2. Dělitelnost

Když nám bylo okolo desíti let, naučili jsme se dělit celá čísla. V této kapitole se na toto téma podíváme blíže a dostaneme se k zajímavým výsledkům. Některé z nich jsou vysoce užitečné v oblasti výpočetní techniky, tato kapitola také tvoří základ pro řešení diofantických rovnic (kapitola 4) a počítání modulo (kapitola 3).

2a. Dělitelnost

Začneme přesnou definicí situace, kdy můžeme celé číslo vydělit (beze zbytku) jiným. Jak už jsme vysvětlili v kapitole 1b, matematici preferují specifikaci, která nepoužívá operaci dělení.

Definice.
Nechť $a, b \in \mathbb{Z}$. Řekneme, že a **dělí** b, značeno $a \mid b$, jestliže existuje $k \in \mathbb{Z}$ takové, že $b = k \cdot a$. V takovém případě říkáme, že a je **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 $a \mid b$, if there is $k \in \mathbb{Z}$ such that $b = k \cdot a$. Then we say that a is a **factor** of b and that b is a **multiple** of a.

Příklad 2a.a: Evidentně $3 \mid 12$, protože $12 = 4 \cdot 3$, podmínka z definice je proto splněna s celým číslem $k = 4$.

Na druhou stranu neplatí $5 \mid 13$. My to samozřejmě víme, ale dokáže to poznat i definice? Umíme napsat $13 = k \cdot 5$? Samozřejmě. Má to ale háček, jediné takové k je $\frac{13}{5}$, což není celé číslo. Výrok z definice proto není splněn a tudíž opravdu 5 nedělí 13.

Chceme tím upozornit na jednu důležitou věc: Ta specifikace „$k \in \mathbb{Z}$“ není jen formalita, jako že každá proměnná se má odněkud brát, ale je to zároveň klíčová část definice, 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 je celé číslo. To je obvykle velmi snadné, ale to neznamená, že to lze opominout.
△

Je zjevné, že pojem dělitelnosti má něco společného s dělením. Například tu konstantu k v příkladě jsme mohli uhodnout, ale asi jsme spíš jen vydělili. Tato podobnost například svádí k tomu, abychom vztah, že a dělí b, v praxi nahrazovali podmínkou, že $\frac{b}{a}$ je celé číslo. Jak ale brzy uvidíme, není to totéž, a proto bychom se zlomkové formě měli v úvahách o dělitelnosti důsledně vyhýbat.

Již teď vidíme první rozdíl mezi dělením a dělitelností: Obojí sice pracuje s dvojicemi čísel, ale dělení je operace, která z té dvojice vyrobí nové číslo (které nás mimochodem v této kapitole až na pár výjimek nebude vůbec zajímat). Naopak dělitelnost je vztah, který pro danou rovnici je či není pravdivý. Dá se říci, že výstupem dělitelnosti je tedy pravdivostní hodnota. Na další rozdíly mezi těmito dvěma pojmy narazíme brzy. Myšlenka na dělení občas zejména začátečníky svádí na scestí, a proto bychom zde čtenáři poradili, aby se snažil spíš zapomenout, že umí dělit.

Pro některá populární čísla a existují triky, jak snadno poznat, která čísla jsou tímto a dělitelná, čtenář jistě zná kritérium pro dělitelost dvěma (číslo je sudé), pro další viz cvičení 2a.10 a 3a.13 a poznámka 3a.14.

Dělitelnost je velice důležitý pojem a to nejen v teorii čísel, často se používá například při práci s polynomy. Lze třeba říct, že polynom $x - 1$ dělí polynom $x^2 - 1$, protože $x^2 - 1 = (x - 1)(x + 1)$.

Matematici se o pojmech snaží zjistit, jaké mají vlastnosti a jak fungují, a dělitelnost není výjimku. Začneme něčím očividným.

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

S **Rozbor:** Podívejme se na (ii). Máme si vzít libovolné $a \in \mathbb{Z}$ coby reprezentanta všech celých čísel a ukázat, že dělí samo sebe. V typickém důkaze pracujeme s implikací, tedy díky předpokladu víme, odkud vycházíme, a také kam máme dojít. To nám pomáhá najít správné kroky. Tady ale žádný předpoklad není, jde o jednoduché tvrzení typu „tak to je“. Výchozí bod si tedy musíme vymyslet sami, což není vždy jednoduché najít.

Opět pomůže, když si rozmyslíme, co vlastně chceme. Potřebujeme čtenáře přesvědčit, že $a \mid a$, tedy podle definice chceme ověřit platnost vzorce $a = k \cdot a$ pro nějaké vhodné celočíselné k. Dokážeme toto uskutečnit? Pokud ano, pak víme, jak důkaz vést, a od kterého všeobecně známého faktu jej začít. Je to náš první pořádný důkaz, napíšeme jej podrobněji.

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

Důkaz (i) a (iii) je obdobný a tak snadný, že jej s důvěrou necháme jako cvičení 2a.2.

□

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

Ta poznámka 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 věnovat čas ověření, že jsou opravdu splněny (v tomto případě cca 0.7 sec).

Začátečníka může zarazit, že (ii) a (iii) lze aplikovat i na $a = 0$ (preambule říká $a \in \mathbb{Z}$, tedy lze mít i $a = 0$). Opravdu dělí nula nulu? O něco uvěřitelněji to vypadá, pokud použijeme alternativní názvosloví: Nula je násobkem nuly. Jistotu nám samozřejmě dá podmínka z definice. Existuje $k \in \mathbb{Z}$ tak, aby $0 = k \cdot 0$? Samozřejmě ano, třeba $k = 13$ bude fungovat. Potvrdili jsme, že $0 \,|\, 0$.

Můžeme si všimnout, že na rozdíl od úvodního příkladu zde to hledané k nedokážeme získat dělením, protože nulou dělit nelze, ani nulu. Vztah, který zde studujeme, ale mezi nulou a nulou existuje. Toto opět ukazuje, že pojem dělitelnosti se zásadně liší od dělení jako matematické operace a je dobré je nemíchat.

Práci s dělitelností nám usnadní užitečná pravidla.

Věta 2a.2.
Nechť $a, b, c \in \mathbb{Z}$.
(i) Jestliže $a \,|\, b$ a $a \,|\, c$, pak $a \,|\, (b + c)$.
(ii) Jestliže $a \,|\, b$, pak $a \,|\, (cb)$.
(iii) Jestliže $a \,|\, b$ a $b \,|\, c$, pak $a \,|\, c$.

S **Rozbor:** Podíváme se na důkaz (i). Výchozí situace je následující:

- Známo: a dělí b; a dělí c
- Chceme: a dělí $b + c$.

Napišme si přesně podle definice, co to vlastně znamená.

- Známo: $b = k \cdot a$ pro nějaké $k \in \mathbb{Z}$; $c = l \cdot a$ pro nějaké $l \in \mathbb{Z}$
- Chceme: $b + c = m \cdot a$ pro nějaké $m \in \mathbb{Z}$.

Za poznámku stojí, že v definici dělitelnosti se mluví o čísle k, ale toto písmeno lze zaměnit za libovolné jiné podle potřeby, viz 1a.5. V našem případě jsme použitím k v prvním řádku již určili jeho hodnotu. Sice ji neznáme, ale záleží na a a b a je pevně dána. Není žádný důvod, proč by stejné číslo muselo fungovat pro dvojici a a c, proto jsme tam museli použít jiné označení proměnné, abychom tomuto číslu dali volnost vybrat si svou hodnotu. Ta je pak ovšem čísly a a c pevně dána, tudíž potřebujeme ještě třetí písmeno pro $b + c$. Pokud bychom si jako cíl omylem vytyčili, že chceme dojít k $b + c = k \cdot a$, tak k němu nedokážeme dojít.

Jsme v situaci, kdy pomocí faktů z levého sloupce potřebujeme odvodit platnost výroku napravo. Má povahu existenčního výroku, formálně řečeno tam stojí, že existuje číslo m s určitou vlastností. Musíme tedy čtenáře přesvědčit, že toto m lze opravdu najít. Jeho hodnota záleží na tom, jaké je číslo $b + c$, konkrétněji bychom rádi číslo $b + c$ přepsali tak, aby se ve výsledku nějak objevilo číslo a. Nabízí se levý sloupec, kde vidíme informaci o b a c. Tím je už vlastně dán způsob, jak pomocí levého sloupce udělat pravý, tedy máme plán důkazu.

Důkaz (rutinní, poučný)**:** (i): Mějme $a, b \in \mathbb{Z}$ libovolné. Z předpokladu $a \,|\, b$ máme $b = ka$ pro nějaké konkrétní $k \in \mathbb{Z}$, podobně $c = la$ pro nějaké $l \in \mathbb{Z}$. Pak $b + c = (k + l)a$. Protože $k, l \in \mathbb{Z}$, platí i $m = k + l \in \mathbb{Z}$ a také $b + c = ma$, proto podle definice $a \,|\, (b + c)$.

(ii) a (iii) fungují obdobně, viz cvičení 2a.3.

□

Protože je to náš první důkaz s dělitelností, napsali jsme jej podrobněji. S přibývající zkušeností lze věci vynechat, například by se nepotřeboval symbol m, pracovalo by se přímo s číslem $k + l$. Uvidíme to v dalších důkazech. Upozorníme ještě na oblíbenou chybu méně zkušených dokazovačů, že se totiž nechají příliš fascinovat pravým sloupcem a začnou důkaz slovy „nechť $b + c = la$“. To je ale něco, co chceme dokázat, a proto z toho nelze vyjít, musíme k tomu dojít. Podrobněji viz 1c.2.

Poznatky z bodů (i) a (ii) se často spojují do jednoho tvrzení:

Důsledek 2a.3.
Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \,|\, b$ a $a \,|\, c$, pak pro všechny $\beta, \gamma \in \mathbb{Z}$ platí $a \,|\, (\beta b + \gamma c)$.

Naopak pokud známe platnost tohoto tvrzení, pak volbami $\beta = \gamma = 1$, popřípadě $\gamma = 0$ dostaneme zpětně tvrzení (i) a (ii) výše.

V úvodní kapitole jsme se zmínili, že matematici mají rádi ekvivalence. Naskýtá se zajímavá otázka, zda tvrzení 2a.2 (i) platí i v opačném směru, 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 jedné. To se občas hodí, tak si to vyjádříme způsobem, který ještě později párkrát použijeme.

Fakt 2a.4.
Nechť $a, b, c \in \mathbb{Z}$. Jestliže $a \,|\, (b + c)$ a $a \,|\, b$, pak $a \,|\, c$.

Šlo by to dokázat přímo prací s násobky (zkuste si to jako cvičení), ale ukážeme důkaz jiný, protože je na něm vidět jeden typický rys matematiky: matematici rádi recyklují již provedenou práci, aby ji nemuseli dělat znovu. Poskládáme tedy již známé výsledky: Z předpokladu $a \,|\, b$ díky větě 2a.2 (ii) dostaneme $a \,|\, (-b)$, máme také $a \,|\, (b+c)$ a tudíž podle věty 2a.2 (i) musí a dělit číslo $(b + c) + (-b) = c$. Hotovo.

→ Zhruba řečeno jsou dvě základní podoby důkazů. Je možné se hrabat v detailech, což by zde reprezentoval přímý důkaz pomocí násobků. Na druhou stranu v okamžiku, kdy už má člověk nějaké věci dokázané, je často možné získávat nové věci chytrým skládáním známého. Takovéto důkazy bývají obvykle kratší a také přehlednější, protože pozornost není rozptýlena upravováním výrazů a podobnou manuální prací. U mnoha tvrzení této knihy je na výběr, lze je dokázat přímo pomocí definic a mravenčí práce, nebo využitím již dokázaného. Matematici obvykle volí druhou cestu, ale jsou výjimky, protože přímý důkaz někdy dodá intuitivní ← pochopení situace.

Poznámka: Začátečníky někdy mate, že se při matematické práci písmenka různě mění a občas jakoby jedno dělalo více věcí. Například my jsme v důkazu, kde písmeno b značilo určité číslo, použili tvrzení z věty, kde mělo b jinou roli. Zde zase hraje roli ona lokálnost významu. Fomálně si lze pomoci přejmenováním symbolů. Můžeme si například vyjádřit část (i) věty 2a.2 takto:

- Jestliže $\alpha \,|\, \beta$ a $\alpha \,|\, \gamma$, pak $\alpha \,|\, (\beta + \gamma)$.

V našem důkazu pak toto aplikujeme v situaci, kdy $\alpha = a$, $\beta = b + c$ a $\gamma = -b$. Takovéto úpravy proměnných zvyšují pochopitelnost úvah, ale u snadnějších věcí se s tím lidem obvykle nechce zdržovat. Pro zkušeného není problém v jednodušších úvahách pracovat s „různými“ b jako v důkazu výše.
△

Jaká je souvislost mezi dělitelností a velikostí čísel?

Věta 2a.5.
Nechť $a, b \in \mathbb{Z}$.
(i) $a \,|\, b$ právě tehdy, když $|a|$ dělí $|b|$.
(ii) Jestliže $a \,|\, b$ a $b \neq 0$, tak $|a| \leq |b|$.

V části (i) vidíme logickou spojku ekvivalenci, což nás jistě těší, protože vazbu mezi těmi dvěma poznatky můžeme používat v obou směrech. Ekvivalence je vlastně jako implikace tam i zpět a přesně tak to dokážeme.

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

(i): $\Longrightarrow$: Předpokládejme, že $a \,|\, b$. Pak $b = ka$ pro nějaké $k \in \mathbb{Z}$. Odtud $|b| = |k| \cdot |a|$ a $|k| \in \mathbb{Z}$, tedy dle definice $|a| \,|\, |b|$.

$\Longrightarrow$: Předpokládejme, že $|a| \,|\, |b|$. Pak $|b| = k|a|$ 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 $z_a = \pm 1$. Dosadíme do vzorce z dělitelnosti: $bz_b = kaz_a$ neboli $b = \frac{kz_a}{z_b} \cdot a$. Protože $kz_a \in \mathbb{Z}$ a $z_b = \pm 1$, je $\frac{kz_a}{z_b} \in \mathbb{Z}$ a máme $a \,|\, b$.

Jiný přístup k důkazu (i) se uvede ve cvičení 2a.4.

(ii): $a \mid b$ dává $b = ka$ pro nějaké $k \in \mathbb{Z}$. Jestliže $b \neq 0$, tak také $k \neq 0$, tudíž $|k| \in \mathbb{N}$. To znamená, že $|k| \geq 1$ a proto $|b| = |k| \cdot |a| \geq |a|$.

□

Co jsme se dozvěděli? Bod (i) vlastně říká, že při dělitelnosti záleží jen na velikosti zúčastněných čísel, znaménko je irelevantní. Proto se někteří autoři od začátku omezují na dělitelnost nezáporných čísel. Tvrzení (ii) jistě nepřekvapilo, za zmínku stojí podmínka $b \neq 0$. Rozmyslete si, že v případě $b = 0$ umíte najít a takové, že $a \mid b$ a přitom $|a| > 0$. Je tedy důvod být opatrný.

Nula nám to bude komplikovat i na dalších stránkách. Nedivím se, že někteří autoři látku této kapitoly vykládají pouze pro čísla z $\mathbb{N}$. Pro praktické účely to téměř vždy stačí a ušetří si psaní. Z pohledu teorie je ale zajímavější mít úplnou informaci, tak se zde nebudeme omezovat.

Věta 2a.6.
Nechť $a, b \in \mathbb{N}_0$. Jestliže $a \mid b$ a $b \mid a$, pak $a = b$.

Toto tvrzení rozhodně neplatí na $\mathbb{Z}$. Například $13 \mid (-13)$ a $(-13) \mid 13$, ale neplatí $-13 = 13$. Máme tady názornou ukázku, že pokud bychom pracovali jen v $\mathbb{N}_0$, tak je nám lépe, protože máme k dispozici nástroje navíc. Tento rozdíl lze vystihnout jazykem relací, viz kapitola 7a.

Co se týče důkazu, nejjednodušší bude využít předchozího poznatku o dělitelnosti a velikosti zúčastněných čísel. Protože to ale neplatí v případě nuly, budeme ji muset rozebrat zvlášť.

Důkaz (rutinní)**:** $a, b \in \mathbb{Z}$ lib. Jestliže $a = 0$, tak b coby násobek nuly musí být také 0, tedy $a = b$. Pokud $b = 0$, dostáváme symetricky $a = 0$ a zase $a = b$.

Zbývá případ, kdy jsou a, b nenulová čísla. Podle věty 2a.5 (ii) 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 $a = b$.

□

I na dalších stránkách se budeme setkávat s případy, kdy nějaké tvrzení platí obecně, ale v důkazu budeme muset případ nuly řešit zvlášť. Je to nuda, ale přežijeme to.

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 $a = 13$ a $d = 3$ máme $13 = 4 \cdot 3 + 1$, ale také $13 = 2 \cdot 3 + 7$. 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 1 je správný zbytek po dělení 13 číslem 3, píšeme $13 \bmod 3 = 1$. Částečný podíl jsme uvedli jen pro úplnost, o dělení se tu nechceme bavit, nicméně přiznáme, že tu máme bonusovou sekci 2c, kde přeci jen o něm něco zmíníme (fakt 2c.5).

Tato definice je typu, kdy nic netestujeme, ale přímo řekneme, co chceme. Má to ale zásadní otázku: Existuje vůbec ta věc, kterou jsme právě označili jménem? Zajímavá otázka také je, kolik takových věcí případně existuje. V řadě situací se totiž hodí, aby jistý objekt existoval jen jeden. Na obojí otázky odpoví následující tvrzení.

Věta 2a.7. (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.

Situace je tedy nejlepší možná, zbytky existují a vždy je jen jeden. To mimo jiné znamená, že výraz $a \bmod d$ označuje jedno konkrétní číslo, takže jej můžeme pohodlně používat ve výpočtech. Důkaz na chvíli odložíme, při jeho psaní nám totiž pomůže, když se nejprve zamyslíme, jak se dá takový zbytek najít.

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. 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 $q < 0$). Kolikrát máme odebrat? Tak, aby výsledek byl mezi nulou a d (ostře), což lze zjistit zkusmo. Prostě (pro kladná čísla) od a opakovaně odečítáme d, dokud nejsme s výsledkem spokojeni, jmenovitě se snažíme dostat co nejblíže k nule. To se dá realizovat jednoduchou smyčkou a odečítání je pro počítač mnohem rychlejší (a vůbec bezproblémovější) operace než dělení.

Příklad 2a.b: Vyzkoušíme si to na našem příkladě $a = 13$ a $d = 3$, kde jsme už odhalili správný zbytkový zápis $13 = 4 \cdot 3 + 1$. Alternativa: Začínáme s $a = 13$, odečteme $d = 3$, dostaneme nové $a = 10$, to je moc. Zkusíme postupně $a = 10 - 3 = 7$, $a = 4$, $a = 1$ a jsme spokojeni.

Na první pohled to vypadá delší, ale pro velká čísla to i pro člověka může být příjemnější než dělit. Je to pro mnoho lidí i intuitivnější, když dojde na jiná čísla než kladná.

Uvažujme $a = -13$ a $d = -3$. Na první pohled by stačilo jen změnit znaménka v algebraické rovnosti na $-13 = 4 \cdot (-3) + (-1)$, což sice platí, ale nevyhovuje požadavku $r \geq 0$. Správně tedy musíme psát $-13 = 5 \cdot (-3) + 2$, tedy zbytek je 2, také psáno $-13 \bmod (-3) = 2$. Můžeme si také všimnout, že částečný podíl 13 a 3 byl 4, ale částečný podíl -13 a -3 je 5.

Ne že by to bylo těžké, ale přece jen člověk musí trochu zostražitět. Na druhou stranu je hned vidět, že abychom se od $a = -13$ dostali k nule či nad ni, tak musíme přičítat 3 (formálně bychom odečítali opakovaně $d = -3$), uděláme to párkrát a doskáčeme k číslu 2.

Ne vždy je opakované odečítání nejlepší. Asi by se nám nechtělo opakovaně odčítat 37 od čísla 4147, abychom se dostali k nule, to raději zkusíme povědomý výpočet napravo. Zjistíme, že $4147 \bmod 37 = 3$.

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

O výhodnosti odečítání rozhoduje, nakolik jsou si čísla a a d blízká. V této knize nás konkrétní implementace funkce modulo nebude trápit, prostě prohlásíme „vezmeme a mod b“ a detaily neřešíme.

△

Viděli jsme, že zbytek i částečný podíl se mohou změnit při změně znaménka vstupních dat. Existují na to obecná pravidla, viz cvičení 2a.6, která nám umožní omezit se jen na počítání s kladnými čísly a ostatní případy dořešit těmi pravidly. Například z posledního výsledku výše bychom pak odvodili, že $4147 \bmod (-37) = 3$, zatímco $-4147 \bmod 37 = 34$ a $-4147 \bmod (-37) = 34$. Je to ale jen pro zajímavost, nehodláme se ta pravidla učit, protože se to pro malá čísla nevyplatí (ta potkáme ve škole) a pro velká to udělá počítač.

Z teoretického pohledu ta pravidla znamenají, že se stačí v důkazech zaměřit na případ, kdy $d > 0$ a $a \geq 0$, což nás přivádí zpět k větě o dělení se zbytkem a jejímu důkazu, který ale uděláme pro všechna d, abychom se neodvolávali na cvičení. Použijeme tam k nalezení zbytku tu fintu s opakovaným odčítáním. Všechny možné výsledky onoho opakovaného přičítání/odčitání shromáždíme do množiny a pak vybereme ten správný.

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

1) Nejprve 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. Evidentně $r \geq 0$ a $a = q_0 d + r$ pro nějaké $q_0 \in \mathbb{Z}$, polovina tvrzení je splněna. Platí také $r < d$?

Kdyby ne, pak $a - q_0 d \geq d$, šlo by tedy ještě jednou odečíst d. Formálně, číslo $r_1 = a - (q_0 + 1)d$ splňuje $r_1 \geq 0$, tedy $r_1 \in M$, a $r_1 < r$, což je spor s tím, že r je nejmenší prvek M. Proto $r \geq d$ nemůže nastat.

2) Případ $d < 0$: Pak $-d = |d| > 0$ a dle první části 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.

3) Jednoznačnost: Předpokládejme, že $a = qd + r$ a $a = q'd + r'$, kde $0 \leq r < |d|$ a $0 \leq r' < |d|$. Pak $qd + r = q'd + r'$, proto $(q - q')d = r - r'$. Díky $r, r' \geq 0$ lze odhadovat $-|d| < -r' \leq r - r' \leq r < |d|$ neboli $|r - r'| < |d|$. Takže $|q - q'| \cdot |d| < |d|$, což znamená $|q - q'| < 1$. Ale $(q - q') \in \mathbb{Z}$, proto $q - q' = 0$ a tedy i $q = q'$. Pak také $r = r'$.

□

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 8 o indukci, náš konkrétní problém pak řeší tzv. Princip dobrého uspořádání (viz 4c.14).

Toto souvisí s dalším zajímavým důkazem Věty o dělení, viz poznámky a .

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 2a.8.
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 dělí 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 2a.5. 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 2a.c:
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.

Označme $n = 10a + r$, přičemž a je to počáteční devítimístné číslo a $r = a \bmod 11$. Pak $a = 11k + r$, proto $n = 110k + 10r + r = 11(10k + r)$, tedy číslo 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. Pokud by to vyšlo, tak je buď číslo dobře, nebo se pokazila víc než jedna cifra a zrovna tak šikovně, že to dělitelnost nezkazilo. Kód tedy neodhalí chyby všechny.

Mimochodem, proč jsme použili zrovna jedenáctku? Pokud použijeme menší číslo, pak chybu v jedné cifře nemusí odhalit. Například pokud bychom použili dělitelnost desíti, tak nepoznáme správné číslo 20 od chybného čísla 30. Podobně když se rozhodneme testovat dělitelnost čtyřmi a správné číslo je 36, pak chyba v cifře v čísle 32 není dělitelností poznatelná.

Číslo 11 je tedy nejmenší (tudíž nejpraktičtější), které v testu dělitelnosti umí odhalit chybu v jedné číslici (rozmyslete si, že záměna jedné číslice v čísle nutně vede ke změně zbytku po dělení jedenácti).

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 2c.d v bonusové sekci.

Cvičení

Cvičení 2a.1 (rutinní)**:** Najděte částečný podíl a zbytek pro 2018/87, 8/2, −3/7, 2/17, 0/7, −1030/13.

