

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 a kapitolu 3 o počítání modulo.

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 $a|b$, 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 $a|b$, 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 $3|12$, protože $12 = 4 \cdot 3$, podmínka z definice je proto splněna s celým číslem $k = 4$.

Na druhou stranu neplatí $5|13$. 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.

△

Pro některá populární čísla a existují triky, jak snadno poznat, která čísla jsou tímto a dělitelná, čtenář jistě zná kritérium pro dělitelnost 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 $x^2 - 1 = (x - 1)(x + 1)$. To nás ale čeká až později, teď se podívejme, co se dá říct o dělitelnosti celých čísel. Některé věci jsou očividné.

Fakt 2a.1.

Pro každé $a \in \mathbb{Z}$ platí:

- (i) $1|a$;
- (ii) $a|a$;
- (iii) $a|0$.

Důkaz je tak snadný, že jej s důvěrou necháme jako cvičení 2a.2. 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? Podle definice by mělo existovat $k \in \mathbb{Z}$ tak, aby $0 = k \cdot 0$, což se nám hravě podaří splnit, třeba $k = 13$ bude fungovat. Takže ano, $0|0$.

Toto ukazuje, že pojem dělitelnosti se zásadně liší od dělení jako matematické operace, protože samozřejmě nulou dělit nelze nic, ani nulu. Pojem dělitelnosti $a|b$ vypovídá o určitém vztahu mezi čísly a a b , odpovědí je ano či ne. Dělení je matematická operace, jejímž výsledkem je číslo, je to tedy něco jiného (a to číslo nás mimochodem v této kapitole nebude (až na pár výjimek) vůbec zajímat). Samozřejmě je mezi těmito dvěma pojmy souvislost, ale liší se výrazně zejména tím, jak s nimi pracujeme. Proto silně doporučujeme, aby se čtenář při práci s dělitelností zlomkům vyhýbal. Platí to zejména o důkazech, protože v nich zlomky svádí na zcestí. I my je zde budeme používat jen výjimečně, když to nepůjde jinak.

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
- Chceme: a dělí $b + c$.
- a dělí c

Napišme si přesně podle definice, co to vlastně znamená.

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

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 $b + c$.

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): Z předpokladu $a \mid b$ 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 $a \mid (b + c)$.

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

Protože je to náš první důkaz s dělitelností, napsali jsme jej podrobněji. S přibývajícím 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 $a \mid b$ a $a \mid c$, pak pro všechny $\beta, \gamma \in \mathbb{Z}$ platí $a \mid (\beta b + \gamma c)$.

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. Naskytá se zajímavá otázka, zda tvrzení 2a.2 (i) platí i v opačném směru, tedy zda lze z platnosti $a \mid (b + c)$ odvodit, že automaticky $a \mid b$ a $a \mid c$. Trocha experimentování rychle ukáže, že to obecně neplatí, například $3 \mid (2 + 4)$, ale neplatí $3 \mid 2$ ani $3 \mid 4$. Trochu delší experimentování by mohlo naznačit zajímavou věc, že když platí $a \mid (b + c)$, tak buď dělitelnost u b a c funguje, nebo se pokazí rovnou obě, 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 $a \mid (b + c)$ a $a \mid b$, pak $a \mid c$.

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 $a \mid b$ díky větě 2a.2 (ii) dostaneme $a \mid (-b)$, máme také $a \mid (b + c)$ 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. Formálně 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 $|a| \leq |b|$.

Důkaz (rutinní, poučný): (i): Viz cvičení 2a.4.

(ii): $a|b$ 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 $a|b$ 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 $a|b$ a $b|a$, pak $a = b$.

Toto tvrzení rozhodně neplatí na \mathbb{Z} . Například $13|(-13)$ a $(-13)|13$, ale neplatí $-13 = 13$. Máme tedy názornou ukázkou, 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): Jestliže $a = 0$, tak b coby násobek nuly musí být také 0, tedy $a = b$. Pokud $b = 0$, dostáváme symetricky $a = 0$ a zase $a = b$.

Nechť jsou tedy 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.

Co uděláme v situaci, kdy číslo a nedělí číslo b , ale my nějak dělit potřebujeme? Ukážeme dvě možné reakce, obě budou dále užitečné.

Jedna možnost je vydělit v oboru reálných čísel a zaokrouhlit. V analýze bývá zvykem zaokrouhlovat na nejbližší celé číslo, v diskrétní matematice zaokrouhlujeme dolů a nahoru.

Definice.

Definujme následující funkce na \mathbb{R} :

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}; \quad (\text{zaokrouhlení dolů})$$

$$\lceil x \rceil = \min\{n \in \mathbb{Z} : n \geq x\}. \quad (\text{zaokrouhlení nahoru})$$

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

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

Příklad 2a.b: 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

$$\lfloor 13.23 \rfloor = \max\{\dots, 0, \dots, 10, 11, 12, 13\} = 13 \quad \text{a}$$

$$\lceil 13.23 \rceil = \min\{14, 15, 16, \dots\} = 14.$$

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

$$\lfloor -13.23 \rfloor = \max\{\dots, -17, -16, -15, -14\} = -14 \quad \text{a}$$

$$\lceil -13.23 \rceil = \min\{-13, -12, -11, \dots, 0, \dots\} = -13.$$

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 2a.7.

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.

S Rozbor: Jde o výbornou příležitost k nácviku, protože je to vlastně opakování základních principů. Každé z tvrzení je ekvivalence, budeme proto vždy dokazovat implikaci zleva doprava a implikaci zprava doleva. Například u tvrzení (i) bude třeba dokázat pravdivost těchto dvou výroků:

$$\forall x \in \mathbb{R} \forall n \in \mathbb{Z} : \lfloor x \rfloor = n \implies n \leq x < n + 1;$$

$$\forall x \in \mathbb{R} \forall n \in \mathbb{Z} : n \leq x < n + 1 \implies \lfloor x \rfloor = n.$$

Nabízí se přímý důkaz, tedy dostáváme se k závěru pomocí toho, co nám říká předpoklad, u našich funkcí budeme samozřejmě používat podmínku z definice.

Důkazy jsou opravdu snadné, stačí se podívat na definici pojmů a mírně se zamyslet, dokonce ani nebude třeba něco počítat. Pokud vás to nenapadne hned, podívejte se na důkaz tvrzení (i) a další už určitě zvládnete.

Důkaz (pro úplnost): (i) \implies : 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 $n + 1 \leq n$ neboli platí $n + 1 > n$.

(i) \impliedby : 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) \implies : Jestliže je $n = \lceil x \rceil$, pak podle (i) je $n \leq x$ a také $x < n + 1$, což je $x - 1 < n$.

(iii) \impliedby : 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 2a.8.

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 2a.9.

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) \implies : Definujme $\varepsilon = x - \lfloor x \rfloor = x - n$. Pak $x = n + \varepsilon$ a podle (i) z faktu 2a.7 také $0 \leq \varepsilon < 1$.

(i) \impliedby : 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 2a.7 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 ukázkou a v rámci tréninku je i dokážeme. Rovnou podotkneme, že pro nás nebudou důležité, takže nemá smysl se je učit nazpaměť.

Fakt 2a.10.

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 2a.7 (ii) platí $n - 1 < x \leq n$. Potom také platí $-n + 1 > -x \geq -n$, tedy $(-n) \leq -x < (-n) + 1$ a podle faktu 2a.7 (i) je $-n = \lfloor -x \rfloor$.

Důkaz (ii) je podobný.

(iii): Označme si $n = \lfloor x \rfloor$. Pak podle faktu 2a.7 (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 2a.7 (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 2a.c: Máte USB flashku o velikosti 12GB. Kolik se na ni vejde filmů o velikosti 700MB?

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

△

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

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

△

Druhá možnost, jak se vypořádat se situací, kdy jedno číslo nedělí druhé, je použít dělení se zbytkem. I to je něco, co známe už dávno, zde se na to podíváme pořádně. Začneme tím, že v této knize neradi vidíme dělení, a proto známý vztah $\frac{a}{d} = q + \frac{r}{d}$ určitě uvidíme raději ve tvaru $a = qd + r$. Podobných vyjádření je ovšem více, například pro $a = 13$ a $d = 3$ máme $13 = 4 \cdot 3 + 1$, ale také $13 = 2 \cdot 3 + 7$. Jak poznáme to správné?

Věta 2a.11. (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.

Věta tedy preferuje verzi $13 = 4 \cdot 3 + 1$. Než ji dokážeme, podíváme se trochu kolem. Věta nám garantuje existenci dvou speciálních čísel, která si nazveme.

Definice.

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

Takže 4 je částečný podíl po dělení 13 číslem 3 a $13 \bmod 3 = 1$. To bylo snadné, trochu opatrnější lidé bývají u záporných čísel. Určitě se například nechceme ukvapit a napsat, že částečný podíl čísel -13 a 3 je -4 , protože to by znamenalo $-13 = (-4) \cdot 3 + (-1)$. Definice ovšem neumožňuje záporný zbytek. Správně tedy musíme psát $-13 = (-5) \cdot 3 + 2$, tedy $(-13) \bmod 3 = 2$ a částečný podíl je -5 . Toto mimo jiné ukazuje, že výpočet $a \bmod d$ je citlivý na změnu znaménka u čísel a, d . Existují na to pravidla, která nemá smysl se učit, viz cvičení 2a.6. Jejich existence nicméně znamená, že se při dělení se zbytkem (a hlavně v důkazech, které s ním pracují) můžeme omezit na případ, kdy $d > 0$ a $a \geq 0$.

Náš příklad také ukazuje, že je-li q částečný podíl a a d , tak se nelze spoléhat, že by $-q$ bylo částečným podílem čísel $-a$ a d . I zde existuje pravidlo.

Fakt 2a.12.

Nechť $a, d \in \mathbb{Z}$, $d \neq 0$, nechť je q částečný podíl a a d . Pak $q = \lfloor \frac{a}{d} \rfloor$ pro $d > 0$ a $q = \lceil \frac{a}{d} \rceil$ 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 2a.9 (i) a (ii) dávají žádaný výsledek. □

Jak tyto věci počítáme v praxi? Dělení nepatří mezi nejoblíbenější operace, proto se ke zbytku často pohodlněji dostaneme tak, že od čísla a opakovaně odečítáme d , popřípadě jej přičítáme, podle znamének a a d , a děláme to, dokud se výsledkem nedostaneme do nuly či těsně nad nulu (nejblíže, co to jde). Počet odečítání/přičítání pak určí q .

Příklad 2a.e: Vyzkoušíme si to na našem příkladě $a = -13$ a $d = 3$, kde jsme už odhalili správný zápis $-13 = (-5) \cdot 3 + 2$. Alternativa: $q = \lfloor \frac{-13}{3} \rfloor = \lfloor -4.33... \rfloor = -5$, to souhlasí. Zrovna v tomto případě je možná rychlejší si představit, co se stane s číslem -13 při opakovaném přičtení trojky.

Povědomý výpočet napravo nám zase říká, že $4147 \bmod 37 = 3$. V tomto případě by se nám asi nechtělo opakovaně odčítat 37 od čísla 4147. Vidíme, že každá z metod je někdy vhodnější a někdy méně.

Podle cvičení 2a.6 pak také $4147 \bmod (-37) = 3$, zatímco $-4147 \bmod 37 = 34$ a $-4147 \bmod (-37) = 34$.

△

Otázka konkrétní implementace je nad rámec tohoto textu. Zmíníme jen jeden aspekt: Zdálo by se, že pokud je a výrazně větší než d , tak by těch odčítacích cyklů bylo mnoho a je lepší použít dělení. To má ovšem háček, protože pokud se to dělení dělá tradičním způsobem, tak je to pro velká čísla také výpočetně náročná záležitost.

