ZÁKLADY TEORIE ČÍSEL A JEJÍCH APLIKACÍ PRO NEMATEMATIKY

PAVEL JAHODA

Text byl vytvořen v rámci realizace projektu *Matematika pro inženýry 21. století* (reg. č. CZ.1.07/2.2.00/07.0332), na kterém se společně podílela Vysoká škola báňská – Technická univerzita Ostrava a Západočeská univerzita v Plzni

Pavel Jahoda
Základy teorie čísel a jejích aplikací pro nematematiky

© Pavel Jahoda, 2010
ISBN

Předmluva pro nematematiky i pro matematiky

Váženým matematikům důrazně doporučuji, aby dále nepokračovali ve čtení a využili ke studiu teorie čísel nějakou jinou, vážněji psanou publikaci. Pro začátek jich naleznou dost v seznamu literatury.

Už jsou pryč? Dobře. Jak jste již jistě pochopili, milí nematematici, následující stránky jsou určeny Vám. Tím chci říci, že se Vám v textu pokusím vše podrobně vysvětlit a ukázat na jednoduchých příkladech. Také jsem se, alespoň z počátku, než se po matematické stránce trochu zocelíte, snažil vyvarovat sdělení typu „důkaz je triviální a proto jej ponecháme čtenáři za cvičení," případně „ s využitím dobře známé věty XY si čtenář snadno odvodí, že platí WZ." Pokud jsem se snad někdy této zásady v návalu matematického tranzu nedržel, hluboce se omlouvám. Své cenné připomínky a kletby, prosím, posílejte na adresu pavel.jahoda@vsb.cz.

V případě, že během studia narazíte na nějaký nepochopitelný problém, nejedná se s největší pravděpodobností o projev Vaší duševní méněcennosti, ale o projev autorova zapomínání věcí, které při studiu teorie čísel mohou dělat i snaživému studentovi problémy. Další možností je také překlep přehlédnutý při korekturách, i v tomto případě Vás prosím o zaslání upozornění na pavel.jahoda@vsb.cz.

Ostrava 10. 8. 2010 Autor :)

Obsah

Co je dobré vědět před tím, než začnete číst první kapitolu

0.1 Učivo SŠ a VŠ

Samozřejmě budeme předpokládat, že čtenář je obeznámen s učivem matematiky střední školy. Zejména mu nesmí činit obtíže úpravy algebraických výrazů, grafy elementárních funkcí, elementární výroková logika (logické spojky a, nebo, jestliže-pak, právě tehdy když) a operace s množinami (průnik, sjednocení, rozdíl). Z vysokoškolské matematiky bude třeba připomenout si učivo týkající se posloupností, limit posloupností a řad.

Takže, pokud cítíte jisté obavy, že tento požadavek nesplňujete, sáhněte po své staré učebnici, nalistujte si danou kapitolu a vypočítejte všechny příklady. Pokud tak neučiníte, budete se při dalším čtení jen trápit. Přes snahu autora o vysvětlování krok za krokem Vám pak nezbyde, než mu věřit místo toho, aby jste si vlastním rozumem ověřili pravdivost uváděných tvrzení.

0.2 Matematické symboly

Hotovo? Tak můžeme pokračovat. V textu se budou vyskytovat obvykle užívané matematické symboly, například:

$\mathbb{N} = \{1, 2, 3, \dots\}$ označuje množinu *přirozených čísel*.

$\mathbb{Z} = \{\dots -3, -2, -1, 0, 1, 2, 3, \dots\}$ označuje množinu *celých čísel*.

$\mathbb{Z}^+ = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}$ označuje množinu *nezáporných celých čísel*.

$\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}\}$ označuje množinu *racionálních čísel*.

$\mathbb{R}$ označuje množinu *reálných čísel*.

Symbol $\forall$ znamená „pro každé.“

Symbol $\exists$ znamená „existuje.“

Symbol $\exists!$ znamená „existuje právě jedno.“

Pár příkladů pro ilustraci.

1. $\forall x \in A : x \geqq 4$ čteme „pro každé x z množiny A platí, že $x \geqq 4$.“ Matematik tím chtěl říci, že všechny prvky množiny A jsou větší, nebo rovny čtyřem.
2. $\forall x \in A\ \exists y \in A : x + y = 0$ čteme „pro každé x z množiny A existuje y z A takové, že $x + y = 0$.“ Matematik tím chtěl říci, že ať si vybereme jakýkoli prvek z množiny A (označíme jej x), pak jsme k němu schopni v množině A nalézt druhý prvek (označíme jej y) tak, že jejich součet bude roven 0.
3. $\exists! a \in A : \forall x \in A : x + a = x$ „existuje právě jedno $a \in A$ takové, že pro každé $x \in A$ platí $x + a = x$.“ A co je tím myšleno? Máme libovolně vybraný prvek x z množiny A a zajímá nás, jestli se v množině A najde prvek a takový, aby platilo $x + a = x$. Uvedený výrok tvrdí, že takové a najdeme, ale pouze jediné, tzn. pokud je $b \neq a, b \in A$, potom $x + b \neq x$.

Budeme samozřejmě používat i další obvykle zažité matematické symboly. Které, že to jsou? No tak pro jistotu:

$\in$ ... *náleží* (Např. $x \in A$ znamená, že prvek x náleží množině A.)

$\subseteq$ ... *podmnožina* (Např. $A \subseteq B$ znamená, že A je podmnožina množiny B, přičemž může nastat $A = B$.)

$\subset$ ... Tento symbol bývá některými autory používán se stejným významem jako předchozí, my však pomocí něho budeme značit tzv. *vlastní podmnožinu* (Např. $A \subset B$ znamená, že A je podmnožina množiny B, přičemž nemůže (!) nastat $A = B$.)

$\cap$ ... *průnik* (Průnik daných množin obsahuje jejich společné prvky, např. $\{1, 3, 5\} \cap \{2, 4, 5\} = \{5\}$.)

$\cup$ ... *sjednocení* (Sjednocení daných množin obsahuje všechny prvky těchto množin, např. $\{1, 3, 5\} \cap \{2, 4, 5\} = \{1, 2, 3, 4, 5\}$.)

$A - B$ ... *rozdíl množin A a B* (Množina $A - B$ obsahuje ty prvky z A, které nepatří do B např. $\{1, 3, 5\} - \{2, 4, 5\} = \{1, 3\}$ ale pozor, $\{2, 4, 5\} - \{1, 3, 5\} = = \{2, 4\}$.)

$\#A$ ... *počet prvků konečné množiny* A (Takto budeme značit počet prvků konečné množiny $A \subset \mathbb{N}$. Například pro $A = \{2, 4, 5\}$ platí $\#A = 3$.)

$\cap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$ ... Pokud uvažujeme průnik více množin, můžeme zápis zkrátit tímto způsobem (např. v případě $n = 3$ dostáváme $\cap_{i=1}^{3} A_i = A_1 \cap \cap A_2 \cap A_3$.)

$\cup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$ ... Pokud uvažujeme sjednocení více množin, můžeme zápis zkrátit tímto způsobem (např. v případě $n = 3$ dostáváme $\cup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3$.)

$\sum$ ... *suma*. Pomocí symbolu suma zkracujeme součet několika čísel (např. $\sum_{k=1}^{4} \frac{1}{k} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}$. Pozor! Pokud se v textu vyskytne např. zápis $\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{1}{1^2} + + \frac{1}{2^2} + \frac{1}{3^2} + \ldots$, je tím myšleno, že $\sum_{k=1}^{\infty} \frac{1}{k^2} = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{k^2}$.)

$\prod$ ... *součin*. Pomocí tohoto symbolu zkracujeme součin několika čísel (např. $\prod_{k=1}^{4} \frac{1}{k} = \frac{1}{1} \cdot \frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{4}$. Pozor! Pokud se v textu vyskytne např. zápis $\prod_{k=1}^{\infty} \frac{1}{k^2+1} = = \frac{1}{1^2+1} \cdot \frac{1}{2^2+1} \cdot \frac{1}{3^2+1} \cdot \ldots$, je tím myšleno, že $\prod_{k=1}^{\infty} \frac{1}{k^2+1} = \lim_{n\to\infty} \prod_{k=1}^{n} \frac{1}{k^2+1}$.)

$\wedge$ ... Je symbolem logické spojky *a zároveň*.

$\vee$ ... Je symbolem logické spojky *nebo*.

$\Rightarrow$ ... Je symbolem logické spojky *jestliže - pak*.

$\Leftrightarrow$ ... Je symbolem logické spojky *právě tehdy když*.

A' ... Označuje *negaci výroku* A.

$g(x) = O(x)$ ... Znamená, že

$$\limsup_{x\to\infty} \frac{|g(x)|}{x} = c = konst. < \infty,$$

(kde $x \in \mathbb{R}$, nebo $x \in \mathbb{N}$.) To znamená, že $\forall \varepsilon > 0\, \exists x_0 \in \mathbb{R}$ takové, že pro každé $x > x_0$ platí $\frac{|g(x)|}{x} < c + \varepsilon$.

$g(x) = o(x)$ ... Znamená, že

$$\lim_{x\to\infty} \frac{g(x)}{x} = 0,$$

(kde $x \in \mathbb{R}$, nebo $x \in \mathbb{N}$.) To znamená, že $\forall \varepsilon > 0\, \exists x_0 \in \mathbb{R}$ takové, že pro každé $x > x_0$ platí $|\frac{g(x)}{x}| < 0 + \varepsilon$.

Hodnoty $\frac{g(x)}{x}$ se při $x \to \infty$ blíží číslu 0.

$g(x) = O(h(x))$ ... Znamená, že

$$\limsup_{x\to\infty} \frac{|g(x)|}{h(x)} = c = konst. < \infty,$$

(kde $x \in \mathbb{R}$, nebo $x \in \mathbb{N}$.) To znamená, že $\forall \varepsilon > 0\, \exists x_0 \in \mathbb{R}$ takové, že pro každé $x > x_0$ platí $\frac{|g(x)|}{h(x)} < c + \varepsilon$.

Nepřesně řečeno, pro „dostatečně velká“ x můžeme tvrdit, že funkce $|g(x)|$ se chová podobně jako funkce $h(x)$.

$g(x) = o(h(x))$ ... Znamená, že

$$\limsup_{x\to\infty} \frac{g(x)}{h(x)} = 0,$$

(kde $x \in \mathbb{R}$, nebo $x \in \mathbb{N}$.) To znamená, že $\forall \varepsilon > 0\, \exists x_0 \in \mathbb{R}$ takové, že pro každé $x > x_0$ platí $|\frac{g(x)}{h(x)}| < 0 + \varepsilon$.

Hodnoty $\frac{g(x)}{h(x)}$ se při $x \to \infty$ blíží číslu 0.

0.2.1 Cvičení

1. Dokažte, že $-O(x) = O(x)$.

2. Dokažte, že $O(x) + O(x) = O(x)$.

3. Dokažte, že $O(g(x)) + O(g(x)) = O(g(x))$.

4. Dokažte, že pro každé $r \in \mathbb{R}$ platí $r.O(x) = O(x)$.

5. Dokažte, že pro $f(n) = \frac{1}{n+1}$ platí $f(n) = O\left(\frac{1}{n}\right)$.

6. Dokažte, že $\ln(x + 1) = O(\ln x)$.

7. Dokažte, že $1. \ln 1 - 1 = O(\ln x)$.

8. Dokažte, že $-1 + \frac{1}{x}O(\ln x) = O(1)$.

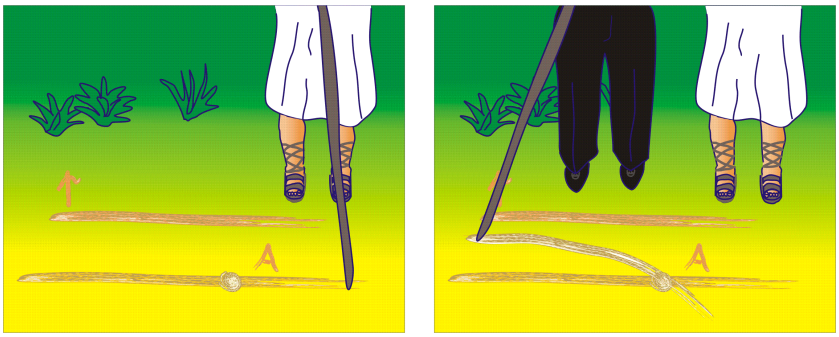
0.3 Základy matematiky, aneb axiomatická výstavba matematiky

Nebojte, jen letmo a převážně nevážně.[1] Pro počáteční vážněji pojaté studium této problematiky doporučuji skripta doc. Buriana [4].

Představte si, že jste zakladateli vědecké disciplíny *matematika*. Není tedy známo ještě vůbec nic. Jste však všemi mastmi mazaní vědátoři s ambiciózním plánem stvořit nejexaktnější a nejčistší vědu (v tom smyslu, že naprosto přesně formulujete pojmy, problémy i jejich řešení, které musí být provedeno na základě nezpochybnitelných důkazů) ze všech exaktních a čistých věd!

A první, co vás napadne, je načmárat klackem do písku čáru a vedle ní puntík. I zrodil se první problém vaší skvělé vědy! Řeknete si, no tak takovéhle čáře budu říkat *přímka* a takovému puntíku *bod*. A otázka zní, kolik přímek můžu vést bodem (puntíkem v písku) tak, aby neprotínala zadanou přímku (tu co jsem před chvílí načmáral do písku)?

Kolemjdoucí Eukleides vám hned začne šeptat do ucha: „Ale pane kolego, to je přece triviální, jen jednu. Takhle, rovnoběžně s tou zadanou!“



Obr. 1 Eukleides versus Lobačevskij

V tom klepe milému Euklidovi na rameno pan Lobačevskij a shovívavě říká: „Ehm, pane kolego, zdá se, že tak trochu neuváženě plácáte!“ Chytne klacek a do písku přičmárne ještě jednu čáru, která prochází daným bodem a zadanou přímku neprotíná (viz obrázek 1)! Eukleides se zamračí a pohoršeně zahučí: „Dělat si blázny z člověka, kterému je o pár set let víc než vám! Chováte se jako dětina, pane Lobačevskij! Vždyť ta vaše přímka je nějaká křivá, to není žádná přímka!“

„No no, nic ve zlém, ale nějak si nevzpomínám, že by se řeklo, co to vlastně přímka je! Tak proč by nemohla být trošičku křivá?“

A v tuto chvíli se všichni přítomní hluboce zastydí. Takové plány jsme měli, jak tu matematiku budeme poctivě a nanejvýš přesně budovat a formulovat a hned

[1] Události popisované v této kapitole jsou smyšlené a podobnost s historickými událostmi a osobami je čistě záměrná.

na začátku jsme toto předsevzetí porušili! Vždyť nemáme definici přímky, ani bodu! Taková ostuda! No nic, hned to napravíme. Takže, ehmmm, řekněme, že *přímka je to, co má jen délku a ne šířku, nemá to konec a ani začátek* a *bod je to, co nemá žádný rozměr*. Spokojen, pane Lobačevskij?

„Éee, no ani ne.“

„Cože?! Co zas?!“

„Já jen, že nemáme definici pojmů jako *rozměr, délka, šířka, konec, začátek, to, ...*, takže tyto definice přímky a bodu tak nějak nic neříkají. A kdybychom se pokusili definovat rozměr, délku, šířku, konec, začátek a to, byli bychom nuceni v definicích použít slova, které zase nemáme definované! Takže tudy asi cesta nevede.“

Frustrace, zmar a beznaděj. Tak to můžeme celé zabalit, přesné vymezení daného pojmu pomocí definice není z principu možné! Končíme, matematika nebude, prostě to nejde.