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

Cvičení 2a.3 (rutinní)**:** (i) Nechť $a, b \in \mathbb{Z}$. Dokažte, že jestliže $a \mid b$, pak $a \mid (cb)$ pro všechna $c \in \mathbb{Z}$.
(ii) Nechť $a, b, c \in \mathbb{Z}$. Dokažte, že jestliže $a \mid b$ a $b \mid c$, pak $a \mid c$.
Viz věta 2a.2.

Cvičení 2a.4 (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) $(-a) \mid (-b)$,
(v) $|a| \mid |b|$.
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. Pak toho využijte k důkazu ekvivalence (i) a (v).

Cvičení 2a.5 (rutinní)**:** Nechť $a, b \in \mathbb{Z}$, $a > 0$. Dokažte, že $a \mid b$ právě tehdy, když $b \bmod a = 0$.

Cvičení 2a.6 (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 2a.7 (rutinní)**:** Nechť $a, b, c, d \in \mathbb{Z}$. Dokažte, že jestliže $a \mid c$ a $b \mid d$, pak $ab \mid cd$.

Cvičení 2a.8 (rutinní)**:** Nechť $a, b, c \in \mathbb{Z}$. Dokažte, že jestliže $ac \mid bc$ a $c \neq 0$, pak $a \mid b$.
Co by se stalo, kdyby $c = 0$?

Cvičení 2a.9 (poučné)**:** Nechť $a, b, c \in \mathbb{Z}$. Dokažte/vyvraťte, že jestliže $a \mid bc$, pak $a \mid b$ nebo $a \mid c$.

Cvičení 2a.10 (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.

Cvičení 2a.11 (poučné)**:** Dokažte, že součin libovolných tří po sobě následujících celých čísel je vždy dělitelný 6.

Řešení:
2a.1: $q = 23$, $r = 17$; $q = 4$, $r = 0$; $q = -1$, $r = 4$; $q = 0$, $r = 2$; $q = 0$, $r = 0$; $q = -80$, $r = 10$.
2a.2: $a = a \cdot 1$ a $a \in \mathbb{Z}$, $a = 1 \cdot a$ a $1 \in \mathbb{Z}$, $0 = 0 \cdot a$ a $0 \in \mathbb{Z}$.
2a.3: (i): $b = ka, k \in \mathbb{Z} \implies cb = (ck) \cdot a$ a $ck \in \mathbb{Z}$. (ii):$b = ka, k \in \mathbb{Z} \wedge cb, l \in \mathbb{Z} \implies c = (kl)a$ a $kl \in \mathbb{Z}$.
2a.4: (i) $\implies$ (ii): $a \,|\, b \implies b = ka, k \in \mathbb{Z} \implies b = -k \cdot (-a) \wedge -k \in \mathbb{Z} \implies -a \,|\, b$.
(ii) $\implies$ (iii), (iii) $\implies$ (iv), (iv) $\implies$ (i) obdobně.
(i) $\implies$ (v): $a \,|\, b \implies b = ka, k \in \mathbb{Z} \implies |b| = |k| \cdot |a| \wedge |k| \in \mathbb{Z} \implies |a| \,|\, |b|$.
(v) $\implies$?: $|a| \,|\, |b| \implies |b| = k|a|$. Zbavíme se absolutních hodnot, podle znamének a a b se ve vztahu objeví plusy či mínusy $\pm b = k(\pm a)$, tedy důkaz se rozpadne na čtyři případy, pokaždé se skončí nějakou konkrétní situací $(\pm a) \,|\, (\pm b)$ neboli jedním z tvrzení (i) až (iv), které všechny vedou na (i)..
2a.5: Jestliže $a \,|\, b$, pak $b = ka = ka + 0$, kde $k \in \mathbb{Z}$ a $0 < a$, tedy $r = 0$.
Jestliže $b \bmod a = 0$, pak $\exists q \in \mathbb{Z}$ aby $b = qa + 0 = qa$.
2a.6: 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 $a = (-q)(-d) + r$ 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 $\pm a \bmod \pm d = 0$.
2a.7: $c = ka, d = lb \wedge k, l \in \mathbb{Z} \implies cd = (kl)ab \wedge (kl) \in \mathbb{Z} \implies ab \,|\, cd$.
2a.8: $ac \,|\, bc \implies bc = kac \wedge k \in \mathbb{Z} \implies b = ka \wedge k \in \mathbb{Z} \implies a \,|\, b$.
Kdyby $c = 0$, tak nelze zkrátit a důkaz je neplatný. Jiný důkaz vymyslet nelze, tvrzení s $c = 0$ neplatí, viz $a = 13$, $b = 23$, $c = 0$.
2a.9: Neplatí, $6 \,|\, (4 \cdot 9)$, ale není $6 \,|\, 4$ ani $6 \,|\, 9$.
2a.10: (i) Označme $n = 10a + b$, tedy b je poslední cifra. Protože 5 dělí 10, tak podle důsledku 2a.3 a faktu 2a.4 $5 \,|\, n$ právě tehdy, když $5 \,|\, b$. Pro jednociferné číslo b ale $5 \,|\, b$ jen pro $b = 0$ a $b = 5$.
(ii): Označte $n = 100a + b$, kde b je dvouciferné. Protože 4 dělí 100, tak ...
2a.11: Jedno z nich musí být sudé, jedno z nich musí být dělitelné třemi, viz fakt 2b.7.

2b. Dělitelé a nejmenší společný dělitel

Jedna ze zajímavých věcí, na kterou se lze u celých čísel zeptat, jsou jejich dělitelé. Některá čísla mají dělitelů mnoho, například číslo 60 se dá dělit výrazně více čísly než jiná podobně velká čísla. Právě proto si jej před cca 4000 lety vybrali staří Babylóňané jako základ číselné soustavy. Je tedy zajímavé podívat se, jaké dělitele má dané celé číslo. Protože dělitelnost nezáleží na znaménku, je taková množina dělitelů symetrická ve smyslu, že ke každému číslu obsahuje i číslo s opačným znaménkem. K poznání této množiny tedy stačí dívat se jen na její polovinu, proto se tradičně zaměřujeme na kladné dělitele.

Kolik dělitelů může mít nějaké přirozené číslo a? Určitě sebe sama a jedničku coby univerzálního dělitele. Pro $a = 1$ to ovšem znamená totéž, takže číslo 1 má (kladných) dělitelů nejméně, jen jednoho. Ostatní čísla už mají alespoň dva. Některá čísla si s tímto minimem vystačí.

Definice.
Nechť $a \in \mathbb{N}$, $a \neq 1$.
Řekneme, že je to **prvočíslo** (**prime**), jestliže jediná přirozená čísla, která a dělí, jsou 1 a a.
Řekneme, že a je **složené číslo** (**composite number**), jestliže to není prvočíslo.

Vidíme, že 1 není prvočíslo ani složené číslo, do této systematizace nám nezapadá. Mohli bychom jej zahrnout mezi prvočísla, ostatně podmínku z definice splňuje, ale pak by to způsobilo velké problémy v teorii. Proto jsme ji z definice hned první větou vyloučili a smíříme se s tím, že jednička je exotické nezařazené číslo.

Tato kapitola se úzce dotýká toho, jak jsou čísla poskládána z menších pomocí násobení. Prvočísla v tomto představují základní cihličky, ty již nelze dále dělit jako součin menších. Ostatně čtenář patrně ví, že každé přirozené číslo lze rozložit na součin mocnin prvočísel. Důkazy těchto tvrzení silně využívají indukci, kterou probereme až v kapitole 8. Proto jsme některé významné poznatky o prvočíslech shromáždili až do bonusové kapitoly 15 ke konci knihy.

Zde na prvočísla občas narazíme (bez nich to opravdu nejde), ale vystačíme si jen s několika základními vlastnostmi, například s touto.

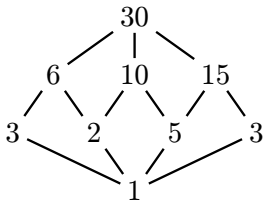
Fakt 2b.1.
Nechť $n \in \mathbb{N}$, $n \neq 1$. Pak existuje prvočíslo p takové, že $p|n$.

Důkaz se najde v kapitole o prvočíslech (fakt 15.1). Další potřebné poznatky probereme, až na to bude vhodný čas.

2b.2 Množina dělitelů

Jak množina dělitelů daného kladného čísla a vypadá? Víme už, že není prázdná, kromě případu $a = 1$ je dokonce alespoň dvouprvková. Na druhou stranu podle věty 2a.5 (ii) musí každý dělitel d čísla a splňovat $d \leq a$, takže množina dělitelů čísla a je shora omezená, přesněji řečeno je to nějaká neprázdná podmnožina množiny $\{1, 2, \dots, a\}$.

Má zajímavou vnitřní strukturu: Jestliže je d nějaký dělitel a, tak podle věty 2a.2 (iii) i všichni jeho dělitelé jsou děliteli čísla a. Ovšem i dělitelé dělitelů splňují tuto vlastnost, takže se množina „větví“. Množinu všech (kladných) dělitelů a si proto můžeme představit jako jakési stromečky, s každým dělitelem se v množině ocitne i podstromeček jeho dalších dělitelů.



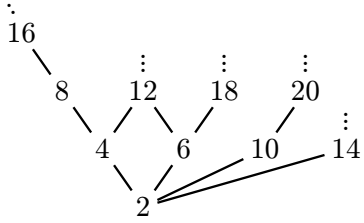
Na obrázku vpravo jsme symbolicky znázornili stromeček množiny dělitelů čísla 30, kde spojnice reprezentují vztah dělitelnosti číslem. Dá se po nich jezdit mezi „patry“, takže třeba hned vidíme, že dvojka dělí šestku, desítku a také třicítku, ale nedělí patnáctku, zatímco jednička dělí vše nad sebou. Trojku jsme tam dali dvakrát, abychom od té na kraji nemuseli dělat skoro vodorovnou čáru na opačný kraj a křížící vše po cestě, bylo by to ošklivé. Zatím si jen tak hrajeme, tak jsme si to mohli dovolit, můžeme si třeba představit, že je to namalované na válečku a je to vlastně jen jedna trojka nahlížená ze dvou stran. Na otázku zachytitelnosti vztahů se pořádně podíváme v kapitole 7a, tam už si tohle nebudeme moci dovolit.

Třicítka má celkem 7 kladných dělitelů odlišných od sebe sama, takže je ten obrázek ještě rozumně velký. Mimochodem, pokud bychom se neomezili jen na kladné dělitele, tak bychom museli přidat ještě jeden identicky vypadající stromeček, jen se zápornými čísly, takže bychom se stejně nic nového nedozvěděli.

Protože dělitelnost nezávisí na znaménku, bude mít číslo -30 přesně stejný strom kladných dělitelů. Jinak řečeno, pokud se něco dozvíme o množině dělitelů pro přirozená čísla, pak to bude platit i pro záporná celá čísla. Na základě tohoto pokusu a případně dalších si například můžeme začít myslet, že celý strom by se měl sbíhat dolů do kořene 1, což už víme je univerzální dělitel, a bude omezen shora daným číslem. V patře nad jedničkou bychom čekali prvočísla z prvočíselného rozkladu. Platí toto vždy?

Skoro, je tu jedna výjimka. Nula je univerzální násobek, má tedy jako kladné dělitele celou nekonečnou množinu přirozených čísel. Neplatí tedy pro ni skoro nic z našich dohadů, množina je nekonečná a není shora omezená, například ani tou danou nulou. Pokud bychom budovali oficiální teorii o množině dělitelů, tak bychom se s tím museli nějak vyrovnat, ale ono to vůbec není snadné udělat tak, aby speciální pravidla pro nulu dobře ladila s pravidly pro ostatní čísla. Jednodušší proto bude bavit se o kladných dělitelích neoficiálně, díky čemuž se problému nuly vyhneme, jen si budeme pamatovat, že si na ni musíme dát pozor.

Teď se podíváme, jak vypadá množina kladných násobků přirozeného čísla a. My vlastně víme, že každý takový násobek musí mít tvar ka pro $k \in \mathbb{Z}$, takže množina násobků je přesně tato: $\{k|a| : k \in \mathbb{N}\}$. Z tohoto pohledu jde tedy o výrazně jednodušší situaci než u dělitelů, množinu lze elegantně zapsat. Je tu ale zase jiná komplikace, tato množina je zjevně nekonečná, tudíž asi budou problémy s obrázkem. Zakreslíme si jen několik násobků, abychom měli představu, co se asi děje. Zase naznačíme spojnicemi vztah dělitelnosti. Tím se ovšem struktura obrázku zkomplikuje, nelze totiž udělat jeden řetízek spojující čísla $a, 2a, 3a$ atd., protože číslo $2a$ určitě nedělí číslo $3a$.



Napravo vidíme část stromu násobků čísla 2 (zakreslili jsme je až po dvacítku) a mimo jiné obsahuje i podstrom násobků šestky. I zde tedy strom obsahuje další podstromečky, které zase obsahují další atd., protože „násobky násobků jsou násobky“. Lze z tohoto příkladu odhadnout něco o množinách dělitelů přirozených čísel? Vypadá to, že se všechny „cestičky“ sbíhají dolů do daného a, zatímco směrem „nahoru“ se rozbíhají nekonečně patry, a že by tak možná šlo generovat abstraktní moderní umění.

Obdobné obrázky budeme dostávat i pro záporná čísla, takže již tradičně zlobí nula. Jaké kladné násobky má nula? Žádné, její množina kladných násobků je prázdná. Nula tedy jeden svůj násobek má, jmenovitě nulu, ale ten bohužel není kladný. I zde využijeme toho, že zatím nebudujeme oficiální teorii, a raději to nebudeme řešit.

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 $d|a$ a $d|b$.
Číslo $d \in \mathbb{N}$ je **společný násobek** (**common multiple**) čísel a, b, jestliže $a|d$ a $b|d$.

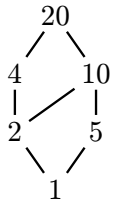
Například číslo 1 je určitě společným dělitelem čísel 40 a 60, zatímco $40 \cdot 60 = 2400$ je určitě jejich společným násobkem. Čtenář ale asi tuší, že nás budou zajímat méně triviální odpovědi, třeba 20 jako společný dělitel a 120 jako společný násobek. Z definice vyplývá, že množinu společných dělitelů získáme tak, že pronikneme množinu kladných dělitelů čísla a s množinou kladných dělitelů čísla b, obdobně pro násobky.

Jak vlastně takto vzniklé množiny všech společných násobků a společných dělitelů vypadají? Rovnou poznamenejme, že pokud $a = b$, tak vlastně pracujeme s množinou kladných dělitelů jednoho čísla, to už máme prozkoumáno. Uvažujme tedy případ dvou různých přirozených čísel a, b.

2b.3 Společní dělitelé

Co víme o množině společných dělitelů? Podobně jako u dělitelů jednoho čísla odvodíme, že je to nějaká neprázdná podmnožina množiny $\{1, 2, \dots, \min(a, b)\}$. Určitě obsahuje číslo 1.

Napravo vidíme stromeček společných dělitelů čísel 40 a 60. Je v mnohém typický. Zase se sbíhá se do kořene 1, v patře nad ním jsou prvočísla a nahoře je strom omezen danými čísly. Dobrá otázka je, zda je toto pravidlem. Tato pozorování se snadno upraví pro záporná celá čísla, pak zjistíme, že množina společných dělitelů je shora omezená číslem $\min(|a|, |b|)$. V obrázku je ještě jedna zajímavá věc, celý stromeček se sbíhá i nahoře do špičky 20. Není jasné, zda je to náhoda nebo pravidlo.

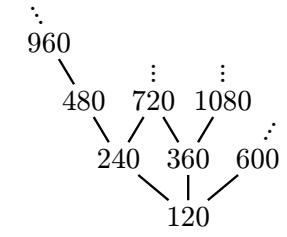


Jak to dopadne s nulami? Začneme případem, kdy hledáme společné dělitele nenulového a a nuly. Protože nulu dělí vše, tak nic neomezuje a vlastně zase jen hledáme kladné dělitele čísla a. V tomto případě tedy strom vypadá tak, jak čekáme (omezený shora, sbíhá se dole do jedničky), ale už neplatí, že by byl shora omezen číslem $\min(a, 0)$, jen omezen jen tím a. Do celkového obrazu tedy nezapadá přesně, ale to hlavní, co budeme brzy potřebovat, je pořád funkční.

Totéž nelze říct o případu společných dělitelů čísel 0 a 0, což je zase celá množina $\mathbb{N}$. Tento případ tedy budeme muset řešit zvlášť, až konečně začneme budovat oficiální teorii.

Jak vypadá množina společných násobků přirozených čísel a, b? Je neprázdná (obsahuje číslo ab) a není shora omezená, protože kdykoliv najdeme nějaký společný násobek m čísel a, b, pak i jeho libovolný kladný násobek je zase společným násobkem a a b a přinese svůj podstrom násobků. V rámci každého řetízku některá čísla dělí jiná, řetízky se navzájem proplétají, prostě vznikají zajímavé struktury.

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. Stejný obrázek čekáme, pokud by některé číslo bylo záporné (a celé). Zajímavým prvkem je, že se celý stromeček sbíhá do kořene 120 (obrázek to alespoň naznačuje), ale v této chvíli není jasné, zda je to pravidlem, dokonce ani zda to je správně, protože nevidíme celý nekonečný strom.



Jak to dopadne s nulami? Zde už bude problémem i případ nenulového čísla a a nuly. Jediným možným násobkem nuly je nula, tím je výběr omezen a číslo a už s tím nic nesvede, i kdyby třeba taky bylo nula. Žádné společné násobky tedy nemáme, jakmile máme ve dvojici nějakou nulu. Je zde situace, na kterou si musíme dát pozor, ale jiná než u společných dělitelů.

Shrňme si to podstatné. Množina společných dělitelů dvou čísel by měla být neprázdná a shora omezená, tedy měla by mít svůj největší prvek. Výjimkou je případ dvou nul. Množina společných násobků dvou čísel by měla být neprázdná a zdola omezená, tedy měla by mít svůj nejmenší prvek. Výjimkou je případ, kdy je alespoň jedno z čísel nula. Teď už jsme připraveni na jednu z klíčových definic této kapitoly.

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 tato jsou nejpoužívanější. Oba pojmy se dají zobecnit na více čísel, viz cvičení 2b.9. Již jsme v této kapitole naznačili, že existenci minim a maxim se budeme věnovat dále, pro tuto chvíli se spokojíme s naší zkušeností, že by neměl být problém najít největší prvek konečné množiny či nejmenší prvek podmnožiny přirozených čísel.

Po našich pozorováních výše nepřekvapí, že případy $\gcd(0, 0)$ a $\operatorname{lcm}(0, a)$ bylo třeba definovat speciálním způsobem. Jak jsme již poznamenali, mnoho autorů se omezuje na přirozená čísla a mají po starostech, začínáme jim už jemně závidět. Zvídavému člověku to ale nedá, chce vědět, zda by tato teorie nešla vybudovat pro všechna celá čísla. 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.

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 2b.4.
Nechť $a, b \in \mathbb{Z}$ splňují $a \neq 0$ 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 se nedají rozumně udělat i pro případy s nulou. Dá se to zachránit přechodem k poněkud slabším odhadům, viz cvičení 2b.3, ale obvykle lidem nestojí za to dělat z toho oficiální tvrzení, my stejně nuly řešíme zvlášť.

Další vlastnost je také snadná. Vzhledem k tomu, že u dělitelnosti znaménko nehraje roli, můžeme totéž čekat i u nových pojmů.

Fakt 2b.5.
Nechť $a, b \in \mathbb{Z}$. Pak $\gcd(a, b) = \gcd(|a|, |b|)$ a $\operatorname{lcm}(a, b) = \operatorname{lcm}(|a|, |b|)$.

Důkaz (rutinní)**:** Případy s $a = 0$ či $b = 0$ se snadno rozmyslí, zaměříme se na případ $a, b \neq 0$.

Společní dělitelé a, b jsou kladná čísla d splňující $d \mid a$ a $d \mid b$, což jsou podle věty 2a.5 přesně čísla splňující $d \mid |a|$ a $d \mid |b|$. Množina společných dělitelů čísel a, b je tedy stejná jako množina společných dělitelů čísel $|a|, |b|$, tudíž se musejí rovnat i největší prvky těchto množin.

Důkaz pro $\operatorname{lcm}(a, b)$ je obdobný.

□

Praktický dopad je, že stačí umět pracovat s kladnými či nulovými čísly, a to i v důkazech. Kromě znamének nás ještě nemusí zajímat jedna věc, a to je pořadí.

Fakt 2b.6.
Nechť $a, b \in \mathbb{Z}$. Pak $\gcd(a, b) = \gcd(b, a)$ a $\operatorname{lcm}(a, b) = \operatorname{lcm}(b, a)$.

Důkaz je docela obtížný, paradoxně proto, že jde o velmi snadné tvrzení. Právě u věci, které jsou na první pohled jasné, se důkazy zejména začátečníkům píšou těžce, protože není jasné, co k tomu ještě dodávat. Docela často pak pomůže odvolat se na definici, která navede.

Podívejme se na gcd a rovnou uvažujme $a, b \neq 0$, protože případy s nulou se snadno ověří přímo z definice. Protože gcd je pro nenulová čísla definováno jako největší prvek jisté množiny, potřebujeme ukázat, že množina všech společných dělitelů dvojice a, b je totožná s množinou všech společných dělitelů dvojice b, a. Zase je to něco, co zní naprosto zjevně, tak se podíváme na definici, kdy jsou dvě množiny shodné. Musíme ukázat, že prvky jedné množiny jsou v druhé a naopak. Co o tom říká definice společného dělitele?

- $d \in \mathbb{N}$ je společný dělitel $a, b \iff d \,|\, a \wedge d \,|\, b$.
- $d \in \mathbb{N}$ je společný dělitel $b, a \iff d \,|\, b \wedge d \,|\, a$.

Výrazy napravo jsou logicky shodné, tudíž každý dělitel dvojice a, b je i dělitelem dvojice b, a a naopak, což dokončuje náš neformální důkaz.

Nebyl to zrovna důkaz typický, ale snad byl poučný. Například jsme se dozvěděli, že možnost prohazovat vstupní data v gcd (a obdobně v lcm) se vlastně odvíjí od faktu, že logická konjunkce je komutativní operace. Autor si je vědom, že mnohé ze čtenářů to asi nějak významněji nenadchne, ale snad to potěšilo alespoň některé.

Teď si zodpovíme jednu z otázek o podobě stromečků.

Fakt 2b.7.
Nechť $a, b \in \mathbb{Z}$. Každý společný násobek a a b je dělitelný číslem $\operatorname{lcm}(a, b)$.

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

1) Případ $a, b, n > 0$. Protože je n společným násobkem a, b, tak podle definice určitě platí $\operatorname{lcm}(a, b) \leq n$. Ukážeme, že je tam dokonce vztah dělitelnosti.

Nechť podle věty o dělení $n = q \operatorname{lcm}(a, b) + r$. Protože a dělí $\operatorname{lcm}(a, b)$, tak dělí i $q \operatorname{lcm}(a, b)$. Podle předpokladu rovněž $a \,|\, n$, proto podle důsledku 2a.3 musí a také dělit r. Stejně ukážeme, že i b dělí r, je to tedy kandidát na společný násobek. Jsou dvě možnosti.

Pokud by bylo $r > 0$, tak to opravdu je společný násobek a, b. Ovšem $\operatorname{lcm}(a, b)$ je mezi společnými náasobky nejmenší, proto by platilo $\operatorname{lcm}(a, b) \leq r$. Coby zbytek po dělení ovšem r také musí splňovat $r < \operatorname{lcm}(a, b)$, což je spor. Varianta $r > 0$ není možná.

Protože pro zbytek musí platit $r \geq 0$, zbývá jedině možnost $r = 0$, tedy $n = q \operatorname{lcm}(a, b)$ pro nějaké $q \in \mathbb{Z}$.

2) Nulové případy: Pokud $n = 0$, tak jsou dělitelem n všechna čísla, proto je předpoklad i závěr dokazované implikace pravdivý, tedy i celá implikace platí.

Pokud $a = 0$, tak díky $a \,|\, n$ máme i $n = 0$ a jsme v případě, který už je vyřešen, obdobně pro $b = 0$.

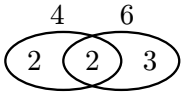
3) Jestliže je některé z čísel záporné, tak využijeme toho, že dělitelnost i lcm ignorují znaménka. Konkrétně:

Jestliže $a \,|\, n$ a $b \,|\, n$, pak (viz věta 2a.5) $|a| \,|\, |n|$ a $|b| \,|\, |n|$. Podle části 1), popř. 2) pak platí i $\operatorname{lcm}(|a|, |b|) \,|\, |n|$ neboli $\operatorname{lcm}(|a|, |b|) \,|\, n$. K závěru nás pak dovede fakt 2b.5.