Zajímavý přístup je najít nejprve nějak chytře $\frac{1}{d}$, protože násobení $a \cdot \frac{1}{d}$ je sice také náročné, ale umíme jej zrychlit (viz kapitola 12c). To $\frac{1}{d}$ pak stačí najít přibližným výpočtem, populární je třeba tzv. Newton-Raphsonovo dělení, které hledá aproximaci $\frac{1}{d}$ použitím Newtonovy metody na nalezení kořene funkce $f(x) = \frac{1}{x} - d$. Vychází iterační schéma $x_{n+1} = x_n(2 - dx_n)$, které je kvadratického řádu, přibližně řečeno s každou iterací zdvojnásobí počet správně nalezených desetinných míst. Jako u mnohých numerických receptů, i zde číhají nebezpečné zákuty a je dobré si to nastudovat, například se ukáže, že dobrá iniciační hodnota je $x_0 = \frac{48}{17} - \frac{32}{17}d$.

To už se ale dostáváme někam daleko, zde nebudeme technické nalezení q a r řešit, prostě oznámíme „nechť $r = a \bmod d$ “ a volbu implementace necháme na uživateli.

Teď je čas dokázat Větu o dělení. Dá se na to jít více způsoby, my zkusíme odít do matematického hávu ten trik s odčítáním. Všechny možné výsledky onoho opakovaného přičítání/odčítání shromáždíme do množiny a pak vybereme ten správný.

Důkaz (dobrý, poučný): 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 $a - qd \in M$, 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 $a = q_0d + r$ pro nějaké $q_0 \in \mathbb{Z}$, polovina tvrzení je splněna. Platí také $r < d$?

Kdyby ne, pak $a - q_0d \geq d$, 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 průšvih, 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.13.

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.f:

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 devítimístního 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 nezkažilo. Kód tedy neodhalí chyby všechny.

Mimořádně, proč jsme použili zrovna jedenáctku? Pokud použijeme menší číslo, pak chybu v jedné cifře nemusí odhalit. Například pokud bychom použili dělitelnost desítkou, 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, druhý 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 devítimístního 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 číslem 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 naprogramovanou 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, ..., 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.

△

Příklad 2a.g: 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 $n = (a_k \dots a_1 a_0)_b$. To znamená, že $n = \sum_{k=0}^n a_i b^i$. Chytrě si to rozepíšeme:

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

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 $\frac{n}{b} = a_k b^{k-1} + \dots + a_2 b + a_1 + \frac{a_0}{b}$, přičemž 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 $a_k b^{k-1} + \dots + a_2 b + a_1 = (a_k b^{k-2} + \dots + a_2) b + a_1$, ze které bychom rádi nějak vydělili a_1 . Nabízí se, že zopakujeme předchozí trik, tedy vydělíme číslem b atd. Z toho vychází algoritmus. 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. Nebudeme preferovat nějaký existující jazyk, raději použijeme pseudokód srozumitelný snad každému.

Verze 1.

procedure *conversion* (n, b : positive integer)

$q := n; k := -1;$

repeat

$k := k + 1;$

$a_k := q \bmod b;$

$q := \lfloor \frac{q}{b} \rfloor;$

until $q = 0;$

output: $n = (a_k \dots a_1 a_0)_b;$

Verze 2.

procedure *conversion* (n, b : positive integer)

$q := n; k := -1;$

repeat

$k := k + 1;$

$x := \lfloor \frac{q}{b} \rfloor;$

$a_k := q - xb;$

$q := x;$

until $q = 0;$

output: $n = (a_k \dots a_1 a_0)_b;$

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

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

(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 $cb = a_{-1} + a_{-2} \frac{1}{b} + a_{-3} \frac{1}{b^2} + \dots$, 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 $cb - a_{-1} = a_{-2} \frac{1}{b} + a_{-3} \frac{1}{b^2} + \dots$ 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: $c = (0.a_{-1}a_{-2}a_{-3} \dots)_b;$

△

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 $1|a, a|a$ a $a|0$ (viz fakt 2a.1).

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

(ii) Nechť $a, b, c \in \mathbb{Z}$. Dokažte, že jestliže $a|b$ a $b|c$, pak $a|c$.

Viz věta 2a.2.

Cvičení 2a.4 (rutinní, poučné): Nechť $a, b \in \mathbb{Z}$. Dokažte, že následující podmínky jsou ekvivalentní:

(i) $a|b,$

(ii) $(-a)|b,$

(iii) $a|(-b),$

- (iv) $(-a) | (-b)$,
 (v) $|a| || b|$.

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 $a | b$ 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 $a | c$ a $b | d$, pak $ab | cd$.

Cvičení 2a.8 (rutinní): Nechť $a, b, c \in \mathbb{Z}$. Dokažte, že jestliže $ac | bc$ a $c \neq 0$, pak $a | b$.

Co by se stalo, kdyby $c = 0$?

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

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.

Cvičení 2a.12 (rutinní): Kolik bajtů (bytes) je třeba na zakódování informace v délce 4/10/500/3000 bitů (bits)?

Cvičení 2a.13 (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 2a.14 (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 2a.15 (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 2a.16 (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 2a.17 (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 2a.18 (poučné, dobré): Dokažte či vyvráťte 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) $\forall x \in \mathbb{R}: \lfloor \lceil x \rceil \rfloor = \lfloor x \rfloor$.
 (viii) $\forall x \in \mathbb{R}: \lceil \lfloor x \rfloor \rceil = \lceil x \rceil$.
 (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) $\forall x \in \mathbb{R}: \lceil \sqrt{\lfloor x \rfloor} \rceil = \lceil \sqrt{x} \rceil$.

Cvičení 2a.19:

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

Nápověda: Použijte fakt 2a.9, rozeberte případy $\varepsilon < \frac{1}{2}$ a $\varepsilon \geq \frac{1}{2}$.

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.9.

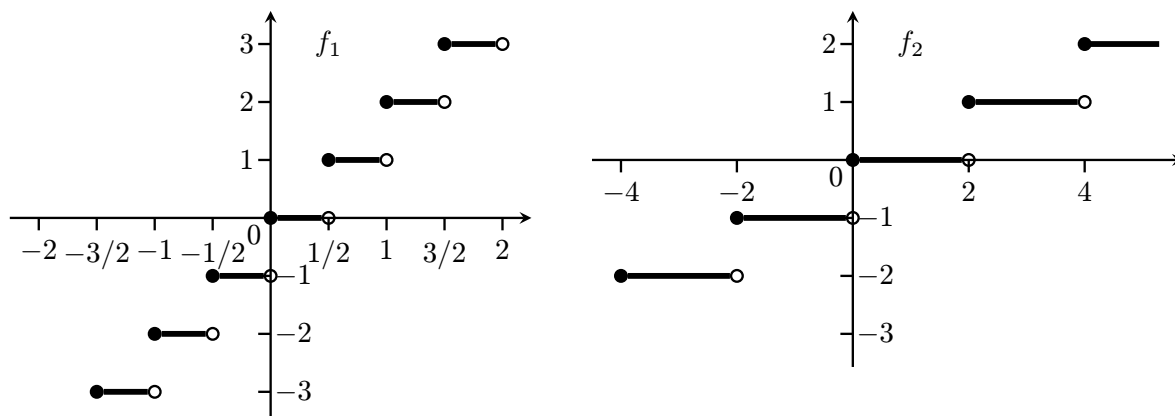
2a.12: 1 byte je 8 bits, takže: $\lceil \frac{4}{8} \rceil = 1, \lceil \frac{10}{8} \rceil = 2, \lceil \frac{500}{8} \rceil = 63, \lceil \frac{3000}{8} \rceil = 375.$

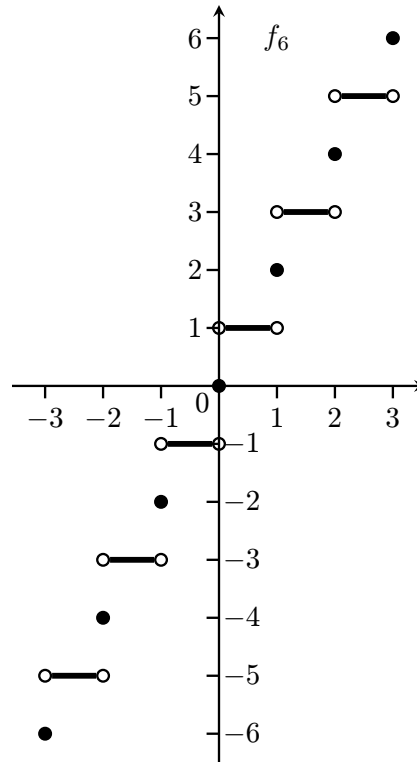
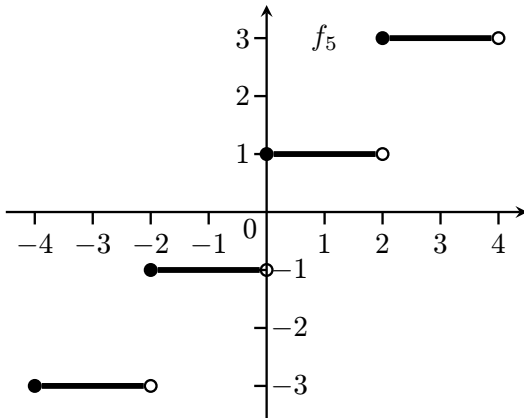
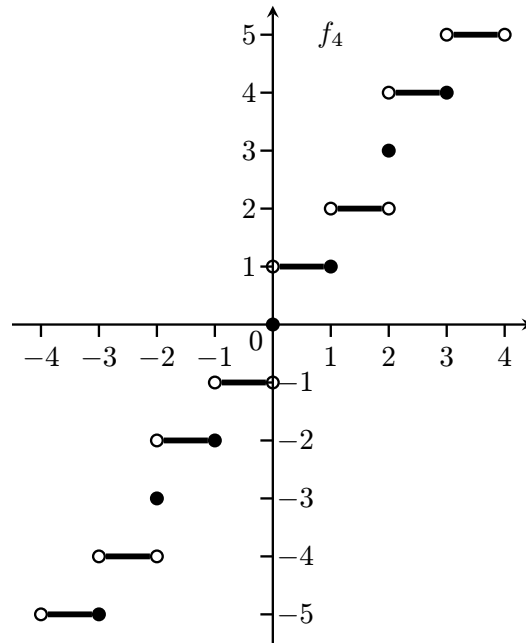
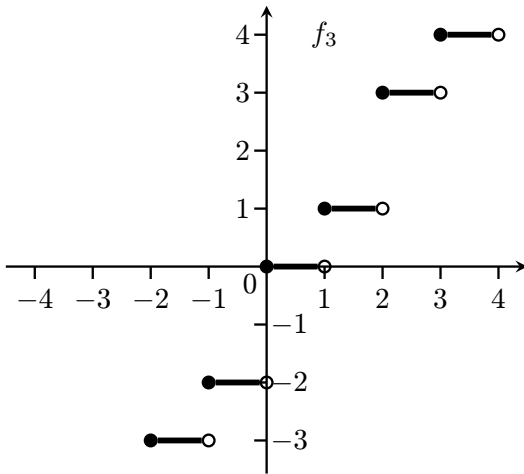
2a.13: Toto chce hodně experimentovat se zaokrouhlováním. (i): $\lfloor b \rfloor - \lfloor a \rfloor + 1;$ (ii): $\lfloor b \rfloor - \lfloor a \rfloor - 1.$

2a.14: Nechť $x = n + r,$ kde $r \in \langle 0,1 \rangle.$ Jestliže $r = 0,$ pak $\lfloor x \rfloor = \lceil x \rceil = n,$ jinak $\lfloor x \rfloor = n$ a $\lceil x \rceil = n + 1.$

2a.15: 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 $\lfloor \frac{n}{2} \rfloor = \lfloor k + \frac{1}{2} \rfloor = k = \frac{n-1}{2}.$

2a.16:





2a.17: (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 $\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil = k(k + r)$, zatímco $\lfloor \frac{n^2}{4} \rfloor = \lfloor \frac{4k^2 + 4kr + r^2}{4} \rfloor = k^2 + kr + \lfloor \frac{r^2}{4} \rfloor = k^2 + kr = k(k + r)$.

2a.18: (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 $x + y = n + y + r$, 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 $\lceil x \rceil \in \mathbb{Z}$, 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 $(n-1)^2 < x \leq n^2$.

