6. Dělitelnost a prvočísla

Tato kapitola má jednak význam vysoce praktický pro computer science, zároveň je to také jemný úvod do oblasti zvané teorie čísel, která se zabývá mimo jiné prvočísly a má za sebou úctyhodnou historii a zajímavé a hluboké výsledky, o některých se zde občas lehce zmíníme. Velice úzce souvisí s kapitolou následující, dokonce to původně byla jedna kapitola, než narostla tak, že už to na jednu bylo moc.

6a. Dělitelnost

Zde se pořádně matematicky podíváme na situace, kdy jedno číslo dělí druhé, mnohé z toho čtenář jistě zná.

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

Let $a, b \in \mathbb{Z}$. We say that a **divides** b, denoted $a \mid b$, if there is $k \in \mathbb{Z}$ such that $b = k \cdot a$.
Then we say that a is a **factor** of b and that b is a **multiple** of a.

Příklad 6a.a: Evidentně $3 \mid 12$, protože $12 = 4 \cdot 3$, na druhou stranu neplatí $5 \mid 13$.
△

Dělitelnost je velice důležitý pojem v teorii čísel a pro některá a existují algoritmy, jak snadno poznat, zda dělí určité b, čtenář jistě zná kritérium pro dělitelost dvěma (číslo je sudé), pro další viz cvičení 6a.11 a 7a.4 a poznámka 7a.14. Teď se podíváme, jaké vlastnosti pojem dělitelnosti splňuje, některé věci jsou jasné hned.

Fakt 6a.1.
Pro každé $a \in \mathbb{Z}$ platí:
(i) $1 \mid a$;
(ii) $a \mid a$;
(iii) $a \mid 0$.

Důkaz je tak snadný, že jej s důvěrou necháme jako cvičení 6a.2. Začátečníka může zarazit, že Fakt lze aplikovat i na $a = 0$. 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, $0 \mid 0$.

Toto ukazuje, že pojem dělitelnosti se zásadně liší od dělení jako matematické operace, protože samozřejmě nulou dělit nelze nic, ani nulu. Pojem dělitelnosti $a \mid b$ se ptá, zda lze jedno číslo nějak získat z druhého, zkoumáme tedy jistý vzájemný vztah. Na druhou stranu když napíšeme $\frac{a}{b}$, tak nás zajímá výsledek jakési operace, což nás (až na pár výjimek) nebude v této kapitole zajímat. Silně čtenáři doporučujeme se zlomkům vyhýbat, zejména v důkazech, protože svádí na zcestí. I my je zde použijeme výjimečně.

Příklad 6a.b: Zvolme si nějaké $d \in \mathbb{N}$. Kolik existuje násobků d, které jsou menší než nějaké $n \in \mathbb{N}$? Jinými slovy, kolik z přirozených čísel z $\{1, 2, \ldots, n\}$ je dělitelných d?

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

Práci s dělitelností nám usnadní užitečná pravidla.

Věta 6a.2.
Nechť $a, b, c \in \mathbb{Z}$.
(i) Jestliže $a \mid b$ a $a \mid c$, pak $a \mid (b + c)$.
(ii) Jestliže $a \mid b$, pak $a \mid (nb)$ pro všechna $n \in \mathbb{Z}$.
(iii) Jestliže $a \mid b$ a $b \mid c$, pak $a \mid c$.
(iv) $a \mid b$ právě tehdy, když $|a| \mid |b|$.
(v) Jestliže $a \mid b$ a $b \neq 0$, tak $|a| \leq |b|$.

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 $b + c = (k + l)a$ a $(k + l) \in \mathbb{Z}$, proto podle definice $a \mid (b + c)$.

(ii) a (iii) viz cvičení 6a.3.

(iv): Viz cvičení 6a.4, ukazuje se tam, že na znaménku opravdu nezáleží.

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

□

S **6a.3 Poznámka o důkazech:** Důkazy byly velice snadné a vysoce poučné. Měly stejné schéma: Začalo se danými předpoklady, z nich se získala nějaká informace podle definice dělitelnosti. Pak se tato informace použila k bližšímu nahlédnutí na objekt, který jsme měli zkoumat (třeba na $b + c$ v prvním tvrzení). Toto schéma bude čtenáři dobře sloužit v důkazech jednodušších tvrzení ze všech oborů matematiky.

Využijeme důkazu tvrzení (i) k upozornění na dva faktory, které někdy působí začátečníkům potíže.

1. Aby se ze studenta stal zkušený důkazovník, musí se mimo jiné naučit, kdy má svobodu volby písmenka a kdy ne. Občas je u studenta možné vidět takovýto začátek důkazu: Máme dáno, že $b = k \cdot a$ a $c = k \cdot a$. To první je dobře, druhé ne. Ve chvíli, kdy píšeme ten první vztah, můžeme na místě k dát libovolné písmeno (kromě a, b), zde máme svobodu, proč tedy nevzít tradiční k.

Jakmile ale napíšeme, že $b = k \cdot a$, tak už k získalo nějakou pevnou hodnotu, kterou sice neznáme, ale ona existuje (závisí na a, b), takže k už není k dispozici. Proto když začneme pracovat s číslem c, musíme nutně zvolit v definici dělitelnosti jiné písmenko. Jinak bychom totiž dostali $b = k \cdot a$, $c = k \cdot a$ a tedy vynutili $b = c$, což rozhodně nemusí být pravda.

2. V důkazech tohoto typu se často objevuje klasická začátečnická chyba, kdy důkaz začne slovy „nechť $b+c = k \cdot a$“. Pokud ještě student následně napíše, že z předpokladu získá $b = k \cdot a$, tak najel do slepé uličky, protože jedno k hraje dvě rozdílné role a to už nerozchodí.

Představme si tedy studenta trochu chytřejšího, který k předpokladu $b + c = ka$ ještě přidá, že $b = xa$ a $c = ya$ pro nějaká $x, y \in \mathbb{Z}$. Jednoduchou úpravou pak získá rovnost $k = x + y$, tu dvakrát podtrhne a je spokojen. Bohužel však nemá platný důkaz. Začal totiž něčím, co nemá k dispozici, co naopak chce získat na konci.

Samozřejmě že když důkaz vymýšlíme, tak si položíme otázku, kam chceme dojít, a odpověď $b + c = ka$ nás pak navádí správným směrem, Po rozmyšlení situace je pak ale třeba začít psát pořádně důkaz, tedy začít tím, co je dáno, a skončit tím, co chceme dokázat, jak jsme to udělali v dukazu Faktu výše.

△

Vraťme se k tvrzením z Faktu. Bod (iv) ukazuje, že u dělitelnosti stačí dobře rozumět, jak funguje na $\mathbb{N}_0$, a už jí rozumíme všude. Někteří autoři by tuto kapitolu dělali výhradně pro čísla z $\mathbb{N}$, čímž by se také elegantně vyhnuli problémům s nulou, která se občas musí dělat jako zvláštní případ. Bylo by to pak snažší, ale my budeme potřebovat některé z poznatků pro všechna čísla ze $\mathbb{Z}$, tak to tu probereme v plné obecnosti.

Zkušenost naznačuje, že směr v (i) nejde obecně obrátit, například $3 \mid (2 + 4)$, ale neplatí $3 \mid 2$ ani $3 \mid 4$. Trocha experimentování ukáže, že když platí $a \mid (b + c)$, ale neplatí výrok „$a \mid b$ a $a \mid c$“, tak se musí pokazit obě jeho části, nelze to zkazit jen u jedné. To se občas hodí, tak si to vyjádříme. Přidáme i zajímavou kombinaci tvrzení z (i) a (ii), mohlo by vám to připomenout lineární kombinace z lineární algebry.

Důsledek 6a.4.
Nechť $a, b, c \in \mathbb{Z}$.
(i) Jestliže $a \mid b$ a $a \mid c$, pak $a \mid (mb + nc)$ pro všechna $m, n \in \mathbb{Z}$.
(ii) Jestliže $a \mid (b + c)$ a $a \mid b$, pak $a \mid c$.

Druhé tvrzení plyne hned, protože z $a \mid b$ díky Větě 6a.2 (ii) dostaneme $a \mid (-b)$ a tudíž podle Věty 6a.2 (i) musí a dělit číslo $(b + c) + (-b) = c$. Nemusíme tedy jít do hloubky, do detailů, stačilo chytře poskládat již dokázané výsledky. Tomuto se někdy říká „měkký důkaz“ a máme je rádi, je samořejmě efektivní nedělat věci znovu, když už můžeme využít plodů naší předchozí práce. Zde by mimochodem důkaz přes definici také nebyl těžký, zkuste si to jako cvičení.

Teď si připomeneme něco z kapitoly 4b.

! **Věta 6a.5.**
Relace $a \mid b$ je částečné uspořádání na $\mathbb{N}$ a na $\mathbb{N}_0$.

Důkaz (rutinní)**:** Důkaz provedeme společně pro obě množiny. Reflexivita plyne z Faktu 6a.1 (ii), tranzitivita zase z Věty 6a.2 (iii). Zbývá antisymetrie.

Nechť $a, b \in \mathbb{N}_0$ splňují $a \mid b$ a $b \mid a$. Pak $b = ka$ a $a = lb$ pro nějaké $k, l \in \mathbb{Z}$. Pokud by alespoň jedno z čísel a, b bylo nula, pak z našich dvou rovností okamžitě dostáváme, že i druhé je nula. Dostáváme tedy $a = b$ a antisymetrie pro tento případ funguje.

Zbývá prozkoumat situaci, kdy jsou obě a, b kladné, tudíž musí být kladné i k, l, tedy $k, l \in \mathbb{N}$. Když z první rovnosti dosadíme do druhé, dostaneme $a = kla$, také $a \neq 0$, tedy $kl = 1$. Protože $k \geq 1$, máme $1 = kl \geq l \geq 1$, tedy $l = 1$, odtud $k = 1$. Proto $a = b$. Antisymetrie dokázána.

□

Rozhodně neplatí, že by relace $a \mid b$ byla uspořádáním na $\mathbb{Z}$, tam ztrácíme antisymetrii. Například $13 \mid (-13)$ a $(-13) \mid 13$, ale neplatí $-13 = 13$. To je jeden z důvodů, proč se s dělitelností pracuje lépe jen na $\mathbb{N}$. Připomeňme také, že v kapitole jsme viděli, že uspořádání dělitelností není lineární ani dobré.

Při práci s dělitelností se vyplatí umět dělit se zbytkem, tedy pro daná a, d umět spočítat $\frac{a}{d} = q + \frac{r}{d}$. Protože zde se dělení a zlomkům vyhýbáme, přepíšeme tento vztah do jazyka násobení.

! **Věta 6a.6.** (o dělení se zbytkem) (division theorem) (division algorithm)
Nechť $a, d \in \mathbb{Z}$, $d \neq 0$. Pak existují $q \in \mathbb{Z}$ a $r \in \mathbb{N}_0$ takové, že $a = qd + r$ a $0 \leq r < |d|$.
Čísla q a r jsou jednoznačně určena.

Důkaz (dobrý, poučný)**:** Neprve dokážeme existenci q a r pro $d > 0$, a to hned dvakrát za cenu jednoho důkazu, no neberte to.

1) První verze začíná důkazem, že to umíme pro $a, d > 0$, a to indukcí. Vhodná formulace vyžaduje trochu experimentování, autorovi přijde jako dobré východisko tato vlastnost:

$V(n)$: Pro každé $a \in \{1, 2, \ldots, n\}$ a pro každé $d \in \mathbb{N}$ existují q, r dle předpisu.

Dokážeme ji pro $n \in \mathbb{N}$.

(0) $n = 1$: Platí tvrzení pro $a = 1$? Buď $d = 1$, pak $q = 1$ a $r = 0$ splňují zadání ($1 = 1 \cdot 1 + 0$ a $r < d$), nebo $d > 1$, pak $q = 0$ a $r = a = 1$ (ano, $1 = 0 \cdot d + 1$ a $r < d$). Platí.

(1) Pro $n \in \mathbb{N}$ předpokládejme platnost $V(n)$, tedy že umíme dělit se zbytkem čísla $a = 1, 2, \ldots, n$. Dokážeme teď $V(n+1)$. Vezměme tedy libovolné $a \in \{1, 2, \ldots, n, n+1\}$. Jestliže $a \leq n$, pak dělit umíme dle indukčního předpokladu. Co když $a = n + 1$?

Jestliže $d > a$, pak dáme $q = 0$, $r = a$ a je hotovo, $a = 0 \cdot d + a$ a $a < d$.

Jestliže $d = a$, pak dáme $q = 1$, $r = 0$ a je hotovo.

Jestliže $d < a$, pak uvažujme $b = a - d$. Máme $1 \leq b \leq n$, proto dle indukčního předpokladu $b = q'd + r$, kde $0 \leq r < d$. Pak ovšem $a = b + d = (q' + 1)d + r$ a je to hotovo, pořád $0 \leq r < d$.

Tím je dokázána možnost dělení se zbytkem pro $a, d > 0$. Pro $a = 0$ je to triviální ($q = r = 0$), zbývá případ $a < 0$, $d > 0$.

Uvažujme $(-a) > 0$. Podle první části důkazu je $-a = q'|d| + r'$. Jestliže $-a = q'd$, pak $a = (-q')d$ a je to hotovo, $r = 0$. Druhá alternativa je, že $0 < r' < d$. Pak $a = (-q')d - r' = (-q')d - d + d - r' = (-q' - 1)d + (d - r')$ a $r = d - r'$ splňuje $0 < r < d$, hotovo.

2) Teď to zkusíme jinak: Budeme postupně odečítat $d > 0$ od a a čekat, až to dopadne dobře. To se nejlépe udělá najednou chytrou definicí množiny. Uvažujme tedy množinu $M = \{a - qd;\ q \in \mathbb{Z},\ a - qd \geq 0\}$. Tato množina je neprázdná: Jestliže je $a \geq 0$, tak volba $q = 0$ ukazuje $a \in M$. Jestliže $a < 0$, pak stačí zvolit $q = -a$ a máme $a - qd = a(1 - d) \geq 0$, neboť díky $d \geq 1$ máme $(1 - d) \leq 0$.

Už z definice jsou všechny prvky M nezáporné, jsou to samozřejmě celá čísla. Máme tedy neprázdnou podmnožinu $\mathbb{N}_0$, vezmeme její nejmenší prvek r. Evidentně $r \geq 0$ a $a = q_0 d + r$ pro nějaké $q_0 \in \mathbb{Z}$. Platí $r < d$? Kdyby ne, pak $a - q_0 d \geq d$, proto $r_1 = a - (q_0 + 1)d \geq 0$, tedy $r_1 \in M$ a $r_1 < r$, spor s tím, že r je nejmenší prvek M. Proto $r \geq d$ nemůže nastat.

3) Máme tedy dokázánu existenci pro $d > 0$. Pokud $d < 0$, pak $-d > 0$ a dle první části 1) nebo 2) najdeme q, r tak, aby $a = q(-d) + r$, pak $a = (-q)d + r$.

4) Jednoznačnost: Předpokládejme, že $a = qd + r = q'd + r'$, kde $0 \leq r, r' < |d|$. Pak $qd + r = q'd + r'$, proto $(q - q')d = r - r'$. Jelikož $|r - r'| < |d|$, musí být i $|q - q'| \cdot |d| < |d|$, což znamená $|q - q'| < 1$. Ale $(q - q') \in \mathbb{Z}$, proto $q - q' = 0$ a tedy i $q = q'$. Pak také $r = r'$.

□

Všimněte si, že první důkaz potřeboval k platnosti princip matematické indukce a druhý existenci nejmenšího prvku pro $M \subseteq \mathbb{N}$. My už víme, že tyto dvě věci jsou ekvivalentní, viz Věta 5a.8.

Definice.
Nechť $a, d \in \mathbb{Z}$, $d \neq 0$. Číslu r z Věty 6a.6 říkáme **zbytek** (**remainder**) při dělení a číslem d a značíme jej $r = a \bmod d$, čteno „r je a modulo d“.
Číslu q říkáme **částečný podíl** (**quotient**).

Pro q značení zavádět nemusíme, protože máme následující.

Fakt 6a.7.
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 $0 \leq |\frac{r}{d}| < 1$. Čísla q a $\varepsilon = |\frac{r}{d}|$ pak spolu s Faktem 2b.15 (i) a (ii) dávají žádaný výsledek.

□

Dále se budeme pro jednoduchost soustředit na případ $d > 0$. Fakt nabízí možnost, jak se k číslům z Věty 6a.6 dostat, nejprve spočítáme (pro $d > 0$) $q = \lfloor \frac{a}{d} \rfloor$, pak $r = a - qd$. Z hlediska rychlosti výpočtu je klíčové to dělení, kdy je tradiční školní algoritmus zoufale pomalý pro větší čísla. Dá se mu zcela vyhnout metodou z důkazu Věty, kdy prostě necháme od čísla $a > 0$ odečítat číslo d tak dlouho, dokud nedostaneme $0 \leq a - d - \cdots - d < d$. U $a < 0$ zase přičítáme d, dokud nebude $d > a + d + \cdots + d \geq 0$. Počet přičtení/odečtení dá q. To ale znamená, že tento algoritmus funguje rychle jen pro a, d podobná, v případě velkého q by těch cyklů bylo příliš mnoho.

Obecně se tedy dělení vyhnout nelze a zajímavý přístup je najít nejprve nějak chytře $\frac{1}{d}$, protože násobení $a \cdot \frac{1}{d}$ už rychle umíme. 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 zákruty 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.

Příklad 6a.c: Zkusíme si dělení se zbytkem pro $a = 13$ a $d = 3$. Uhodneme, že $13 = 4 \cdot 3 + 1$ a $1 < 4$, proto je 1 zbytek po dělení čísla 13 číslem 3 čili $1 = 13 \bmod 3$, částečný podíl je $q = 4$. Nebo můžeme počítat $\lfloor \frac{13}{3} \rfloor = 4$ a $13 - 4 \cdot 3 = 1$.

Dělit kladná čísla se zbytkem umíme již ze základní školy, například povědomý výpočet napravo ukazuje, že $4147 \bmod 37 = 3$. U menších čísel to vidíme na první pohled, třeba $48 \bmod 16 = 0$ nebo $48 \bmod 15 = 3$. Jak to bude fungovat, když $a < 0$?