□

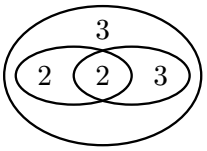
Jinak řečeno, strom společných násobků dvou čísel opravdu musí mít společný kořen $\operatorname{lcm}(a, b)$. Matematicky řečeno, pokud množinu společných násobků uspořádáme pomocí dělitelnosti, tak je $\operatorname{lcm}(a, b)$ nejmenším nejen ve smyslu nerovnosti (velikosti čísel), ale také ve smyslu dělitelnosti, viz kapitola 7b. Je zajímavé, že obdobné tvrzení platí i pro $\gcd(a, b)$, ale tam je důkaz znatelně těžší a musíme si pro něj nejprve připravit nástroje, viz důsledek 2b.21.

Tento fakt má ještě zajímavou interpretaci týkající se běžné práce s čísly. Představme si, že máme číslo n a víme, že jej lze dělit určitými dvěma čísly a, b. Pak určitě obecně neplatí, že by číslo n šlo dělit součinem ab. Například 36 je dělitelné čtyřkou i šestkou, ale rozhodně není dělitelné jejich součinem 24. Pokud ale z nějakého důvodu potřebujeme co nejvíce vydělit něčím, co pochází z čísel a a b, tak nám Fakt říká, že to určitě půjde jejich nejmenším společným násobkem.



Tyto úvahy souvisejí s tím, nakolik se čísla překrývají ve smyslu toho, z jakých základních cihel jsou poskládány. Například čísla čtyři a šest se překrývají dvojkou. Můžeme si to znázornit povědomým obrázkem, který ale teď rozhodně nepředstavuje množiny. Jsou to neoficiální obláčky a čísla v jednotlivých oblastech se spolu násobí.

V této představě také krásně vidíme největší společný dělitel, to je ta společná část, a nejmenší společný násobek, kdy zahrneme jen to nejnutnější, tedy vezmeme celý spojený obláček: $\operatorname{lcm}(4, 6) = 2 \cdot 2 \cdot 3 = 12$.



Situaci výše si pak představíme tak, že jednotlivé obláčky pro 4 a 6 se vejdou do obláčku pro 36, pak by selský rozum napovídal, že se tam vejde i ten nejmenší společný násobek. Pokud ale tato čísla vynásobíme, tak jakoby ty jejich obláčky dáváme vedle sebe a vznikne útvar příliš velký na to, aby se do 36 vešel. Takovéto pohádky samozřejmě nejsou správná matematika, ale při přemýšlení pomáhá, když má člověk nějakou intuitivní představu. Mi zrovna tahle pomáhá, třeba pomůže i vám, nebo máte svou lepší.

Takovéto představy například napovídají, že kdyby se obláčky čísel a, b vůbec nepřekrývaly a oba byly součástí n, tak už by se měl vejít i jejich součin. Například čísla 4 a 9 nemají společný faktor, obě dělí 36 a opravdu, i jejich součin dělí 36. Dává to smysl a bylo by pěkné to teď dokázat, ale kupodivu to není vůbec snadné a musíme si počkat, až vybudujeme silnější nástroje, viz cvičení 2b.6.

Případ, kdy se čísla „překrývají“, působí komplikace a matematici preferují situace, kdy tomu tak není.

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).

V této souvislosti vystupují do popředí prvočísla, protože těm se nemůže stát, že by s jiným číslem „sdílely" kousek sebe. V obláčkové řeči si prvočísla vybírají, buď s nějakým číslem nemají nic společného, nebo jsou v něm obsaženy celé.

Fakt 2b.8.
Nechť p je pročíslo. Pak pro libovolné $a \in \mathbb{Z}$ platí, že buď je p s a nesoudělné, nebo p dělí a.

Důkaz (rutinní)**:** Společní dělitelé se vybírají z 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.

Podobných tvrzení je možno vymyslet více, třeba že když p je prvočíslo a $|a| < p$, tak $\gcd(a, p) = 1$, určitě je dobré si toto rozmyslet a také se podívat do cvičení. Hlavní vzkaz tady je, že v přítomnosti prvočísel bývají věci jednodušší.

Pokud situaci dobře rozumíme, tak nás může napadnout zajímavý trik. Představme si, že máme dvě čísla a potřebovali bychom, aby byly nesoudělné. Ony ale bohužel nejsou. Ovšem pokud obě vydělíme tou společnou částí, tak to, co zbude, už by nemělo mít nic společného.

Fakt 2b.9.
Nechť $a, b \in \mathbb{Z}$, $a, b \neq 0$. Pak jsou $\dfrac{a}{\gcd(a,b)}$ a $\dfrac{b}{\gcd(a,b)}$ nesoudělná celá čísla.

Důkaz (rutinní)**:** Protože $a, b \neq 0$, je také $\gcd(a, b)$ nenulové číslo a dělí a i b. Podíly jsou tedy automaticky celá čísla. Mohla by být soudělná?

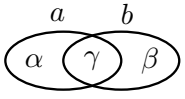
Předpokládejme, že $d \in \mathbb{N}$ je nějaký společný dělitel čísel $\dfrac{a}{\gcd(a,b)}$ a $\dfrac{b}{\gcd(a,b)}$. To znamená, že pro nějaká $k, l \in \mathbb{Z}$ máme $\dfrac{a}{\gcd(a,b)} = kd$ a $\dfrac{b}{\gcd(a,b)} = ld$. Pak $a = k[d\gcd(a, b)]$ a $b = l[d\gcd(a, b)]$, čili $d\gcd(a, b)$ je 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.

□

Tento výsledek také plyne snadno z věty 2b.25 (ii). V matematice se občas stane, že lze provést buď důkaz pomocí základních pojmů a úvah („elementární důkaz"), nebo jiný, často velmi efektní a krátký, pomocí mocnějších nástrojů. Obojí má své výhody, zmíníme jednu souvislost. Jedna z věcí, která matematiky u poznatků zajímá, je jejich „hloubka", jak náročné je dostat se k nim. Když něco dokážeme pomocí mocné věty, tak to jakoby naznačuje, že ten výsledek je také nesnadný (a jak uvidíme, věta 2b.25 bude vyžadovat Bezoutovu identitu, což naznačuje jistou obtížnost). Náš elementární důkaz ukazuje, že právě dokázané tvrzení je v zásadě snadné.

Mimochodem, to že $\dfrac{a}{\gcd(a,b)} \in \mathbb{Z}$ a $\dfrac{b}{\gcd(a,b)} \in \mathbb{Z}$ je zjevné, ale budeme to opakovaně používat, tak na to upozorňujeme.



Poslední vlastnost, kterou si ukážeme, lze také odhadnout z obláčkové představy. Obrázek naznačuje, jak si představujeme situaci pro dvě čísla a, b. Mělo by pak platit $\gcd(a, b) = \gamma$ a $\mathrm{lcm}(a, b) = \alpha\gamma\beta$, pokud tedy pracujeme s kladnými čísly. Co dostaneme, když je spolu vynásobíme?

$$\mathrm{lcm}(a, b) \cdot \gcd(a, b) = \alpha\gamma\beta \cdot \gamma = (\alpha\gamma) \cdot (\beta\gamma) = a \cdot b.$$

Sice jsme napsali matematicky se tvářící vzoreček, ale ten pracoval s obrázkem, takže to důkaz rozhodně nebyl. Teď jeden pořádný uděláme a rovnou si rozmyslíme, jak by ten vzorec měl vypadat pro obecná celá čísla. Ukáže

se, že tentokráte naše speciální definice pro výjimečné případy vedou na stejný vzorec, takže dostáváme obecné tvrzení.

Věta 2b.10.
Nechť $a, b \in \mathbb{Z}$. Pak $\operatorname{lcm}(a,b) \cdot \gcd(a,b) = |a| \cdot |b|$.

Důkaz (poučný)**:** 1) Nejprve uděláme případ $a, b \in \mathbb{N}$.

a) Uvažujme číslo $m = \dfrac{ab}{\gcd(a,b)}$. Máme $m = \dfrac{a}{\gcd(a,b)}b$ a $\dfrac{a}{\gcd(a,b)} \in \mathbb{Z}$, tedy m je násobek b, symetricky také $m = \dfrac{b}{\gcd(a,b)}a$ a m je násobek a. Podle faktu 2b.7 tedy musí $\operatorname{lcm}(a,b)$ dělit m, mimo jiné proto $\operatorname{lcm}(a,b) \leq m$ (viz věta 2a.5 (ii), zde $m > 0$). Po dosazení dostáváme $\operatorname{lcm}(a,b) \cdot \gcd(a,b) \leq ab$.

b) Uvažujme číslo $d = \dfrac{ab}{\operatorname{lcm}(a,b)}$, dle faktu 2b.7 je to přirozené číslo. Máme $a = \dfrac{\operatorname{lcm}(a,b)}{b}d$ a $\dfrac{\operatorname{lcm}(a,b)}{b} \in \mathbb{Z}$, tedy d je dělitel a, symetricky také $b = \dfrac{\operatorname{lcm}(a,b)}{a}d$ a d je dělitel b. Podle definice proto $d \leq \gcd(a,b)$. Po dosazení dostáváme $ab \leq \operatorname{lcm}(a,b) \cdot \gcd(a,b)$.

Spojením nerovností máme $ab = \operatorname{lcm}(a,b) \cdot \gcd(a,b)$.

2) Jsou-li a, b nenulové, ale některé z nich je záporné (či obě), pak výsledek vyplývá z faktu 2b.5.

3) Případy s $a = 0$ nebo $b = 0$ se snadno ověří.

□

Důkazů existuje více, obvykle používají Bezoutovu identitu či její důsledek 2b.21, 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 $\operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$ používat $\operatorname{lcm}(a,b) = \dfrac{a}{\gcd(a,b)}\,b$ či $\operatorname{lcm}(a,b) = \dfrac{b}{\gcd(a,b)}\,a$, protože tento postup nevyžaduje ukládání velkého čísla ab.

Prakticky řečeno to znamená, že nám stačí naučit se počítat $\gcd(a,b)$, což se teď stane našim hlavním cílem.

Příklad 2b.a: Jak bychom našli $\gcd(120,180)$ a $\operatorname{lcm}(120,180)$? U malých čísel lze často postupovat metodou „kouknu a vidím“. Dobře také funguje přístup přes prvočíselný rozklad:

$$120 = 2^3 \cdot 3 \cdot 5,$$
$$180 = 2^2 \cdot 3^2 \cdot 5.$$

Největší společný dělitel získáme zahrnutím všeho, co je společné, $\gcd(120,180) = 2^2 \cdot 3 \cdot 5 = 60$. Nejmenší společný násobek vznikne, když od každého prvočísla vezmeme největší mocninu, proto $\operatorname{lcm}(120,180) = 2^3 \cdot 3^2 \cdot 5 = 360$. △

Prvočíselný rozklad si uděláme pořádně později, v kapitole o prvočíslech, a mimo jiné tam zmíníme, že dělat rozklad pro velká čísla je velmi náročná úloha, a to i pro počítače. Budeme tedy potřebovat nějaký efektivní způsob hledání $\gcd(a,b)$. Začneme tím, že si připomeneme jednoduché případy, ve kterých největší společný dělitel vlastně nemusíme počítat, protože je jasný.

Fakt 2b.11.
Nechť $a \in \mathbb{Z}$. Pak platí:
(i) $\gcd(a,0) = |a|$ a $\operatorname{lcm}(a,0) = 0$;
(ii) $\gcd(a,a) = \operatorname{lcm}(a,a) = |a|$.

Druhé tvrzení v (i) je přímo definice, z té známe i hodnoty $\gcd(0,0) = \operatorname{lcm}(0,0) = 0$ pro (ii). Důkaz ostatního necháme jako cvičení 2b.1. Nás bude zajímat zejména vztah $\gcd(a,0) = |a|$, ke kterému budeme směřovat naše úsilí.

Obvyklá strategie je redukovat rozsah problému tím, že se odvoláme na fakt 2b.5, díky čemuž stačí umět najít gcd pro nezáporná čísla. Nuly a případ stejných čísel jsme už vyřešili výše, a pokud nám dá někdo dvě různá čísla, tak je vždycky umíme seřadit dle velikosti a gcd je pořadí jedno. Vychází nám z toho, že se stačí naučit určovat největší společný dělitel pro čísla a, b splňující $a > b > 0$.

To je podstatná redukce, nicméně se na konci ukáže, že není nutná, protože postup, který odvodíme, funguje zcela obecně. Proč tedy tu redukci lidé dělají a proč ji zde (dočasně) uděláme také? Protože se ten případ dobře představuje, dokazuje a počítá rukou. Takže jdeme na to.

Klíčem k efektivnímu nalezení gcd je následující tvrzení, před jehož čtením je dobré připomenout si počítání zbytku po dělení, viz příklad 2a.b.

Lemma 2b.12.
Nechť $a, b \in \mathbb{Z}$, nechť $r \in \mathbb{Z}$ splňuje $a = qb + r$ pro nějaké $q \in \mathbb{Z}$. Pak platí následující:
(i) $d \in \mathbb{N}$ je společný dělitel a, b právě tehdy, když je to společný dělitel b, r.
(ii) $\gcd(a, b) = \gcd(b, r)$.

Typicky toto lemma používáme s volbou $r = a \bmod b$, dokonce tak často bývá formulováno, pak je potřeba také vyžadovat $b \neq 0$. Později se nám ale bude hodit, že důkaz využívá z definice zbytku po dělení jen ten algebraický vzorec a nevyžaduje omezení $0 \leq r < |b|$.

Důkaz (poučný)**:** Nechť $a, b, r \in \mathbb{Z}$ a $a = qb + r$ pro nějaké $q \in \mathbb{Z}$.

(i) $\Longrightarrow$: Je-li d společný dělitel a a b, pak dělí a i qb, tedy podle faktu 2a.4 musí dělit také r a je to společný dělitel b, r.

(i) $\Longleftarrow$: Důkaz je obdobný. Oba směry je ovšem také možné dokázat přímo, předvedeme to tady. Předpoklady: $d \mid b$, $d \mid r$. Pak $b = kd$ a $r = ld$ pro $k, l \in \mathbb{Z}$. Dosadíme: $a = qb + r = q(kd) + (ld) = (qk + l)d$ a $(qk + l) \in \mathbb{Z}$, proto d dělí a. Dle předpokladu dělí i b, je to tedy společný dělitel a, b.

Pokud bychom takto dokazovali $\Longrightarrow$, dosazovali bychom do $r = a - qb$.

(ii): Podle (i) se množina společných dělitelů čísel a, b rovná množině společných dělitelů čísel b, r, proto se musí rovnat i největší prvky těchto množin.

□

Z tohoto lemma již přímo vyplyne postup pro hledání $\gcd(a, b)$. Jak jsme zmínili, z mnoha možných kandidátů na r budeme chtít právě $a \bmod b$, čímž zajistíme, že se naše situace bude zlepšovat a ne zhoršovat.

Příklad 2b.b: 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 to tak snadné není a počkal by si na jasně rozeznatelnou nulu.

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

△

Postup z příkladu je obecný. Namísto hledání gcd pro dvojici $a > b > 0$ hledáme gcd pro čísla $b > r$, kde $r = a \bmod b$. Pokud $r > 0$, tak aplikujeme lemma znovu, najdeme $r' = b \bmod r$ a namísto dvojice $b > r$ hledáme gcd pro $r > r'$. Takto můžeme pokračovat. Klíčové je, že se při každém kroku přejde na menší čísla. Protože zároveň nelze pomocí zbytků dojít k číslům záporným, máme pro ně k dispozici jen konečnou množinu čísel a postup se tedy musí zarazit.

Kdy se tak stane? Dokud je zbytek kladný, tak se vždy dá dojít následně ještě k menšímu. Proces se tedy zastaví v okamžiku, kdy je zbytek nulový. Pak jsme v situaci, kdy uvažujeme $\gcd(x, 0)$, což hravě určíme podle faktu 2b.11. Tím dostáváme algoritmus k nalezení $\gcd(a, b)$ pro $a > b > 0$.

Uděláme si formální předpis pro tento postup, a to ve dvou podobách. Jedna si pamatuje, co se kdy dělo. Ta bude výhodná při důkazu, že algoritmus dělá to, co má.

Druhá verze se nestará o minulost, což je samozřejmě verze, kterou bychom použili v praxi. Jak už jsme zmínili, budeme předpokládat nějakou implementaci procesu nalezení zbytku po dělení. Nebudeme preferovat nějaký existující jazyk, raději použijeme pseudokód srozumitelný snad každému.

S Algoritmus 2b.13.
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`
$r := a \bmod b$;
$a := b$; $b := r$;
`until` $b = 0$;
`output:` a;

△

Tento algoritmus je starý přibližně 2500 let a má mnohá využití, namátkou lze pomocí něj snadno převádět zlomky do řetězového tvaru. Tím se zde nebudeme zabývat, jako návnadu uvedeme, že z příkladu 2b.b máme hodnoty q 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.

2b.14 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

$408 \bmod 108 = 84 \implies$

a, b
408
108
84

Teď bychom měli posunout registry, což realizujeme tím, že přeneseme pohled na 2. a 3. řádek v tabulce, a začne další krok. Najdeme zbytek, čímž přibude v tabulce čtvrtý řádek, a posuneme pohled na poslední dva řádky. Takto postupujeme, dokud nenajdeme nulu. Kladné číslo, které se objevilo naposledy před nulou, je poslední stav registru a a tedy i hledaný $\gcd(408, 108)$.

a, b
408
108

$\implies$

a, b
408
108
84

$\implies$

a, b
408
108
84
24

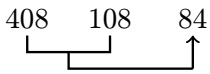
$\implies$

a, b
408
108
84
24
12

$\implies$

a, b
408
108
84
24
12•
0

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



$408 \bmod 108 = 84$

Takto pokračujeme:

$$408 \quad 108 \quad 84 \quad 24 \quad 12\bullet \quad 0$$

Tato metoda je evidentně nejpohodlnější, ale my si tento algoritmus brzy dále rozšíříme, na to bude vhodnější ta první, sloupcová verze.

△

2b.15 Poznámka: Z praktického programátorského pohledu je zajímavé si všimnout, že algoritmus je schopen pracovat pro libovolné vstupy, pokud dáme test na $b = 0$ hned na začátek cyklu. Pokud jej pak spustíme s $b = 0$, tak se rovnou zastaví a dá správný výsledek a. Podívejme se tedy na případ, kdy $b \neq 0$.

Začneme tím, že máme dvě různá kladná čísla, ale zadáme je v pořadí $a < b$. V takovém případě vychází $r = a \bmod b = a$. Pak dojde k posunu registrů a do dalšího kroku algoritmu se vstupuje s dvojicí b, r neboli b, a, která už je seřazena správně dle velikosti a vše probíhá v pořádku. Můžeme si všimnout, že to takto správně proběhne i pro případ $a = 0$.

a
b
a

Seřazení nezáporných čísel podle velikosti tedy není nutné, ale ušetříme jednu iteraci, takže při ručním výpočtu asi stojí za to začínat s čísly v pořadí větší–menší.

Co program udělá, když mu podstrčíme dvě stejná čísla? Pak v prvním kroku najde $r = a \bmod a = 0$, posunem se přesune ke dvojici $a, 0$ a oznámí nám výsledek a, což je správná odpověď.

Zbývá probrat záporné vstupy. Zde je klíčové, že lemma 2b.12 platí i pro záporná čísla. Když tedy přecházíme k novým dvojicím, tak nedochází ke ztrátě správné informace, nová dvojice má pořád stejné gcd jako předchozí.

Zbytky jsou nezáporné, takže pokud program jede déle než jeden krok, tak už počínaje druhým pracuje s nezápornými čísly ve své tradiční podobě a vše je v pořádku. Jediná možná komplikace je, pokud zadáme záporné b, které dělí a. Pak $r = 0$, program po posunu na dvojici $b, 0$ skončí a nabídne jako odpověď b, což je záporné číslo. To ale snadno změníme na kladné a máme odpověď.

U záporných čísel ovšem začíná hrát roli pořadí. Jako příklad si ukážeme nalezení $\gcd(-108, -408)$. Z příkladu 2b.b již víme, že $\gcd(-108, -408) = \gcd(408, 108) = 12$ a stálo nás to 4 kroky algoritmu.

Teď aplikujeme Euklidův algoritmus přímo na daná čísla:

$$-108 \qquad -408 \qquad 300 \qquad 192 \qquad 108 \qquad 84 \qquad 24 \qquad 12 \qquad 0$$

Zde se opravdu vyplatí hledat zbytky posunem, například hned v prvním kroku hledáme $(-108) \bmod (-408)$, tedy z výchozího bodu -108 se nažíme dostat do kladné části celočíselné osy pomocí kroků o velikosti $|-408| = 408$, evidentně stačí jednou přičíst.

V druhém kroku se pak od 300 chceme dostat blíže k nule pomocí 192, tedy jednou odečteme atd.

Pokud spoustíme algoritmus s čísly v opačném pořadí, je to mnohem kratší.

$$-408 \qquad -108 \qquad 24 \qquad 12 \qquad 0$$

Je to dokonce o jednu iteraci rychlejší než běh pro vstup $408, 108$.

Závěr tedy je, že algoritmus funguje pro libovolné vstupy, pokud jej upravíme, aby nejprve testoval, a pro jistotu dáme na výstup absolutní hodnotu:

Euklidův algoritmus (obecná verze) pro nalezení $\gcd(a, b)$ pro $a, b \in \mathbb{Z}$.

```
procedure gcd(a, b: integer)
while b ≠ 0 do
        r := a mod b;
        a := b;  b := r;
output: |a|;
```

V praxi je ale dobré si hlídat, aby na vstupu bylo $|a| \geq |b|$.

Nabízí se otázka, proč je při výkladu zvykem soustředit se na případ $a > b > 0$, když algoritmus funguje obecně? Důvodem je, že je pak jednodušší jej analyzovat, v praxi se často používá pro kladná čísla a jak jsme právě viděli, seřazení dle velikosti je rozumná strategie.

△

Samozřejmě nás zajímá, kde bereme jistotu, že algoritmus dělá, co má. Dodá nám ji vhodná matematická věta.

Věta 2b.16.
Euklidův algoritmus skončí pro libovolný vstup $a, b \in \mathbb{Z}$ po konečném počtu kroků s výstupem $\gcd(a, b)$.

Jak se taková věta dokazuje? To nám napoví teorie algoritmů. V typickém případě se o algoritmu dokazují dvě věci. Jednou je, že algoritmus někdy skončí pro libovolný vstup. V našem případě bychom se odvolali na generovaná čísla $r_{k+1} = r_{k-1} \bmod r_k$, z tohoto vztahu dostáváme $r_{k+1} < r_k$ (pro $k \geq 0$) neboli jde o klesající posloupnost nezáporných čísel. Pokud bychom naše předchozí úvahy o nemožnosti najít takovou nekonečnou posloupnost oděli do matematického hávu, budeme mít důkaz ukončení algoritmu. Poznamenejme, že ukončitelnost běhu programu nemusí být snadnou otázkou, viz poznámka 5a.7.

Druhým krokem je tzv. podmíněná správnost algoritmu, tedy důkaz, že pokud vůbec algoritmus někdy skončí, tak musí mít na výstupu tu správnou věc. Zde je dobré si uvědomit, že algoritmus vlastně v každém kroku zkouší počítat jisté gcd, a ačkoliv zkouší různé dvojice čísel, hledaná hodnota se nemění. Matematicky vzato musíme ukázat, že

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots ,$$

dokud algoritmus neskončí. Vlastně jde o opakovanou aplikaci lemma 2b.12, což se nejlépe dělá indukcí. I tento důkaz tedy odložíme do bonusové kapitoly 16 o Euklidově algoritmu, kde již budeme mít indukci k dispozici.

V dotyčné kapitole se věnujeme i zkoumání rychlosti Euklidova algoritmu, což je pro velká vstupní čísla důležitý praktický aspekt. Zde se na to podíváme z hlediska praktického výpočtu.

2b.17 Zrychlená verze (záporné zbytky)

Při ručním i počítačovém výpočtu nás zajímá, kolik kroků Euklidova algoritmu potřebujeme provést. Zdá se zjevné, že to souvisí s tím, jak rychle se zmenšují zbytky r_k. Protože jsou to zbytky po dělení, nic je nenutí klesat rychle a klidně můžeme mít situaci, kdy $r_{k+1} = r_k - 1$. Kdybychom takto ubírali po jedné pořád, tak by se mohlo

stát, že na nalezení $\gcd(a,b)$ potřebujeme $|b|$ kroků, což je velmi nemilá představa. Naštěstí takovéto malé krůčky nemohou vydržet dlouho, což lze nahlédnout vcelku snadno.