2a.19: $x = \lfloor x \rfloor + \varepsilon$.

1) $\varepsilon < \frac{1}{2}$: Pak $x + \frac{1}{2} = \lfloor x \rfloor + (\varepsilon + \frac{1}{2})$ a $0 \leq \varepsilon + \frac{1}{2} < 1$, podle faktu 2a.9 (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 2a.9 (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 $x + \frac{1}{2} = (\lfloor x \rfloor + \varepsilon) + \frac{1}{2} = (\lfloor x \rfloor + 1) + (\varepsilon - \frac{1}{2})$, podle faktu 2a.9 (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 2a.9 (ii) pak $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$. Spojit: $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1 = \lfloor x \rfloor + (\lfloor x \rfloor + 1) = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

2b. Dělitelé

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. Nejvíce dělitelů má číslo nula, jmenovitě všechna celá čísla. Je to jediný takový zvrhlík, další důvod, proč se nula při praktické práci s dělitelností obvykle neuvažuje. Je také tradiční nebrat v úvahu záporné dělitele, takže když někdo pro určité celé číslo mluví o množině dělitelů, tak se tím myslí jeho kladní dělitelé.

Druhým extrémem co se týče počtu dělitelů je jednička, ta má kladného dělitele jen jednoho, jedničku. Všechna ostatní čísla mají alespoň dva kladné dělitele, jmenovitě jedničku a sebe sama (v absolutní hodnotě). Některá čísla si s tímto minimem vystačí.

Definice.

Nechť $a \in \mathbb{N}$, $a \geq 2$.

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, je to nějaké jiné číslo. Občas si na to budeme muset dát pozor.

Prvočísla tradičně značíme jako p , popý. q . Všimneme si, že číslo $a \in \mathbb{N}$ je složené, jestliže existuje $k \in \mathbb{N}$ takové, že $k|a$ a $1 < k < a$. Ještě jinak: Číslo a je složené, jestliže existují čísla $x, y \in \mathbb{N}$ taková, že $a = xy$ a $x < a$, $y < a$.

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. Ukážeme, že s výjimkou jedničky je najdeme ve všech číslech.

Fakt 2b.1.

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

Důkaz využívá silný princip indukce. Pokud se na to čtenář necítí, může s důkazem počkat, až indukci probereme v kapitole .

Důkaz (poučný): Dokážeme to silnou indukcí na n pro $n \geq 2$.

(0) $n = 2$: Ano, existuje prvočíslo $p = 2$, které dělí $n = 2$.

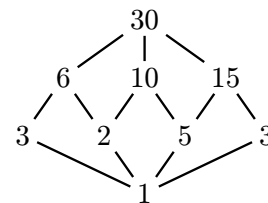
(1) Nechť $n \in \mathbb{N}$, $n \geq 2$. Předpokládejme, že tvrzení platí pro všechna čísla $2, 3, \dots, n$. Uvažujme číslo $n+1$. Pokud je to prvočíslo, tak dáme $p = n+1$ a jsme hotovi.

Pokud to prvočíslo není, pak musí existovat $k \in \mathbb{N}$ takové, že $k|(n+1)$ a $1 < k < n+1$. Pak je ale k z množiny $2, 3, \dots, n$, tudíž existuje prvočíslo p takové, že $p|k$. Spolu s $k|(n+1)$ to díky větě 2a.2 (iii) dává $p|(n+1)$ a jsme hotovi. □

Čtenář samozřejmě ví, že platí víc, každé číslo lze rozložit na součin prvočísel. Důkaz tohoto tvrzení je poněkud delší a indukce v něm hraje ještě větší roli než v tvrzení výše, proto si hlavní poznatky o prvočíslech shromáždíme v bonusové kapitole 15 ke konci knihy. I tak se nám ale prvočísla díky svým speciálním vlastnostem budou v následujících kapitolách objevovat.

2b.2 Poznámka: 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 $\{1, 2, \dots, a\}$.

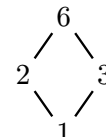
Má zajímavou vnitřní strukturu: Jestliže je d nějaký dělitel a , tak podle věty 2a.2 (iii) i všichni jeho dělitelé jsou děliteli čísla a . Ovšem i dělitelé dělitelů splňují tuto vlastnost, takže se množina „větvi“. Množinu všech (kladných) dělitelů a si proto můžeme představit jako jakési stromečky, s každým dělitelem se v množině očitne i stromeček dalších dělitelů. Na obrázku vpravo jsme symbolicky znázornili stromeček, který do množiny dělitelů čísla 60 přinese jeho dělitel 30, spojnice reprezentují vztah dělitelnosti čísla číslem. Třicítka má celkem 7 kladných dělitelů odlišných od sebe sama, některé z nich jsou dělitelé jiných, zkusili jsme to zachytit obrázkem, takže například vidíme, že číslo 5 dělí desítku, patnáctku a třicítku (funguje to i přes více „pater“), číslo 1 pak dělí všechno.



Trojka se vyskytla vícekrát, to teď nebudeme řešit. Ovšem šedesátka má také dělitel 20, který v tomto stromečku není, nicméně mnohé z dělitelů dvacítky v něm jsou. Je to tedy komplikované, jednotlivé „podstromečky“ se prolínají, proto se ani nebudeme pokoušet nakreslit obrázek všech dvanácti dělitelů čísla 60, cílem nebylo vyvinout nějakou teorii o množině dělitelů, spíš získat intuitivní představu, co se s děliteli daného čísla děje.

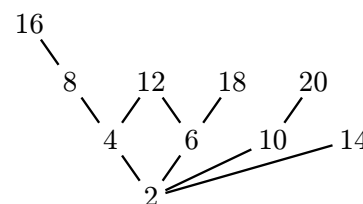
K otázce co nejlepšího zachycení vztahů tohoto typu se dostaneme v kapitole 7a, kde se dozvíme, že jde vlastně o Hasseho diagramy příslušné částečně uspořádané množiny.

Jednu věc víme najisto. Ať už nakreslíme obrázek jakkoliv, tak se v něm všechny „větve“ budou sbíhat nahoře v šedesátce a dole v jedničce, což ilustruje napravo obrázek všech dělitelů šestky.



Když už jsme u toho, jak vypadá množina násobků čísla a ? I zde je případ $a = 0$ výjimečný, jediným násobkem je pak zase nula. Pokud je a nenulové, tak jsou jeho kladné násobky dány jako množina $\{k|a| : k \in \mathbb{N}\}$, tedy pro a kladné jde o množinu $\{a, 2a, 3a, \dots\}$. Z tohoto pohledu jde tedy o výrazně jednodušší situaci než u dělitelů, množinu lze elegantně zapsat. Na druhou stranu je to množina nekonečná, tudíž asi budou problémy s obrázkem. Zkusme si představit obrázek jen některých násobků, těch menších, a zase naznačíme spojnicemi vztah dělitelnosti. Tím se ovšem struktura zase zkomplikuje, nelze totiž udělat jeden řetízek spojující čísla $a, 2a, 3a$ atd., protože číslo $2a$ určitě nedělí číslo $3a$.

I zde tedy vznikají stromečky, tentokrát násobků násobků. Například násobky čísla 2 zahrnují i tento kousek napravo (zakreslili jsme je až po dvacítku). Opět z toho nebudeme dělat nějaké závěry (kromě zjevného pozorování, že se všechny „cestičky“ sbíhají dolů do dvojky, zatímco směrem „nahoru“ se rozbíhají nekonečně patry, a že by tak možná šlo generovat abstraktní moderní umění). Jen si tak trénujeme představivost, ovšem brzy se k tomu vrátíme.



△

Ještě zajímavější to bude, když si vezmeme dvě čísla.

Definice.

Nechť $a, b \in \mathbb{Z}$.

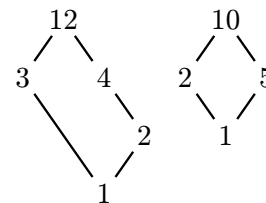
Číslo $d \in \mathbb{N}$ je **společný dělitel (common divisor)** čísel a, b , jestliže $d|a$ a $d|b$.

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

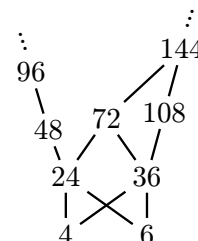
Například číslo 1 je určitě společným dělitelem čísel 40 a 60, zatímco $40 \cdot 60 = 2400$ je určitě jejich společným násobkem. Čtenář ale asi tuší, že nás budou zajímat méně triviální odpovědi, třeba 20 jako společný dělitel a 120 jako společný násobek. Z definice vyplývá, že množinu společných dělitelů 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. Nuly si také odložíme na později, podíváme se blíže na nejčastější případ.

2b.3 Poznámka: Uvažujme dvě různá přirozená čísla a, b . 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.

Co se týče dalších společných dělitelů, zase vznikají stromečky díky následující vlastnosti: Jestliže je d nějaký společný dělitel a a b , tak i všichni jeho dělitelé jsou společnými děliteli čísel a , b a leží ve zkoumané množině. Jde tedy o situaci obdobnou té z poznámky 2b.2. Na obrázku vpravo jsme znázornili symbolicky dva stromečky z množiny společných dělitelů čísel 120 a 180. Opět se nebudeme pokoušet rekonstruovat podobu množiny všech společných dělitelů, jen si rozmyslíme, že ať už je obrázek jakýkoliv, vždy se všechny „cestičky“ budou sbíhat dole v jedničce. Jeden rozdíl od případů dělitelů jednoho čísla tu ovšem je. Zatímco tam bylo jasné, že se všechny cestičky musí sejít nahoře v dotyčném čísle, tady máme dvě různá čísla a , b . Každé číslo v našem obrázku musí nakonec dělit a i b , ale to jsou dva různé cíle. Není tedy v této chvíli vůbec jasné, jak se ten obrázek směrem nahoru vyvrbí. Brzy se dozvíme, jak to je.



Jak vypadá množina společných násobků přirozených čísel a , b ? Opět 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 . I zde se tedy stromečkuje, například společný násobek 24 čísel 4 a 6 do množiny jejich společných násobků přivede řetězky 24, 48, 72, 96, ..., zatímco společný násobek 36 přivede řetězky 36, 72, 108, 144. V rámci každého řetězku některá čísla dělí jiná, řetězky se navzájem proplétají, prostě vznikají zajímavé struktury. Kousek ukazujeme vpravo, šikmé spojnice opět označují vztah býti násobkem. I zde také vidíme rozdíl mezi násobky jednoho čísla a společnými násobky dvou čísel. Zatímco u jednoho čísla se všechny cestičky sbíhají dole u onoho daného čísla, v případě společných násobků dvou čísel není hned zřejmé, co se bude dít.



△

Shrňme si to podstatné. Pokud máme dvě kladná čísla, tak je množina všech dělitelů neprázdná a konečná, tedy i omezená, a množina všech společných násobků je omezená zdola a nekonečná. Protože změna znaménka nemá na vlastnost dělitelnosti vliv, platí toto pro libovolná dvě nenulová čísla. Změní se něco, pokud začneme uvažovat i nuly?

Víme, že nulu dělí všechna čísla, takže pokud bychom měli řekněme případ $b = 0$, tak jsou společní dělitelé dáni čistě číslem a . Pokud by a nebylo nulové, tak dostáváme nějakou neprázdnou podmnožinu \mathbb{N} , která je shora omezená číslem $|a|$. Situace je tedy obdobná dvěma nenulovým číslům a není třeba vymýšlet nic nového. Pokud by ovšem obě čísla byly nula, pak jako množinu společných dělitelů dostáváme celé \mathbb{N} . Je to tedy případ zcela odlišný a v našich úvahách pro něj budeme muset dělat speciální odbočku.

Trochu jiné je to u společných násobků. Jediným možným násobkem nuly je zase nula, což ale není kladné číslo, takže množina kladných násobků nuly je prázdná. Protože společné násobky vznikají průnikem, stačí mít jedno z čísel a , b nulové a množina společných násobků již bude prázdná. Je to zase případ, který bude nutno řešit zvlášť.