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

Pro $a = -13$ a $d = 3$ hravě uhodneme, že $-13 = (-5) \cdot 3 + 2$, tedy $= -13 \bmod 3 = 2$. Neplatí úvaha $-13 = (-4) \cdot 4 - 1$, tedy zbytek -1, konec konců $q = \lfloor \frac{-13}{3} \rfloor = \lfloor -4.33... \rfloor = -5$.

Obecně se dá dokázat, že jestliže pro $a > 0$ máme $a \bmod d = r > 0$, pak $(-a) \bmod d = d - r$ (viz Cvičení 6a.6). Je tedy možné použít běžné dělení se zbytkem pro kladná čísla a pak modifikovat zbytek.
△

Příklad 6a.d: Dělení se zbytkem nabízí efektivní algoritmus, jak najít zápis čísla n vzhledem k základu b. Ukážeme dvě verze, jednu s koeficienty pro matematickou práci a druhou efektivní pro programování. Nebudeme preferovat nějaký existující jazyk, raději použijeme pseudokód srozumitelný snad každému.

Verze 1.
Iniciace: $q_0 := n$, $k := -1$.
Krok: $k := k + 1$, $q_k = q_{k+1}b + a_k$.
Opakovat dokud nenastane $q_k = 0$.
Pak $n = (a_k \dots a_1 a_0)_b$

nebo

Verze 2.
`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:` $n = (a_k \dots a_1 a_0)_b$;

Z praktického hlediska je lepší přidat registr a ušetřit operace, tedy

$k := k + 1$;
$x := \lfloor \frac{q}{b} \rfloor$;
$a_k := q - xb$;
$q := x$;

Jako příklad si převedeme 86 do trojkové soustavy.
Iniciace: $q = 86$, $b = 3$, $k = -1$.
Krok 1: $k = 0$, $x = \lfloor \frac{86}{3} \rfloor = 28$, $a_0 = 86 \bmod 3 = 86 - 28 \cdot 3 = 2$, $q = 28$.
Krok 2: $k = 1$, $x = \lfloor \frac{28}{3} \rfloor = 9$, $a_1 = 28 \bmod 3 = 28 - 9 \cdot 3 = 1$, $q = 9$.
Krok 3: $k = 2$, $x = \lfloor \frac{9}{3} \rfloor = 3$, $a_2 = 9 \bmod 3 = 9 - 3 \cdot 3 = 0$, $q = 3$.
Krok 4: $k = 3$, $x = \lfloor \frac{3}{3} \rfloor = 1$, $a_3 = 3 \bmod 3 = 3 - 1 \cdot 3 = 0$, $q = 1$.
Krok 5: $k = 4$, $x = \lfloor \frac{1}{3} \rfloor = 0$, $a_4 = 1 \bmod 3 = 3 - 0 \cdot 3 = 1$, $q = 0$.
Konec, $86 = (10012)_3$.
Zkouška: $1 \cdot 3^4 + 0 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0 = 81 + 3 + 2 = 86$.

Zajímavou otázkou je, jak převádět (kladná) desetinná čísla. Jejich celou část převedeme algoritmem výše, zbývá vymyslet, jak převést část za desetinnou čárkou. K tomu je dobré nejprve pochopit, jak vlastně dotyčný algoritmus pro celá čísla funguje. 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 $n = \sum_{k=0}^{n} a_i b^i$. Chytře si to rozepíšeme:

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

Potřebujeme, aby se nám cifra a_0 z toho davu nějak vydělila, aby získala jiný charakter. To se stane, pokud n vydělíme číslem b. Dostaneme totiž číslo $\frac{n}{b} = a_k b^{k-1} + \cdots + a_2 b + a_1 + \frac{a_0}{b}$, přičemž 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.

Teď totéž zopakujeme s $a_k b^{k-1} + \cdots + a_2 b + a_1 = (a_k b^{k-2} + \cdots + a_2) b + a_1$ a dostaneme a_1 atd.

Nyní se podívejme na kladné číslo c menší než 1. Takové číslo se v b-soustavě napíše jako

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

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

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

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

△

! Příklad 6a.e: Zde si ukážeme několik praktických aplikací modula.

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

Označme $n = 10a + r$, přičemž a je to počáteční devítimístné číslo a $r = a \bmod 11$. Pak $a = 11k + r$, proto $n = 110k + 10r + r = 11(10k + r)$, tedy číslo dělitelné jedenácti. Jiný důkaz, možná rychlejší (viz příští kapitola): Podle definice máme $a \equiv r \pmod{11}$, také $10 \equiv (-1) \pmod{11}$, proto $10a + r \equiv (-1)r + r = 0 \pmod{11}$.

To znamená, že když nám někdo dá ISBN číslo, my jej zkusíme vydělit 11 a nevyjde to, tak už víme, že se někde stala chyba. Pokud by to vyšlo, tak je buď číslo dobře, nebo se pokazila víc než jedna cifra a zrovna tak šikovně, že to dělitelnost nezkazilo.

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

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

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

Výhody: h je na, rychle se počítá.

Nevýhoda: h není prostá, vznikají tzv. kolize. Jsou nutné strategie, co pak (např. metoda „první následující volné místo“).

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

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

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

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

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

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

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

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

Často se volí $c = 0$, tzv. čistě multiplikativní generátor, pak nechceme $x_k = 0$ a je snaha volit n, a tak, aby vznikl opravdu 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.

△

Následující fakt by měl být čtenáři po menším zamyšlení jasný.

Fakt 6a.8.
Nechť $a, b \in \mathbb{Z}$, $a \neq 0$. Pak $a \,|\, b$ právě tehdy, když $b \bmod |a| = 0$, tedy zbytek po dělení b číslem $|a|$ je 0.

Důkaz necháme jako cvičení 6a.5. Mimochodem, absolutní hodnota u a v textu tvrzení není nutná, protože jsme ve větě o dělení se zbytkem pracovali i se zápornými děliteli a není s nimi problém, ale v praxi stejně znaménko ignorujeme, takže jsme zvolili praktický pohled na věc.

Teď zavedeme nové užitečné pojmy.

! **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 trochu méně triviální odpovědi, třeba 20 jako společný dělitel a 120 jako společný násobek. Jak vlastně množiny všech společných násobků a společných dělitelů vypadají?

Pro každá dvě čísla $a, b \in \mathbb{Z}$ je 1 společným dělitelem, tudíž množina společných dělitelů je neprázdná. Pokud je jedno z čísel a, b nenulové, například a, pak každý společný dělitel d musí splňovat $d \leq |a|$, viz Věta 6a.2 (v). Proto je pak množina společných dělitelů konečná a tudíž má v $\mathbb{N}$ největší a nejmenší prvek.

Kdyby ale bylo $a = b = 0$, tak je společným dělitelem libovolné $d \in \mathbb{N}$, takže vlastně množina společných dělitelů je $\mathbb{N}$. To je nepříjemné a budeme se s tímto případem opakovaně nuceni vypořádávat zvlášť.

U společných násobků je rovněž třeba hlídat nuly, ale trochu jinak. Pokud jsou obě a, b nenulové, tak je $a \cdot b$ společným násobkem. Množina společných násobků je shora neomezená, protože máme-li společný násobek d, pak je i kd společným násobkem pro libovolné $k \in \mathbb{N}$. Množina společných násobků tedy nemá největší prvek, ale jako neprázdná podmnožina $\mathbb{N}$ má určitě prvek nejmenší (všimněte si, že i pro záporná a, b bereme v definici jen kladná čísla jako jejich společné dělitele či násobky).

Pokud je alespoň jedno z čísel a, b nulové, tak máme problém, protože jediným násobkem nuly je zase nula, což definice společného násobku nepřipouští. Množina společných násobků je v tomto případě prázdná.

! **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 $\gcd(0, 0) = 0$.

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

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

Tyto pojmy se dají zobecnit na více čísel, viz cvičení 6a.19.

Volby gcd a lcm pro výjimečné případy jsou vedeny snahou zachovat užitečné vlastnosti. V obou případech je zachován smysl, číslo 0 opravdu dělí 0 a je násobkem 0. U největšího společného dělitele je takových kandidátů nekonečně mnoho (to už jsme viděli), tam byla naše volba rozumná například proto, že teď máme obecně $\gcd(a, b) \leq |a|$ a $\gcd(a, b) \leq |b|$ pro všechna a, b včetně nulových, což je jistě příjemné. U společného násobku to bohužel nevyšlo, jediný násobek čísla 0 je zase 0, tudíž jsme v definici neměli na výběr a musíme se smířit s tím, že $|a| \leq \operatorname{lcm}(a, b)$ a $|b| \leq \operatorname{lcm}(a, b)$ platí jen pro nenulová a, b (musíme být proto opatrní).

Je to další ponouknutí, abychom pracovali jen s čísly $a, b \in \mathbb{N}$, často to bude možné a máme po problémech, ale ne vždy to jde.

Protože $\gcd(a, b)$ dělí a i b, tak pro nenulová a, b máme $\dfrac{a}{\gcd(a,b)} \in \mathbb{Z}$ a $\dfrac{b}{\gcd(a,b)} \in \mathbb{Z}$. To je zjevné, ale budeme to opakovaně používat, tak na to upozorňujeme. Vtělíme to do tvrzení s ještě jedním pozorováním.

! **Fakt 6a.9.**
Nechť $a, b \in \mathbb{Z}$, $a \neq b$. Pak jsou $\dfrac{a}{\gcd(a,b)}$ a $\dfrac{b}{\gcd(a,b)}$ nesoudělná celá čísla.

Důkaz (rutinní)**:** Předpokládejme, že číslo $d \in \mathbb{N}$ je společný dělitel $\dfrac{a}{\gcd(a,b)}$ a $\dfrac{b}{\gcd(a,b)}$. To znamená, že pro nějaká $k, l \in \mathbb{Z}$ máme $\dfrac{a}{\gcd(a,b)} = kd$ a $\dfrac{b}{\gcd(a,b)} = ld$. Pak $a = k[d \gcd(a, b)]$ a $b = l[d \gcd(a, b)]$, čili $d \gcd(a, b)$ je společný dělitel a, b. Protože $\gcd(a, b)$ je mezi společnými děliteli největší, musí být $d \leq 1$, což pro $d \in \mathbb{N}$ znamená nutně $d = 1$.

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

□

Intuitivně je to jasné, když vydělíme obě čísla tím, co mají společné, tak už v nich nic společného zbýt nemůže.

Další zkoumání těchto pojmů začneme pomocným tvrzením, které čtenář jistě zná z vlastní zkušenosti. Pokud je nějaké číslo d dělitelné čísly a, b, tak ještě to d nemusí být dělitelné číslem $a \cdot b$, ale určitě půjde vydělit číslem $\operatorname{lcm}(a, b)$.

Lemma 6a.10.
Nechť $a, b \in \mathbb{Z}$. Jestliže je d společný násobek a, b, pak $\operatorname{lcm}(a, b)$ dělí d.

Důkaz (poučný)**:** Jestliže $a = 0$ nebo $b = 0$, pak společné násobky neexistují a tvrzení platí automaticky. Předpokládejme tedy dále, že $a, b \neq 0$.

Protože je $\operatorname{lcm}(a, b)$ nejmenší společný násobek, musí platit $d \geq \operatorname{lcm}(a, b)$. Nechť podle věty o dělení $d = q \operatorname{lcm}(a, b) + r$. Protože a dělí $\operatorname{lcm}(a, b)$, tak dělí i $q \operatorname{lcm}(a, b)$, dělí rovněž d, proto podle Důsledku 6a.4 (ii) 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 $\operatorname{lcm}(a, b)$ je nejmenší společný násobek a $r < \operatorname{lcm}(a, b)$. Takže $r = 0$ a $d = q \operatorname{lcm}(a, b)$ pro nějaké $q \in \mathbb{Z}$.

□

Dá se to číst i jinak, ukazuje to, že množina společných násobků dvou čísel má zajímavou strukturu, všechny pocházejí od jednoho základního, nemůže se objevit nějaký úplně jiný. Lemma to dokázalo pro čísla kladná, platí to i obecně.

Fakt 6a.11.
Nechť $a, b, n \in \mathbb{Z}$. Jestliže $a \mid n$ a $b \mid n$, pak $\operatorname{lcm}(a, b) \mid n$.

Důkaz (rutinní, možná poučný)**:** Jestliže je $a = 0$ či $b = 0$, tak nutně i $n = 0$ a $\operatorname{lcm}(a, b) = 0$, tvrzení pak platí. Zbývá probrat případ, kdy $a, b \neq 0$.

Jestliže $a \mid n$ a $b \mid n$, pak také $a \mid |n|$ a $b \mid |n|$ (viz cvičení 6a.4), takže $|n|$ je společným násobkem a, b. Podle Lemma 6a.10 tedy musí platit $\operatorname{lcm}(a, b) \mid |n|$, proto i $\operatorname{lcm}(a, b) \mid n$.

□

Ukážeme ještě jedno zajímavé čtení tohoto faktu. Pro $a, b \neq 0$ je $\operatorname{lcm}(a, b)$ definován jako nejmenší prvek množiny společných násobků, přičemž „nejmenší“ je ve smyslu nerovnosti. Právě jsme se dozvěděli, že $\operatorname{lcm}(a, b)$ je také nejmenším prvkem množiny společných násobků vzhledem k relaci dělitelnosti. Obdobné tvrzení platí i pro $\gcd(a, b)$, ale tam je důkaz těžší a postupně se k němu propracujeme.

Naším cílem teď bude odvodit praktické postupy k nalezení $\gcd(a, b)$ a $\operatorname{lcm}(a, b)$. Nejprve si různými pozorováními zredukujeme obecnou situaci na případ $0 < b < a$. Začneme tím, že stačí umět hledat oba pojmy pro čísla z $\mathbb{N}_0$.

! **Fakt 6a.12.**
Nechť $a, b \in \mathbb{Z}$. Pak $\gcd(a, b) = \gcd(|a|, |b|)$ a $\operatorname{lcm}(a, b) = \operatorname{lcm}(|a|, |b|)$.

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

Společní dělitelé a, b jsou kladná čísla d splňující $d \mid a$ a $d \mid b$, což jsou podle Věty 6a.2 (iv) přesně čísla splňující $d \mid |a|$ a $d \mid |b|$. Množina společných dělitelů a, b je tedy stejná jako množina společných dělitelů $|a|, |b|$, tudíž se musejí rovnat i jejich největší prvky.

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

□

Hodnoty $\gcd(0, 0) = 1$ a $\operatorname{lcm}(0, 0) = 0$ známe z definice, snadno nalezneme i hodnoty pro další specifické případy.

! **Fakt 6a.13.**
Nechť $a \in \mathbb{N}$. Pak $\gcd(a, 0) = a$, $\operatorname{lcm}(a, 0) = 0$ a $\gcd(a, a) = \operatorname{lcm}(a, a) = a$.

Druhé tvrzení je přímo definice, důkaz ostatních je snadný a necháme jej jako cvičení 6a.10. Teď si dále zjednodušíme situaci.

! **Věta 6a.14.**
Nechť $a, b \in \mathbb{Z}$. Pak $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = |a| \cdot |b|$.

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

Označme $z = \dfrac{ab}{\gcd(a, b)}$, chceme ukázat, že je to $\operatorname{lcm}(a, b)$. Máme $z = \dfrac{a}{\gcd(a, b)} b$ a $\dfrac{a}{\gcd(a, b)} \in \mathbb{Z}$, tedy z je násobek b, a symetricky také $z = \dfrac{b}{\gcd(a, b)} a$ a z je násobek a. Podle Lemma 6a.10 tedy musí platit $z = q \operatorname{lcm}(a, b)$ pro nějaké $q \in \mathbb{N}$. Potřebujeme ukázat, že $q = 1$.

Všimněme si, že $\operatorname{lcm}(a,b) = \frac{z}{q} = \frac{ab}{q\gcd(a,b)}$. Když využijeme toho, že a i b dělí $\operatorname{lcm}(a,b)$, dostáváme $\frac{a}{q\gcd(a,b)} = \frac{\operatorname{lcm}(a,b)}{b} \in \mathbb{Z}$, tedy $q\gcd(a,b)$ dělí a, a symetricky $\frac{b}{q\gcd(a,b)} = \frac{\operatorname{lcm}(a,b)}{a} \in \mathbb{Z}$, tedy $q\gcd(a,b)$ dělí b. To znamená, že $q\gcd(a,b)$ je společný dělitel a,b, tudíž z definice gcd musí platit $q\gcd(a,b) \leq \gcd(a,b)$. Zároveň ale $q \in \mathbb{N}$, což znamená, že nutně $q = 1$.

2) Jsou-li a,b nenulové, ale některé z nich je záporné (či obě), pak výsledek vyplývá z Faktu 6a.12.

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

□

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

Zůstává otázka, jak najít $\gcd(a,b)$, podle Faktů 6a.12 a 6a.13 už víme, že to musíme hlavně vyřešit pro případ $a,b > 0$, $a \neq b$. Pro malá čísla se to často dělá rozkladem na prvočísla, jenže ten jsme ještě neprobrali a hlavně to je ukrutně výpočetně náročná úloha, tudíž neperspektivní. Existuje lepší způsob, populární a mocný Euklidův algoritmus. Je založen na následujícím pozorování.

!

Lemma 6a.15.
Nechť $a,b \in \mathbb{N}$, 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) $\gcd(a,b) = \gcd(b,r)$.

Důkaz (poučný)**:** Nechť $r = a \bmod b$. (i): $\Longrightarrow$: Je-li d společný dělitel a a b, pak dělí a i qb, tedy podle Důsledku 6a.4 (ii) musí dělit také r a je to společný dělitel b,r. $\Longleftarrow$: Důkaz je obdobný.

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

□

Toto lemma je klíčem k algoritmu. Namísto hledání gcd pro dvojici $a > b$ 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 6a.13. Tím dostáváme algoritmus k nalezení $\gcd(a,b)$ pro $a > b$. Ukážeme jej na příkladě.

! **Příklad 6a.f:** 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 $\gcd(408,108) = \gcd(108,84) = \gcd(84,24) = \gcd(24,12) = \gcd(12,0) = 12$.
Jako obvykle jsme neřešili, kde se ty rozklady berou, já jsem si je dělal tužkou přes $q = \lfloor \frac{x}{y} \rfloor$.
△

Algoritmus ukážeme 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 6a.7, budeme předpokládat nějakou implementaci procesu nalezení q,r.

S **Algoritmus 6a.16. Euklidův algoritmus** pro nalezení $\gcd(a,b)$ pro $a > b \in \mathbb{N}$.