„Snad to přece jen nebude tak zlé,“ prohodí opět shovívavě, ale už i trochu namyšleně Lobačevskij. „Co kdybychom to provedli takhle. Vybereme si pár, ne mnoho, pojmů, říkejme jim *základní pojmy*, které prostě definovat nebudeme, například *množina, bod, přímka ...* a každý ať si pod nimi představí co chce ...“

„Hrůza, anarchie, fůůj!!!“

„Pánové, nepřerušovat prosím! Takže, každý si pod nimi může představit co chce, ale tyto intuitivní představy je žádoucí zhmotnit ve výrocích, nazveme je *axiomy*, které popisují vztahy mezi těmito základními pojmy. Tím vlastně svým způsobem charakterizujeme, co si pod základními pojmy představujeme.“

„Eee???“

„No tak vezměte si třeba náš úvodní problém. Chceme studovat vlastnosti bodů, přímek a jejich vzájemnou polohu v rovině. Zde přítomný vážený kolega Eukleides si pod pojmem bod představil jakýsi mikroskopický puntík a pod přímkou jakousi absolutně rovnou nekonečně tenoučkou nitku, která přichází z nekonečných hlubin vesmíru a zase do nich odsviští. Tuto představu můžeme popsat několika axiomy, například:

A_1: Pro každé dva různé body A, B existuje jediná přímka p tak, že $A, B \in p$. (Tj. Každými dvěma různými body A a B můžeme vést právě jednu přímku.)

A_2: Pro každou přímku existují dva různé body, které na ní leží.

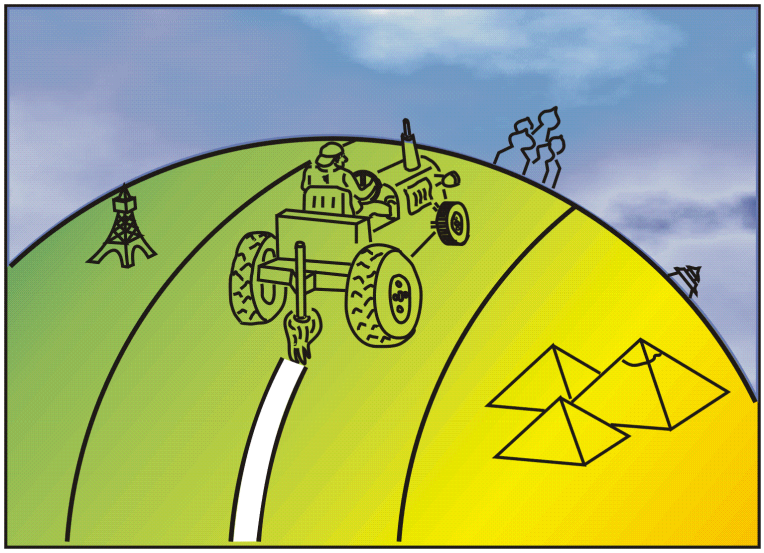
$\vdots$

A_n: Pro každé tři navzájem různé body A, B, C existuje jediná rovina ρ tak, že $A, B, C \in \rho$.

E: Pro každou přímku p a bod A, který na ní neleží, existuje jediná přímka r taková, že bod A leží na r a zároveň se přímky r a p neprotínají[1]. “

Tato představa přímek a bodů (zažilo se pro ni označení *eukleidovská geometrie* [2]) není nijak špatná, naopak, a proto je často využívaná ve fyzice (nerelativistické), v technice a jinde.

Ale nyní si představme svět přímek a bodů, jak jej vidí člověk, který maluje středové čáry na vozovku. Říkejme mu Jarda (viz obr. 2). Ten má každodenní představu trošku jinou, omezenější (bez urážky) – nezajímají jej vesmírné dálky (alespoň v pracovní době ne), přímka se musí pěkně držet země. Představí si ji jako rovnou čáru, kterou namaluje štětkou drženou kolmo k zemi od vidím do nevidím. Pokud přimhouříme oči, můžeme říci, že Země je kulatá, a tak Jardovy přímky nejsou nic jiného, než kružnice se středem ve středu Země a poloměrem rovným poloměru Země – říkejme jim *hlavní kružnice*. Tato představa není o nic horší, než ta Eukleidova. Pro Jardu je dokonce mnohem výhodnější. Popisuje totiž jeho problémy mnohem lépe, než Eukleidovská geometrie. Neříkáme jí však Jardova geometrie, ale je to jeden z modelů tzv. *eliptické geometrie*.



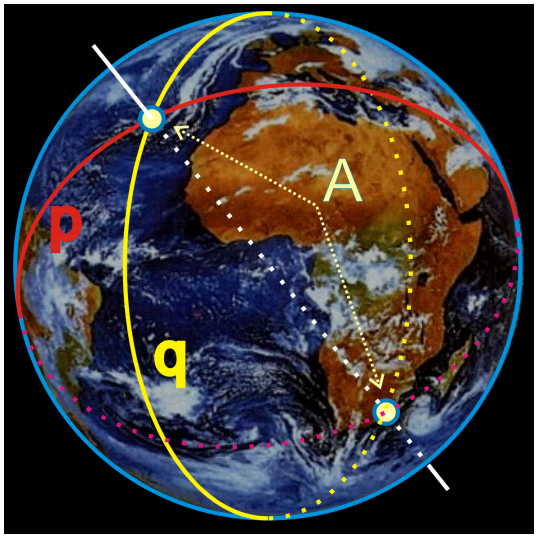
Obr. 2 Jarda v práci

Bodem v tomto modelu rozumíme dvojici bodů na povrchu koule, puntík namalovaný na zemi a puntík na opačné straně zeměkoule tvoří jediný bod. (To

[1] Říkáme, že přímky r a p se protínají právě když existuje bod A takový, že $A \in r$ a $A \in p$. Bod A pak nazveme průsečíkem přímek r a p.

[2] První korektní a ucelenou soustavu axiomů eukleidovské geometrie sestavil matematik David Hilbert ($\star$1862, †1943) ve své knize *Grundlagen der Geometrie*. Z ní jsme si také uvedené axiomy „vypůjčili.“ Hilbertova axiomatická soustava eukleidovské geometrie obsahuje 20 axiomů. Nedefinovanými pojmy jsou *bod*, *přímka* a *rovina*. Základními relacemi je *incidence* (leží na, $\in$), *uspořádání* (bod A leží mezi body B a C, $\mu(B, A, C)$) a *shodnost* (je shodný, $\cong$).

mimo jiné znamená, že dvě různé přímky modelu se protínají v jediném bodě modelu – dvojici „puntíků“ na opačných stranách zeměkoule. Viz obrázek 3.)



Obr. 3 V Jardově modelu eliptické geometrie tvoří puntík namalovaný na zemi a puntík na opačné straně Zeměkoule společně jediný bod A. Takže přímky p a q se protínají v jediném bodu.

A v čem se tyto dvě geometrie liší? Pokud bychom tady měli seznam všech axiomů Eukleidovy geometrie (dejme tomu, že soustavu axiomů Eukleidovské geometrie tvoří axiomy $A_1, A_2, \ldots, A_n$ a E, my jsme uvedli pouze A_1, A_2, A_n a E), mohli bychom ověřit, že všechny, až na jediný, platí i v Jardově modelu eliptické geometrie. Jedinou výjimkou je axiom E. Jak to?

Představte si to třeba na glóbu – modelu zeměkoule. Zadanou přímkou p nechť je třeba Greenwichský (nultý) poledník (vzpomeňte si, Jardovou představou přímky je čára namalovaná kolem Země, takže jde o kružnici na jejím povrchu a se středem v jejím středu) a zadaný bod A je dvojice bodů na povrchu Země, z nichž jeden leží v Ostravě (ten druhý je na opačné straně zeměkoule). Dokážete najít nějakou hlavní kružnici zeměkoule, která prochází touto dvojicí bodů a přitom neprotíná nultý poledník?

Hledáte ...? Nu hledejte, ale ne moc dlouho, je to zbytečné, žádná taková není. V eliptické geometrii platí axiomy $A_1, A_2, \ldots, A_n$ a axiom E^*: „Pro každé dvě různé přímky p a q existuje bod A tak, že $A \in p$ a $A \in q$ (říkáme, že přímky p a q se protínají v bodě A).“

Obdobně můžeme vytvořit takzvanou *hyperbolickou geometrii*. Ta je určena axiomy $A_1, A_2, \ldots, A_n$ a axiomem H: „Pro každou přímku p a bod A, který na ní neleží, existuje více než jedna přímka p^* taková, že bod A na ní leží a navíc p^* neprotíná přímku p (tj. p a p^* nemají žádný společný bod).“

Shrňme si tedy, jak je matematika jako věda budována. V matematice pracujeme s některými pojmy jako je bod, přímka, množina a podobně. Přesné vymezení těchto pojmů neexistuje, nejsou definovány. Můžeme si pod nimi představit v podstatě cokoli a proto se jim říká *základní*, nebo také *primitivní pojmy*. V začátcích matematiky jako vědy existovaly snahy vytvořit jejich definice, nicméně v nich se nutně vyskytují další pojmy, které by bylo třeba definovat a v těchto definicích by figurovaly další pojmy, a tak bychom museli pokračovat do nekonečna, což evidentně nemá smysl.

Ač o samotných nedefinovaných pojmech neříkáme nic (a vlastně právě díky tomu) můžeme si dovolit určovat požadavky na vztahy (*relace*) mezi nimi.

Vlastnosti těchto vztahů určujeme v takzvaných *axiomech* teorie. Příkladem může být teorie euklidovské roviny. Nedefinovanými pojmy jsou zde přímka a bod. Přímka a bod mohou být ve vzájemném vztahu (relaci) „leží na“. Vlastnosti této relace jsou popsány v *soustavě axiomů* (což je množina všech axiomů dané teorie). Například jeden z axiomů říká, že pro každé dva body A, B roviny existuje jediná přímka p roviny taková, že bod A leží na p a zároveň bod B leží na p. Pomocí dané matematické logiky potom na základě axiomů formulujeme matematické věty (např. z axiomů A_1 a A_2 plyne, že platí ...).

Na základě základních pojmů můžeme pomocí *definic* tvořit další pojmy (např. kolmice na přímku p v bodě A je přímka q, pro kterou platí ...).

Na soustavu axiomů matematické teorie klademe ovšem také jisté požadavky. Zřejmě by nemělo smysl, aby jeden axiom říkal : „je to bílé“ a druhý : „je to černé.“ Proto je naprosto přirozený požadavek, aby z dané soustavy axiomů nebylo možné odvodit dvě kontradiktorická tvrzení (tzn. tvrzení, která nemohou platit současně). Této vlastnosti soustavy axiomů se říká *vnitřní bezespornost*.

Pokud by z nějaké ($n-1$) – tice axiomů $A_1, \ldots, A_{n-1}$ plynulo tvrzení zbývajícího n-tého axiomu A_n (v tom případě říkáme, že axiom A_n je *logicky závislý* na $A_1, \ldots, A_{n-1}$), pak by jeho přítomnost v soustavě axiomů byla evidentně zbytečná. Proto od soustavy axiomů požadujeme *vzájemnou logickou nezávislost* jednotlivých axiomů. (Závislost soustavy axiomů je však možno tolerovat, pokud se tak děje z didaktických důvodů.) Matematickou teorií potom nazveme množinu všech vět, které byly na základě dané soustavy axiomů a základních pojmů odvozeny.

0.4 Matematické věty a jejich důkazy

Pojem *matematická věta* není definován. Obvykle pod ním chápeme pravdivý výrok, který se týká matematiky (lépe řečeno, matematických problémů, neboť výrok „Danou hodinu matematiky navštívilo 25 žáků.” asi nebudeme za každou cenu prosazovat jako matematickou větu, přestože se týká matematiky a může být dost dobře pravdivá).

Na matematické věty je kladen požadavek, aby šlo o pravdivé výroky. To

ovšem nebývá vždy na první pohled zřejmé. Jejich pravdivost je tedy třeba dokázat! (plně v souladu s požadavky formulovanými na počátku předchozího odstavce). Tím máme na mysli, že je třeba čtenáři podat podrobné vysvětlení, proč považujeme tuto větu (výrok) za pravdivou. Takže:

Čtenář má plné právo nevěřit ničemu, pokud mu nebyl předložen důkaz.

Mnoho matematických vět má tvar: „Pokud je pravdivý výrok A, potom je pravdivý výrok B." Například:

$$\text{Jestliže } \underbrace{x \in \mathbb{R}}_{A}, \text{ pak } \underbrace{x^2 \geqq 0}_{B}.$$

Formálně tak můžeme tuto matematickou větu zapsat jako výrok ve tvaru „$A \Rightarrow B$." Jak dokázat pravdivost takovéhoto a podobných tvrzení? Existuje více možností. Mezi nejčastější patří *přímý důkaz*, *nepřímý důkaz*, *důkaz sporem*, *důkaz slabou matematickou indukcí* a *důkaz silnou matematickou indukcí*. Je dobré se předem seznámit s postupem u jednotlivých metod dokazování, aby si později čtenář zbytečně nelámal hlavu s tím, proč a jak v důkazu postupujeme právě tak či onak.

Důkaz slabou matematickou indukcí Představme si, že máme dokázat výrok

$$\forall n \in \mathbb{N} \underbrace{\text{ platí rovnost } \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}}_{V(n)},$$

tj. obecně výrok ve tvaru

$$\forall n \in \mathbb{N} : V(n).$$

Jen tak mezi námi, uvedený výrok je skutečně pravdivý. Jak to však ověřit? Mohli bychom dosadit za n nejprve číslo 1 a zjistili bychom, že výrok $V(1)$ je pravdivý, neboť pro $n = 1$ dostáváme

$$\underbrace{\text{platí rovnost } \frac{1}{1.2} = \frac{1}{1+1}}_{V(1)}.$$

Pro $n = 2$ dostáváme

$$\underbrace{\text{platí rovnost } \frac{1}{1.2} + \frac{1}{2.3} = \frac{2}{2+1}}_{V(2)}.$$

Vážený čtenář si jistě sám ověří, že i $V(2)$ je pravdivý výrok. To je sice prima, ale co dál? Až do konce života bychom tak mohli pokračovat, ale nestihli bychom ověřit pravdivost nekonečně mnoha zbývajících výroků $V(3)$, $V(4)$, ...

Vidíte, je třeba se na chvíli zastavit a vymyslet fintu, jak tento zádrhel překonat. Snad nám pomůže klasická intuitivní reakce většiny lidí. Ti si, v případě že ověří platnost výroků $V(1)$, $V(2)$, $V(3)$, $V(4)$, ..., $V(n)$, často pomyslí: „Je to jasné, pravdivý bude i následující výrok $V(n+1)$." V matematice však nestačí věřit, je třeba dokazovat! Co když zrovna $V(14438)$ není pravda?! Proto dokážeme, že když je pravdivý výrok $V(n)$, pak musí být pravdivý i (následující) výrok $V(n+1)$. Je jasné proč? Pokud ne, nezoufejte, uvidíme za chvíli. Shrňme si nejprve postup při dokazování matematickou indukcí.

- Nejprve dokážeme platnost výroku $V(1)$ (případně $V(m)$ pokud dokazujeme $\forall n \in \{m, m+1, m+2, \dots\}$).
- Poté dokážeme pro libovolné pevně zvolené n platnost výroku:

$$V(n) \text{ je pravda} \quad \Rightarrow V(n+1) \text{ je pravda.}$$

- Pokud jsme uspěli v předcházejících dvou krocích, můžeme si gratulovat, neboť jsme tím dokázali pravdivost výroku

$$\forall n \in \mathbb{N} : V(n).$$

Pořád ještě tápete, proč by z prvních dvou bodů mělo plynout, že $V(n)$ je pravda, ať za n dosadíme jakékoli přirozené číslo? Pokud ne, blahopřeji a můžete tento odstaveček přeskočit. Pokud ano, tak podívejte. V prvním bodu jsme dokázali pravdivost $V(1)$. A v druhém kroku jsme dokázali, že potom musí být pravda i $V(2)$. Pak, opět podle druhého bodu, musí být pravda $V(3)$ (neboť už víme, že $V(2)$ je pravda). Odtud analogicky odvodíme, že $V(4)$ je pravdivý výrok (neboť teď už víme, že $V(3)$ je pravda). A tak dále a tak dále. Jedná se o jakousi „řetězovou reakci," která proběhne postupně všemi přirozenými čísly n. Výsledkem je, že jsme dokázali pravdivost $V(n)$, ať je n jakékoli přirozené číslo.

Zkusme provést důkaz motivačního příkladu. To jest, dokážeme pravdivost věty

$$\forall n \in \mathbb{N} \text{ platí rovnost } \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

- Již dříve jsme dokázali platnost výroku $V(1)$, neboť platí

$$\underbrace{\frac{1}{1.(1+1)} = \frac{1}{1+1}}_{V(1)}.$$

- Nyní přistoupíme k takzvanému *indukčnímu kroku*. Spočívá v tom, že pro libovolné pevně zvolené n předpokládáme platnost výroku $V(n)$ - označujeme jej jako *indukční předpoklad* - a dokážeme, že potom platí i $V(n+1)$ (jde o stejný výrok jako $V(n)$, jen tam, kde bylo n, napíšeme $n+1$).