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 $\text{lcm}(a, b)$, jako nejmenší prvek množiny jejich společných násobků, pokud jsou obě a, b nenulové. Jinak definujeme $\text{lcm}(a, 0) = \text{lcm}(0, b) = 0$.

Existují i konkurenční značení, ale tato jsou nejpoužívanější. Oba pojmy se dají zobecnit na více čísel, viz cvičení 2b.8. 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 $\text{lcm}(0, a)$ bylo třeba definovat speciálním způsobem. Jak jsme již poznamenali, většina autorů se omezuje na přirozená čísla a mají po starostech, začínáme jim už jemně závidět. Zvědavému člověku to ale nedá, chce vědět, zda by tato teorie nešla vybudovat pro všechna celá čísla. Hodnoty, které jsme pro speciální případy vybrali, jsou obvyklou volbou, protože pak většina tvrzení o \gcd a lcm platná pro nenulová a, b platí obecně, pro všechna celá čísla. V jejich znění tedy není třeba rozlišovat, ovšem v důkazech se samozřejmě musí speciální případy dělat zvlášť.

Typické důkazy v této části tedy budou následovat následující tradiční postup: Nejprve se tvrzení ukáže pro kladná čísla, pak se poznamená, že změna znaménka nehraje roli, a nakonec se rozeberou případy s nulami. Pomáhají nám při tom následující pozorování.

Fakt 2b.4.

Nechť $a \in \mathbb{Z}$. Pak platí:

- (i) $\gcd(a, 0) = |a|$ a $\text{lcm}(a, 0) = 0$;
- (ii) $\gcd(a, a) = \text{lcm}(a, a) = |a|$.

Druhé tvrzení v (i) je přímo definice, z té známe i hodnoty $\gcd(0, 0) = \text{lcm}(0, 0) = 0$ pro (ii). Důkaz ostatního necháme jako cvičení 2b.1. Každopádně pokud se vám případy s nulami začínou zajídat, nebude zas tak velký problém, když je budete ignorovat. Výjimkou je případ $\gcd(0, a)$, který je v aplikacích potřeba, naštěstí se na něj vztahuje klasická definice (největší prvek množiny společných dělitelů), takže se nemusí řešit zvlášť.

O znaménka se nejen v důkazech postará toto tvrzení.

Fakt 2b.5.

Nechť $a, b \in \mathbb{Z}$. Pak $\gcd(a, b) = \gcd(|a|, |b|)$ a $\text{lcm}(a, b) = \text{lcm}(|a|, |b|)$.

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 $d|a$ a $d|b$, což jsou podle věty 2a.5 přesně čísla splňující $d||a|$ a $d||b|$. 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 $\text{lcm}(a, b)$ je obdobný. □

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

$$\begin{aligned} 120 &= 2^3 \cdot 3 \cdot 5, \\ 180 &= 2^2 \cdot 3^2 \cdot 5. \end{aligned}$$

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

△

Prvočíselný rozklad si uděláme pořádně později, v kapitole o prvočíslech, a mimo jiné tam zmíníme, že dělat rozklad pro velká čísla je velmi nepříjemná úloha. Budeme tedy potřebovat nějaký efektivní způsob hledání $\gcd(a, b)$ a $\text{lcm}(a, b)$. Nejdříve se podíváme na pár základních vlastností nových pojmů. Z diskuse o podobě množin společných dělitelů a násobků okamžitě dostáváme následující tvrzení.

Fakt 2b.6.

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 $\text{lcm}(a, b) \geq \max(|a|, |b|)$.

Co se stane, když je některé číslo nulové? Podívejte se na cvičení 2b.3.

Nejmenší možná hodnota pro $\gcd(a, b)$ signalizuje, že čísla a, b mají specifický vztah.

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).

Prvočísla mají velmi specifickou množinu kladných dělitelů, jedničku a sebe sama. Dostáváme tak jednoduché pozorování.

Fakt 2b.7.

Nechť p je prvočíslo. 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. □

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.

Protože $\gcd(a, b)$ dělí a i b , tak pro nenulová a, b máme $\frac{a}{\gcd(a, b)} \in \mathbb{Z}$ a $\frac{b}{\gcd(a, b)} \in \mathbb{Z}$. To je zjevné, ale budeme to opakovaně používat, tak na to upozornujeme. Jistě také cítíte, že tím dělením odebíráme z a a b vše, co měly společného, takže ty výsledné podíly by už nic společného mít neměly. Potvrdíme si to. Důkaz je přímočarý, prostě se podíváme, jak vypadají společní dělitelé těchto dvou zlomků.

Fakt 2b.8.

Nechť $a, b \in \mathbb{Z}$, $a \neq b$. Pak jsou $\frac{a}{\gcd(a, b)}$ a $\frac{b}{\gcd(a, b)}$ nesoudělná celá čísla.

Důkaz (rutinní): Předpokládejme, že $d \in \mathbb{N}$ je nějaký společný dělitel čísel $\frac{a}{\gcd(a, b)}$ a $\frac{b}{\gcd(a, b)}$. To znamená, že pro nějaká $k, l \in \mathbb{Z}$ máme $\frac{a}{\gcd(a, b)} = kd$ a $\frac{b}{\gcd(a, b)} = ld$. 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.22 (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.22 bude vyžadovat Bezoutovu identitu, což naznačuje jistou obtížnost). Náš elementární důkaz ukazuje, že právě dokázané tvrzení je snadné.

Teď se podíváme blíže na $\text{lcm}(a, b)$.

Fakt 2b.9.

Nechť $a, b, n \in \mathbb{Z}$. Jestliže je $a | n$ a $b | n$, pak $\text{lcm}(a, b) | n$.

Důkaz (poučný): 1) Předpokládejme, že $a, b, n > 0$. Protože $a | n$ a $b | n$, je n společným násobkem a podle definice tedy určitě platí $\text{lcm}(a, b) \leq n$. Ukážeme, že je tam dokonce vztah dělitelnosti.

Nechť podle věty o dělení $n = q \text{lcm}(a, b) + r$. Protože a dělí $\text{lcm}(a, b)$, tak dělí i $q \text{lcm}(a, b)$, dělí rovněž n , proto podle důsledku 2a.3 musí a také dělit r . Stejně ukážeme, že i b dělí r , navíc $r \in \mathbb{N}_0$, takže buď $r = 0$, nebo je r společný násobek a, b . To druhé je ale nemožné, protože $\text{lcm}(a, b)$ je nejmenší společný násobek a $r < \text{lcm}(a, b)$. Proto $r = 0$ a $n = q \text{lcm}(a, b)$ pro nějaké $q \in \mathbb{Z}$.

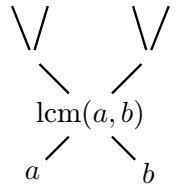
2) Nulové případy: Pokud $n = 0$, tak jsou dělitelem n všechna čísla, proto je předpoklad i závěr dokazované implikace pravdivý, tedy i celá implikace platí.

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 $\text{lcm}(|a|, |b|) | |n|$ neboli $\text{lcm}(|a|, |b|) | n$. K závěru nás pak dovede fakt 2b.5. □

Na toto tvrzení se teď podíváme dvěma způsoby. Jednu situaci čtenář patrně zná. Máme číslo n a víme, že jej lze dělit určitými dvěma čísly a, b . Pak určitě obecně neplatí, že by toto číslo šlo dělit součinem ab , viz například $a = 4$, $b = 6$ a $n = 36$. Fakt potvrzuje známou věc, že číslem $\text{lcm}(a, b)$ lze n vydělit.

Druhá zajímavá interpretace se na tuto záležitost dívá nikoliv z pohledu n , ale z pohledu a a b . V poznámce 2b.3 jsme přemýšleli, jak to vypadá v obrázku společných násobků. Fakt výše říká, že všechny společné násobky jsou dělitelné číslem $\text{lcm}(a, b)$, tedy všechny cestičky se nutně musejí sbíhat v čísle $\text{lcm}(a, b)$. Pokusili jsme se to vpravo znázornit malůvkou.



Matematicky řečeno, pokud množinu společných násobků uspořádáme pomocí dělitelnosti, tak je $\text{lcm}(a, b)$ nejmenším nejen ve smyslu nerovnosti (velikosti čísel), ale také ve smyslu dělitelnosti, viz kapitola 7b. Obdobné tvrzení platí i pro $\text{gcd}(a, b)$, ale tam je důkaz těžší a postupně se k němu propracujeme.

Naším cílem teď bude odvodit praktické postupy k nalezení $\text{gcd}(a, b)$ a $\text{lcm}(a, b)$. Hned se jednoho z nich zbavíme.

Věta 2b.10.

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

Důkaz (poučný): 1) Nejprve budeme předpokládat, že $a, b \in \mathbb{N}$.

a) Uvažujme číslo $m = \frac{ab}{\text{gcd}(a, b)}$. Máme $m = \frac{a}{\text{gcd}(a, b)}b$ a $\frac{a}{\text{gcd}(a, b)} \in \mathbb{Z}$, tedy m je násobek b , symetricky také $m = \frac{b}{\text{gcd}(a, b)}a$ a m je násobek a . Podle faktu 2b.9 tedy musí $\text{lcm}(a, b)$ dělit m , mimo jiné proto $\text{lcm}(a, b) \leq m$ (viz věta 2a.5 (ii), zde $m > 0$). Po dosazení dostáváme $\text{lcm}(a, b) \cdot \text{gcd}(a, b) \leq ab$.

b) Uvažujme číslo $d = \frac{ab}{\text{lcm}(a, b)}$, dle faktu 2b.9 je to přirozené číslo. Máme $a = \frac{\text{lcm}(a, b)}{b}d$ a $\frac{\text{lcm}(a, b)}{b} \in \mathbb{Z}$, tedy d je dělitel a , symetricky také $b = \frac{\text{lcm}(a, b)}{a}d$ a d je dělitel b . Podle definice proto $d \leq \text{gcd}(a, b)$. Po dosazení dostáváme $ab \leq \text{lcm}(a, b) \cdot \text{gcd}(a, b)$.

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

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.18, 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 $\text{lcm}(a, b) = \frac{ab}{\text{gcd}(a, b)}$ používat $\text{lcm}(a, b) = \frac{a}{\text{gcd}(a, b)}b$ či $\text{lcm}(a, b) = \frac{b}{\text{gcd}(a, b)}a$, protože tento postup nevyžaduje ukládání velkého čísla ab .

Takže $\text{lcm}(a, b)$ už řešit nemusíme, stačí najít efektivní způsob počítání $\text{gcd}(a, b)$. Podle faktu 2b.5 lze ignorovat znaménka, čímž máme polovinu problému vyřešenou. Když dále vezmeme v úvahu fakt 2b.4, tak nám vlastně zbývá vyřešit problém nalezení gcd dvou různých kladných čísel. Vzhledem k symetrii situace si je můžeme označit tak, že $a > b > 0$.

Klíčem je následující pozorování.

Lemma 2b.11.

Nechť $a, b \in \mathbb{Z}$ a $b \neq 0$, nechť $r = a \bmod b$. Pak platí následující:

- (i) $d \in \mathbb{N}$ je společný dělitel a, b právě tehdy, když je to společný dělitel b, r .
- (ii) $\text{gcd}(a, b) = \text{gcd}(b, r)$.

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

(i) \implies : 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) \impliedby : Důkaz je obdobný.

(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 algoritmus. Namísto hledání gcd pro dvojici $a > b > 0$ nám stačí hledat gcd pro odpovídající čísla $b > r$, nic nám ale nebrání aplikovat naše lemma znovu, najít $r' = b \bmod r$ a namísto dvojice $b > r$ hledat gcd pro $r > r'$. Takto můžeme pokračovat.

