a dělí, jsou 1 a a.
Řekneme, že a je **složené číslo** (**composite number**), jestliže existují $k, l \in \mathbb{N}$ takové, že $a = kl$, $1 < k < a$ a $1 < l < a$.

Tato definice opět obsahuje testy, takže snadno rozhodneme, zda číslo (větší než 1) je prvočíslo a zda je složené. Všimneme si, že definice složeného čísla podle očekávání mluví o existenci rozkladu, který jej rozdělí na menší kousky, ale v definici prvočísla jsme spíš než rozklad použili počet dělitelů, protože je to takto praktičtější a tradičnější. Díky faktu 1a.2 víme, že každé celé číslo a má dělitele 1 a a, takže prvočísla jsou ta, která už k těmto automatickým dělitelům další kladné nepřidají.

Všimneme si, že definice se nevztahuje na číslo 1, které sice technicky podmínku o jediných dělitelích 1 a a splňuje, ale není mu to nic platné; definice se o něm odmítla vyjádřit a tudíž to není prvočíslo. Není to ani číslo složené, je to prostě číslo, které stojí mimo naše kategorie. Je speciální. Nabízí se otázka, proč jsme v definici zakázali jedničce stát se prvočíslem. Odpověď zní, že by v tom okamžiku přestala platit řada velmi užitečných tvrzení o celých číslech. Je to tedy volba praktická.

V úvodu jsme čísla rozdělili na dva typy, podle toho, zda mají jen triviální rozklady nebo i nějaké jiné navíc. Podvědomě tedy očekáváme, že čísla složená a prvočísla se spolu budou doplňovat. Přesněji řečeno očekáváme následující:

a) Všechna přirozená čísla větší než 1 náleží do těchto dvou kategorií;

b) tyto kategorie se vylučují, tedy žádné číslo nemůže patřit do obou.

Pokud bychom v definici u těchto dvou typů použili shodný test a rozdělovali čísla podle úspěchu a neúspěchu, tak už by tyto dvě vlastnosti byly zaručeny. Protože jsme ale u každého pojmu použili jiný přístup (dělitelé versus netriviální rozklad), tak v této chvíli nevíme, jestli nejsou čísla, která jsou zároveň prvočísla i složená, popřípadě nic z toho. Ukážeme, že k tomu nemůže dojít a věci fungují tak, jak chceme.

Věta 1b.1.
Každé přirozené číslo větší než 1 je buď prvočíslo nebo číslo složené.

M **Poznámka:** Tvrzení obsahuje frázi „buď ... nebo“. To je speciální modifikace logické disjunkce zvaná v počítačovém světě xor, můžeme jí také říkat „vylučovací nebo“. Výrok tvořený standardní disjunkcí platí, pokud splníme některou z komponent nebo třeba i obě. Vylučovací nebo tuto poslední variantu nepřipouští, nutí nás se rozhodnout jen pro jednu z možností. Tvrzení věty tedy spojuje oba požadavky a), b) formulované před větou. △

M **1b.2 Poznámka:** Vraťme se k požadavkům a), b). Ty se v matematice objevují docela často v množinovém jazyce. Ukažme si to na naší situaci. Mluvíme vlastně o třech množinách čísel: $\mathbb{N}_{>1} = \{n \in \mathbb{N} : n \neq 1\}$, dále množině P prvočísel a množině C složených čísel. Naše požadavky lze množinově vyjádřit takto:

a) $\mathbb{N}_{>1} = P \cup S$; (to je to „nebo“ z naší věty)

b) $P \cap C = \emptyset$. (to je to „buď“ z naší věty)

Pokud jsou tyto požadavky splněny, tak řekneme, že množiny P, C tvoří rozklad množiny $\mathbb{N}_{>1}$. Blíže se na to podíváme v části 5.

Jak se takováto tvrzení o množinách dokazují?

Rovnost $A = B$ se v jednodušších případech dá dokázat podle definice, tedy ukáže se shodnot prvků, obvykle touto ekvivalencí: $x \in A \iff x \in B$.

Mnohdy to ale není takto snadné a nejčastěji se místo rovnosti dokazují dvě inkluze $A \subseteq B$ a $A \subseteq B$, obvykle pomocí implikací $x \in A \implies x \in B$ a $x \in A \implies x \in B$.

Tvrzení $A \cap B = \emptyset$ lze dokázat například implikací $x \in A \implies x \notin B$, popřípadě $x \in B \implies x \notin A$, ale jsou i jiné možnosti, třeba důkaz sporem $x \in A \cap B \implies F$.

Pro úplnost (a bude se to hodit) ještě dodejme, že tvrzení $x \in A \cap B$ se dokáže tak, že ukážeme pravdivost výroku „$x \in A \wedge x \in B$“. Obdobně se tvrzení $x \in A \cup B$ dokáže tak, že ukážeme pravdivost výroku „$x \in A \vee x \in B$“.
△

S **Rozbor:** Jaký přístup zvolíme při důkazu naší věty? Nejprve potřebujeme ukázat rovnost $\mathbb{N}_{>1} = P \cup C$. Ovšem podle definice už platí $P \subseteq \mathbb{N}_{>1}$ a $C \subseteq \mathbb{N}_{>1}$ a tedy také $P \cup C \subseteq \mathbb{N}_{>1}$.

Zbývá tedy dokázat, že $\mathbb{N}_{>1} \subseteq P \cup C$. Aplikováním obecných principů z poznámky 1b.2 zjistíme, že potřebujeme dokázat následující:
a) Jestliže je $a \in \mathbb{N}$, $a \neq 1$, pak platí že a je prvočíslo nebo a je složené číslo.
Toto ukážeme rozkladem na případy, viz poznámka 1a.19.

Pro důkaz druhého požadavku zvolíme první z navržených postupů, tedy dokážeme implikaci
b) Jesliže je a složené číslo, tak to není prvočíslo.

Důkaz: a) Nechť $a \in \mathbb{N}$, $a \neq 1$. V případě, že a je prvočíslo, tak už je splněn výrok „a je prvočíslo nebo složené číslo“.

Zbývá tedy vyšetřit případ, kdy a není prvočíslo. Pak musí mít ještě jiného dělitele $l \in \mathbb{N}$ než 1 nebo a. Musí tedy platit $\underline{1 < l < a}$. Protože $l \,|\, a$, tak $\underline{a = l \cdot k}$ pro nějaké $k \in \mathbb{Z}$. Díky $l \neq 0$ můžeme použít $k = \frac{a}{l}$, z čehož pak získáme následující poznatky: Protože $0 < l < a$, tak platí $\underline{k > 1}$. A protože $l > 1$, tak platí $\underline{k < a}$. Ukázali jsme tedy, že a je číslo složené, a tedy i v tomto případě platí tvrzení „a je prvočíslo nebo složené číslo“.

b) Mějme složené číslo a. Podle definice existují $k, l \in \mathbb{N}$ tak, aby $a = kl$ a zároveň platí $1 < k < a$. To znamená, že k dělí a a přitom není rovno ani 1, ani a. Číslo a má tedy alespoň tři různé kladné dělitele a tudíž to není prvočíslo.

□

Prvočísla jsou zajímavá a užitečná, ostatně čtenář patrně ví o rozkladu na prvočísla. Studium prvočísel je součástí diskrétní matematiky a tvoří samostatný obor zvaný „teorie čísel“, který je rozsáhlý a náročný. Protože tato kniha je jen úvodem, tak si zde uvedeme jen to, co potřebujeme pro naši práci, a základy shrneme v bonusové kapitole 13.

U složených čísel je pohled přes netriviální rozklad přirozený, nicméně definice prvočísla naznačuje, že pohled očima dělitelů také může být zajímavý. Začneme otázkou, kolik jich pro dané číslo je. Může to být otázka velmi praktická, například když potřebujeme dělit určitá množství na různý počet částí. Pak oceňujeme čísla s velkým počtem dělitelů. Právě tato úvaha stála za volbou čísla 60 coby základu číselné soustavy ve starověkém Babylóně před cca 4000 lety, protože číslo 60 se dá dělit výrazně více čísly než jiná podobně velká čísla. Dodnes to přežívá u minut a stupňů. V diskrétní matematice pro nás naopak budou občas spíš užitečná čísla, která dělitelů mají málo. Co můžeme čekat?

Víme, že když je d dělitelem jistého čísla, tak je $-d$ také jeho dělitelem. Proto se pro jednoduchost v teorii zaměřujeme čistě na kladné dělitele. Základem je pozorování, že každé celé číslo a má zaručené dělitele 1 a a (fakt 1a.2). To ovšem v případě $a = 1$ znamená totéž číslo a jednička má tedy jen jednoho kladného dělitele, což je nejmenší možný počet. Prvočísla se pak poznají podle toho, že mají přesně dva různé kladné dělitele, protože pro ně už $1 \neq a$. Mimochodem, vidíme, že jednička a prvočísla se přeci jen v něčem liší.

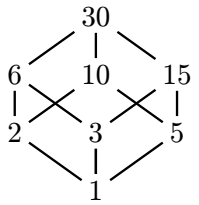
Opačným extrémem je číslo $a = 0$. Coby univerzální násobek je dělitelné všemi celými čísly, takže má nekonečně mnoho kladných dělitelů.

Čísla složená pak mají tři a více kladných dělitelů. Dalo by se čekat, že větší čísla budou mít více dělitelů, ale je to pravda jen do určité míry. Pokud se díváme na stále větší čísla a, tak porůznu potkáváme stále větší množiny kladných dělitelů. Například číslo $a = 2^n$ má n kladných dělitelů. Ovšem tento nárust není plynulý. Jak přecházíme od čísla k číslu, tak počty jejich dělitelů divoce a nepředvídatelně skáčou. Například $a = 12$ má šest kladných dělitelů, jmenovitě $1, 2, 3, 4, 6, 12$, zatímco sousední $a = 13$ jen dva.

Od otázky, kolik mají celá čísla dělitelů, se obraťme k otázce, jak množiny kladných dělitelů vypadají. Podobnou otázku si položíme také o množině kladných násobků.

Je například možné si všimnout, že když si vezmeme celé číslo a, tak jeho množina kladných dělitelů typicky obsahuje více čísel, která se někdy spolu dělí a někdy ne. To se dá vyjádřit graficky následovně: Pokud napíšeme nad sebe dvě čísla a spojíme úsečkou, tak tím říkáme, že to dolní číslo dělí to horní, což je totéž jako říct, že to horní je násobek toho dolního. Když spojovací úsečka chybí, tak mezi čísly vztah dělitelnosti není.

Příklad 1b.a (množina kladných dělitelů a násobků)**:**



Na obrázku vpravo jsme popsaným způsobem zachytili množinu všech kladných dělitelů čísla $a = 30$, což je mimochodem také množina všech kladných dělitelů čísla $a = -30$, protože každý kladný dělitel čísla 30 (včetně čísla 30 samotného) je i kladným dělitelem čísla -30. Vznikl stromeček, ve kterém jsme pro přehlednost nezaznačili úplně všechny vztahy dělitelnosti, například chybí spojnice mezi 2 a 30. My ale vidíme cestu 2–6–30 a ta tu dělitelnost kóduje. Díky větě 1a.24 totiž víme, že z $2 \mid 6$ a $6 \mid 30$ plyne $2 \mid 30$.

Vztahy dělitelnosti tedy existuje mezi každou dvojicí čísel, mezi kterými vede cesta směrem vzhůru. Pokud taková cesta není, tak také neplatí vztah dělitelnosti. Například takový vztah není mezi čísly 2 a 3. Sice existuje cesta 2–6–3, ale nevede vzhůru. Podobně není vztah dělitelnosti mezi 2 a 15.

Tento typ znázornění výborně vystihne vztah dělitelnosti a je inspirací pro obecný nástroj, který zavedeme v kapitole 6, kde se také naučíme, jak jej správně kreslit. Zatím jen podotkněme, že to může být pěkný způsob generování moderního umění.

Fakt 1a.24 nám říká také toto: Pokud je d nějaký kladný dělitel čísla a, pak také všichni dělitelé d jsou dělitelé a. To znamená, že jakmile se v našem obrázku objevilo číslo 6, tak si s sebou přivedlo svůj vlastní strom svých kladných dělitelů. To samozřejmě platí i pro ostatní dělitele.

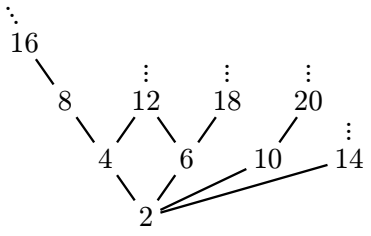
Protože je 1 univerzální dělitel, dělí také všechny kladné dělitele čísla a, což vizuálně znamená, že od každého čísla ve stromu musí vést cesta dolů až do 1. Jinak řečeno, celý strom se nutně musí dole seběhnout do kořene 1.

Víme také, že každý kladný dělitel d čísla a by měl splňovat $d \leq |a|$ a dělit $|a|$, takže nás nepřekvapuje, že se strom nahoře sbíhá do $|a|$. Ovšem ona věta 1a.26 obsahovala důležitou podmínku, že platí jen pro $a \neq 0$.

Na číslo $a = 0$ se tedy toto omezení jeho dělitelů nevztahuje a ono toho využije, protože jsme už zmínili, že množina kladných dělitelů nuly je celé $\mathbb{N}$. Budeme si na tuto výjimku muset dávat pozor. Shrňme si to podstatné, co se nám bude hodit dále.

- Množina kladných dělitelů celého čísla je vždy neprázdná podmnožina $\mathbb{N}$ a obsahuje číslo 1, které ji omezuje zdola.
- Pro $a \neq 0$ je množina kladných dělitelů čísla a vždy konečná a omezená shora číslem $|a|$.
- Množina kladných dělitelů čísla $a = 0$ je $\mathbb{N}$.

Teď se podíváme, jak vypadá množina kladných násobků celého čísla a. My víme, že každý násobek musí mít tvar ak pro $k \in \mathbb{Z}$, takže množina kladných násobků je přesně tato: $\{|a|k : k \in \mathbb{N}\}$. Na rozdíl od množiny dělitelů tedy máme k dispozici jednoduchý popis množiny kladných násobků. V rámci této množiny zase někdy máme vztah dělitelnosti a někdy ne, například násobek $2a$ dělí násobek $12a$, ale násobek $2a$ nedělí násobek $3a$ ani naopak. Opět vznikne zajímavá struktura.



Napravo vidíme část stromu kladných násobků čísla 2, který je také stromem kladných násobků čísla -2, zakreslili jsme jej až po dvacítku. Asi si umíme představit, jak pokračuje dále do výšky a šířky. Všimneme si něčeho zajímavého? Protože strom obsahuje násobky a, tak je $|a|$ všechny dělí a proto se všechny cesty musejí dole sbíhat do společného kořene $|a|$.

Zase platí, že je-li m násobkem a, tak i všechny jeho násobky jsou násobkem a. Takže v tom stromě například vidíme podstrom všech kladných násobků čísla 4.

Je asi jasné, že tento strom není shora omezený, násobky se táhnou až k nekonečnu. Tato podoba stromu násobků je typická, ale na základě předchozí zkušenosti víme, že bychom se měli podívat na nulu.

Jediným násobkem nuly je nula, což není kladné číslo. Nula tedy nemá žádné kladné násobky. Nabízí se otázka, jestli se tedy raději nebavit o nezáporných násobcích, ale tím by se nám zase vyskytly problémy jinde. Nezbývá než se smířit s následujícím stavem věcí:

- Množina kladných násobků nenulového celého čísla a je nekonečná množina zdola omezená číslem $|a|$.
- Množina kladných násobků čísla $a = 0$ je prázdná.

△

Ještě zajímavější to bude, když si vezmeme dvě čísla.

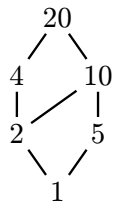
Definice.
Nechť $a, b \in \mathbb{Z}$.
Číslo $d \in \mathbb{N}$ je **společný dělitel** (**common divisor**) čísel a, b, jestliže $d \mid a$ a $d \mid b$.
Číslo $m \in \mathbb{N}$ je **společný násobek** (**common multiple**) čísel a, b, jestliže $a \mid m$ a $b \mid m$.

Například číslo 1 je určitě společným dělitelem čísel 40 a 60, zatímco $40 \cdot 60 = 2400$ je určitě jejich společným násobkem. Čtenář ale asi tuší, že nás budou zajímat méně triviální odpovědi, třeba 20 jako společný dělitel a 120 jako společný násobek oněch dvou čísel. Abychom se tam dostali, podíváme se, jak množiny společných dělitelů

a společných násobků vypadají. Nejprve si ale všimneme, že už nemusíme psát „společní kladní dělitelé“, protože jsme v definici požadavek na kladnost zapracovali do názvu „společní dělitelé“ tím $d \in \mathbb{N}$, podobně pro společné násobky.

Příklad 1b.b (společní dělitelé a násobky čísel)**:**

Z definice vyplývá, že množinu společných dělitelů získáme tak, že pronikneme množinu kladných dělitelů čísla a s množinou kladných dělitelů čísla b, obdobně pro násobky. Můžeme tedy využít poznatků z příkladu 1b.a.



Pro ilustraci si ukážeme stromeček společných dělitelů čísel 40 a 60. Je v mnohém typický. Víme už, že všechny množiny kladných dělitelů obsahují číslo 1, kterým jsou zdola omezeny a do kterého se sbíhají. Musí to platit i pro jejich průniky a náš strom to plní. Dělitelé nenulových čísel jsou shora omezeni, což omezuje i náš strom, v tomto případě danými čísly 40 a 60. Ta se ovšem tentokráte mezi společnými děliteli nenajdou.

V obrázku je ještě jedna zajímavá věc, celý stromeček se sbíhá i nahoře do špičky 20. Není jasné, zda je to náhoda nebo pravidlo, a časem se k tomu vrátíme.