  Indukčním předpokladem tedy je, že platí vztah

$$\underbrace{\frac{1}{1.2}+\frac{1}{2.3}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}}_{V(n)}. \tag{1}$$

  Snažíme se dokázat, že v tom případě platí také vztah

$$\underbrace{\frac{1}{1.2}+\frac{1}{2.3}+\cdots+\frac{1}{(n+1)((n+1)+1)}=\frac{n+1}{(n+1)+1}}_{V(n+1)}. \tag{2}$$

  To nebude nijak těžké. Levou stranu rovnice (2) můžeme rozepsat do tvaru

$$\underbrace{\frac{1}{1.2}+\frac{1}{2.3}+\cdots+\frac{1}{n(n+1)}}_{\text{Podle (1) je tato část rovna } \frac{n}{n+1}}+\underbrace{\frac{1}{(n+1)((n+1)+1)}}_{\frac{1}{(n+1)(n+2)}}.$$

  Odtud

$$\frac{n}{n+1}+\frac{1}{(n+1)(n+2)}=$$

$$=\frac{n(n+2)}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)}=\frac{n(n+2)+1}{(n+1)(n+2)}=$$

$$=\frac{n^2+2n+1}{(n+1)(n+2)}=\frac{(n+1)^2}{(n+1)(n+2)}=$$

$$=\frac{n+1}{(n+2)}=\frac{n+1}{(n+1)+1}.$$

  Dospěli jsme k pravé straně vztahu (2), čímž jsme ověřili jeho pravdivost.

- Tím jsme dokázali pravdivost výroku

$$\forall n\in\mathbb{N} \text{ platí rovnost } \frac{1}{1.2}+\frac{1}{2.3}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}.$$

Důkaz silnou matematickou indukcí Princip silné matematické indukce je logicky ekvivalentní s principem slabé matematické indukce. Opět dokazujeme tvrzení ve tvaru

$$\forall n \in \mathbb{N} : V(n).$$

Postup při silné matematické indukci je následující.

- Nejprve dokážeme platnost výroku $V(1)$[1].
- Poté dokážeme pro libovolné pevně zvolené $n > 1$ platnost výroku:

  $$V(k) \text{ je pravda pro každé } k \in \{1, 2, \ldots, n-1\}^2 \Rightarrow V(n) \text{ je pravda.}$$

  To jest, předpokládáme, že $V(k)$ platí pro všechna přirozená k menší, než n a snažíme se dokázat, že výrok $V(n)$ je potom také pravdivý.
- Jestliže jsme uspěli v předcházejících dvou krocích, pak jsme tím dokázali pravdivost výroku

  $$\forall n \in \mathbb{N} : V(n).$$

Přímý důkaz Tato metoda dokazování je poměrně jednoduchá. Víme-li, že výrok $A \Rightarrow B$ a také výrok $B \Rightarrow C$ je pravdivý, potom musí být pravdivý i výrok $A \Rightarrow C$.[3] A právě tohoto faktu využívá metoda přímého důkazu. Máme-li dokázat pravdivost výroku $A \Rightarrow B$, snažíme se najít výroky A_1, A_2, …, A_n tak, abychom dostali posloupnost implikací

$$A \Rightarrow A_1 \Rightarrow A_2 \cdots \Rightarrow A_n \Rightarrow B.$$

Máme tím na mysli, že dokážeme platnost výroků $A \Rightarrow A_1$, $A_1 \Rightarrow A_2$, …, $A_n \Rightarrow B$.

Ukažme si to na příkladě. Máme dokázat větu: „Jestliže k nám domů přijede babička na návštěvu a tatínek je doma, pak tatínek musí vyhledat lékařské ošetření.“ Víme při tom, že následující výroky V_1, V_2 a V_3, jsou pravdivé:

[1] Případně $V(m)$ pokud dokazujeme $\forall n \in \{m, m+1, m+2, \ldots\} : V(n)$

[2] Případně $k \in \{m, \ldots, n-1\}$ pokud dokazujeme $\forall n \in \{m, m+1, m+2, \ldots\} : V(n)$

[3] Důkaz je možné provést následovně. Ukážeme pomocí pravdivostní tabulky, že výrok $V = [(A \Rightarrow B) \wedge (B \Rightarrow C)] \Rightarrow (A \Rightarrow C)$ je vždy pravdivý.

A	B	C	$A \Rightarrow B$	$B \Rightarrow C$	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$A \Rightarrow C$	V
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
0	1	0	1	0	0	1	1
0	0	1	0	1	0	1	1
0	0	0	0	1	0	1	1

V_1 = „Jestliže k nám přijede babička na návštěvu, vždy s sebou přiveze svého psa Bobíka."

V_2 = „Jestliže je u nás doma Bobík a zároveň tatínek, pak tatínek dostane alergický záchvat."

V_3 = „Jestliže tatínek dostane alergický záchvat, pak tatínek musí vyhledat lékařské ošetření."

Předpokladem věty je

$$A = \underbrace{\text{k nám domů přijede babička na návštěvu}}_{A^*} \text{ a } \underbrace{\text{tatínek je doma}}_{A^{**}}.$$

Máme dokázat, že v případě pravdivosti A musí nastat

$$B = \text{tatínek musí vyhledat lékařské ošetření.}$$

To jest, ověřujeme platnost výroku $(A^* \wedge A^{**}) \Rightarrow B$. Označme A_1 = „Tatínek dostane alergický záchvat." Z předpokladu A^* a z V_1 plyne, že u nás doma je Bobík. Předpoklad A^{**} říká, že je doma také tatínek. Podle V_2 pak tatínek dostane alergický záchvat. A tak jsme odvodili platnost výroku

$$A \Rightarrow A_1.$$

Dále víme, že V_3 je pravdivý výrok a snadno si rozmyslíme, že $V_3 = (A_1 \Rightarrow B)$. Dospěli jsme tak k posloupnosti implikací

$$A \Rightarrow A_1 \Rightarrow B.$$

Tím je důkaz pravdivosti výroku $A \Rightarrow B$ dokončen.

Nepřímý důkaz Než začneme objasňovat postup při nepřímém dokazování, zkuste si uvědomit, že následující dva výroky říkají totéž.

- (věta) Jestliže den X je čtvrtek, pak popeláři v den X do 16:00 odvezou odpad z našich popelnic.
- (věta obměněná) Jestliže v den X popeláři do 16:00 neodvezou odpad z našich popelnic, pak den X není čtvrtek.

Metoda nepřímého důkazu využívá skutečnosti, že věta a její obměněná věta jsou logicky ekvivalentní. Je tím myšleno, že výrok (věta) ve tvaru $A \Rightarrow B$ je pravdivý právě tehdy, když je pravdivý výrok $B' \Rightarrow A'$ (věta obměněná). Ještě jinak, výrok $(A \Rightarrow B) \Leftrightarrow (B' \Rightarrow A')$ je vždy pravdivý. [1]

[1] Důkaz tohoto faktu můžeme opět provést pomocí pravdivostní tabulky.

A	B	B'	A'	$A \Rightarrow B$	$B' \Rightarrow A'$	$(A \Rightarrow B) \Leftrightarrow (B' \Rightarrow A')$
1	1	0	0	1	1	1
1	0	1	0	0	0	1
0	1	0	1	1	1	1
0	0	1	1	1	1	1

Můžeme proto konstatovat, že výrok $A \Rightarrow B$ říká totéž, jako výrok $B' \Rightarrow A'$. A tak, pokud dokážeme pravdivost $B' \Rightarrow A'$, musí být pravdivá i věta $A \Rightarrow B$.

Při nepřímém dokazování dané věty ve tvaru $A \Rightarrow B$ vytvoříme větu obměněnou ($B' \Rightarrow A'$) a tu dokazujeme. Ukažme si to na triviálním příkladu. Dokážeme větu:

$$\text{Jestliže } \underbrace{n^2 + 2n + 1 \text{ je sudé}}_{A}, \text{ potom } \underbrace{n \text{ je liché číslo}}_{B}.$$

Mohli bychom použít metodu přímého důkazu, ale nepřímý důkaz v tomto případě představuje pohodlnější cestu k výsledku. Vytvoříme proto větu obměněnou:

$$\text{Jestliže } \underbrace{n \text{ je sudé číslo}}_{B'}, \text{ potom } \underbrace{n^2 + 2n + 1 \text{ je liché}}_{A'}.$$

a dokážeme ji metodou přímého důkazu.

Jestliže n je sudé, pak $n = 2k$, kde $k \in \mathbb{N}$. Proto

$$n^2 + 2n + 1 = (2k)^2 + 2.2k + 1 = 2(2k^2 + 2k) + 1 = 2K + 1,$$

kde $K = 2k^2 + 2k \in \mathbb{Z}$. Z toho plyne, že $n^2 + 2n + 1$ je liché číslo.

Důkaz sporem Chceme-li dokázat platnost dané věty, stačí ověřit, že nemůže nastat její negace. Proto k dané větě (výroku) V vytvoříme negaci V' a snažíme se z ní odvodit nějaký výrok S, který je nepravdivý (říkáme, že jsme dospěli ke sporu). Zapsána pomocí logických spojek, metoda důkazu sporem vypadá následovně.

- Dokážeme, že výrok $V' \Rightarrow S$ je pravdivý.
- Ukážeme, že výrok S je nepravdivý.

A co z toho? Podívejme se na níže uvedenou tabulku.

V	V'	S	$V' \Rightarrow S$
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	0

Z ní plyne, že tato situace může nastat pouze v případě, kdy výrok V je pravdivý[1]. Tím jsme dokázali pravdivost věty V.

[1] viz druhý řádek tabulky. Pouze zde je $V' \Rightarrow S$ pravda a S nepravda. Avšak v tomto případě je V pravda - viz první sloupec druhý řádek.

Pro ilustraci dokážeme sporem větu:

$$\underbrace{\text{Nechť } n \in \mathbb{N}, n \geqq 2. \text{ Pak číslo } n! - 1 \text{ není dělitelné číslem } m \in \{2, \ldots, n\}.}_{V}$$

Negací této věty je:

$$\underbrace{\text{Nechť } n \in \mathbb{N}, n \geqq 2. \text{ Pak existuje } m \in \{2, \ldots, n\} \text{ tak, že } m \text{ je dělitelem čísla } n! - 1.}_{V'}$$

Pokud by V' byla pravda, znamenalo by to, že existuje $k \in \mathbb{Z}$ tak, že

$$n! - 1 = k.m,$$

kde m $\in \{2, \ldots, n\}$. Protože $n! = 2. \cdots .n$, dostáváme

$$(2. \cdots .m. \cdots .n) - 1 = k.m,$$

$$(2. \cdots .m. \cdots .n) - k.m = 1.$$

Vytkneme-li m, dostaneme vztah

$$m(k_0 - k) = 1,$$

kde $k_0 = \frac{n!}{m} \in \mathbb{N}$. To by ale znamenalo, že

$$\underbrace{\text{číslo 1 je násobkem čísla } m, \text{ které patří do množiny } \{2, \ldots, n\}.}_{S}$$

S je zjevně nepravdivý výrok! Navíc, k výroku S jsme dospěli zcela korektně na základě předpokladu, že V' je pravdivý výrok. Proto můžeme tvrdit, že $V' \Rightarrow S$ je pravdivý výrok. Podle výše uvedeného to znamená, že výrok V (dokazovaná věta) je pravdivý.

Kapitola 1

Dělitelnost na množině celých čísel

1.1 Definice a základní vlastnosti

S pojmem dělitelnosti jste se jistě setkali již na střední škole[1]. Vzpomenete si? Dělí trojka šestku? A dělí trojka pětku? Jistě jste na první otázku odpověděli kladně a na druhou záporně. Ale jak jste na to vlastně přišli? Zřejmě jste zkusili nejdříve podělit šestku trojkou a pak pětku trojkou. V prvém případě je výsledkem přirozené číslo ($6 : 3 = 2$, tj. dělení beze zbytku), ale v druhém případě výsledkem není přirozené číslo ($5 : 3 = 1,666\ldots$). To vás dovedlo ke správným odpovědím. Mohli bychom však tyto úvahy přeformulovat.

Trojka dělí šestku, protože šestka je násobkem trojky. Trojka nedělí pětku, protože pětka není násobek trojky. To je intuitivní návod, jak definovat dělitelnost na množině celých čísel $\mathbb{Z}$. Obecně můžeme říci, že celé číslo a dělí celé číslo b právě tehdy, když b je násobkem a. A co to znamená, že b je násobkem a? Symbolicky tuto skutečnost zapisujeme „$\exists k \in \mathbb{Z}$ takové, že $b = k \cdot a$“ (například pro $b = 6$ a $a = 3$ je $k = 2$ tj. $6 = 2 \cdot 3$).

Nyní už snad nebude problém s pochopením následující definice.

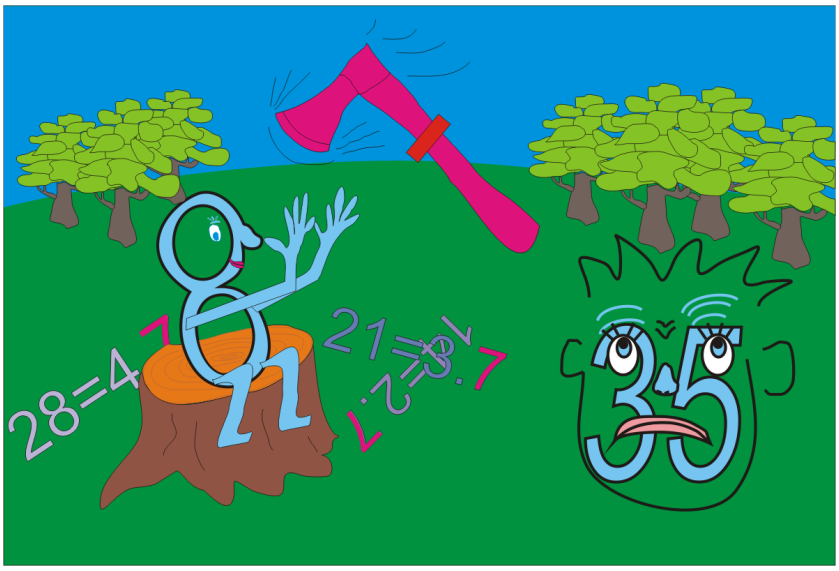
Definice 1.1. (*a dělí b*) Nechť $a, b \in \mathbb{Z}$. Říkáme, že a dělí b (nebo také a je dělitel b, nebo b je násobek a), právě tehdy, když existuje $k \in \mathbb{Z}$ tak, že

$$b = ka.$$

Skutečnost, že a dělí b symbolicky zapíšeme $a \mid b$.

Příklad 1.2. Procvičme si pojem dělitelnosti na konkrétních příkladech.

[1] Dělitelnost budeme studovat na množině celých čísel $\mathbb{Z}$. To pro naše potřeby bude stačit. Šlo by to ovšem obecněji, třeba na libovolném oboru integrity $(Z, +, .)$. Viz [6], kapitola VIII.



Obr. 1.1 Dělitelnost sedmičkou.Číslo 8 není dělitelné číslem 7, číslo 35 ano.

- Nalezněte všechny dělitele čísla 12.

  Řešení : Dělitelé čísla 12 jsou čísla 1, -1, 2, -2, 4, -4, 6, -6, 12 a -12.

- Nalezněte všechny dělitele čísla 0.

  Řešení : Celé číslo a je dělitelem čísla 0 právě když existuje celé číslo k takové, že $0 = k \cdot a$. Všimněte si, že v případě, kdy zvolíme za k nulu, obdržíme $0 = 0 \cdot a$ a tato rovnost platí pro libovolné $a \in \mathbb{Z}$! Děliteli čísla 0 jsou proto všechna celá čísla.

  Pozor! Vidíme, že nula je dělitelná i sama sebou, neboť je dělitelná libovolným celým číslem. Ale jen ve smyslu Definice 1.1! Neznamená to, že by byl definován zlomek $\frac{0}{0}$!!!