Protože se v každém kroku to menší číslo dále zmenší, ale nikdy není záporné, tak tento postup nemůže trvat do nekonečna, ale musí se zarazit. Kdy se tak stane? Kdy vlastně nemůžeme lemma použít? Když některé z čísel (či obě) opustí \mathbb{N} , což se nejdříve stane tomu menšímu, tedy zbytku po dělení. Zbytek po dělení opustí \mathbb{N} tehdy, je-li nulový, takže opakujeme lemma tak dlouho, dokud nenarazíme na nulový zbytek, $\gcd(x, 0)$ pak hravě určíme podle faktu 2b.4. Tím dostáváme algoritmus k nalezení $\gcd(a, b)$ pro $a > b$. Ukážeme jej na příkladě.

! Příklad 2b.b: Chceme najít $\gcd(408, 108)$.

Máme $408 = 3 \cdot 108 + 84$, proto $\gcd(408, 108) = \gcd(108, 84)$.

Máme $108 = 1 \cdot 84 + 24$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24)$.

Máme $84 = 3 \cdot 24 + 12$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24) = \gcd(24, 12)$.

Máme $24 = 2 \cdot 12 + 0$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24) = \gcd(24, 12) = \gcd(12, 0) = 12$.

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

△

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 po faktu 2a.12, budeme předpokládat nějakou implementaci procesu nalezení q, r .

S Algoritmus 2b.12.

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: $k := k + 1, r_{k-1} = q_k \cdot r_k + r_{k+1}$

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.13 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 $\gcd(408, 108)$:

$$\begin{array}{|c|} \hline a, b \\ \hline 408 \\ \hline 108 \\ \hline \end{array} \quad 408 \bmod 108 = 84 \quad \Rightarrow \quad \begin{array}{|c|} \hline a, b \\ \hline 408 \\ \hline 108 \\ \hline 84 \\ \hline \end{array}$$

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 $\gcd(408, 108)$.

$$\begin{array}{|c|} \hline a, b \\ \hline 408 \\ \hline 108 \\ \hline \end{array} \Rightarrow \begin{array}{|c|} \hline a, b \\ \hline 408 \\ \hline 108 \\ \hline 84 \\ \hline \end{array} \Rightarrow \begin{array}{|c|} \hline a, b \\ \hline 408 \\ \hline 108 \\ \hline 84 \\ \hline 24 \\ \hline \end{array} \Rightarrow \begin{array}{|c|} \hline a, b \\ \hline 408 \\ \hline 108 \\ \hline 84 \\ \hline 24 \\ \hline 12 \\ \hline \end{array} \Rightarrow \begin{array}{|c|} \hline a, b \\ \hline 408 \\ \hline 108 \\ \hline 84 \\ \hline 24 \\ \hline 12 \bullet \\ \hline 0 \\ \hline \end{array}$$

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

$$\begin{array}{ccc} 408 & 108 & 84 \\ & \longleftarrow & \uparrow \\ & & 408 \bmod 108 = 84 \end{array}$$

Takto pokračujeme:

408 108 84 24 12• 0

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

△

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

Věta 2b.14.

Euklidův algoritmus skončí pro libovolný vstup $a > b > 0$ 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 $r_{k+1} < r_k$ neboli jde o klesající posloupnost nezáporných čísel. Pokud bychom naše předchozí úvahy o nemožnosti najít nekonečnou takovou posloupnost oděli do matematického hávu, budeme mít důkaz ukončení algoritmu. Na to budeme připraveni po kapitole 8 o indukci, takže se má čtenář na co těšit, viz například 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. To se obvykle dělá matematickou indukcí.

Důkaz (poučný): 1) Uvažujme nějaký běh algoritmu pro jistá vstupní data $a > b > 0$, který vytvoří čísla r_k pro $k = 0, 1, \dots, K, K + 1$, přičemž $r_{K+1} = 0$.

Tvrdíme, že následující platí pro všechna $k \in \{1, \dots, K + 1\}$:

• $V(k)$: Jestliže $r_{k-1} > 0$, pak $\gcd(r_{k-1}, r_k) = \gcd(a, b)$.

(0) Pro $k = 1$ to platí, neboť $r_0 = a$ a $r_1 = b$. Takže $\gcd(r_0, r_1) = \gcd(a, b)$.

(1) Nechť $k \in \{1, \dots, K\}$, a předpokládejme, že platí $V(k)$, tedy $\gcd(r_{k-1}, r_k) = \gcd(a, b)$ pokud $r_{k-1} > 0$. Chceme ukázat platnost vlastnosti $V(k + 1)$.

Pokud $r_{(k+1)-1} = r_k \leq 0$, tak je předpoklad implikace nepravdivý a tedy celá implikace pravdivá, $V(k + 1)$ platí.

Nechť tedy $r_k > 0$. Pak algoritmus neskončil a vytvořil $r_{k+1} = r_{k-1} \bmod r_k$, také $r_{k-1} > r_k > 0$, tedy implikace indukčního předpokladu $V(k)$ je splněna a tedy $\gcd(r_{k-1}, r_k) = \gcd(a, b)$. Podle lemma 2b.11 také máme $\gcd(r_k, r_{k+1}) = \gcd(r_{k-1}, r_k)$, proto $\gcd(r_k, r_{k+1}) = \gcd(a, b)$ a tedy $V(k + 1)$ platí.

Tím je vlastnost V dokázána.

V okamžiku, kdy algoritmus skončil, je na výstupu číslo r_K . Podle faktu 2b.4 a vlastnosti $V(K + 1)$ je $r_K = \gcd(r_K, 0) = \gcd(r_K, r_{K+1}) = \gcd(a, b)$. □

Objevila se nám tu matematická indukce, která je v diskrétní matematice významným nástrojem. Protože se na ni chceme pořádně podívat dříve, než ji budeme hlouběji používat, odložíme další zkoumání tohoto algoritmu do kapitoly 16. Zde se jen zmíníme, že dalším významným aspektem, který se u algoritmů studuje, je rychlost. U Euklidova algoritmu se dá přibližně říct, že počet operací nutných k výpočtu (což zhruba odpovídá času běhu algoritmu) je úměrný číslu $[\log(b)]^2$. Z hlediska computer science je jednodušší hovořit o bitech zápisu čísla, můžeme například říct, že při práci s n -bitovými čísly je potřeba zhruba n^2 základních operací. V kapitole 11b si o náročnosti povíme víc, pak budeme říkat, že náročnost Euklidova algoritmu je $O(\log_2^2(b))$.

Zajímavé je, že se zde neobjevuje a . Je to ale vcelku pochopitelné, protože hned prvním krokem algoritmu přejdeme ke dvojici b, r , kde číslo r je z rozsahu $\{0, 1, \dots, b - 1\}$, takže velikost a přestává hrát roli.

Protože je tento algoritmus užitečný, lidé přemýšleli nad jeho urychlením. 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 čísly, pak aplikujeme opakovaně druhý či třetí vzorec, dokud nedostaneme dvě sudá čísla, to zase redukuje dělením dvěma a pořád dokola.

Zpracovat se dá také na procesu nalézání zbytku. Dá se ukázat ([cite]), že při výpočtu Euklidova algoritmu vznikají s vysokou pravděpodobností malá q (pravděpodobnosti pro $q = 1, 2, 3, 4$ jsou po řadě 41.5%, 17.0%, 9.3%, 5.9%), jinými slovy v polovině případů lze čekat $q = 1$ či $q = 2$, což jsou případy, kdy se opravdu vyplácí hledání q a r odečítáním.

Nejrychlejší má být verze, kdy hledáme i „záporné zbytky“, tedy pracujeme s rozkladem $a = qb+r$, kde tentokrát chceme $-\frac{b}{2} \leq r \leq \frac{b}{2}$. Ona čísla r pak klesají rychleji ([cite]). Ukážeme si to na příkladě.

Příklad 2b.c: Zkusíme najít $\gcd(408, 108)$ metodou nejmenších zbytků.

Nejmenší zbytek se najde tak, že se podíl $\frac{a}{b}$ nezaokrouhluje dolů, ale k nejbližšímu celému číslu, někdy se to značí $\lfloor \frac{b}{a} \rfloor$. Jinak je algoritmus obdobný.

Krok 1: $\frac{408}{108} = 3.78\dots$, tedy $q = 4$ a $408 = 4 \cdot 108 + (-24)$.

Krok 2: Hledáme $\gcd(108, -24) = \gcd(108, 24)$: $\frac{108}{24} = 4.5$, tedy $q = 4$ a $108 = 4 \cdot 24 + 12$.

Krok 3: Hledáme $\gcd(24, 12)$: $\frac{24}{12} = 2$, tedy $q = 2$ a $24 = 2 \cdot 12 + 0$. Výpočet skončil, $\gcd(408, 108) = 12$.

Je vidět, že oproti standardnímu algoritmu (viz příklad 2b.b) jsme ušetřili jeden krok.

△

V zásadě lze ale říct, že lépe než k $\log_2^2(b)$ se stejně nedostaneme.

2b.15 Poznámka: Z praktického programátorského pohledu je zajímavé si všimnout, že algoritmus je schopen pracovat i v případě, že jej nakrmíme čísla $a < b$. V takovém případě totiž vychází $a = 0 \cdot b + a$, tedy bereme $r = a$. Co udělá algoritmus? Pro přehlednost si teď jména proměnných algoritmu značíme velkými písmeny, ať je odlišíme od obsahu. Výchozí stav je $A = a$, $B = b$ a algoritmus spočítá $R = a$. Pak nastane posun registrů $A := B = b$, $B := R = a$ a začne se znovu, tentokrát s hodnotami $A = b$ a $B = a$, kde už máme $A > B$. Takže algoritmus si v případě zlomyslného zadání v prvním cyklu čísla srovná podle velikosti.

Co program udělá, když mu podstrčíme dvě stejná čísla? Ve stavu $A = a$, $B = a$ najde $R = a \bmod a = 0$, pak udělá posun $A := B = a$ a $B := R = 0$, čímž skončí a oznámí nám výsledek $A = a$, což je správná odpověď.

A co záporné vstupy? Pro $b \neq 0$ lze modulus (zbytek po dělení) vždy najít a je nezáporný, takže nejpozději po druhém kroku už algoritmus pracuje s kladnými čísly a vše probíhá normálně, i klíčové lemma 2b.11 platí pro záporná čísla. 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:

$$\begin{array}{ccccccccccc} -108 & -408 & 300 & 192 & 108 & 84 & 24 & 12 & 0 & & \end{array}$$

V opačném pořadí to je mnohem kratší.

$$\begin{array}{ccccccc} -408 & -108 & 24 & 12 & 0 & & \end{array}$$

Celkově se dá říct, že algoritmus funguje pro libovolné nenulové vstupy, je ale rozumné si hlídat, aby bylo $|a| > |b|$, případné prohození dvou čísel nás moc nezaměstná.

Nabízí se otázka, proč jsme se ve výkladu omezovali na případ $a > b > 0$, když algoritmus funguje obecně? Důvodem je, že je pak jednodušší jej analyzovat, proto je už tradicí pracovat s $a > b > 0$.

△

Tak jsme se naučili hledat efektivně největší společný dělitel (tedy i nejmenší společný násobek) a vrátíme se zase k teorii.

Věta 2b.16. (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 $a, b \neq 0$.

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 nespĺňuje 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.17.

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 $A, B \in \mathbb{Z}$.

Všechna čísla ve tvaru $Aa + Bb$ pro nějaká $A, B \in \mathbb{Z}$ jsou pak násobky $\gcd(a, b)$.

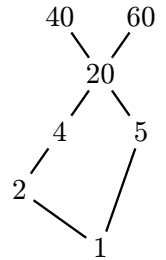
Protože $\gcd(a, b) = Aa + Bb$, tak pomocí důsledku 2a.3 hned dostáváme

Důsledek 2b.18.

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

Tím se nám mimo jiné rozluštila otázka ohledně struktury množiny společných dělitelů, viz 2b.3. Zůstala tam otevřena otázka, zda a kam se sbíhají různé stromečky směrem nahoru. Poslední důsledek říká, že všichni společní dělitelé a, b musí dělit $\gcd(a, b)$, čili číslo $\gcd(a, b)$ se stává oním cílem pro všechny cestičky směrem vzhůru v obrázku. Jako příklad vidíme vpravo množinu společných dělitelů čísel 40 a 60.