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

△

nebo

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

Teď dokážeme, že algoritmus dělá, co má.

1) Algoritmus skončí: Variantem je r_k, to splňuje $r_1 > r_2 > r_3 > \cdots$ a zároveň $r_k \in \mathbb{N}_0$, proto musí dojít k terminační podmínce $r_k = 0$.

2) Algoritmus má na výstupu $\gcd(a,b)$: Pomocí indukce dokážeme následující
$V(k)$: Jestliže $r_k > 0$, pak $\gcd(r_k, r_{k+1}) = \gcd(a,b)$.
(0) Pro $k = 0$ to platí, neboť $r_0 = a$ a $r_1 = b$.
(1) Nechť $k \in \mathbb{N}_0$ a předpokládejme, že $\gcd(r_k, r_{k+1}) = \gcd(a,b)$ a $r_k > 0$.
Nechť také $r_{k+1} > 0$. Pak $r_k = qr_{k+1} + r_{k+2}$ podle věty o dělení a podle Lemma 6a.15 máme $\gcd(r_{k+1}, r_{k+2}) = \gcd(r_k, r_{k+1})$, spolu s indukčním předpokladem pak $\gcd(r_{k+1}, r_{k+2}) = \gcd(a,b)$, tedy $V(k+1)$ platí.

$V(k)$ je dokázáno. V okamžiku terminace máme $r_k > 0$ a $r_{k+1} = 0$, tedy podle $V(k)$ a Faktu 6a.13 je $\gcd(a,b) = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k$.

! 6a.17 Ruční výpočet.

Při ručním počítání zachycujeme stavy registrů tabulkou, existuje několik verzí. Začneme verzí podrobnou, která přesně ilustruje běh algoritmu. Každý jeho krok dělá dvě věci, nejprve spočítá r a pak si připraví půdu pro nové kolo posunem dat v registrech. Totéž uděláme v tabulce, nejprve si spočítáme r a zapíšeme jej do nového řádku jako novou hodnotu b, pak doplníme na nový řádek starou hodnotou b jako nové a a tím se připravíme na další kolo. Ukážeme si to pro náš předchozí příklad.

Najdeme $\gcd(408, 108)$ pomocí Euklidova algoritmu.

a	b
408	108

$408 \bmod 108 = 84 \implies$

a	b
408	108
	84

a	b
408	108
108	84

$108 \bmod 84 = 24 \implies$

a	b
408	108
108	84
	24

a	b
408	108
108	84
84	24

$84 \bmod 24 = 12 \implies$

a	b
408	108
108	84
84	24
	12

a	b
408	108
108	84
84	24
24	12

$24 \bmod 12 = 0 \implies$

a	b
408	108
108	84
84	24
24	12
	0

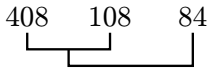
a	b
408	108
108	84
84	24
24	12
12•	0

Když počítáme takto ručně, tak se nemusíme přesně držet algoritmu a lze vynechat tu poslední tabulku. Jakmile se nám objeví na řádku nula, tak si přečteme hodnotu $\gcd(a,b)$ v políčku nad tou nulou.

Zásadní nedostatek tohoto algoritmu je, že se v něm každé číslo objevuje dvakrát, což je zbytečné. Mnohem jednodušší je použít jen jeden sloupec a pracovat vždy se dvěma posledními čísly. Opět si najdeme $\gcd(408, 108)$.

a,b	$\implies$	a,b	$\implies$	a,b	$\implies$	a,b	$\implies$	a,b
408		408		408		408		408
108		108		108		108		108
		84		84		84		84
				24		24		24
						12		12•
								0

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



$408 \bmod 108 = 84$

Takto pokračujeme:

$$408 \quad 108 \quad 84 \quad 24 \quad \boxed{12} \quad 0$$

Tato metoda je evidentně nejpohodlnější, ale my si tento algoritmus brzy dále rozšíříme a pak mnozí dávají přednost tomu předchozímu svislému zápisu.

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

△

Jak je tento algoritmus rychlý?

Věta 6a.18. (Lamého věta)
Nechť $a > b \in \mathbb{N}$. Pak Euklidův algoritmus pro $\gcd(a,b)$ vyžaduje nanejvýš tolik kroků, kolik je pětkrát počet cifer v b.

Důkaz (drsný, poučný)**:** Nejprve si všimněme následujícího. V každém kroku počítáme $r_{k-1} = q_k \cdot r_k + r$, kde $r < r_k$. Kdyby bylo $q_k = 0$, tak dostáváme $r = r_{k-1}$, což by znamenalo $r_{k-1} < r_k$, jenže v našem algoritmu je to přesně naopak, my máme $r_{k-1} > r_k$. Proto musí být vždy $q_k \geq 1$.

Je to vidět i jinak. Protože je $r_{k-1} > r_k$, tak při hledání zbytku po dělení musíme r_k alespoň jednou odečíst od r_{k-1}.

Každopádně máme $r_{k-1} = q_k \cdot r_k + r_{k+1} \geq r_k + r_{k+1}$.

Jak to vypadá pro případ, kdy $r_{k+1} = 0$, tedy poslední krok algoritmu? Pak $r_{k-1} = q_k \cdot r_k$. Kdyby bylo $q_k = 1$, pak dostáváme $r_{k-1} = r_k$, což zase není možné. Je tedy $q_k \geq 2$ a máme pro poslední nenulové r_k nerovnost $r_{k-1} \geq 2r_k$.

Uvažujme teď běh algoritmu pro konkrétní $a > b$ a předpokládejme, že skončil pro jisté $n \in \mathbb{N}$ s $r_{n+1} = 0$ a $r_n = \gcd(a,b)$. Tvrdíme následující:

Pro $k = 1, \ldots, n$ platí $V(k)$: $r_{n-k+1} \geq F_{k+1}$, kde F_m jsou Fibonacciho čísla, viz příklad 9a.c. Dokážeme to indukcí na k (modifikovaným principem s návratem o dva kroky).

(0) Pro $k = 1$ rovnost říká $r_n \geq F_2$, tedy $r_n \geq 1$, což je pravda, r_n je poslední nenulový zbytek.

Pro $k = 2$ tvrzení říká, že $r_{n-1} \geq F_3$, tedy $r_{n-1} \geq 2$. To je pravda, protože pro poslední krok jsme odvodili $r_{n-1} \geq 2r_n \geq 2$.

(1) Předpokládejme, že tvrzení platí pro $1, \ldots, k$, kde $k \geq 2$. Chceme odhad pro $r_{n-(k+1)+1} = r_{n-k}$. Použijeme nerovnici odvozenou na začátku důkazu, dává $r_{n-k} \geq r_{n-k+1} + r_{n-k+2} = r_{n-k+1} + r_{n-(k-1)+1}$. Pomocí indukčního předpokladu a vlastností Fibonacciho čísel pak dostaneme

$$r_{n-(k+1)+1} = r_{n-k} \geq F_{k+1} + F_{(k-1)+1} = F_{k+1} + F_k = F_{k+2} = F_{(k+1)+1}.$$

$V(k+1)$ a tím i krok (1) jsou dokázány. Indukce potvrdila, že $V(k)$ platí pro $k = 1, \ldots, n$.

Z $V(n)$ máme $r_1 \geq F_{n+1}$, tedy počet kroků programu n splňuje nerovnost $F_{n+1} \leq b$. Co z toho plyne pro n?

Z výsledků příkladu 9a.c máme následující. Když označíme $\alpha = \dfrac{1+\sqrt{5}}{2}$, pak $F_n \geq \alpha^{n-1}$. Pro nás to znamená, že $\alpha^n \leq b$, proto $n \log_{10}(\alpha) \leq \log_{10}(b)$. Kalkuliho přístroj potvrdí, že $\log_{10}(\alpha) > \frac{1}{5}$, z čehož dostaneme $n \leq 5\log_{10}(b)$. Důkaz je hotov.

□

Říkáme tím vlastně, že výpočetní náročnost algoritmu je řádově $\log(b)$, jenže jsme nezapočítali nároky na výpočet rozkladu $a = qb + r$, zvolená implementace výslednou náročnost dost ovlivní. Používané algoritmy mají obdobnou náročnost (závisí na délce dělitele), takže obecně lze říci, že celková výpočetní náročnost Euklidova algoritmu je řádově $[\log(b)]^2$. 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 9b si o náročnosti povíme víc, pak budeme říkat, že náročnost Euklidova algoritmu je $O(n^2)$.

Mimochodem, zajímavé je, že efektivní implementace dělení celých čísel dokážou průměrnou náročnost hledání zbytku, takže postup přes $q = \left\lfloor \frac{a}{b} \right\rfloor$ zase není tak špatný. Dá se ale ukázat, 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 $q = 2$ a to už se hledání q a r odečítáním opravdu vyplatí.

Zajímavou alternativou je použití různých fint, například je možné použít tyto rovnosti:

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

Takže nejprve opakovaným dělením dvěma (což je relativně levná operace) dosáhneme situace s jedním či dvěma lichými čisly, pak aplikujeme opakovaně druhý či třetí vzorec, dokud nedostaneme dvě sudá čísla, to zase redukujeme dělením dvěma a pořád dokola. V zásadě lze ale říct, že lépe než k n^2 se stejně nedostaneme.

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

! **Věta 6a.19.** (Bezoutova věta/rovnost) (Bezout's identity)
Nechť $a, b \in \mathbb{Z}$. Pak existují $A, B \in \mathbb{Z}$ takové, že $\gcd(a,b) = Aa + Bb$.

Důkaz (drsný, 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 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) existuje její nejmenší prvek c. Tvrdíme, že $c = \gcd(a,b)$.

1) Podle Důsledku 6a.4 (i) každý společný dělitel a a b dělí všechny prvky M, mimo jiné také c.
I $\gcd(a,b)$ je společný dělitel a, b, proto $\gcd(a,b) \,|\, c$, tedy $\gcd(a,b) \leq c$.

2) Ukážeme, že c je společný dělitel a a b. Nechť $a = qc + r$, kde $0 \leq r < c$. Máme $r = a - qc = a - (Aa + Bb) = (1 - A)a + Bb$, takže kdyby platilo $r > 0$, tak už $r \in M$ a zároveň $r < c$, což je spor s tím, že c je nejmenší v M. Proto $r = 0$ a $c \,|\, a$. Obdobně také ukážeme, že $c \,|\, b$. Takže c je společný dělitel, proto musí splňovat $c \leq \gcd(a,b)$.

Spojením 1) a 2) dostáváme, že opravdu $c = \gcd(a,b)$. Ale $c \in M$, proto se dá $\gcd(a,b)$ coby prvek M napsat jako $\gcd(a,b) = Aa + Bb$.

□

Když víme, že $c = \gcd(a,b)$, tak lze pozorování z 1) formulovat takto:

Důsledek 6a.20.
Nechť $a, b \in \mathbb{Z}$. Jestliže je d společný dělitel a, b, pak d dělí $\gcd(a,b)$.

Takže opravdu je $\gcd(a,b)$ největším společným dělitelem i vůči uspořádání dělitelností. Tím jsme splnili jeden dloužek z počátku této kapitoly.

Jak se taková kombinace najde? Někdy se to dá uhádnout. Víme například, že $\gcd(24, 60) = 12$, a uhádneme $12 = 3 \cdot 24 + (-1) \cdot 60$. Je ovšem také možné zkusit třeba $12 = (-2) \cdot 24 + 1 \cdot 60$. Bezoutova věta netvrdila, že je jediná možnost, ve skutečnosti je jich nekonečně mnoho, viz Diofantické rovnice 6c. Z hlediska aplikací mezi těmito možnostmi není rozdíl, cílem je najít nějaké takové vyjádření pro $\gcd(a,b)$. Existuje na to algoritmus vycházející ze zpětného chodu Euklidovým algoritmem. Vraťme se k předchozímu příkladu.

Příklad 6a.g: Zjistili jsme, že $\gcd(408, 108) = 12$. Jak vyjádříme 12 jako lineární kombinaci 408 a 108? Přečteme si 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 $\gcd(408, 108) = 4 \cdot 408 + (-15) \cdot 108$.

△

Takto to samozřejmě dělat nechceme, raději hledání A, B zabudujeme přímo do Euklidova algoritmu, dostaneme tak jeho rozšířenou verzi. V tomto algoritmu již nebudeme moci používat $r = a \bmod b$, protože i částečný podíl q_k bude hrát roli. Opět uvedeme jednu verzi indexovanou pro důkazy a jednu verzi počítací.

S **Algoritmus 6a.21. Rozšířený Euklidův algoritmus** pro nalezení $\gcd(a,b) = Aa + Bb$ pro $a > b \in \mathbb{N}$.

Verze 1.
Inicializace: $r_0 := a$, $r_1 := b$, $k := 0$,
$A_0 := 1$, $A_1 := 0$, $B_0 := 0$, $B_1 := 1$.
Krok: $k := k + 1$, $r_{k-1} = q_k \cdot r_k + r_{k+1}$,
$A_{k+1} := A_{k-1} - q_k A_k$, $B_{k+1} := B_{k-1} - q_k B_k$.
Opakovat dokud nenastane $r_{k+1} = 0$.
Pak $\gcd(a,b) = r_k = A_k a + B_k b$.

△

nebo

Verze 2.
`procedure` *gcd-Bezout* (a, b: integer, $a > b > 0$)
$A_0 := 1$; $A_1 := 0$; $B_0 := 0$; $B_1 := 1$;
`repeat`
$a = q \cdot b + r$;
$a := b$; $b := r$;
$r_a := A_0 - qA_1$;
$r_b := B_0 - qB_1$;
$A_0 := A_1$; $A_1 := r_a$;
$B_0 := B_1$; $B_1 := r_b$;
`until` $b = 0$;
`output:` a, A_0, B_0;

Všimněte si, že nový zbytek počítáme jako $r_{k+1} = r_{k-1} - q_k \cdot r_k$, což je přesně stejný vzorec jako pro A_{k+1} a B_{k+1}, dokonce používají stejné číslo q_k. To znamená, že jakmile si zjistíme $q_k = \lfloor \frac{r_{k-1}}{r_k} \rfloor$, tak už všechna tři čísla z nové generace počítáme stejným způsobem.

! `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;

Tento postup je ideálním vychodiskem pro ruční výpočet. Znamená to totiž, že jakmile doplníme políčko s q, tak do dalšího řádku dopočítáváme „nové b“, „nové A_1“ a „nové B_1“ pomocí stejného cestování tabulkou.

S 6a.22 Ruční výpočet. Najdeme $\gcd(408, 108)$ a vyjádříme jej jako lineární kombinaci 408 a 108. Začneme verzí se svislým zápisem (do řádků).

Nejprve je třeba vytvořit dva iniciační řádky. Hodnoty 408 a 108 jsou jasné, hodnoty pro A, B si je třeba pamatovat, například tak, že vypadají jako jednotková matice. Pak spočítáme $q = 3$ jako částečný podíl a zapíšeme do tabulky.

a, b	q	A	B
408		1	0
108		0	1

a, b	q	A	B
408		1	0
108	3	0	1

V normálním Euklidově algoritmu následně najdeme zbytek $408 - 3 \cdot 108 = 84$, který zapíšeme pod 108. To znamená, že když se podíváme na první sloupec, tak děláme postup „číslo v předposledním mínus q krát číslo v posledním, výsledek zapíšeme na nový řádek“. Přesně tento vzorec pak aplikujeme na dvojici sloupců pro A a B, dostáváme $1 - 3 \cdot 0 = 1$ jako „nové A“ a $0 - 3 \cdot 1 = -3$ jako „nové B“. Tím jsme zkompletovali nový řádek a jsme připraveni celý algoritmus opakovat. To děláme tak dlouho,dokud v levém sloupci nebude nula.

a, b	q	A	B
408		1	0
108	3	0	1
84		1	−3

a, b	q	A	B
408		1	0
108	3	0	1
84	1	1	−3
24		−1	4

a, b	q	A	B
408		1	0
108	3	0	1
84	1	1	−3
24	3	−1	4
12		4	−15

a, b	q	A	B
408		1	0
108	3	0	1
84	1	1	−3
24	3	−1	4
12•	2	4•	−15•
0			

Výsledek najdeme jako obvykle v řádku nad nulou, opravdu $12 = 4 \cdot 408 + (-15) \cdot 108$.

Všimněte si, že stejný vztah platí i pro řádek před tím: $24 = (-1) \cdot 408 + 4 \cdot 108$. A také ten před tím atd., až se dostaneme na první dva řádky: $108 = 0 \cdot 408 + 1 \cdot 108$ a $408 = 1 \cdot 408 + 0 \cdot 108$. To pro někoho může být další mnemotechnická pomůcka, jak si pamatovat výchozí hodnoty pro A, B. Zároveň to bude níže východiskem pro důkaz správnosti rozšířeného Euklidova algoritmu.

Tento výpočet svislou tabulkou se zdá býti vhodným kompromisem mezi praktičností a zároveň názorností, budeme jej proto v této knize používat. Pro úplnost ukážeme ještě jeden algoritmus, který je graficky úspornější, vychází z vodorovného zápisu Euklidova algoritmu. Probíhá ve dvou fázích, začneme tak, že prostě provedeme Euklidův algoritmus s tím, že do prvního řádku píšeme hodnoty a, b a pod to odpovídající hodnoty q.

a, b	408	108	84	24	12	0
q		3	1	3	2	

Teď vytvoříme třetí řádek, ten ale děláme zprava doleva. Nejprve pod poslední hodnoty q napíšeme (zprava) 0 a 1.

a,b	408	108	84	24	12	0
q		3	1	3	2	
				1	0	

Jsme připraveni k druhé fázi algoritmu, která funguje následovně: Vezmeme poslední číslo v třetím řádku (teď 0) a odečteme od něj předposlední číslo (teď 1) vynásobené koeficientem q nad předposledním číslem (teď 3), dostaneme $0-1\cdot 3=-3$ a napíšeme to doleva od předposledního čísla, tedy pod jedničku. Proces opakujeme, jen se vzorec přesune v tabulce o pole doleva. Vezmeme druhé číslo zprava (jedničku), odečteme číslo nalevo (tedy -3) vynásobené číslem nad ním (jedničkou), výsledek $1-(-3)\cdot 1=4$ zapíšeme ještě o jedno doleva. V posledním kroku počítáme $-3-4\cdot 3=-15$ a zapíšeme zcela doleva.

a,b	408	108	84	24	12	0
q		3	1	3	2	
	-15	4	-3	1	0	

Co teď s tím? Začněme zprava, v horním a dolním řádku vidíme napravo dvojice $12\leftrightarrow 0$ a $24\leftrightarrow 1$. Když hodnoty z dolního řádku prohodíme, dostaneme $12\leftrightarrow 1$ a $24\leftrightarrow 0$ a $12\cdot 1+24\cdot 0=12=\gcd(408,108)$. Posuňme se o jedno doleva. Porovnáním horního a dolního řádku máme dvojice $24\leftrightarrow 1$ a $84\leftrightarrow -3$, prohodíme $24\leftrightarrow -3$ a $84\leftrightarrow 1$ a dostaneme $24\cdot(-3)+84\cdot 1=12$. Další posun si zkusíte sami. Happy end: V levých dvou sloupcích máme $408\leftrightarrow -15$ a $108\leftrightarrow 4$, prohodíme $408\leftrightarrow 4$ a $108\leftrightarrow -15$ a dostaneme $408\cdot 4+108\cdot(-15)=12$, což je přesně hledaná Bezoutova identita. Náhoda? Nikoliv, takto to funguje vždy.