- Nalezněte všechna čísla, která jsou dělitelná číslem 0.

  Řešení : Celé číslo a je dělitelné nulou, právě když $a = k \cdot 0$. To ovšem znamená, že $a = 0$. Zjistili jsme tak, že nulou je dělitelné pouze číslo nula.

Definici máme za sebou a teď nějaké základní vlastnosti dělitelnosti v $\mathbb{Z}$. Zkuste si nejprve sami rozmyslet odpovědi na následující otázky.

Dělí dané celé číslo sebe sama? Když víme, že a dělí b a také b dělí c, můžeme tvrdit, že a dělí c? Platí, že když a dělí b, pak také b dělí a? Když a dělí b,

znamená to, že a dělí také násobky b (tj. čísla ve tvaru nb)? Když číslo a dělí m a také a dělí n, musí a dělit $m+n$? ...

Odpovědi na tyto a některé další otázky nyní zapíšeme symbolicky a dokážeme jejich pravdivost.

Lemma 1.3. *Platí:*

1) Pro každé $a \in \mathbb{Z}$ platí, že $a \mid a$.

2) Pro každé $a, b, c \in \mathbb{Z}$ platí, že když $a \mid b$ a zároveň $b \mid c$, pak také $a \mid c$.

3) Neplatí, že když $a \in \mathbb{Z}$ dělí $b \in \mathbb{Z}$, pak také b dělí a. Jinak řečeno, existují $a, b \in \mathbb{Z}$ takové, že $a \mid b$ a zároveň b nedělí a.

4) Pro každé $a, b \in \mathbb{Z}$ platí, že $|a| = |b| \Leftrightarrow (a \mid b \ \wedge \ b \mid a)$.

5) Pro každé $a, b, c \in \mathbb{Z}$ platí: $ab \mid c \Rightarrow (a \mid c \ \wedge \ b \mid c)$.

6) Nechť $a, m, n \in \mathbb{Z}$, potom platí: $(a \mid m \ \wedge \ a \mid n) \Rightarrow a \mid (m+n)$.

7) Pro každé $a, b, n \in \mathbb{Z}$ platí: $a \mid b \Rightarrow a \mid nb$.

8) Pro každé $a, b \in \mathbb{Z} - \{0\}$ platí: $a \mid b \Rightarrow |a| \leqq |b|$.

Důkaz. ad1) Pro každé $a \in \mathbb{Z}$ platí, že $a = 1 \cdot a$. Protože $1 \in \mathbb{Z}$, můžeme podle Definice 1.1 psát $a \mid a$.

ad2) Pro každé $a, b, c \in \mathbb{Z}$ platí, že když $a \mid b$ a zároveň $b \mid c$, pak existují $k_1, k_2 \in \mathbb{Z}$ takové, že $b = k_1 a$ a zároveň $c = k_2 b$. Z těchto dvou rovností (první dosadíme do druhé) dostáváme $c = k_2 k_1 a$. Součin dvou celých čísel je opět celé číslo, a tak $c = k_2 k_1 a = ka$, kde $k = k_2 k_1 \in \mathbb{Z}$. Podle Definice 1.1 to znamená, že $a \mid c$.

ad3) [1] Dokazujeme, že neplatí, že když $a \in \mathbb{Z}$ dělí $b \in \mathbb{Z}$, pak také b dělí a. Jinak řečeno, existují $a, b \in \mathbb{Z}$ takové, že $a \mid b$ a zároveň b nedělí a. Vezměme například $a = 5$ a $b = 10$. Vidíme, že $a \mid b$, ale b nedělí a.

[1] Pro zvídavější čtenáře nastíníme, jak toto tvrzení dokázat v případě, že studujeme dělitelnost na nějakém obecném oboru integrity $(Z, +, \cdot)$. Tj. dokazujeme, že existují $a, b \in Z$ takové, že $a \mid b$ a zároveň b nedělí a.

Dělitelnost v Z definujeme analogicky jako v $\mathbb{Z}$, a tak $a \mid b$ znamená, že existuje $k \in Z$ takové, že $b = ka$. Naopak, b nedělí a znamená, že neexistuje žádné $k \in Z$ takové, aby $b = k \cdot a$. Najdeme v Z takové a a b?

V každém oboru integrity existuje nulový a jednotkový prvek (a jsou navzájem různé). Označme je 0_Z a 1_Z. Navíc, když nulový prvek vynásobíme libovolným prvkem ze Z, výsledkem je opět nulový prvek. Takže $0_Z \cdot 1_Z = 0_Z$. To znamená, že $1_Z \mid 0_Z$.

Kdyby mělo platit $0_Z \mid 1_Z$, muselo by existovat $k \in Z$ takové, že $1_Z = k \cdot 0_Z$. Jak ale víme, $k \cdot 0_Z = 0_Z$, a to by vedlo ke tvrzení $1_Z = 0_Z$. To je spor s tím, že $1_Z \neq 0_Z$. Z toho plyne, že žádné takové $k \in Z$ neexistuje, a tak 0_Z nedělí 1_Z.

Našli jsme tak $a = 1_Z \in Z$ a $b = 0_Z \in Z$ splňující $a \mid b$, ale b nedělí a.

ad4) Pokud $a, b \in \mathbb{Z}$ a $|a| = |b|$, potom $a = \pm b$. Potom $(a \mid b \ \wedge \ b \mid a)$, neboť $b = \pm 1 \cdot a$ a $a = \pm 1 \cdot b$.

Nyní dokážeme obrácenou implikaci. Předpokládáme, že $(a \mid b \ \wedge \ b \mid a)$. Podle Definice 1.1 v takovém případě existují $k_1, k_2 \in \mathbb{Z}$ takové, že $b = k_1 a$ a $a = k_2 b$. Pokud do první rovnosti dosadíme za a výraz $k_2 b$ (druhá rovnost), pak dostáváme vztah

$$b = k_1 k_2 b$$

- Za předpokladu, že $b \neq 0$ odtud dostáváme $1 = k_1 k_2$. Víme, že $k_1, k_2 \in \mathbb{Z}$. Položme si otázku, čemu musí být rovno k_1 a čemu k_2? Součin kterých dvou přirozených čísel je roven 1? Jsou pouze dvě možnosti, a to $k_1 = k_2 = 1$, nebo $k_1 = k_2 = -1$. Z první z výše uvedených možností pak plyne, že $b = k_1 a = 1 \cdot a = a$ a $a = k_2 b = 1 \cdot b = b$. Tj. $a = b$. Z druhé z výše uvedených možností pak plyne, že $b = k_1 a = -1 \cdot a = -a$ a $a = k_2 b = -1 \cdot b = -b$. Tj. $a = -b$. V obou případech pak platí $|a| = |b|$.
- Za předpokladu, že $b = 0$ dostáváme přímo z předpokladu $(a \mid b \wedge b \mid a)$ tvrzení $0 \mid a$. To jest, $a = k \cdot 0 = 0$. Odtud $|a| = |b| = 0$.

ad5) Nechť $a, b, c \in \mathbb{Z}$. Jestliže $ab \mid c$, potom (podle Def. 1.1) musí existovat $k \in \mathbb{Z}$ takové, že $c = kab$. Označme $k_1^* = ka$ a $k_2^* = kb$ a dosaďme do předcházející rovnosti. Obdržíme vztahy

$$c = k_1^* b \qquad \text{a} \qquad c = k_2^* a.$$

To znamená, že c je násobek čísla a a zároveň je násobek čísla b. A tak, podle Definice 1.1, můžeme říci, že $a \mid c \ \wedge \ b \mid c$.

ad6) Jestliže $a \mid m$ a také $a \mid n$, pak m je násobek a a také n je násobek a. To jest, existují $k_1, k_2 \in \mathbb{Z}$, takové, že $m = k_1 a$, $n = k_2 a$. Potom

$$m + n = k_1 a + k_2 a = (k_1 + k_2) a = ka, \tag{1.1}$$

kde $k = k_1 + k_2 \in \mathbb{Z}$. Z rovnosti 1.1 můžeme usoudit, že číslo $m + n$ je násobek čísla a, a tak $a \mid m + n$.

ad7) Pro každé $a, b, n \in \mathbb{Z}$ platí: $a \mid b \Rightarrow b = ka$, kde $k \in \mathbb{Z} \Rightarrow nb = nka = k^* a$, kde $k^* = nk \in \mathbb{Z} \Rightarrow a \mid nb$.

ad8) Pro každé $a, b \in \mathbb{Z} - \{0\}$ platí: $a \mid b \Rightarrow b = ka$, kde $k \in \mathbb{Z} - \{0\}$. To znamená, že $|b| = |k||a|$. A protože $k \in \mathbb{Z} - \{0\}$, musí platit $|k| \geqq 1$. A tak

$$|b| = |k||a| \geqq 1 \cdot |a| = |a|.$$

□

Příklad 1.4. Pokud vám snad není zcela jasný význam symbolických zápisů v Lemmatu 1.3, prostudujte si níže uvedené příklady a poznámky.

ad1) Bod 1) tvrdí, že každé přirozené číslo dělí samo sebe, např. $5 \mid 5$, $10 \mid 10$, ...

ad2) Rozmyslete si konkrétní případ, kdy $a = 3$, $b = 12$ a $c = 24$. Vidíme, že $3 \mid 12$ a zároveň $12 \mid 24$. Bod 2) říká, že v tom případě také musí platit, že $3 \mid 24$ (a jak si snadno ověříte, opravdu je tomu tak!). Obdobně, $5 \mid 10$ a zároveň $10 \mid 100\,000$. Z toho můžeme usuzovat na to, že $5 \mid 100\,000$.

Této vlastnosti se říká *tranzitivnost*, tj. můžeme říci, že relace *a dělí b*, je tranzitivní.

ad3) V důkazu jsme uvedli příklad $a = 5$ a $b = 10$. Vidíme, že $a \mid b$, ale b nedělí a. Určitě dokážete sami nalézt i další příklady (např. $a = 3$ a $b = 12$, nebo $a = 4$ a $b = 16$, ...).

ad5) Pro každé $a, b, c \in \mathbb{Z}$ platí: $ab \mid c \Rightarrow (a \mid c \ \wedge \ b \mid c)$. Zkusme tvrzení ověřit alespoň na jednom příkladu. (Pozor! Ověření na jednom příkladu není důkaz, neboť zbývá nekonečně mnoho případů, které neověříme! Jde jen o lepší pochopení tvrzení, pokud si ještě nejste stoprocentně jisti jeho významem.) Tak tedy slibovaný příklad. Vezměme $a = 5$, $b = 7$, $c = 5.7.2 = = 70$. Evidentně je číslo 70 násobkem čísla $5.7 = 35$, a tedy $5.7 \mid 70$. Tvrzení bodu 5) říká, že potom musí platit $5 \mid 70$ a také $7 \mid 70$. Je to tak? (Jasně že je!)

ad6) Nechť $a, m, n \in \mathbb{Z}$, potom platí: $(a \mid m \wedge a \mid n) \Rightarrow a \mid (m+n)$. K čemu tohle využít? Vezměme $a = 6$, víme, že $6 \mid 36$, a také $6 \mid 66$. Potom si můžeme být jisti, že číslo 6 dělí číslo $102 = 36 + 66$. Triviální? No jistě, ale mohli bychom uvažovat i součet mnohem větších čísel, a dělit toto velikánské číslo číslem 6 (abychom ověřili, že tento součet je opět dělitelný číslem 6) by se nám třeba nemuselo chtít. A my teď už víme, že by to stejně byla jen ztráta času - víme už, jak by to dopadlo.

ad7) Víme, že číslo a dělí číslo b, bod sedmý Lemmatu 1.3 tvrdí, že potom číslo a dělí také násobky čísla b, tj. čísla ve tvaru nb. Například, víme, že číslo 7 dělí číslo 21. Můžeme si proto být jisti tím, že číslo 7 dělí také násobky čísla 21, tj. čísla ve tvaru $n21$ (např. 21, 42, 63, 84, ...).

ad8) Každý kladný dělitel a kladného čísla b je menší, nebo roven číslu b. Tj. když $a \mid b$, pak $a \leqq b$.

1.2 Největší společný dělitel

Uvažujme čísla $a = 24$ a $b = 36$. Kterými celými čísly jsou obě dělitelná? Čísla a a b nejsou příliš velká, takže nebude problém ověřit u všech čísel, která jsou v absolutní hodnotě menší, nebo rovny 24 (jiné číslo nemůže být dělitelem čísla $a = 24$), zda dělí jak $a = 24$, tak $b = 36$. Tímto způsobem dojdeme k tomu, že hledanými čísly jsou:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12.$$

Nu a když z těchto čísel vybereme to největší, tedy 12, nalezli jsme největšího společného dělitele čísel $a = 24$ a $b = 36$. Skutečnost, že $d = 12$ je největším společným dělitelem čísel $a = 24$ a $b = 36$ se obvykle zapisuje $\gcd(24, 36) = 12$.

Obecně, $\gcd(a, b)$ značí největší společný dělitel čísel a a b (z anglického *greatest common divisor*). V literatuře je též možno setkat se s označením (a, b) místo $\gcd(a, b)$.

No a to by k největšímu společnému děliteli stačilo a zbytek odstavce věnujeme fotbalu .... Ne! Samozřejmě, že by to nestačilo! Jestlipak přijdete na to, proč tato informace pro nás není dostatečná? Přemýšlíte?! Přemýšlejte!

Tak co, máme? Pokud ano, gratuluji, pokud ne, nevadí. Tak podívejte. Vynořují se pochybnosti. Existuje vůbec pro každou dvojici celých čísel největší společný dělitel? Když ano, je jediný, nebo jich může býti více různých? Navíc, zkuste výše uvedeným postupem najít největšího společného dělitele čísel $a = 14\,892$ a $b = 36\,138$. Že se vám do toho nechce? Ani se nedivím. Kontrolovat 14 892 čísel, zda dělí $a = 14\,892$ i $b = 36\,138$, není příliš efektivní postup, že? Chceme proto také najít nějaký lepší způsob určování $\gcd(a, b)$.

A protože hodláme řešit problém korektně, je třeba začít definicemi.

Definice 1.5. (*Společný dělitel*) Společným dělitelem (nebo zkráceně jen dělitelem) čísel $a_1, \ldots, a_n \in \mathbb{Z}$ nazveme každé $d \in \mathbb{Z}$ splňující

$$d \mid a_1, \ldots, d \mid a_n.$$

Vidíme, že čísla $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$ z úvodního příkladu jsou společnými děliteli čísel $a = 24$ a $b = 36$. Jak tušíme (už podle názvu), největším společným dělitelem má být číslo 12. Všimněte si, že všichni ostatní dělitelé $(\pm 1, \pm 2, \pm 3, \pm 4, \pm 6)$ dělí také číslo 12. Proč tomu tak je, na tomto místě řešit nebudeme, ale není to náhoda. Inspirováni těmito intuitivními představami definujeme největšího společného dělitele následovně.

Definice 1.6. (*Největší společný dělitel*) Největším společným dělitelem čísel $a_1, \ldots, a_n \in \mathbb{Z}$ nazveme každé $d \in \mathbb{Z}$ splňující podmínky:

1) $d \geqq 0$

2) Číslo d je společným dělitelem čísel $a_1, \ldots, a_n$, tj. $d \mid a_1, \ldots, d \mid a_n$.

3) Jestliže d^* je dělitelem čísel $a_1, \ldots, a_n$, potom $d^* \mid d$.

Fakt, že d je největším společným dělitelem čísel $a_1, \ldots, a_n$, budeme značit $d = \gcd(a_1, \ldots, a_n)$.

Největším společným dělitelem čísel $a_1, \ldots, a_n$ je tedy ten z nezáporných společných dělitelů, kterého všichni ostatní dělí.

Definice 1.7. Říkáme, že celá čísla a a b jsou nesoudělná právě když $\gcd(a, b) = 1$. V opačném případě, kdy $\gcd(a, b) \neq 1$ říkáme, že jsou soudělná.

Poznámka 1.8.

- Podmínky první a třetí v Definici 1.6 zajišťují, že číslo $\gcd(a_1, \ldots, a_n)$ je opravdu největší mezi všemi společnými děliteli čísel a_1, $\ldots$, a_n. Toto neplatí pouze v případě, kdy $a_1 = \cdots = a_n = 0$ - podrobněji viz Příklad 1.9.