Pro jednoduchost předpokládejme, že $a > b > 0$, pak je posloupnost r_k klesající a kladná. Víme, že r_{k+1} vzniklo jako $r_{k+1} = r_{k-1} - qr_k$, tedy od r_{k-1} jsme několikrát odebrali r_k. Protože $r_k < r_{k-1}$, museli jsme odebrat alespoň jednou, možná i vícekrát, můžeme tedy odhadovat:

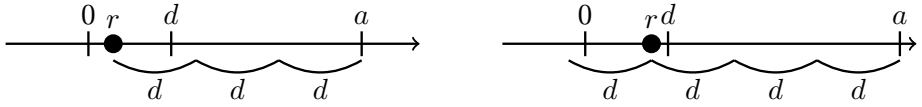
$$r_{k+1} = r_{k-1} - qr_k \leq r_{k-1} - r_k.$$

Řečeno slovy, každé nové číslo v tabulce Euklidova algoritmu nemůže být větší než rozdíl dvou předchozích čísel. To znamená, že pokud se v některém kroku algoritmu r_k sníží oproti r_{k-1} jen trochu, pak ten následující r_{k+1} musí být nutně velmi malý.

Toto pozorování lze formulovat i jinak: Pokud se podíváme na čísla generovaná Euklidovým algoritmem, tak každé musí být alespoň tak velké jako je součet dvou následujících. Můžete se ze zvědavosti dívat do tabulek všech příkladů, jestli to opravdu funguje. Samozřejmě že ano, a je to klíčem k důkazu výsledku z kapitoly 16, že těch kroků v Euklidově algoritmu může být nejvýše $5\log_2(|b|)$, což je výrazně lepší než pesimistické $|b|$. Přesto ale stojí za úvahu, zda bychom nemohli nějak dosáhnout rychlejšího zmenšování čísel r_k.

Uvažujme čísla $a > d > 0$. Zbytek získáme tak, že se po celočíselné ose posunujeme od a k nule pomocí skoků o velikosti d tak, abychom získali co nejmenší nezáporné číslo. Pak nelze zabránit tomu, abychom neskončili blízko k d.

Pokud ovšem z požadavku vynecháme to slovo „nezáporné“, tak se situace změní. Jestliže se umíme posunovat o skoky velikosti d, pak vždy dokážeme dojít k nule do vzdálenosti nejvýše $\frac{1}{2}d$. Graficky je to zcela jasné, na obrázku vidíme dvě typické situace s vyznačeným zbytkem r.



Toto bližší číslo má řadu vlastností společných se zbytkem, což ospravedlňuje 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, zatímco pro získání záporného zbytku zaokrouhlujeme na nejbližší celé číslo. Toto zaokrouhlení se někdy značí $\left\lfloor \frac{a}{d} \right\rceil$.

Někdy to vyjde nastejno, třeba zbytek po dělení $a = 13$ číslem 6 je $r = 1$ a je to i záporný zbytek, je dostatečně malý. Statisticky vzato v polovině případů to ale dopadne jinak.

Uvažujme čísla $a = 408$, $b = 108$. Můžeme odhadnout, že na co nejbližší přiblížení k nule, ale bez jejího překročení, je potřeba od 408 odebrat 108 třikrát. Dostaneme $408 \bmod 108 = 84$. Zároveň ale vidíme, že pokud odebreme 108 ještě jednou, dostaneme se k nule blíže, proto záporný zbytek bude -24.

Pomocí dělení: $\frac{408}{108} = 3.77...$. Pokud zaokrouhlíme dolů, získáme standardní částečný podíl $q = 3$ a potvrdíme, že pro získání standardního zbytku je třeba počítat $408 - 3 \cdot 108$. Ovšem nejbližší celé číslo je 4, tedy záporný zbytek je $408 - 4 \cdot 108$.

Již jsme upozornili, že důkaz klíčového lemma 2b.12 vyžadoval pouze rovnost $a = qb + r$, tedy platí i pro záporné zbytky. To znamená, že také Euklidův algoritmus musí fungovat i se zápornými zbytky.

Jak rychlý pak bude? Pro všechna k dostáváme $|r_{k+1}| \leq \frac{1}{2}|r_k|$, také platí $|r_1| = |b|$, odtud indukcí snadno odvodíme, že $|r_k| \leq \frac{1}{2^{k-1}}|b|$. To je geometrická rychlost klesání. Pokud algoritmus skončí po N krocích, tak $r_{N+1} \neq 0$ a $r_{N+2} = 0$ (například pokud hned $a \bmod b = 0$, tedy algoritmus skončil po prvním kroku, tak je $r_1 = b \neq 0$ a $r_2 = 0$). Pak $1 \leq |r_{N+1}| \leq \frac{1}{2^N}|b|$ neboli $1 \leq \frac{1}{2^N}|b|$. Snadnou úpravou vyjde $N \leq \log_2(|b|)$.

Porovnáme-li to s odhadem pro standardní Euklidův algoritmus, vidíme, že je zde potenciál na až pětinásobné urychlení. V praxi to až tak skvělé není, ale v průměru se používání záporných zbytků vyplácí. Proto jde o variantu velmi rozšířenou v aplikacích.

Příklad 2b.c: Najdeme $\gcd(408, 108)$ metodou nejmenších zbytků. Pro porovnání ukážeme i standardní Euklidův algoritmus (viz příklad 2b.b) a uvedme hodnotu koeficientu q použitého ke zmenšování čísel.

a,b	q
408	
108	3
84	1
24	3
12•	2
0	

a,b	q
408	
108	4
-24	-4
12•	-2
0	

Co se dělo? Záporný zbytek pro 408 a 108 jsme si už rozmysleli dříve. Pro čísla 108 a -24 vidíme, že chceme velikost 24 odebrat od 108 čtyřikrát. To znamená, že číslo -24 chceme přidat, což se odrazí na záporném znaménku koeficientu $q = -4$. Ty koeficienty mohou být trochu zmatečné, naštěstí při provádění Euklidova algoritmu ručně je nemusíme řešuit, prostě posouváme intuitivně. Bohužel, brzy uvidíme, že nás tyto koeficienty budou zajímat, pak jsou dvě možnosti. Buď se s nimi člověk naučí žít, nebo prostě záporné zbytky nebude používat a má klid.

Při intuitivním přístupu se nám klidně může stát, že -24 přidáme nikoliv čtyřikrát, ale pětkrát. Pak nám vyjde -12. To není na závadu, znaménko snadno upravíme. Při používání záporných zbytků se musí počítat s tím, že se kandidát na $\gcd(a,b)$ ještě bude muset doupravit.

△

V této souvislosti je zajímavé poznamenat, že nacházení zbytků, standardních i záporných, bývá snažší odčítáním v připadech, kdy je jsou si a, b relativně blízké neboli když q je spíš menší. Zajímavou shodou okoností se přesně toto dá u Euklidova algoritmu očekávat. 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. Praktický závěr z toho je, že pro praktický výpočet je to odčítání (popřípadě přičítání pro b záporné) doporučovaný přístup.

Existují i jiné přístupy k urychlení Euklidova algoritmu. Jednou možností je použití různých fint, například tyto rovnosti:

- $\gcd(a,b) = 2\gcd(a/2, b/2)$, 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 relativně levná operace, zejména při zápisu v binárním kódu) dosáhneme situace s jedním či dvěma lichými čisly, pak aplikujeme opakovaně druhý či třetí vzorec, dokud nedostaneme dvě sudá čísla, to zase redukujeme dělením dvěma a pořád dokola. Při ručním výpočtu to jde docela rychle, ale pro nás to není perspektivní, protože na rozdíl od Euklidova algoritmu to není vhodné pro následující téma.

2b.18 Bezoutova identita

Z matematického hlediska má Euklidův algoritmus významnou nevýhodu. Sice nám poskytne vazbu $\gcd(a,b)$ na vstupní data a, b, ale ve formě procedury, tedy není to něco, so by se dalo použít ve vzorcích a s čím by se dalo vhodně manipulovat. Tento nedostatek napravuje následující tvrzení.

Věta 2b.19. (Bezoutova věta/rovnost) (Bezout's identity)
Nechť $a, b \in \mathbb{Z}$. Pak existují čísla $A, B \in \mathbb{Z}$ taková, že $\gcd(a,b) = Aa + Bb$.

Důkaz (poučný)**:** Nejprve poznamenejme, že pokud $a = 0$, pak $\gcd(0,b) = b = 0 \cdot a + 1 \cdot b$, podobně identita platí pro $b = 0$. Dále tedy budeme předpokládat, že $a, b \neq 0$ libovolná.

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 (4c.14, viz předchozí diskuse) existuje její nejmenší prvek c. Označme $c = A_c a + B_c b$. Tvrdíme, že $c = \gcd(a,b)$.

1) Protože $\gcd(a,b)$ dělí a i b, tak podle důsledku 2a.3 dělí i c. Díky $c > 0$ to podle věty 2a.5 (ii) znamená, že $\gcd(a,b) \leq c$.

2) Ukážeme, že c je společný dělitel a a b. Nechť $a = qc + r$, kde $0 \leq r < c$. Pak

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

je to tedy také celočíselná lineární kombinace čísel a, b. Nemůže ale být v M, protože c je nejmenší prvek M a zároveň máme $r < c$. Proto r nesplňuje druhou podmínku z definice množiny M, tedy neplatí $r > 0$. Takže $r = 0$ a tedy c dělí a. Obdobně ukážeme, že $c \,|\, b$. Protože je c společný dělitel, musí splňovat $c \leq \gcd(a,b)$.

Spojením 1) a 2) 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 2b.20.
Nechť $a, b \in \mathbb{Z}$. Jestliže $a \neq 0$ a $b \neq 0$, tak $\gcd(a, b)$ je nejmenší kladné číslo, které lze získat jako $Aa + Bb$ pro nějaká $A, B \in \mathbb{Z}$.

Bezoutova identita je dost možná to nejužitečnější tvrzení, které v této kapitole najdeme, a to jak pro teorii, tak pro praktické výpočty. Začneme několika ukázkami její síly v důkazech.

Uvažujme čísla $a, b \in \mathbb{Z}$. Podle Bezoutovy identity lze vyjádřit $\gcd(a, b) = Aa + Bb$. Pokud je d společný dělitel a, b, pak podle důsledku 2a.3 musí dělit i $Aa + Bb$ a hned dostáváme

Důsledek 2b.21.
Nechť $a, b \in \mathbb{Z}$. Jestliže je d společný dělitel a, b, pak d dělí $\gcd(a, b)$.

Jinak řečeno, každý strom společných dělitelů se musí nahoře spojit do společného vrcholu $\gcd(a, b)$, čím jsme kladně zodpověděli otázku ze sekce 2b.3. Řečeno jazykem kapitoly 7a, 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.

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“, a už by mělo být „celé v b“. To zní jako něco, co je evidentně pravdivé, takže možná překvapí, že to nejde dokázat snadno jen hrátkami s dělitelností, musíme nasadit mocnější nástroj.

Lemma 2b.22. (Euklidovo lemma)
Nechť $a, b \in \mathbb{Z}$ a $d \in \mathbb{N}$. Jestliže $d \mid ab$ a čísla d, a jsou nesoudělná, pak $d \mid b$.

Důkaz (poučný)**:** Mějme $a, b \in \mathbb{Z}$ a $d \in \mathbb{N}$. Podle předpokladu existuje $k \in \mathbb{Z}$ takové, že $ab = kd$. 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 $b = Ddb + Akd = (Db + Ak)d$. Díky $b, k, A, D \in \mathbb{Z}$ také $Db + Ak \in \mathbb{Z}$, což ukazuje, že d dělí b.

□

Zdá se, že by toto lemma také mělo jít dokázat pomocí prvočíselného rozkladu, což se při troše opatrnosti ohledně zápisu dá. Je v tom ale háček. Na to, abychom dokázali existenci prvočíselného rozkladu, potřebujeme právě Euklidovo lemma, viz kapitola 15. Dokazovat jej pomocí prvočísel by znamenalo, že se dělá důkaz kruhem, což, navzdory svému jménu, není důkaz.

Toto lemma se nám ještě bude hodit, o jeho významu ostatně výmluvně hovoří už to, že má jméno. Hned si ukážeme jeden užitečný důsledek.

Důsledek 2b.23.
Nechť $a, b \in \mathbb{Z}$ a p je prvočíslo. Jestliže $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.

Důkaz (poučný)**:** Jestliže $p \mid a$, pak je závěr pravdivý a důkaz je hotov. Druhá (a poslední) možnost je, že p nedělí a. Pak podle faktu 2b.8 musí být p nesoudělné s a, tudíž podle Euklidova lemmatu $p \mid b$ a závěr je zase pravdivý.

□

Toto tvrzení se dá snadno zobecnit na součin libovolně mnoha čísel.

Lemma 2b.24.
Nechť $a_1, \ldots, a_m \in \mathbb{N}$ a p je prvočíslo. Jestliže $p \mid (a_1 a_2 \cdots a_m)$, pak existuje i takové, že $p \mid a_i$.

Důkaz uděláme v kapitole 15 o prvočíslech.

Další výsledek by také neměl překvapit nikoho, kdo už začíná mít pocit, že vidí do toho, jak jsou čísla „poskládána“. Když čísla a, b vynásobíme obě shodným číslem $k \in \mathbb{N}$, tak jej „přidáváme“ do té části, kterou mají společnou, tudíž by se mělo objevit i v největším společném děliteli.

Věta 2b.25.
Nechť $a, b \in \mathbb{Z}$. Pak pro každé $k \in \mathbb{N}$ 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: Nechť $a, b \in \mathbb{Z}$, $k \in \mathbb{N}$ libovolné.

(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 $k \gcd(a, b) = kaA + kbB$. Protože $\gcd(ka, kb)$ dělí čísla ka a kb, musí dělit i celou lineární kombinaci napravo a tedy i číslo $k \gcd(a, b)$ nalevo. Protože jsou obě čísla kladná, vychází z toho $\gcd(ka, kb) \leq k \gcd(a, b)$.

Teď potřebujeme ukázat, že $k \gcd(a, b)$ dělí $\gcd(ka, kb)$. Toto již lze udělat elementárními postupy, kdy si čtenář rozmyslí, kdo koho dělí, necháme to jako cvičení 2b.7. Na toto cvičení odkážeme i ohledně důkazu části (ii). □

I toto tvrzení vypadá tak samozřejmě, že by člověk čekal, že to půjde celé nějak umlátit hrátkami s dělitelností. Už jsem zažil mnoho pokusů, ale žádný úspěšný. Bez Bezouta to prostě nejde.

Jako poslední teoretický přínos Bezoutovy identity se vrátíme k nesoudělnosti. Testovat ji pro velká může být dost práce, ale dá se to dělat i po částech. Opět je to něco, co vypadá naprosto jasně, ale důkaz nakonec zase musí použít známou identitu.

Lemma 2b.26.
Nechť $d, a, b \in \mathbb{N}$. Pak $\gcd(d, ab) = 1$ právě tehdy, když $\gcd(d, a) = 1$ a $\gcd(d, b) = 1$.

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

1) $\Longrightarrow$: Předpokládejme, že $\gcd(d, ab) = 1$. Nechť $x \in \mathbb{N}$ je společný dělitel d a a. Pak podle věty 2a.2 (ii) x dělí také d a ab, tedy platí $x \leq \gcd(d, ab) = 1$. Jediný společný dělitel a a d je tedy 1, proto jsou nesoudělná. Důkaz pro d, b je obdobný.

2) Druhý směr dokážeme obměnou. Předpokládejme, že $\gcd(d, ab) > 1$. Pak existuje číslo $k > 1$, které dělí d i ab. Podle faktu 2b.1 tudíž musí existovat i provočíslo p, které dělí k, to pak je i společným dělitelem d a ab. Lemma 2b.24 ovšem tvrdí, že si p musí vybrat, řekněme, že $p \,|\, a$. Pak ale p dělí d i a, proto $\gcd(d, a) \geq p > 1$. Neplatí tedy výrok „$\gcd(d, a) = 1$ a $\gcd(d, b) = 1$“.

□

I toto se snadno indukcí zobecní na více čísel. Přivádí nás to k dalšímu tématu, které se ještě bude hodit. Máme-li více čísel $n_1, \ldots, n_m$, jak vyjádříme, že spolu nemají nic společného? Je možné říct, že neexistuje žádné číslo $d > 1$, které by je dělilo všechny. To se ale v mnoha aplikacích ukazuje jako nedostatečné, zejména v situacích, kdy si z dotyčných čísel porůznu vybíráme a potřebujeme, aby ani ta vybraná čísla neměla nic společného.

Problém tady je, že společné dělitele je možné omezit byť jediným ze zúčastěných čísel. Stačí si zvolit $n_1 = 1$, pak jediný společný dělitel čísel $n_1, n_2, \ldots, n_m$ je jednička, ať už jsou ta ostatní čísla jakákoliv, třeba i čísla $1, 50, -50$ mají jediného společného dělitele jedničku, ačkoliv čísla 50 a -50 mají zjevně mnoho společného z hlediska dělitelnosti.

Proto se obvykle používá pojem, že čísla $n_1, \ldots, n_m$ jsou **po dvou nesoudělná**. Znamená to, že si můžeme z množiny $\{n_1, \ldots, n_m\}$ vybrat libovolná dvě čísla a, b a bude platit $\gcd(a, b) = 1$.

Pak už jsou vyloučeny jakékoliv společné faktory mezi libovolnými z čísel. Platí například, že si můžeme z této množiny vybrat několik čísel a vynásobit je spolu, pak vybrat jiná čísla a vynásobit a výsledné dva součiny budou pořád nesoudělné. Speciální případ tohoto jevu se nám bude ještě hodit, tak si jej uvedeme formálně.

Lemma 2b.27.
Nechť $n_1, \ldots, n_m \in \mathbb{N}$ jsou po dvou nesoudělná. Pak je n_1 nesoudělné s číslem $n = n_2 \cdot n_3 \cdots n_m$.

Důkaz: Dokážeme to sporem.

Kdyby tomu tak nebylo, pak by existovalo přirozené číslo $d > 1$ dělící n_1 i n. Pomocí faktu 2b.1 najdeme prvočíslo p, které dělí d, to pak musí dělit i n_1 a $n = n_2 \cdot n_2 \cdots n_m$. Podle lemma 2b.24 by tedy p dělilo některé n_j a máme spor s $\gcd(n_1, n_j) = 1$.

□

Jak brzy uvidíme, Bezoutova identita má i důležité praktické aplikace, což nás přivádí k otázce, jak vlastně ty „Bezoutovy koeficienty“ najít. Někdy se to dá uhádnout. 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 4, takových vyjádření existuje dokonce nekonečně mnoho. To je ovšem 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?

Příklad 2b.d: V příkladu 2b.b jsme zjistili, že $\gcd(408, 108) = 12$. Jak vyjádříme 12 jako lineární kombinaci 408 a 108? Přečteme si příslušný běh Euklidova algoritmu od konce.

Máme $d = 12$ a poslední rozklad říká, že $84 = 3 \cdot 24 + d$, tedy $d = 84 - 3 \cdot 24$. Řádek předtím dá $108 = 84 + 24$, tedy $24 = 108 - 84$, a proto $d = 84 - 3 \cdot (108 - 84) = (-3) \cdot 108 + 4 \cdot 84$. První řádek dá $408 = 3 \cdot 108 + 84$, tedy $84 = 408 - 3 \cdot 108$, a proto $d = (-3) \cdot 108 + 4 \cdot (408 - 3 \cdot 108) = 4 \cdot 408 + (-15) \cdot 108$.

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 2b.e: Víme, že $\gcd(408, 108) = 12$. Jak jsem viděli (důsledek 2b.20), 12 je tedy nejmenší kladné číslo, které lze získat ve formě lineární kombinace $A \cdot 408 + B \cdot 108$. Když už to neumíme uhodnout, zkusíme alespoň vyjádřit jiná čísla jako takovouto lineární kombinaci. Hned dvě se nabízejí.

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

My ovšem doufáme, že takto vyjádříme menší číslo. Zde je dobré si připomenout, že s rovnicemi umíme provádět stejné operace, jaké jsme používali při hledání zbytku, tedy odčítání násobků. Víme, jak získat co nejmenší nezáporné číslo z čísel 408 a 108, stejnou operaci provedeme i s rovnicemi: Tu druhou odečteme třikrát od první. Na pravé straně ale nebudeme roznásobovat, určitě budeme chtít zachovat čísla 108 a 408, takže si jen budeme hlídat, kolikrát se vyskytují.

$$\begin{aligned} 408 &= 1 \cdot 408 + 0 \cdot 108 \\ 108 &= 0 \cdot 408 + 1 \cdot 108 \qquad \Big/ (\#1) - 3 \times (\#2) \\ 408 - 3 \cdot 108 &= 1 \cdot 408 - 0 \cdot 408 + 0 \cdot 108 - 3 \cdot 108 \\ 84 &= 1 \cdot 408 + (-3) \cdot 108 \end{aligned}$$

Dostáváme tak Bezoutovo vyjádření pro nové číslo 84. Když tuto novou rovnici odečteme od té předchozí, dostaneme Bezoutovo vyjádření pro ještě menší číslo. Jak to dopadne na pravé straně? Jedna 408 se odebere od nulového počtu 408, tedy bude tam -1 kusů 408. Dále jsme měli 1 kus čísla 108 a jednou odebereme -3 kusy neboli tři přidáme, vzniknou čtyři. Zatím to ted vypadá takto.

$$\begin{aligned} 408 &= 1 \cdot 408 + 0 \cdot 108 \\ 108 &= 0 \cdot 408 + 1 \cdot 108 \qquad \Big/ (\#1) - 3 \times (\#2) \\ 84 &= 1 \cdot 408 + (-3) \cdot 108 \qquad \Big/ (\#2) - 1 \times (\#3) \\ 24 &= (-1) \cdot 408 + 4 \cdot 108. \end{aligned}$$

Udělejme několik klíčových pozorování. Jediné, co se mění, je levá strana a koeficienty před vstupními daty 408, 108. To znamená, že si stačí pamatovat tato tři čísla a dívat se, jak se mění. Při každé úpravě se tato čísla vytvářejí zcela stejným procesem. V třetí rovnici vznikla nová čísla pomocí předchozích takto:

$$\begin{aligned} 84 &= 408 - 3 \times 108 \\ 1 &= 1 - 3 \times 0 \\ -3 &= 0 - 3 \times 1 \end{aligned}$$

Použila se stejná operace $\#1 - 3 \times \#2$, která se aplikovala na tři sloupce. Pak jsme první rovnici ignorovali a použili druhou a třetí, takže se vlastně posunuly do pozice první a druhé, a při vzniku další rovnice jsme třikrát používali operaci $\#1 - 1 \times \#2$. Všechny tři měněná čísla tedy vždy měníme simultánně. Jak jsme poznali, kolikrát máme odebírat do dolní? Podle levého sloupce, a to stejným způsobem jako u Euklidova algoritmu pro hledání $\gcd(408, 108)$. Zkuste tento výpočet dokončit, ověřte si, že vidíte, odkud přišla ta klíčová tři čísla v posledním

řádku.

$$\begin{aligned}
408 &= 1\cdot 408 + 0\cdot 108 \\
108 &= 0\cdot 408 + 1\cdot 108 && / \ -3\times \\
84 &= 1\cdot 408 + (-3)\cdot 108 && / \ -1\times \\
24 &= (-1)\cdot 408 + 4\cdot 108 && / \ -3\times \\
12 &= 4\cdot 408 + (-15)\cdot 108
\end{aligned}$$

Kontrola posledního kroku: Na levé straně jsme třikrát odečetli číslo 24 od čísla 84. U 408 jsme třikrát odečetli násobek -1 od násobku 1, což je totéž jako přičíst trojku, vzniklo číslo 4. U 108 jsme třikrát odečetli násobek 4 od násobku -3.

Dostali jsme přesně to vyjádření pro $\gcd(408, 108)$, které jsme hledali.
△

Tento postup ukazuje, že si v průběhu Euklidova algoritmu můžeme rovnou vytvářet správné koeficienty. Potřebujeme si pamatovat tři druhy čísel. Pro čísla na levé straně jsme už u Euklidova algoritmu zavedli označení r_k z Euklidova algoritmu, takže ještě zavedeme další dvě posloupnosti A_k a B_k pro násobky před vstupními daty a, b. Na začátku je nastavíme jako v příkladu a na konci algoritmu nám dají, co potřebujeme.