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.



Bezoutova identita je dost možná to nejužitečnější tvrzení, které v této kapitole najdeme. Ukážeme si několik věcí, které se s ním dají udělat.

Zkušenost nám říká, že pokud obecně číslo d dělí součin ab , tak nemusí dělit ani jedno z čísel, viz třeba případ $d = 4$, $a = 6$, $b = 10$. Pokud by ovšem číslo d „nemělo společnou část“ s číslem a , matematicky řečeno pokud by bylo s a nesoudělné, tak už bychom čekali, že jej „najdeme v b “ neboli že d dělí 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.19. (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): 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 $1 = \gcd(d, a) = Dd + Aa$. Pak $b = Ddb + Aab$, tedy $b = Ddb + Akd$, tedy $b = (Db + Ak)d$, přičemž díky $b, k, A, D \in \mathbb{Z}$ také $Db + Ak \in \mathbb{Z}$. To ukazuje, že d dělí b . □

Studenti se toto lemma mnohdy pokoušejí 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.20.

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.7 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.21.

Nechť $a_1, \dots, a_m \in \mathbb{N}$ 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.22.

Nechť $a, b \in \mathbb{Z}$. Pak pro každé $a, b, k \in \mathbb{N}$ 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: (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.6. Na toto cvičení odkážeme i ohledně důkazu části (ii). \square

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.

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 uhadneme $12 = 3 \cdot 24 + (-1) \cdot 60$. 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 $\gcd(408, 108) = 4 \cdot 408 + (-15) \cdot 108$.

\triangle

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: V průběhu Euklidova algoritmu jsme přecházeli od čísla k číslu. Všimneme si, že ta první dvě, se kterými začínáme, umíme vyjádřit jako lineární kombinaci a a b .

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

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

V prvním kroku algoritmu jsme odečetli třikrát 108 od 408. My ovšem také umíme odečítat rovnice, přičemž určitě budeme chtít zachovat čísla 108 a 408:

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

$$108 = 0 \cdot 408 + 1 \cdot 108 \quad / \times 3$$

$$84 = 1 \cdot 408 + (-3) \cdot 108$$

Dostáváme tak Bezoutovo vyjádření pro nové číslo 84. V levém sloupci vidíme přesně tabulku, kterou jsme měli v Euklidově algoritmu pro hledání $\gcd(408, 108)$. Proč to tak nedotáhnout do konce?

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

$$108 = 0 \cdot 408 + 1 \cdot 108 \quad / \times 3$$

$$84 = 1 \cdot 408 + (-3) \cdot 108 \quad / \times 1$$

$$24 = (-1) \cdot 408 + 4 \cdot 108 \quad / \times 3$$

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

Dostali jsme přesně to vyjádření, které jsme hledali.

\triangle

Tento postup ukazuje, že si v průběhu Euklidova algoritmu můžeme rovnou vytvářet správné koeficienty. Vidíme, že čísla 408 a 108 se jen kopírovala, to podstatné se dělo s koeficienty u nich. Stačí si proto zavést další dva registry, nazveme je A_k a B_k , které na začátku nastavíme jako v příkladu a na konci algoritmu nám dají, co potřebujeme. Klíčové pozorování: Když jsme odčítali určitou rovnici, tak jsme v ní všechny důležité části (levou „Euklidovskou“ stranu, koeficienty napravo) násobili stejným číslem, tím, které pocházelo z dělení se zbytkem nalevo. Takže jakmile v Euklidově algoritmu najdeme q z rozkladu $a = qb + r$, tak jej rovnou použijeme i pro pomocné registry, které se dopočítávají stejným vzorcem jako číslo nalevo.

S Algoritmus 2b.23.

Rozšířený Euklidův algoritmus pro nalezení $\gcd(a, b) = Aa + Bb$ pro $a, b \in \mathbb{N}$, $a > b$.

Verze 1.

Inicializace: $r_0 := a$, $r_1 := b$, $k := 0$,
 $A_0 := 1$, $A_1 := 0$, $B_0 := 0$, $B_1 := 1$.

Krok: $k := k + 1$, $q_k = \lfloor \frac{r_{k-1}}{r_k} \rfloor$,

$r_{k+1} := r_{k-1} - q_k r_k$,
 $A_{k+1} := A_{k-1} - q_k A_k$,
 $B_{k+1} := B_{k-1} - q_k B_k$.

Opakovat dokud nenastane $r_{k+1} = 0$.

Pak $\gcd(a, b) = r_k = A_k a + B_k b$.

Verze 2.

procedure *gcd-Bezout* (a, b : integer, $a > b > 0$)

$A_0 := 1$; $A_1 := 0$; $B_0 := 0$; $B_1 := 1$;

repeat

$q = \lfloor \frac{a}{b} \rfloor$;

$r = a - q \cdot b$;

$r_a := A_0 - qA_1$;

$r_b := B_0 - qB_1$;

$a := b$; $b := r$;

$A_0 := A_1$; $A_1 := r_a$;

$B_0 := B_1$; $B_1 := r_b$;

until $b = 0$;

output: a, A_0, B_0 ;

△

Poznamenejme, že pořad 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.24 Ruční výpočet.

Najdeme $\gcd(408, 108)$ a vyjádříme jej jako lineární kombinaci 408 a 108.

Nejtradičnější je, když se jednotlivé cykly algoritmu zapisují do řádků, podobně jako u Euklidova algoritmu, zde si ovšem musíme pamatovat tři čísla. Pro pomocné proměnné známe počáteční hodnoty. Může pomoci, když si představíme, že vedle tradičního „Euklidovského“ sloupce přidáme jednotkovou matici.

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

Teď najdeme částečný podíl $q = \lfloor \frac{408}{108} \rfloor = 3$. Bývá zvykem si to q do tabulky poznamenat, ale není to třeba. Já to tady budu dělat, aby měl čtenář přehled, co se děje. Teď ve všech třech sloupcích počítáme tak jako v levém (viz pozorování výše), tedy odečteme trojnásobek čísla dole od čísla nahoře. Vlastně to znamená, že jakoby od prvního řádku odečteme trojnásobek druhého, tím vznikne nový řádek.

Je zde jasná podoba s postupem v příkladě 2b.e, vlastně si v naší tabulce kódujeme odčítání rovnic, však jsme také zvyklí, že si při práci s lineárními rovnicemi stačí hlídat měnící se koeficienty.

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	

Pokud vám to trochu připomíná řádkové úpravy s maticemi (odečítání násobku řádku od jiného), tak to je výborný způsob, jak si algoritmus zapamatovat. V kapitole 4 o diofantických rovnicích uvidíme, že to navíc není náhodná podobnost, ale je tu souvislost.

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.

Můžeme si ověřit, že opravdu v každém řádku funguje ona lineární kombinace, například $24 = (-1) \cdot 408 + 4 \cdot 108$.

Existují i verze stručnější, ale bývají zase náchylnější na chybu, tento algoritmus je vhodným kompromisem a navíc nabízí zajímavé souvislosti, ke kterým se dostaneme v dalších kapitolách.

Bezoutova identita byla dokázána pro všechna celá čísla a, b , ale náš algoritmus jsme zavedli jen pro $a > b > 0$. Jak se najde vyjádření $\gcd(a, b) = Aa + Bb$ pro případná záporná čísla? Máme dvě možnosti. Jedna je zbavit se znamének podle faktu 2b.5, tedy aplikovat standardní postup na čísla $|a|$ a $|b|$, a výsledek pak zpětně adaptovat na původní zadání. To je velmi snadné, stačí selský rozum.

Druhá varianta je využít již dříve diskutovaného faktu, že vlastně tento algoritmus funguje pro libovolná čísla na vstupu (kromě $b = 0$). Obojí ukážeme.

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

Víme, že $\gcd(-108, 408) = \gcd(|-108|, |408|) = \gcd(408, 108)$, tou druhou rovností jsme si to upravili, aby $a = 408$ bylo větší než $b = 108$. Nyní aplikujeme běžný Euklidův rozšířený algoritmus (viz výše) a dostaneme $\gcd(408, 108) = 12 = 4 \cdot 408 + (-15) \cdot 108$. Teď už jen vyrobíme správná znaménka u čísel:

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

Dal by se napsat obecný algoritmus na určení A, B v závislosti na znaménkách, ale snad to není nutné.

Teď si vyzkoušíme běh algoritmu s původními čísly:

a, b	A	B	
-108	1	0	
408	0	1	-1
300	1	1	1
108	-1	0	2
84	3	1	1
24	-4	-1	3
12●	15●	4●	2
0	-34	-9	

Takže to taky šlo, získali jsme správné vyjádření $\gcd(-108, 408) = 15 \cdot (-108) + 4 \cdot 408$. Poznamenejme, že záporné číslo $q = -1$ v řádku u 408 znamená, že se druhý řádek jednou přičte k prvnímu.

Ještě si vyzkoušíme blahodárný vliv prohození čísel na vstupu tak, aby $|a| > |b|$.

a, b	A	B	
408	1	0	
-108	0	1	-3
84	1	3	-2
60	2	7	1
24	-1	-4	2
12●	4●	15●	2
0			

Potvrzuje se vyjádření $\gcd(408, -108) = 4 \cdot 408 + 15 \cdot (-108)$. Při tomto postupu jsme dvakrát násobek přičítali místo odečítali, bylo to o krok kratší.

Na závěr si vyzkoušíme postup, který by měl být nejrychlejší, tedy použití obecných zbytků. Protože se v této situaci zdá, že používání q spíš mate, tak se na něj vykašleme a prostě budeme vždy pracovat se situací, že se opakovaným odečítáním či přičítáním druhého řádku k prvnímu snažíme dosáhnout co nejmenšího čísla (v absolutní hodnotě) v levém sloupci, v tomto případě klidně i záporného, pro nově vzniklý řádek.

a, b	A	B
408	1	0
-108	0	1
-24	1	4
-12	-4	-15
0		
12●	4●	15●

Zrychlení na dvojnásobek už docela jde, jen jsme pak ještě museli změnit znaménko řádku. Někteří lidé ale dělají při ručním zpracování záporných vstupů více chyb (i já jsme musel občas přemýšlet), takže u zkoušky bych spíš radil tu úplně první verzi. Samozřejmě počítači znaménka nevadí, ten by rád tu poslední.

△

Takže algoritmus umíme. Ještě bychom se potřebovali ujistit, že opravdu funguje, a také se o něm dají říct různé zajímavé věci (třeba že ze všech možných Bezoutových vyjádření nabízí to nejekonomičtější, tedy s nejmenšími možnými čísly), ale to už vyžaduje docela dobré pochopení indukce. Odložíme to proto do kapitoly 16.

Na závěr kapitoly se ještě vrátíme k prvočíslnům a nesoudělnosti. Lemma 2b.21 nám umožňuje testovat nesoudělnost „po částech“.

Lemma 2b.25.

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): $1) \implies$: 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 pročísl p , které dělí k , to pak je i společným dělitelem d a ab . Lemma 2b.21 ovšem tvrdí, že si p musí vybrat, ýekněme, že $p \mid a$. 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 indukci zobecní na více čísel. Přivádí nás to k dalšímu tématu, které se ještě bude hodit. Máme-li více čísel n_1, \dots, 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 zúčastněných čísel. Stačí si zvolit $n_1 = 1$, pak jediný společný dělitel čísel n_1, n_2, \dots, 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, \dots, n_m jsou **po dvou nesoudělná**. Znamená to, že si můžeme z množiny $\{n_1, \dots, n_m\}$ 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.26.

Nechť $n_1, \dots, n_m \in \mathbb{N}$ jsou po dvou nesoudělná. Pak je n_1 nesoudělné s číslem $n = n_2 \cdot n_3 \cdot \dots \cdot n_m$.

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 prvočísl p , které dělí d , to pak musí dělit i n_1 a $n = n_2 \cdot n_3 \cdot \dots \cdot n_m$. Podle lemma 2b.21 by tedy p dělilo některé n_j a máme spor s $\gcd(n_1, n_j) = 1$.