Tento způsob je bezesporu nejúspornější, ale je to už docela černá magie, je tedy více náchylný na chybu. Je například snadné zapomenout na to, že se mají na konci výsledná dvě čísla prohodit. Pokud má čtenář pocit, že mu chyby nehrozí (ani na písemce, kde přijde nervozita, nevyspání atd.), pak tento postup samozřejmě může s úspěchem používat. V této knize nicméně budeme po mnoha zkušenostech se studenty u zkoušek raději používat ten bezpečnější předchozí algoritmus.

Poznámka důkaz správnosti algoritmu:

Potvrdíme správnost našeho pozorování o tabulce. Přesně řečeno, dokážeme modifikovaným principem indukce (zpětný krok o dva) následující tvrzení pro $k\in\mathbb{N}_0$:

$V(k)$: Jestliže $r_k>0$, pak $r_k=A_ka+B_kb$.

(0) $k=0$: $r_0=a$, $A_0a+B_0b=a$, v pořádku.

$k=1$: $r_1=b$, $A_1a+B_1b=b$, v pořádku.

(1) Nechť $k\geq 2$, předpokládáme, že V platí pro k a $k-1$. Pak

$$\begin{aligned} r_{k+1}&=r_{k-1}-q_k\cdot r_k=(A_{k-1}a+B_{k-1}b)-q_k(A_ka+B_kb)\\ &=(A_{k-1}-q_kA_k)a+(B_{k-1}-q_kB_k)b=A_{k+1}a+B_{k+1}b.\end{aligned}$$

Důkaz správnosti algoritmu je hotov.

Pro úplnost ještě dokážeme, že ten kratší a adrenalinovější algoritmus opravdu funguje. Nejprve se vrátíme ke značení z důkazu správnosti Euklidova algoritmu, kde jsme zvolili $r_0=a$, $r_1=b$ a poté definovali rekurzí $q_k=\left\lfloor\frac{r_{k-1}}{r_k}\right\rfloor$, $r_{k+1}=r_{k-1}-q_kr_k$. Toto se opakuje, dokud nenastane $r_{n+1}=0$, pak $r_n=\gcd(a,b)$.

Nyní definujeme $s_0=0$, $s_1=1$ a $s_{k+1}=s_{k-1}-q_{n-k}s_k$ pro $k=1,\dots,n-1$. Tvrdíme, že pro každé $k=1,\dots,n$ platí $r_{n-k+1}s_k+r_{n-k}s_{k-1}=r_n$, dokážeme to indukcí.

(0) Pro $k=1$ začneme levou stranou vzorce: $r_{n-1+1}s_1+r_{n-1}s_0=r_n\cdot 1+r_{n-1}\cdot 0=r_n$, souhlasí.

(1) Nechť $k\in\{1,\dots,n-1\}$, předpokládejme, že $r_{n-k+1}s_k+r_{n-k}s_{k-1}=r_n$. Dosadíme za r_{n-k+1} z rekurentní definice a po úpravě dostaneme vzorec, který potřebujeme pro $k+1$:

$$\begin{aligned} r_n&=r_{n-k+1}s_k+r_{n-k}s_{k-1}=(r_{n-k-1}-q_{n-k}r_{n-k})s_k+r_{n-k}s_{k-1}=r_{n-k-1}s_k-q_{n-k}r_{n-k}s_k+r_{n-k}s_{k-1}\\ &=r_{n-k-1}s_k+r_{n-k}(s_{k-1}-q_{n-k}s_k)=r_{n-k-1}s_k+r_{n-k}s_{k+1}=r_{n-k}s_{k+1}+r_{n-k-1}s_k\\ &=r_{n-(k+1)+1}s_{k+1}+r_{n-(k+1)}s_{(k+1)-1}.\end{aligned}$$

Tím je naše tvrzení dokázáno. Teď jej použijeme pro $k=n$:

$$\gcd(a,b)=r_n=r_1s_n+r_0s_{n-1}=b\cdot s_n+a\cdot s_{n-1}.$$

Opravdu tedy Bezoutovu identitu získáme pomocí posledních dvou čísel zpětného chodu, když je prohodíme. △

! Bezoutova identita byla dokázána pro všechna celá čísla a,b, ale náš algoritmus funguje jen pro $a>b>0$. Jak se najde vyjádření $\gcd(a,b)=Aa+Bb$ pro jiné možnosti? Pokud je některé z čísel nulové, tak je to triviální, viz důkaz Bezoutovy identity. Pokud $|a|=|b|$, pak taky není co řešit, viz Fakta 6a.12 a 6a.13. Zbývá případ, kdy je $|a|\neq|b|>0$, ale to už se snadno udělá s trochou selského rozumu.

Příklad 6a.h: 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 jenom vyrobíme správná znaménka u čísel:

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

△

Dal by se napsat obecný algoritmus, ale snad to není nutné.

Bezoutova identita je velice mocný nástroj pro praktické výpočty, jak ještě uvidíme zde níže i dalších kapitolách, ale také se nám bude hodit v důkazech. Jako ukázku si pomocí této identity ukážeme tvrzení, že když umíme číslem d vydělit součin ab, ale číslo d nemá nic společného s a, pak už musíme to d najít celé v b. To zní jako něco, co je evidentně pravdivé, ale bez pomoci Bezouta by se to dokazovalo překvapivě obtížně.

! **Lemma 6a.23.**
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 (rutinní)**:** Podle předpokladu existuje $k \in \mathbb{Z}$ takové, že $ab = kd$. Protože jsou d, a nesoudělná, musí existovat čísla $A, B \in \mathbb{Z}$ taková, že $1 = \gcd(d, a) = Dd + Aa$. Pak $b = Ddb + Aab$, tedy $b = Ddb + Akd$, tedy $b = (Db + Ak)d$. To ukazuje, že d dělí b.

□

Cvičení

Cvičení 6a.1 (rutinní)**:** Najděte částečný podíl a zbytek pro $2002/87$, $-1030/13$, $0/7$, $2/17$, $-3/7$, $8/2$.

Cvičení 6a.2 (rutinní)**:** Dokažte, že pro každé $a \in \mathbb{Z}$ platí $1 \mid a$, $a \mid a$ a $a \mid 0$ (viz Fakt 6a.1).

Cvičení 6a.3 (rutinní, zkouškové)**:** (i) Nechť $a, b \in \mathbb{Z}$. Dokažte, že jestliže $a \mid b$, pak $a \mid (nb)$ pro všechna $n \in \mathbb{Z}$.
(ii) Nechť $a, b, c \in \mathbb{Z}$. Dokažte, že jestliže $a \mid b$ a $b \mid c$, pak $a \mid c$ (viz Věta 6a.2).

Cvičení 6a.4 (rutinní, poučné)**:** Nechť $a, b \in \mathbb{Z}$. Dokažte, že následující podmínky jsou ekvivalentní:
(i) $a \mid b$,
(ii) $(-a) \mid b$,
(iii) $a \mid (-b)$,
(iv) $(-a) \mid (-b)$,
(v) $|a| \mid |b|$.
Nápověda: Vytvořte z implikací nějaký uzavřený cyklus zahrnující (i) až (iv), třeba (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) $\implies$ (i) a dokažte jej. Rozmyslete si, že pak už z toho plyne libovolná implikace mezi nějakými dvěma podmínkami z těchto čtyř, jsou tedy všechny ekvivalentní. Pak toho využijte k důkazu ekvivalence (i) a (v).

Cvičení 6a.5 (rutinní)**:** Nechť $a, b \in \mathbb{Z}$, $a > 0$. Dokažte, že $a \mid b$ právě tehdy, když $b \bmod a = 0$.

Cvičení 6a.6 (poučné, zkouškové)**:** Dokažte, že pro každé $a, d \in \mathbb{N}$ takové, že $r = a \bmod d \neq 0$, platí $(-a) \bmod d = d - r$.
Jak to funguje pro případ $a \bmod d = 0$?

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

Cvičení 6a.8 (rutinní, zkouškové)**:** Nechť $a, b, c \in \mathbb{Z}$. Dokažte, že jestliže $ac \mid bc$ a $c \neq 0$, pak $a \mid b$.

Cvičení 6a.9 (poučné)**:** Nechť $a, b, c \in \mathbb{Z}$. Dokažte/vyvraťte, že jestliže $a \mid bc$, pak $a \mid b$ nebo $a \mid c$.

Cvičení 6a.10 (rutinní, poučné)**:** Dokažte, že pro $a \in \mathbb{N}$ platí $\gcd(a, 0) = a$ a $\gcd(a, a) = \operatorname{lcm}(a, a) = a$ (viz Fakt 6a.13).

Cvičení 6a.11 (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 6a.12 (poučné)**:** Dokažte, že součin libovolných tří po sobě následujících celých čísel je vždy dělitelný 6.

Cvičení 6a.13 (rutinní, poučné, zkouškové)**:** Dokažte, že pro každé $n \in \mathbb{N}_0$ platí následující dělitelnosti:
(i) $2 \mid (n^2 - n)$; (iii) $3 \mid (n^3 + 2n)$; (v) $6 \mid (n^3 - n)$;
(ii) $2 \mid (n^2 + n)$; (iv) $5 \mid (n^5 - n)$; (vi) $21 \mid (4^{n+1} + 5^{2n-1})$ (zde $n \geq 1$).
Nápověda: Indukce to jistí.

Cvičení 6a.14 (rutinní, zkouškové)**:** Pro následující dvojice $a, b \in \mathbb{Z}$ najděte $\gcd(a, b)$ faktorizací, pak rozšířeným Euklidovým algoritmem a napište příslušnou Bezoutovu identitu. Pak najděte $\operatorname{lcm}(a, b)$.
(i) $a = 420, b = 231$; (ii) $a = -60, b = -156$; (iii) $a = 118, b = -131$.

Cvičení 6a.15 (poučné)**:** Nechť $a, b \in \mathbb{Z}$. Dokažte, že jestliže $\gcd(a, b) = 1$, pak $\operatorname{lcm}(a, b) = |a| \cdot |b|$.

Cvičení 6a.16 (rutinní)**:** Dokažte, že 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 $\gcd\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{\gcd(a,b)}{k}$.

Cvičení 6a.17 (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 6a.18 (drsné)**:** Dokažte: Vybereme-li $n+1$ různých čísel z množiny $\{1, 2, 3, \ldots, 2n\}$, pak mezi nimi musí být dvě takové, že jedno dělí druhé.
Viz také příklad 11b.k.

Cvičení 6a.19 (drsné)**:** Jak zobecníme pojem gcd a lcm pro více čísel? Jsou dva obecné přístupy.
Jedna možnost je přes indukci. Pro tři čísla $a, b, c \in \mathbb{N}$ můžeme definovat $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ a $\operatorname{lcm}(a, b, c) = \operatorname{lcm}(\operatorname{lcm}(a, b), c)$, gcd i lcm se pokaždé aplikují jen na dvě čísla.
Když to umíme pro tři, můžeme pro čtyři čísla $a, b, c, d \in \mathbb{N}$ definovat $\gcd(a, b, c, d) = \gcd(\gcd(a, b, c), d)$ a $\operatorname{lcm}(a, b, c, d) = \operatorname{lcm}(\operatorname{lcm}(a, b, c), d)$, atd., indukcí tak dokážeme zadefinovat oba pojmy pro libovolný (konečný) počet čísel.
Druhý přístup je významový, $\gcd(a_1, a_2, \ldots, a_n)$ definujeme jako největší přirozené číslo d splňující vlastnost, že $d \mid a_i$ pro všechna i, obdobně $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$ definujeme jako nejmenší přirozené číslo d splňující vlastnost, že $a_i \mid d$ pro všechna i.
Dá se ukázat, že oba přístupy dávají stejné výsledky. To by bylo na jedno cvičení trochu moc, dokažte tedy následující:
Nechť $a, b, c \in \mathbb{N}$ jsou libovolná. Nechť d je největší přirozené číslo takové, že $d \mid a$, $d \mid b$ a $d \mid c$. Pak $d = \gcd(\gcd(a, b), c)$.

Cvičení 6a.20 (poučné)**:** Nechť $a_1, a_2, \ldots, a_n \in \mathbb{N}$.
Rozmyslete si, zda platí $\operatorname{lcm}(a_1, a_2, \ldots, a_n) = \frac{a_1 \cdot a_2 \cdots a_n}{\gcd(a_1, a_2, \ldots, a_n)}$.
Rozmyslete si, zda platí, že když jsou a_i po dvou nesoudělná, pak $\operatorname{lcm}(a_1, a_2, \ldots, a_n) = a_1 \cdot a_2 \cdots a_n$.
Pro případný důkaz platnosti viz cvičení 6b.4

Řešení:
6a.1: $q = 23$, $r = 17$; $q = -80$, $r = 10$; $q = 0$, $r = 0$; $q = 0$, $r = 2$; $q = -1$, $r = 4$; $q = 4$, $r = 0$.
6a.2: $a = a \cdot 1$, $a = 1 \cdot a$, $0 = 0 \cdot a$.
6a.3: (i): $b = ka \implies bn = \ldots$ (ii) podobně.
6a.4: (i) $\implies$ (ii): $a \mid b \implies b = ka, k \in \mathbb{Z} \implies b = -k \cdot (-a) \wedge -k \in \mathbb{Z} \implies -a \mid b$. (ii) $\implies$ (iii), (iii) $\implies$ (iv), (iv) $\implies$ (i) obdobně.
(i) $\implies$ (v): $a \mid b \implies b = ka, k \in \mathbb{Z} \implies |b| = |k| \cdot |a| \wedge |k| \in \mathbb{Z} \implies |a| \,|\, |b|$.
(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 $(\pm a) \mid (\pm b)$ neboli jedním z tvrzení (i) až (iv).
6a.5: Jestliže $a \mid b$, pak $b = ka = ka + 0$, tedy $r = 0$.
Jestliže $b \bmod a = 0$, pak $b = qa + 0 = qa$ a $q \in \mathbb{Z}$.
Jestliže $r = a \bmod d$, pak $a = qd + r$ pro nějaké $q \in \mathbb{N}_0$ a $0 \leq r < d$. Předpoklad dále dává $r > 0$. Pak také $(-a) = (-q)d - r$ a $-d < -r < 0$, proto $(-a) = (-q-1)d + (d-r)$. Teď $(-q-1) \in \mathbb{Z}$ a $0 < d - r < d$, číslo $d - r$ proto splňuje podmínku z definice $(-a) \bmod d$.
Jestliže $r = 0$ neboli $d \mid a$, pak $(-a) \bmod d = 0 = r$.

Cvičení 6a.6 (poučné, zkouškové)**:** Dokažte, že pro každé $a, d \in \mathbb{N}$ platí: $(-a) \bmod d = d - a \bmod d$.
Nápověda: Označte si $r = a \bmod d$.
6a.7: $c = ka, d = lb \wedge k, l \in \mathbb{Z} \implies cd = (kl)ab \wedge (kl) \in \mathbb{Z} \implies ab \mid cd$.
6a.8: $ac \mid bc \implies bc = kac \wedge k \in \mathbb{Z} \implies b = ka \wedge k \in \mathbb{Z} \implies a \mid b$.

6a.9: Neplatí, $6\,|\,(4\cdot 9)$, ale není $6\,|\,4$ ani $6\,|\,9$.
6a.10: Libovolné $d\in\mathbb{N}$ dělí 0, proto je množina společných dělitelů $a,0$ totožná s množinou dělitelů $d\in\mathbb{N}$ čísla a. Takoví dělitelé nutně splňují $d\le a$ a víme, že také $a\,|\,a$, tudíž a náleží do množiny společných dělitelů a je tam největší.
$\gcd(a,a)$ má být největší dělitel a, což je samozřejmě a. Důkaz pro $\operatorname{lcm}(a,a)$ je obdobný.
6a.11: (i) Označme $n=10a+b$, tedy b je poslední cifra. Protože $10a=(2a)\cdot 5$, tak (podle Důsledku 6a.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.
6a.12: Jedno z nich musí být sudé, jedno z nich musí být dělitelné třemi, viz Fakt 6a.11.
6a.13: Vše indukcí.
(i): (0) $n=0\implies n^2-n=0$, $2\,|\,0$.
(1) Nechť $n\in\mathbb{N}_0$ libovolné, předpoklad: $2\,|\,(n^2-n)\implies(n^2-n)=2k$, $k\in\mathbb{Z}$. Pak
$(n+1)^2-(n+1)=n^2+n=(n^2-n)+2n=2k+2n=2(k+n)$ a $n+k\in\mathbb{Z}$, tedy $2\,|\,[(n+1)^2-(n+1)]$.
(vi): (0) $n=1\implies 21\,|\,(16+5)$ platí.
(1) Nechť $n\in\mathbb{N}$ libovolné, předpoklad: $21\,|\,(4^{n+1}+5^{2n-1})\implies(4^{n+1}+5^{2n-1})=21k$ pro $k\in\mathbb{Z}$. Pak
$4^{(n+1)+1}+5^{2(n+1)-1}=4\cdot 4^{n+1}+25\cdot 5^{2n-1}=4\cdot 4^{n+1}+4\cdot 5^{2n-1}+21\cdot 5^{2n-1}=4(4^{n+1}+5^{2n-1})+21\cdot 5^{2n-1}$
$=4\cdot 21k+21\cdot 5^{2n-1}=21(4k+5^{2n-1})$, kde $(4k+5^{2n-1})\in\mathbb{Z}$.
6a.14: (i):

420		1	0	$\gcd(2^2\cdot 3\cdot 5\cdot 7, 3\cdot 7\cdot 11)=3\cdot 7=21$
231	1	0	1	$\operatorname{lcm}(2^2\cdot 3\cdot 5\cdot 7, 3\cdot 7\cdot 11)=2^2\cdot 3\cdot 5\cdot 7\cdot 11=4620$
189	1	1	-1	
42	4	-1	2	
21•	2	5•	-9•	
0				

$\gcd(420,231)=21=5\cdot 420+(-9)\cdot 231$.
(ii): Hledat $\gcd(|-60|,|-156|)=\gcd(156,60)$.