Jak jsme to dělali? Čísla r_k se měnila přesně jako u EUklidova algoritmu, ale vzorce přímo převzít nemůžeme. Tam nás totiž nezajímalo, jak přesně jsme zbytek po dělení našli, hlavně že byl. Stačilo tedy do algoritmu napsat $r_{k+1} = r_{k-1} \bmod r_k$. Teď ale budeme pracovat i s čísly A_k, B_k a jak jsme viděli v příkladu, tato čísla vznikají přesně stejnou operací jako onen Euklidovský zbytek. Musíme si proto v každém kroku algoritmu zapamatovat, jaký částečný podíl q_k jsme potřebovali, abychom vyrobili $r_{k+1} = r_{k-1} - q_k r_k$, a obdobný vzorec s tímto q_k aplikovat 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 se zápornými vstupy skončí hned nebo po prvním kroku a nabídne záporného kandidáta na gcd, což pak musíme opravit.

S Algoritmus 2b.28.
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:
$k := k + 1$, $q_k = \left\lfloor \frac{r_{k-1}}{r_k} \right\rfloor$,
$r_{k+1} := r_{k-1} - q_k r_k$,
$A_{k+1} := A_{k-1} - q_k A_k$,
$B_{k+1} := B_{k-1} - q_k B_k$.
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`
$q = \left\lfloor \frac{a}{b} \right\rfloor$;
$r = a - q \cdot b$;
$r_a := A_0 - qA_1$;
$r_b := B_0 - qB_1$;
$a := b$; $b := r$;
$A_0 := A_1$; $A_1 := r_a$;
$B_0 := B_1$; $B_1 := r_b$;
`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 získané z výpočtu $r_{k-1} \bmod r_k$.

S 2b.29 Ruční výpočet.
Nejtradičnější je, když se jednotlivé kroky algoritmu zapisují do řádků podobně jako u Euklidova algoritmu, zde si ovšem musíme pamatovat tři čísla. Ukážeme to na výpočtu pro $\gcd(408, 108)$.

Potřebujeme sloupec pro vstupní data a, b a pak sloupce pro násobky před vstupními daty při vytváření lineárních kombinací. Počáteční hodnoty pro tyto pomocné sloupce si můžeme pamatovat, může pomoci, když si představíme, že vedle tradičního „Euklidovského“ sloupce přidáme jednotkovou matici. Hodně napoví, když si za těmi dvěma řádky představíme odpovídající lineární kombinace.

a, b	A	B
408	1	0
108	0	1

a, b	A	B	
408	1	0	
108	0	1	3
84	1	-3	

Teď najdeme částečný podíl $q = \left\lfloor \frac{408}{108} \right\rfloor = 3$. Nebo si všimneme, že abychom se od čísla 408 dostali co nejblíže k nule (ale chceme zůstat v nezáporných číslech), potřebujeme odečíst 108 třikrát. Pak ve všech třech sloupcích počítáme tak jako v levém, tedy odečteme trojnásobek čísla dole od čísla nahoře.

Někteří autoři radí si to q do tabulky poznamenat. Není to třeba, já to zde udělám, aby čtenář viděl, co se v tabulce děje. Zde je třeba mít na paměti, že je při tom automaticky bráno, že se q-krát odčítá. Já osobně si spíš než koeficient q raději poznamenám celou operaci, tedy psal bych „$-3\times$“, ale tady se budu držet obvyklého postupu. Čtenář si jistě vymyslí vlastní značení, které mu bude dávat smysl.

Klíčovým prvkem tohoto postupu je správně rozumět, jak vznikají nová čísla. Můžeme si představit, že v každém kroku děláme paralelně tři stejné postupy najednou ve všech sloupcích, nebo třeba že manipulujeme najednou celé řádky tabulky. Kdo umí řádkovou eliminaci u matic, tak přesně totéž dělá tady. V kapitole 4 o diofantických rovnicích uvidíme, že to navíc není náhodná podobnost, ale je tu souvislost.

Takto pokračujeme dál, pokaždé odčítáme celé řádky, násobitel je vždy určen levým sloupcem. Výsledek vypadá následovně:

a, b	A	B	
408	1	0	
108	0	1	3
84	1	-3	1
24	-1	4	3
12●	4●	-15●	2
0	-9	34	

Měli byste vidět, jak tato tabulka odráží postup z příkladu 2b.e.

Výsledek najdeme jako obvykle v řádku nad nulou, opravdu $12 = 4 \cdot 408 + (-15) \cdot 108$. Evidentně není nutné ten poslední řádek počítat celý, jakmile vidíme, že v levém sloupci vyšla nula, jsme hotovi. Nicméně v kapitole o rovnicích uvidíme, že i ten poslední řádek nese užitečnou informaci.

Je velmi užitečné, pokud toto nevnímáme jako mechanický proces, ale vidíme za tím práci s lineárními kombinacemi, které jsou kódovány jednotlivými řádky tabulky. Například v třetím řádku zdola vidíme $24 = (-1) \cdot 408 + 4 \cdot 108$, což opravdu platí. Toto pochopení nám umožní přizpůsobit si algoritmus našim potřebám.

Druhá důležitá věc je rozumět vazbě mezi pomocnými soupci a vstupními daty. Tato vazba je dána jedničkami v přípravných řádcích. Pokud chceme mít jistotu, ke kterému vstupnímu číslu patří spočítaný koeficient -15, tak sjedeme ve sloupci pohledem nahoru a podíváme se, ve kterém řádku je první jednička. Vidíme ji v řádku nadepsaném vlevo číslem 108, takže v lineární kombinaci -15 a 108 patří k sobě. Já si obvykle již přo sestavování tabulky takto v záhlaví připomenu, který sloupec se váže ke kterému číslu, ale nevnucuji to.

Toto je tedy nejrozšířenější verze ručního zápisu algoritmu. Není nejstručnější, ale je vhodným kompromisem mezi výkonem a spolehlivostí (u ručního výpočtu) a navíc nabízí zajímavé souvislosti, ke kterým se dostaneme v dalších kapitolách. Pro zajímavost představíme jednu velmi stručnou verzi (ale rizikovější) v kapitole 16, kde také najdeme důkaz věty, že rozšířený Euklidův algoritmus dělá, co má. V důkazu správnosti hraje klíčovou roli právě to, že každý řádek tabulky odpovídá příslušné lineární kombinaci vstupních dat, což se dokazuje indukcí.

V předchozí sekci jsme zjistili, že Euklidův algoritmus funguje pro všechny celočíselné vstupy, takže pokud hledáme Bezoutovu identitu pro čísla, z nichž některá jsou záporná, tak by mělo stačit aplikovat algoritmus přímo na ně. To je postup, který doporučuji. Některým lidem ale vyhovují postupy jiné, na dva docela populární se podíváme v příkladu.

Příklad 2b.f: Chceme najít $\gcd(-108, 408)$ a vyjádřit jej Bezoutovým způsobem.

Doporučený postup: Aplikujeme rozšířený Euklidův algoritmus přímo na stupní data. Již jsme viděli, že pokud bychom data dosadili v zadaném pořadí, tak by to běh algoritmu prodloužilo o dva kroky, proto je seřadíme od většího k menšímu. Abychom se v tom lépe vyznali, vyznačíme si do záhlaví souvislost pomocných sloupců a dat, kterou vystupujeme podle jedniček v prvních dvou řádcích.

Záporné b nás nutí hned v prvním kroku druhý řádek přičítat, tedy q je záporné. Tady se opravdu hodí mít na značení systém, který čtenáři vyhovuje, já bych si k druhému řádku poznamenal „+3×“.

Každopádně přečteme, že $\gcd(408,-108) = 4\cdot 408 + 15\cdot(-108)$. Abychom se přizpůsobili zadání, ještě to přepíšeme na $\gcd(-108,408) = 15\cdot(-108) + 4\cdot 408$.

Pokud bychom chtěli, aby nám vyšla přímo kombinace ve správném pořadí, mohli bychom prohodit roli pomocných sloupců odlišným umístěním jedniček:

a,b	$\overset{-108}{A}$	$\overset{408}{B}$
408	0	1
−108	1	0
⋮	⋮	⋮
12•	15•	4•
0		

a,b	$\overset{108}{A}$	$\overset{-108}{B}$	q
408	1	0	
−108	0	1	−3
84	1	3	−2
60	2	7	1
24	−1	−4	2
12•	4•	15•	2
0			

To je právě jedna z věcí, kterou si člověk může dovolit, pokud algoritmu rozumí.

Někteří lidé nemají moc rádi ta záporná q neboli přičítání řádků, raději by pracovali jen s kladnými čísly v levém sloupci. Je to možné. Jednoduché řešení je připomenout si, že $\gcd(-108,408) = \gcd(|-108|,|408|)$. Můžeme tedy najít $\gcd(408,108)$ uživatelsky přívětivým způsobem včetně Bezoutovy identity, jak jsme to udělali v předchozím příkladě: $\gcd(408,108) = 12 = 4\cdot 408 + (-15)\cdot 108$. Pak už jen stačí tuto kombinaci přepsat tak, aby se u vstupních dat objevila správná znaménka a správné pořadí:

$$\gcd(-108,408) = 12 = 15\cdot(-108) + 4\cdot 408.$$

Toto spárování dat a koeficientů je velmi důležité, protože v aplikacích nás mnohdy nezajímá přímo Bezoutova identita, ale jen konkrétní koeficient. Pokud by například u tohoto příkladu očekávala koeficient u -108 a my bychom místo toho poskytli -15 či dokonce 4, bylo by to fatální.

Druhá možnost je sofistikovanější a opět se odvíjí od znalosti, že tabulka kóduje lineární kombinace. Pokud totiž do některého z prvních dvou řádků dáme -1 místo 1, tak už se pomocný sloupec nenaváže na číslo vlevo, ale jeho opačné číslo. Je tedy možné pracovat v levém sloupci pěkně pohodlně s nezápornými čísly a zároveň dostat přímo správné koeficienty (a pohlídat si, kdo s kým je svázán, raději si to hned při sestavování tabulky připomeneme v záhlaví).

a,b	$\overset{-108}{A}$	$\overset{408}{B}$	
408	0	1	
108	−1	0	3
84	3	1	1
24	−4	−1	3
12•	15•	4•	2
0			

Čtenář by si měl vybrat přístup, který mu vyhovuje, a toho se držet.
△

Pokud už se čtenář odváží vstoupit do rozšířeného Euklidova algoritmu se zápornými čísly, pak se možná nebude bát ani záporných zbytků.

Příklad 2b.g: Tentokráte se v každém kroku odčítáním zatím posledního od předposledního řádku snažíme dostat co nejblíže k nule bez ohledu na znaménko. Vzhledem ke snaze zkrátit běh také prohodíme vstupní data do pořadí větší-menší a pak prohodíme role pomocných sloupců, abychom rovnou dostali správné pořadí koeficientů.

a,b	$\overset{-108}{A}$	$\overset{408}{B}$	q
408	0	1	
−108	1	0	−4
−24	4	1	−4
−12	−15	−4	−2
0			
12•	15•	4•	

Vyšlo nám záporné gcd, což se občas stane, ale pronásobení řádku mínusem to napravilo. Obvykle to děláme rovnou při psaní výsledné identity, což je mimochodem $\gcd(-108,408) = 15\cdot(-108) + 4\cdot 408$, do tabulky jsme přidali odpovídající řádek z pedagogických důvodů.

Je totiž zajímavá otázka, zda na to máme právo. Odpověď zní, že každý řádek v tabulce reprezentuje jistou rovnost s lineární kombinací dat, a tuto rovnost můžeme přenásobit číslem, aniž by pozbyla platnosti. Takže i

v tabulce můžeme libovolný řádek vynásobit (nenulovým) číslem, pokud chceme. Tento trik se nám také bude později hodit.

Pokud si to čtenář zkoušel sám, možná se v jednom kroku rozešel s naším řešením. Někdy totiž u záporných zbytků máme na výběr mezi dvěma stejně velkými čísly. V ukázkovém výpočtu jsem volil zápornou možnost, abych dostal stejný výsledek jako předtím. Obvykle ale preferujeme kladné číslo, což v tomto případě vede na jiný výsledek: $\gcd(-108, 408) = (-19) \cdot (-108) + (-5) \cdot 408$.

To není problém, i tato Bezoutova identita platí.

△

a, b	$\overset{-108}{A}$	$\overset{408}{B}$	q
408	0	1	
-108	1	0	-4
-24	4	1	-5
$12\bullet$	$-19\bullet$	$-5\bullet$	2
0			

Viděli jsme, že jsme získali dvě různé Bezoutovy identity. Je to dáno tím, že při použití záporných zbytků je algoritmus v průměru rychlejší, ale ztrácí některé vlastnosti, například už není jednoznačný. My víme, že Bezoutových identit existuje nekonečně mnoho (brzy to i dokážeme), a většina z nich má velké koeficienty, což se v praxi moc nehodí. V kapitole 16 mimo jiné ukážeme, že standardní forma rozšířeného Euklidova algoritmu (s nezápornými zbytky) nabízí to nejekonomičtější ze všech možných Bezoutových vyjádření. Ostatně i zde vidíme, že ta alternativa trochu narostla z dvojice $4, 15$ na dvojici (v absolutní hodnotě) $5, 19$.

Vracíme se k otázce volby algoritmu. Zkušenost ukazuje, že verze se zápornými zbytky sice mívá méně kroků, ale při ručním výpočtu nad těmi zápornými komplikacemi člověk trochu déle přemýšlí, takže to kolikrát časově trvá déle, navíc se zvyšuje procento numerických chyb (což je u zkoušky významný faktor). Ale borci a borky to zvládají. Je tedy na čtenáři, jestli se na to cítí.

Ve cvičení 2b.9 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 2d.6.

Cvičení

Cvičení 2b.1 (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 2b.11).

Cvičení 2b.2 (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 2b.3 (poučné)**:** Přesvědčte se, že odhady $\gcd(a, b) \leq \min(|a|, |b|)$ a $\operatorname{lcm}(a, b) \geq \max(|a|, |b|)$ (viz fakt 2b.4) neplatí v případě, že jedno z čísel je nulové a druhé ne.
Upravte výrazy na pravé straně tak, aby už fungovaly i pro nulu, tedy obecně.

Cvičení 2b.4 (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 2b.5 (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 2b.6 (poučné)**:** Nechť $a, b \in \mathbb{Z}$. Dokažte, že jestliže $\gcd(a, b) = 1$, pak $\operatorname{lcm}(a, b) = |a| \cdot |b|$.

Cvičení 2b.7 (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 2b.22.

Cvičení 2b.8 (dobré, poučné)**:** Dokažte, že pro každé $a, b, k \in \mathbb{N}$ platí:
(i) $k \gcd(a, b) \leq \gcd(ka, kb)$.
(ii) Jestliže k dělí a i b, pak $\gcd\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{\gcd(a,b)}{k}$.
Nápověda: (ii) lze dokázat pomocí (i).

Cvičení 2b.9 (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 2b.10 (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 d splňující vlastnost, že $a_i \,|\, d$ pro všechna i.
Dokažte následující:
Nechť $a, b, c \in \mathbb{N}$ jsou libovolná. Nechť $d = \gcd(a, b, c)$. Pak $d = \gcd(\gcd(a, b), c)$.

Cvičení 2b.11 (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 2b.12 (poučné)**:** Nechť $a_1, a_2, \dots, a_n \in \mathbb{N}$.
Rozmyslete si, zda platí $\operatorname{lcm}(a_1,a_2,\dots,a_n) = \frac{a_1 \cdot a_2 \cdots a_n}{\gcd(a_1,a_2,\dots,a_n)}$.
Rozmyslete si, zda platí, že když jsou a_i po dvou nesoudělná, pak $\operatorname{lcm}(a_1,a_2,\dots,a_n) = a_1 \cdot a_2 \cdots a_n$.
Pro případný důkaz platnosti viz cvičení .

Řešení:
2b.1: 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 $d \le |a|$ 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.
2b.2: Případ $a = 0$ dává $\gcd(a,ka) = \gcd(0,0) = 0 = |a|$ $\gcd(a,a^k) = \gcd(0,0) = 0 = |a|$, obdobně pro lcm. Předpokládejme proto $a \neq 0$. Kdyby dále $k = 0$ v (i), tak $\gcd(a,ka) = \gcd(a,0) = |a|$ a $\gcd(a,ka) = \gcd(a,0) = 0 = |ka|$. Dále tedy předpokládejme $k \neq 0$.
(i): Případ $a = 0$ dává $\gcd(a,ka) = \gcd(0,0) = 0 = |a|$, obdobně pro lcm. Kdyby dále $k = 0$ v (i), tak $\gcd(a,ka) = \gcd(a,0) = |a|$ a $\operatorname{lcm}(a,ka) = \gcd(a,0) = 0 = |ka|$. Zbývají případy $a \neq 0$, $k \neq 0$.
Protože $|a|$ dělí a i ka, patří do množiny společných dělitelů. A protože každý společný dělitel d musí splňovat $d \le |a|$, tak žádné větší číslo než $|a|$ v té množině není.
Obdobný rozbor ukáže $\operatorname{lcm}(a,ka) = |ka|$.
(ii): Podobně jako (i), zde není nutno řešit $k = 0$.
2b.3: Obecně platí $\gcd(a,b) \le \max(|a|,|b|)$ a $\operatorname{lcm}(a,b) \ge \min(|a|,|b|)$.
2b.4: (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			

$\gcd(131, 2\cdot 59) = 1$
$\operatorname{lcm}(131, 2\cdot 59) = 131\cdot 2\cdot 59 = 15458$
$\gcd(118,131) = 1 = 10\cdot 118 + (-9)\cdot 131$

2b.5: (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			

$\gcd(353,-605) = 1 = 12\cdot 353 + 7\cdot(-605)$

2b.6: Stačí použít $\operatorname{lcm}(a,b)\cdot\gcd(a,b) = |a|\cdot|b|$.
Správný matematický přístup je využívat již odvedené práce.

2b.7: Z předpokladů $c = ka$, $c = lb$ a $1 = Aa + Bb$, kde $k, l, A, B \in \mathbb{Z}$. Vynásobením Bezouta $c = Aac + Bbc = Aa(lb) + Bb(ka) = (Al + Bk)ab$ a $Al + Bk \in \mathbb{Z}$, tedy $(ab) \mid c$.
2b.8: (i): Označme $d = \gcd(a, b)$ a $e = \gcd(ka, kb)$. Pak d dělí a, b, proto kd dělí ka, kb, platí tedy $kd \leq e$. Naopak: Podle Bezouta $d = Aa + Bb$, proto $kd = Aka + Bkb$, e dělí obě napravo, proto dělí i kd a tedy $e \leq kd$.
(ii) Aplikujte (i) na $a' = \frac{a}{k}$ a $b' = \frac{b}{k}$.
2b.9: 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.
2b.10: Označme $D = \gcd(\gcd(a, b), c)$. 1) Z definice $D \mid c$ a $D \mid \gcd(a, b)$, odtud pak zase $D \mid a$ a $D \mid b$. Takže D je společný dělitel všech čísel a, b, c, tudíž $D \leq d$, neboť d je největší takový.
Pokud je d největší společný dělitel a, b, c, pak je to i společný dělitel a, b, tudíž musí platit $d \mid \gcd(a, b)$. Také $d \mid c$, takže d je společný dělitel čísel $\gcd(a, b)$ a c, tudíž $d \leq D$.
2b.11: 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 2b.21 dokonce $\gcd(a, b, c)$ dělí $\gcd(a, b)$.
Toto se snadno zobecní, pokud je množina různých přirozených čísel $\{a_1, a_2, \dots, a_n\}$ podmnožinou množiny různých přirozených čísel $\{b_1, b_2, \dots, b_m\}$, pak $\gcd(b_1, \dots, b_m)$ dělí $\gcd(a_1, \dots, a_n)$.
2b.12: Je dorbé 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 $\frac{2\cdot3\cdot4}{\gcd(2,3,4)} = 24$.
Experimenty či intuice (zejména pokud už čtenář trochu umí pracovat s provočíselnými rozklady) naznačí, že pokud jsou ovšem a_i po dvou nesoudělná, pak už vzorec $\operatorname{lcm}(a_1, a_2, \dots, a_n) = a_1 \cdot a_2 \cdots a_n$ platí.

2c. Zaokrouhlování

Kromě práce se zbytkem existuje další možnost, jak pracovat s dělením celých čísel a přitom zůstat v tomto číselném oboru, jmenovitě zaokrouhlování. Pro počítačové vědy to je užitečný nástroj, tak se na něj podíváme blíže. V analýze bývá zvykem zaokrouhlovat na nejbližší celé číslo, v diskrétní matematice zaokrouhlujeme dolů a nahoru.

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

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

Anglicky se těmto funkcím říká **floor** (podlaha) a **ceiling** (strop), značení to trochu napovídá.

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 2c.a: Podle definice

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

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

Snadno také nahlédneme, že

$$\lfloor 13.23 \rfloor = \max\{\dots, 0, \dots, 10, 11, 12, 13\} = 13 \qquad \text{a}$$
$$\lceil 13.23 \rceil = \min\{14, 15, 16, \dots\} = 14.$$

Zdá se, že definice dělá, co má. Máme ovšem také

$$\lfloor -13.23 \rfloor = \max\{\dots, -17, -16, -15, -14\} = -14 \qquad \text{a}$$
$$\lceil -13.23 \rceil = \min\{-13, -12, -12, \dots, 0, \dots\} = -13.$$

Poprvé to možná překvapí, ale dává to smysl. To „dolů“ se myslí ve smyslu reálné osy neboli doleva, od čísla 13.23 sjedeme doleva k 13 a stejně tak od čísla -13.23 sjedeme doleva k nejbližšímu celému číslu na -14. Funkce $\lfloor x \rfloor$ je tedy něco jiného než funkce „část čísla před desetinnou tečkou/čárkou“, na to je třeba dát pozor při programování. Pokud pracujeme s kladnými čísly, tak to vyjde nastejno a máme o starost méně (což už nás nepřekvapuje).
△

Doporučujeme, aby si teď čtenář namaloval grafy obou funkcí.
Při hledání $\lfloor x \rfloor$ to správné celé číslo poznáme podle podmínky z definice, ale lze to i jinak.

Fakt 2c.1.
Nechť $x \in \mathbb{R}$, $n \in \mathbb{Z}$. Pak platí:
(i) $\lfloor x \rfloor = n$ právě tehdy, když $n \leq x < n+1$.
(ii) $\lceil x \rceil = n$ právě tehdy, když $n-1 < x \leq n$.
(iii) $\lfloor x \rfloor = n$ právě tehdy, když $x-1 < n \leq x$.
(iv) $\lceil x \rceil = n$ právě tehdy, když $x \leq n < x+1$.

Opravdu to funguje? Zkusíme najít $\lfloor -13.23 \rfloor$. Podle (i) je odpovědí celé číslo n splňující $n \leq -13.23 < n+1$, to je $n = -14$, správně. Podle (iii) zase hledáme celé číslo n splňující $-14.23 < n \leq -13.23$, i zde to najde $n = -14$. Zdá se, že by to mohlo být dobře, stojí za to pokusit se o důkaz.

Důkaz (pro úplnost)**:** (i) $\Longrightarrow$: Předpokládejme, že $n = \lfloor x \rfloor$. Pak $n = \max\{m \in \mathbb{Z} : m \leq x\}$. To mimo jiné znamená, že n v té množině leží, tudíž $n \leq x$. Protože je to ale maximální celé takové číslo, tak už v ní $n+1$ neleží, proto neplatí $n+1 \leq x$ neboli platí $n+1 > x$.
(i) $\Longleftarrow$: Předpokládejme, že celé číslo n splňuje $n \leq x < n+1$. Pak toto n leží v množině $\{m \in \mathbb{Z} : m \leq x\}$. Z nerovnosti $x < n+1$ ale vidíme, že $n+1$ už v této množině neleží. Neleží tam ani čísla větší (také nesplňují $m \leq x$), proto je n největší číslo z této množiny, tedy $n = \lfloor x \rfloor$.
(ii) se dokazuje podobně.
(iii) $\Longrightarrow$: Jestliže je $n = \lfloor x \rfloor$, pak podle (i) je $n \leq x$ a také $x < n+1$, což je $x - 1 < n$.
(iii) $\Longleftarrow$: Nechť celé číslo n splňuje $x - 1 < n \leq x$. Z levé nerovnosti máme $x < n+1$, proto $n \leq x < n+1$ a podle (i) je $n = \lfloor x \rfloor$. Důkaz (iv) je podobný.