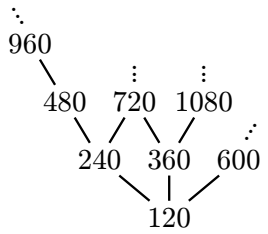
Pro nenulová čísla $a, b \in \mathbb{Z}$ víme, že jejich společní dělitelé d jsou shora omezeny čísly $|a|$ a také $|b|$. Dá se to zachytit nerovností $d \leq \min(|a|, |b|)$.

Co když se nám mezi čísla a, b dostane nula, jejíž množina kladných dělitelů je celé $\mathbb{N}$? Pokud je ve dvojici jen jedna, tak její množinu $\mathbb{N}$ budeme pronikat s množinou M kladných dělitelů pro to druhé nenulové číslo. Protože $M \cap \mathbb{N} = M$, vidíme, že množina společných dělitelů čísel 0 a $b \neq 0$ je stejná jako množina kladných dělitelů čísla b, což znamená, že je shora omezená (číslem $|b|$). Máme tedy případ podobný tomu výše.

Jediný problém nastane, pokud hledáme společné dělitele čísel 0 a 0, pak dostáváme $\mathbb{N} \cap \mathbb{N} = \mathbb{N}$. Shrnuto:

• Pokud je alespoň jedno z čísel a, b nenulové, tak množina jejich společných dělitelů je neprázdná, konečná a shora omezená. Společní dělitelé nenulových čísel a, b jsou omezeny shora číslem $\min(|a|, |b|)$, společní dělitelé čísla 0 a nenulového b jsou omezeny shora číslem $|b|$.

• Množina společných dělitelů čísel $0, 0$ je $\mathbb{N}$.



Množina společných násobků čísel a, b vznikne proniknutím individuálních množin kladných násobků čísla a a čísla b. Vpravo vidíme kousek stromu společných násobků čísel 40 a 60. Co se dá čekat? Určitě bychom čekali, že takový strom bude shora neomezený, ale zdola ohraničený danými dvěma čísly (v absolutní hodnotě).

Ani v tomto případě nečekáme, že by daná čísla 40 a 60 byla v naší množině společných násobků, ale přesto má naše množina společný kořínek, jmenovitě 120. I zde se nabízí otázka, zda jde o pravidlo, což se časem dozvíme.

Jak tyto vlastnosti ovlivní případné nuly? Víme, že množina kladných násobků nuly je prázná, což má při průniku okamžitý dopad. U násobků tedy stačí, aby jen jediné číslo z a, b byla nula, a už bude množina společných násobků prázdná.

• Pokud jsou čísla a, b nenulová, tak množina jejich společných násobků je neprázdná a zdola omezená číslem $\max(|a|, |b|)$.

• Pokud je alespoň jedno z čísel a, b nulové, tak množina jejich společných násobků je prázdná.

Pro společné dělitele a společné násobky tedy máme případ typický a pak případ speciální, přičemž ten speciální případ je pokaždé trochu jiný. Musíme si na to dát pozor.

△

Protože za typických podmínek je množina společných dělitelů neprázdná a konečná, lze najít její maximum, viz kapitola 6b. Tam se také dozvíme, že pro neprázdnou množinu násobků lze najít minimum. To ukazuje, že následující definice vždy poskytne žádané číslo.

Definice.
Nechť $a, b \in \mathbb{Z}$.
Definujeme jejich **největší společný dělitel** (**greatest common divisor**), značeno $\gcd(a, b)$, jako největší prvek množiny jejich společných dělitelů, pokud je alespoň jedno z a, b nenulové. Jinak definujeme $\gcd(0, 0) = 0$.

Definujeme jejich **nejmenší společný násobek** (**least common multiple**), značeno $\operatorname{lcm}(a, b)$, jako nejmenší prvek množiny jejich společných násobků, pokud jsou obě a, b nenulové. Jinak definujeme $\operatorname{lcm}(a, 0) = \operatorname{lcm}(0, b) = 0$.

Existují i konkurenční značení, ale ta naše jsou nejpoužívanější. Oba pojmy se dají zobecnit na více čísel, viz cvičení 1b.12.

Po našich pozorováních výše nepřekvapí, že případy $\gcd(0,0)$ a $\operatorname{lcm}(0,b)$ bylo třeba definovat speciálním způsobem. Hodnoty, které jsme pro speciální případy vybrali, nejsou jediné, na které lze narazit, ale jsou s přehledem nejpopulárnější. Mají podstatnou výhodu, že většina tvrzení o gcd a lcm pak platí pro všechna celá čísla, takže při jejich formulování nebudeme muset vyjmenovávat speciální případy. V důkazech ale ty speciální případy budeme samozřejmě muset dělat zvlášť.

Poznamenejme, že požadavek „obě a,b nenulové“ pro typickou situaci u lcm se standardně zapisuje $a,b\neq 0$, ale existuje i trikové vyjádření $a\cdot b\neq 0$. Opačný požadavek „alespoň jedno z a,b je nulové“ (speciální případ z definice lcm) se pak přirozeně vyjádří $a\cdot b=0$. U gcd se speciální případ „obě a,b jsou nulové“ elegantně zapíše $a=b=0$. Typický případ to má těžší, můžeme zkusit doslovný přepis $a\neq 0\vee b\neq 0$, dá se také zkusit třeba $\max(|a|,|b|)>0$, ale to už by čtenář musel luštit.

Příklad 1b.c: Uvažujme čísla $a=-8$ a $b=12$. Když si sepíšeme krátký seznam kladných dělitelů čísla 8 a ověříme, který z nich také dělí 12, tak snadno zjistíme, že společní dělitelé 8 a 12 tvoří množinu $\{1,2,4\}$. Její největší prvek dává $\gcd(-8,12)=4$.

Množina společných násobků začíná $\{24,48,92,\dots\}$, takže $\operatorname{lcm}(-8,12)=24$. Jak se na tu množinu přišlo? Popravdě řečeno podvodem, využili jsme to, co se teprve dozvíme, protože tak snadno jako u těch dělitelů to nejde.

△

Nejprve se přesvědčíme, že speciální volby v definici pořád vyhovují základnímu požadavku.

Fakt 1b.3.
Nechť $a,b\in\mathbb{Z}$. Pak $\gcd(a,b)$ dělí a i b a $\operatorname{lcm}(a,b)$ je násobkem a i b.

Důkaz: 1) $\gcd(a,b)$: Pokud je alespoň jedno z čísel a,b nenulové, pak $\gcd(a,b)$ je největším prvkem množiny společných dělitelů čísel a,b, takže je obě dělí.

V případě $a=b=0$ definice dává $\gcd(a,b)=0$ a nula opravdu dělí $a=0$ i $b=0$, viz fakt 1a.2.

2) $\operatorname{lcm}(a,b)$: Pokud $ab\neq 0$, pak $\operatorname{lcm}(a,b)$ je nejmenším prvkem množiny společných násobků čísel a,b, takže je násobkem obou.

Pokud je alespoň jedno z čísel nulové, řekněme $a=0$, tak $\operatorname{lcm}(a,b)=0$, což je násobek libovolného čísla, tedy i a a b.

□

1b.4 Poznámka: Tato definice má na pohled odlišnou podobu od předchozích. Nedefinujeme tam pojmy pomocí testů, ale natvrdo určujeme hodnoty. To je obzvláště patrné u těch speciálních případů, ale vypadá to tak i u těch typických, kde pracujeme s množinami společných dělitelů. Tam to je ale komplikovanější. Jak vlastně poznáme největší a nejmenší prvek? To oficiálně probereme až v kapitole 6b, ale měli bychom s tím umět pracovat již nyní a nakonec zase skončíme u testu.

Aby bylo číslo g největším prvkem množiny společných dělitelů čísel a,b (a tedy jejich gcd), tak musí splňovat tyto podmínky:
a) g musí v této množině ležet;
b) prvky této množiny musí být menší nebo rovny g.

Konkrétněji, číslo g je $\gcd(a,b)$ právě tehdy, když platí následující:
a) g je společný dělitel čísel a,b;
b) každý společný dělitel d čísel a,b splňuje $d\leq g$.

Formálně zapsáno, kandidát na $\gcd(a,b)$ musí splnit následující test:
a) $g\,|\,a$, $g\,|\,b$;
b) $\forall d\in\mathbb{N}$: $(d\,|\,a\wedge d\,|\,b)\implies d\leq g$.

Tento způsob identifikace největšího společného dělitele testem se někdy hodí v důkazech. Ukážeme si proto i podmínku, která v případě $ab\neq 0$ rozpozná, že číslo l je $\operatorname{lcm}(a,b)$:
a) l je společný násobek čísel a,b;
b) každý společný násobek m čísel a,b splňuje $l\leq m$.

△

Máme nové pojmy, takže obvyklá otázka: Co od nich můžeme čekat? Z diskuse o podobě množin společných dělitelů a násobků okamžitě dostáváme následující tvrzení.

Fakt 1b.5.
Nechť $a, b \in \mathbb{Z}$, $a, b \neq 0$. Pak $1 \leq \gcd(a,b) \leq \min(|a|,|b|)$ a $\operatorname{lcm}(a,b) \geq \max(|a|,|b|)$.

Bohužel zrovna tyto užitečné odhady neplatí pro speciální případy, takže jsme se v tvrzení museli omezovat. Dají se vymyslet podobné odhady, které už platí pro libovolné $a, b \in \mathbb{Z}$, viz cvičení 1b.5, ale ty jsou slabší, takže nejsou moc užitečné. U dalších poznatků už se projeví rozumná volba speciálních hodnot a budeme moci dělat obecná tvrzení, což hned uvidíme.

Vzhledem k tomu, že u dělitelnosti znaménka nehrají roli, dá se podobné chování čekat i u nových pojmů.

Fakt 1b.6.
Nechť $a, b \in \mathbb{Z}$. Pak $\gcd(a,b) = \gcd(|a|,|b|)$ a $\operatorname{lcm}(a,b) = \operatorname{lcm}(|a|,|b|)$.

S **Rozbor:** V tomto tvrzení máme ukázat rovnost typu $\gcd(x,y) = \gcd(u,v)$. Protože obě entity v porovnání vznikly obdobným postupem, ukáže se jako nejlepší přístup tento postup následovat a ukázat, že pro obě dvojice skončí stejným výsledkem. Obdobně budeme postupovat pro největší společné násobky.

Tento přístup ovšem funguje jen pro typické případy, pro speciální hodnoty je definice jiná a musí se udělat zvlášť.

Důkaz (rutinní)**:** Dáno $a, b \in \mathbb{Z}$.

1) $\gcd(a,b)$: Případ $a = b = 0$: Pak díky $|0| = 0$ platí $\gcd(|0|,|0|) = \gcd(0,0)$.

Případ $a \neq 0 \vee b \neq 0$: Každé číslo $d \in \mathbb{N}$ splňující $d \mid a$, $d \mid b$ musí podle věty 1a.17 splňovat i $d \mid |a|$, $d \mid |b|$ a naopak. Množina společných dělitelů čísel a, b tedy obsahuje stejná čísla jako množina společných dělitelů čísel $|a|, |b|$, neboli jde o stejnou množinu. Proto se musejí rovnat i největší prvky těchto množin.

2) $\operatorname{lcm}(a,b)$: Případ $a = 0$: Podle definice $\operatorname{lcm}(0,|b|) = 0 = \operatorname{lcm}(0,b)$.

Případ $b = 0$ je obdobný, případ $a, b \neq 0$ se dělá podobně jako pro $\gcd(a,b)$.

□

Praktický dopad je, že stačí umět najít $\gcd(a,b)$ a $\operatorname{lcm}(a,b)$ pro nezáporná celá čísla. Kromě znamének nás ještě nemusí zajímat další věc, a to je pořadí.

Fakt 1b.7.
Nechť $a, b \in \mathbb{Z}$. Pak $\gcd(a,b) = \gcd(b,a)$ a $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a)$.

Důkaz: Nechť $a, b \in \mathbb{Z}$.

1) $\gcd(a,b)$: Případ $a = b = 0$: Pak prohozením nul získáme

$$\gcd(a,b) = \gcd(0,0) = \gcd(0,0) = \gcd(b,a).$$

Případ $a \neq 0 \vee b \neq 0$: Množina společných dělitelů čísel a, b obsahuje čísla $d \in \mathbb{N}$ splňující $d \mid a$ a $d \mid b$, což je totéž jako splňovat $d \mid b$ a $d \mid a$. Tato množina je proto rovna množině společných dělitelů čísel b, a a tedy mají i shodné největší prvky.

2) Rovnost $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a)$ se dokáže obdobně.

□

Definice nám poskytla výsledky pro speciální případy. Přidáme několik dalších zajímavých situací.

Fakt 1b.8.
Nechť $a \in \mathbb{Z}$. Pak $\gcd(0,a) = |a|$, $\gcd(a,a) = |a|$ a $\operatorname{lcm}(a,a) = |a|$.

Důkaz: Dáno $a \in \mathbb{Z}$.

1) $\gcd(0,a)$: Případ $a = 0$: Podle speciální definice platí

$$\gcd(0,a) = \gcd(0,0) = 0 = |a|.$$

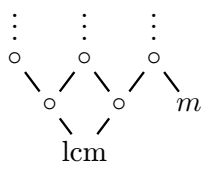
Případ $a \neq 0$: Použijeme poznámku 1b.4 k důkazu, že $|a| = \gcd(0,a)$. Evidentně platí $|a| \mid 0$ a $|a| \mid a$. Zbývá ověřit poslední podmínku. Vezměme společný dělitel $d \in \mathbb{N}$ čísel 0 a a. Pak $d \mid a$ a $a \neq 0$, proto podle věty 1a.26 platí $d \leq |a|$.

2,3) Důkazy pro $\gcd(a,a)$ a $\operatorname{lcm}(a,a)$ jsou obdobné.

□

Podobné důkazy nám poskytnou ještě další jednoduché situace, kdy výsledky hned vidíme, viz cvičení 1b.4.

Víme, že pro $a, b \neq 0$ je $\operatorname{lcm}(a, b)$ nejmenším číslem ve stromě společných násobků. Je tedy ve spodním patře, ale to ještě nezaručuje, že bude společným kořenem všech dělitelnostních cestiček. My víme, že když je číslo m násobkem čísla $\operatorname{lcm}(a, b)$, které je pro změnu násobkem a a b, tak automaticky je i m násobkem čísel a a b. To tedy znamená, že celý strom kladných násobků čísla $\operatorname{lcm}(a, b)$ musí být součástí stromu společných násobků čísel a, b.



Zatím ale nevíme, zda takto vznikne celý strom násobků čísel a, b. Podle našich dosavadních znalostí by se mohlo stát, že se najde nějaký společný násobek m čísel a, b, který ale není dělitelný číslem $\operatorname{lcm}(a, b)$, což v našem obrázku znamená, že of m nevede cesta dolů k $\operatorname{lcm}(a, b)$. Náš strom by pak neměl jeden společný kořen.

Následující tvrzení ukazuje, že to není možné, a v každém stromě společných násobků vedou od všech míst cesty do společného kořene $\operatorname{lcm}(a, b)$. To ukazuje, že $\operatorname{lcm}(a, b)$ je nejmenší nejen vzhledem ke vztahu nerovnosti, ale také vzhledem k uspořádání dělitelností, viz kapitola 6b.

Věta 1b.9.
Nechť $a, b \in \mathbb{Z}$. Každý společný násobek a a b je dělitelný číslem $\operatorname{lcm}(a, b)$.

S Rozbor: Jako obvykle budeme muset zvlášť pojednat speciální případ, který bude jako obvykle snadný. Pro typický případ se nenabízí zjevná cesta, tako tomu bylo u snadných implikací dříve. Je to náročnější matematický důkaz, který vyžaduje inspiraci a nápad. Nedá se tedy očekávat, že by na to přišel typický čtenář sám, ale měl by být schopen sledovat, kudy se důkaz ubírá a jak dává smysl.

Jedno pomocné tvrzení se bude dokazovat sporem, viz poznámka 1a.30.

Důkaz (dobrý, poučný)**:** Mějme čísla $a, b \in \mathbb{Z}$ a předpokládejme, že $m \in \mathbb{N}$ je jejich společný násobek.

1) Případ $ab = 0$. Pak žádné společné násobky neexistují a tvrzení triviálně platí.

2) Případ $ab \neq 0$. Protože je m společný násobek a $\operatorname{lcm}(a, b)$ je mezi společnými násobky nejmenší, tak $\operatorname{lcm}(a, b) \leq m$.

Protože $\operatorname{lcm}(a, b) \neq 0$, můžeme aplikovat větu o dělení (1a.29) a najít $q, r \in \mathbb{Z}$ takové, že $m = q \operatorname{lcm}(a, b) + r$ a $0 \leq r < \operatorname{lcm}(a, b)$.

Máme $r = m - q \operatorname{lcm}(a, b)$. Podle předpokladu $a \mid m$, podle definice $a \mid \operatorname{lcm}(a, b)$, proto podle důsledku 1a.23 také a dělí r. Obdobně ukážeme, že i b dělí r.

Ukážeme sporem, že $r = 0$.

Předpokládejme opak, tedy $r \neq 0$. Ovšem coby zbytek po dělení nemůže r být záporný, musel by tedy splňovat $r > 0$. Také jsme ukázali, že r je násobkem a i b, takže by to byl společný násobek a, b. Protože $\operatorname{lcm}(a, b)$ je mezi společnými násobky nejmenší, muselo by platit $\operatorname{lcm}(a, b) \leq r$. Ovšem r coby zbytek po dělení číslem $\operatorname{lcm}(a, b)$ také splňuje $r < \operatorname{lcm}(a, b)$. Spojením dostáváme nemožnou nerovnost $r < r$, což je onen kýžený spor.