156		1	0	$\gcd(-2^2\cdot 3\cdot 5, -2^2\cdot 3\cdot 13)=2^2\cdot 3=12$
60	2	0	1	$\operatorname{lcm}(-2^2\cdot 3\cdot 5, -2^2\cdot 3\cdot 13)=2^2\cdot 3\cdot 5\cdot 13=780$
36	1	1	-2	
24	1	-1	3	
12•	2	2•	-5•	
0				

$\gcd(-60,-156)=12=2\cdot 156+(-5)\cdot 60$;
(iii): Hledat $\gcd(|-131|,118)=\gcd(131,118)$.

131		1	0	$\gcd(-131, 2\cdot 59)=1$
18	1	0	1	$\operatorname{lcm}(-131, 2\cdot 59)=131\cdot 2\cdot 59=15458$
13	9	1	-1	
1•	13	-9•	10•	
0				

$\gcd(118,-131)=1=(-9)\cdot 131+10\cdot 118=10\cdot 118+9\cdot(-131)$.
6a.15: Stačí použít $\operatorname{lcm}(a,b)=\frac{|a|\cdot|b|}{\gcd(a,b)}$.
Správný matematický přístup je využívat již odvedené práce.
6a.16: (i): Označme $d=\gcd(a,b)$ a $e=\gcd(ka,kb)$. Pak d dělí a,b, proto kd dělí ka,kb, platí tedy $kd\le e$. Naopak: Podle Bezouta $d=Aa+Bb$, proto $kd=Aka+Bkb$, e dělí obě napravo, proto dělí i kd a tedy $e\le kd$.
(ii) Podobně jako v (i) nebo přímo, aplikujte (i) na $a'=\frac{a}{k}$ a $b'=\frac{b}{k}$.
6a.17: Podle Bezouta $\gcd(a,b)=A_ba+Bb$ a $\gcd(a,c)=A_ca+Cb$.
Pak $\gcd(a,b)\gcd(a,c)=a(A_bA_ca+A_bCb+A_cBb)+bcBC$. $\gcd(a,bc)$ dělí a i bc, tudíž musí dělit i ten součin.
6a.18: Indukcí na n.
(0) $n=1$: Vybereme dvě různá čísla z $\{1,2\}$, pak to jsou 1 a 2 a $1\,|\,2$.
Ze zvědavosti $n=2$: Vybereme tři různá čísla z $\{1,2,3,4\}$, pokud je mezi nimi 1, tak ta určitě dělí nějaké další. Pokud mezi nimi 1 není, tak jsme nutně vybrali $2,3,4$ a $2\,|\,4$.
(1) Předpokládejme platnost pro nějaké $n\in\mathbb{N}$. Teď vyberme $(n+1)+1=n+2$ čísel z množiny $\{1,2,\dots,2n,2n+1,2n+2=2(n+1)\}$. Dvě možnosti:
a) Jestliže je alespoň $n+1$ z těchto čísel vybráno z množiny $\{1,2,\dots,2n\}$, tak aplikujeme indukční předpoklad a najdeme mezi nimi dvě, že jedno dělí druhé.

b) Z těch $n+2$ čísel je v množině $\{1, 2, \dots, 2n\}$ jen n. To znamená, že jsme nutně vybrali čísla $2n+1$ a $2n+2$. Pokud jsme vybrali i číslo $n+1$, tak jsme hotovi.
Zbývá následující situace: Vybrali jsme čísla $2n+1$, $2n+2$ a ještě množinu M obsahující n různých čísel z množiny $\{1, 2, \dots, 2n\}$, přičemž M neobsahuje $n+1$. Pak je $M \cup \{n+1\}$ množina obsahující $n+1$ různých čísel z množiny $\{1, 2, \dots, 2n\}$, proto podle indukčního předpokladu v této množině existují a, b taková, že $a \mid b$. Z toho plyne $a < b$, proto a nemůže být $n+1$. Pokud ani b není $n+1$, pak $a, b \in M$, jsou tedy i v původním výběru a jedno dělí druhé, hotovo.
Zbývá možnost, že $b = n+1$, pak je v M číslo, které dělí $n+1$, což zase dělí $2n+2$, které taktéž je v našem výběru, takže v našem původním výběru je číslo dělící $2n+2$, hotovo.
6a.19: 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.
2) 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 $d \leq D$.

6b. Prvočísla

Teď se budeme soustředit na čísla z $\mathbb{N}$. Podíváme se na speciální druh čísel, která jsou z hlediska dělitelnosti základními stavebními bloky všech čísel.

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

Prvočísla tradičně značíme jako p, popř. q. Vidíme, že 1 není prvočíslo ani složené číslo, je to nějaké jiné číslo. Občas si na to budeme muset dát pozor.

Všimneme si, že číslo $a \in \mathbb{N}$ je složené, jestliže existuje $k \in \mathbb{N}$ takové, že $k \mid a$ a $1 < k < a$. Ještě jinak: Číslo a je složené, jestliže existují $x, y \in \mathbb{N}$ takové, že $a = xy$ a $x < a$, $y < a$.

Příklad 6b.a: Prvočísla byla zkoumána už od nepaměti a každý určitě nějaká zná. Mezi první stovkou přirozených čísel jsou tato prvočísla (je jich 25):

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Další je pak 101.
△

Prvočísla najdeme ve všech číslech (skoro, kromě jedničky).

Fakt 6b.1.
Nechť $n \in \mathbb{N}$, $n \neq 1$. Pak existuje prvočíslo p takové, že $p \mid n$.

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 $k \mid (n+1)$ a $1 < k < n+1$. Pak je ale k z množiny $2, 3, \dots, n$, tudíž existuje prvočíslo p takové, že $p \mid k$. Spolu s $k \mid (n+1)$ a tranzitivitou této relace dostáváme $p \mid (n+1)$ a jsme hotovi.
□

Při manipulací s dělitelností máme občas problém, že nám číslo d dělí součin $a \cdot b$, ale my z toho nejsme schopni nic říct. Třeba $6 \mid (4 \cdot 9)$, ale neplatí ani $6 \mid 4$, ani $6 \mid 9$, intuitivně se kousek šestky schoval do 4 a druhý kousek do 9. S provočísly takové problémy nenastanou.

Lemma 6b.2.
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 (poučný)**:** Dokážeme to indukcí na m.

(0) Jestliže $m = 1$, tak předpokládáme $p \mid a_1$, z čehož plyne $i = 1$ a je to.

(1) Předpokládejme, že pro nějaké $m \geq 1$ tvrzení Lemma platí pro libovolné $a_1, \ldots, a_m \in \mathbb{Z}$. Mějme teď $a_1, \ldots, a_m, a_{m+1} \in \mathbb{Z}$ takové, že $p \mid (a_1 \cdots a_m a_{m+1})$. Protože jediní dělitelé p jsou p a 1, tak je i $\gcd(p, a_{m+1})$ buď p nebo 1. V prvním případě je p dělitelem a_{m+1}, tedy $p \mid a_{m+1}$ a jsme hotovi.

V opačném případě $\gcd(p, a_{m+1}) = 1$. Označme $b = a_1 \cdots a_m$, máme tedy situaci, kdy $p \mid (a_{m+1} b)$ a také $\gcd(p, a_{m+1}) = 1$, tudíž Lemma 6a.23 říká, že $p \mid b$, tedy $p \mid (a_1 \cdots a_m)$. Pak ale podle indukčního předpokladu musí existovat i takové, že $p \mid a_i$.

□

Jako rychlý důsledek si dokažme jednu užitečnou ekvivalenci.

Lemma 6b.3.
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) $\Longrightarrow$: Předpokládejme, že $\gcd(d, ab) = 1$. Nechť $x \in \mathbb{N}$ je společný dělitel d a a. Pak podle Věty 6a.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 6b.1 tudíž musí existovat i provočíslo p, které je společným dělitelem d a ab. Lemma 6b.2 ovšem tvrdí, že si p musí vybrat, řekněme, 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 $\gcd(d, b) = 1$“.

□

Lemma 6b.2 bude hrát hlavní roli při důkazu následující věty.

! **Věta 6b.4.** (Fundamentální věta aritmetiky) (Fundamental theorem of arithmetics)
Nechť $n \in \mathbb{N}$. Pak existují prvočísla $p_1, p_2, \ldots, p_m$ a exponenty $k_1, k_2, \ldots, k_m \in \mathbb{N}_0$ takové, že

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} = \prod_{i=1}^{m} p_i^{k_i}.$$

Jestliže pro $n \geq 2$ přidáme podmínky $p_1 < p_2 < \ldots < p_m$ a $k_i > 0$, tak je tato dekompozice jednoznačně určena.

Důkaz (poučný, drsný)**:** 1) K důkazu existence dekompozice použijeme silný princip indukce na $n \in \mathbb{N}$.

(0) Jestliže $n = 1$, tak zvolíme libovolné prvočíslo, třeba $p = 13$, a $k_1 = 0$, dostáváme $1 = p^0$.

(1) Předpokládejme, že rozklad existuje pro všechna čísla $1, 2, \ldots, n$. Uvažujme nyní číslo $n + 1$.

Jestliže je to prvočíslo, pak zvolíme $p_1 = n + 1$ a $k_1 = 1$, hotovo.

Jinak je to číslo složené, tedy existují $a, b \in \mathbb{N}$ takové, že $n+1 = a \cdot b$ a $a, b < n+1$. Podle indukčního předpokladu máme $a = \prod_{i=1}^{M} q_i^{k_i}$ a $b = \prod_{i=1}^{N} r_i^{k_i}$ pro nějaká prvočísla q_i, r_j. Pak $n+1 = \prod_{i=1}^{M} q_i^{K_i} \prod_{i=1}^{N} r_i^{L_i}$, takže je to opravdu součin mocnin prvočísel. Aby to odpovídalo formálně, provedeme přejmenování: Označíme $m = M + N$, $p_i = q_i$ a $k_i = K_i$ pro $i = 1, \ldots, M$, dále $p_i = r_{i-M}$ a $k_i = L_{i-M}$ pro $i = M + 1, \ldots, m$ a dostáváme $n + 1 = \prod_{i=1}^{m} p_i^{k_i}$. Důkaz je hotov.

2) Teď jednoznačnost: Nechť $n \in \mathbb{N}$, $n \geq 2$, a předpokládejme, že $n = \prod_{i=1}^{m} p_i^{k_i}$ a $n = \prod_{i=1}^{M} q_i^{l_i}$, kde $p_1 < \cdots < p_m$, $q_1 < \cdots < q_M$ a $k_i, l_j > 0$.

a) Nejprve ukážeme, že $p_i = q_i$ pro každé i takové, že p_i či q_i existuje. Dokážeme to silnou indukcí na číslo i.

(0) Protože je p_1 prvočíslo a dělí n, musí podle Lemma 6b.2 dělit i jedno z čísel q_j. Jenže q_j má jen dělitele 1 a q_j a p_1 coby prvočíslo není 1, proto $p_1 = q_j$. Protože jsou prvočísla srovnaná dle velikosti, vyplývá z toho také, že $q_1 \leq q_j = p_1$.

Naopak prvočíslo q_1 dělí n, proto symetricky musí existovat p_j takové, že $q_1 = p_j$, a tedy $p_1 \leq p_j = q_1$.

Tyto dvě nerovnosti dávají $p_1 = q_1$.

(1) Předpokládejme, že už máme $p_1 = q_1, \ldots, p_i = q_i$. Pokud p_{i+1} existuje, pak dělí n a musí existovat q_j takové, že $p_{i+1} = q_j$. Jenže $q_1, \ldots, q_i$ jsou už obsazena jinými p, musí platit $j \geq i + 1$ (takže existuje i q_{i+1} a možná nějaká další). Máme tedy $q_{i+1} \leq q_j = p_{i+1}$. Symetrickým argumentem z existence q_{i+1} dostaneme $p_{i+1} \leq q_{i+1}$, tedy i $p_{i+1} = q_{i+1}$.

Tím je dokončen indukční krok, zároveň z toho vyplývá nemožnost situace $m < M$ či $M < m$.

b) Teď již víme, že oba rozklady zahrnují stejná prvočísla, tedy máme $n = \prod_{i=1}^{m} p_i^{k_i}$ a $n = \prod_{i=1}^{m} p_i^{l_i}$. Potřebujeme ukázat, že $k_i = l_i$ pro všechna $i = 1, \dots, m$. Vezměme nějaké takové i a ze symetrie situace předpokládejme, že $k_i \leq l_i$. Vydělíme oba rozklady číslem $p_i^{k_i}$ a dostaneme dva rozklady pro číslo $\frac{n}{p_i^{k_i}}$. V tom prvním se p_i vůbec nevyskytuje, v tom druhém je s exponentem $l_i - k_i \geq 0$. Ale podle části a) aplikované na tyto dva vydělené rozklady musí mít oba stejná provočísla, což nastane jedině v případě, že $l_i - k_i = 0$, tedy $k_i = l_i$.

Důkaz pro $n \geq 2$ je hotov.

□

Jednoznačnost vlastně platí i pro $n = 1$, ale je to trikem, proto jsme to do věty nezahrnuli. Jak se vůbec vyjádří 1 pomocí prvočísel, když máme podmínku $k_1 > 0$? Zvolíme $m = 0$ (prvočísla žádná nevybíráme), pak se v součinu $\prod_{i=1}^{0}$ násobí přes prázdnou množinu, což je podle definice právě 1. Jiná možnost není.

Vyjádření čísla n jako ve větě říkáme **prvočíselný rozklad**. V mnoha situacích máme rádi jednoznačnost z části b), ale někdy je pro změnu výhodné si dovolit přidat do rozkladu prvočísla s mocninou 0 (třeba $13 = 13 \cdot 3^0 = 13 \cdot 23^0 \cdot 33^0$), což například umožní sjednotit použitá prvočísla pro více čísel. Dobrým příkladem je následující aplikace prvočíselného rozkladu na dělitelnost.

Lemma 6b.5.
Nechť $a \in \mathbb{N}$ je číslo s prvočíselným rozkladem $\prod_{i=1}^{m} p_i^{k_i}$, nechť $d \in \mathbb{N}$. Číslo d dělí a právě tehdy, když existují čísla $K_i \in \mathbb{N}_0$ splňující pro všechna i podmínku $0 \leq K_i \leq k_i$ taková, že $d = \prod_{i=1}^{m} p_i^{K_i}$.

Přeloženo do lidštiny, aby číslo d dělilo číslo a, nemůže mít v rozkladu prvočísla jiná, než jsou v a, a prvočíslo, které v d je, tam nemůže být vicekrát, než je v a.

Důkaz je variací na důkaz předchozí Věty. Pokud d dělí a, tak se pro každé p z rozkladu d ukáže, že musí být v rozkladu a, načež se vydělením p^k ukáže, že v čísle a musí být exponent alespoň tak velký jako u d. Pokud naopak nějaké prvočíslo p z rozkladu a chybí v daném rozkladu d, tak jej tam prostě přidáme s mocninou 0.

Odtud hned dostaneme následující tvrzení, které matematicky potvrdí oblíbený způsob hledání gcd a lcm pro menší čísla. Obě čísla napíšeme pomocí prvočíselného rozkladu, gcd se pak získá pomocí nejmenších mocnin a lcm pomocí největších mocnin u prvočísel (pokud nějaké prvočíslo z jednoho rozkladu chybí v druhém, dodáme jej tam s mocninou 0). Formálně řečeno:

Fakt 6b.6.
Nechť $a, b \in \mathbb{N}$. Předpokládejme, že máme prvočísla $p_1 < \cdots < p_m$ a čísla $k_i, l_i \in \mathbb{N}_0$ taková, že $a = \prod_{i=1}^{m} p_i^{k_i}$ a $b = \prod_{i=1}^{m} p_i^{l_i}$. Pak $\gcd(a,b) = \prod_{i=1}^{m} p_i^{\min(k_i,l_i)}$ a $\operatorname{lcm}(a,b) = \prod_{i=1}^{m} p_i^{\max(k_i,l_i)}$.

Důkaz (z povinnosti)**:** 1) Označme $n = \prod_{i=1}^{m} p_i^{\min(k_i,l_i)}$. Protože má n ve svém rozkladu stejná prvočísla jako a i b a jejich exponenty splňují $\min(k_i, l_i) \leq k_i$ a $\min(k_i, l_i) \leq l_i$, podle předchozího Lemmatu $n \mid a$ a $n \mid b$. Je to tedy společný dělitel. Zbývá ukázat, že je největší.

Nechť d je nějaký společný dělitel a, b. Pak podle předchozího Lemmatu musí existovat čísla K_i taková, že $d = \prod_{i=1}^{m} p_i^{K_i}$ a přitom $K_i \leq k_i$ a $K_i \leq l_i$ pro všechna i. To pak ale znamená, že $K_i \leq \min(k_i, l_i)$ pro všechna i, tudíž zase podle Lemmatu $d \mid n$.

Takže n je opravdu největší společný dělitel a, b.

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

□

Z toho hned dostaneme zajímavý důkaz Věty 6a.14. Pro všechna $k, l \in \mathbb{N}_0$ platí $\max(k,l) + \min(k,l) = k + l$ (zkuste si to rozmyslet, stačí rozebrat varianty podle toho, které z těcho čísel je větší), což dává

$$\begin{aligned}\gcd(a,b) \cdot \operatorname{lcm}(a,b) &= \prod_{i=1}^{m} p_i^{\min(k_i,l_i)} \cdot \prod_{i=1}^{m} p_i^{\max(k_i,l_i)} = \prod_{i=1}^{m} p_i^{\min(k_i,l_i)+\max(k_i,l_i)} \\ &= \prod_{i=1}^{m} p_i^{k_i+l_i} = \prod_{i=1}^{m} p_i^{k_i} \cdot \prod_{i=1}^{m} p_i^{l_i} = a \cdot b.\end{aligned}$$

Pro úplnost ukážeme několik příkladů na hledání gcd a lcm pomocí rozkladu.