□

Když do vztahů (iii) a (iv) dosadíme namísto n příslušnou funkci, dostáváme následující:

Důsledek 2c.2.
Pro všechna $x \in \mathbb{R}$ platí $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$.

Ukážeme si ještě jiný způsob, jak poznat, že nějaké číslo n je správnou hodnotou.

Fakt 2c.3.
Nechť $x \in \mathbb{R}$, $n \in \mathbb{Z}$. Pak platí:
(i) $n = \lfloor x \rfloor$ právě tehdy, když existuje ε splňující $0 \leq \varepsilon < 1$ a $x = n + \varepsilon$.
(ii) $n = \lceil x \rceil$ právě tehdy, když existuje ε splňující $0 \leq \varepsilon < 1$ a $x = n - \varepsilon$.

Důkaz (pro úplnost)**:** (i) $\Longrightarrow$: Definujme $\varepsilon = x - \lfloor x \rfloor = x - n$. Pak $x = n + \varepsilon$ a podle (i) z faktu 2c.1 také $0 \leq \varepsilon < 1$.
(i) $\Longleftarrow$: Předpokládejme, že $x = n + \varepsilon$ a $0 \leq \varepsilon < 1$. Pak $n \leq x$ a z $\varepsilon < 1$ máme $x < n + 1$, tudíž je splněna podmínka v (i) faktu 2c.1 a tudíž $n = \lfloor x \rfloor$.
Důkaz (ii) je obdobný.

□

Někteří autoři definují $\lfloor x \rfloor$ a $\lceil x \rceil$ pomocí podmínek z tohoto faktu.

Matematici mají rádi, když věci splňují rozličná pravidla, protože se pak s nimi lépe pracuje. Líbily by se nám věci jako $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ či podobné pravidlo pro násobení, ale zrovna tohle nefunguje (zkuste najít protipříklady). Zato platí desítky různých speciálních vzorečků. Některé si předvedeme jako názornou ukázku a v rámci tréninku je i dokážeme. Rovnou podotkněme, že pro nás nebudou důležité, takže nemá smysl se je učit nazpaměť.

Fakt 2c.4.
Nechť $x \in \mathbb{R}$. Pak platí:
(i) $\lfloor -x \rfloor = -\lceil x \rceil$.
(ii) $\lceil -x \rceil = -\lfloor x \rfloor$.
(iii) $\lfloor x + a \rfloor = \lfloor x \rfloor + a$ pro všechna $a \in \mathbb{Z}$.
(iv) $\lceil x + a \rceil = \lceil x \rceil + a$ pro všechna $a \in \mathbb{Z}$.

Důkaz (rutinní)**:** (i): Nechť $n = \lceil x \rceil$. Pak podle faktu 2c.1 (ii) platí $n - 1 < x \leq n$. Potom také platí $-n + 1 > -x \geq -n$, tedy $(-n) \leq -x < (-n) + 1$ a podle faktu 2c.1 (i) je $-n = \lfloor -x \rfloor$.

Důkaz (ii) je podobný.

(iii): Označme si $n = \lfloor x \rfloor$. Pak podle faktu 2c.1 (i) je $n \leq x < n + 1$. Pak $n + a$ je celé číslo splňující $n + a \leq x + a < n + a + 1$, tudíž podle faktu 2c.1 (i) je $n + a = \lfloor x + a \rfloor$.

Důkaz (iv) je obdobný.

□

Další vzorečky viz cvičení. A teď pár aplikací (další zase viz cvičení nebo třeba fakt 11b.6).

Příklad 2c.b: Máte USB flashku o velikosti 12GB. Kolik se na ni vejde filmů o velikosti 700MB?

Odpověď: $\left\lfloor \frac{12 \cdot 1024}{700} \right\rfloor = 17$.

△

Příklad 2c.c: Zvolme si nějaké $d \in \mathbb{N}$. Kolik přirozených čísel z množiny $\{1, 2, \ldots, n\}$ pro nějaké $n \in \mathbb{N}$ je dělitelných d?

Pomůže postřeh, že ještě v množině $\{1, 2, \ldots, d-1\}$ není žádné, v množinách $\{1, 2, \ldots, d\}$ až $\{1, 2, \ldots, 2d-1\}$ je jedno, v množinách $\{1, 2, \ldots, 2d\}$ až $\{1, 2, \ldots, 3d-1\}$ jsou dvě a tak dále. Rozmyslete si, že se to dá vzorcem vyjádřit snadno takto: Těchto čísel je $\left\lfloor \frac{n}{d} \right\rfloor$.

△

Funkcí zaokrouhlování dolů jsme už neoficiálně použili, když jsme v předchozí sekci někdy hledali zbytek přes dělení a částečný podíl. Správný vzorec si potvrdíme oficiálním tvrzením.

Fakt 2c.5.
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 $d < 0$.

Důkaz (rutinní, poučný)**:** Máme $a = qd + r$ a $0 \leq r < |d|$. Pak $\frac{a}{d} = q + \frac{r}{d}$, přičemž $q \in \mathbb{Z}$ a $0 \leq \left|\frac{r}{d}\right| < 1$. Čísla q a $\varepsilon = \left|\frac{r}{d}\right|$ pak spolu s faktem 2c.2 (i) a (ii) dávají žádaný výsledek.

□

Ukažme si jednu užitečnou aplikaci.

Příklad 2c.d: Dělení se zbytkem nabízí efektivní algoritmus, jak najít zápis čísla n vzhledem k základu b. Představme si číslo $n \in \mathbb{N}$ vyjádřené vzhledem k základu b, tedy $n = (a_k \ldots a_1 a_0)_b$. To znamená, že $n = \sum_{k=0}^{n} a_i b^i$. Chytře si to rozepíšeme:

$$n = a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0 = (a_k b^{k-1} + \cdots + a_2 b + a_1) \cdot b + a_0.$$

Potřebujeme, aby se nám cifra a_0 z toho davu nějak vydělila, aby získala jiný charakter. To se stane, pokud n vydělíme číslem b. Dostaneme totiž číslo $\frac{n}{b} = a_k b^{k-1} + \cdots + a_2 b + a_1 + \frac{a_0}{b}$, přičemž napravo všechny části až na tu poslední jsou celá čísla, zatímco díky $a_0 < b$ je to poslední desetinné, menší než 1. Jinými slovy, a_0 je přesně zbytek po dělení n číslem b.

Zaokrouhlení dolů nám poskytne celou část po dělení $a_k b^{k-1} + \cdots + a_2 b + a_1 = (a_k b^{k-2} + \cdots + a_2) b + a_1$, ze které bychom rádi nějak vydělili a_1. Nabízí se, že zopakujeme předchozí trik, tedy vydělíme číslem b atd. Z toho vychází algorimus. Ukážeme dvě verze, jedna se na to dívá matematicky, kde přímo říkáme, co chceme, jak jsme to výše vymysleli, a druhá ušetří výpočet modula výměnou za registr navíc.

Verze 1.

```
procedure conversion (n, b: positive integer)
q := n; k := −1;
repeat
        k := k + 1;
        a_k := q mod b;
        q := ⌊q/b⌋;
    until q = 0;
output: n = (a_k ... a_1 a_0)_b;
```

Verze 2.

```
procedure conversion (n, b: positive integer)
q := n; k := 0;
repeat
        x := ⌊q/b⌋;
        a_k := q − xb;
        q := x;
        k := k + 1;
    until q = 0;
output: n = (a_k ... a_1 a_0)_b;
```

Jako příklad si převedeme 32 do trojkové soustavy.
Iniciace: $q = 32$, $b = 3$, $k = -1$.
Krok 1: $k = 0$. $x = \lfloor \frac{32}{3} \rfloor = 10$, $a_0 = 32 \bmod 3 = 32 - 10 \cdot 3 = 2$, $q = 10$.
Krok 2: $k = 1$. $x = \lfloor \frac{10}{3} \rfloor = 3$, $a_1 = 10 \bmod 3 = 10 - 3 \cdot 3 = 1$, $q = 3$.
Krok 3: $k = 2$. $x = \lfloor \frac{3}{3} \rfloor = 1$, $a_2 = 3 \bmod 3 = 3 - 1 \cdot 3 = 0$, $q = 1$.
Krok 4: $k = 3$. $x = \lfloor \frac{1}{3} \rfloor = 0$, $a_3 = 1 \bmod 3 = 3 - 0 \cdot 3 = 1$, $q = 0$.
Konec, $32 = (1012)_3$.
Zkouška: $1 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0 = 27 + 3 + 2 = 32$.

Zajímavou otázkou je, jak převádět (kladná) desetinná čísla. Jejich celou část převedeme algoritmem výše, zbývá vymyslet, jak převést část za desetinnou čárkou. Zase se na to podíváme zblízka. Uvažujme kladné číslo c menší než 1, napíšeme jej v b-soustavě jako

$$c = \sum_{k=1}^{\infty} a_{-k} b^{-k} = a_{-1} \frac{1}{b} + a_{-2} \frac{1}{b^2} + a_{-3} \frac{1}{b^3} + \cdots$$

(rozvoj může a nemusí být nekonečný). Potřebujeme vypreparovat cifry a_{-k} pomocí počítání s celými čísly. Dokážeme nějak zařídit, aby se ten první člen s a_{-1} nějak vydělil svou povahou od ostatních? Ano, stačí c vynásobit číslem b. Dostaneme pak $cb = a_{-1} + a_{-2} \frac{1}{b} + a_{-3} \frac{1}{b^2} + \cdots$, přičemž první číslo a_{-1} je celé a ostatní části jsou menší než 1, dokonce i po sečtení (to je třeba trochu prozkoumat matematicky, není to tak těžké). Cifru a_{-1} tedy vidíme jako celou část čísla cb, zatímco desetinná část nám dá ten zbytek.

Ten lze zapsat jako $cb - a_{-1} = a_{-2} \frac{1}{b} + a_{-3} \frac{1}{b^2} + \cdots$ a máme teď šanci vyseparovat cifru a_{-2} tím, že toto číslo zase vynásobíme číslem b. Tak pokračujeme buď donekonečna, nebo dokud nedostaneme jako zbytek nulu.

`procedure` *conversion* (c: real $\in (0,1)$, b: positive integer)
$x = c$, $k := 0$;
`repeat`
$k := k - 1$;
$a_k := \lfloor xb \rfloor$;
$x := xb - a_k$;
`until` $x = 0$;
`output:` $c = (0.a_{-1}a_{-2}a_{-3} \ldots a_k)_b$;
△

Cvičení

Cvičení 2c.1 (rutinní)**:** Kolik bajtů (bytes) je třeba na zakódování informace v délce 4/10/500/3000 bitů (bits)?

Cvičení 2c.2 (dobré)**:** Nechť $a < b \in \mathbb{R}$.
(i) Kolik celých čísel se nachází v intervalu $\langle a, b \rangle$?
(ii) Kolik celých čísel se nachází v intervalu (a, b)?

Cvičení 2c.3 (poučné)**:** Dokažte, že pro $x \in \mathbb{R}$ platí $\lceil x \rceil - \lfloor x \rfloor = \begin{cases} 1, & x \notin \mathbb{Z}; \\ 0, & x \in \mathbb{Z}. \end{cases}$

Cvičení 2c.4 (poučné)**:** Dokažte, že pro $n \in \mathbb{Z}$ platí $\lfloor n/2 \rfloor = \begin{cases} n/2, & n \text{ sudé}; \\ (n-1)/2, & n \text{ liché}. \end{cases}$

Cvičení 2c.5 (dobré)**:** Načrtněte grafy funkcí $f_1(x) = \lfloor 2x \rfloor$, $f_2(x) = \lfloor x/2 \rfloor$, $f_3(x) = \lfloor x \rfloor + \lfloor x/2 \rfloor$, $f_4(x) = \lceil x \rceil + \lfloor x/2 \rfloor$, $f_5(x) = \lceil 2\lfloor x/2 \rfloor + \frac{1}{2} \rceil$ a $f_6(x) = \lceil x - 2 \rceil + \lfloor x + 2 \rfloor$.

Cvičení 2c.6 (dobré)**:** Dokažte, že pro všechna $n \in \mathbb{Z}$ platí:
(i) $\lfloor \lfloor n/2 \rfloor / 2 \rfloor = \lfloor n/4 \rfloor$;
(ii) $\lfloor n/2 \rfloor \cdot \lceil n/2 \rceil = \lfloor n^2/4 \rfloor$.

Cvičení 2c.7 (poučné, dobré)**:** Dokažte či vyvraťte následující tvrzení:
(i) $\forall x \in \mathbb{R}$: $\lfloor 2x \rfloor = 2\lfloor x \rfloor$.
(ii) $\forall x, y \in \mathbb{R}$: $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$.
(iii) $\forall x, y \in \mathbb{R}$: $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$.
(iv) $\forall x, y \in \mathbb{R}$: $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil$ je 0 nebo 1.
(v) $\forall x, y \in \mathbb{R}$: $\lceil xy \rceil = \lceil x \rceil \cdot \lceil y \rceil$.
(vi) $\forall x, y \in \mathbb{R}$: $\lfloor xy \rfloor = \lfloor x \rfloor \cdot \lfloor y \rfloor$.
(vii) $\forall x \in \mathbb{R}$: $\lfloor \lceil x \rceil \rfloor = \lceil x \rceil$.

(viii) $\forall x \in \mathbb{R}$: $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$.

(ix) $\forall x \in \mathbb{R}$: $\lfloor \sqrt{\lceil x \rceil} \rfloor = \lfloor \sqrt{x} \rfloor$.

(x) $\forall x \in \mathbb{R}$: $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$.

(xi) $\forall x \in \mathbb{R}$: $\lceil \sqrt{\lceil x \rceil} \rceil = \lceil \sqrt{x} \rceil$.

Cvičení 2c.8:

Dokažte, že pro každé $x \in \mathbb{R}$ platí $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Nápověda: Použijte fakt 2c.2, rozeberte případy $\varepsilon < \frac{1}{2}$ a $\varepsilon \geq \frac{1}{2}$.

Řešení:

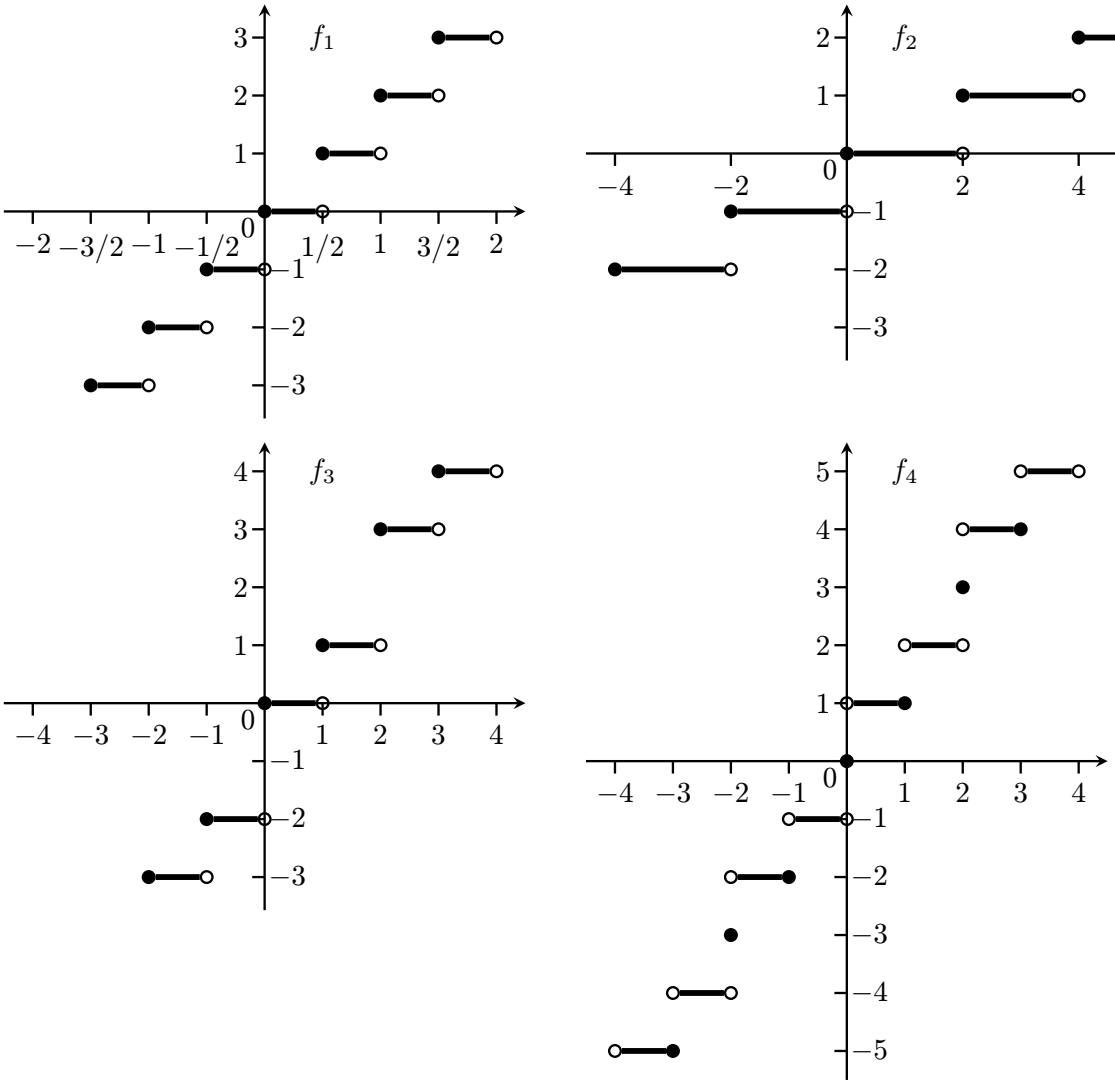
2c.1: 1 byte je 8 bits, takže: $\lceil \frac{4}{8} \rceil = 1$, $\lceil \frac{10}{8} \rceil = 2$, $\lceil \frac{500}{8} \rceil = 63$, $\lceil \frac{3000}{8} \rceil = 375$.

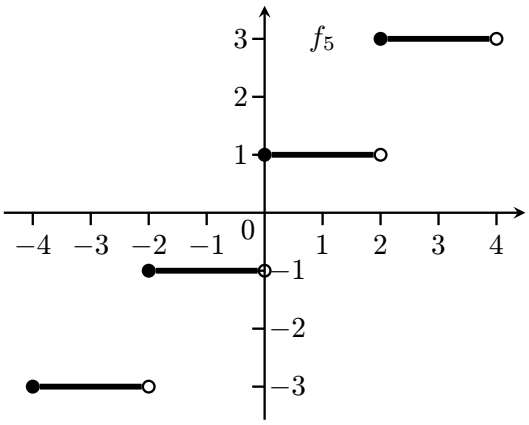
2c.2: Toto chce hodně experimentovat se zaokrouhlováním. (i): $\lfloor b \rfloor - \lceil a \rceil + 1$; (ii): $\lceil b \rceil - \lfloor a \rfloor - 1$.

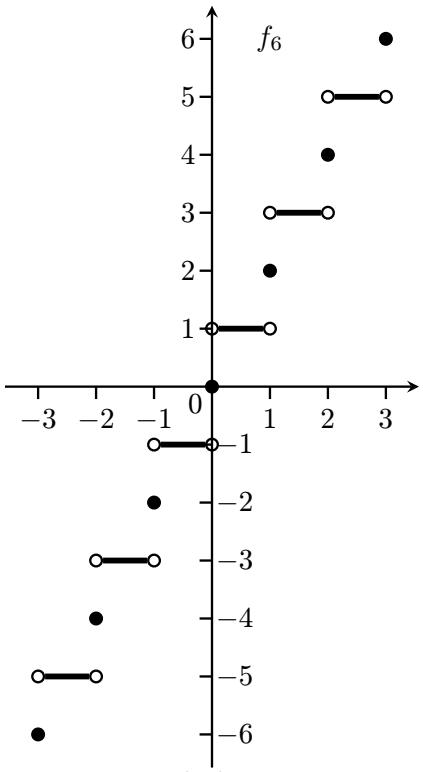
2c.3: Nechť $x = n + r$, kde $r \in \langle 0.1)$. Jestliže $r = 0$, pak $\lfloor x \rfloor = \lceil x \rceil = n$, jinak $\lfloor x \rfloor = n$ a $\lceil x \rceil = n + 1$.

2c.4: Je-li n sudé, pak $n = 2k$ pro $k \in \mathbb{Z}$ a proto $\lfloor \frac{n}{2} \rfloor = \lfloor k \rfloor = k = \frac{n}{2}$. Je-li n liché, pak $n = 2k + 1$ pro $k \in \mathbb{Z}$ a proto $\lfloor \frac{n}{2} \rfloor = \lfloor k + \frac{1}{2} \rfloor = k = \frac{n-1}{2}$.

2c.5:







2c.6: (i): Nechť $n = 4k + r$ pro $k \in \mathbb{Z}$ a $r = 0, 1, 2, 3$. Pak $\lfloor \frac{r}{2} \rfloor$ je 0 nebo 1, tedy $\lfloor \frac{1}{2} \lfloor \frac{r}{2} \rfloor \rfloor = 0$ a proto $\lfloor \frac{1}{2} \lfloor \frac{n}{2} \rfloor \rfloor = \lfloor \frac{1}{2} \lfloor 2k + \frac{r}{2} \rfloor \rfloor = \lfloor k + \frac{1}{2} \lfloor \frac{r}{2} \rfloor \rfloor = k + \lfloor \frac{1}{2} \lfloor \frac{r}{2} \rfloor \rfloor = k = \lfloor \frac{n}{4} \rfloor$.
(ii): Nechť $n = 2k + r$, kde $k \in \mathbb{Z}$ a $r = 0, 1$. Pak $\lfloor \frac{n}{2} \rfloor = k$ a $\lceil \frac{n}{2} \rceil = k + r$, proto $\lfloor \frac{n}{2} \rfloor \cdot \lfloor \frac{n}{2} \rfloor = k(k + r)$, zatimco $\lfloor \frac{n^2}{4} \rfloor = \lfloor \frac{4k^2+4kr+r^2}{4} \rfloor = k^2 + kr + \lfloor \frac{r^2}{4} \rfloor = k^2 + kr = k(k + r)$.
2c.7: (i): Neplatí, třeba: $\lfloor 2 \cdot 0.7 \rfloor = 1$, ale $2\lfloor 0.7 \rfloor = 0$.
(ii): Neplatí, třeba $\lfloor 0.5 + 0.5 \rfloor = 1$, ale $\lfloor 0.5 \rfloor + \lfloor 0.5 \rfloor = 0$.
(iii): Neplatí, třeba $\lceil 0.4 + 0.4 \rceil = 1$, ale $\lceil 0.4 \rceil + \lceil 0.4 \rceil = 2$.
(iv): Platí, případy: pokud $x, y \in \mathbb{Z}$, pak evidentně vyjde 0. Pokud $x \in \mathbb{Z}$ a $y \notin \mathbb{Z}$, pak $x = n+r$ a $x+y = x+y+r$, kde $n \in \mathbb{Z}$, $n + y \in \mathbb{Z}$ a $0 < r < 1$, proto $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil = n + 1 + y - (n + y + 1) = 0$. Zbývá případ $x, y \notin \mathbb{Z}$, tedy $x = n + r$, $y = m + s$, kde $m, n \in \mathbb{Z}$ a $0 < r, s < 1$. Dva případy. Pokud $r + s > 1$, pak $\lceil x \rceil + \lceil y \rceil - \lceil x+y \rceil = n+1+y+1-(n+y+2) = 0$. Pokud $r+s \leq 1$, pak $\lceil x \rceil + \lceil y \rceil - \lceil x+y \rceil = n+1+y+1-(n+y+1) = 1$.
(v): Neplatí, třeba $\lceil 1.1 \cdot 1.1 \rceil = \lceil 1.21 \rceil = 2$, ale $\lceil 1.1 \rceil \cdot \lceil 1.1 \rceil = 2 \cdot 2 = 4$.
(vi): Neplatí, třeba $\lfloor 4 \cdot 0.5 \rfloor = \lfloor 2 \rfloor = 2$, ale $\lfloor 4 \rfloor \cdot \lfloor 0.5 \rfloor = 4 \cdot 0 = 0$.
(vii) a (viii): Platí, protože $\lfloor x \rfloor \in \mathbb{Z}$ a $\lfloor x \rfloor \in \mathbb{Z}$, takže aplikace dalšího zaokrouhlení již nic neovlivní.
(ix): Neplatí, nechť $x = 1.9^2 = 3.61$, pak $\lfloor \sqrt{\lceil x \rceil} \rfloor = 2$, ale $\lfloor \sqrt{x} \rfloor = 1$.
(x): Platí. Pro $x \geq 0$ nechť $n \in \mathbb{N}_0$ je číslo takové, že $n^2 \leq x < (n + 1)^2$. Pak $n \leq \sqrt{x} < n + 1$, proto $\lfloor \sqrt{x} \rfloor = n$. Jelikož $n^2 \in \mathbb{Z}$, bude i $n^2 \leq \lfloor x \rfloor < (n + 1)^2$ a tedy $n \leq \sqrt{\lfloor x \rfloor} < n + 1$, proto i $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = n$.
(xi): Platí, důkaz jako v (xi), pro dané $x \geq 0$ se vybere $n \in \mathbb{N}$ tak, aby $(n - 1)^2 < x \leq n^2$.
2c.8: $x = \lfloor x \rfloor + \varepsilon$.
1) $\varepsilon < \frac{1}{2}$: Pak $x + \frac{1}{2} = \lfloor x \rfloor + \left(\varepsilon + \frac{1}{2}\right)$ a $0 \leq \varepsilon + \frac{1}{2} < 1$, podle faktu 2c.2 (ii) platí $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor$. Také $2x = 2\lfloor x \rfloor + (2\varepsilon)$ a $0 \leq 2\varepsilon < 1$, podle faktu 2c.2 (ii) platí $\lfloor 2x \rfloor = 2\lfloor x \rfloor$. Spojit: $\lfloor 2x \rfloor = 2\lfloor x \rfloor = \lfloor x \rfloor + \lfloor x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.
2) $\frac{1}{2} \leq \varepsilon < 1$: Pak $0 \leq \varepsilon - \frac{1}{2} < 1$. Také $x + \frac{1}{2} = (\lfloor x \rfloor + \varepsilon) + \frac{1}{2} = (\lfloor x \rfloor + 1) + \left(\varepsilon - \frac{1}{2}\right)$, podle faktu 2c.2 (ii) pak $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor + 1$.
$\frac{1}{2} \leq \varepsilon < 1$ dává $1 \leq 2\varepsilon < 2$, tedy $0 \leq 2\varepsilon - 1 < 1$. Také $2x = 2\lfloor x \rfloor + 2\varepsilon = (2\lfloor x \rfloor + 1) + (2\varepsilon - 1)$, podle faktu 2c.2 (ii) pak $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$. Spojit: $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1 = \lfloor x \rfloor + (\lfloor x \rfloor + 1) = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

2d. Matice nad celými čísly

Ve světě celých čísel se dají dělat i komplikovanější výpočty, například pracovat s maticemi, které mají celočíselné prvky, říkáme jim „matice nad $\mathbb{Z}$“. Protože máme stejné operace sčítání a násobení jako obvykle, bude i sčítání a násobení matic fungovat obvyklým způsobem. Podstatné zde je, že když sečteme či vynásobíme dvě matice s celočíselnými prvky, bude i výsledná matice obsahovat pouze celá čísla. Problém nevzniká ani při transponování matice.