□

Cvičení

Cvičení 2b.1 (rutinní, poučné): Dokažte, že pro $a \in \mathbb{N}$ platí $\gcd(a, 0) = |a|$ a $\gcd(a, a) = \text{lcm}(a, a) = |a|$ (viz fakt 2b.4).

Cvičení 2b.2 (rutinní, poučné): Dokažte, že pro $a \in \mathbb{Z}$ platí:

- (i) $\gcd(a, ka) = |a|$ a $\text{lcm}(a, ka) = |ka|$ pro libovolné $k \in \mathbb{Z}$;
(ii) $\gcd(a, a^k) = |a|$ a $\text{lcm}(a, a^k) = |a^k|$ pro libovolné $k \in \mathbb{N}$.

Cvičení 2b.3 (poučné): Přesvědčte se, že odhady $\gcd(a, b) \leq \min(|a|, |b|)$ a $\text{lcm}(a, b) \geq \max(|a|, |b|)$ (viz fakt 2b.6) 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 $\text{lcm}(a, b)$ 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 (poučné): Nechť $a, b \in \mathbb{Z}$. Dokažte, že jestliže $\gcd(a, b) = 1$, pak $\text{lcm}(a, b) = |a| \cdot |b|$.

Cvičení 2b.6 (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.7 (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.8 (poučné):

Jak zobecníme pojem gcd a lcm pro více čísel? Pro nenulová $a_1, \dots, a_n \in \mathbb{Z}$ definujeme $\gcd(a_1, a_2, \dots, a_n)$ jako největší přirozené číslo d splňující vlastnost, že $d \mid a_i$ pro všechna i , obdobně $\text{lcm}(a_1, a_2, \dots, a_n)$ definujeme jako nejmenší přirozené číslo d splňující vlastnost, že $a_i \mid d$ 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.9 (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.10 (poučné): Nechť $a_1, a_2, \dots, a_n \in \mathbb{N}$.

Rozmyslete si, zda platí $\text{lcm}(a_1, a_2, \dots, a_n) = \frac{a_1 \cdot a_2 \cdot \dots \cdot a_n}{\gcd(a_1, a_2, \dots, a_n)}$.

Rozmyslete si, zda platí, že když jsou a_i po dvou nesoudělná, pak $\text{lcm}(a_1, a_2, \dots, a_n) = a_1 \cdot a_2 \cdot \dots \cdot a_n$.

Pro případný důkaz platnosti viz cvičení 2b.4.

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 $d \leq |a|$ a víme, že také $|a| \mid a$, 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 $\text{lcm}(a, a)$ je obdobný.

2b.2: Příklad $a = 0$ 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): Příklad $a = 0$ 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 $\text{lcm}(a, ka) = \gcd(a, 0) = 0 = |ka|$. 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 $d \leq |a|$, tak žádné větší číslo než $|a|$ v té množině není.

Obdobný rozbor ukáže $\text{lcm}(a, ka) = |ka|$.

(ii): Podobně jako (i), zde není nutno řešit $k = 0$.

2b.3: Obecně platí $\gcd(a, b) \leq \max(|a|, |b|)$ a $\text{lcm}(a, b) \geq \min(|a|, |b|)$.

2b.4: (i):

420	1	0	
231	0	1	1
189	1	-1	1
42	-1	2	4
21●	5●	-9●	2
0			

$\gcd(2^2 \cdot 3 \cdot 5 \cdot 7, 3 \cdot 7 \cdot 11) = 3 \cdot 7 = 21$
 $\text{lcm}(2^2 \cdot 3 \cdot 5 \cdot 7, 3 \cdot 7 \cdot 11) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 4620$
 $\gcd(420, 231) = 21 = 5 \cdot 420 + (-9) \cdot 231$

(ii): Hledat $\gcd(|-60|, |-156|) = \gcd(156, 60)$.

156	1	0	
60	0	1	2
36	1	-2	1
24	-1	3	1
12●	2●	-5●	2
0			

$\gcd(-2^2 \cdot 3 \cdot 5, -2^2 \cdot 3 \cdot 13) = 2^2 \cdot 3 = 12$
 $\text{lcm}(-2^2 \cdot 3 \cdot 5, -2^2 \cdot 3 \cdot 13) = 2^2 \cdot 3 \cdot 5 \cdot 13 = 780$
 $\gcd(-60, -156) = 12 = 2 \cdot 156 + (-5) \cdot 60$

(iii): Hledat $\gcd(|-131|, 118) = \gcd(131, 118)$.

131	1	0	
18	0	1	1
13	1	-1	9
1●	-9●	10●	13
0			

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

2b.5: Stačí použít $\text{lcm}(a, b) \cdot \gcd(a, b) = |a| \cdot |b|$.

Správný matematický přístup je využívat již odvedené práce.

2b.6: (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.7: Podle Bezouta $\gcd(a, b) = A_b a + B b$ a $\gcd(a, c) = A_c a + C c$.

Pak $\gcd(a, b) \gcd(a, c) = a(A_b A_c + A_b C c + A_c B b) + b c B C$. $\gcd(a, bc)$ dělí a i bc , tudíž musí dělit i ten součin.

2b.8: 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.9: 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.18 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.10: Je dobré začít s co nejméně čísly, tedy třemi, a pracujeme se k situaci, kdy lze použít příslušný vzorec pro dvě čísla, kde je dokázán: $\text{lcm}(a, b, c) = \text{lcm}(\text{lcm}(a, b), c) = \frac{\text{lcm}(a, b)c}{\gcd(\text{lcm}(a, b), c)} = \frac{abc}{\gcd(a, b)\gcd(\text{lcm}(a, b), c)}$.

Mohlo by platit $\frac{abc}{\gcd(a, b)\gcd(\text{lcm}(a, b), c)} = \frac{abc}{\gcd(a, b, c)}$ neboli $\gcd(a, b)\gcd(\text{lcm}(a, b), c) = \gcd(a, b, c)$? 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 $\gcd(\text{lcm}(a, b), c) = 1$. 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 $\text{lcm}(2, 3, 4) = 12$, zatímco $\frac{2 \cdot 3 \cdot 4}{\gcd(2, 3, 4)} = 24$.

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 $\text{lcm}(a_1, a_2, \dots, a_n) = a_1 \cdot a_2 \cdots a_n$ platí.

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

Nejprve spočítáme $\det(A) = -1$, takže 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.

2c.2 Řádkové úpravy matic nad celými čísly

Klíčem ke Gaussově eliminační metodě (GEM) jsou řádkové operace s maticemi. Ve světě reálných čísel používáme tři:

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

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.

Dalším užitečným pozorováním je, že tyto operace lze realizovat tak, že danou matici násobíme zleva „transformačními maticemi“.

• Aby se u matice přičtel c -násobek řádku i k řádku j , použijeme matici, která vznikne přidáním čísla c na pozici j, i do jednotkové matice. Pokud například vynásobíme 3×3 matici zleva maticí

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 5 & 1 \end{pmatrix}$$

tak to v původní matici přičte pětinasobek druhého řádku (pětka je ve druhém sloupci) ke třetímu řádku (pětka je na třetím řádku).

• Aby se u matice vynásobil řádek i číslem c , použijeme matici, která vznikne z jednotkové matice nahrazením diagonální jedničky číslem c v řádku i .

• Transformační matice, která způsobí prohození řádků i a j , vznikne prohozením řádků i a j v jednotkové matici.

To, že lze operace vrátit, se do jazyka transformačních matic přeloží tak, že ke každé transformační matici existuje jiná transformační matice, která je k ní inverzní.

Například víme, která operace je inverzní k přičtení c -násobku řádku k jinému, proto by mělo platit, že matice

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -5 & 1 \end{pmatrix}$ je inverzní k matici $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 5 & 1 \end{pmatrix}$. Ověřte si jejich vynásobením, že je to pravda.

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 matice, takže lze pomocí nich snadno spočítat determinant větších matc.

Gaussova eliminační metoda dokáže pomocí těchto tří operací převést 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. Z praktického pohledu není třeba vyžadovat u pivotů jedničky, budeme proto uvažovat následující slabší pojem. Pro zjednodušení nebudeme vypisovat, že se u $n \times m$ matice automaticky berou řádkové indexy i, j z rozmezí $1, \dots, n$ a sloupcový index k se bere z rozmezí $1, \dots, m$.

Definice 2c.3.

Řekneme, že je matice A 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 $k \leq N$.

Řečeno slovy, taková matice má nulové řádky (pokud nějaké jsou) soustředěny ve své spodní části a nenulové řádky mají svůj první nenulový prvek vždy doprava od prvního nenulového prvku předchozího řádku. Tento tvar je ideální pro rychlé řešení soustav lineárních rovnic či počítání determinantu.

Algoritmus GEM na převod libovolné dané matice pomocí základních tří řádkových operací do řádkově redukovaného tvaru je všeobecně znám, nás zajímá, co se s ním stane v situaci, kdy žijeme ve světě celých čísel.

Mějme tedy matici s celočíselnými prvky a zamysleme se na třech řádkových operacích.

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.

Třetí 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, matice vzniklá nahrazením jedné z jedniček číslem c^{-1} by měla být celočíselná. Takových celých čísel ovšem mnoho není.

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

Celočíselné řádkové operace:

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

Násobení řádku jedničkou není zrovna nejužitečnější, z praktického pohledu je tedy jen jediná rozumná možnost násobení řádku, jmenovitě změna znamének u všech jeho prvků.

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 celočíselnými řádkovými úpravami nemění.

Omezení našich možností ohledně druhé operace 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 celých 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 redukcí prvního sloupce matice do potřebného tvaru odečtením dvojnásobku prvního řádku od druhého.

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

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

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

Dostali jsme správnou inverzní matici. Je to náhoda? Ne tak úplně. Základem Gaussovy eliminace je schopnost přeměnit daný sloupec matice na tvar, kdy je v prvním řádku číslo a pod ním samé nuly. Tento postup lze úspěšně vykonat i ve světě celých čísel.

S Algoritmus 2c.4.

Pro převedení matice, jejíž sloupec j 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 j je roven $\begin{matrix} d \\ 0 \\ \vdots \\ 0 \end{matrix}$ pro nějaké $d \in \mathbb{Z}$.

1. Pokud je ve sloupci j nejvýše jedno nenulové číslo, případným prohozením řádků jej přemístíte do prvního řádku.

Algoritmus skončil.

2. Nechť se nejmenší nenulové číslo sloupce j nachází v řádku i , označme jej d (říkáme mu „pivot“). Odečtete vhodné násobky řádku i od ostatních řádků tak, aby ve sloupci j 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 $a = cd + r$, kde $0 \leq r < |d|$. Odečteme-li c -násobek řádku i od řádku j , vznikne v příslušném sloupci číslo $a - dc = r$, 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 $|d_1| > |d_2| > |d_3| > \dots$. Kdyby algoritmus nikdy neskončil, vznikla by nekonečná klesající posloupnost nezáporných celých čísel, což je nemožné. Algoritmus tedy nutně musí dříve či později skončit.

Jeho běh lze urychlit, když si uvědomíme, že nám nic nebrání hledat záporné zbytky po dělení. To znamená, že v kroku 2 lze vyžadovat, aby ve sloupci j vznikla v řádcích jiných než i čísla, jejichž absolutní hodnota je nejvýše $\frac{1}{2}|d|$. Protože se následný pivot hledá mezi těmito čísly, dostáváme nerovnost $|d_{k+1}| < \frac{1}{2}|d_k|$. To nám umožňuje udělat jednoduchý odhad výpočetní náročnosti. Předpokládejme, že bylo třeba opakovat krok 2 celkem N -krát. To znamená, že máme pivoty d_N, d_{N-1}, \dots, d_1 splňující onu podmínku s polovinami, také $|d_N| \geq 1$. Máme tedy $|d_{N-1}| \geq 2|d_N| \geq 2$, $|d_{N-2}| \geq 2|d_{N-1}| \geq 4$, $|d_{N-3}| \geq 2|d_{N-2}| \geq 8 = 2^3$ a tak dále, snadno si rozmyslíme, že $|d_1| \geq 2^{N-1}$. Odtud $N \leq \log_2(|d_1|)$.