Příklad 6b.b: Uvažujme čísla 24 a 60. Jejich prvočíselné rozklady jsou $24 = 2^3 \cdot 3$ a $60 = 2^2 \cdot 3 \cdot 5$, takže máme $\gcd(24, 60) = \gcd(2^3 \cdot 3 \cdot 5^0, 2^2 \cdot 3 \cdot 5) = 2^2 \cdot 3 = 12$ a $\operatorname{lcm}(24, 60) = 2^3 \cdot 3 \cdot 5 = 120$.

Podobně $\gcd(2 \cdot 3^2 \cdot 5 \cdot 7^2, 3 \cdot 7^4 \cdot 13) = 3 \cdot 7^2$ a $\operatorname{lcm}(2 \cdot 3^2 \cdot 5 \cdot 7^2, 3 \cdot 7^4 \cdot 13) = 2 \cdot 3^2 \cdot 5 \cdot 7^4 \cdot 13$.

△

Tento postup je ovšem jako obecný přístup neperspektivní, protože prvočíselný rozklad daného čísla je jedním z nejnáročnějších problémů.

6b.7 Rozklad na prvočísla. Zásadním problém je najít k danému číslu n nějaké prvočíslo p, které jej dělí. Pokud toto umíme, tak aplikací téhož postupu na číslo n/p atd. získáme nakonec rozklad. Budeme se tedy soustředit na problém nalezení prvočíselného dělitele.

Jako první metoda se nabízí prostě zkoušet dělit rozkládané číslo n čísly $2, 3, 4, \ldots$. To asi čtenář zná. Vezme 45, zkusí vydělit dvojkou, nic, zkusí trojkou, zásah, máme $45 \div 3 = 15$. Pokračujeme s patnáctkou, zkusíme zase trojku, bingo, $15 \div 3 = 5$, rozklad hotov, $45 = 3^2 \cdot 5$.

U malých čísel toto může fungovat efektivně, zejména když si vzpomeneme na rozličná kritéria dělitelnosti, viz například cvičení 6a.11 a 7a.4.

Pro větší čísla je tento přístup totální katastrofa, protože pokud máme smůlu (n je prvočíslo), tak musíme projít všechna čísla $1, 2, \ldots, n$, náročnost algoritmu je tedy n, a to jsme ještě ani nevzali v úvahu, že samotné rozhodování, zda nějaké číslo d dělí n, také něco stojí. Jisté zlepšení se nabízí.

! **Fakt 6b.8.**
Jestliže je n složené číslo, pak existuje jeho prvočíselný dělitel menší či roven číslu $\sqrt{n}$.

Důkaz: Předpokládejme, že $n = ab$ a $a, b > 1$. Tvrdíme, že buď $a \leq \sqrt{n}$ nebo $b \leq \sqrt{n}$. V opačném případě bychom totiž měli $ab > \sqrt{n} \cdot \sqrt{n} = n$.

Takže předpokládejme, že třeba $a \leq \sqrt{n}$. Vezměme libovolné prvočíslo z p z prvočíselného rozkladu a, to pak splňuje $p \leq a \leq \sqrt{n}$ a dělí n.

□

To znamená, že pokud dané číslo n nedělí nic až po $\sqrt{n}$, tak už víme, že je to prvočíslo. Podobně lze ukázat, že pokud nějaké číslo n vzniklo jako součin tří prvočísel, pak to nejmenší z nich nesmí být větší než $\sqrt[3]{n}$, a tak dále.

Náročnost našeho naivního algoritmu (kterému se také říká „direct search algorithm“ či „trial division“) je tedy $\sqrt{n}$ kroků, když do toho započítáme náročnost dělení, budeme na tom ještě hůř. V praxi se často velikost čísla soudí podle počtu cifer $m = \log_2(n)$, pak $n = 2^m$ a lze říci, že v nejhorším případě potřebujeme pro m-ciferné číslo použít $2^{m/2}$ kroků, což je hodně.

Při postupném dělení čísly $2, 3, 4, \ldots$ by pomohlo, kdybychom měli tabulku prvočísel, protože pak bychom nemuseli dělit n všemi čísly až po $\sqrt{n}$, stačilo by brát jen prvočísla. Těch je relativně málo, například jsme viděli, že je jen 25 prvočísel menších než 100. To znamená, že kdybychom chtěli udělat rozklad čísla 10003, tak bychom nemuseli zkoušet dělit všemi čísly až po $\sqrt{10001} \sim 100$, ale jen oněmi 25 prvočísly.

Takovou tabulku naštěstí nemusíme tvořit postupným testováním čísel, existuje metoda, která to zvládá relativně efektivně.

! **Příklad 6b.c:** Pokud potřebujeme identifikovat všechna prvočísla v rozmezí 1 až n, pak můžeme s úspěchem použít metodu zvanou **Eratosthenovo síto** (sieve of Eratosthenes). Funguje to následovně.

Nejprve si všechna čísla od 2 do n napíšeme na papír, třeba do tabulky nebo za sebe, to je jedno:

$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, \ldots$

Začneme s $a = 2$. Je to prvočíslo, tak jej označíme a pak ze seznamu vyškrtneme všechny jeho násobky:

$\boxed{2}, 3, \ , 5, \ , 7, \ , 9, \ , 11, \ , 13, \ , 15, \ , 17, \ , \ldots$

Podíváme se do seznamu a najdeme první další nevyškrtnuté a neoznačené číslo, je to $a = 3$. Musí to být prvočíslo, tak jej označíme a pak ze seznamu vyškrtneme všechny jeho násobky, které tam ještě zbyly:

$\boxed{2}, \boxed{3}, \ , 5, \ , 7, \ , \ , \ , 11, \ , 13, \ , \ , \ , 17, \ , \ldots$

Podíváme se do seznamu a najdeme první další neoznačené číslo, tedy $a = 5$. Označíme jej coby prvočíslo a pak ze seznamu vyškrtneme atd.: $\boxed{2}, \boxed{3}, \ , \boxed{5}, \ , 7, \ , \ , \ , 11, \ , 13, \ , \ , \ , 17, \ , \ldots$

Takto pokračujeme, dokud nedojdeme k $\sqrt{n}$. Všimněte si, že nemusíme dělit, jen sčítáme (3, $3+3$, $6+3$, $9+3$, $\ldots$), což je mnohem lepší, a ještě hezčí je, že k vyřazení každého neprvočísla jsme potřebovali jen jednu operaci. Je to tedy velmi efektivní metoda.

△

Metoda je to sice pěkná, ale my většinou potřebujeme faktorizovat či testovat na prvočíselnost čísla řádu třeba 10^{200} a vyrábět si kvůli tomu tak velké monstrózní síto by bylo pořád nepředstavitelně drahé. Tak či onak, pokud zkoušíme najít rozklad n-ciferného (n-bitového) čísla pomocí podobných přímočarých metod, tak se v zásadě díváme na náročnost okolo $e^{n/2}$ operací.

Faktorizaci už teď opustíme, poznamenejme jen, že nejpoužívanější veřejné šifrování na Internetu je založeno na tom, že faktorizovat velké číslo by i dnešním superpočítačům zabralo desítky až stovky let. Vrátíme se k tomu v kapitole 7a, v příkladě 7a.m si popovídáme i o dokazování, že nějaké číslo je či není prvočíslem.

Ve zbytku této sekce se podíváme blíže na prvočísla. Začneme jednoduchou odpovědí na otázku, kolik jich je.

! **Věta 6b.9.**
Pročísel je nekonečně mnoho.

Důkaz (poučný)**:** Ukážeme si klasický Euklidův důkaz, takže jdeme až ke starým Řekům, cca 300 př.n.l. Dělá se sporem, předpokládáme, že existuje jen konečně mnoho prvočísel $p_1, p_2, \dots, p_m$.

Vezměme číslo $a = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$. Podle Faktu 6b.1 existuje prvočíslo p takové, že dělí a. Podle předpokladu to ale musí být jedno z těch p_i, proto také p dělí ten součin $p_1 \cdot p_2 \cdot \ldots \cdot p_m$. Máme $p \mid a$, $p \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_m)$, proto nutně p dělí jejich rozdíl, viz Důsledek 6a.4 (ii). Takže $p \mid 1$ a to je spor, neboť $p \geq 2$.

□

Zajímavé je, že ve skutečnosti jsou čísla typu $a = p_1 \cdot p_2 \cdot \ldots \cdot p_m + 1$ docela často prvočísla, třeba $2 \cdot 3 + 1 = 7$, $2 \cdot 3 \cdot 5 + 1 = 31$ nebo $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. Známá čísla tohoto typu se používají pro testování kvality nových superpočítačů.

Víme, že prvočísel je nekonečně mnoho, což samozřejmě už po staletí nedá lidem spát a snaží se najít co největší. Je to věc prestiže, výsledky jsou kombinací brutální výpočetní síly a vysoce sofistikovaných matematických metod (viz třeba příklad 7a.m). Má to ale i praktické důsledky, třeba pro bezpečnost šifrování. Posledních 300 let byla největší nalezená prvočísla ve tvaru $2^p - 1$ pro prvočíslo p. Samozřejmě ne každé takové číslo je prvočíslem, to by bylo moc snadné, například $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ jsou prvočísla, ale $2^{11} - 1 = 2047 = 23 \cdot 89$. Říká se jim Mersennova prvočísla a jsou populární díky tomu, že výrazy typu $2^p - 1$ se relativně dobře testují na prvočíselnost.

Sice jsme odpověděli na otázku, kolik je prvočísel, ale to byla snadná odpověď. Lepší otázka je, kolik jich je relativně, třeba takto: Označme pro $n \in \mathbb{N}$ jako $\pi(n)$ počet prvočísel p splňujících $p \leq n$ (seznámek $2, 3, 5, 7$ ukazuje, že $\pi(10) = 4$, už třeba víme, že $\pi(100) = 25$). Jak rychle tato funkce roste? Hluboké výsledky říkají, že pro velká n je $\pi(n)$ přibližně rovno $\frac{n}{\ln(n)}$. (Má to dost komplikované důkazy, jako hypotéza se to objevilo v 19. století, první důkaz 1896.) Znamená to tedy, že relativní hustota prvočísel mezi prvními n čísly je přibližně $\frac{1}{\ln(n)}$, takže se zvětšujícím se n klesá, tedy prvočísel je čím dál relativně méně.

Tento výsledek se dá interpretovat různými způsoby, třeba takto: Jestliže si mezi čísly 1 až n zvolíte náhodně jedno, tak je pravděpodobnost $\frac{1}{\ln(n)}$, že to bude prvočíslo. Ještě jinak: Tato pravděpodobnost je nepřímo úměrná počtu cifer čísla n (čím víc cifer, tím menší pravděpodobnost). Dá se také říct, že průměrná vzdálenost mezi prvočísly okolo čísla n je zhruba $\ln(n)$.

Přesto je prvočísel v jistém smyslu dost. Připomeňme si známou divergentní harmonickou řadu $\sum_{k=1}^{\infty} \frac{1}{k} = \infty$. Když z té řady vynecháme relativně dost členů (neboli necháme si jich relativně málo), tak začne konvergovat. Pokud například označíme jako M množinu všech druhých mocnin přirozených čísel, tak již $\sum_{k \in M} \frac{1}{k}$ konverguje. Když si ale vezmeme množinu P všech prvočísel, pak $\sum_{p \in P} \frac{1}{p} = \infty$ (Eulerův výsledek). Takže jich zase tak málo není.

Víme, že prvočísla nám dají všechna přirozená čísla prostřednictvím násobení. Zajímavá otázka je, jestli je jich dost na to, aby nám dala přirozená čísla prostřednictvím sčítání. K tomu se váže Goldbachova hypotéza (1742), která říká: Každé liché $n \in \mathbb{N}$ větší než 5 je součtem tří prvočísel. Tato hypotéza má i ekvivalentní vyjádření: Každé sudé $n \in \mathbb{N}$ větší než 2 je součtem dvou prvočísel. Neví se, zda toto platí, zatím je dokázáno, že každé sudé $n \in \mathbb{N}$ větší než 2 je součtem nejvýše 6 prvočísel, což je od cíle dost daleko.

Hodně úsilí šlo do odhalování různých pravidelností ve výskytu prvočísel. Hned na začátku je třeba říct, že celkově v jejich výskytu žádná pravidelnost není. Mohou se ale vyskytovat zajímavé pravidelnosti dočasné, lokální. Několik výsledků:

• Kdykoliv zvolíme a, b nesoudělné, pak v aritmetické posloupnosti $\{an+b\}$ najdeme nekonečně mnoho prvočísel (Dirichletova věta).

• V opačném směru je tu hypotéza: Pro libovolné m existuje $a, d \in \mathbb{N}$ takové, že $a, a+d, a+2d, \ldots, a+md$ jsou prvočísla. Krátce řečeno, lze vytvořit konečné aritmetické posloupnosti libovolných délek, které se skládají z prvočísel. Zdá se, že je to pravda, v roce 2004 byl prezentován důkaz, ale byl tak hrozný, že ještě v době psaní tohoto skripta nebyl pořádně prověřen.

Určitě ale víme, že nejde najít nekonečnou aritmetickou posloupnost z prvočísel.

• Pro libovolné $n \in \mathbb{N}$ existuje mezi prvočísly někde mezera délky alespoň n. Ekvivalentně, existuje n po sobě jdoucích čísel takových, že jsou složená. Toto je vlastně snadné, začne se číslem $(n+1)!+2$ a skončíme $(n+1)!+(n+1)$. Pro každé $2 \leq k \leq n+1$ totiž platí, že k dělí $(n+1)!$, proto jsou pak čísla $(n+1)!+k$ dělitelná k a tedy složená.

• Hodně by pomohlo najít funkci takovou, aby $f(n)$ bylo prvočíslo pro všechna $n \in \mathbb{N}$. Zatím ji nikdo nenašel, i když se zajímavé věci našly, například funkce $f(n) = n^2 - n + 41$, která dává prvočísla pro $n = 1, \ldots, 40$, ale pak už ne, $f(41) = 41^2$. Jenže takovéto polynomy jsou stejně slepá ulička, pro každý polynom p s celočíselnými koeficienty existuje $y \in \mathbb{N}$ takové, že $p(y)$ je složené.

I to je vlastně snadné. Nechť $p(x) = a_n x^n + \cdots + a_0$. Jestliže $a_0 \neq 0$, pak $f(|a_0|) = a_0(\pm a_n a_0^{n-1} \pm \cdots \pm 1)$ a máme číslo složené, v případě $a_0 = 0$ pak $p(x) = x(a_n x^{n-1} + \cdots + 1)$ a stačí dosadit jakékoliv $a \in \mathbb{N}$.

• Není známo, zda existuje nekonečně mnoho prvočísel typu n^2+1. Zatím je známo, že pro nekonečně mnoho n je n^2+1 buď prvočíslo, nebo součin dvou prvočísel.

• Není známo, zda existuje nekonečně mnoho dvojic p, $p+2$, kde obě jsou prvočísla (známe třeba dvojice 3 a 5, 11 a 13, 17 a 19 atd).

Takto by se dalo pokračovat ještě dlouho, ale jako úvod do teorie čísel to stačí.

Cvičení

Cvičení 6b.1 (rutinní)**:** Najděte faktorizaci následujících čísel: (i) 156; (ii) 165; (iii) 504.

Cvičení 6b.2: Dokažte/vyvraťte: Existují tři po sobě jdoucí lichá čísla, která jsou prvočísla, tj. p, $p+2$, $p+4$.

Cvičení 6b.3 (drsné)**:** Najděte nějaký předpis používající prvočísla a prvočíselné rozklady pro následující posloupnosti:
(i) $0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, \ldots$
(ii) $1, 2, 3, 2, 5, 2, 7, 2, 3, 2, 11, 2, 13, 2, \ldots$
(iii) $1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 5, \ldots$
(iv) $1, 2, 3, 3, 5, 5, 7, 7, 7, 7, 11, 11, 13, 13, \ldots$
(v) $1, 2, 6, 30, 210, 2310, 30030, 510510, 9699690, 223092870, \ldots$

Cvičení 6b.4 (poučné)**:** Nechť $a_1, a_2, \ldots, a_n \in \mathbb{N}$. Dokažte, že když jsou a_i po dvou nesoudělná, pak $\operatorname{lcm}(a_1, a_2, \ldots, a_n) = a_1 \cdot a_2 \cdots a_n$.

Řešení:
6b.1: (i): $156 = 2^2 \cdot 3 \cdot 13$;
(ii): $165 = 3 \cdot 5 \cdot 11$;
(iii): $504 = 2^3 \cdot 3^2 \cdot 7$.
6b.2: $3, 5, 7$.
6b.3: (i): prvočíslo ano/ne; (ii): a_n je nejmenší prvočíselný dělitel n; (iii): počet kladných dělitelů; (iv): a_n je největší prvočíslo $\leq n$; (v): součin prvních $n-1$ prvočísel.
6b.4: Označme $a = a_1 \cdot a_2 \cdots a_n$. Protože $a_i \,|\, a$, pak také $\operatorname{lcm}(a_1, a_2, \ldots, a_n) \,|\, a$. Potřebujeme opačný směr.
Nechť $a = \prod_j p_j^{k_j}$ je prvočíselný rozklad. Zvolme nějaké j. Pak podle Lemma 6b.2 musí existovat i takové, že $p_j \mid a_i$. Protože jsou všechna a_k po dvou nesoudělná, tak už žádné jiné a_k nemůže mít p_j jako dělitele, tudíž dokonce $p_j^{k_j} \mid a_i$, tedy i $p_j^{k_j} \mid \operatorname{lcm}(a_1, a_2, \ldots, a_n)$. Ukázali jsme, že všechny prvočíslé faktory $p_j^{k_j}$ z rozkladu a dělí $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$, tedy a dělí $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$.

6c. Diofantické rovnice

Teď si ukážeme jedno praktické použití toho, co jsme se zatím naučili. V mnoha aplikacích pracujeme zcela přirozeně ve světě celých čísel, což je ale problém, protože naše obvyklé metody řešení rovnic pracují v množině reálných čísel. Ilustruje to následující příklad:

Příklad 6c.a: Představme si letadlo, kde sedadlo v turistické třídě zabírá 6 decimetrů délky trupu, zato sedadlo v business class zabírá 8 dm. Celková délka trupu je 305 dm. My potřebujeme rozdělit letadlo na turistickou a lepší třídu, čili vybrat, kolik řad bude turistických (označme to t) a kolik bude pro business class b. Samozřejmě nechceme plýtvat prostorem, takže dostáváme rovnici $6t + 8b = 305$.