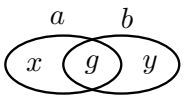
To ukazuje, že i náš předpoklad $r \neq 0$ musí být nepravdivý. Potvrdili jsme, že $r = 0$ a tedy $m = q \operatorname{lcm}(a, b)$, kde $q \in \mathbb{Z}$, neboli $\operatorname{lcm}(a, b)$ dělí m.

□

Již dříve jsme si rozmysleli, že každý kladný násobek $\operatorname{lcm}(a, b)$ patří do množiny společných násobků čísel a, b. Teď jsme dokázali i opačný směr, takže jde o jednu a tutéž množinu. To nám umožňuje efektivně zapsat, jak množina společných násobků čísel $a, b \neq 0$ vypadá: $\{\operatorname{lcm}(a, b) \cdot k : k \in \mathbb{N}\}$.

Rádi bychom obdrželi obdobu věty 1b.9 pro $\gcd(a, b)$, ale na to budeme nejprve muset vytvořit správné nástroje.

Pocitově $\gcd(a, b)$ obsahuje vše, co mají a, b společné z pohledu faktorizace. V obrázku je tato společná část označena g. Máme $a = gx$ a $b = gy$, kde $x, y \in \mathbb{Z}$. Na druhou stranu $\operatorname{lcm}(a, b)$ je to nejmenší číslo, které ještě obsáhne a i b. Z obrázku by se zdálo, že jej můžeme získat jako gxy.



Je to pravda, ale je zvykem to vyjádřit jinak.

$$\operatorname{lcm}(a, b) = gxy = \frac{g^2 xy}{g} = \frac{(gx)(gy)}{g} = \frac{ab}{\gcd(a, b)}.$$

Jako obvykle preferujeme kvůli možným nulám součinovou verzi, výraz ještě upravíme s ohledem na možná záporná čísla. I toto tvrzení má nerutinní důkaz založený na nápadu.

Věta 1b.10.
Nechť $a, b \in \mathbb{Z}$. Pak $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = |a| \cdot |b|$.

Důkaz (dobrý, poučný)**:** 1) Případ $a, b > 0$: Pak také $\gcd(a, b) \neq 0$ a $\operatorname{lcm}(a, b) \neq 0$.

a) Uvažujme číslo $m = \frac{a \cdot b}{\gcd(a,b)}$. Protože $\gcd(a,b)$ dělí b, platí $b = \gcd(a,b)k$ pro nějaké $k \in \mathbb{Z}$. Proto

$$m = \frac{a \gcd(a,b)k}{\gcd(a,b)} = ak,$$

tedy m je celé číslo a také je násobkem a. Obdobně ukážeme, že m je násobkem b, také $m > 0$ a tedy m je společný násobek a, b. Protože $\operatorname{lcm}(a,b)$ je mezi nimi nejmenší, musí platit $\operatorname{lcm}(a,b) \leq m$. Po dosazení dostáváme, že $\gcd(a,b) \cdot \operatorname{lcm}(a,b) \leq ab$.

b) Uvažujme číslo $d = \frac{ab}{\operatorname{lcm}(a,b)}$. Protože je ab společným násobkem a, b, musí dle faktu 1b.9 být také násobkem $\operatorname{lcm}(a,b)$ a d je tedy přirozené číslo.

Protože $\operatorname{lcm}(a,b)$ je násobkem b, platí $\operatorname{lcm}(a,b) = bl$ pro nějaké $l \in \mathbb{Z}$. Ze vzorce pro d pak máme

$$a = \frac{d \operatorname{lcm}(a,b)}{b} = \frac{dbl}{b} = dl,$$

tedy d dělí a. Obdobně ukážeme $d \mid b$ a platí $d \in \mathbb{N}$, takže d je společný dělitel a, b. Protože $\gcd(a,b)$ je mezi nimi největší, musí platit $d \leq \gcd(a,b)$. Po dosazení dostáváme, že $ab \leq \gcd(a,b) \operatorname{lcm}(a,b)$.

Spojením nerovností z a), b) máme $\operatorname{lcm}(a,b) \cdot \gcd(a,b) = ab$, což je $|a| \cdot |b|$ díky $a, b > 0$.

2) Případ $a, b \neq 0$: Pak $|a| > 0$ a $|b| > 0$, podle případu 1) tedy $\gcd(|a|,|b|) \operatorname{lcm}(|a|,|b|) = |a| \cdot |b|$. Podle faktu 1b.6 pak $\gcd(|a|,|b|) \operatorname{lcm}(|a|,|b|) = \gcd(a,b) \operatorname{lcm}(a,b)$.

3) Případ $a = 0$: Podle definice lcm a faktu 1b.8 platí

$$\gcd(0,b) \operatorname{lcm}(0,b) = |b| \cdot 0 = |a| \cdot |b|.$$

Případ $b = 0$ se dokáže obdobně.

□

Důkazů existuje více, mnohdy používají Bezoutovu identitu či její důsledek 1b.16, aniž by byly znatelně kratší. Na předvedeném důkazu se mi líbí právě to, že nepotřebuje žádnou další teorii a vystačí si s prostými úvahami o dělitelnosti, další eleganci mu dodává jakási symetrie mezi oběma hlavními částmi.

Tato věta nám dává vzorec pro výpočet nejmenšího společného násobku, v počítači je ale samozřejmě lepší namísto $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$ používat $\operatorname{lcm}(a,b) = \frac{a}{\gcd(a,b)}\, b$ či $\operatorname{lcm}(a,b) = \frac{b}{\gcd(a,b)}\, a$, protože tento postup nevyžaduje ukládání velkého čísla ab.

Obrázek s komponentami, který inspiroval předcházející větu, je také inspirací pro hledání $\gcd(a,b)$ a $\operatorname{lcm}(a,b)$ pomocí prvočísel, kdy hledáme společné, popřípadě chceme zahrnout vše.

Příklad 1b.d: Uvažujme $a = 108$, $b = 408$. Provedeme prvočíselný rozklad.

$$108 = 2^2 \cdot 3^3,$$
$$408 = 2^3 \cdot 3 \cdot 17.$$

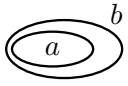
Největší společný dělitel získáme zahrnutím všeho, co je společné, $\gcd(100, 408) = 2^2 \cdot 3 = 12$. Nejmenší společný násobek vznikne, když od každého prvočísla vezmeme největší mocninu, proto $\operatorname{lcm}(108, 408) = 2^3 \cdot 3^3 \cdot 17 = 3672$.

Ke stejnému výsledku se dobereme podle obrázku výše. Společná část je zjevně $g = 2^2 \cdot 3$, takže máme $108 = g \cdot 3^2$ a $408 = g \cdot 2 \cdot 17$. Podle značení z obrázku je $x = 9$ a $y = 34$ a tedy $\operatorname{lcm}(108, 408) = 12 \cdot 8 \cdot 34$.

△

Tento postup je vcelku funkční pro malá čísla, ale pro velká čísla se stává nepoužitelným, protože prvočíselný rozklad je jednou z výpočetně nejnáročnějších úloh i pro počítače. Další nevýhodou je, že tento postup neposkytne jistou bonusovou informaci, kterou brzy budeme velmi potřebovat. Proto v sekci 1b.27 vyvineme jiný způsob.

Intuitivně vnímáme $\gcd(a,b)$ jako největší možnou společnou část čísel a, b. Máme také intuitivní představu o pojmu dělitelnosti, třeba tu obláčkovou vpravo. Když to dáme dohromady, tak nám z toho vyjde další situace, kdy už $\gcd(a,b)$ rovnou vidíme.

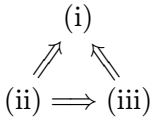


Věta 1b.11.
Nechť $a, b \in \mathbb{Z}$. Pak jsou následující tvrzení ekvivalentní:
(i) a dělí b;
(ii) $\gcd(a,b) = |a|$;
(iii) $\operatorname{lcm}(a,b) = |b|$.

M **1b.12 Poznámka:** Formálně vzato věta tvrdí, že platí následující ekvivalence:

$$\text{(i)} \iff \text{(ii)}, \qquad \text{(i)} \iff \text{(iii)}, \qquad \text{(ii)} \iff \text{(iii)}.$$

Každá z nich reprezentuje dvě implikace, ale naštěstí nebude třeba dokazovat šest implikací. Bude stačit propojit daná tři tvrzení jedním cyklem (kolotočem), například tím na obrázku napravo, a ostatní implikace již automaticky platí. Kupříkladu pravdivost implikace (ii) $\implies$ (i) se pak odvodí dokázanými implikacemi (ii) $\implies$ (iii) $\implies$ (i).



△

S **Rozbor:** Každou z potřebných implikací dokážeme jiným způsobem. Při důkazu (i) $\implies$ (ii) máme potvrdit, že v případě $a \mid b$ je $\gcd(a,b)$ rovno jistému číslu. To je přesně ten typ situace, pro kterou jsme si rozmysleli test v poznámce 1b.4.

V porovnání s posledními dvěma důkazy je tento snažší, protože nevyžaduje inspiraci, všechny kroky se nabízejí.

Důkaz (poučný)**:** 1) (i) $\implies$ (ii): Předpokládejme, že $a \mid b$.

Případ $a = 0$: Podle předpokladu $b = ak$ pak $b = 0$ a máme

$$\gcd(a,b) = \gcd(0,0) = 0 = |a|.$$

Případ $a \neq 0$: Ukážeme, že číslo $|a|$ splňuje požadavky na $\gcd(a,b)$.

a) Podle předpokladu $a \mid b$, podle faktu 1a.2 $a \mid a$. Díky větě 1a.17 pak $|a| \mid b$ a $|a| \mid a$, také $|a| \in \mathbb{N}$ a tedy $|a|$ je společným dělitelem čísel a, b.

b) Nechť d je nějaký společný dělitel a, b. Pak $d \mid b$ a $d \mid a$, díky $a \neq 0$ z věty 1a.26 plyne $d \leq |a|$. Takže $|a|$ je mezi společnými děliteli největší.

2) (ii) $\implies$ (iii): Předpokládejme, že $\gcd(a,b) = |a|$. Podle věty 1b.10 pak

$$|a| \cdot \operatorname{lcm}(a,b) = |a| \cdot |b|.$$

Jestliže $a \neq 0$, pak zkrácením vyjde $\operatorname{lcm}(a,b) = |b|$.

Jestliže $a = 0$, pak $\gcd(a,b) = \gcd(0,b) = |b|$, což je podle předpokladu rovno $|a|$. Máme tedy $a = b = 0$ a proto $\operatorname{lcm}(a,b) = \operatorname{lcm}(0,0) = 0 = |b|$.

3) (iii) $\implies$ (i): Předpokládejme, že $\operatorname{lcm}(a,b) = |b|$. Pak podle faktu 1b.3 musí být $|b|$ násobkem a a tedy dle věty 1a.17 a dělí b.

□

Směr (i) $\implies$ (ii) lze dokázat více způsoby, oblíbené jsou přístupy pomocí mocných vět, které paradoxně bývají někdy delší a komplikovanější, viz cvičení 1b.7. Ve cvičení 1b.6 si tento směr přeformulujeme a rozšíříme.

Poznámka: Vypozoroval jsem, že pro některé lidi je v důkazu bodu b) příjemnější použít nepřímý důkaz, tedy dokazují obměnu: Jestliže d splňuje $d > |a|$, tak nemůže být společným dělitelem a, b. Využijí k tomu důsledek 1a.27.

△

Definice nám poskytla $\gcd(a,b)$ nikoliv ve formě algebraického vzorce, ale jako výsledek postupu. To působí komplikace ve výpočtech i důkazech. Tento nedostatek napravuje následující tvrzení.

Věta 1b.13. (Bezoutova věta/rovnost/identita) (Bezout's identity)
Nechť $a, b \in \mathbb{Z}$. Pak existují čísla $A, B \in \mathbb{Z}$ taková, že $\gcd(a,b) = Aa + Bb$.

Víme například, že $\gcd(24,60) = 12$, a uhodneme $12 = 3 \cdot 24 + (-1) \cdot 60$. Je ovšem také možné zkusit třeba $12 = (-2) \cdot 24 + 1 \cdot 60$. Bezoutova věta neříká, že by byla jen jediná možná kombinace. Jak uvidíme v kapitole 3, takových vyjádření existuje dokonce nekonečně mnoho.

M **1b.14 Poznámka:** Ve světě matematiky často vytváříme nové objekty z původních a obvykle preferujeme, aby se tak dělo jednoduššími operacemi. Snad nejpříjemnější jsou sčítání a násobení číslem, kdy z objektů $\heartsuit, \diamondsuit$ vytvoříme $\alpha\heartsuit + \beta\diamondsuit$ (pokud tedy dotyčné objekty takové operace připouštějí). Výslednému objektu pak říkáme lineární kombinace vstupních dat. Lineárními kombinacemi se zabývá zejména obor lineární algebra, který má přesah do mnoha dalších oborů matematiky, což poznáme i v některých dalších kapitolách.

Důsledek 1a.23 lze shrnout do věty, že když a dělí dvě čísla, tak už dělí i jejich libovolnou celočíselnou lineární kombinaci. Bezoutova věta nám říká, že $\gcd(a,b)$ lze získat jako celočíselnou lineární kombinaci čísel a, b. To je luxusní.

△

Když je věta pojmenována podle nějakého matematika, tak je to obvykle znamení, že je důležitá a že nebylo snadné ji získat. Důkaz Bezoutovy věty splňuje tato očekávání a rozhodně není rutinní. Na druhou stranu je pořád veden podle hlavních zásad a čtenář by měl být schopen sledovat, co a jak se děje.

Důkaz (dobrý, poučný)**:** Případ $a = b = 0$: Pak $\gcd(0,0) = 0 = 0 \cdot a + 0 \cdot b$. Dále tedy budeme předpokládat, že alespoň jedno a a, b je nenulové. Pak se $\gcd(a,b)$ určuje pomocí množiny společných dělitelů.

Uvažujme množinu $M = \{Aa + Bb : A, B \in \mathbb{Z},\ Aa + Bb > 0\}$, tedy všechna kladná čísla, která lze dostat jako celočíselné lineární kombinace a, b. Pak evidentně $M \neq \emptyset$, třeba $|a| + |b| \in M$, protože toto číslo dostaneme sečtením $s_a a + s_b b$ pro vhodně zvolená $s_a, s_b = \pm 1$. Je to neprázdná podmnožina $\mathbb{N}$, proto dle principu dobrého uspořádání (6b.14, viz předchozí diskuse) existuje její nejmenší prvek c. Podle definice M musel vzniknout jako $c = A_c a + B_c b$ pro nějaká $A_c, B_c \in \mathbb{Z}$. Tvrdíme, že $c = \gcd(a,b)$.

1) Protože $\gcd(a,b)$ dělí a i b, tak podle důsledku 1a.23 dělí i c. Díky $c > 0$ to podle věty 1a.26 znamená, že $\gcd(a,b) \leq c$.

2) Ukážeme, že c je společný dělitel a a b.

Nejprve sporem ukážeme, že c dělí a. Předpokládejme opak. Pak $r = a \bmod c > 0$. Platí $a = qc + r$ pro něaké $q \in \mathbb{Z}$, takže

$$r = a - qc = a - q(A_c a + B_c b) = (1 - qA_c)a + qB_c b,$$

tedy r je celočíselná lineární kombinace čísel a, b, která je kladná a tedy $r \in M$. Protože je c nejmenší v M, musí platit $c \leq r$, ale coby zbytek při dělení c musí r splňovat $r < c$, což je spor. Dokázali jsme, že $c \mid a$.

Obdobně dokážeme, že $c \mid b$, coby kladné číslo je to tedy společný dělitel a, b.

Protože je $\gcd(a,b)$ mezi společným děliteli největší, musí podle 2) platit $c \leq \gcd(a,b)$. Spolu s 1) dostáváme, že $c = \gcd(a,b)$, tedy $\gcd(a,b) = A_c a + B_c b$.

□

Hlavní trik použitý v důkazu se někdy hodí, vypíchneme si jej:

Důsledek 1b.15.
Nechť $a, b \in \mathbb{Z}$. Jestliže $a \neq 0$ nebo $b \neq 0$, tak $\gcd(a,b)$ je nejmenší kladné číslo, které lze získat jako $Aa + Bb$ pro nějaká $A, B \in \mathbb{Z}$.

Bezoutovu identitu budeme výrazně používat v teorii, ale také v aplikacích. Ovšem hledat ty „Bezoutovy koeficienty“ A, B postupem v důkazu (či tomto důsledku) není perspektivní, takže to je také úkol pro sekci 1b.27. Zatím se podíváme, co nám Bezoutova věta pomůže zjistit o největším společném děliteli.

Začneme návratem k otázce, jestli se strom společných dělitelů musí nutně celý sbíhat do jednoho vrcholu (viz příklad 1b.b). Odpověď zní, že ano.

Věta 1b.16.
Nechť $a, b \in \mathbb{Z}$. Jestliže je d společný dělitel a, b, pak d dělí $\gcd(a,b)$.

Důkaz: Uvažujme čísla $a, b \in \mathbb{Z}$. Podle Bezoutovy identity lze vyjádřit $\gcd(a,b) = Aa + Bb$ pro nějaké $A, B \in \mathbb{Z}$. Pokud je d společný dělitel a, b, pak podle důsledku 1a.23 musí dělit i $Aa + Bb$ a tedy i $\gcd(a,b)$.

□

Řečeno jazykem kapitoly 6b, nejenže je $\gcd(a,b)$ největším číslem (ve smyslu velikosti) z množiny společných dělitelů a, b, je to také největší prvek této množiny, když ji uspořádáme relací dělitelnosti.