Stejně tak lze počítat determinant čtvercové matice, který je podle definice součtem součinů prvků, tedy opět celé číslo. Lze jej počítat i rozvojem podle řádku či sloupce, neboť opět používáme jen operace, které vedou na

celá čísla. Dalším důležitým pojmem je inverzní matice. I ve světě celých čísel lze k dané čtvercové matici A hledat takovou matici B, aby platilo $AB = E_n$ a $BA = E_n$. Zde se situace zajímavě zkomplikuje.

Podle pravidla počítání determinantů by pak mělo platit $\det(A) \cdot \det(B) = 1$. Ovšem čísla $\det(A), \det(B)$ jsou celá, což nedává moc možností. Vidíme, že pokud není determinant matice A roven ± 1, tak inverzní matici prostě mít nemůže. Platí to i naopak.

Věta 2d.1.
Ke čtvercové matici A nad $\mathbb{Z}$ existuje matice inverzní právě tehdy, když $\det(A) = \pm 1$.
Tato inverzní matice je pak dána vzorcem $A^{-1} = \det(A)^{-1} D^T$, kde D je matice kofaktorů.

Připomeňme, že prvek d_{ij} matice D získáme tak, že z matice A vyškrtneme řádek i a sloupec j, spočítáme determinant výsledné matice a vynásobíme jej číslem $(-1)^{i+j}$. Coby determinant je d_{ij} zase celé číslo, tedy matice D je celočíselná, v tom problém není. Slabinou je to dělení číslem $\det(A)$. Naši větu lze říci i jinak, způsobem, který ukáže její návaznost na obdobnou větu pro reálné matice.

• Čtvercová matice A nad $\mathbb{Z}$ je invertibilní právě tehdy, když má $\det(A)$ inverzní číslo.

Tato formulace je velmi obecná. Například v oboru reálných čísel mají inverzní číslo všechna nenulová čísla, takže to souhlasí, tam jsou inverzní všechny matice s nenulovým determinantem.

Invertibilní celočíselné matice jsou velmi důležité v mnoha aplikovaných oborech, například řízení či optimalizaci. Říkají jim „unimodulární“ (zhruba řečeno matice s jednotkovou velikostí, což zde můžeme brát jako připomínku onoho determinantu ± 1, ale váže se to i k jejich působení) a dokazují o nich různé užitečné vlastnosti. My se zde tomuto tématu věnovat nebudeme.

Příklad 2d.a: Najdeme A^{-1} pro $A = \begin{pmatrix} 3 & 2 \\ 5 & 3 \end{pmatrix}$.

Nejprve spočítáme $\det(A) = -1$, takže už víme, že by inverzní matice měla existovat.

Teď sestavíme matici D: d_{11} dostaneme vyškrtnutím prvního řádku a sloupce z A a nalezením determinantu výsledné matice $(\,3\,)$, výsledek je $d_{11} = (-1)^{1+1} \cdot 3 = 3$, podobně je $d_{12} = (-1)^{1+2} \cdot 5 = -5$, $d_{21} = (-1)^{2+1} \cdot 2 = -2$, $d_{22} = (-1)^{2+2} \cdot 3 = 3$. Proto $D = \begin{pmatrix} 3 & -5 \\ -2 & 3 \end{pmatrix}$ a tedy

$$A^{-1} = (-1)^{-1} \begin{pmatrix} 3 & -5 \\ -2 & 3 \end{pmatrix}^T = \begin{pmatrix} -3 & 2 \\ 5 & -3 \end{pmatrix}.$$

Ověřte, že opravdu $\begin{pmatrix} 3 & 2 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} -3 & 2 \\ 5 & -3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

△

Čtenáře možná napadne, proč jsme nepoužili mnohem efektivnější metodu, jmenovitě Gaussovu eliminaci. Důvodem je, že to s ní není tak jednoduché, jak jsme zvyklí z reálných čísel. Konkrétně, v oboru reálných čísel bychom matici $(A|E_2)$ upravili na tvar $(E_2|A^{-1})$, což obvykle vyžaduje dělení řádků vhodnými čísly. To je ovšem v oboru celých čísel značný problém.

Protože je to téma, které se ukáže jako důležité, podíváme se na úpravy matic podrobněji. Nejprve si zopakujeme základní fakta o klasické Gaussově eliminační metodě (GEM). Pro zjednodušení nebudeme dále vypisovat, že se u $n \times m$ matice automaticky berou řádkové indexy i, j z rozmezí $1, \ldots, n$ a sloupcový index k se bere z rozmezí $1, \ldots, m$.

Jejím cílem je upravit danou matici na příjemnější tvar. Cílová podoba se liší podle aplikace. Někdy se chceme dostat k jednotkové matici, někdy nám stačí dolní trojúhelníkový tvar, obecně se každá matice dá převést na řádkově redukovaný tvar. Intuitivně řečeno, taková matice má levý dolní roh vyplněný nulami tuto oblast čarou oddělíme, dostaneme schodiště.

$$\left(\begin{array}{ccccc} 13 & 0 & 2 & 14 & -1 \\ \hline 0 & 0 & 23 & 7 & 0 \\ 0 & 0 & 0 & -6 & 13 \\ \hline 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Formální definice to vyjadřuje trochu komplikovaně, ale dá se to rozluštit.

Definice 2d.2.
Řekneme, že matice A je v řádkově redukovaném tvaru, jestliže pro každý řádek i a číslo N platí, že pokud $a_{ik} = 0$ pro $k < N$, pak musí platit $a_{jk} = 0$ pro všechna $j > i$ a $k \leq N$.

Tento tvar matice je ideální pro rychlé řešení soustav lineárních rovnic či počítání determinantu. Gaussova eliminace dokáže každou matici převést na tento tvar. Provádí řádkové operace, tedy operace provádíme s celými řádky, což v praxi znamená, že zvolený vzorec se simultánně použije ve všech sloupcích zároveň.

Proces je rozdělen do etap. V každé etapě se soustředíme na jeden konkrétní sloupec a pomocí řádkových operací se jej snažíme dostat do tvaru, kdy je nahoře číslo a pod ním nuly. Pokaždé, když se to povede, popojdeme o sloupec doprava a zároveň ignorujeme ty řádky nahoře, které už jsou v žádaném tvaru.

Existuje specializovaná verze (Gauss-Jordanova metoda), která se ve sloupci i snaží dosáhnout situace, kdy je v řádku i jednička a nad ní a pod ní nuly. Toto už není možné vždy, jen u invertibilních matic, a používáme to někdy k výpočtu inverzní matice, zejména na střední škole. Při praktických výpočtech s většími maticemi je ale rychlejší odvodit inverzní matici z řádkově redukovaného tvaru, takže vlastně tuto speciální verzi nepotřebujeme.

Povolené řádkové operace jsou tři:

- Přičtení násobku jednoho řádku k jinému;
- prohození dvou řádků;
- vynásobení řádku nenulovým číslem.

Rovnou poznamenejme, že třetí operaci potřebujeme jen u té specializované Gauss-Jordanovy verze, takže se bez ní dokážeme obejít.

Co je u těchto operací důležité? Účinek každé z nich lze pomocí těchto operací neutralizovat, tedy umíme matici zase vrátit do původního stavu. Například pokud aplikujeme prohození určitých dvou řádků, tak stejná operace zase matici vrátí, matici s řádkem vynásobeným číslem c vrátíme zpět vynásobením téhož řádku číslem c^{-1} (připomeňme, že dělení v teorii nepoužíváme). Mluvíme zde o operaci inverzní k jiné operaci. Pokud přičteme c-násobek řádku i k řádku j, tak inverzní operací je přičtení $(-c)$-násobku řádku i k řádku j.

Je zajímavé, že vlastně inverzní operace je vždy stejného typu jako původní, jen případně s jinou konstantou.

Další důležitá vlastnost základních tří řádkových operací je, že pokud daná matice reprezentuje soustavu lineárních rovnic, tak po provedení řádkových úprav má nově vzniklá soustava stejnou množinu řešení (jde o ekvivalentní úpravy). O těchto operacích také víme, jaký mají vliv na determinant výsledné matice, takže lze pomocí Gaussovy eliminace snadno spočítat determinant větších matic. Jmenovitě, přičtením násobku řádku k jinému se determinant nemění a prohozením znaménka se změní jeho znaménko. Pokud tedy zůstaneme u těchto operací (což máme v plánu), tak se absolutní hodnota determinantu nebude při těchto operacích měnit. Pro úplnost dodáme, že pokud vynásobíme řádek matice číslem c, tak se tím vynásobí i determinant.

Nás teď zajímá, co se s těmito postupy stane v situaci, kdy žijeme ve světě celých čísel.

2d.3 Řádkové úpravy matic nad celými čísly

Mějme tedy matici s celočíselnými prvky a zamysleme se na třemi řádkovými operacemi.

První typ řádkové operace, přičtení c-násobku řádku k jinému, kde teď c je celé číslo, je zcela v pořádku, protože zase vytvoří matici nad celými čísly a inverzní operace, tedy přičtení $(-c)$-násobku, je zase operace přístupná ve světě celých čísel, $-c \in \mathbb{Z}$. Je to vidět i z toho, že transformační matice takové operace je zase matice nad celými čísly.

Druhá operace, prohození řádků, je sama sobě inverzí a opět jde o operaci produkující celočíselnou matici, i její transformační matice je celočíselná. Tyto dvě operace tedy lze přenést do světa celých čísel.

Jak se dá čekat, problém je s operací třetí. Chceme-li vynásobit řádek matice číslem $c \in \mathbb{Z}$, pak potřebujeme, aby i inverzní operace byla proveditelná ve světě celých čísel, jinak řečeno, číslo c^{-1} by mělo být celé. To je ovšem možné jen tehdy, když $|c| = 1$.

Dostáváme tedy následující seznam řádkových operací, které jsou povoleny ve světě celých čísel.

Celočíselné řádkové operace:

- Přičtení c-násobku jednoho řádku k jinému, kde $c \in \mathbb{Z}$;
- prohození dvou řádků.
- vynásobení řádku číslem 1 či -1;

Jak už jsme poznamenali, pro Gaussovu eliminaci tu třetí operaci nepotřebujeme, ale přidali jsme ji pro úplnost. Občas se nám bude z estetických či praktických důvodů hodit, když po eliminaci v nějakém řádku změníme znaménka.

Název „celočíselné řádkové operace“ je neoficiální, ale výstižný. Odborně se jim říká „unimodulární řádkové operace“ (ale jak už jsme psali, této teorii se zde věnovat nebudeme). Souvislost s unimodulárními maticemi je přímá, tyto operace je totiž zachovávají. Snadno nahlédneme, že nemění absolutní hodnotu determinantu, jediná možná změna je v jeho znaménku. To znamená, že když začneme s maticí, která nad celými čísly je či není invertibilní, tak se tato její vlastnost celočíselnmi řádkovými úpravami nemění.

Omezení našich možností má evidentně významný dopad na GEM. Pokud bychom například chtěli redukovat matici $A = \begin{pmatrix} 3 & 2 \\ 5 & 3 \end{pmatrix}$, pak bychom ve světě reálných čísel odečetli $c = \frac{5}{3}$-násobek prvního řádku od druhého. Ve světě celých čísel je nám ovšem tato možnost odepřena.

To nezní moc povzbudivě, je tu ale jedna zajímavá možnost. Odečteme první řádek od druhého, a pak nový druhý od prvního.

$$\begin{pmatrix} 3 & 2 \\ 5 & 3 \end{pmatrix} \sim \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}.$$

Máme v prvním řádku jedničkový pivot a hravě dokončíme redukci prvního sloupce matice do potřebného tvaru odečtením dvojnásobku prvního řádku od druhého.

$$\begin{pmatrix} 3 & 2 \\ 5 & 3 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Je vidět, že bychom tuto matici dokázali převést celočíselnými řádkovými úpravami dokonce na jednotkovou matici, což otevírá cestu oblíbenému algoritmu pro nalezení inverzní matice:

$$\left(\begin{array}{cc|cc} 3 & 2 & 1 & 0 \\ 5 & 3 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 3 & 2 & 1 & 0 \\ 2 & 1 & -1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 1 & 2 & -1 \\ 2 & 1 & -1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 1 & 2 & -1 \\ 0 & -1 & -5 & 3 \end{array}\right)$$
$$\sim \left(\begin{array}{cc|cc} 1 & 0 & -3 & 2 \\ 0 & -1 & -5 & 3 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & -3 & 2 \\ 0 & 1 & 5 & -3 \end{array}\right).$$

Dostali jsme správnou inverzní matici. To je ovšem příliš ambiciózní cíl, zastavme se u momentu, kdy se nám povedlo v prvním sloupci vytvořit nulu pod jedničkou. Úprava vybraného sloupce do žádaného tvaru (nenulové číslo nahoře a pod ním nuly) je srdcem Gaussovy eliminace a postup naznačený výše jej dokáže realizovat i v celočíselném oboru.

S Algoritmus 2d.4.

Pro převedení matice, jejíž sloupec k je roven $\begin{matrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{matrix}$ pro $a_i \in \mathbb{Z}$, pomocí celočíselných řádkových operací na tvar, kdy je sloupec k roven $\begin{matrix} d \\ 0 \\ \vdots \\ 0 \end{matrix}$ pro nějaké $d \in \mathbb{Z}$.

1. Pokud je ve sloupci k nejvýše jedno nenulové číslo, případným prohozením řádků jej přemístěte do prvního řádku.
Algoritmus skončil.
2. Nechť se nejmenší nenulové číslo sloupce k nachází v řádku i, označme jej d (říkáme mu „pivot“). Odečtěte vhodné násobky řádku i od ostatních řádků tak, aby ve sloupci k vznikla v řádcích jiných než i čísla, jejichž absolutní hodnota je menší než $|d|$.
Vraťte se na krok **1**.
△

Je tento algoritmus korektní? Máme-li v řádku i pivot d a v jiném řádku j a ve stejném sloupci číslo a, tak vždy dokážeme podle věty o dělení najít rozklad $a = qd + r$, kde $0 \leq r < |d|$. Odečteme-li q-násobek řádku i od řádku j, vznikne v příslušném sloupci číslo $r = a - qd$, tedy číslo splňující $|r| < |d|$. Vidíme, že druhý krok algoritmu lze vždy provést.

Opakováním kroku 2 vznikají pivoty d_1, d_2, d_3, které splňují $|d_1| > |d_2| > |d_3| > \cdots$. Kdyby algoritmus nikdy neskončil, vznikla by nekonečná klesající posloupnost nezáporných celých čísel, což je nemožné. Algoritmus tedy nutně musí dříve či později skončit.

Čtenáři to jistě připomíná postup při Euklidově algoritmu, k čemuž se samozřejmě brzy dostaneme. Zatím se jen inspirujeme a poznamenáme, že nám i při celočíselné Gaussově eliminaci nic nebrání hledat záporné zbytky po dělení. To znamená, že v kroku 2 lze vyžadovat, aby ve sloupci k vznikla v řádcích jiných než i čísla, jejichž absolutní hodnota je nejvýše $\frac{1}{2}|d|$. Proces se tak v průměru urychlí a stejně jako u Euklidova algoritmu odvodíme, že na převedení sloupce na konečný tvar stačí nejvýše $\log_2(|d_1|)$ kroků 2.

Tady se to ovšem zkomplikuje, protože jeden krok zahrnuje manipulaci s více řádky v matici, takže při výšce sloupce n můžeme očekávat, že jeho zpracování zabere řádově $n \log_2(|d_1|)$ řádkových operací. Při každé pracujeme s m sloupci, takže celkové úsilí na zpracování jednoho sloupce je řádově úměrné číslu $mn \log_2(|d_1|)$. Navíc je známo, že při celočíselných operacích mají prvky matice tendenci ke zvětšování, což je další výpočetní komplikace. Provozovat tento algoritmus s většími maticemi se tedy může protáhnout.

Jakmile máme potvrzenu platnost algoritmu 2d.4, již nám nic nebrání aplikovat jej postupně na jednotlivé

sloupce (přičemž se postupně omezujeme na spodní řádky matice) tak, jak to dělá Gaussova eliminační metoda. Dostáváme tak následující dobrou zprávu.

Fakt 2d.5.
Každou matici nad celými čísly lze pomocí celočíselných řádkových operací převést na celočíselnou matici v řádkově redukovaném tvaru.

Vraťme se k problematice invertibilních matic. Matice v řádkově redukovaném tvaru je také horní trojúhelníková, její determinant je tedy dán součinem diagonálních prvků. Rozeberme možné situace.

První je, že se nám v redukované matici na diagonále objeví i jiná (celá!) čísla než ± 1. Pak už její determinant nemůže být ± 1. Protože celočíselné řádkové operace nemění velikost determinantu (mohou měnit jedině jeho znaménko), musela mít i původní matice determinant jiný než ± 1 a tedy nebyla invertibilní. Proto nás ani nemrzí, že bychom ji neuměli celočíselnou eliminací převést na jednotkový tvar, stejně by to k ničemu nebylo.

Druhá možnost je, že na diagonále redukované matice vidíme jen čísla ± 1. Pak stejnou úvahou dojdeme k závěru, že původní matice byla invertibilní. Teď ale máme na diagonále čísla ± 1 a změna znaménka řádků je tedy povolena, tudíž snadno upravíme matici tak, aby byly na diagonále jedničky, a poté celočíselnými úpravami vyrobíme nuly i nad nimi. Jinak řečeno, pokud je daná matice invertibilní, tak ji celočíselná GEM umí převést na jednotkovou.

Máme tedy potvrzeno, že i ve světě celých čísel nám postup $(A|E_n) \mapsto (E_n|A^{-1})$ (nebo pokus o něj) spolehlivě rozezná ivnertibilní matice od ostatních a pro ty invertibilní poskytuje inverzní matice.

2d.6 Řádková eliminace a Euklidův algoritmus

Pokud čtenáře při přemýšlení nad algoritmem 2d.4 napadlo, že se práce se sloupcem nápadně podobá Euklidovu algoritmu, tak to byl správný pocit. Nejlépe to ukáže příklad, aplikujeme jej na čísla 108 a 60 a rovnou zkusíme rozšířenou verzi k nalezení Bezoutovy identity.

a, b	A	B
108	1	0
60	0	1
48	1	-1
$12\bullet$	$-1\bullet$	$2\bullet$
0	5	-9

Vždy jsme pracovali jen se dvěma řádky, takže jsme vlastně dělali toto:

$$\left(\begin{array}{c|cc} 108 & 1 & 0 \\ 60 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 48 & 1 & -1 \\ 60 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 48 & 1 & -1 \\ 12 & -1 & 2 \end{array}\right) \sim \left(\begin{array}{c|cc} 0 & 5 & -9 \\ 12 & -1 & 2 \end{array}\right)$$

U Euklidova algoritmu jsme následovali obvyklý postup, tedy hledali jsme nezáporné zbytky, ale při práci s maticemi už toto omezení obvykle nevnímáme ani pocitově, prostě vyrábíme nejmenší možná čísla. Verze se zápornými zbytky je tedy přirozená.

Spolehlivost tohoto postupu se odvíjí od dvou faktů. Za prvé, největší společný dělitel čísel v prvním sloupci zůstává stejný. Protože čísla v prvním sloupci vznikají přes zbytky, stačí se zde odvolat na lemma 2b.12.

Druhý fakt je, že v každé matici a v každém jejím řádku je zakódovaná lineární kombinace, která je stále platná. I toto se dá snadno dokázat obdobně jako v důkazu, že funguje rozšířený Euklidův algoritmus.

Zápis maticí je samozřejmě delší než tabulkový, ale umožňuje přirozené zobecnění na více čísel.

Definice.
Uvažujme čísla $a_1, \dots, a_n \in \mathbb{Z}$ taková, že alespoň jedno z nich je nenulové. Definujeme jejich **největší společný dělitel**, značeno $\gcd(a_1, \dots, a_n)$, jako největší prvek množiny jejich společných nezáporných dělitelů.

Význam je intuitivně jasný, takže by neměly překvapit např9klad tyto vlastnosti.

Fakt 2d.7.
Pro všechna čísla $a_1, \dots, a_n \in \mathbb{Z}$ platí následující:
(i) $\gcd(a_1, a_2, \cdots, a_n) = \gcd(b_1, b_2, \cdots, b_n)$ pro libovolnou permutaci $b_1, \dots, b_n$ čísel $a_1, \dots, a_n$;
(ii) $\gcd(a_1, a_2, \cdots, a_n) = \gcd(-a_1, a_2, \cdots, a_n)$;

Důkaz: (i): Protože to, zda číslo d je či není společným dělitelem množiny čísel, nezáleží na jejich pořadí, bude množina společných dělitelů čísel $a_1, \dots, a_n$ stejná jako množina společných dělitelů čísel $b_1, \dots, b_n$. Pak se musí rovnat i největší prvky těchto shodných množin.

(ii): Množina dělitelů čísla $-a_1$ je stejná jako množina dělitelů čísla a_1. Dále se postupuje obdobně jako u (i). □

Jinak řečeno, i u obecné verze nezáleží na pořadí a znaménkách čísel.

Trochu jsme se na tento pojem podívali ve cvičení 2b.9 a mimo jiné se ukázalo, že je možné takovýto hromadný největší společný dělitel počítat kaskádovitě po dvojicích, tedy nejprve by se spočítal $d_1 = \gcd(a_1, a_2)$, pak $d_2 = \gcd(d_1, a_3)$ atd., až nakonec $d = \gcd(d_{n-2}, a_n)$. Teoreticky bychom tedy nemuseli nic nového vymýšlet, ale moc praktický přístup to není. Raději se zamyslíme, jak adaptovat Euklidův algoritmus, a rovnou jeho rozšířenou verzi.