Takovéto rovnice umíme řešit. Víme, že má nekonečně mnoho řešení, snadno se zjistí, že pro libovolnou hodnotu parametru t je dvojice $\left(t, \frac{305}{8} - \frac{3}{4}t\right)$ řešením.

My ale těžko budeme do letadla cpát třeba tři čtvrtiny sedadla. Zajímají nás tedy výhradně celočíselná řešení. Nabízí se nápad začít zkoušet, jestli pro nějakou hodnotu t nevyjdou t a b celé, ale zrovna u tohoto příkladu by to trvalo docela dlouho, protože to nikdy nevyjde.

Je tedy jasné, že omezit se na celá čísla může znamenat, že běžné postupy začnou selhávat. Je potřeba vyvinout specializované nástroje.

△

Rovnice, kde máme koeficienty i očekávaná řešení celá, se nazývají diofantické rovnice (Diophantine euqations). Jmenují se podle člověka jménem Diofanus z Alexandrie, který je zkoumal ve 3. století, ale najdeme je třeba i ve starých textech indických (už od 800 př.n.l s důležitými aplikacemi v astronomii, okolo roku 800 zase jistý Brahmagupta zkoumal rovnici $x^2 + y^2 = z^2$ neboli pravoúhlé trojúhelníky s celočíselnými stranami). Většinou byly zkoumány izolovaně, ucelená teorie přišla teprve ve 20. století.

Mohou se zkoumat buď rovnice velice obecné, pak se toho nevyzkoumá moc, nebo se omezujeme na pěknější poddruhy. Jednou zkoumanou třídou jsou rovnice polynomiální, tedy rovnice ve tvaru $p(x_1, x_2, \ldots, x_n) = 0$, kde p je polynom. Dobrým příkladem je rovnice o třech proměnných $x^n + y^n = z^n$, o jejíž celočíselná řešení se zajímal v 17. století Fermat a tvrdil, že pro $n \geq 3$ žádná nejsou, což je ona slavná Fermatova věta. My se zde zaměříme na rovnice typu, který jsme potkali v leteckém příkladě.

! **Definice.**
Pojmem **lineární diofantická rovnice** označujeme libovolnou rovnici typu $ax + by = c$ s neznámými x, y, kde $a, b, c \in \mathbb{Z}$ a vyžadujeme také řešení $x, y \in \mathbb{Z}$.

Takovéto rovnice nám mohou odpovědět třeba na tyto otázky:
- Lze vyplatit c korun pomocí mincí o hodnotách a a b?
- Lze vyměřit c litrů pomocí nádob o objemu a a b?

O řešitelnosti má konečné slovo následující tvrzení.

! **Věta 6c.1.**
Lineární diofantická rovnice $ax + by = c$ má alespoň jedno řešení právě tehdy, když c je násobkem $\gcd(a, b)$.

Důkaz (poučný)**:** 1) $\Longrightarrow$: Předpokládejme, že existují $x, y \in \mathbb{Z}$ takové, že $ax + by = c$. Protože $\gcd(a, b)$ dělí a i b, musí podle Důsledku 6a.4 (i) dělit i c.

2) $\Longleftarrow$: Předpokládejme, že $c = k \gcd(a, b)$ pro nějaké $k \in \mathbb{Z}$. Podle Bezoutovy rovnosti existují $A, B \in \mathbb{Z}$ takové, že $Aa + Bb = \gcd(a, b)$. Pak $kAa + kBb = k \gcd(a, b)$ neboli $a(kA) + b(kB) = c$, tedy celá čísla $x = kA$, $y = kB$ řeší $ax + by = c$.

□

Víme tedy, kdy má taková úloha řešení, důkaz nám dokonce dává návod, jak jedno najít pomocí Bezouta.

S Algoritmus 6c.2. pro nalezení nějakého celočíselného řešení x, y rovnice $ax + by = c$.

0. Jestliže c není násobkem $\gcd(a, b)$, tak řešení neexistuje.

1. Jestliže c je násobkem $\gcd(a, b)$, tak například rozšířeným Euklidovým algoritmem najděte $A, B \in \mathbb{Z}$ takové, že $\gcd(a, b) = Aa + Bb$. Když tuto rovnici vynásobíme (celým) číslem $\frac{c}{\gcd(a, b)}$, tak hned vidíme, že čísla $x = A\frac{c}{\gcd(a, b)}$, $y = B\frac{c}{\gcd(a, b)}$ jsou řešením dané rovnice.

△

Příklad 6c.b: Lze vyplatit 1250 korun pomocí mincí o hodnotách 6 a 15? Zajímá nás tedy řešení rovnice $6x + 15y = 1250$. Víme, že $\gcd(6, 15) = 3$, a číslo 1250 není dělitelné třemi, proto to podle Věty nejde.

△

Příklad 6c.c: Lze odměřit 1251 litrů pomocí nádob s objemem 6 a 15 litrů?

Doplňující otázka: Ve kterém filmu se řešila podobná úloha?

Hledáme řešení rovnice $15x + 6y = 1251$, dali jsme si větší číslo jako a, abychom to měli připraveno na rozšířený Euklidův algoritmus. Hned vidíme, že $\gcd(15, 6) = 3$, a protože $\frac{1251}{3} = 417 \in \mathbb{Z}$, je tato úloha řešitelná. Potřebujeme koeficienty Bezoutovy identity.

a, b	q	A	B
15		1	0
6		0	1

a, b	q	A	B
15		1	0
6	2	0	1
3		1	-2

a, b	q	A	B
15		1	0
6	2	0	1
3•	2	1•	-2•
0			

Máme $3 = 1 \cdot 15 + (-2) \cdot 6$. Tuto rovnost vynásobíme číslem 417, u těch součinů opatrně, potřebujeme, aby tam zůstaly koeficienty rovnice 6 a 15. Dostáváme $15 \cdot 417 + 6 \cdot (-834) = 1251$. Porovnáním se zadanou rovnicí vidíme, že $x = 417$ a $y = -834$ je hledané řešení. Takže nejprve do nádrže přidáme 417 krát obsah patnáctilitrové nádoby, pak odebereme 834 krát obsah šestilitrové a zůstane nám 1251 litrů. Z praktického pohledu asi bude lepší nalévání a vybírání střídat, abychom nepotřebovali nádrž o objemu $417 \cdot 15 = 6225$.

Poznámka: V případě, že vidíme $\gcd(a, b)$ hned a dělí c, tak se může vyplatit celou rovnici tímto číslem pokrátit, čímž samozřejmě vznikne ekvivalentní úloha, která se řeší stejně, ale při výpočtech používáme menší čísla. V našem příkladě bychom z rovnice $15x + 6y = 1251$ dělením trojkou dostali rovnici $5x + 2y = 417$, na kterou pak aplikujeme stejný postup. Rozšířený Euklidův algoritmus aplikovaný na čísla $5, 2$ (s gcd rovným 1) dá rovnost $1 = 1 \cdot 5 + (-2) \cdot 2$, vynásobíme ji číslem 417 a dostaneme $417 = 5 \cdot 417 + 2 \cdot (-834)$, odtud pak máme hledaná řešení $x = 417$ a $y = -834$. Dokonce ani nemusíme používat Euklidův algoritmus, protože rovnost $1 = 1 \cdot 5 + (-2) \cdot 2$ lze snadno uhodnout.

Doplňující odpověď: Die Hard 3 (with a Vengeance). Bruce Willis neznal diofantické rovnice a málem na to doplatil.

△

Toto řešení není úplně uspokojivé, nabízí se otázka, zda náhodou neexistuje i jiné a úspornější, v ideálním případě takové, které by vodu jen nalévalo. U Bezoutovy věty výše jsme zmínili, že možností, jak gcd vyjádřit pomocí a, b, je obecně hodně, z nich dostáváme více řešení diofantické rovnice. Takže odpověď zní, že ano, máme si z čeho vybírat. Posouváme se tedy k další otázce: Máme-li řešitelnou lineární diofantickou rovnici, chceme určit množinu všech jejích řešení.

Na to se budeme muset hlouběji zamyslet nad tím, jakou má tato množina strukturu. V této chvíli bude lepší dívat se na určité řešení jako na vektor $(x, y) \in \mathbb{Z}^2$, například v případě s vodou bychom mohli napsat, že $(417, -834)$ je řešením dané rovnice. Množina všech řešení je pak určitou podmnožinou postoru $\mathbb{Z}^2$.

Čtenáře obeznámeného s lineární algebrou následující pasáže jistě nepřekvapí, protože už něco podobného viděl u soustav lineárních rovnic. Linearita je mocná vlastnost, a jakmile ji máme, spousta věcí už vyplyne.

! **Definice.**
Je-li dána lineární diofantická rovnice $ax + by = c$, pak definujeme její **přidruženou homogenní rovnici** jako $ax + by = 0$.

Následující tvrzení je klasikou pro lineární rovnice a umožní nám redukovat problematiku hledání všech řešení jen na případ homogenních rovnic.

! **Věta 6c.3.**
Uvažujme lineární diofantickou rovnici $ax + by = c$. Nechť $(x_p, y_p) \in \mathbb{Z}^2$ je nějaké její řešení.
$(x, y) \in \mathbb{Z}^2$ je řešení této rovnice právě tehdy, když existuje $(x_h, y_h) \in \mathbb{Z}^2$ takové, že $(x, y) = (x_p, y_p) + (x_h, y_h)$ a (x_h, y_h) řeší přidruženou homogenní rovnici.

Důkaz (poučný)**:** Mějme nějaké řešení (x_p, y_p) dané rovnice.

2) $\Longleftarrow$: Předpokládejme, že $(x_h, y_h) \in \mathbb{Z}^2$ řeší přidruženou homogenní rovnici. Dosaďme tedy $x = x_p + x_h$ a $y = y_p + y_h$ do dané rovnice, začneme levou stranou a uvidíme, co se z ní vyvrbí:

$ax + by = a(x_p + x_h) + b(y_p + y_h) = (ax_p + by_p) + (ax_h + by_h) = c + 0 = c$. Ano, (x, y) je opravdu řešením dané rovnice.

1) $\Longrightarrow$: Předpokládejme, že (x, y) řeší danou rovnici. Definujme $x_h = x_p - x$ a $y_h = y_p - y$. Pak $(x, y) = (x_p, y_p) + (x_h, y_h)$ a $(x_h, y_h) \in \mathbb{Z}^2$, zbývá ukázat, že (x_h, y_h) řeší přidruženou homogenní rovnici. Zkusíme dosadit do její levé strany, využijeme pak toho, že (x_p, y_p) i (x, y) jsou řešení:

$ax_h + by_h = a(x_p - x) + b(y_p - y) = (ax_p + by_p) - (ax + by) = c - c = 0$. Ano, (x_h, y_h) řeší přidruženou homogenní rovnici.

□

! Takže jakmile už jedno konkrétní řešení (x_p, y_p) dané diofantické rovnice máme (tomu pak říkáme **partikulární řešení** a umíme ho najít tím algoritmem výše), tak lze množinu všech (celočíselných) řešení získat takto:

$$\{(x_p, y_p) + (x_h, y_h);\ (x_h, y_h) \in \mathbb{Z}^2\ \wedge\ ax_h + by_h = 0\}.$$

Zbývá vymyslet, jak zcela řešit homogenní rovnice, tedy jak najít všechna celočíselná řešení takových rovnic. To nám prozradí následující věta, ale nejprve si to zkusme rozmyslet. Rovnici $ax + by = 0$ lze přepsat jako $ax = -by$. Snadno pak uhádneme jedno řešení, stačí dát třeba $x = -b$ a $y = a$. Všimněme si také, že jakmile máme jedno řešení (x_0, y_0), tak získáme další vynásobením čísel x_0, y_0 libovolým celým číslem k, protože toto k lze po dosazení do rovnice $ax = -by$ na obou stranách vykrátit. Řešení tedy bude nekonečně mnoho, například všechna ve tvaru $x = -bk$, $y - ak$ pro $k \in \mathbb{Z}$. Kritická otázka ovšem je, jestli jsou i jiná.

Představme si na chvíli, že a, b v rovnici $ax = -by$ jsou nesoudělná. Koeficient b dělí levou stranu ax, ale je nesoudělný s a, takže (viz Lemma 6a.23) musí dělit x. Jinými slovy, řešení x hledáme jen mezi násobky b. Obdobně budeme hledat y jen mezi násobky čísla a. Ona řešení z předchozího odstavce tedy budou (pro a, b nesoudělná) jediná možná.

Co když a, b nesoudělná nejsou? Pak jsou i řešení jiná než $(-kb, ka)$. Například u rovnice $4x + 6y = 0$ nám předchozí postup dává řešení ve tvaru $x = -6k$, $y = 4k$ neboli $(-6k, 4k)$ pro $k \in \mathbb{Z}$, ale vidíme také řešení $x = 3$, $y = -2$, které nelze volbou $k \in \mathbb{Z}$ získat z toho obecného vzorce. Situace je tedy obecně složitější.

Naštěstí existuje jednoduchý trik: Když rovnici $ax = -by$ vydělíme číslem $\gcd(a, b)$, vznikne ekivalentní rovnice $\frac{a}{\gcd(a,b)}x = -\frac{b}{\gcd(a,b)}y$, která už má (celé) nesoudělné kořeny a tudíž dokážeme najít všechna řešení postupem předvedeným výše. Dostaneme se tak k následujícím tvrzení.

! **Věta 6c.4.**
Uvažujme rovnici $ax + by = 0$ pro $a, b \in \mathbb{Z}$. Pak množina všech jejích celočíselných řešení je

$$\left\{\left(k\frac{b}{\gcd(a,b)}, -k\frac{a}{\gcd(a,b)}\right);\ k \in \mathbb{Z}\right\}.$$

Důkaz (poučný)**:** 1) Nejprve ověříme, že dvojice $x = k\frac{b}{\gcd(a,b)}$, $y = -k\frac{a}{\gcd(a,b)}$ jsou opravdu řešení ze $\mathbb{Z}$. Celočíselnost plyne z toho, že $\frac{b}{\gcd(a,b)}$ a $\frac{a}{\gcd(a,b)}$ jsou celá čísla, po dosazení x, y do rovnice pak okamžitě dostáváme $ax + by = ak\frac{b}{\gcd(a,b)} - bk\frac{a}{\gcd(a,b)} = 0$. Takže to souhlasí.

2) Zbývá ukázat, že řešení daná tímto předpisem jsou všechna, tj. že žádné jiné neexistuje. Nechť je tedy x, y nějaké řešení rovnice $ax + by = 0$. Vydělíme ji číslem $\gcd(a, b)$ a převedeme jeden člen na druhou stranu: $\frac{b}{\gcd(a,b)}y = -\frac{a}{\gcd(a,b)}x$. Vidíme, že celé číslo $\frac{b}{\gcd(a,b)}$ musí dělit $\frac{a}{\gcd(a,b)}x$, jenže podle Faktu 6a.9 jsou $\frac{b}{\gcd(a,b)}$ a $\frac{a}{\gcd(a,b)}$ nesoudělná čísla, tudíž musí podle Lemma 6a.23 číslo $\frac{b}{\gcd(a,b)}$ dělit x. Existuje tedy $k \in \mathbb{Z}$ takové, že $x = k\frac{b}{\gcd(a,b)}$, z rovnice $by = -ax$ pak snadno dostaneme příslušný vzorec pro y.

□

Pozorný čtenář si jistě všimnul, že ve znění věty je znaménko mínus u y, zatímco v úvahách před větou bylo u x. Vysvětlení je snadné, nás zajímá množina všech řešení a tam na umístění znaménka nesejde. Pokud bychom například při řešení rovnice $3x + 4y = 0$ použili intuitivní přístup předvedený před Větou, dostaneme množinu $x = -4k$, $y = 3k$ pro $k \in \mathbb{Z}$. Volbou $k = 3$ pak dostaneme konkrétní řešení $x = -12$, $y = 9$ neboli $(-12, 9)$. Pokud bychom použili vzorec $(4k, -3k)$ z věty, pak totéž řešení dostaneme volbou $k = -3$. To ukazuje, proč v případě, že necháme k proběhnout všemi celými čísly, dostáváme nakonec v obou případech shodné množiny dvojic. V praxi většinou volíme tu variantu, která nám přijde příjemnější, například u rovnice $10x - 15y$ dostáváme buď řešení ve tvaru $(3k, 2k)$, $k \in \mathbb{Z}$ nebo ve tvaru $(-3k, -2k)$, $k \in \mathbb{Z}$, první se mi líbí víc.

Podobně podle situace volíme i zápis. V teoretických úvahách je lepší pracovat s vektory, u praktických úloh bývá často příjemnější používat zápis $x = ...$, $y = ...$

Teď už umíme řešit homogenní lineární diofantické rovnice. Když shrneme naše dosavadní výsledky, dostáváme následující.

! **Důsledek 6c.5.**
Uvažujme lineární diofantickou rovnici $ax+by=c$. Předpokládejme, že c je násobkem $\gcd(a,b)$. Nechť $A,B\in\mathbb{Z}$ splňují $\gcd(a,b)=Aa+Bb$. Pak množina všech řešení dané rovnice je

$$\Big\{\Big(A\frac{c}{\gcd(a,b)}+k\frac{b}{\gcd(a,b)},B\frac{c}{\gcd(a,b)}-k\frac{a}{\gcd(a,b)}\Big);\ k\in\mathbb{Z}\Big\}.$$

! **Příklad 6c.d** (pokračování 6c.c)**:** Řešili jsme rovnici $15x+6y=1251$ a zjistili jsme, že $\gcd(15,6)=3=1\cdot15+(-2)\cdot6$, což dělí pravou stranu $c=1251$. Podle Důsledku máme množinu řešení

$$\big\{\big(1\cdot417-k\tfrac{6}{3},(-2)\cdot417+k\tfrac{15}{3}\big);\ k\in\mathbb{Z}\big\}=\{(417-2k,5k-834);\ k\in\mathbb{Z}\}$$

neboli $x=417-2k$, $y=5k-834$ pro $k\in\mathbb{Z}$ (znaménko u k jsme umístili tak, aby u každé neznámé byl alespoň jeden kladný člen, protože nám to tak přišlo hezčí, ale klidně si to udělejte jinak).