Ukážeme si další dvě vlastnosti čísla $\gcd(a,b)$, které by měly znít samozřejmě podle naší představy o dělitelnosti. Pokud čísla a, b vynásobíme stejným k, tak jsme jej vlastně přdali do společné části (v kladné verzi, gcd > 0). Když naopak obě a, b nějakým k vydělíme (pokud to jde v oboru celých čísel), tak odebíráme ze společné části. Zní to tak samozřejmě, že by člověk čekal elementární důkaz, ale hrátkami s dělitelností lze dokázat jen polovinu toho, co potřebujeme. Na druhou polovinu musíme použít Bezoutovu větu.

Věta 1b.17.
Nechť $a, b \in \mathbb{Z}$. Pak pro každé $k \in \mathbb{Z}$, $k \neq 0$ platí:
(i) $\gcd(ka, kb) = |k| \gcd(a,b)$.
(ii) Jestliže k dělí a i b, pak $\gcd\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{\gcd(a,b)}{|k|}$.

Důkaz (dobrý, poučný)**:** Nechť $a, b, k \in \mathbb{Z}$, $k \neq 0$ libovolné.

Pokud $a = b = 0$, pak všechna gcd ve vzorcích jsou nulová a tedy se rovnají.

Dále tedy předpokládejme, že alespoň jedno z a, b je nenulové, pak jsou všechna gcd ve vzorcích kladná a našla se pomocí množiny společných děitelů.

(i): Nejprve ukážeme, že číslo $\gcd(ka, kb)$ musí dělit číslo $|k|\gcd(a, b)$. Podle Bezoutovy identity najdeme čísla $A, B \in \mathbb{Z}$ tak, aby $\gcd(a, b) = aA + bB$. Pak také platí $|k|\gcd(a, b) = |k|aA + |k|bB$. Protože $\gcd(ka, kb)$ dělí čísla ka a kb, musí dělit i čísla $|k|a$ a $|k|b$. Proto dělí i jejich lineární kombinaci napravo a tedy i číslo $|k|\gcd(a, b)$ nalevo. Protože jsou obě čísla kladná, vychází z toho $\gcd(ka, kb) \leq |k|\gcd(a, b)$.

Protože $\gcd(a, b) \mid a$ a $\gcd(a, b) \mid b$, platí také $(|k|\gcd(a, b)) \mid (ka)$ a $(|k|\gcd(a, b)) \mid (kb)$. Proto je $|k|\gcd(a, b)$ společným dělitelem čísel ka, kb. Mezi těmito děliteli je $\gcd(ka, kb)$ největší, proto $|k|\gcd(a, b) \leq \gcd(ka, kb)$.

Spojením nerovností dostáváme $\gcd(ka, kb) = |k|\gcd(a, b)$.

(ii): Máme vlastně ukázat, že $|k|\gcd\left(\frac{a}{k}, \frac{b}{k}\right) = \gcd(a, b)$. Důkaz lze tedy provést pomocí (i), viz cvičení 1b.10. □

Číslo $\gcd(a, b)$ nám říká, jak moc mají čísla a, b společného, tedy jak moc se „překrývají“. V mnoha situacích pomůže, když se nepřekrývají vůbec.

Definice.
Řekneme, že čísla $a, b \in \mathbb{Z}$ jsou **nesoudělná** (**relatively prime**, **coprime**), jestliže $\gcd(a, b) = 1$.

Nesoudělnost se bude často vyskytovat jako předpoklad v tvrzeních, je to opravdu užitečná vlastnost. Jen pro zajímavost, dá se spočítat, že pokud vybereme náhodně dvě přirozená čísla, tak pravděpodobnost, že jsou nesoudělná, je $\frac{6}{\pi^2} \sim 0.61$ (viz např. Knuth: The Art of Computer Programming Vol 2, kde se také vysvětlí, co se přesně míní tou pravděpodobností).

Příklad 1b.e: Protože $\gcd(13, 23) = 1$, jsou to čísla nesoudělná. Podobně jsou nesoudělná čísla $40 = 2^3 \cdot 5$ a $81 = 3^4$. Naopak čísla $12, 20$ jsou soudělná, protože zjevně $\gcd(12, 20) = 4$.

Nesoudělnost je problematická, když se mezi čísla zaplete nula. Ze vzorce $\gcd(0, a) = |a|$ plyne, že 0 je nesoudělná jen s číslem 1 a s ostatními je soudělná. Je sice pravda, že například čísla $0, 13$ jsou obě dělitelná třinácti a tudíž mají podstatnou společnou část, ale je otázka, nakolik je na to připravena naše intuice. Není snadné si zvyknout, že nula coby univerzální násobek v sobě vlastně „obsahuje“ všechna čísla. Také je potřeba si zvyknout, že ze vzorce $\gcd(0, 0) = 0$ vycházejí čísla $0, 0$ jako soudělná. Musíme si tedy u soudělnosti na nulu dávat pozor, co si pod tím vlastně představit.

Dobrá zpráva je, že v aplikacích se pojem soudělnosti používá pro nenulová čísla.
△

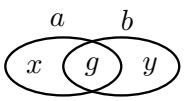
Pokud se nám někdy nehodí situace, kdy se čísla „překrývají“, tak uvítáme prvočísla, protože těm se nemůže stát, že by s jiným číslem „sdílely“ kousek sebe. Jsou extrémní a když se potkají s jiným číslem, tak s ním buď nemají nic společného, nebo jsou v něm obsaženy celé.

Fakt 1b.18.
Nechť p je pročíslo. Pak pro libovolné $a \in \mathbb{Z}$ platí, že buď je p s a nesoudělné, nebo p dělí a.

Důkaz (poučný)**:** Společní dělitelé a, p se vybírají z kladných dělitelů p, v úvahu tedy připadají 1 nebo p. Pokud je jediný společný dělitel 1, tak $\gcd(a, p) = 1$ a tvrzení je pravdivé. Jinak je společným dělitelem i p, tedy p dělí a a jsme zase hotovi.

□

Tato vlastnost je jednou ze silných stránek prvočísel a projevuje se blahodárně v mnoha situacích.



Oblíbený obrázek znázorňuje situaci, kdy $g = \gcd(a, b)$, pak $a = gx$ a $b = gy$ pro nějaká $x, y \in \mathbb{Z}$. Selský rozum napovídá, že jestli jsme do g shromáždili vše, co mají a, b společné, tak by už ty zbytky x, y neměly mít společného nic. Potvrdíme si to. Čtenář si může všimnout, že v důkazu nepoužijeme žádné věty. Je to snadný výsledek, který jsme klidně mohli dokázat dříve, ale ještě jsme neměli zavedenu nesoudělnost.

Fakt 1b.19.
Nechť $a, b \in \mathbb{Z}$, Pokud je alespoň jedno z čísel a, b nenulové, pak jsou $\dfrac{a}{\gcd(a, b)}$ a $\dfrac{b}{\gcd(a, b)}$ nesoudělná celá čísla.

Důkaz (rutinní)**:** Protože neplatí $a = b = 0$, je také $\gcd(a, b)$ nenulové číslo a dělí a i b, takže podíly z tvrzení jsou automaticky celá čísla, z nichž alespon jedno není nula. To znamená, že jejich gcd se určí jako největší prvek množiny společných dělitelů.

Předpokládejme, že $d \in \mathbb{N}$ je nějaký společný dělitel čísel $\frac{a}{\gcd(a,b)}$ a $\frac{b}{\gcd(a,b)}$. To znamená, že pro nějaká $k, l \in \mathbb{Z}$ máme $\frac{a}{\gcd(a,b)} = dk$ a $\frac{b}{\gcd(a,b)} = dl$. Pak $a = [d\gcd(a,b)]k$ a $b = [d\gcd(a,b)]l$, čili $d\gcd(a,b)$ je společný dělitel a, b. Protože $\gcd(a, b)$ je mezi společnými děliteli největší, musí být $d\gcd(a,b) \leq \gcd(a,b)$. Proto $d \leq 1$, což pro $d \in \mathbb{N}$ znamená nutně $d = 1$.

Takže jediný společný dělitel těch dvou čísel je 1, jsou tedy nesoudělná.

□

Poznámka: Zajímavou alternativou je dokázat nesoudělnost těch dvou podílů sporem.

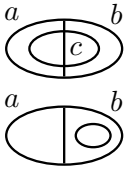
Předpokládejme, že $\frac{a}{\gcd(a,b)}$ a $\frac{b}{\gcd(a,b)}$ nejsou nesoudělné. To znamená, že existuje jejich společný dělitel $d \in \mathbb{N}$ splňující $d > 1$. Pak existují $k, l \in \mathbb{Z}$ tak, aby

$$\frac{a}{\gcd(a,b)} = dk \quad \text{a} \quad \frac{b}{\gcd(a,b)} = dl.$$

Odtud $a = \gcd(a, b)dk$ a $b = \gcd(a, b)dl$. Protože $k, l \in \mathbb{Z}$, je $\gcd(a, b)d$ společným dělitelem čísel a, b, který je díky $d > 1$ větší než $\gcd(a, b)$. To je spor s tím, že $\gcd(a, b)$ je mezi společnými děliteli největší.

△

Zkušenost nám říká, že pokud obecně číslo d dělí součin ab, tak nemusí dělit ani jedno z čísel, viz třeba případ $d = 4$, $a = 6$, $b = 10$. Intuitivně cítíme, že část čísla d je schovaná v a a druhá část v b. Někdy takové situaci potřebujeme zabránit. Intuice nám napoví, že by stačilo číslu d zakázat, aby s a „mělo společnou část“ (nabízí se pojem nesoudělnosti), a už by mělo být „celé v b“. Tento výsledek je hlubší, důkaz vyžaduje Bezoutovu větu.



Lemma 1b.20. (Euklidovo lemma)
Nechť $d, a, b \in \mathbb{Z}$. Jestliže $d \mid ab$ a čísla d, a jsou nesoudělná, pak $d \mid b$.

M 1b.21 Poznámka: Název „lemma“ se v matematice tradičně používá pro tvrzení, které nám pomáhá odůvodnit kroky v důkazech, odvozování či výpočtech. Často je to tvrzení pomocné, bez vlastního přímého praktického využití. To zrovna není případ tohoto lemmatu, které je samo o sobě zajímavé, ostatně jeho kvality podtrhuje fakt, že je po někom pojmenováno. Název lemma se k němu pojí tradičně a odkazuje na velkou užitečnost. Například v této knize jej použijeme možná dvacetkrát.

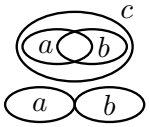
△

Důkaz (poučný)**:** Mějme $d, a, b \in \mathbb{Z}$. Podle předpokladu existuje $k \in \mathbb{Z}$ takové, že $ab = dk$. Protože jsou d, a nesoudělná, musí existovat čísla $D, A \in \mathbb{Z}$ taková, že $1 = \gcd(d, a) = Dd + Aa$. Vynásobením získáme $b = Ddb + Aab$, dosazením za ab z předpokladu pak $b = Ddb + Adk = d(Db + Ak)$. Díky $b, k, A, D \in \mathbb{Z}$ také $Db + Ak \in \mathbb{Z}$, což ukazuje, že d dělí b.

□

V poznámce za faktem1a.14 jsme se ptali, zda v situai, kdy máme čísla $a, b, c \in \mathbb{Z}$, platí implikace $a \mid b \implies a \mid (bc)$ také v opačném směru. Euklidovo lemma nám říká, že abychom mohli od $a \mid bc$ dojít k $a \mid b$, tak ještě potřebujeme informaci, že $\gcd(a, c) = 1$.

Další zajímavá situace je, když dvě celá čísla a, b dělí třetí celé číslo c. Pak nemusí platit, že by součin ab zase dělil c, viz například $a = 4$, $b = 6$, $c = 12$. Obrázek naznačuje, že problém je v „překrytí“ čísel a, b uvnitř c, takže se obě vlezou, zatímco „vedle sebe“ neboli v součinu ab už ne.



Obrázek také napoví, jaku podmínkou bychom mohli zajistit, aby součin ab už c dělil: Zakážeme číslům a, b, aby se překrývaly.

Lemma 1b.22.
Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \mid c$, $b \mid c$ a čísla a, b jsou nesoudělná, pak $(ab) \mid c$.

Důkaz je natolik podobný důkazu Eulerova lemmatu 1b.20, že jej s důvěrou necháme jako cvičení 1b.9.

Testovat nesoudělnost u velkých čísel dá práci. Pokud u čísla známe nějaký rozklad na faktory, tak se dá jeho nesoudělnost s jiným testovat „po částech“.

Lemma 1b.23.
Nechť $d, a, b \in \mathbb{Z}$. Pak $\gcd(d, ab) = 1$ právě tehdy, když $\gcd(d, a) = 1$ a $\gcd(d, b) = 1$.

Ekvivalenci dokážeme jako dvě implikace. U jedné z nich použijeme nepřímý důkaz, viz poznámka 1a.13.

Důkaz (poučný)**:** Mějme libovolné $d, a, b \in \mathbb{N}$.

Případ $d = 0$: Pak $\gcd(d, ab) = \gcd(0, ab) = |ab|$, $\gcd(d, a) = |a|$ a $\gcd(d, b) = |b|$. Takže $\gcd(d, ab) = 1$ právě tehdy když $|ab| = 1$, což je pro celá čísla právě tehdy, když $|a| = |b| = 1$, což je právě tehdy, když $\gcd(d, a) = \gcd(d, b) = 1$.

Dále tedy předpokládejme $d \neq 0$. To znamená, že všechny gcd v dokazovaném tvrzení jsou určeny pomocí množin společných dělitelů.

1) $\Longrightarrow$: Předpokládejme, že $\gcd(d, ab) = 1$. Nechť $x \in \mathbb{N}$ je společný dělitel d a a. Pak podle věty 1a.14 x dělí také d a ab, tedy je to jejich společný dělitel. Proto $x \leq \gcd(d, ab) = 1$.

Ukázali jsme, že jediný společný dělitel a a d je 1, proto jsou nesoudělná. Důkaz pro d, b je obdobný.

2) $\Longleftarrow$: Dokážeme obměnu: Jestliže $\gcd(d, ab) > 1$, pak $\gcd(d, a) > 1$ nebo $\gcd(d, b) > 1$.

Předpokládejme tedy, že $g = \gcd(d, ab) > 1$. Jestliže $\gcd(g, a) > 1$, tak jsme obměnu dokázali.

Zbývá případ $\gcd(g, a) = 1$. Protože g dělí ab, podle lemma 1b.20 musí g dělit b a tedy podle faktu 1b.11 $\gcd(g, b) = g > 1$.

□

Například snadno nahlédneme, že $d = 8$ je nesoudělné s $a = 27$ a $b = 125$, takže je nesoudělné i s jejich součinem 3375.

Jako bonus si ukážeme verze pro víc čísel. Budou se hodit v důkazech v rovněž bonusové sekci v kapitole 2, takže čtenář, který necítí potřebu jít do hloubky či šířky, může chtít tuto pasáž přeskočit a jít rovnou k sekci o praktickém hledání $\gcd(a, b)$ a Bezoutovy identity.

Abychom mohli předchozí dva výsledky upravit pro více čísel, tak si musíme nejprve rozmyslet, jak zajistit, aby se více čísel „nepřekrývalo“. Uvažujme čísla $a_1, \dots, a_n \in \mathbb{Z}$. Nabízí se podmínka, že $\gcd(a_1, a_2, \dots, a_n) = 1$, tedy že jediné kladné číslo, které všechna a_i dělí (společný dělitel), je jednička (viz cvičení 1b.12). To je ale příliš slabá podmínka, protože společný dělitel více čísel se snadno ovlivní jedním z nich bez ohledu na ostatní. Například čísla $1, 13, -13$ mají jediného společného dělitele jedničku, tedy $\gcd(1, 13, -13) = 1$, ale čísla 13 a -13 mají spolu společného hodně.

Proto se obvykle požaduje víc.

Definice.
Řekneme, že čísla $a_1, a_2, \dots, a_n \in \mathbb{Z}$, kde $n \in \mathbb{N}$, jsou **po dvou nesoudělná** (**pairwise coprime**), jestliže $\gcd(a_i, a_j) = 1$ pro všechna $i \neq j \in \{1, 2, \dots, n\}$.

Stojí za to vyjasnit, že pokud máme jedno číslo a_1 neboli $n = 1$, tak se žádná dvojice $i \neq j \in \{1\}$ nenajde. Tím pádem jde o prázdný test, který nemůže selhat (není protipříklad) a tudíž automaticky platí. Jedno číslo tedy tvoří po dvou nesoudělnou množinu. V praxi se to samozřejmě nepoužívá a mohli jsme ten případ vyloučit podmínkou $n \geq 2$, ale nebude nám vadit.

Tato nová podmínka zaručí, že v obrázkové představě budou v součinu $a_1 \cdot a_2 \cdots a_n$ čísla „vedle sebe“, a nepřekvapí nás následující:

Lemma 1b.24.
Nechť $c, a_1, a_2, \dots, a_n \in \mathbb{Z}$, kde $n \in \mathbb{N}$. Jestliže $a_i \,|\, c$ pro všechna $i \in \{1, 2, \dots, n\}$, a čísla a_i jsou po dvou nesoudělná, pak $(a_1 a_2 \cdots a_n) \,|\, c$.

Důkaz se provede matematickou indukcí, kterou teprve probereme v kapitole 7. Zacyklení naštěstí nehrozí, protože v dotyčné kapitole se dělitelnost vůbec nepoužívá. Pokud je pro čtenáře indukce nová, může se k důkazu vrátit po probrání příslušné kapitoly.

Důkaz: (0) $n = 1$: Máme dokázat, že pokud $a_1 \,|\, c$, tak $a_1 \,|\, c$, což zjevně platí.

(1) Nechť $n \geq 1$. Předpokládejme, že tvrzení platí pro libovolná čísla $d, b_1, \dots, b_n \in \mathbb{Z}$.