- Všimněte si, že z Definice 1.6 je okamžitě patrná rovnost $\gcd(a, b) = \gcd(b, a)$. Jinak řečeno, nezáleží na pořadí, v jakém uvádíme čísla a a b.

Příklad 1.9. Vyřešíme pár příkladů, abychom plně porozuměli definici největšího společného dělitele.

1. Ověřte podle definice, že $\gcd(8, 12) = 4$.

Řešení : Dokážeme, že $\gcd(8, 12) = 4$.

(a) $4 \geqq 0$

(b) $4 \mid 8$ a také $4 \mid 12$

(c) Společnými děliteli čísel 8 a 12 jsou čísla ± 1, ± 2, ± 4. Všechna tato čísla jsou děliteli čísla 4.

Proto číslo 4 splňuje všechny podmínky z Definice 1.6 na to, aby bylo největším společným dělitelem čísel 8 a 12.

2. Určete $\gcd(4, 0)$ a dokažte, že čísla 4 a 0 mají právě jednoho největšího společného dělitele.

Řešení : Podle Definice 1.6 musí být $\gcd(4,0)$ nezáporné číslo a musí být společným dělitelem čísel 4 a 0. Nezáporní dělitelé čísla 4 jsou čísla

$$1, 2, 4.$$

Nezápornými děliteli čísla 0 jsou čísla (viz Příklad 1.2)

$$0, 1, 2, 3, 4, \ldots$$

Nezápornými společnými děliteli čísel 4 a 0 jsou proto čísla z množiny

$$D = \{1, 2, 4\}.$$

Největším společným dělitelem čísel 4 a 0 je ten prvek z množiny D, který je dělitelný všemi prvky z D (potom bude samozřejmě dělitelný i čísly k nim opačnými). Tuto podmínku splňuje pouze číslo 4, protože je dělitelné číslem 1, 2 i 4. Jednička není dělitelná dvojkou a čtyřkou a dvojka zase není dělitelná čtyřkou. Proto $\gcd(4,0) = 4$ a žádné jiné číslo nemůže být největším společným dělitelem čísel 4 a 0.

3. Dokažte, že $\gcd(a,0) = a$ pro každé $a > 0$ a ukažte, že čísla a a 0 nemají žádného jiného největšího společného dělitele.

Řešení : Řešení tohoto příkladu je zobecněním předchozího řešení. Množina všech nezáporných společných dělitelů čísel a a 0 je rovna množině D všech nezáporných dělitelů čísla $a > 0$. Do D jistě patří i samotné číslo a a to je dělitelné všemi prvky z D (svými děliteli). Splňuje tak i třetí podmínku z definice největšího společného dělitele. Proto je $a = \gcd(a,0)$. Všechna ostatní čísla z D jsou v absolutní hodnotě menší než $|a|$ a jsou různá od nuly, a tak nejsou dělitelná číslem $a \in D$. Proto nemohou být největším společným dělitelem čísel a a 0 (nesplňovaly by třetí podmínku z definice největšího společného dělitele).

4. Dokažte, že $\gcd(0,0) = 0$ a ukažte, že čísla 0 a 0 nemají žádného jiného největšího společného dělitele.

Řešení : Množina všech nezáporných dělitelů čísla 0 je množina

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

Množina všech nezáporných společných dělitelů čísel 0 a 0 je proto opět množina

$$D = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}.$$

Pouze nula je dělitelná všemi čísly z množiny D. Libovolné jiné číslo z množiny D, označme jej n, není dělitelné větším číslem než je samo, například číslem $n + 1$. Ale $n + 1$ jistě také patří do D. Proto $n \neq 0$ nemůže být $\gcd(0,0)$. Pouze nula vyhovuje všem podmínkám z definice největšího společného dělitele čísel 0 a 0, žádné jiné číslo je nesplňuje.

Jsme připraveni rozptýlit jednu z výše uvedených pochybností. Dvě celá čísla nemohou mít několik různých největších společných dělitelů.

Věta 1.10. *Nechť $a, b \in \mathbb{Z}$. Jestliže existuje jejich největší společný dělitel* $\gcd(a, b)$*, pak je jediný.*

Důkaz. Příklad 1.9 ukazuje, že Věta 1.10 je splněna v případě, kdy jedno, nebo obě z čísel a a b jsou rovny nule. Uvažujme proto $a, b \neq 0$.

Předpokládejme, že $d_1 = \gcd(a, b)$ a také $d_2 = \gcd(a, b)$. Protože $a, b \neq 0$, musí být $d_1, d_2 \geqq 1$. Číslo d_1 je podle předpokladu největším společným dělitelem čísel a a b. Podle Definice 1.6 jej proto musí dělit všichni ostatní dělitelé čísel a a b, tedy i číslo d_2. Dostáváme $d_2 \mid d_1$. Z Lemmatu 1.3 bodu 8.) pak plyne

$$d_2 \leqq d_1 \tag{1.2}$$

Analogickou úvahu můžeme provést i pro d_2. Číslo d_2 je podle předpokladu největším společným dělitelem čísel a a b. Podle Definice 1.6 jej proto musí dělit všichni ostatní dělitelé čísel a a b, tedy i číslo d_1. Dostáváme $d_1 \mid d_2$. Z Lemmatu 1.3 bodu 8.) pak plyne

$$d_1 \leqq d_2 \tag{1.3}$$

Spojením nerovnic (1.2) a (1.3) obdržíme nerovnosti $d_2 \leqq d_1 \leqq d_2$. To ovšem znamená, že $d_1 = d_2$.

□

Definice 1.11. (*Celá část*) Celou částí reálného čísla r nazveme celé číslo z splňující:

$$z \leqq r < z + 1.$$

Celou část reálného čísla r budeme značit $[r]$.

Pár příkladů pro ilustraci: $[3, 14] = 3$; $[2, 6] = 2$; $[7] = 7$. Pozor u záporných čísel! Podle definice $[-6, 51] = -7$; $[-3, 01] = -4$; ... protože $-7 \leqq -6, 51 < -6$; $-4 \leqq -3, 01 < -3$ ....

Ze základní a střední školy si jistě vzpomenete na dělení se zbytkem. Například $26 : 4$. Typická správná odpověď, jakou chce slyšet paní učitelka, je „$26 : 4 = 6$, zbytek 2.“ V podstatě tím není myšleno nic jiného, než že $26 = 6 \cdot 4 + 2$. Zvídavějšího žáčka by možná napadlo, jestli to je jediné řešení. Paní učitelka by jej jistě, a zcela správně, ujistila, že ano. My se ujistíme podáním důkazu.

Věta 1.12. *Pro každé $a, b \in \mathbb{N}$, $b \geqq a$ existuje právě jedno $q \in \mathbb{N}$ a právě jedno $r \in \mathbb{N}$, $0 \leqq r < a$ takové, že*

$$b = qa + r.$$

Důkaz. Nejprve dokážeme, že pro každé $a, b \in \mathbb{N}$, $b \geqq a$ existují $q \in \mathbb{N}$ a $r \in \mathbb{N}$, $0 \leqq r < a$ takové, že

$$b = qa + r.$$

Ukážeme, že hledané q je rovno celé části reálného čísla $\frac{b}{a}$, tj. $q = [\frac{b}{a}]$. Podle Definice 1.11 musí celé číslo $q = [\frac{b}{a}]$ splňovat:

$$q \leqq \frac{b}{a} < q + 1,$$

$$qa \leqq b < qa + a,$$

$$0 \leqq b - qa < a. \tag{1.4}$$

Označíme-li $r = b - qa$, potom evidentně $b = qa + r$, $r \in \mathbb{Z}$ a podle vztahu (1.4) platí $0 \leqq r < a$. Tím jsme dokázali, že hledaná čísla q a r existují. Nyní ukážeme, že to jsou jediná čísla q a r s požadovanými vlastnostmi.

Předpokládejme, že $b = qa + r$, kde $0 \leqq r < a$ a také $b = q_1 a + r_1$, kde $0 \leqq r_1 < a$ (a snažíme se nyní dokázat, že nemohou existovat dvě různá řešení, to jest, že musí platit $q = q_1$ a $r = r_1$). Potom

$$qa + r = q_1 a + r_1,$$

$$qa - q_1 a = r_1 - r,$$

$$a(q - q_1) = r_1 - r. \tag{1.5}$$

Pokud by $r_1 \neq r$, můžeme bez újmy na obecnosti předpokládat, že třeba $r_1 > r$. Potom $r_1 - r = k \in \mathbb{N}$. A protože $a > r_1$, musí platit $a > r_1 - r = k$. Ze vztahu (1.5) plyne, že

$$a(q - q_1) = k.$$

Předpoklad $q - q_1 = 0$ vede ke sporu, neboť pak by bylo $k = r_1 - r = 0$, ale my předpokládáme, že $k \in \mathbb{N}$, a tudíž $k \neq 0$. Další možností je $q - q_1 \neq 0$. To by ale znamenalo, že číslo a dělí číslo k. A to je znovu spor! Nemůže nastat $a \mid k$, neboť $a > k$ (viz Lema1.3). Tak či onak jsme dospěli ke sporu, a tak nemůže nastat $r_1 \neq r$.

Pokud $r_1 = r$, plyne z (1.5), že

$$a(q - q_1) = 0,$$

$$q - q_1 = 0,$$

$$q = q_1.$$

□

Nyní jsme již vybaveni k tomu, abychom dokázali odvodit poměrně efektivní způsob hledání největšího společného dělitele dvou čísel, který je znám jako *Euklidův algoritmus* . Ukažme si jej nejprve na příkladě.

Příklad 1.13. Vrátíme se k úvodnímu problému. Dejme tomu, že máme nalézt největšího společného dělitele čísel $a = 14\,892$ a $b = 36\,138$. Prvním krokem je podělit větší číslo tím menším a určit zbytek. Takže:

$$b = q_1 a + r_1,$$

$$36\,138 = 2 \cdot 14\,892 + 6354.$$

Nyní provedeme totéž s čísly $a = 14\,892$ a $r_1 = 6\,351$:

$$a = q_2 r_1 + r_2,$$

$$14892 = 2 \cdot 6\,354 + 2\,184.$$

Další krok provedeme s čísly $r_1 = 6\,351$ a $r_2 = 2\,184$:

$$r_1 = q_3 r_2 + r_3,$$

$$6354 = 2 \cdot 2\,184 + 1\,986.$$

A jak dlouho takto budeme pokračovat? Dokud nedojdeme k poslednímu nenulovému zbytku. Takže:

$$r_2 = q_4 r_3 + r_4,$$

$$2\,184 = 1 \cdot 1\,986 + 198.$$

$$r_3 = q_5 r_4 + r_5,$$

$$1986 = 10 \cdot 198 + \mathbf{6}.$$

$$r_4 = q_6 r_5 + r_6,$$

$$198 = 33 \cdot \mathbf{6} + 0.$$

Posledním nenulovým zbytkem bylo číslo $r_5 = 6$. Potom si můžeme být jisti, že $\gcd(14\,892, 36\,138) = 6$. A proč si můžeme být jisti? To si ukážeme v důkazu následující věty, která obecně popisuje Euklidův algoritmus.

Korektnost postupu Euklidova algoritmu dokážeme. Budeme k tomu potřebovat následující lemma.

Lemma 1.14. *Neexistuje nekonečná klesající posloupnost přirozených čísel.*

Důkaz. Důkaz provedeme sporem. Předpokládejme, že $\{k_n\}_{n=1}^{\infty}$ je nekonečná klesající posloupnost přirozených čísel. To jest

$$k_1 > k_2 > k_3 > \cdots > k_n > \dots$$

Uvažme, že každý následující člen této posloupnosti je alespoň o jedničku menší, než jeho předchůdce. Proto $k_2 \leqq k_1 - 1$, $k_3 \leqq k_1 - 2 \dots$. Obecně $k_i \leqq k_1 - (i-1)$. Dosazením za $i = k_1 + 1$ obdržíme $k_{k_1+1} \leqq 0$. To je spor, neboť předpokládáme, že číslo $k_{k_1+1} \in \mathbb{N}$. □

Věta 1.15. (Euklidův algoritmus) *Nechť $a, b \in \mathbb{N}$, $b \geqq a$. Jestliže $a = b$, potom* $\gcd(a,b) = a$. *Jestliže $b > a$, potom existuje $n \in \mathbb{N} \cup \{0\}$ tak, že existují čísla $r_{-1} = b$, $r_0 = a$, $q_j \in \mathbb{N}$, $r_j \in \mathbb{N} \cup \{0\}$ pro $j = 1, \dots, n+1$ takové, že pro každé $i = -1, \dots, n-1$ platí*

$$r_i = q_{i+2} r_{i+1} + r_{i+2},\ 0 \leqq r_{i+2} < r_{i+1},$$

$$a = r_0 > \cdots > r_{n+1} = 0.$$

Největším společným dělitelem čísel a a b je pak číslo r_n (poslední nenulový zbytek, případně $r_n = r_0 = a$), tj. $\gcd(a,b) = r_n$.

Důkaz. Existence čísel $q_j \in \mathbb{N}$, $r_j \in \mathbb{N} \cup \{0\}$, $j = 1, \dots, n+1$ takových, že pro každé $i = -1, 0, \dots, n-1$ platí

$$r_i = q_{i+2} r_{i+1} + r_{i+2},\ 0 \leqq r_{i+2} < r_{i+1}$$

okamžitě plyne z Věty 1.12. Že nakonec dojdeme k nějakému nulovému zbytku ($r_{n+1} = 0$) plyne z toho, že nemůže existovat (nekonečná!) klesající posloupnost přirozených čísel (zbytků) $r_i > 0$. (viz Lemma 1.14.)

Zatím jsme tak ukázali, že výše uvedeným postupem - Euklidovým algoritmem - vždy nakonec dojdeme k nějakému poslednímu nenulovému zbytku r_n (případně $r_n = r_0 = a$, další zbytek r_{n+1} už bude roven nule). Zbývá dokázat, že $\gcd(a,b) = r_n$. Ukážeme, že číslo r_n splňuje podmínky kladené na největšího společného dělitele čísel a a b (viz Definice 1.6). To jest, že platí podmínky:

1) $r_n \geqq 0$.

1) Číslo r_n je společným dělitelem čísel a, b, tj. $r_n \mid a, r_n \mid b$.

2) Jestliže d^* je dělitelem čísel a, b, potom $d^* \mid r_n$.

První podmínka je jistě splněna. Plyne to okamžitě z nerovnosti $0 \leqq r_{i+2} < r_{i+1}$ při $i = n-2$.

A co druhá podmínka? Víme, že pro $i = -1, 0, \ldots, n-1$ platí

$$r_i = q_{i+2} r_{i+1} + r_{i+2}. \tag{1.6}$$

Takže pro $i = n-1$ obdržíme rovnici

$$r_{n-1} = q_{n+1} r_n + r_{n+1} = q_{n+1}.r_n, \tag{1.7}$$

neboť $r_{n+1} = 0$. Z rovnosti (1.7) plyne, že $r_n \mid r_{n-1}$. Dále (pokud $n > 0$), podle (1.6) platí:

$$r_{n-2} = q_n r_{n-1} + r_n = q_n q_{n+1} r_n + r_n = (q_n q_{n+1} + 1) r_n. \tag{1.8}$$

Z rovností (1.7) a (1.8) plyne, že $r_n \mid r_{n-1}$ a $r_n \mid r_{n-2}$. Dále (pokud $n > 1$), podle (1.6) platí:

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} = q_{n-1}(q_n q_{n+1} + 1) r_n + q_{n+1} r_n = (q_{n-1}(q_n q_{n+1} + 1) + q_{n+1}) r_n. \tag{1.9}$$

Z rovností (1.7), (1.8) a (1.9) plyne, že $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$ a $r_n \mid r_{n-3}$. Analogicky bychom mohli pokračovat dále. Došli bychom tak k poznatku, že

$$r_n \mid r_n,\ r_n \mid r_{n-1},\ \ldots,\ r_n \mid r_0,\ r_n \mid r_{-1}.$$

Vzhledem k tomu, že jsme označili $r_0 = a$ a $b = r_{-1}$, je dokázána platnost druhé podmínky $r_n \mid a, r_n \mid b$.