To znamená, že počet opakování kroku 2 je úměrný logaritmu nejmenšího čísla daného sloupce, což prakticky znamená počtu cifer v tomto čísle. Logaritmické náročnosti máme velmi rádi, takže to je dobrá zpráva. Pak je ovšem nutno vzít v úvahu, že v každém kroku 2 musíme manipulovat s řádky matice, množství operací na jeden krok 2 je úměrné počtu prvků v matici, což může být hodně. To není až tak dobrá zpráva. Navíc je známo, že při operacích mají prvky tendenci ke zvětšování, což je další výpočetní komplikace. Provozovat tento algoritmus s většími čísly se tedy může protáhnout.

Poznamenejme, že podobný odhad pro počet iterací lze odvodit i pro standardní Euklidův algoritmus, ale dá to více práce. Rozdíl je v tom, že tam máme pro zbytky odhad $r_{k+1} < r_k$, citelně tam chybí ta polovina. Můžete se podívat na větu 6a.xx.

Jakmile máme potvrzenou platnost algoritmu 2c.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 2c.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. Víme, že celočíselné řádkové úpravy mohou změnit jen znaménko determinantu, čímž dostáváme zajímavou situaci. Pokud se nám při eliminaci objeví na diagonále jiné (celé!) číslo než ± 1 , tak už matice nemůže mít determinant roven ± 1 a tudíž není invertibilní, proto nám ani nevádí, že se pomocí celočíselné GEM nedostaneme k jednotkové matici.

Druhá (a poslední) alternativa je, že redukovaná matice má na diagonále čísla ± 1 . Pak je invertibilní, navíc nám celočíselné řádkové operace umožňují změnit na diagonále znaménka na plusová a vidíme, že při eliminaci dokážeme coby pivoty získávat jedničky. Pak je možné převést danou čtvercovou matici na jednotkovou, jinými slovy, lze získat její inverzní matici obvyklým eliminačním postupem.

Máme tedy potvrzeno, že i ve světě celých čísel nám postup $(A|E_n) \mapsto (E_n|A^{-1})$ spolehlivě poskytuje inverzní matice vždy, když existují.

2c.6 Řádková eliminace a Euklidův algoritmus

Pokud čtenáře při přemýšlení nad algoritmem 2c.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●	-1●	2●
0	5	-9

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

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

První matice je zajímavá, protože reprezentuje soustavu dvou rovnic, $1 \cdot x + 0 \cdot y = 108$ a $0 \cdot x + 1 \cdot y = 60$, pokud se tedy smíříme s tím, že sloupec pravých stran přilepujeme k matici soustavy nalevo. To funguje obecně, dva řádky, kterými začínáme Euklidův algoritmus, odpovídají soustavě dvou rovnic.

$$\left(\begin{array}{c|cc} a & 1 & 0 \\ \hline b & 0 & 1 \end{array} \right) \iff \begin{array}{l} 1 \cdot x + 0 \cdot y = a \\ 0 \cdot x + 1 \cdot y = b \end{array}$$

Tato soustava má evidentně jediné řešení, $x = a$ a $y = b$. Jak jsme viděli, Euklidův algoritmus vlastně odpovídá převodu této matice na řádkově redukovaný tvar. Vzniká tak nová soustava rovnic, nás zajímá druhá rovnice, která je $(-1) \cdot x + 2 \cdot y = 12$. Protože jsou celočíselné řádkové operace ekvivalentní, musí mít nová soustava stejnou množinu řešení jako ta původní, takže musí také platit $(-1) \cdot 108 + 2 \cdot 60 = 12$. Z teorie víme, že výsledné číslo v prvním sloupci musí být $\gcd(108, 60)$, a pomocí soustav rovnic teď vidíme, proč Euklidův algoritmus dává Bezoutovu identitu.

Tento pohled je užitečný ze dvou důvodů. Za prvé, z pohledu řádkových úprav se nemusíme omezovat na hledání nezáporných zbytků, díky čemuž dostáváme onu rychlejší verzi algoritmu. U našeho příkladu bychom tedy v prvním kroku neodčítali druhý řádek od prvního jednou, ale dvakrát.

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

Ušetřili jsme jeden krok algoritmu. Ještě je třeba upravit znaménko v prvním řádku, ale to je snadné.

Protože vždy měníme jen jeden řádek, je možné tento postup zachytit obdobnou tabulkou jako předtím.

a, b	A	B
108	1	0
60	0	1
-12	1	-2
0		
12●	-1●	2●

Kromě návodu na zrychlení nabízí pohled skrze soustavy další podnět: Jak to bude fungovat s více čísly? Ukáže se, že velice dobře. Začneme definicí.

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.

U menších čísel je opět možné nejprve u všech čísel najít prvočíselné rozklady a poté si vyzobat společné členy, tak snadno nahlédneme, že třeba $\gcd(12, -18, 24) = 6$. U větších čísel už je to nepraktické a zamysleme se nad napodobením postupu nastíněného výše.

Jsou-li dána čísla a_1, \dots, a_n , je vždycky možné sestavit soustavu

$$\begin{array}{l} 1 \cdot x_1 + 0 \cdot x_2 + \dots + 0 \cdot x_n = a_1 \\ 0 \cdot x_1 + 1 \cdot x_2 + \dots + 0 \cdot x_n = a_2 \\ \vdots \\ 0 \cdot x_1 + 0 \cdot x_2 + \dots + 1 \cdot x_n = a_n \end{array}$$

a přejít k její rozšířené matici (s pravými stranami nalevo)

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

Pomocí algoritmu 2c.4 ji umíme převést na tvar

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

Protože původní soustava má zcela zjevně jediné řešení, jmenovitě $x_i = a_i$, musí mít stejné řešení i soustava odpovídající výsledné matici, dostáváme tedy $d = A_1 a_1 + \dots + A_n a_n$. To vypadá nadějně, úplně jako Bezoutova identita. Ještě musíme zjistit, co je vlastně to výsledné číslo d . Postup je obdobný jako v případě dvou čísel, potřebujeme lemma.

Lemma 2c.7.

Pro všechna čísla $q, a_1, \dots, a_n \in \mathbb{Z}$ platí následující:

- (i) $\gcd(a_1, a_2, \dots, a_n) = \gcd(b_1, b_2, \dots, b_n)$ pro libovolnou permutaci b_1, \dots, b_n čísel a_1, \dots, a_n ;
- (ii) $\gcd(a_1, a_2, \dots, a_n) = \gcd(-a_1, a_2, \dots, a_n)$;
- (iii) $\gcd(a_1, a_2, \dots, a_n) = \gcd(a_1, a_2 - qa_1, \dots, a_n)$.

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).

(iii): 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. □

Lemma nám vlastně říká, že když na matici aplikujeme celočíselné řádkové operace, tak se v jejích sloupcích nezmění největší společný dělitel. Pečlivého čtenáře možná napadne, že jsme v lemma dokázali jen případy, kdy měníme znaménko v prvním řádku a odčítáme první od druhého. Není to ale problém, protože ostatní operace se zvládnou pomocí části (i). Například pokud chceme změnit znaménko třetího řádku, tak jej nejprve prohodíme s prvním, pak použijeme (ii) a zase prohodíme první s třetím, lemma zaručuje, že se během těchto operací nezmění gcd. Podobně ukážeme, že lze beztréstně odečítat i násobek libovolného řádku od jiného.

Podívejme se tedy na závěr. Pokud aplikujeme lemma na všechny řádkové úpravy, které nás dovedly k matici v tvaru

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

pak musí platit $\gcd(a_1, \dots, a_n) = \gcd(d, 0, \dots, 0)$. To číslo napravo ovšem snadno určíme přímo z definice a dostáváme, že $\gcd(a_1, \dots, a_n) = |d|$.

Dokázali jsme tak následující tvrzení.

Věta 2c.8.

Uvažujme čísla $a_1, a_2, \dots, a_n \in \mathbb{Z}$, z nichž alespoň jedno je nenulové.

Algoritmus 2c.4 aplikovaný na matici

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

vede na matici

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

kde $|d| = \gcd(a_1, \dots, a_n)$ a platí $d = A_1 a_1 + \dots + A_n a_n$.

Příklad 2c.b: Najdeme $\gcd(364, -234, 156)$.

Sestavíme matici a upravíme ji do žádaného tvaru.

$$\left(\begin{array}{c|ccc} 364 & 1 & 0 & 0 \\ -234 & 0 & 1 & 0 \\ 156 & 0 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{c|ccc} 52 & 1 & 0 & -2 \\ -78 & 0 & 1 & 1 \\ 156 & 0 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{c|ccc} 52 & 1 & 0 & -2 \\ -26 & 1 & 1 & -1 \\ 0 & -3 & 0 & 7 \end{array} \right) \sim \left(\begin{array}{c|ccc} 0 & 3 & 2 & -5 \\ -26 & 1 & 1 & -1 \\ 0 & -3 & 0 & 7 \end{array} \right)$$

Z druhého řádku máme $-26 = 1 \cdot 364 + 1 \cdot (-234) + (-1) \cdot 156$, takže můžeme udělat závěr, že $\gcd(364, -234, 156) = 26 = (-1) \cdot 364 + (-1) \cdot (-234) + 1 \cdot 156$.

Vidíme, že posledním kroku stačilo spočítat první sloupec, zbytek matice už novou informaci nepřinesl, podobně jako u standardního rozšířeného Euklidova algoritmu není třeba dopočítávat řádek začínající nulou.

△

Nabízí se samozřejmě možnost upravit v případě nutnosti znaménko v onom důležitém řádku vynásobením celého řádku číslem -1 tak, aby d vycházelo kladné. Nemuseli bychom pak v teoretických tvrzeních používat absolutní hodnotu. Přiznám se ale, že se mi kvůli tomu nechce znovu opisovat celou matici, takže to raději řeším až na konci jako v příkladě.

Potvrzením korektnosti algoritmu jsme v zásadě dokázali, že Bezoutova identita platí i pro více čísel než jen dvě.

Věta 2c.9.

Nechť $a_1, \dots, a_n \in \mathbb{Z}$.

Pak existují celá čísla A_1, \dots, A_n taková, že $\gcd(a_1, \dots, a_n) = \sum_{i=1}^n A_i a_i$.

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 .

Na souvislost s maticemi se podíváme ještě jednou a hlouběji v kapitole 4e.

2d. 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 $a_n x^n + \dots + a_1 x + a_0$, 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 $a_i x_i$ 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 svázané. Konkrétně, jedna ze základních vlastností polynomů nad reálnými čísly je, že formální polynomy (tedy výrazy typu $a_n x^n + \dots + a_0$) 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 $a_n x^n + \dots + a_0$ 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.11). Při vzájemném poměrování kandidátů na zbytek se namísto velikosti používá stupeň. Shrňme si to základní ve větě.

Věta 2d.1.

Uvažujme polynomy p, q nad \mathbb{R} . Pak platí následující:

- (i) $\text{st}(pq) = \text{st}(p) + \text{st}(q)$.
- (ii) Existují jediné polynomy d a r takové, že $p = d \cdot q + r$ a $\text{st}(r) < \text{st}(q)$.
- (iii) Polynom p má nejvýše $\text{st}(p)$ 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 $q \mid p$ 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 npracuje.

Obdobně můžeme definovat $\mathbb{Z}[x]$ jako množinu všech polynomů $a_n x^n + \dots + a_0$, 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 2d.a: Uvažujme polynomy $p = 4x^2 + 14x + 6$ a $q = 4x^2 - 2x - 2$. Máme rozklady

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

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

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

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 $\text{gcd}(4x^2 + 14x + 6, 4x^2 - 2x - 2) = x + \frac{1}{2}$. Příklad také ukazuje, že v \mathbb{Z} už toto není možné. Protože toto je jen natukávací kapitola, opustíme toto téma a zvědavého čtenáře odkážeme na knihu o maticích, kde se s polynomy nad celými čísly dělají zajímavé věci.