Mějme nyní čísla $d, a_1, \dots, a_n, a_{n+1} \in \mathbb{Z}$ taková, že $a_i \,|\, c$ pro všechna $i = 1, \cdots, n+1$. Označme $b_1 = a_1$, …, $b_{n-1} = a_{n-1}$ a $b_n = a_n a_{n+1}$. Pak zjevně $b_1 \,|\, c$, … , $b_{n-1} \,|\, c$. Dále víme, že $a_n \,|\, c$, $a_{n+1} \,|\, c$ a $\gcd(a_n, a_{n+1}) = 1$,

proto podle lemma 1b.22 také $(a_n a_{n+1}) \mid c$ neboli $b_n \mid c$. Čísla b_j proto splňují indukční předpoklad a podle něj $(b_1 \cdots b_n) \mid c$. Ovšem

$$b_1 \cdots b_n = a_1 \cdots a_n a_{n+1}$$

a tedy $(a_1 \cdots a_n a_{n+1}) \mid c$, což jsme měli dokázat.

□

Obdobně si zobecníme pravidlo pro ověřování nesoudělnosti.

Lemma 1b.25.
Nechť $d, a_1, \dots, a_n \in \mathbb{Z}$ pro $n \in \mathbb{N}$. Pak $\gcd(d, a_1 \cdots a_n) = 1$ právě tehdy, když $\gcd(d, a_i) = 1$ pro všechna $i = 1, \dots, n$.

Důkaz: (0) $n = 1$: Máme dokázat, že $\gcd(d, a_1) = 1 \iff \gcd(d, a_1) = 1$, což zjevně platí.
(1) Nechť $n \geq 1$. Předpokládejme, že tvrzení platí pro libovolná čísla $d, b_1, \dots, b_n \in \mathbb{Z}$.
Mějme nyní čísla $d, a_1, \dots, a_n, a_{n+1} \in \mathbb{Z}$. Označme $b_1 = a_1, \dots, b_{n-1} = a_{n-1}$ a $b_n = a_n a_{n+1}$. Pak

$$a_1 \cdots a_n a_{n+1} = b_1 \cdots b_n.$$

1) $\Longrightarrow$: Jestliže $\gcd(d, a_1 \cdots a_n \cdot a_{n+1}) = 1$, pak také $\gcd(d, b_1 \cdots b_n) = 1$. Podle indukčního předpokladu tedy $\gcd(d, b_j) = 1$ pro všechna $j = 1 \dots, n$. Máme tedy $\gcd(d, a_i) = 1$ pro $i = 1, \dots, n-1$ a také $\gcd(d, b_n) = 1$ neboli $\gcd(d, a_n a_{n+1})$, což podle lemma 1b.23 dává $\gcd(d, a_n) = 1$ a $\gcd(d, a_{n+1}) = 1$.
2) $\Longleftarrow$: Jestliže $\gcd(d, a_i) = 1$ pro všechna $i = 1, \dots, n+1$, tak podle označení také $\gcd(d, b_j) = 1$ pro $j = 1, \dots, n-1$ a lemma 1b.23 aplikované na $a_n a_{n+1}$ dává $\gcd(d, b_n) = 1$. Podle indukčního předpokladu pak $\gcd(d, b_1 \cdots b_n) = 1$ neboli $\gcd(d, a_1 \cdots a_n a_{n+1}) = 1$.

□

Dalším přirozeným krokem je následující tvrzení:

Důsledek 1b.26.
Nechť $a_1, \dots, a_n, b_1, \dots .b_m \in \mathbb{Z}$ pro $n, m \in \mathbb{N}$. Pak $\gcd(a_1 \cdots a_n, b_1 \cdots b_m) = 1$ právě tehdy, když $\gcd(a_i, b_j) = 1$ pro všechna $i = 1, \dots, n$ a $j = 1, \dots, m$.

To vede na zajímavou interpretaci, která se bude hodit. Pokud máme čísla, která jsou po dvou nesoudělná, rozdělíme je na dvě skupiny a z každé uděláme součin, tak ta dvě výsledná čísla budou nesoudělná.

1b.27 Euklidův algoritmus: výpočet gcd a Bezoutovy identity

V této sekci vyvineme způsob, jak efektivně hledat $\gcd(a, b)$ a odpovídající Bezoutovu identitu. Podotkněme, že díky větě 1b.10 pak už snadno dopočítáme i $\operatorname{lcm}(a, b)$.

Nejprve si připomeneme, že pro některá vstupní data už rovnou máme výsledek. Jmenovitě jde o následující:
- $\gcd(a, 0) = |a|$ a $\operatorname{lcm}(a, 0) = 0$;
- $\gcd(a, a) = \operatorname{lcm}(a, a) = |a|$.

Dále víme, že na znaménkách nezáleží, takže nám vlastně stačí umět najít $\gcd(a, b)$ pro dvě různá kladná čísla, která navíc můžeme seřadit podle velikosti. Budeme se tedy (dočasně) soustředit na případ $a > b > 0$. Sice se časem ukáže, že toto omezení není nutné, ale obvykle se dělá, protože usnadňuje některé teoretické úvahy a také pomáhá při ručním výpočtu.

Klíčem k postupu je následující výsledek.

Lemma 1b.28.
Nechť $a, b \in \mathbb{Z}$, nechť $r \in \mathbb{Z}$ splňuje $r = a - qb$ pro nějaké $q \in \mathbb{Z}$. Pak $\gcd(a, b) = \gcd(b, r)$.

Toto je krásný příklad technického lemmatu, jehož účelem je zjednodušit několik důkazů. Rovnost gcd již tradičně odvodíme tak, že ukážeme shodnost množin společných násobků, jako obvykle také musíme speciální případy udělat zvlášť.

Důkaz (poučný)**:** Dáno $a, b, r \in \mathbb{Z}$, kde $r = a - qb$ pro nějaké $q \in \mathbb{Z}$.
1) Případ $b = 0$: Pak $r = a - q \cdot 0 = a$. Máme tedy potvrdit, že $\gcd(a, 0) = \gcd(0, a)$, což jsme již udělali, viz fakt 1b.7.
2) Případ $b \neq 0$. Pak oba gcd vznikly pomocí množiny společných dělitelů.
Ukážeme, že množiny společných dělitelů dvojic a, b a b, r jsou shodné.

Je-li d společný dělitel a a b, pak podle důsledku 1a.23 musí dělit také $r = a - qb$, tedy je to společný dělitel b, r.

Naopak je-li d společný dělitel b a r, pak podle důsledku 1a.23 musí dělit také $a = r + qb$, tedy je to společný dělitel a, b.

Protože se množiny společných dělitelů dvojic a, b a b, r shodují, musí se také shodovat jejich největší prvky zvané $\gcd(a, b)$ a $\gcd(b, r)$.

□

Případ $b = 0$ je zahrnut spíš kvůli úplnosti, v praxi se nepoužívá. Spíš bývá běžné, že se v praxi používají a v tomto lemmatu formulují více specializované verze, například se s ním pracuje jen pro $a > b$, případně jen pro $r = a - b$. Jedna oblíbená verze, kterou zde budeme hojně využívat, souvisí s tím, že vzorec $r = a - qb$ jsme již potkali v příkladě 1a.c, kde jsme počítali zbytek po dělení pomocí představy posunů. Takže jedním z množných r je $r = a \bmod b$. V tomto případě se dá smysl tohoto lemmatu vyjádřit rovností

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Tato rovnost je klíčem k efektivnímu výpočtu $\gcd(a, b)$.

Příklad 1b.f: Chceme najít $\gcd(408, 108)$. Aplikujeme opakovaně lemma, zbytky počítáme oblíbenou metodou, například odčítáním.
Máme $408 \bmod 108 = 84$, proto $\gcd(408, 108) = \gcd(108, 84)$.
Máme $108 \bmod 84 = 24$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24)$.
Máme $84 \bmod 24 = 12$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24) = \gcd(24, 12)$.
Máme $24 \bmod 12 = 0$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24) = \gcd(24, 12) = \gcd(12, 0) = 12$.

Asi jsme mohli skončit o krok dříve, protože $\gcd(24, 12) = 12$ vidíme, ale pro počítač je jednodušší si počkat na jasně rozeznatelnou nulu.

Pro úplnost si ještě dopočítáme $\operatorname{lcm}(408, 108) = \dfrac{408 \cdot 108}{\gcd(408, 108)} = 408\,\dfrac{108}{12} = 408 \cdot 9 = 3672$. Přesně totéž jsme dostali pomocí prvočísel.

△

Postup z příkladu je obecný. Pokud se nám nelíbí úloha $\gcd(a, b)$ pro čísla $a > b > 0$, tak přejdeme k úloze $\gcd(b, a \bmod b)$, která díky $a \bmod b < b$ zaručeně obsahuje menší čísla a opět jsou v pořadí větší-menší. Takže pokud stále nejsme spokojeni, můžeme postup opakovat. Dostáváme tím algoritmus na výpočet $\gcd(a, b)$, který je mimochodem starý asi 2300 let. Z hlediska programovacího si stačí v každé iteraci pamatovat jen poslední dvě čísla. Ovšem pokud budeme chtít tento algoritmus zkoumat, pak se hodí mít záznam o celém běhu. Ukážeme tedy dvě podoby algoritmu.

S Algoritmus 1b.29.
Euklidův algoritmus (Euclidean algorithm) pro nalezení $\gcd(a, b)$ pro $a, b \in \mathbb{N}$, $a > b$.

Verze 1.
Iniciace: $r_0 := a$, $r_1 := b$, $k := 0$.
Krok: $k := k + 1$, $r_{k+1} := r_{k-1} \bmod r_k$
Opakovat dokud nenastane $r_{k+1} = 0$.
Pak $\gcd(a, b) := r_k$.

Verze 2.
```
procedure gcd(a, b: integer, a > b > 0)
repeat
    r := a mod b;
    a := b;  b := r;
until b = 0;
output: a;
```

△

Kdykoliv vymyslíme algoritmus neboli postup řešení nějaké úlohy, je třeba si položit dvě otázky.

1. Je zaručeno, že běh algoritmu pokaždé skončí? V našem algoritmu pracujeme s řetězcem klesajících celočíselných zbytků r_k, které nemohou být záporné. Protože se každé r_{k+1} zmenší oproti r_k alespon o jedničku, dříve či později musí nastat stav $r_K = 0$ a algoritmus skončí.

2. Když algoritmus skončí, dá správnou odpověď? Ano, protože se díky lemmatu 1b.28 při vytváření řetězce dvojic nikdy nemění hodnota jejich gcd.

Toto samozřejmě byl jen nástin. Pořádné důkazy a další dokázané poznatky o tomto algoritmu najde čtenář v bonusové kapitole 14.

S Příklad 1b.g (ruční výpočet)**:**

Při ručním počítání zachycujeme stavy registrů tabulkou. Existuje několik verzí, ukážeme tu nejpoužívanější. Začneme tím, že si pod sebe dáme čísla a, b tak, aby to větší bylo nahoře. Pak spočítáme zbytek po dělení a zapíšeme do třetího řádku.

Ukážeme si to pro náš předchozí příklad $\gcd(408, 108)$:

a, b
408
108

$408 \bmod 108 = 84 \longrightarrow$

a, b
408
108
84

Zbytky se obvykle hledají posunovým způsobem, v každém kroku si tedy klademe otázku: Kolikrát máme odečíst dolní číslo od horního, abychom se co nejvíce přiblížili k nule (ale nespadli pod ni)? Zde máme $84 = 408 - 3 \cdot 108$. Máme částečný podíl $q = 3$, který za chvíli použijeme u pokročilejší verze tohoto algoritmu. Autoři tedy doporučují si toto q psát do pomocného sloupce.

Pro mě osobně je příjemnější naznačit si k dolnímu („pracovnímu“) číslu, kolikrát jej mám odečíst od toho nad ním. Vypadalo by to tedy takto, vlevo verze oficiální, vpravo moje. Čtenář třeba preferuje ještě něco jiného, nebo se bez toho obejde.

a, b	q
408	
108	3
84	

$-3\times$

a, b
408
108
84

Teď bychom měli posunout registry, což realizujeme tím, že přeneseme pohled na poslední dva řádky v tabulce, a začneme znovu. Vhodným odečtením spodního čísla od toho nad ním najdeme zbytek, čímž přibude v tabulce nový řádek a zase posuneme pohled na poslední dva řádky. Takto postupujeme, dokud nenajdeme nulu. Kladné číslo, které se objevilo naposledy nad nulou, je poslední stav registru a a tedy i hledaný $\gcd(408, 108)$.

a, b
408
108

$\longrightarrow$

$-3\times$

a, b
408
108
84

$\longrightarrow$

$-1\times$

a, b
408
108
84
24

$\longrightarrow$

$-3\times$

a, b
408
108
84
24
12

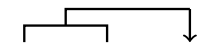
$\longrightarrow$

$-2\times$

a, b	q
408	
108	3
84	1
24	3
12•	2
0	

V poslední tabulce jsme pro úplnost (a pro příznivce tradičního značení) přidali i částečné podíly q.

Samozřejmě není důvod psát pod sebe, nejjednodušší je psát čísla za sebe, začneme s čísly 408 a 108, z nich odvodíme další.



408	108	84	24	12	0
	$(-3\times$	$-1\times$	$-3\times$	$-2\times)$	

Tento zápis výrazně prostorově úspornější, ale my si tento algoritmus brzy dále rozšíříme a na to bude vhodnější ta první, sloupcová verze.

Mimochodem, pro naše předky bylo u tohoto algoritmu zajímavé, že pomocí něj lze snadno převádět zlomky do řetězového tvaru. Jsou k tomu potřeba ona q. Zde jsou rovny $3, 1, 3, 2$ a odtud $\frac{408}{108} = 3 + \frac{1}{1+\frac{1}{3+\frac{1}{2}}}$. Pokud vás to zaujalo, Internet vás navede dál.

△

1b.30 Poznámka: Z praktického programátorského pohledu je zajímavé si všimnout, že algoritmus je schopen pracovat pro libovolné vstupy. Jen si musíme dát pozor a přesunout podmínku nulovosti na začátek, protože se nula může objevit na vstupu a pak bychom nemohli nalézt hned první zbytek.

Tím odpadly technické problémy, kroky lze aplikovat a klíčové lemma 1b.28 jsme záměrně dokázali pro všechna $a, b \in \mathbb{Z}$, takže pokud algoritmus skončí, tak dá správný výsledek.

Jak víme, že skončí, když se v běhu mohou objevovat záporná čísla? Hned třetí a čtvrté číslo (pokud tam algoritmus dojde) vznikají jako zbytek, tedy jsou nezáporná a v pořadí větší-menší. To znamená, že počínaje třetím krokem běh pokračuje jako standardní Euklidův algoritmus, o kterém víme, že správně skončí.

Než tuto obecnější (a finální) verzi algoritmu napíšeme, všimneme si jedné zajímavosti. V případě, že máme čísla $0 \leq a < |b|$, tak $r = a \bmod b = a$. To znamená, že první krok algoritmu nás od dvojice a, b zavede ke dvojici b, a. Tento algoritmus opravdu preferuje mít vstupní čísla v pořadí větší-menší, a když mu nevyhovíme, tak si to pro $a \geq 0$ sám opraví. Pro $a < 0$ už neprohazuje, ale přizpůsobí se jinak, v obou případech ale za to platíme krokem navíc.