Nakonec ukážeme, že je splněna i třetí podmínka. Předpokládejme, že d^* je dělitelem čísel a a b, tj. $d^* \mid a$ a $d^* \mid b$. Chceme dokázat, že potom $d^* \mid r_n$.

Vyjdeme z rovnice $r_{-1} = q_1 r_0 + r_1$, tj. $b = q_1 a + r_1$.

Pokud $n = 0$, pak $r_n = r_0 = a$. Podle předpokladu $d^* \mid a$ a tak $d^* \mid r_n$.

Pokud $n > 0$, pak jednoduchou úpravou dostaneme

$$r_1 = b - q_1 a. \tag{1.10}$$

Podle předpokladu $d^* \mid a$, $d^* \mid b$ a Lemmatu 1.3 bod 6) musí platit $d^* \mid r_1$.

Z rovnice $a = q_2 r_1 + r_2$ (pokud pokud $n > 1$) jednoduchou úpravou dostaneme

$$r_2 = a - q_2 r_1. \tag{1.11}$$

Z předchozího víme, že $d^* \mid a$ a $d^* \mid r_1$. Pak podle Lemmatu 1.3 bod 6) musí platit $d^* \mid r_2$.

Analogicky bychom z rovnic $r_i = q_{i+2}.r_{i+1} + r_{i+2}$ a předpokladů $d^* \mid r_i$, $d^* \mid r_{i+1}$ dospěli k závěru, že $d^* \mid r_{i+2}$, a to pro všechna $i = -1, 0, \ldots, n-2$. Takže v případě $i = n-2$ obdržíme vztah $d^* \mid r_n$.

□

Poznámka 1.16. Z předchozí Věty 1.15 plyne, že pomocí Euklidova algoritmu jsme schopni nalézt největšího společného dělitele libovolných dvou **přirozených** čísel. Z definice největšího společného dělitele celých čísel ovšem okamžitě plyne, že pro každé $a, b \in \mathbb{Z}$ platí

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

Navíc $\gcd(a, 0) = a$ pro $a \in \mathbb{Z}$ (viz Příklad 1.9). A tak můžeme tvrdit, že jsme schopni pomocí Euklidova algoritmu nalézt největšího společného dělitele libovolných dvou **celých** čísel.

Pomocí Euklidova algoritmu jsme již schopni nalézt největšího společného dělitele dvou celých čísel. Jak však nalézt největšího společného dělitele tří, čtyř a více celých čísel? Postup si ukážeme nejprve na příkladě, pak jej formulujeme obecně jako větu.

Příklad 1.17. Nalezněte největšího společného dělitele čísel 32, 84, 24, tj. hledáme $d = \gcd(32, 84, 24)$. Hodnotu d určíme jako $d = \gcd(\gcd(32, 84), 24)$. Nejprve Euklidovým algoritmem určíme $d_1 = \gcd(32, 84)$ a pak $d = \gcd(d_1, 24)$.

$$84 = 2 \cdot 32 + 20$$
$$32 = 1 \cdot 20 + 12$$
$$20 = 1 \cdot 12 + \mathbf{4}$$
$$12 = 3 \cdot \mathbf{4} + 0$$

Proto $d_1 = \gcd(32, 84) = 4$. Dále hledáme $d = \gcd(d_1, 24) = \gcd(4, 24)$.

$$24 = 6 \cdot \mathbf{4} + 0$$

Proto $d = \gcd(d_1, 24) = \gcd(4, 24) = 4$.

Příklad 1.18. Nalezněte největšího společného dělitele čísel 147, 84, 245, 63, 112, tj. hledáme $d = \gcd(147, 84, 245, 63, 112)$. Budeme postupovat obdobně jako v předcházejícím příkladě. Hodnotu d určíme jako

$$d = \gcd(\gcd(147, 84, 245, 63), 112) = \gcd(\gcd(\gcd(147, 84, 245), 63), 112) =$$
$$= \gcd(\gcd(\gcd(\gcd(147, 84), 245), 63), 112).$$

Nejprve Euklidovým algoritmem určíme $d_1 = \gcd(147, 84)$

$$147 = 1 \cdot 84 + 63$$
$$84 = 1 \cdot 63 + \mathbf{21}$$
$$63 = 3 \cdot \mathbf{21} + 0$$

Proto $d_1 = \gcd(147, 84) = 21$. Dále hledáme $d_2 = \gcd(d_1, 245) = \gcd(21, 245)$.

$$245 = 11 \cdot 21 + 14$$

$$21 = 1 \cdot 14 + \mathbf{7}$$

$$14 = 2 \cdot \mathbf{7} + 0$$

Proto $d_2 = \gcd(21, 245) = 7$. Dále hledáme $d_3 = \gcd(d_2, 63) = \gcd(7, 63)$.

$$63 = 9 \cdot \mathbf{7} + 0$$

Proto $d_3 = \gcd(7, 63) = 7$. Dále hledáme $d = d_4 = \gcd(d_3, 112) = \gcd(7, 112)$.

$$112 = 16 \cdot \mathbf{7} + 0$$

Proto $d = \gcd(147, 84, 245, 63, 112) = d_4 = \gcd(d_3, 112) = \gcd(7, 112) = 7$.

Věta 1.19. (O existenci největšího společného dělitele.) *Nechť* $a_1, \ldots, a_n \in \mathbb{Z}$, $n \geqq 2$. *Potom* $\gcd(a_1, \ldots, a_n)$ *existuje a platí*

$$\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n).$$

Důkaz. Důkaz provedeme indukcí podle n. V případě $n = 2$ dokazovaná věta říká, že $\gcd(a_1, a_2)$ existuje a platí $\gcd(a_1, a_2) = \gcd(\gcd(a_1), a_2)$. Existence $\gcd(a_1, a_2)$ je podle Věty 1.15 a Poznámky 1.16 zaručena - největšího společného dělitele dvou celých čísel vždy umíme najít. Snadno ověříme, že $\gcd(a_1) = a_1$. Věta 1.19 je tedy pro $n = 2$ pravdivá.

Následuje indukční krok. Předpokládáme pravdivost věty pro $n = r - 1$ a snažíme se na základě tohoto předpokladu dokázat pravdivost věty pro $n = r$. Předpokládáme tedy, že $\gcd(a_1, \ldots, a_{r-1})$ existuje (to nám bude stačit). Dokážeme, že platí

$$\gcd(a_1, \ldots, a_r) = \gcd(\gcd(a_1, \ldots, a_{r-1}), a_r).$$

Označme $d = \gcd(a_1, \ldots, a_{r-1})$ a $D = \gcd(d, a_r) = \gcd(\gcd(a_1, \ldots, a_{r-1}), a_r)$. Ukážeme, že číslo D je největším společným dělitelem čísel $a_1, \ldots, a_{r-1}, a_r$, tj. $D = \gcd(a_1, \ldots, a_{r-1}, a_r) = \gcd(a_1, \ldots, a_r)$.

Aby tomu tak bylo, muselo by číslo D dělit čísla $a_1, \ldots, a_{r-1}, a_r$. Je tomu tak?

Označili jsme $D = \gcd(d, a_r)$, proto $D \mid d$ a zároveň $D \mid a_r$. Protože $d = \gcd(a_1, \ldots, a_{r-1})$, musí číslo d dělit čísla $a_1, \ldots, a_{r-1}$. A protože $D \mid d$, musí D také dělit čísla $a_1, \ldots, a_{r-1}$ (viz Lema 1.3 bod 2)). Ověřili jsme tak, že D dělí čísla $a_1, \ldots, a_{r-1}, a_r$ (první podmínka z Definice 1.6).

Zbývá dokázat, že když číslo d^* dělí čísla $a_1, \ldots, a_{r-1}, a_r$, pak d^* také dělí číslo D (druhá podmínka z Definice 1.6).

Protože d^* dělí čísla $a_1, \ldots, a_{r-1}$, musí dělit i jejich největšího společného dělitele, tj. $d^* \mid d$. Navíc, podle předpokladu také platí, že $d^* \mid a_r$. Číslo d^* tak musí dělit i největšího společného dělitele čísel d a a_r, ale tím je právě číslo D, tj. $d^* \mid D$.

□

Nyní už umíme pro libovolnou n-tici celých čísel nalézt jejich největšího společného dělitele. Takže bychom už konečně mohli být spokojeni? Musím vás zklamat, pořád ještě ne! Nalezli jsme řešení problému - umíme najít $\gcd(a_1, \ldots, a_n)$ - ale musíme se ještě ujistit, že je to řešení jediné. (Teoreticky je tu zatím možnost, že bychom jiným postupem, než jsme uvedli, mohli najít i jiného největšího společného dělitele daných čísel. Ukážeme, že k tomu nemůže dojít.)

Věta 1.20. (O jednoznačnosti největšího společného dělitele) *Pro libovolná pevně zvolená čísla $a_1, \ldots, a_n \in \mathbb{Z}$, $n \in \mathbb{N}$ existuje právě jedno $d \in \mathbb{N}$ takové, že*

$$d = \gcd(a_1, \ldots, a_n).$$

Důkaz. Předpokládejme, že $d = \gcd(a_1, \ldots, a_n)$ a také $k = \gcd(a_1, \ldots, a_n)$. Dokážeme, že potom $d = k$ (z toho plyne, že nemohou existovat dva různí největší společní dělitelé čísel $a_1, \ldots, a_n$).

Podle předpokladu je číslo k největší společný dělitel čísel $a_1, \ldots, a_n$. Potom podle druhé podmínky v Definici 1.6 platí, že číslo k dělí čísla $a_1, \ldots, a_n$. Podle třetí podmínky v Definici 1.6 potom musí platit, že číslo k dělí největšího společného dělitele těchto čísel, a tím je, podle předpokladu, také číslo d. Proto $k \mid d$.

Analogicky (záměnou k za d a d za k) bychom mohli dokázat, že $d \mid k$. Dospěli jsme k závěru, že $k \mid d$ a zároveň $d \mid k$. Podle Lemmatu 1.3 bod 4) z toho plyne, že $|k| = |d|$. Ale k a d jsou největší společní dělitelé a ti jsou vždy nezáporní. Proto $k = d$.

□

Teď už známe vše, co je třeba k určování $\gcd(a_1, \ldots, a_n)$. Pokud by nám šlo jen o to, mohli bychom tuto kapitolu ukončit. Nicméně dokážeme i další vlastnosti $\gcd(a_1, \ldots, a_n)$, které použijeme později.

Lemma 1.21. *Nechť $a, b \in \mathbb{N}$. Potom existují čísla $x_0, y_0 \in \mathbb{Z}$ takové, že* $\gcd(a, b) = x_0 a + y_0 b$.

Důkaz. Definujme $A = \{xa + yb \in \mathbb{N} \mid x, y \in \mathbb{Z}\}$. Do množiny A tedy patří **přirozená** čísla ve tvaru $xa+yb$. Označme[1] $d = x_0 a + y_0 b$ nejmenší prvek množiny A.

Dokážeme, že $d = \gcd(a, b)$. Číslo $d \in A \subseteq \mathbb{N}$. Proto $d \geqq 0$. První podmínka z Definice 1.6 je splněna.

[1] Uvažovaná množina $A \subseteq \mathbb{N}$ je jistě neprázdná, má proto také svůj nejmenší prvek.

Vezměme libovolný pevně zvolený prvek $xa + yb \in A$. Číslo d je nejmenší prvek množiny A, a tak $xa+yb \geqq d$. Potom, podle Věty 1.12, existují čísla $q \in \mathbb{N}$, $r \in \mathbb{Z}$, $0 \leqq r < d$ takové, že

$$xa + yb = qd + r. \tag{1.12}$$

Protože $d = x_0a + y_0b$, můžeme psát

$$xa + yb = q(x_0a + y_0b) + r$$

$$xa + yb = qx_0a + qy_0b + r$$

$$(x - qx_0)a + (y - qy_0)b = r$$

Označíme-li $x_1 = x - qx_0$, $y_1 = y - qy_0$, pak

$$x_1a + y_1b = r$$

Může číslo $x_1a+y_1b = r$ být přirozené číslo? Nemůže! Kdyby ano, pak by muselo (vzhledem ke svému tvaru) patřit do množiny A. Ale $r < d$ a d je nejmenším prvkem množiny A! To je spor! Takže $0 \leqq r < d$ a navíc r není přirozené číslo. V tom případě existuje jediná možnost, a to $r = 0$. Vzhledem k rovnici (1.12) platí

$$xa + yb = qd.$$

Číslo $xa+yb \in A$ bylo libovolně zvolené, proto můžeme říci, že d dělí libovolný prvek z množiny A. Do množiny A patří také čísla a a b, neboť $a = 1.a + 0.b$ a $b = 0.a+1.b$. Odtud dostáváme $d \mid a$ a zároveň $d \mid b$ (druhá podmínka z Definice 1.6 je splněna).

Nyní dokážeme, že číslo d splňuje i třetí podmínku z Definice 1.6. Předpokládejme, že $d^* \mid a$ a také $d^* \mid b$. Potom $a = k_1d^*$, $b = k_2d^*$, kde $k_1, k_2 \in \mathbb{Z}$. Dosadíme-li do vztahu

$$d = x_0a + y_0b,$$

obdržíme

$$d = x_0k_1d^* + y_0k_2d^*,$$

$$d = (x_0k_1 + y_0k_2)d^*.$$

Proto $d^* \mid d$.

□

Předchozí lemma říká, že největšího společného dělitele dvou přirozených čísel a a b můžeme vyjádřit ve tvaru $\gcd(a,b) = x_0a + y_0b$. Zobecníme toto tvrzení i pro libovolnou dvojici celých čísel a a b.

Lemma 1.22. *Nechť $a, b \in \mathbb{Z}$. Potom existují čísla $x, y \in \mathbb{Z}$ takové, že* $\gcd(a,b) = xa + yb$.

Důkaz. V případě $b = 0$ platí $\gcd(a,b) = \gcd(a,0) = a = 1 \cdot a + 0 \cdot b$. V případě $a = 0$ platí $\gcd(a,b) = \gcd(0,b) = b = 0 \cdot a + 1 \cdot b$ (viz Příklad 1.9).

Dále uvažujme $a, b \neq 0$. V takovém případě $|a|, |b| \in \mathbb{N}$. Podle Lemmatu 1.21 existují $x_0, y_0 \in \mathbb{Z}$ takové, že

$$\gcd(|a|, |b|) = x_0|a| + y_0|b|.$$

Uvažme, že existují[1] $x, y \in \mathbb{Z}$ splňující $x_0|a| = xa$ a $y_0|b| = yb$. Proto

$$\gcd(a,b) = \gcd(|a|, |b|) = xa + yb.$$

□

Uvažujme číslo k, které dělí součin čísel ab. Dále předpokládejme, že čísla a a k jsou nesoudělná, tj. $\gcd(a,k) = 1$. Dokážeme, že v takovém případě musí k dělit číslo b. Pro ilustraci uveďme konkrétní příklad, kdy $k = 3$, $ab = 5 \cdot 6 = 30$. Evidentně 3 dělí číslo 30 a $\gcd(5,3) = 1$. Potom nelze jinak, než že $3 \mid 6$ (a vidíme, že je tomu opravdu tak).

Lemma 1.23. *Nechť $k, a, b \in \mathbb{Z}$. Jestliže $k \mid ab$,* $\gcd(k,a) = 1$, *potom $k \mid b$*

Důkaz. Jestliže $\gcd(k,a) = 1$ potom podle Lemmatu 1.22 existují celá čísla $x, y \in \mathbb{Z}$ takové, že

$$\gcd(k,a) = 1 = xk + ya.$$

Rovnici vynásobíme číslem b a obdržíme vztah

$$b = xkb + yab.$$

Podle předpokladu $k \mid ab$, proto musí existovat $k_0 \in \mathbb{Z}$ takové, že $ab = k_0k$. A tak

$$b = xkb + yk_0k,$$

$$b = (xb + yk_0)k. \tag{1.13}$$

Číslo $xb + yk_0 \in \mathbb{Z}$, potom z rovnice (1.13) a Definice 1.1 plyne, že $k \mid b$. □

[1] Číslo $x = x_0$ pro $a \geqq 0$ a $x = -x_0$ pro $a < 0$; $y = y_0$ pro $b \geqq 0$ a $y = -y_0$ pro $b < 0$;

Předpokládejme, že hledáme společného dělitele čísel 24 a 88. Snadno odhadneme, že obě čísla jsou násobky čísla 4, neboť $24 = 4 \cdot 6$ a $88 = 4 \cdot 22$. Potom $\gcd(24, 88)$ můžeme určit jako čtyřnásobek $\gcd(6, 22)$. Tj.

$$\gcd(24, 88) = 4 \cdot \gcd(6, 22) = 8.$$

Toto tvrzení si můžeme dovolit na základě následujícího lemmatu.