Můžeme udělat zkoušku, jako obvykle dosazením do rovnice:

$$15\cdot(417-2k)+6\cdot(5k-834)=6255-30k+30k-5004=1251.$$

Vyšla.

Jestliže nás zajímají řešení z oboru $\mathbb{N}_0$, tak potřebujeme, aby $5k-834\geq0$ a $417-2k\geq0$ neboli $k\geq\frac{834}{5}$ a $k\leq\frac{417}{2}$. Taková k existují, jmenovitě jde o všechna $k\in\mathbb{N}$ splňující $167\leq k\leq208$. Mohli bychom si tedy vypsat všechna řešení $(x,y)\in\mathbb{N}_0^2$, ale je jich docela dost, tak se spokojíme s jedním. Zvolíme třeba $k=200$ a vidíme, že 1251 litrů získáme například tak, že do nádrže nalejeme 17 patnáctilitrových nádob a 166 šestilitrových.
△

S **Praktický výpočet.** Při praktickém výpočtu je možné postupovat více způsoby, jedna možnost je použít právě předvedený postup, kdy použijeme výsledný vzorec pro množinu všech řešení. Na tom není nic špatného, má ale jednu nevýhodu: Je zcela závislý na zapamatování vzorce, který je v látce poněkud izolovaný a tudíž se snadno zapomene. Mnoho lidí dává přednost postupu vícekrokovému, jehož hlavní struktura vychází z obecné teorie lineárních rovnic, je to tedy postup, který se zde ještě několikrát objeví a čtenář jej již může znát z lineární algebry. Jmenovitě, nejprve se najde partikulární řešení dané rovnice a pak se vyřeší homogenní rovnice. Tento postup vychází z pochopení fungování rovnic, takže pokud čtenář látku zná, v zásadě si už skoro nic navíc nemusí pamatovat. Oblíbeným trikem, který se může a nemusí použít, je také vykrácení rovnice co nejdříve, zejména pokud dokážeme $\gcd(a,b)$ hned uhodnout.

Možných přístupů je tedy několik, čtenář si vybere dle toho, v jakém bodě na škále mezi pamatováním a porozuměním se nejlépe cítí. My zde uvedeme (a budeme používat) algoritmus přemýšlecí a strukturovaný, který autorovi přijde nejlepší.

S **Algoritmus 6c.6.** pro nalezení všech celočíselných řešení rovnice $ax+by=c$.

Verze 1 bez hádání.

0. Pomocí například rozšířeného Euklidova algoritmu najděte $\gcd(a,b)=Aa+Bb$.

1. Jestliže c není násobkem $\gcd(a,b)$, pak řešení rovnice neexistuje.

2. Případ $\gcd(a,b)$ dělí c:

a) Získanou rovnici $aA+bB=\gcd(a,b)$ vynásobte číslem $c'=\dfrac{c}{\gcd(a,b)}\in\mathbb{Z}$ tak, aby se zachovaly koeficienty a,b, a dostanete $a(Ac')+b(Bc')=c$, tudíž i jedno partikulární řešení $x_p=Ac'$, $y_p=Bc'$ neboli vektor (Ac',Bc').

b) Přidruženou homogenní rovnici $ax+by=0$ zkraťte číslem $\gcd(a,b)$ na tvar $a'x+b'y=0$ neboli $a'x=-b'y$, což dává řešení $x_h=-b'k$, $y_h=a'k$ neboli dvojice $(-b'k,a'k)$ pro $k\in\mathbb{Z}$.

c) Sečtením partikulárního a obecného homogenního řešení získáte množinu všech celočíselných řešení

$$\{(Ac'-kb',Bc'+ka');\ k\in\mathbb{Z}\}\text{ neboli }x=Ac'-kb',\ y=Bc'+ka'\text{ pro }k\in\mathbb{Z}.$$

Verze 2 s hádáním.

1. Uhodněte $\gcd(a,b)$ a danou rovnici zkraťte tímto číslem. Pokud to nejde, tedy jestliže c není násobkem $\gcd(a,b)$, pak řešení rovnice neexistuje.

2. Případ $\gcd(a,b)$ dělí c:

Vydělte danou rovnici číslem $\gcd(a,b)$, dostanete novou diofantickou rovnici $a'x+b'y=c'$, kde teď a',b' jsou nesoudělné.

a) Pomocí například rozšířeného Euklidova algoritmu najděte $1=\gcd(a',b')=Aa'+Bb'$. Získanou rovnici $a'A+b'B=1$ vynásobte číslem c' tak, aby se zachovaly koeficienty, dostanete $a(Ac')+b(Bc')=c'$ a tudíž i jedno partikulární řešení $x_p=Ac'$, $y_p=Bc'$ neboli vektor (Ac',Bc').

b) Přidruženou homogenní rovnici $a'x+b'y=0$ si přepište jako $a'x=-b'y$, což napoví řešení $x_h=-b'k$, $y_h=a'k$ neboli dvojice $(-b'k,a'k)$ pro $k\in\mathbb{Z}$.

c) Sečtením partikulárního a obecného homogenního řešení získáte množinu všech celočíselných řešení

$$\{(Ac' - kb', Bc' + ka');\ k \in \mathbb{Z}\} \text{ neboli } x = Ac' - kb',\ y = Bc' + ka' \text{ pro } k \in \mathbb{Z}.$$

U obou verzí je možné dát mínus k y_h namísto k x_h.
△

Někteří studenti u homogenní rovnice $a'x + b'y = 0$ už žádné úpravy nedělají a prostě si pamatují, že prohozené koeficienty (s jedním mínusem) dávají řešení.

Pokud chceme získat řešení z $\mathbb{N}_0^2$ a máme $a', b' > 0$, pak k musí splňovat podmínky $-\frac{Ac'}{b'} \le k \le \frac{Bc'}{a'}$.

I tento algoritmus si ukážeme na úloze s nádobami.

! Příklad 6c.e (pokračování 6c.c)**:** Rovnici $15x + 6y = 1251$ vyřešíme strukturovaně. Číslo $\gcd(15, 6) = 3$ umíme uhádnout, třeba tak, že 6 má netriviální dělitele 2 a 3, jen jeden z nich dělí i 15. Rovnici tedy vydělíme číslem 3 a dostáváme rovnici $5x + 2y = 417$, dělení proběhlo bez problémů a tudíž je rovnice řešitelná v celočíselném oboru.

Snadno pomocí rozšířeného Euklidova algoritmu najdeme popřípadě uhodneme, že $\gcd(5, 2) = 1 = 1 \cdot 5 + (-2) \cdot 2$. Rovnici $1 = 5 \cdot 1 + 2 \cdot (-2)$ vynásobíme číslem 417 a dostaneme $5 \cdot 417 + 2 \cdot (-834) = 417$, máme tedy partikulární řešení $x_p = 417$, $y_p = -834$.

Přidružená homogenní rovnice $5x + 2y = 0$ neboli $5x = -2y$ má obecné řešení $x_h = -2k$, $y_h = 5k$ pro $k \in \mathbb{Z}$.

Sečtením dostáváme obecné celočíselné řešení $x = 417 - 2k$, $y = 5k - 834$ pro $k \in \mathbb{Z}$.

Již jsme odvodili, že pokud bychom chtěli řešení jen z $\mathbb{N}_0$, tak použijeme $167 \le k \le 208$. Je možné zkusit i další optimalizaci.

Představme si například, že pro nás není váhový rozdíl mezi 15 a 6 litry až tak velký, ale vadí nám běhání pro vodu. Ocenili bychom řešení, u kterého běháme nejméně, což znamená řešení s co nejmenším počtem použitých nádob. Matematicky to znamená, že chceme minimalizovat $x + y = (417 - 2k) + (5k - 834) = 3k - 417$, ale zajímají nás jen hodnoty k mezi 167 a 208. Řešením je evidentně volba co nejmenšího možného k, tedy $k = 167$. Nejméně se naběháme, pokud použijeme $x = 83$ patnáctilitrovek a jednu šestilitrovku.
△

Zdá se, že je to takto příjemnější než řešení předchozí, ale rozhodnutí, který algoritmus používat, je samozřejmě na čtenáři. Na závěr dva příklady, první příjemný a druhý standardní písemkový.

! Příklad 6c.f: Dostali jste stokorunu s tím, že za ni máte nakoupit lízátka a bonbóny na dětský den. Lízátko stojí šest korun a bonbón dvě koruny. Jaké se nabízí možnosti, jestliže si nechcete nechat nic od cesty ani nákup dotovat ze svého?

Máme hledat řešení rovnice $6l + 2b = 100$ z oboru $\mathbb{N}_0$. Protože hned vidíme, že $\gcd(6, 2) = 2$, vydělíme rovnici, ono to jde, budou tedy řešení.

Řešíme rovnici $3l + b = 50$. K nalezení partikulárního řešení potřebujeme najít vyjádření 1 pomocí 3 a 1, tedy $1 = 3A + B$. To snadno uhádneme, $3 \cdot 1 + 1 \cdot (-2) = 1$. Tuto rovnici vynásobíme padesáti, ať máme správnou pravou stranu. Dáme si přitom pozor, abychom na levé straně dali padesát na správná místa, potřebujeme zachovat koeficienty 3 a 1: $3 \cdot 50 + 1 \cdot (-100) = 50$, tedy vidíme řešení $l_p = 50$, $b_p = -100$.

Přidružená homogenní rovnice $3l + b = 0$ neboli $3l = -b$ má obecné řešení $l_h = -k$, $b_h = 3k$, dostáváme tak obecné celočíselné řešení pro danou úlohu jako $l = 50 - k$, $b = 3k - 100$ pro $k \in \mathbb{Z}$.

Která řešení splňují $l, b \ge 0$? Dostáváme rovnice $50 \ge k$ a $3k \ge 100$, což dává rozmezí $34 \le k \le 50$. Máme tedy řešení $(16, 2)$, $(15, 5)$, $(14, 8)$, $(13, 11)$, $(12, 14)$, $(11, 17)$, $(10, 20)$, $(9, 23)$, $(8, 26)$, $(7, 29)$, $(6, 32)$, $(5, 35)$, $(4, 38)$, $(3, 41)$, $(2, 44)$, $(1, 47)$, $(0, 50)$.

Na řešeních je možné dělat další analýzy, například pokud bychom chtěli, aby bylo lízátek a bonbónů stejně, řešili bychom rovnici $3k - 100 = 50 - k$ neboli $4k = 150$, což dává $k = 37.5$, takže hodnoty $k = 37$ a $k = 38$ dávají výsledky nejblíže rovnováze, dostáváme $l = 13$, $b = 11$, případně $l = 12$, $b = 14$. To druhé asi bude lepší, protože bude víc sladkostí.

Mohl bychom také chtít koupit co nejvíce věcí, takže bychom maximalizovali funkci $s(k) = x + y = 2k - 50$ na intervalu $\langle 34, 50 \rangle$. Funkce s rostoucím k roste, její největší hodnotu tedy dostaneme v co největším možném k. Nejvíce sladkostí dává volba $k = 50$, tedy žádná lízátka a 50 bonbónů.

Poznámka: Víme, že Bezoutův rozklad není jednoznačný, někdo třeba uhodne $1 = 3 \cdot (-1) + 1 \cdot 4$. Pak bychom dostali $3 \cdot (-50) + 1 \cdot 200 = 50$ a řešení $x = -50 - k$, $y = 200 + 3k$ pro $k \in \mathbb{Z}$. Zde by asi bylo lepší volit v homogenním řešení znaménka naopak, řešení je pak elegantnější, $x = k - 50$, $y = 200 - 3k$ pro $k \in \mathbb{Z}$. Jsou to sice jiné vzorečky, ale jako množinu všech řešení dostáváme totéž. Například vyrovnanou variantu 12 lízátek a 14 bonbónů jsme předtím dostali volbou $k = 38$, u nových vzorečků ji dostaneme volbou $k = 62$.

To se samořejmě dalo čekat, věta o struktuře řešení (viz 6c.3 a poznámka za ní) zaručuje, že při vytváření množiny všech řešení lze to partikulární volit libovolně.
△

! Příklad 6c.g: Vyřešíme rovnici $154x - 259y = 105$.

Asi by se $\gcd(154, -259)$ dal i uhádnout, ale zopakujeme si Euklidův aloritmus na číslech 259 a 154.

a, b	q	A	B
259		1	0
154	1	0	1
105	1	1	-1
49	2	-1	2
7•	7	3•	-5•
0			

Dostáváme $\gcd(154, -259) = \gcd(259, 154) = 7$, takže podělíme rovnici: $22x - 37y = 15$. Šlo to, rovnice je řešitelná.

Dostali jsme také vyjádření $7 = 3 \cdot 259 + (-5) \cdot 154$. Abychom měli na levé straně 105, vynásobíme tuto identitu patnácti, na pravé straně si chceme zachovat čísla 154 a 259: $105 = 45 \cdot 259 + (-75) \cdot 154$. Ještě si tuto rovnost přeorganizujeme, aby souhlasila znaménka a pořadí: $154 \cdot (-75) - 259 \cdot (-45) = 105$. Porovnáním s danou rovnicí vidíme řešení $x_p = -75$, $y_p = -45$.

Vykrácenou rovnici upravíme na homogenní: $22x - 37y = 0$. Dostáváme řešení $x_h = 37k$, $y_h = 22k$ pro $k \in \mathbb{Z}$.

Sečtením partikulárního a homogenních řešení dostáváme obecné řešení dané rovnice $x = 37k - 75$, $y = 22k - 45$ pro $k \in \mathbb{Z}$.

Kdyby to někdo chtěl množinově, tak množina všech řešení dané rovnice je

$$\{(37k - 75, 22k - 45);\ k \in \mathbb{Z}\}.$$

Zkouška: Dosadíme do dané rovnice: $154 \cdot (37k - 75) - 259 \cdot (22k - 45) = 5698k - 11550 - 5698k + 11655 = 105$.

Pokud bychom chtěli řešení z $\mathbb{N}_0$, dostali bychom jich nekonečně mnoho, $x = 37k - 75$, $y = 22k - 45$ pro $k \in \mathbb{Z}$, $k \geq 3$.

Poznámka: Pokud někdo postupu dobře rozumí, může se od něj někdy výhodně odchýlit. Podívejte se na třetí řádek v tabulce algoritmu. Říká se tam, že $105 = 1 \cdot 259 + (-1) \cdot 154$. Takže přímo v tabulce vidíme kombinaci koeficientů, která dává původní pravou stranu. Po úpravě $154 \cdot (-1) - 259 \cdot (-1) = 105$ a hned vidíme alternativní partikulární řešení $x_p = -1$, $y_p = -1$.
△

Cvičení

Cvičení 6c.1 (rutinní, zkouškové)**:** Najděte všechna řešení $(x, y) \in \mathbb{Z}^2$ a $(x, y) \in \mathbb{N}_0^2$ pro následující diofantické rovnice:

(i) $6x + 9y = 204$;
(ii) $10x - 15y = 131$;
(iii) $10x - 4y = 26$;
(iv) $105x - 75y = 0$;
(v) $819x + 315y = 126$;
(vi) $65x + 273y = 157$.

Cvičení 6c.2 (dobré)**:** Máte k dispozici klasické váhy s dvěma miskami a libovolný počet závaží o váze 15 nebo 55 gramů. Jakou nejmenší hmotnost jste schopni odvážit?

Cvičení 6c.3 (dobré)**:** Máte dvě tyče, jedna má délku 60 dm a druhá má délku 25 dm. Jaká je nejmenší délka látky, kterou pomocí nich dokážete odměřit, pokud si odměřujete podél okraje a děláte čárky?

Řešení:

6c.1: (i): $\gcd(6, 9) = 3$ uhodneme, řešíme $2x + 3y = 68$: $\gcd(3, 2) = 1 = 1 \cdot 3 + (-1) \cdot 2$, proto $\gcd(2, 3) = 1 = (-1) \cdot 2 + 1 \cdot 3$, po vynásobení $2 \cdot (-68) + 3 \cdot 68 = 68$. Řešení $(x, y) = (-68 + 3k, 68 - 2k)$ neboli $x = 3k - 68$, $y = 68 - 2k$ pro $k \in \mathbb{Z}$. Řešení v $\mathbb{N}_0$: $23 \leq k \leq 34$.
(ii): $\gcd(10, -15) = 5$ nedělí 131. Nemá řešení.
(iii): $\gcd(10, -4) = 2$ uhodneme, řešíme $5x - 2y = 13$: $\gcd(5, 2) = 1 = 1 \cdot 5 + (-2) \cdot 2$, proto $\gcd(5, -2) = 1 = 1 \cdot 5 + 2 \cdot (-2)$, po vynásobení $5 \cdot 13 - 2 \cdot 26 = 13$. Řešení $(x, y) = (13 - (-2)k, 26 + 5k)$ neboli $x = 2k + 13$, $y = 5k + 26$ pro $k \in \mathbb{Z}$. Řešení v $\mathbb{N}_0$: $k \geq -5$.
(iv): $\gcd(105, 75) = 15$, $7x - 5y = 0$ homogenní rovnice. Řešení $(x, y) = (5k, 7k)$ neboli $x = 5k$, $y = 7k$ pro $k \in \mathbb{Z}$. Řešení v $\mathbb{N}_0$: $k \geq 0$.
(v): $\gcd(819, 315) = 63$, $13x + 5y = 2$. $\gcd(819, 315) = 63 = 2 \cdot 819 + (-5) \cdot 315$, proto $819 \cdot 4 + 315 \cdot (-10) = 126$. Řešení $(x, y) = (4 - 5k, -10 + 13k)$ neboli $x = 4 - 5k$, $y = 13k - 10$ pro $k \in \mathbb{Z}$. Řešení v $\mathbb{N}_0$: nelze.
(vi): $\gcd(65, 273) = 13$ nedělí 157. Nemá řešení.

6c.2: Váhu c odměříme, pokud lze napsat $c = 15x + 55y$, kde $x, y \in \mathbb{Z}$ a záporné hodnoty znamenají, že takováto závaží dáváme na stejnou misku jako dotyčný předmět. Rovnice má řešení, pokud $\gcd(15, 55)$ dělí c, tedy nejmenší váha je 5 gramů.

6c.3: Délku c odměříme, pokud lze napsat $c = 60x + 25y$, kde $x, y \in \mathbb{Z}$ a záporné hodnoty znamenají, že nanášíme na opačnou stranu. Rovnice má řešení, pokud $\gcd(60, 25)$ dělí c, tedy nejmenší délka je 5 dm.