$-0\times$

a
b
a

Počítači je to jedno, ale při ručním výpočtu se vyplatí data seřadit tak, aby $|a| > |b|$.
△

Euklidův algoritmus (obecná verze) pro nalezení $\gcd(a,b)$ pro $a,b \in \mathbb{Z}$.
`procedure` *gcd* $(a,b$: integer$)$
`while` $b \neq 0$ `do`
    $r := a \bmod b$;
    $a := b$; $b := r$;
`output:` $|a|$;

S Příklad 1b.h (ruční výpočet: obecné vstupy)**:** Najdeme $\gcd(-108,-408)$.
Jedna možnost je využít toho, že výsledek nezáleží na znaménkách vstupních čísel a jejich pořadí. Takže se znamének zbavíme, pak čísla seřadíme v pořadí větší-menší a dojdeme k alternativnímu zadání $\gcd(408,108)$. To jsme již našli v příkladu 1b.g a stálo nás to 4 kroky algoritmu. Závěrem konstatujeme, že

$$\gcd(-108,-408) = \gcd(408,108) = 12.$$

Toto by se dalo považovat za standardní postup a má své výhody.
Teď se podíváme, jak to dopadne při aplikaci Euklidova algoritmu přímo na vstupní data.
Připravíme si tradiční tabulku a položíme si otázku: Jsme na pozici -108. Jakými kroky o velikosti $|-408| = 408$ se dostaneme doprava k nule či dál, ale ne zbytečně daleko? Zjevně stačí jeden krok doprava, tedy chceme přičíst 408 neboli odečíst -408. Budeme tedy jednou odečítat dolní řádek od horního. Operaci si označíme jednak oficiálním částečným podílem q, jednak si ji pro sebe označím dle svého.

a,b
-108
-408

Máme situaci napravo a opět si klademe otázku, jak se kroky o velikosti 300 dostaneme z pozice -408 doprava od nuly. Vidíme, že potřebujeme dva. Algebraicky, potřebujeme přičíst dolní číslo dvakrát k hornímu, což si poznamenám a provedu. Ti, kteří preferují pracovat s q, si musí uvědomit, že algoritmus formálně odčítá, tedy je nutný tento zápis:

	a,b	q
	-108	
$-1\times$	-408	1
	300	

$$-408 + 2\cdot 300 = -408 - (-2)\cdot 300.$$

Takže $q = -2$. Dostáváme následující tabulku.
Dostali jsme kladná čísla seřazená větší-menší, takže dál už algoritmus bude probíhat obvyklým způsobem. Čtenář si může ověřit, že to dopadne (ve stručném zápise) takto:

$$-108 \quad -408 \quad 300 \quad 192 \quad 108 \quad 84 \quad 24 \quad 12 \quad 0.$$

	a,b	q
	-108	
$-1\times$	-408	1
$+2\times$	300	-2
	192	

Výpočet vyžadoval 7 kroků, což je téměř dvojnásobek oproti verzi s kladnými vstupy. Je ovšem třeba říct, že to není pravidlem, někdy je naopak výpočet se zápornými vstupy kratší než ten s kladnými. Ostatně pokud budeme následovat doporučení a seřadíme si vstupy podle velikosti, dostáváme následující běh:

$$-408 \quad -108 \quad 24 \quad 12 \quad 0.$$

V prvním kroku jsme číslo -108 odečetli čtyřikrát od čísla -408.
Tentokrát je výpočet dokonce o jeden krok kratší než verze s kladnými vstupy. Poučení je, že pokud budeme vstupy řadit podle velikosti, tak rozdíl mezi verzí s kladnými vstupy a verzí s obecnými vstupy není v efektivitě, ale v pohodlí ruční práce. Ačkoliv jde v zásadě o stále stejnou algebru, pro řadu lidí je mentálně namáhavější, když se v tabulce vyskytnou záporná čísla, podle mých zkušeností se pak také při ručním výpočtu častěji objevují numerické chyby. Je tedy na čtenáři, jak si věří.
Tento algoritmus si ještě dvakrát modifikujeme a pokaždé se na jedné straně zvětší mentální náklady práce se zápornými čísly, ale zase přibudou benefity.
△

V tomto praktickém koutku jsme se při výpočtu zbytku soustředili na posunový způsob a ignorovali postup pomocí dělení, který funguje lépe, pokud jsou a,b velmi odlišná. Je pro to dobrý důvod. Je dokázáno, že při výpočtu standardního Euklidova algoritmu vznikají $q = 1,2,3,4$ s pravděpodobností po řadě 41.5%, 17.0%, 9.3% a 5.9%. Jinými slovy, v polovině případů lze čekat jedno či dvě odečtení a přinejmenším ve třech čtvrtinách případů vidíme hned pohledem, kolikrát je třeba posunout. Jak čtenář uvidí ve výkladu a cvičeních, v běžných ručních výpočtech se s komplikovanější algebrou téměř nesetkáme.
Proč se tu vlastně bavíme o ručním výpočtu, když to v praxi stejně řeší počítače? Jsou dva důvody. První je pedagogický. Zkušenost potvrzuje, že je snažší pochopit funkci algoritmu a jeho rozličné aspekty, když si to člověk sám vyzkouší. Druhý důvod je, že brzy budeme potřebovat hledání gcd jako součást dalších postupů a není pohodlné kvůli tomu sebou pořád nosit počítač. V neposlední řadě to možná čtenáři budou muset umět ke zkoušce.

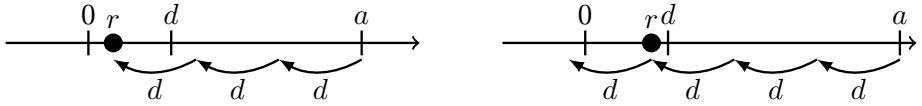
1b.31 Poznámka (záporné zbytky):

V kapitole 14 mimo jiné zkoumáme i rychlost Euklidova algoritmu, konkrétně kolik asi musíme udělat kroků. Je to užitečné nejen pro ty, kdo počítají ručně, ale i pro počítače, protože v praxi se hledají $\gcd(a,b)$ pro masivní čísla klidně i o několika stech cifrách. V dotyčné kapitole se dočteme, že počet iterací je v nejhorším pětinásobek počtu cifer menšího ze vstupů, když jej vyjádříme v desítkové soustavě. Například u vstupu $408, 108$ je to v nejhorším $5 \cdot 3 = 15$ kroků. Odhad je v tomto případě zbytečně pesimistický, ale lépe to kvůli méně přátelským případům nejde a pořád je to velmi slušná rychlost. Euklidův algoritmus je téměř nejrychlejší způsob, jak se ke $\gcd(a,b)$ dostat.

Přesto se nabízí otázka, jestli by to nešlo lépe (zejména pokud nás čeká ruční výpočet). Rychlost Euklidova algoritmu zjevně souvisí s tím jak rychle se zmenšují jednotlivé zbytky. Víme, že zbytky při dělení číslem d mohou být v rozmezí 0 až $|d|-1$, takže se může stát, že se jedním krokem algoritmu naše situace téměř nezlepší. Například ze vstupů $130, 45$ máme jako další číslo 40, to jsme si moc nepomohli. Pesimista už vidí, jak se v extrémním případě s každým krokem číslo v tabulce sníží o jedničku.

Při bližším pohledu se ale ukáže, že situace není tak špatná, protože funguje jakýsi zákon rovnováhy. Pokud se v jednom kroku číslo moc nesníží, tak se výrazně sníží v dalším, a naopak. V našem příkladě by výpočet pokračoval číslem 5, což je dost velké zmenšení z předchozích 40. Tato rovnováha vyplývá z výsledku, který dokážeme v kapitole 14: Pokud je v nějakém řádku naší tabulky číslo r, tak se mu musí rovnat součet následujících dvou řádků (ano, $40+5=45$). To je dobrá zpráva, nicméně to naznačuje, že zhruba v polovině kroků nelze čekat významný pokrok.

Což nás přivádí ke klíčové otázce. Podstata Euklidova algoritmu je, že v každém kroku začneme v předposledním čísle a pak se pomocí posledního čísla d zkoušíme dostat co nejblíže k nule, ale zprava. Skončíme někde mezi čísly 0 a $|d|-1$. Náhodně vzato, v polovině případů jsme dokonce do poloviny tohoto rozsahu, tedy $r \leq \frac{1}{2}|d|$, což je dobré. Bohužel, v druhé polovině případů máme zbytek větší. V takovém případě se ovšem umíme dostat blíž k nule, ale z druhé strany.



Toto bližší číslo má řadu vlastností společných se zbytkem, což ospravedlňuje následující název.

Nechť $a, d \in \mathbb{Z}$, $d \neq 0$. Definujeme „záporný zbytek“ po dělení čísla a číslem d jako číslo r splňující $a = qd + r$ pro nějaké $q \in \mathbb{Z}$ a zároveň $-\frac{1}{2}|d| < r \leq \frac{1}{2}|d|$.

Je možné dokázat obdobu věty o dělení, tedy záporný zbytek existuje a je jednoznačně určen. Hledáme jej podobným postupem jako zbytek běžný, tedy v praxi docela snadno postupnými posuny o d, jen s jinak definovaným cílem, nebo pomocí dělení. Rozdíl je, že u zbytku standardního podíl $\frac{a}{d}$ zaokrouhlujeme dolů či nahoru podle znaménka d (viz fakt 1a.34), zatímco pro získání záporného zbytku zaokrouhlujeme na nejbližší celé číslo. Toto zaokrouhlení se někdy značí $\left\lfloor \frac{a}{d} \right\rceil$.

Krása je v tom, že jsme klíčové lemma 1b.28 dokázali pro všechna r získatelná posuny, takže platí i na záporné zbytky. Proto lze Euklidův algoritmus modifikovat tak, že se v každém kroku chceme dostat co nejblíže k nule bez ohledu na znaménko. Například v našem obvyklém příkladě jsme se v prvním kroku dostali z pozice 408 trojnásobným posunem o 108 na číslo 84, ale dalším posunem bychom se dostali k číslu -24, které je výrazně menší.

Jaké jsou benefity? Je zaručeno, že tato modifikace nebude pomalejší, a často je i rychlejší než běžný Euklidův algoritmus, a to statisticky až o třetinu. V zásadě je to nejrychlejší (přímočarý) algoritmus.

Čím za to zaplatíme? Může se stát, že předposlední číslo v běhu pak vyjde záporné, ale to není problém, jako $\gcd(a,b)$ vezmeme jeho absolutní hodnotu. Při ručním výpočtu pak hrozí snížená psychická pohoda, popřípadě větší chybovost.

△

S Příklad 1b.i (ruční výpočet: záporné zbytky)**:**

Najdeme $\gcd(a,b)$ pro čísla 380 a 131 v různých znaménkových mutacích. Použijeme standardní Euklidův algoritmus, nejprve v klasické podobě, tedy pro dvě kladná čísla, a pak s různými znaménky na vstupu. Protože se máme rádi, čísla na začátku srovnáme podle velikosti. Doporučujeme, aby se čtenář vždy jen podíval na zadání a pak si nejprve sám zkusil tabulku dopočítat, aby tak ocenil pohodlnost výpočtu. Označení operací ukazujeme obojí, s q i s mým.

	a,b	q
	380	
$-2\times$	131	2
$-1\times$	118	1
$-9\times$	13	9
$-13\times$	1•	13
	0	

	a,b	q
	380	
$+2\times$	−131	−2
$+2\times$	118	−2
$-1\times$	105	1
$-8\times$	13	8
$-13\times$	1•	13
	0	

	a,b	q
	−380	
$+3\times$	131	−3
$-10\times$	13	10
$-13\times$	1•	13
	0	

	a,b	q
	−380	
$+3\times$	−131	−3
$+11\times$	13	−11
$-1\times$	12	1
$-12\times$	1•	12
	0	

Vidíme, že někdy přítomnost záporných čísel výpočet prodloužila a někdy naopak urychlila. Délka běhu je kombinací znamének a toho, jak si čísla sednou, a z praktického pohledu je neodhadnutelné, která z těchto čtyř znaménkových možností bude příznivá a která ne. Čtenář si může vyzkoušet, že ve všech případech by se výpočet prodloužil o jeden krok, pokud bychom vstupní data použili v pořadí malé-velké.

Nyní pro srovnání spočítáme stejné úlohy pomocí záporných zbytků.

	a,b	q
	380	
$-3\times$	131	3
$+10\times$	−13	−10
$+13\times$	1•	−13
	0	

	a,b	q
	380	
$+3\times$	−131	−3
$+10\times$	−13	−10
$-13\times$	−1•	13
	0	

	a,b	q
	−380	
$+3\times$	131	−3
$-10\times$	13	10
$-13\times$	1•	13
	0	

	a,b	q
	−380	
$-3\times$	−131	3
$+10\times$	13	−10
$+13\times$	−1•	−13
	0	

Vidíme, že na délku běhu modifikovaného Euklidovského algoritmu neměly znaménka vliv a vždy jsme se dostali k nejlepší rychlosti dosažené výše. Dá se tedy říci, že použití záporných zbytků v jednom případě zachovalo rychlost a ve třech ji zvýšilo. To urychlení není nějak zásadní, což je ovšem dáno tím, že zde ukazujeme jen příklady s malým počtem iterací.

Čtenář může porovnat, zda mu více vyhovuje zápis operací s q nebo nějaký jiný, popřípadě žádný (ale časem se ten zápis bude hodit). K otázce volby mezi rychlostí a bezpečností nám později přibude ještě faktor víceprací, takže se k ní vrátíme. Pro počítač je samozřejmě jedno, s jakými čísly počítá, takže záporné zbytky jsou jednoznačná volba.

Podívejme se na závěr. Ve dvou případech jako předposlední číslo vidíme -1. Připomeňme si, že tabulka je vlastně zápisem opakovaného použití lemmatu 1b.28, v tomto případě tedy například

$$\gcd(380,-131)=\gcd(-131,-13)=\gcd(-13,-1)=\gcd(-1,0)$$

a odpověď je tedy $|-1|=1$. Záporná čísla nám nevadí.

→ Poznámka pro drsně: Protože gcd nevadí změna znaménka, nabízí se ještě jedna možnost:

$$\gcd(380,131)=\gcd(131,-13)=\gcd(131,13).$$

Lze tedy začít s kladnými verzemi čísel a pak v každém kroku postupovat následovně: Najdeme záporný zbytek (r nejbližší nule), napíšeme jej do tabulky a pak mu případně změníme znaménko. Vznikne algoritmus, který je stejně rychlý jako ten modifikovaný Euklidův a navíc můžeme pohodlně počítat s kladnými čísly. Tento postup nedoporučuji z více důvodů.

První je praktický, z tabulky pak není jasné, jak se počítalo, což mimo jiné komplikuje hledání případných numerických chyb. Hlavní důvod ale je, že my ve škole nepočítáme rukou, abychom to pak celý život uměli, ale abychom si přiblížili, co se děje v počítači, protože ty to pak za nás budou dělat v praxi. Nemá tedy smysl počítat způsobem, který se v praxi nepoužívá. ←

△

Poznámka: Existují i jiné přístupy k rychlému výpočtu $\gcd(a,b)$ a některé nabízejí značnou efektivitu díky využití faktu, že se čísla ukládají v binárním kódu. Některé operace jsou pak velmi levné, například dělení dvěma. Jeden postup je založen na opakovaném využití těchto identit:

- $\gcd(a,b)=2\gcd(a/2,b/2)$, jsou-li a,b sudá,
- $\gcd(a,b)=\gcd(a/2,b)$, je-li a sudé a b liché,
- $\gcd(a,b)=\gcd(a-b,b)$, jsou-li a,b lichá.

Takže nejprve opakovaným dělením dvěma (což je v binárním kódu jen posun bitů) dosáhneme situace s jedním či dvěma lichými čisly, pak aplikujeme opakovaně druhý či třetí vzorec, dokud nedojdeme k nule.

My zůstaneme s Euklidovým algoritmem, protože jej záhy naučíme dělat i další užitečnou věc.

△

Naučili jsme se hledat $\gcd(a,b)$, ale v praxi často potřebujeme také odpovídající Bezoutovu identitu. My víme, že jich je dokonce nekonečně mnoho, ale to je chabá útěcha ve chvíli, kdy máme najít potřebnou kombinaci a nenapadá nás ani jedna. Konec konců, spočítali jsme, že $\gcd(408,108)=12$. Dokážete uhodnout nějaké Bezoutovo vyjádření?

Pomůže Euklidův algoritmus. Když už jsme jej použili, je možné se k němu vrátit a využít jednotlivé kroky k nalezení identity.

Příklad 1b.j: V příkladu 1b.g jsme zjistili, že $g = \gcd(408, 108) = 12$. Jak vyjádříme $g = 12$ jako lineární kombinaci 408 a 108? Přečteme si příslušný běh Euklidova algoritmu od konce.

Číslo 12 vzniklo z předchozích dvou řádků jako $g = 84 - 3 \cdot 24$. Řádek předtím dá $24 = 108 - 84$, a proto $g = 84 - 3 \cdot (108 - 84) = (-3) \cdot 108 + 4 \cdot 84$. První krok dá $84 = 408 - 3 \cdot 108$, a proto $g = (-3) \cdot 108 + 4 \cdot (408 - 3 \cdot 108) = 4 \cdot 408 + (-15) \cdot 108$.

Máme $\gcd(408, 108) = 4 \cdot 408 + (-15) \cdot 108$.

△

Tento zpětný chod je možné použít kdykoliv, je to ale pracné. Ukážeme, že žádanou lineární kombinaci lze najít přímo v průběhu Euklidova algoritmu.

Příklad 1b.k: Hledáme vyjádření $12 = A \cdot 408 + B \cdot 108$. Když už to neumíme uhodnout, zkusíme alespoň vyjádřit jiná čísla jako lineární kombinaci vstupů. Hned dvě se nabízejí.

$$408 = 1 \cdot 408 + 0 \cdot 108$$
$$108 = 0 \cdot 408 + 1 \cdot 108$$

Euklidův algoritmus nám dovoluje získat ze vstupů 408, 108 menší číslo, jmenovitě tak, že odečteme od prvního třikrát to druhé. My ovšem takto můžeme odečítat celé rovnosti a pravidla pro práci s rovnicemi říkají, že nová rovnost bude také platit. Dostáváme následující:

$$\begin{aligned} 408 &= 1 \cdot 408 + 0 \cdot 108 \\ 108 &= 0 \cdot 408 + 1 \cdot 108 \qquad \Big/ \ (\#1) - 3 \times (\#2) \\ 408 - 3 \cdot 108 &= 1 \cdot 408 + 0 \cdot 108 - 3 \cdot (0 \cdot 408 + 1 \cdot 108) \end{aligned}$$

My ovšem napravo potřebujeme zachovat čísla 408 a 108, proto je nezahrneme do výpočtů a jen si zjistíme, kolikrát se tam které objeví:

$$\begin{aligned} 84 &= (1 - 3 \cdot 0) \cdot 408 + (0 - 3 \cdot 1) \cdot 108 \\ &= 1 \cdot 408 + (-3) \cdot 108. \end{aligned}$$

Dostáváme tak Bezoutovo vyjádření pro nové číslo 84.

Ted umíme Bezoutovsky vyjádřit čísla 108 a 84, tak se podíváme pro inspiraci do Euklidova algoritmu a dozvíme se, že odečtením druhého od prvního získáme ještě menší číslo, jmenovitě 24. Opět místo toho odečteme celou poslední rovnost od předposlední:

$$\begin{aligned} 108 &= 0 \cdot 408 + 1 \cdot 108 \\ 84 &= 1 \cdot 408 + (-3) \cdot 108 \qquad \Big/ \ (\#1) - 1 \times (\#2) \\ 24 &= 0 \cdot 408 + 1 \cdot 108 - 1 \cdot (1 \cdot 408 + (-3) \cdot 108) \\ &= (0 - 1 \cdot 1) \cdot 408 + (1 - 1 \cdot (-3)) \cdot 108 \\ &= (-1) \cdot 408 + 4 \cdot 108. \end{aligned}$$

Podle Euklidova algoritmu bychom měli poslední rovnost odečíst třikrát od předposlední. Rovnou si napravo pohlídáme, kolikrát se vyskytne 408 a kolikrát 108:

$$\begin{aligned} 84 &= 1 \cdot 408 + (-3) \cdot 108 \\ 24 &= (-1) \cdot 408 + 4 \cdot 108 \qquad \Big/ \ (\#1) - 3 \times (\#2) \\ 12 &= (1 - 3 \cdot (-1)) \cdot 408 + ((-3) - 3 \cdot 4) \cdot 108 \\ &= 4 \cdot 408 + (-15) \cdot 108. \end{aligned}$$

Dostali jsme Bezoutovu identitu pro $12 = \gcd(408, 108)$.