Mějme čísla $a_1, \dots, a_n \in \mathbb{Z}$. Sestavíme z nich první sloupec matice, zbytek doplníme jednotkovou maticí. V této matici nás zajímá gcd prvního sloupce. Stejně důležité je rozmyslet si, že každý řádek přidané matice kóduje lineární kombinaci vstupních dat, která dává číslo nalevo. Například v prvním řádku vidíme $a_1 = 1 \cdot a_1 + 0 \cdot a_2 + \dots + \cdot a_n$, což jistě platí.

$$\left(\begin{array}{c|cccc} a_1 & 1 & 0 & \dots & 0 \\ a_2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & 0 & \dots & 1 \end{array}\right)$$

Nyní máme v plánu na tuto matici aplikovat řádkové operace, přičemž nechceme ztratit informace. Zobecníme si klíčové lemma. Protože už víme, že na pořadí čísel v gcd nezáleží, stačí dokázat, že můžeme pomocí prvního řádku beztrestně modifikovat druhý, a bude to platit i pro ostatní řádky.

Lemma 2d.8.
Pro všechna čísla $a_1, \dots, a_n, q \in \mathbb{Z}$ platí následující:

$$\gcd(a_1, a_2, \cdots, a_n) = \gcd(a_1, a_2 - qa_1, \cdots, a_n).$$

Důkaz: Jestliže číslo d dělí $a_1, \dots, a_n$, pak tedy dělí a_1, a_2 a podle důsledku 2a.3 také d dělí $a_2 - qa_1$, proto je d společným dělitelem čísel $a_1, a_2 - qa_1, a_3, \dots, a_n$.

Naopak pokud je číslo d dělitelem čísel a_1 a $a_2 - qa_1$, pak je dělitelem čísla $a_2 = (a_2 - qa_1) + qa_1$, tedy společný dělitel čísel $a_1, a_2 - qa_1, a_3, \dots, a_n$ musí být i společným dělitelem čísel $a_1, a_2, a_3, \dots, a_n$.

Potože mají obě množiny čísel stejné dělitele, musejí mít i stejného největšího dělitele. □

Teď tedy víme, že když daná čísla seskupíme do sloupce a provádíme řádkové operace, bude výsledné gcd stejné. Pokud tyto operace provádíme dle algoritmu 2d.4, vznikne sloupec s čísly $d, 0, \dots, 0$, jejichž největší společný dělitel je d. Právě jsme ukázali, že jsme schopni zobecnit základní Euklidův algoritmus pro hledání gcd na více čísel.

Příklad 2d.b: Najdeme $\gcd(204, 168, 144, 84)$. Čísla sestavíme do sloupce. Dle algoritmu máme vybrat nejmenší, to je 84. Vhodným odečtením od předchozích čísel je zmenšíme. Zde předvedeme klasickou podobu Euklidova algoritmu, tedy použijeme nezáporné zbytky.

Dostáváme sloupec, který vidíme napravo. Opět vybereme nejmenší číslo a použijeme jej ke zmenšení ostatních. Takto pokračujeme a dostaneme následující kroky, na závěr uděláme úpravu, kterou bychom museli dělat v rámci Gaussovy eliminace, ale zde nemusíme.

$$\begin{pmatrix} 36 \\ 0 \\ 60 \\ 84 \end{pmatrix}$$

$$\begin{pmatrix} 204 \\ 168 \\ 144 \\ 84 \end{pmatrix} \sim \begin{pmatrix} 36 \\ 0 \\ 60 \\ 84 \end{pmatrix} \sim \begin{pmatrix} 36 \\ 0 \\ 24 \\ 12 \end{pmatrix} \sim \begin{pmatrix} 0 \\ 0 \\ 0 \\ 12 \end{pmatrix} \sim \begin{pmatrix} 12 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Zjistili jsme, že $\gcd(204, 168, 144, 84) = 12$. Kupodivu to není třináct.
△

Protože můžeme u řádků v matici měnit znaménka (násobení číslem -1) lze i při obecném vstupu a používání záporných zbytků zařídit, aby ono zbývající číslo d bylo kladné a tedy rovnou dávalo největší společný dělitel.

Abychom ověřili, že rozšířený algoritmus najde Bezoutovu identitu, ukážeme následující tvrzení:

• Mějme matici $\left(\begin{array}{c|ccc} d_1 & A_{1,1} & \dots & A_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ d_n & A_{n,1} & \dots & A_{n,n} \end{array}\right)$. Předpokládejme, že v každém řádku i platí pro jistá čísla $a_1, \dots, a_n$ rovnost $d_i = \sum_{k=1}^{n} A_{i,k} a_k$. Pokud v matici přičteme q-násobek řádku i k řádku j, pak nový řádek bude opět splňovat dotyčnou rovnost pro stejná čísla a_k.

Nový řádek je dán vzorci $d_j^* = d_j + qd_i$, $A_{j,k}^* = A_{j,k} + qA_{i,k}$. Pak pro něj platí

$$d_j^* = d_j + qd_i = \sum_{k=1}^{n} A_{j,k}a_k - q\sum_{k=1}^{n} A_{i,k}a_k = \sum_{k=1}^{n}\Big(A_{j,k}a_k - qA_{i,k}a_k\Big)$$
$$= \sum_{k=1}^{n}(A_{j,k} - qA_{i,k})a_k = \sum_{k=1}^{n} A_{j,k}^* a_k.$$

Již jsme viděli, že první sloupec bude po eliminaci obsahovat skoro samé nuly s výjimkou jednoho čísla d, přičemž lze mít $d > 0$. Víme, že pak d je gcd čísel a_k. Odpovídající řádek ve tvaru $(d\ A_1\ \dots\ A_n)$ pak podle nejnovějšího poznatku dává $\gcd(a_1, \dots, a_n) = d = \sum_{k=1}^{n} A_k a_k$ neboli Bezoutovu identitu.

Pokud bychom tento argument uděali se všemi detaily, byl by to vlastně důkaz následujícího tvrzení.

Věta 2d.9.
Uvažujme čísla $a_1, a_2, \dots, a_n \in \mathbb{Z}$, z nichž alespoň jedno je nenulové.
Algoritmus 2d.4 aplikovaný na matici

$$\begin{pmatrix} a_1 & 1 & 0 & 0 & \dots & 0 \\ a_2 & 0 & 1 & 0 & \dots & 0 \\ a_3 & 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \ddots & \vdots \\ a_n & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

dokáže vytvořit matici

$$\begin{pmatrix} d & A_1 & A_2 & A_3 & \dots & A_n \\ 0 & \vdots & \vdots & \vdots & & \vdots \\ \vdots & & & & & \\ 0 & & & & & \end{pmatrix},$$

kde $d > 0$.
Pak platí $\gcd(a_1, \dots, a_n) = d = A_1a_1 + \dots + A_na_n$.

Tímto způsobem by šlo také dokázat zobecnění Bezoutovy věty.

Věta 2d.10.
Nechť $a_1, \dots, a_n \in \mathbb{Z}$.
Pak existují celá čísla $A_1, \dots, A_n$ taková, že $\gcd(a_1, \dots, a_n) = \sum_{k=1}^{n} A_k a_k$.

Opět platí, že pokud je alespoň jedno z čísel $a_1, \dots, a_n$ nenulové, tak je $\gcd(a_1, \dots, a_n)$ nejmenší kladná celočíselná lineární kombinace čísel $a_1, \dots, a_n$.

Příklad 2d.c: Vrátíme se ke $\gcd(204, 168, 144, 84)$. Aplikujeme maticovou verzi rozšířeného Euklidova algoritmu pro více čísel.

$$\left(\begin{array}{c|cccc} 204 & 1 & 0 & 0 & 0 \\ 168 & 0 & 1 & 0 & 0 \\ 144 & 0 & 0 & 1 & 0 \\ 84 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cccc} 36 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & -2 \\ 60 & 0 & 0 & 1 & -1 \\ 84 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cccc} 36 & 1 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & -2 \\ 24 & -1 & 0 & 1 & 1 \\ 12 & -2 & 0 & 0 & 5 \end{array}\right)$$
$$\sim \left(\begin{array}{c|cccc} 0 & 7 & 0 & 0 & -17 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 3 & 0 & 1 & -9 \\ 12 & -2 & 0 & 0 & 5 \end{array}\right) \sim \left(\begin{array}{c|cccc} 12 & -2 & 0 & 0 & 5 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 3 & 0 & 1 & -9 \\ 0 & 7 & 0 & 0 & -17 \end{array}\right).$$

Poslední úprava byla estetická, ale pokud bychom chtěli pokračovat s dalšími sloupci v rámci Gaussovy eliminace, pak by byla potřebná. Nás zde ale poslední tři řádky nezajímají, z prvního přečteme

$$\gcd(204, 168, 144, 84) = 12 = (-2) \cdot 204 + 0 \cdot 168 + 0 \cdot 144 + 5 \cdot 84,$$

což snadno ověříme.
△

Ony řádky začínající nulou jsme nemuseli dopočítávat. Existuje zajímavá souvislost mezi tímto postupem a řešením soustav diofantických rovnic, kdy bude potřeba i informace z těchto řádků, viz část 4e.

Příklad 2d.d: Pro zajímavost zkusíme ještě $\gcd(713, 506, -897)$, tentokráte pomocí záporných zbytků.

$$\left(\begin{array}{c|ccc} 713 & 1 & 0 & 0 \\ 506 & 0 & 1 & 0 \\ -897 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} 207 & 1 & -1 & 0 \\ 506 & 0 & 1 & 0 \\ 115 & 0 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} -23 & 1 & -5 & -2 \\ 46 & 0 & -7 & -4 \\ 115 & 0 & 2 & 1 \end{array}\right)$$
$$\sim \left(\begin{array}{c|ccc} -23 & 1 & -5 & -2 \\ 0 & 2 & -17 & -8 \\ 0 & 5 & -23 & -9 \end{array}\right) \sim \left(\begin{array}{c|ccc} 23 & -1 & 5 & 2 \\ 0 & 2 & -17 & -8 \\ 0 & 5 & -23 & -9 \end{array}\right).$$

Dostali jsme $\gcd(713, 506, -897) = 23 = (-1) \cdot 713 + 5 \cdot 506 + 2 \cdot (-897)$.

△

Máme tedy funkční algoritmus. Přidáme ještě dvě poznámky.

2d.11 Poznámka: Opisování matic je docela solidní opruz. Nešlo by to dělat nějakou nápodobou tabulkového zápisu? Šlo. Proč jsme to tedy neprobrali? Protože tohle ručně nikdo nedělá, toto téma je spíš důležité teoreticky a tam se ten maticový přístup hodí. Ale pokud jste zvědavi na tabulkovou verzi, ukážeme si to na příkladě $\gcd(204, 168, 144, 84)$.

Zadaná čísla sepíšeme pod sebe do tabulky, je dobré dát nejmenší z čísel (v absolutní hodnotě) do posledního řádku. Pokud hledáme i Bezoutovo vyjádření, přilepíme napravo pomocné sloupce.

204	1	0	0	0
168	0	1	0	0
144	0	0	1	0
84	0	0	0	1

Pak opakujeme následující kroky.

1. Zkusmo se podíváme, jaké zbytky (klidně i nezáporné) lze vyrobit ze zatím nevyškrtnutých čísel ve sloupci (kromě posledního) dělením tím posledním (nejmenším). Zapamatujeme si, ze kterého čísla a jsme ten nejmenší zbytek dostali.

Pokud nám při tom zkusmém dělení u některého čísla vyšel zbytek nula, rovnou jej škrtneme.

2. Dolů do sloupce přidáme řádek s tím nejmenším získaným zbytkem. Jeho zdrojové číslo a v tabulce škrtneme.

Takto pokračujeme, dokud dokážeme vyrábět nové nenulové číslo. V našem příkladě v první etapě rovnou škrtneme 168 a použijeme číslo 204 (které pak také škrtneme) k získání nového řádku. V druhé etapě pomocí 84 získáme 12. Zde je celý průběh.

204	1	0	0	0
168	0	1	0	0
144	0	0	1	0
84	0	0	0	1

$\Longrightarrow$

~~204~~	1	0	0	0
~~168~~	0	1	0	0
144	0	0	1	0
84	0	0	0	1
36	1	0	0	−2

$\Longrightarrow$

~~204~~	1	0	0	0
~~168~~	0	1	0	0
~~144~~	0	0	1	0
~~84~~	0	0	0	1
36	1	0	0	−2
12	−2	0	0	5

$\Longrightarrow$

~~204~~	1	0	0	0
~~168~~	0	1	0	0
~~144~~	0	0	1	0
~~84~~	0	0	0	1
~~36~~	1	0	0	−2
12	−2	0	0	5

Dostali jsme $\gcd(204, 168, 144, 84) = 12 = (-2) \cdot 204 + 0 \cdot 168 + 0 \cdot 144 + 5 \cdot 84$.

Vidíme, že jsme nejen nemuseli opisovat matice, ale navíc tento postup poznal, že některé kombinace nebudou nakonec potřebné, tak jsme je nemuseli přepočítávat, nakonec jsme dělali jen dvě. Takže docela účinné, ale asi to nevyužijeme.

△

2d.12 Poznámka: Existuje zcela odlišný pohled na to, proč eliminace dokáže najít Bezoutovu identitu.

Jsou dány čísla $a_1, \ldots, a_n$ a my vytvoříme povědomou matici:

$$\left(\begin{array}{c|ccc} a_1 & 1 & 0 & \ldots & 0 \\ a_2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & 0 & \ldots & 1 \end{array}\right)$$

Pokud bychom si ten levý sloupec představili přilepený napravo, hned poznáme rozšířenou matici soustavy lineárních rovnic, jmenovitě této:

$$\begin{aligned} 1 \cdot x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_n &= a_1 \\ 0 \cdot x_1 + 1 \cdot x_2 + \cdots + 0 \cdot x_n &= a_2 \\ &\vdots \\ 0 \cdot x_1 + 0 \cdot x_2 + \cdots + 1 \cdot x_n &= a_n \end{aligned}$$

Je vcelku jasné, že tato soustava má jediné řešení, jmenovitě $x_i = a_i$.

Pomocí algoritmu 2d.4 matici převedeme na tvar

$$\begin{pmatrix} d & A_1 & A_2 & \dots & A_n \\ 0 & \vdots & \vdots & & \vdots \\ \vdots & & & & \\ 0 & & & & \end{pmatrix}.$$

Tato matice kóduje novou soustavu rovnic, nás zajímá ta první:

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = d.$$

Protože šlo o ekvivalentní úpravy, tato nová soustava musí mít stejné řešení $x_i = a_i$, tedy platí

$$A_1a_1 + A_2a_2 + \cdots + A_na_n = d$$

a máme Bezoutovu identitu. Tento argument neumí dokázat, že toto d je nejmenší možné neboli že d je to gcd, na to přeci jen potřebujeme poznatky o dělitelnosti.

△

Cvičení

Cvičení 2d.1 (rutinní)**:** Pro následující trojice $a, b, c \in \mathbb{Z}$ najděte $\gcd(a, b, c)$ a příslušnou Bezoutovu identitu.
(i) $a = 364, b = -234, c = 156$; (ii) $a = -759, b = 598, c = 437$.

Řešení:
2d.1: (i)

$$\left(\begin{array}{c|ccc} 364 & 1 & 0 & 0 \\ -234 & 0 & 1 & 0 \\ 156 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} 52 & 1 & 0 & -2 \\ -78 & 0 & 1 & 1 \\ 156 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} 52 & 1 & 0 & -2 \\ -26 & 1 & 1 & -1 \\ 0 & -3 & 0 & 7 \end{array}\right) \sim \left(\begin{array}{c|ccc} 0 & 3 & 2 & -4 \\ -26 & 1 & 1 & -1 \\ 0 & -3 & 0 & 7 \end{array}\right).$$

$\gcd(364, -234, 156) = 26 = (-1) \cdot 364 + (-1) \cdot (-234) + 1 \cdot 156.$
(ii)

$$\left(\begin{array}{c|ccc} -759 & 1 & 0 & 0 \\ 598 & 0 & 1 & 0 \\ 437 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} 115 & 1 & 0 & 2 \\ 161 & 0 & 1 & -1 \\ 437 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} 115 & 1 & 0 & 2 \\ 46 & -1 & 1 & -3 \\ -23 & -4 & 0 & -7 \end{array}\right) \sim \left(\begin{array}{c|ccc} 0 & -19 & 0 & -33 \\ 0 & -9 & 1 & -17 \\ -23 & -4 & 0 & -7 \end{array}\right).$$

$\gcd(-759, 598, 437) = 23 = 4 \cdot (-759) + 0 \cdot 598 + (-7) \cdot 437.$

2e. Polynomy nad celými čísly

Jedním z důležitých pojmů je polynom. V této doplňkové kapitole si jen pootevřeme některá témata, aby měl čtenář představu, co se dá dělat.

Polynomy nad $\mathbb{R}$ jsou výrazy typu $a_nx^n + \cdots + a_1x + a_0$, jejichž koeficienty a_i jsou z $\mathbb{R}$, třeba $p = \sqrt{2}\,x^5 - \pi x + e$. Množina všech takovýchto polynomů se značí $\mathbb{R}[x]$. Pro polynomy máme pravidla pro sčítání a násobení číslem (třeba umíme spočítat $3p$ pro ten polynom výše) i pro násobení polynomů mezi sebou, například pro $p = x + 1$ a $q = x - 1$ dostáváme $p \cdot q = x^2 - 1$.

Abychom se vyhnuli technickým problémům, uděláme rovnou dohodu, že členy a_ix_i s nulovým koeficientem se nemusí psát a neuvažují se při posuzování rovnosti polynomů, takže například polynomy $0 \cdot x^{13} - 6x^2 + 1$ a $-6x^2 + 0x + 1$ považujeme za stejný polynom.

Každý polynom zároveň dává vzniknout funkci, tedy zobrazení $x \mapsto p(x)$. Čistě formálně jde o dvě různé věci, polynom a funkce z něj vznikající, ale zrovna u polynomů nad $\mathbb{R}$ se to nějak neřeší, protože polynomy a z nich vznikající funkce jsou úzce svázány. Konkrétně, jedna ze základních vlastností polynomů nad reálnými čísly je, že formální polynomy (tedy výrazy typu $a_nx^n + \cdots + a_0$) a funkce jimi definované si jednoznačně odpovídají: Pokud se dva polynomy rovnají svými hodnotami, pak musí mít i stejné koeficienty, tedy jde o stejný polynom. To je užitečné v mnoha aplikacích, například pokud víme, že pro jisté parametry a, b, c platí rovnice $ax^2 + bx + c = x^2 + 13x + 14$ pro všechna $x \in \mathbb{R}$, pak nutně musí být $a = 1$, $b = 13$ a $c = 14$.

U polynomů $a_nx^n + \cdots + a_0$ umíme obecně zadefinovat stupeň polynomu jako největší koeficient i takový, že $a_i \neq 0$, a pro polynomy reálné se stupeň chová velice rozumně. Reálné polynomy dokonce umíme i navzájem dělit se zbytkem a zbytek po dělení i částečný podíl jsou jednoznačné (viz Věta o dělení pro čísla 2a.7). Při vzájemném poměřování kandidátů na zbytek se namísto velikosti používá stupeň. Shrneme si to základní ve větě.

Věta 2e.1.
Uvažujme polynomy p, q nad $\mathbb{R}$. Pak platí následující:
(i) $\mathrm{st}(pq) = \mathrm{st}(p) + \mathrm{st}(q)$.
(ii) Existují jediné polynomy d a r takové, že $p = d \cdot q + r$ a $\mathrm{st}(r) < \mathrm{st}(q)$.
(iii) Polynom p má nejvýše $\mathrm{st}(p)$ kořenů v $\mathbb{R}$.
(iv) $a \in \mathbb{R}$ je kořenem p právě tehdy, když polynom $x - a$ dělí p.

Pro polynomy můžeme definovat i dělitelnost naprosto stejným způsobem jako pro celá čísla, tedy $q \,|\, p$ pokud existuje polynom r tak, aby $p = qr$. Například polynom $q = x - 1$ dělí polynom $p = x^2 - x$, protože $p = q \cdot r$ pro volbu $r = x$. U polynomů nad reálnými čísly se ale s tímto pojmem moc nepracuje.

Obdobně můžeme definovat $\mathbb{Z}[x]$ jako množinu všech polynomů $a_n x^n + \cdots + a_0$, jejichž koeficienty jsou ze $\mathbb{Z}$, kupodivu pak věci fungují úplně stejně. Zase si odpovídají polynomy jako výrazy s funkcemi, přesně řečeno koeficienty takového výrazu jsou jednoznačně určeny hodnotami z něj vzniklé funkce. To se občas velice hodí a my to využijeme v kapitole 12b v tzv. metodě neučitých koeficientů. Také bychom teď mohli opsat větu výše, jen se změnou $\mathbb{R}$ v $\mathbb{Z}$, a platila by, stejně jako je pro $\mathbb{Z}[x]$ pravdivá i poznámka za ní o dělitelnosti. U polynomů nad celými čísly už dělitelnost začíná být zajímavá a dá se do napodobit látka kapitoly o dělitelnosti.

Dá se například zavést pojem největšího společného dělitele a není těžké ukázat, že rozšířený Euklidův algoritmus (který využívá jen dělitelnost se zbytkem) funguje i pro polynomy, dá i jakousi obdobu Bezoutovy identity. U největšího společného dělitele je mimochodem zádrhel, na který nejsme zvyklí. Podívejme se na příklad.

Příklad 2e.a: Uvažujme polynomy $p = 4x^2 + 14x + 6$ a $q = 4x^2 - 2x - 2$. Máme rozklady

$$p = (4x + 2)(x + 3), \qquad q = (4x + 2)(x - 1),$$

takže $4x + 2$ je společný dělitel. Máme ovšem také

$$p = (2x + 1)(2x + 6), \qquad q = (2x + 1)(2x - 2),$$

takže i $2x + 1$ je společný dělitel. Žádný společný dělitel stupně dva či více není, takže „největší společný dělitel“ by se měl vybírat z dvojice $4x + 2$ a $2x + 1$. Namísto velikosti používáme stupeň, ale oba polynomy jsou stupně jedna, to si nepomůžeme. U polynomů tedy namísto jedné odpovědi získáme někdy celou množinu polynomů. Ve světě reálných čísel bychom jich dokonce získali nekonečně mnoho, libovolný polynom $2ax + a$ pro $a \neq 0$ dělí p i q.
△

Problém s nejednoznačností lze u reálných polynomů vyřešit tak, že si vybereme z oné nekonečné množiny kandidátů jeden speciální, nabízí se polynom, u kterého je koeficient u nejvyšší mocniny roven jedné. V našem příkladě by pak ve světě reálných čísel bylo $\gcd(4x^2 + 14x + 6, 4x^2 - 2x - 2) = x + \frac{1}{2}$. Příklad také ukazuje, že v $\mathbb{Z}$ už toto není možné. Protože toto je jen naťukávací kapitola, opustíme toto téma a zvědavého čtenáře odkážeme na knihy o maticích, kde se s polynomy nad celými čísly dělají zajímavé věci. Ale abychom jej jen tak neodbyli, ukážeme příklad.

Příklad 2e.b: Hledáme největší společný dělitel polynomů $p = 2x^5 - x^4 - 3x^3 - x + 2$ a $q = 2x^4 + x^3 - x^2 - 3x - 2$.
Ukážeme tabulku a pak vysvětlíme kroky.

a, b	A	B	
$2x^5 - x^4 - 3x^3 - x + 2$	1	0	
$2x^4 + x^3 - x^2 - 3x - 2$	0	1	$x - 1$
$2x^3 - x^2 - 2x$	1	$-(x - 1)$	$x + 1$
$2x^2 - x - 2\bullet$	$-(x - 1)\bullet$	$x^2\bullet$	x
0			

V prvním kroku „dlouhým dělením“ zjistíme, že se polynom q musí od polynomu p odečíst $(x-1)$ krát, abychom dostali zbytek r. Tolikrát tedy odečteme druhý řádek v tabulce od prvního.

Následně dělením zjistíme, že r je třeba od q odečíst $(x+1)$ krát. Vznikne další řádek tabulky. Protože $2x^2 - x - 2$ dělí r, je to i řádek klíčový.

Zjistili jsme, že

$$\begin{aligned}\gcd(2x^5 - x^4 - 3x^3 - x + 2, 2x^4 + x^3 - x^2 - 3x - 2) &= 2x^2 - x - 2 \\ &= -(x - 1) \cdot (2x^5 - x^4 - 3x^3 - x + 2) \\ &\quad + x^2 \cdot (2x^4 + x^3 - x^2 - 3x - 2).\end{aligned}$$

Je to masakr. Ale funguje to.
△