Lemma 1.24. *Jestliže* $a, b, c \in \mathbb{Z}$, *potom* $\gcd(ca, cb) = |c| \cdot \gcd(a, b)$.

Důkaz. V případě $c = 0$ je tvrzení lemmatu pravdivé, neboť $\gcd(0, 0) = 0$. Dále uvažujme $c \neq 0$. Podle Lemmatu 1.22 existují celá čísla $x, y \in \mathbb{Z}$ taková, že

$$\gcd(ca, cb) = xca + ycb,$$

$$\gcd(ca, cb) = c(xa + yb) = {}^{1}|c||xa + yb|. \tag{1.14}$$

Dokážeme, že $\gcd(a, b) = |xa + yb|$. To nebude těžké, neboť z (1.14) okamžitě plyne, že

$$(|c||xa + yb|) \mid ca \ \wedge \ (|c||xa + yb|) \mid cb.$$

Existují tedy čísla $k_1, k_2 \in \mathbb{Z}$ takové, že

$$k_1 c|xa + yb| = ca \ \wedge \ k_2 c|xa + yb| = cb,$$

$$k_1|xa + yb| = a \ \wedge \ k_2|xa + yb| = b.$$

A tak $(|xa + yb|) \mid a$, $(|xa + yb|) \mid b$ (což je druhá podmínka toho, aby $\gcd(a, b) = |xa + yb|$ - viz Definice 1.6, první podmínka $|xa + yb| \geqq 0$ je evidentně splněna).

Nyní ověříme platnost třetí podmínky z Definice 1.6. Předpokládejme, že $d^* \mid a$, $d^* \mid b$. Potom existují čísla $m_1, m_2 \in \mathbb{Z}$ takové, že $m_1 d^* = a$, $m_2 d^* = b$. Proto

$$xa + yb = xm_1 d^* + ym_2 d^*,$$

$$xa + yb = (xm_1 + ym_2) d^*.$$

Odtud dostáváme $d^* \mid (|xa + yb|)$ (třetí podmínka v Definici 1.6). Tím jsme dokázali, že $\gcd(a, b) = |xa + yb|$. Ze vztahu (1.14) dostáváme

$$\gcd(ca, cb) = |c| \gcd(a, b).$$

□

[1] Uvažte, že $\gcd(ca, cb)$ je nezáporné číslo.

1.2.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.1.1.

1. Dokažte, že pro každé $r \in \mathbb{R}$ platí: $2r - 1 - 2r < [2r] - 2[r] < 2r - 2(r-1)$.
2. Dokažte, že $\forall x \in \mathbb{R}$ a $\forall p, k \in \mathbb{N}$ platí $\left[\frac{x}{p^k}\right] = \left[\frac{n}{p^k}\right]$, kde $n = [x]$.
3. Dokažte, že pro každé $x \in \mathbb{R}^+$ a $p \in \mathbb{N}$ platí $\frac{1}{x}\left[\frac{x}{p^k}\right] \leqq \frac{1}{p^k}$.
4. Nalezněte celá čísla x_0 a y_0 tak, aby $\gcd(36, 14) = x_0 36 + y_0 15$. Tj. vyjádřete největšího společného dělitele čísel 36 a 14 jako jejich lineární kombinaci.
5. Nalezněte největšího společného dělitele čísel 2 328 a 3 581

1.3 Kanonický rozklad přirozeného čísla

Mezi přirozenými čísly se najdou taková, která jsou, co se týče dělitelnosti, poněkud vzpurná, neboť se nenechají podělit jen tak něčím, nebo někým. Uvažujme, jakým přirozeným číslem je dané přirozené číslo n dělitelné. Určitě číslem 1, neboť $n \cdot 1 = n$ a také číslem n ze stejného důvodu. A jinak? A jinak si nemůžeme být jisti. Třeba už žádným přirozeným číslem. Jako v případě čísla $n = 7$. Je dělitelné přirozenými čísly 1 a 7 a to je vše. Jistě už tušíte, je řeč o prvočíslech. Takže, pro formu, uvedeme jejich definici.

Definice 1.25. (*Prvočíslo*) Prvočíslem na množině $\mathbb{N}$ nazveme libovolné $p \in \mathbb{N}$, $p \geqq 2$ právě když pro každé $a \in \mathbb{N}$ platí

$$a \mid p \Leftrightarrow (a = 1 \ \vee a = p).$$

(Všimněte si, že číslo 1 *nepovažujeme za prvočíslo.)*

Definice 1.26. *(Číslo složené)* Číslem složeným nazveme na množině $\mathbb{N}$ libovolné $s \in \mathbb{N}$, $s \geqq 2$, pro které platí

$$s = d_1 d_2,$$

kde $d_1, d_2 \in \mathbb{N}$, $d_1 > 1$, $d_2 > 1$.

Všimněte si, že přirozené číslo větší, nebo rovné dvěma, je buď prvočíslo, a nebo číslo složené. Tento poznatek formulujeme jako lemma a dokážeme jeho pravdivost.

Lemma 1.27. *Číslo $n \geqq 2$ je složené číslo právě tehdy, když není prvočíslo.*

Důkaz. Musíme dokázat, že číslo $n \geqq 2$ je složené číslo právě tehdy, když není prvočíslo.

Nejprve předpokládejme, že $n \geqq 2$ je složené číslo. Podle Definice 1.26 $n = d_1 d_2$, kde $d_1, d_2 \in \mathbb{N}$, $d_1 > 1$, $d_2 > 1$. To, podle Definice 1.1, znamená, že $d_2 > 1$ dělí číslo n. Navíc d_2 nemůže být rovno n, protože pak by $n = d_1 d_2 = d_1 n$, a to by znamenalo, že $d_1 = 1$, což je spor. Potom ale n nemůže být prvočíslo (viz Definice 1.25).

Nyní dokážeme, že v případě, kdy n není prvočíslo, musí být n číslem složeným. Pokud n není prvočíslo, musí existovat nějaký dělitel čísla n, označme jej d_2, který je různý od n i od 1, tj. $d_2 \neq n$, a také $d_2 \neq 1$. Podle Definice 1.1 můžeme psát $n = k.d_2$ a nic nebrání tomu, abychom označili $k = d_1$. A tak dostáváme $n = d_1 d_2$. Může být d_1 rovno jedné? V tom případě by platilo $n = 1 \cdot d_2 = d_2$, což je spor s tím, že $d_2 \neq n$. Zjistili jsme tedy, že $n = d_1 d_2$, kde d_1 a d_2 jsou přirozená čísla různá od jedné. A tak $d_1 > 1$ a $d_2 > 1$. Podle Definice 1.26 musí být n číslo složené (a to jsme chtěli dokázat).

□

Prvočísla fungují jako základní stavební jednotky, z nichž se pomocí operace násobení tvoří ostatní přirozená čísla. Ukážeme si, že každé přirozené číslo, větší, nebo rovné dvěma, můžeme napsat jako součin prvočísel (nebo je samo prvočíslo). Například $2 = 2$, $3 = 3$, $4 = 2 \cdot 2$, $5 = 5$, $6 = 2 \cdot 3$, $\ldots$, $140 = 2 \cdot 2 \cdot 5 \cdot 7$, $\ldots$.

Navíc dokážeme, že dané přirozené číslo můžeme rozložit na součin prvočísel pouze jediným způsobem (až na pořadí prvočísel, tj. $n = 2 \cdot 3 \cdot 5$ a $n = 3 \cdot 2 \cdot 5$ považujeme za totožné rozklady přirozeného čísla n). Takovému rozkladu říkáme *kanonický rozklad přirozeného čísla.*

Lemma 1.28. *Každé přirozené číslo $n \geqq 2$ je rovno součinu prvočísla a přirozeného čísla. Tj. $\forall n \in \mathbb{N}\ \exists p, k \in \mathbb{N}$, kde p je prvočíslo takové, že*

$$n = pk.$$

Důkaz. Důkaz provedeme silnou indukcí. Pro $n = 2 = 2 \cdot 1$ je tvrzení dokazovaného lemmatu jistě pravdivé.

Předpokládejme, že tvrzení je pravdivé také pro všechna přirozená čísla větší, nebo rovna číslu 2 a menší než než n. Dokážeme, že potom je tvrzení lemmatu pravdivé také pro n.

Nejprve uvažujme případ, kdy n je prvočíslo. Potom je situace jednoduchá, stačí zvolit $p = n$ a $k = 1$, a evidentně $n = pk$.

V případě, že n není prvočíslo, musí být číslem složeným (viz Lemma 1.27). A tak, podle Definice 1.26, existují přirozená čísla p_1 a k_1, které jsou větší než 1, takové, že

$$n = p_1 k_1.$$

Je tak zřejmé, že $2 \leqq p_1 < n$. Podle předpokladu proto můžeme číslo p_1 napsat ve tvaru $p_1 = pk_2$, kde p je prvočíslo. A tak

$$n = pk_2k_1 = pk,$$

kde $k = k_2k_1$ je přirozené číslo. □

Vraťme se k původnímu problému. Dokážeme, že každé složené číslo je možné rozložit na součin prvočísel. Například $50 = 2{\cdot}5{\cdot}5 = 2{\cdot}5^2$ a podobně. Takovému rozkladu přirozeného čísla n říkáme *kanonický rozklad přirozeného čísla* n.

Věta 1.29. (O kanonickém rozkladu) *Každé přirozené číslo větší než jedna lze napsat jako součin prvočísel. To jest, pro každé přirozené číslo $n \neq 1$ existují prvočísla $p_1, \ldots, p_s$ taková, že*

$$n = p_1 \cdots p_s.$$

Důkaz. Důkaz provedeme silnou indukcí. Pro $n = 2$ je tvrzení dokazovaného lemmatu jistě pravdivé ($p_1 = 2$, $s = 1$).

Předpokládejme, že tvrzení je pravdivé také pro všechna přirozená čísla větší, nebo rovna číslu 2 a menší než než n. Dokážeme, že potom je tvrzení lemmatu pravdivé také pro n.

Použijeme Lemma 1.28. Podle něj každé přirozené číslo $n \geqq 2$ můžeme napsat ve tvaru

$$n = pk,$$

kde p je prvočíslo a $k \in \mathbb{N}$.

- Nejprve uvažujme případ, kdy $k = 1$. Potom $n = p = p_1$.
- V případě, že $k > 1$ z rovnosti $n = pk$ plyne, že $2 \leqq k < n$. Podle indukčního předpokladu je potom možné napsat číslo k jako součin prvočísel. A tak $n = pk = p_1 \cdots p_s$.

□

Důsledek 1.30. Pro každé přirozené číslo $n \neq 1$ existují navzájem různá prvočísla $p_1, \ldots, p_m$ a čísla $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ taková, že

$$n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}.$$

Důkaz. Tvrzení Důsledku 1.30 plyne okamžitě z Věty 1.29. Stačí si uvědomit, že mezi prvočísly $p_1, \ldots, p_s$ mohou být některá stejná. Ty, která jsou stejná, označíme stejně, vynásobíme a napíšeme ve tvaru mocniny (např. u $p_1p_2p_3p_4p_5 = 2{\cdot}2{\cdot}3{\cdot}5{\cdot}5$ můžeme přeznačit na $p_1^2p_2p_3^2 = 2^2{\cdot}3{\cdot}5^2$). □

Příklad 1.31. Nalezněte kanonické rozklady přirozených čísel 112, 238, 17 a dalších, které si zajisté vymyslíte sami.

Řešení:

$$112 = 2{\cdot}56 = 2{\cdot}2{\cdot}28 = 2{\cdot}2{\cdot}2{\cdot}14 = 2{\cdot}2{\cdot}2{\cdot}2{\cdot}7 = 2^4{\cdot}7$$

$$238 = 2{\cdot}119 = 2{\cdot}7{\cdot}17$$

$$17 = 17$$

Ukázali jsme si, že každé přirozené číslo kromě jedničky můžeme napsat jako součin prvočísel (v případě, že je toto číslo samo prvočíslem, bereme to jako speciální případ: $p = p_1$). Mohli by jsme si položit otázku, zda to můžeme udělat pouze jedním způsobem, nebo jestli dané číslo n lze rozložit na součin prvočísel více způsoby.

Například, víme, že $1100 = 11{\cdot}100 = 11{\cdot}10^2 = 11{\cdot}5^2{\cdot}2^2$. Někdo nám však může tvrdit, že také platí $1100 = 61{\cdot}3^2{\cdot}2$. Může mít pravdu? Následující Věta 1.33 - bývá označována jako „*Základní věta aritmetiky.*“ - říká, že ani náhodou! Nemohou existovat dva různé kanonické rozklady téhož přirozeného čísla! (Navíc $61{\cdot}3{\cdot}3{\cdot}2 = 183{\cdot}3{\cdot}2 = 549{\cdot}2 = 1098$, takže těsně vedle ;).)

Nejprve však musíme dokázat Lemma 1.32, které budeme potřebovat v důkazu Věty 1.33. Toto lemma říká, že když prvočíslo p dělí součin čísel, musí p dělit alespoň jedno z těchto čísel.

Lemma 1.32. *Nechť p je prvočíslo, $s \in \mathbb{N}$. Jestliže $p \mid (a_1 \cdots a_s)$, potom p dělí alespoň jedno z čísel $a_1, \ldots, a_s$, tj. $p \mid a_1 \vee \cdots \vee p \mid a_s$.*

Důkaz. Důkaz provedeme matematickou indukcí. V případě, kdy $s = 1$ je věta evidentně pravdivá. Můžeme proto přistoupit k indukčnímu kroku.

Předpokládáme, že když $p \mid (a_1 \cdots a_n)$, potom p dělí alespoň jedno z čísel $a_1, \ldots, a_n$. Musíme dokázat, že když $p \mid (a_1 \cdots a_n a_{n+1})$, potom p je dělitelem alespoň jednoho z čísel $a_1, \ldots, a_n, a_{n+1}$.

Jestliže $p \mid (a_1 \cdots a_n a_{n+1})$, mohou nastat dvě možnosti.

- Buď $p \mid a_{n+1}$, potom p je dělitelem alespoň jednoho z čísel $a_1, \ldots, a_n, a_{n+1}$.
- A nebo p nedělí a_{n+1}. Potom $\gcd(p, a_{n+1}) = 1$. Podle Lemmatu 1.23 z předpokladu $p \mid (a_1 \cdots a_n a_{n+1})$ plyne, že $p \mid (a_1 \cdots a_n)$.

  Indukční předpoklad říká, že potom p dělí alespoň jedno z čísel $a_1, \ldots, a_n$.

Dokázali jsme, že mohou nastat dvě možnosti. Buď $p \mid a_{n+1}$, nebo p dělí alespoň jedno z čísel $a_1, \ldots, a_n$. To jest, p dělí alespoň jedno z čísel $a_1, \ldots, a_n, a_{n+1}$. □

Věta 1.33. (O jednoznačnosti kanonického rozkladu - Základní věta aritmetiky) *Pro každé přirozené číslo $n \neq 1$ existuje právě jeden kanonický rozklad na součin prvočísel. Tj. pokud $p_1, \ldots, p_m, q_1, \ldots, q_s$ jsou prvočísla (nemusí být navzájem různá) a platí*

$$n = p_1 \cdots p_m = q_1 \cdots q_s, \tag{1.15}$$

potom $m = s$ a pro každé $i \in \{1, \ldots, m\}$ existuje $j_i \in \{1, \ldots, s\}$ takové, že $p_i = q_{j_i}$.

Důkaz. Podle předpokladu věty

$$p_1 \cdots p_m = q_1 \cdots q_s. \tag{1.16}$$

Z rovnosti (1.16) dostáváme

$$p_1 \mid (q_1 \cdots q_s).$$

Podle Lemmatu 1.32 pak p_1 je dělitelem alespoň jednoho z čísel $q_1, \ldots, q_s$. To jest, existuje $q_{j_1} \in \{q_1, \ldots, q_s\}$ takové, že $p_1 \mid q_{j_1}$. Podle definice prvočísla (viz Defeinice 1.25) to znamená, že $p_1 = q_{j_1}$ (p_1 je prvočíslo, a tak $p_1 \neq 1$!!).