Podstatné je, že čísla 408 a 108 se napravo vůbec neúčastnila výpočtů, jen hlídala, aby se ty koeficienty u nich správně skládaly a navzájem nepomíchaly. Lépe to bude vidět, když si místo nich představíme symboly:

$$\begin{aligned} 84 &= 1\heartsuit + (-3)\diamondsuit \\ 24 &= (-1)\heartsuit + 4\diamondsuit \qquad \Big/ \ (\#1) - 3 \times (\#2) \\ 12 &= (1 - 3 \cdot (-1))\heartsuit + ((-3) - 3 \cdot 4)\diamondsuit \\ &= 4\heartsuit + (-15)\diamondsuit. \end{aligned}$$

Vidíme, že když kombinujeme řádky, tak spolu čísla reagují ve sloupcích, ve třech oddělených skupinách. Takže vlastně vůbec nepotřebujeme rovnítka a symboly, stačí tři sloupce s daty:

$$\begin{array}{ccc} 84 & 1 & -3 \\ 24 & -1 & 4 \\ (84-3\cdot 24) & 1-3\cdot(-1) & (-3)-3\cdot 4 \\ 12 & 4 & -15 \end{array} \quad \Big/ \ (\#1)-3\times(\#2)$$

Základní operací v Euklidovském algoritmu je, že dolní číslo několikrát odečteme od horního. Všimněte si, že jsme to udělali v levém sloupci a pak přesně stejnou operaci zopakovali v dalších dvou sloupcích. Vždy to bylo „horní mínus třikrát dolní“. Pokud je čtenář seznámen s řádkovými operacemi s maticemi, tak to je přesně ono. Máme řádky čísel a ty násobíme a odčítáme tak, že vždy totéž provedeme všem číslům v řádku. Jinak řečeno, ve sloupcích se věci vždy dějí stejně a synchronně.

Při rozhodování, jakou operaci aplikovat na poslední dvě rovnosti (či řádky v našem schématu) jsme se řídili levým sloupcem a Euklidovským algoritmem. Jakmile jsme se vlevo k něčemu rozhodli, pak jsme totéž aplikovali také na čísla v pravých dvou sloupcích, které v každém řádku ukazují Bezoutovy koeficienty k vyjádření čísla nalevo (to víme, když si místo schématu zase napíšeme plné rovnosti). Tato operace se dá zakódovat číslem q (odečteme poslední rovnost/řádek q-krát od předposledního), které najdeme jako částečný podíl čísel v levém sloupci.

Shrňme si celý postup:

$$\begin{array}{ccc|ll} 408 & 1 & 0 & & \\ 108 & 0 & 1 & \swarrow\ (\#1)-3\times(\#2) & [q=3] \\ 84 & 1 & -3 & \swarrow\ (\#1)-1\times(\#2) & [q=1] \\ 24 & -1 & 4 & \swarrow\ (\#1)-3\times(\#2) & [q=3] \\ 12 & 4 & -15 & \swarrow\ (\#1)-2\times(\#2) & [q=2] \\ 0 & -9 & 34 & & \end{array}$$

Můžeme si všimnout, že levý sloupec a také sloupec čísel q odpovídají zápisu z příkladu 1b.g. My jsme jen přidali další dva sloupce a v nich napodobovali operace z levého sloupce.

Protože každý řádek kóduje rovnost, víme, že v něm dvě čísla vpravo jsou Bezoutovy koeficienty pro číslo vlevo. To, ke kterému číslu který koeficient patří, se pozná z prvních dvou řádků. Ve sloupci vpravo vidíme jedničku v řádku druhém, který kóduje $108 = 1\cdot 108$. Tento sloupec tedy označuje koeficient příslušný k druhému číslu 108. V prostředním sloupci jednička odkazuje na první řádek a číslo $408 = 1\cdot 408$. Proto dostáváme $12 = 4\cdot 408 + (-5)\cdot 108$.

Na závěr se ještě vraťme k otázce urychlení pomocí záporných zbytků. Všimneme si, že z čísel 84 a 24 lze získat 12 i -12. Pokud bychom volili druhou variantu, náš výpočet by skončil takto:

$$\begin{array}{ccc|ll} 84 & 1 & -3 & \swarrow\ (\#1)-1\times(\#2) & [q=1] \\ 24 & -1 & 4 & \swarrow\ (\#1)-4\times(\#2) & [q=4] \\ -12 & 5 & -19 & \swarrow\ (\#1)+2\times(\#2) & [q=-2] \\ 0 & 9 & 34 & & \end{array}$$

Předposlední řádek kóduje rovnost $-12 = 5\cdot 408 + (-19)\cdot 108$. Vynásobením číslem -1 získáme

$$12 = (-5)\cdot 408 + 19\cdot 108.$$

Tuto identitu také můžeme získat vynásobením předposledního řádku číslem -1, což je povoleno (řádek kóduje dotyčnou rovnos) a lze to zahrnout jako součást postupu.

Všimneme si, že vyšla jiná Bezoutova identita než u standardního algoritmu. Opět připomínáme, že Bezoutových identit je nekonečně mnoho. Jistě preferujeme co nejekonomičtější variantu, tedy takovou, kde koeficienty jsou v rámci možností co nejmenší. V kapitole 14 dokážeme, že standardní Euklidův algoritmus poskytuje právě takovéto koeficienty, zatímco u verze se zápornými zbytky už to není zaručeno.

△

Popsaný postup generuje tři druhy čísel. V levém sloupci jde o čísla r_k z Euklidova algoritmu, v dalších sloupcích máme čísla A_k, B_k, která v každém řádku kódují Bezoutovu identitu pro r_k. Čísla A_k, B_k se mění stejným posunovým způsobem jako r_k, takže tentokráte nestačí psát r_k jako zbytky, ale musíme se zabývat tím, jak vznikají, tedy potřebujeme pracovat s částečnými podíly q_k. Ty splňují $r_{k+1} = r_{k-1} - q_k r_k$, stejný vzorec s tímto q_k se pak aplikuje na A_k a B_k.

Zase ukážeme dva algoritmy, jeden si pamatuje průběh a druhý šetří místo. Rovnou je upravíme tak, aby byly schopny pracovat s libovolnými vstupy, jak jsme to diskutovali u Euklidova algoritmu. Pak se může stát, že algoritmus nabídne záporného kandidáta na gcd, což pak musíme opravit. Tím se nám také otevře možnost používat záporné zbytky. Vše záleží na tom, podle jakého kritéria určujeme q_k, buď se chceme dostat co nejblíže

k nule, ale ne zleva (standardní algoritmus), nebo prostě jen co nejblíže. V obou případech lze q_k určit z podílu $\frac{r_{k-1}}{r_k}$ nebo prací s posuny, to necháme na uživateli.

S Algoritmus 1b.32.
Rozšířený Euklidův algoritmus pro nalezení $\gcd(a,b) = Aa + Bb$ pro $a, b \in \mathbb{Z}$.

Verze 1.
Inicializace: $r_0 := a$, $r_1 := b$, $k := 0$,
$A_0 := 1$, $A_1 := 0$, $B_0 := 0$, $B_1 := 1$.
Dokud platí $r_{k+1} \neq 0$, opakovat kroky:
$k := k + 1$,
volba q_k aby $r_{k-1} - q_k r_k$ optimální,
$r_{k+1} := r_{k-1} - q_k r_k$,
$A_{k+1} := A_{k-1} - q_k A_k$,
$B_{k+1} := B_{k-1} - q_k B_k$.
Pokud $r_k < 0$, změnit znaménka u r_k, A_k, B_k.
Pak $\gcd(a,b) = r_k = A_k a + B_k b$.

Verze 2.
`procedure` *gcd-Bezout* (a, b: integer)
$A_0 := 1$; $A_1 := 0$; $B_0 := 0$; $B_1 := 1$;
`while` $b \neq 0$ `do`
`fix` q `to get` $a - q \cdot b$ `optimal`
$r := a - qb$;
$r_a := A_0 - qA_1$;
$r_b := B_0 - qB_1$;
$a := b$; $b := r$;
$A_0 := A_1$; $A_1 := r_a$;
$B_0 := B_1$; $B_1 := r_b$;
`If` $a < 0$ `do` $a := -a$, $A_0 := -A_0$, $B_0 := -B_0$;
`output:` a, A_0, B_0;

△

Poznamenejme, že pořád platí $r_{k+1} = r_{k-1} \bmod r_k$ jako v Euklidově algoritmu, ale obdobný vztah neplatí pro A_k a B_k, protože při jejich výpočtu nepoužíváme „jejich“ q, ale q_k získané z výpočtu $r_{k-1} \bmod r_k$.

S Příklad 1b.l (ruční výpočet Bezoutovy identity: kladná čísla)**:**
Spočítáme $\gcd(380, 131)$, viz příklad 1b.i.

Připravíme si tabulku. Do levého sloupce dáme vstupní data v pořadí velký/malý, přesně jako u Euklidova algoritmu. Vedle připojíme dva pomocné sloupce a doplníme nuly a jedničky, rozmístění vpravo (viz jednotková matice) odpovídá algoritmu výše.

a, b	(380)	(131)
380	1	0
131	0	1

Obvykle se nadepisují A, B jako v Bezoutově identitě, ale to pomáhá, jen pokud jsme správně označili data. Při praktickém počítání je klíčové navázání jednotlivých pomocných sloupců na vstupní data. V prvním řádku začínajícím číslem 380 vidíme jedničku v levém pomocném sloupci, proto je tento svázán s 380 a napsali jsme si to do záhlaví. Obdobně nám druhý řádek pozicí jedničky ukáže, že sloupec vpravo je navázán na číslo 131.

Pak zahájíme první krok. Stejně jako u Euklidova algoritmu usoudíme v levém sloupci, že z pozice 380 se nejblíže k nule zprava dostaneme dvojnásobným odečtením čísla 131. Provedeme tedy operaci „horní mínus dvakrát dolní“ v levém sloupci a pak zcela stejnou operaci aplikujeme na pomocné sloupce a čísla, která tam máme. V levém pomocném sloupci tedy počítáme $1 - 2 \cdot 0$ a v pravém $0 - 2 \cdot 1$. Operaci jsme zaznačili standardním q a intuitivním značením vlevo.

	a, b	(380)	(131)	q
	380	1	0	
$-2\times$	131	0	1	2
	118	1	−2	

Takto pokračujem. V druhém kroku použijeme ve všech třech sloupcích operaci „horní mínus dolní“, další řádek vznikne operací „horní mínus devětkrát dolní“ a tak dále. V posledním kroku jsme mohli zkončit hned, když jsme v levém sloupci dostali nulu, ale řádek jsme dokončili z cvičných důvodů. Nad nulou vidíme $\gcd(380, 131)$ a vpravo od něj Bezoutovy koeficienty, v záhlaví pomocných sloupců už jsme si zaznačili, ke kterým datům patří. Máme tedy následující výsledek:

	a, b	(380)	(131)	q
	380	1	0	
$-2\times$	131	0	1	2
$-1\times$	118	1	−2	1
$-9\times$	13	−1	3	9
$-13\times$	1•	10•	−29•	13
	0	−131	380	

$$\gcd(380, 131) = 1 = 10 \cdot 380 + (-29) \cdot 131.$$

Čtenář si může rozmyslet, zda mu pomáhá značit si operace, aby je ve všech třech sloupcích dělal stejně (mi ano), popřípadě který způsob mu vyhovuje.

Je dobré mít stále na paměti, že při práci s řádky pracujeme s rovnostmi, přesněji řečeno s lineárními kombinacemi vyjadřujícími číslo vlevo. Obdoba Bezoutova vyjádření tak funguje v každém řádku, například opravdu platí (viz tabulka)

$$13 = (-1) \cdot 380 + 3 \cdot 131.$$

Toto pochopení nám později umožní přizpůsobit si algoritmus našim potřebám.
△

Tato rozšířená verze Euklidova algoritmu s ním sdílí řadu vlastností, třeba poznatky týkající se rychlosti. Tabulka v příkladu ovšem naznačuje i další věci. Například si všimneme znaménka mínus, které putuje dolů pomocnými sloupci metodou cik-cak. Toto je pravidlem pro kladné vstupy. Také jste si jistě všimli, že se v posledním (nulovém) řádku zase objevila vstupní data (až na to putující znaménko). To pravidlem není, jak ukazuje příklad 1b.k, ale evidentně tohle nemohlo vzniknout náhodou. Ve skutečnosti v nulovém řádku najdeme (až na znaménko) vstupní data dělená jejich gcd. Důkaz najdeme jako obvykle v kapitole 14, kde také najdete důkaz věty, že rozšířený Euklidův algoritmus dělá, co má, a další poznatky.

Podívejme se na možnosti výpočtu pro obecné vstupy.

S Příklad 1b.m (ruční výpočet Bezoutovy identity: obecná čísla)**:**

Spočítáme $\gcd(131,-380)$.

1) Přímá aplikace algoritmu na vstupní data.

Data nasázíme v pořadí, ve kterém přišla, abychom pak i Bezoutovy koeficienty dostali ve správném pořadí. Sice to bude o krok delší, protože máme nahoře menší číslo, ale jsme počítač a tak nám to nevadí. Jako obvykle jsme si podle jedniček v prvních dvou řádcích ujasnili, ke komu se vztahují koeficienty v pomocných sloupcích.

	a,b	(131)	(−380)	q
	131	1	0	
$-0\times$	−380	0	1	0
$+3\times$	131	1	0	−3
$-10\times$	13	3	1	10
$-13\times$	1•	−29•	−10•	13
	0	380	131	

Pak jsme použili standardní Euklidův algoritmus se zbytky. Dle očekávání si algoritmus v prvním kroku upravil pořadí. Po přiměřeném počtu kroků jsme dospěli k nule a můžeme napsat Bezoutovu identitu, kde v ní chceme zachovat vstupní data včetně pořadí.

$$\gcd(131,-380)=1=(-29)\cdot 131+(-10)\cdot(-380).$$

Toto je vhodný postup pro počítač a pro studenty, kteří si věří. Pokud mají rádi adrenalinové sporty, mohou ještě použít modifikaci se zápornými zbytky (pokud nám nevadí, že nemusí dávat optimální verzi Bezoutovy identity). Zrovna v tomto příkladě by to vedlo na stejný běh, protože všechny obdržené zbytky byly optimální.

2) Bezpečná verze.

Tento postup nejprve najde Bezoutovu identitu pro kladná vstupní data vhodně seřazená podle velikosti, tedy místo $\gcd(131,-380)$ se hledá $\gcd(380,131)$. To už jsme dělali a došli jsme k identitě

$$\gcd(380,131)=1=10\cdot 380+(-29)\cdot 131.$$

Nyní zaměníme pořadí čísel nalevo a napravo a v gcd snadno upravíme znaménka.

$$\gcd(131,-380)=1=(-29)\cdot 131+10\cdot 380.$$

	a,b	(380)	(131)	q
	380	1	0	
$-2\times$	131	0	1	2
$-1\times$	118	1	−2	1
$-9\times$	13	−1	3	9
$-13\times$	1•	10•	−29•	13
	0	−131	380	

Ještě potřebujeme upravit napravo znaménko u 380. Někdy si jej stačí půjčit od odpovídajícího koeficientu, zde to uděláme tak, že přidáme mínus k našemu číslu i ke koeficientu.

$$\gcd(131,-380)=1=(-29)\cdot 131+(-10)\cdot(-380).$$

Výhodou tohoto postupu je větší spolehlivost při ručním výpočtu. Nevýhodou nutnost zpracování výsledku.

3) Chytrá aplikace algoritmu na vstupní data (rychlá verze).

Ukážeme si ji na úloze $\gcd(-131,380)$.

Data vložíme do tabulky včetně znamének, ale v pořadí větší-menší, tedy prohodili jsme je. Tím se ale prohodil i význam pracovních sloupců. Možná by se nám líbilo, kdyby pomocné sloupce odpovídaly původnímu pořadí dat, tedy abychom mohli na konci přímo napsat Bezoutovu identitu. Toho dosáhneme změnou pozice jedniček v prvních řádcích. Pokud chceme mít sloupec koeficientu u 380 jako druhý, tak také jednička v řádku začínajícím 380 musí být až na druhém místě. Obdobně u řádku začínajícím 131.

	a,b	(−131)	(380)	q
	380	0	1	
$+3\times$	−131	1	0	−3
$-10\times$	−13	3	1	10
$-13\times$	−1	−29	−10	13
	0	380	131	
$\cdot(-1)$	1•	29•	10•	

Pak jsme použili rychlý Euklidův algoritmus se zápornými zbytky. Dostali jsme řádek, kde kandidát na gcd byl záporný, proto jsme přidali ještě jeden krok, ten řádek jsme vynásobili celý mínus jedničkou (což je povolená operace pro práci s rovností, která je schovaná za dotyčným řádkem). V pracovních sloupcích pak přečteme správnou identitu.

$$\gcd(-131,380)=1=29\cdot(-131)+10\cdot 380.$$

Je dobré si všimnout, že tuto identitu bychom dostali čistě reorganizací identity pro $\gcd(131,-380)$ tak, aby vstupní data dostala správné znaménko.

4) Chytrá aplikace algoritmu na vstupní data (bezpečná verze).

Namísto vstupních dat $131,-380$ jsme do algoritmu vložili správně seřazené kladné verze. Zároveň ale chceme v pomocných sloupcích dostat správné koeficienty ve správném pořadí. Toho dosáhneme jednak prohozením jedniček a jednak úpravou znaménka. Rovnost kodovaná druhým řádkem teď zní $131=(-1)\cdot(-131)+0\cdot 380$, takže pracuje se správnými daty.

	a,b	(-131)	(380)	q
	380	0	1	
$-2\times$	131	-1	0	2
$-1\times$	118	2	1	1
$-8\times$	13	-3	-1	9
$-13\times$	1•	29•	10•	13
	0	-131	380	

Standardní Euklidův algoritmus nás dovedl do cíle a v řádku začínajícím jedničkou vidíme správné koeficienty pro žádanou Bezoutovu identitu:

$$\gcd(-131,380)=1=29\cdot(-131)+10\cdot 380.$$

Pro počítač je samozřejmě jasnou volbou první verze, tedy přímá aplikace algoritmu na vstupní data a výpočet se zápornými zbytky. Nabízí se otázka, proč zde rozebíráme možnosti, kterí mají smysl jen pro ruční výpočet, který nakonec dělat nebudeme. Odpověd zní, že nám to pomohlo lépe si ujasnit flexibilitu spojenou s tímto algoritmem a také si tam třeba našel svého favorita student, který bude muset přece jen něco počítat ručně.
△

Ve cvičení 1b.12 jsme se podívali na možnost zavedení pojmu největšího společného dělitele pro více čísel. Není to nic překvapivého, funguje to tak, jak by člověk čekal, stejně jako nejmenší společný násobek. Zajímavá otázka je, jak si s touto situací poradí Euklidův algoritmus. Odpověď zní, že s přehledem, a to včetně rozšířené verze a záporných zbytků. Blíže se na toto podíváme v sekci 16.6.

Cvičení

Cvičení 1b.1 (rutinní)**:** Pro následující dvojice $a,b\in\mathbb{Z}$ najděte $\gcd(a,b)$ a $\operatorname{lcm}(a,b)$ faktorizací, pak potvrďte $\gcd(a,b)$ rozšířeným Euklidovým algoritmem a napište příslušnou Bezoutovu identitu.
(i) $a=420,b=231$; (ii) $a=60,b=156$; (iii) $a=118,b=131$.

Cvičení 1b.2 (rutinní)**:** Pro následující dvojice $a,b\in\mathbb{Z}$ najděte $\gcd(a,b)$ a příslušnou Bezoutovu identitu.
(i) $a=-299,b=130$; (ii) $a=221,b=-136$; (iii) $a=353,b=-605$.

Cvičení 1b.3 (rutinní, poučné)**:** Dokažte, že pro $a\in\mathbb{N}$ platí $\gcd(a,0)=|a|$ a $\gcd(a,a)=\operatorname{lcm}(a,a)=|a|$ (viz fakt 1b.8).

Cvičení 1b.4 (rutinní, poučné)**:** Dokažte, že pro $b\in\mathbb{Z}$ platí $\gcd(1,b)=1$ a $\operatorname{lcm}(1,b)=|b|$.

Cvičení 1b.5 (poučné)**:** Přesvědčte se, že odhady $\gcd(a,b)\le\min(|a|,|b|)$ a $\operatorname{lcm}(a,b)\ge\max(|a|,|b|)$ (viz fakt 1b.5) neplatí v případě, že jedno z čísel je nulové a druhé ne.
Najděte alternativní odhady, které už platí pro všechna $a,b\in\mathbb{Z}$.
Nápověda: Víme, jaké výsledky a odhady máme pro případy s nulami.
Pro $\gcd(a,b)$ je třeba najít vzorec $V(a,b)$, který by splňoval $\min(|a|,|b|)\le V(a,b)$ a také $|b|\le V(|a|,|b|)$ a $|a|\le V(|a|,|b|)$.
Pro $\operatorname{lcm}(a,b)$ je třeba najít vzorec $W(a,b)$, který by splňoval $\max(|a|,|b|)\ge W(a,b)$ a také $W(0,|b|)=0$ a $W(|a|,0)=0$.

Cvičení 1b.6 (rutinní, poučné)**:** Dokažte, že pro $a\in\mathbb{Z}$ platí:
(i) $\gcd(a,ka)=|a|$ a $\operatorname{lcm}(a,ka)=|ka|$ pro libovolné $k\in\mathbb{Z}$;
(ii) $\gcd(a,a^k)=|a|$ a $\operatorname{lcm}(a,a^k)=|a^k|$ pro libovolné $k\in\mathbb{N}$.

Cvičení 1b.7 (poučné)**:**
Ve faktu 1b.11 jsme dokázali, že pro $a,b\in\mathbb{Z}$ platí: Jestliže $a\,|\,b$, pak $\gcd(a,b)=|a|$.
(i) Dokažte toto tvrzení pro $a,b\in\mathbb{N}$ pomocí věty 1b.17.
(ii) Dokažte toto tvrzení pro $a,b\in\mathbb{N}$ pomocí Bezoutovy identity.
Nápověda: Bezoutova identita poskytne pouze jednu nerovnost, druhou je třeba přidat jinak.

Cvičení 1b.8 (poučné)**:** Nechť $a,b\in\mathbb{Z}$, $a,b\neq 0$. Dokažte, že $\gcd(a,b)=1$ právě tehdy, když $\operatorname{lcm}(a,b)=|a|\cdot|b|$.
Poznámka: Rozmyslete si, že $\gcd(a,b)=1\implies\operatorname{lcm}(a,b)=|a|\cdot|b|$ platí i v případě nul. Najděte protipříklad pro opačnou implikaci.

Cvičení 1b.9 (dobré, poučné)**:** Dokažte, že pro každé $a, b, k \in \mathbb{Z}$, $k \neq 0$ platí: Jestliže k dělí a i b, pak $|k| \gcd\left(\frac{a}{k}, \frac{b}{k}\right) = \gcd(a, b)$.
Použijte k tomu fakt, že $|k| \gcd(a, b) = \gcd(ka, kb)$, viz věta 1b.17.

Cvičení 1b.10 (poučné)**:** Nechť $a, b, c \in \mathbb{Z}$. Dokažte, že jestliže $a \,|\, c$, $b \,|\, c$ a $\gcd(a, b) = 1$, pak $(ab) \,|\, c$.
Nápověda: Podívejte se na důkaz Euklidova lemmatu 1b.20.

Cvičení 1b.11 (dobré)**:** Dokažte, že pro každé $a, b, c \in \mathbb{N}$ platí, že $\gcd(a, bc)$ dělí $\gcd(a, b) \cdot \gcd(a, c)$

Cvičení 1b.12 (poučné)**:**
Jak zobecníme pojem gcd a lcm pro více čísel? Pro nenulová $a_1, \ldots, a_n \in \mathbb{Z}$ definujeme $\gcd(a_1, a_2, \ldots, a_n)$ jako největší přirozené číslo d splňující vlastnost, že $d \,|\, a_i$ pro všechna i, obdobně $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$ definujeme jako nejmenší přirozené číslo m splňující vlastnost, že $a_i \,|\, m$ pro všechna i.
Dokažte následující:
Nechť $a, b, c \in \mathbb{N}$ jsou libovolná. Nechť $g = \gcd(a, b, c)$. Pak $g = \gcd(\gcd(a, b), c)$.

Cvičení 1b.13 (poučné)**:** Jaký je obecný vztah mezi čísly $\gcd(a, b)$ a $\gcd(a, b, c)$, kde $a, b, c \in \mathbb{N}$ jsou libovolné?

Cvičení 1b.14 (dobré, poučné)**:** Nechť $a_1, a_2, \ldots, a_n \in \mathbb{N}$. Využijte lemma 1b.24 k důkazu, že když jsou a_i po dvou nesoudělná, pak $\operatorname{lcm}(a_1, a_2, \ldots, a_n) = a_1 \cdot a_2 \cdots a_n$.

Cvičení 1b.15 (dobré, poučné)**:** Nechť $a_1, a_2, \ldots, a_n \in \mathbb{N}$.
Rozmyslete si, zda platí $\operatorname{lcm}(a_1, a_2, \ldots, a_n) = \frac{a_1 \cdot a_2 \cdots a_n}{\gcd(a_1, a_2, \ldots, a_n)}$.

Řešení:

1b.1: (i):

420	1	0	
231	0	1	1
189	1	−1	1
42	−1	2	4
21•	5•	−9•	2
0			

$\gcd(2^2 \cdot 3 \cdot 5 \cdot 7, 3 \cdot 7 \cdot 11) = 3 \cdot 7 = 21$
$\operatorname{lcm}(2^2 \cdot 3 \cdot 5 \cdot 7, 3 \cdot 7 \cdot 11) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 4620$
$\gcd(420, 231) = 21 = 5 \cdot 420 + (-9) \cdot 231$

(ii):

156	1	0	
60	0	1	2
36	1	−2	1
24	−1	3	1
12•	2•	−5•	2
0			

$\gcd(2^2 \cdot 3 \cdot 5, 2^2 \cdot 3 \cdot 13) = 2^2 \cdot 3 = 12$
$\operatorname{lcm}(2^2 \cdot 3 \cdot 5, 2^2 \cdot 3 \cdot 13) = 2^2 \cdot 3 \cdot 5 \cdot 13 = 780$
$\gcd(60, 156) = 12 = (-5) \cdot 60 + 2 \cdot 156$

(iii):

131	1	0	
18	0	1	1
13	1	−1	9
1•	−9•	10•	13
0			

$\gcd(131, 2 \cdot 59) = 1$
$\operatorname{lcm}(131, 2 \cdot 59) = 131 \cdot 2 \cdot 59 = 15458$
$\gcd(118, 131) = 1 = 10 \cdot 118 + (-9) \cdot 131$

1b.2: (i):

−299	1	0	
130	0	1	−3
91	1	3	1
39	−1	−2	2
13•	3•	7•	3
0			

$\gcd(-2990, 130) = 13 = 3 \cdot (-299) + 7 \cdot 130$

(ii):

221	1	0	
−136	0	1	−1
85	1	1	−2
34	2	3	2
17•	−3•	−5•	2
0			

$\gcd(221, -136) = 17 = (-3) \cdot 221 + (-5) \cdot (-136)$

(iii):

−605	1	0	
353	0	1	−2
101	1	2	3
50	−3	−5	2
1•	7•	12•	50
0			

$\gcd(353, -605) = 1 = 12 \cdot 353 + 7 \cdot (-605)$

1b.3: Libovolné $d \in \mathbb{N}$ dělí 0, proto je množina společných dělitelů $a, 0$ totožná s množinou dělitelů $d \in \mathbb{N}$ čísla a. Takoví dělitelé nutně splňují $d \leq |a|$ a víme, že také $|a| \,|\, a$, tudíž $|a|$ náleží do množiny společných dělitelů a je tam největší.
$\gcd(a, a)$ má být největší dělitel a, což je samozřejmě $|a|$. Důkaz pro $\operatorname{lcm}(a, a)$ je obdobný.
1b.4: Případ $b = 0$ dává $\gcd(1, 0) = 1$ a $\operatorname{lcm}(1, 0) = 0 = |b|$.
Případ $b \neq 0$: 1 dělí 1 i b. Pokud je d společný dělitel 1 a b, tak z $d \,|\, 1$ máme $d \leq 1$. Tedy 1 je největší společný dělitel.
$|b|$ je násobkem 1 i b. Pokud je m společný násobek 1 a b, tak $b \,|\, m$, proto $|b| \,|\, m$ a tedy $|b| \leq m$.
1b.5: Nabízí se $\gcd(a, b) \leq \max(|a|, |b|)$ a $\operatorname{lcm}(a, b) \geq \min(|a|, |b|)$.
1b.6: 1) Případ $a = 0$ dává $\gcd(a, ka) = \gcd(0, 0) = 0 = |a|$ a $\gcd(a, a^k) = \gcd(0, 0) = 0 = |a|$,
$\operatorname{lcm}(a, ka) = \operatorname{lcm}(0, 0) = 0 = |ka|$ a $\operatorname{lcm}(a, a^k) = \operatorname{lcm}(0, 0) = 0 = |ka|$,
2) Případ $a \neq 0$.
(i) Kdyby $k = 0$, tak $\gcd(a, ka) = \gcd(a, 0) = |a|$ a $\operatorname{lcm}(a, ka) = \operatorname{lcm}(a, 0) = 0 = |ka|$.
Dále tedy předpokládejme $a, k \neq 0$.
Protože $|a| > 0$ dělí a i ka, je to jejich společný dělitel. Je největší, protože libovolný společný dělitel d musí dělit a a proto $d \leq |a|$.
Protože $|ka| > 0$ je násobkem a i ka, patří do množiny společných násobků. A protože každý společný násobek m musí splňovat $m \leq |ka|$, tak žádné menší číslo než $|ka|$ v té množině není.
(ii): Podobně jako (i), využijeme $k \geq 1$ a tedy $|a^k| \geq |a|$.
1b.7: (i) $a \,|\, b$ dává $b = ak$, $k \in \mathbb{Z}$. Protože $a > 0$, podle doporučené věty máme
$\gcd(a, b) = \gcd(a, ka) = a \gcd(1, k) = a \cdot 1 = k$.
(ii) $a \,|\, b$ dává $b = ak$. Pak lze napsat $a = (1 - k + k)a = (1 - k)a + ka = (1 - k)a + 1 \cdot b$. Toto je identita Bezoutova typu, což ukazuje, že $\gcd(a, b) \leq a$.
Ovšem a je společný dělitel a, b, takže nemůže být větší než ten největší, tedy $a \leq \gcd(a, b)$.
1b.8: Stačí použít $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = |a| \cdot |b|$. Protipříklad: $a = 0$, $b = 13$.
1b.9: Označte $\tilde{a} = \frac{a}{k}$ a $\tilde{b} = \frac{b}{k}$. Podle předpokladu $\tilde{a}, \tilde{b} \in \mathbb{Z}$, lze tedy aplikovat napovězený vzorec.
1b.10: Z předpokladů $c = ka$, $c = lb$ a $1 = Aa + Bb$, kde $k, l, A, B \in \mathbb{Z}$. Vynásobením Bezouta $c = Aac + Bbc = Aa(lb) + Bb(ka) = ab(Al + Bk)$ a $Al + Bk \in \mathbb{Z}$, tedy $(ab) \,|\, c$.
1b.11: Podle Bezouta $\gcd(a, b) = A_b a + Bb$ a $\gcd(a, c) = A_c a + Cc$.
Pak $\gcd(a, b) \gcd(a, c) = a(A_b A_c a + A_b Cc + A_c Bb) + bcBC$. $\gcd(a, bc)$ dělí a i bc, tudíž musí dělit i ten součin.
1b.12: Označme $G = \gcd(\gcd(a, b), c)$. 1) Z definice $G \,|\, c$ a $G \,|\, \gcd(a, b)$, odtud pak zase $G \,|\, a$ a $G \,|\, b$. Takže G je společný dělitel všech čísel a, b, c, tudíž $G \leq g$, neboť g je největší takový.
Největší společný dělitel g čísel a, b, c je to i společný dělitel a, b, tudíž musí platit $g \,|\, \gcd(a, b)$. Také $g \,|\, c$, takže g je společný dělitel čísel $\gcd(a, b)$ a c, tudíž $g \leq G$.
1b.13: Protože $\gcd(a, b, c)$ dělí a a b, je to jejich společný dělitel, proto $\gcd(a, b, c) \leq \gcd(a, b)$. Podle důsledku 1b.16 dokonce $\gcd(a, b, c)$ dělí $\gcd(a, b)$.
Toto se snadno zobecní, pokud je množina různých přirozených čísel $\{a_1, a_2, \ldots, a_n\}$ podmnožinou množiny různých přirozených čísel $\{b_1, b_2, \ldots, b_m\}$, pak $\gcd(b_1, \ldots, b_m)$ dělí $\gcd(a_1, \ldots, a_n)$.
1b.14: Protože je $m = a_1 \cdots a_n$ společným násobkem a_i, musí platit $\operatorname{lcm}(a_1, \ldots, a_n) \leq m$.
Protože $a_i \,|\, \operatorname{lcm}(a_1, \ldots, a_n)$ a a_i jsou po dvou nesoudělné, musí podle lemma 1b.24 platit $m \,|\, \operatorname{lcm}(a_1, \ldots, a_n)$ a tedy $m \leq \operatorname{lcm}(a_1, \ldots, a_n)$.
1b.15: Je dobré začít s co nejméně čísly, tedy třemi, a propracujeme se k situaci, kdy lze použít příslušný vzorec pro dvě čísla, kde je dokázán: $\operatorname{lcm}(a, b, c) = \operatorname{lcm}(\operatorname{lcm}(a, b), c) = \frac{\operatorname{lcm}(a,b)c}{\gcd(\operatorname{lcm}(a,b),c)} = \frac{abc}{\gcd(a,b)\gcd(\operatorname{lcm}(a,b),c)}$.
Mohlo by platit $\frac{abc}{\gcd(a,b)\gcd(\operatorname{lcm}(a,b),c)} = \frac{abc}{\gcd(a,b,c)}$ neboli $\gcd(a, b) \gcd(\operatorname{lcm}(a, b), c) = \gcd(a, b, c)$? Podle předchozího cvičení máme $\gcd(a, b) \geq \gcd(a, b, c)$, vzorec tedy bude fungovat jedině tehdy, když platí $\gcd(a, b) = \gcd(a, b, c)$ a $\gcd(\operatorname{lcm}(a, b), c) = 1$. To ovšem obecně platit nebude, takže ani onen zkoumaný vzorec platit obecně nemůže.
Jako protipříklad (inspirovaný předchozím rozborem) stačí vzít $a = 2$, $b = 3$ a $c = 4$, pak $\operatorname{lcm}(2, 3, 4) = 12$, zatímco $\frac{2 \cdot 3 \cdot 4}{\gcd(2,3,4)} = 24$.