Při vhodném přeindexování[1] čísel $q_1, \ldots, q_s$ tak z (1.16) dostáváme

$$p_1 p_2 \cdots p_m = p_1 q_2 \cdots q_s.$$

$$p_2 \cdots p_m = q_2 \cdots q_s.$$

Pokud výše uvedený postup provedeme m-krát, zjistíme, že pro každé $i \in \{1, \ldots, m\}$ existuje $j_i \in \{1, \ldots, s\}$ takové, že $p_i = q_{j_i}$ a nakonec obdržíme rovnost

$$1 = q_{s-m} \cdots q_s.$$

Z toho plyne, že $s = m$. □

Zobecnění Věty 1.33 pro celá čísla vypadá následovně.

Věta 1.34. *Pro každé celé číslo $z \neq 1$ existují prvočísla $p_1, \ldots, p_m$ a $j \in \{-1, 0, 1\}$ taková, že*

$$z = j p_1 \cdots p_m.$$

Tento rozklad na součin je, až na pořadí činitelů, jednoznačný.

Pokud známe kanonické rozklady přirozených[2] čísel a a b, je jednoduché nalézt jejich největšího společného dělitele. Ukážeme si to na konkrétním příkladě.

[1] Číslo $q_{j_1} = p_1$ přeznačíme na q_1 a naopak.

[2] Hledání největšího společného dělitele celých čísel $a, b \neq 0$ lze převést na hledání Hledání největšího společného dělitele přirozených čísel, neboť $\gcd(a, b) = \gcd(|a|, |b|)$

Příklad 1.35. Vezměme $a = 2^3 \cdot 5^2 \cdot 11^3$ a $b = 2^4 \cdot 5^1 \cdot 7^4$. Hledáme $d = \gcd(a, b)$. Uvažujme, jak musí vypadat kanonický rozklad čísla d? Obecně $d = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Potřebujeme zjistit o jaká prvočísla $p_1, \ldots, p_n$ konkrétně jde. Číslo d má být dělitelem (a to největším možným) čísel $a = 2^3 \cdot 5^2 \cdot 11^3$ a $b = 2^4 \cdot 5^1 \cdot 7^4$.

Která čísla dělí a? Ze vztahu

$$a = 2^3 \cdot 5^2 \cdot 11^3$$

je zřejmé, že jen ta, která mají ve svém kanonickém rozkladu pouze některá z prvočísel 2, 5 a 11. [1] A to s mocninami, které nepřevyšují mocniny těchto prvočísel v kanonickém rozkladu čísla a. (Tj. čísla ve tvaru $2^{k_1} \cdot 5^{k_2} \cdot 11^{k_3}$, kde $0 \leqq k_1 \leqq 3$, $0 \leqq k_2 \leqq 2$, $0 \leqq r_3 \leqq 3$.)

Která čísla dělí b? Ze vztahu

$$b = 2^4 \cdot 5^1 \cdot 7^4$$

je zřejmé, že jen ta, která mají ve svém kanonickém rozkladu pouze některá z prvočísel 2, 5 a 7. A to s mocninami, které nepřevyšují mocniny těchto prvočísel v kanonickém rozkladu čísla b. (Tj. čísla ve tvaru $2^{r_1} \cdot 5^{r_2} \cdot 7^{k_3}$, kde $0 \leqq r_1 \leqq 4$, $0 \leqq r_2 \leqq 1$, $0 \leqq r_3 \leqq 4$.)

Číslo, které má dělit a i b, musí splňovat obě tyto podmímky. Takže musí mít ve svém kanonickém rozkladu pouze některá z prvočísel 2, 5. A to s mocninami, které nepřevyšují mocniny těchto prvočísel v kanonickém rozkladu čísel a a b. Jde tedy o čísla ve tvaru $2^{m_1} \cdot 5^{m_2}$, kde $0 \leqq m_1 \leqq 3$, $0 \leqq m_2 \leqq 1$. A které z těchto čísel je největší? Přece

$$\gcd(a, b) = 2^3 \cdot 5^1 = 40.$$

Příklad 1.36. Určete největšího společného dělitele čísel

a) $a = 3^4 \cdot 5^3 \cdot 7^2$, $b = 2^4 \cdot 5^4 . 7$

b) $a = 5^3 \cdot 11^2$, $b = 2^3 \cdot 5^4 \cdot 7 \cdot 11^4$

c) $a = 5^4 \cdot 7^2$, $b = 2^3 \cdot 11^4$

Návod k řešení nám dal předchozí příklad. Sepíšeme do součinu pouze ta prvočísla, která se vyskytují v kanonickém rozkladu a i b. Pak k nim připíšeme menší z mocnin, které se u nich vyskytly v kanonických rozkladech a a b.

[1] No jen uvažte, může třeba číslo $m = 7 \cdot 5 \cdot 11$ dělit $a = 2^3 \cdot 5^2 \cdot 11^3$? Kdyby tomu tak bylo, znamenalo by to, že $a = km$, kde $k \in \mathbb{N}$. Odtud $a = 2^3 \cdot 5^2 \cdot 11^3 = k \cdot 7 \cdot 5 \cdot 11$. To by znamenalo, že $7 \mid 2^3 \cdot 5^2 \cdot 11^3$. Podle Lemmatu 1.32 pak musí 7 dělit alespoň jedno z čísel 2, 5 a 11 to je spor! Obecně bychom tímto způsobem snadno dokázali, že číslo $m = pm_1$, kde $m_1 \in \mathbb{N}$ a p je prvočíslo různé od 2, 5 a 11, nemůže dělit $a = 2^3 \cdot 5^2 \cdot 11^3$.

ad a) $a = 3^4 \cdot \mathbf{5^3} \cdot 7^2$, $b = 2^4 \cdot 5^4 \cdot \mathbf{7}$, potom $\gcd(a,b) = 5^3 \cdot 7$

ad b) $a = \mathbf{5^3} \cdot \mathbf{11^2}$, $b = 2^3 \cdot 5^4 \cdot 7 \cdot 11^4$, potom $\gcd(a,b) = 5^3 \cdot 11^2$

ad c) $a = 5^4 \cdot 7^2$, $b = 2^3 \cdot 11^4$, potom $\gcd(a,b) = 1$

Postup použitý ve výše uvedených příkladech můžeme formulovat jako lemma.

Lemma 1.37. *Nechť $a, b \in \mathbb{N}$, $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ a $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$, kde pro každé $i \in \{1, \ldots, n\}$ platí, že p_i je prvočíslo a $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$. Potom*

$$\gcd(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_n^{\min\{\alpha_n,\beta_n\}}.$$

Důkaz. Číslo $p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_n^{\min\{\alpha_n,\beta_n\}}$ vyhovuje všem podmínkám kladeným na největšího společného dělitele čísel a a b.

- Číslo $p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_n^{\min\{\alpha_n,\beta_n\}}$ je jistě větší než nula.
- Číslo $p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_n^{\min\{\alpha_n,\beta_n\}}$ je jistě dělitelem čísla a i b.
- Každý společný dělitel čísel a a b ve svém kanonickém rozkladu může obsahovat pouze prvočísla $p_1, \ldots, p_n$. Navíc se p_i v tomto kanonickém rozkladu může vyskytovat nanejvýš v mocnině $\min\{\alpha_i, \beta_i\}$. Proto je každý společný dělitel čísel a a b dělitelem čísla $p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_n^{\min\{\alpha_n,\beta_n\}}$.

□

Pomocí kanonických rozkladů snadno dokážeme následující lemma, které budeme potřebovat v podkapitole 2.3.

Lemma 1.38. *Pro každé číslo $n \in \mathbb{N}$ existují $a, b \in \mathbb{N}$ takové, že $n = a^2 b$ a číslo b ve svém kanonickém rozkladu obsahuje prvočísla pouze s mocninou rovnou jedné, nebo nula (tj. $b = q_1 \cdots q_r$, kde $q_1, \ldots, q_r$ jsou navzájem různá prvočísla, nebo $b = 1$).*

Důkaz. V případě $n = 1$ platí $n = 1^2 \cdot 1$. Podle Důsledku 1.30 pro každé přirozené číslo $n \neq 1$ existují navzájem různá prvočísla $p_1, \ldots, p_m$ a čísla $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$ taková, že

$$n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}.$$

Některá z čísel $\alpha_1, \ldots, \alpha_m$ mohou být sudá a některá lichá, nebo jsou všechna sudá, nebo jsou všechna lichá.

V případě, že jsou všechna sudá, existují $\beta_1, \ldots, \beta_m \in \mathbb{N}$ taková, že $\alpha_1 = 2\beta_1, \ldots, \alpha_m = 2\beta_m$. Potom

$$n = p_1^{2\beta_1} \cdots p_m^{2\beta_m} = (\underbrace{p_1^{\beta_1} \cdots p_m^{\beta_m}}_{=a})^2 = a^2 \cdot \underbrace{1}_{=b} = a^2 b.$$

V případě, že všechna čísla $\alpha_1, \ldots, \alpha_m$ jsou lichá, existují $\beta_1, \ldots, \beta_m \in \mathbb{N} \cup \{0\}$ taková, že $\alpha_1 = 2\beta_1 + 1, \ldots, \alpha_m = 2\beta_m + 1$. Potom

$$n = p_1^{2\beta_1+1} \cdots p_m^{2\beta_m+1} = (\underbrace{p_1^{\beta_1} \cdots p_m^{\beta_m}}_{=a})^2 \underbrace{p_1 \cdots p_m}_{=b} = a^2 b.$$

V případě, že některá z čísel $\alpha_1, \ldots, \alpha_m$ jsou sudá a některá lichá, můžeme zvolit označení tak, že $\alpha_1, \ldots, \alpha_s$ jsou sudá a $\alpha_{s+1}, \ldots, \alpha_m$ jsou lichá. Takže existují $\beta_1, \ldots, \beta_m \in \mathbb{N} \cup \{0\}$ taková, že $\alpha_1 = 2\beta_1, \ldots, \alpha_s = 2\beta_s$ a $\alpha_{s+1} = 2\beta_{s+1} + + 1, \ldots, \alpha_m = 2\beta_m + 1$. Potom

$$n = p_1^{2\beta_1} \cdots p_s^{2\beta_s} \cdot p_{s+1}^{2\beta_{s+1}+1} \cdots p_m^{2\beta_m+1} = (\underbrace{p_1^{\beta_1} \cdots p_m^{\beta_m}}_{=a})^2 \underbrace{p_{s+1} \cdots p_m}_{=b} = a^2 b.$$

□

1.3.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.1.2.

1. Nalezněte kanonický rozklad čísla 196.

2. Nalezněte kanonický rozklad čísla $(196)^3$.

3. Nalezněte kanonický rozklad čísla $(567)^2(196)^3$.

4. Nalezněte kanonický rozklad čísel $(180)^2$, $(250)^3$ a určete $\gcd((180)^2, (250)^3)$.

5. Nalezněte kanonický rozklad čísla 99 221.

1.4 Nejmenší společný násobek

Na tento pojem si pravděpodobně také vzpomenete ze střední školy. Zkuste najít nejmenší společný násobek čísel $a = 4$ a $b = 6$. Správná odpověď zní 12. Je to nejmenší nezáporné číslo, které je dělitelné jak číslem a, tak číslem b. Snadno bychom vypozorovali, že všechny společné násobky čísel $a = 4$ a $b = 6$ jsou násobky čísla 12 (společnými násobky čísel $a = 4$ a $b = 6$ jsou například 12, 24, 48, ...).

Intuitivní představu pojmu *nejmenší společný násobek* už máme, a tak uvedeme jeho definici.

Definice 1.39. (*Nejmenší společný násobek*) Nechť $a, b \in \mathbb{Z}$. Potom nejmenším společným násobkem čísel a a b nazveme číslo $n(a,b) \in \mathbb{Z}$ splňující podmínky

1.) $n(a,b) \geqq 0$

2.) $a \mid n(a,b)$ a zároveň $b \mid n(a,b)$
(tj. $n(a,b)$ je společným násobkem čísel a a b).

2.) Jestliže $a \mid n$ a zároveň $b \mid n$, potom $n(a,b) \mid n$
(tj. číslo $n(a,b)$ musí dělit všechny společné násobky čísel a a b).

Jak najít nejmenší společný násobek daných čísel a a b? Můžeme využít toho, že již umíme najít $\gcd(a,b)$ a následující věty.

Věta 1.40. *Nechť $a, b \in \mathbb{Z} - \{0\}$. Potom platí*

$$n(a,b) = \frac{|ab|}{\gcd(a,b)}.$$

Důkaz. Dokážeme, že číslo $\frac{|ab|}{\gcd(a,b)}$ splňuje podmínky z Definice 1.39.

- $\frac{|ab|}{\gcd(a,b)} > 0$, protože $|ab| > 0$ a také $\gcd(a,b) > 0$.
- Víme (viz definice $\gcd(a,b)$ - Definice 1.6), že $\gcd(a,b) \mid a$ a zároveň $\gcd(a,b) \mid b$. Existují tedy $k_1, k_2 \in \mathbb{Z} - \{0\}$ taková, že $a = k_1 \cdot \gcd(a,b)$ a $b = k_2 \cdot \gcd(a,b)$. Označme

$$x = \frac{|ab|}{\gcd(a,b)}. \tag{1.17}$$

Potom, podle předchozího,

$$x = \frac{|ab|}{\gcd(a,b)} = \frac{|k_1| \cdot \gcd(a,b) \cdot |b|}{\gcd(a,b)} = |k_1||b| = k_1^* b, \tag{1.18}$$

kde $k_1^* \in \mathbb{Z}$ a zároveň

$$x = \frac{|ab|}{\gcd(a,b)} = \frac{|a||k_2| \cdot \gcd(a,b)}{\gcd(a,b)} = |k_2||a| = k_2^* a, \tag{1.19}$$

kde $k_2^* \in \mathbb{Z}$. Z (1.18) a (1.19) plyne, že x je společným násobkem čísel a a b, neboť $a \mid x$ (podle (1.19)) a zároveň $b \mid x$ (podle (1.18)).

- Zbývá dokázat, že x je také nejmenším společným násobkem čísel a a b. To jest, když n je společný násobek čísel a a b, potom $x \mid n$. Pro $n = 0$ je tento požadavek jistě splněn. Předpokládejme proto, že $a \mid n$ a zároveň $b \mid n$, kde $n \neq 0$. Odtud $n = m_1 a = m_2 b$, kde $m_1, m_2 \in \mathbb{Z}$. Podle Lemmatu 1.22 $\gcd(a,b) = x_0 a + y_0 b$, kde $x_0, y_0 \in \mathbb{Z}$. S využitím těchto vztahů a (1.17) můžeme psát

$$\begin{aligned} x &= \frac{|ab|}{\gcd(a,b)} \\ |ab| &= x \gcd(a,b) \\ |ab| &= x(x_0 a + y_0 b) \\ |m_1 m_2 ab| &= x|x_0 m_1 m_2 a + y_0 m_1 m_2 b| \\ n^2 &= x|x_0 m_2 n + y_0 m_1 n| \\ |n| &= x|x_0 m_2 + y_0 m_1| \end{aligned} \tag{1.20}$$

  Z (1.20) plyne, že $x \mid n$ a to jsme chtěli dokázat.

□

Příklad 1.41. Pomocí Věty 1.40 určete $n(a,b)$, kde $a = 238$, $b = 21$. Nejprve Euklidovým algoritmem určíme $\gcd(a,b)$.

$$238 = 11 \cdot 21 + 7,$$

$$21 = 3 \cdot 7 + 0.$$

Posledním nenulovým zbytkem je 7, proto $\gcd(a,b) = 7$.

$$n(a,b) = \frac{|ab|}{\gcd(a,b)} = \frac{238 \cdot 21}{\gcd(238,7)} = \frac{4998}{7} = 714.$$

Nejmenší společný dělitel násobek a a b můžeme najít také pomocí kanonického rozkladu (obdobně jako $\gcd(a,b)$, viz Příklad 1.36).

Příklad 1.42. Pomocí kanonického rozkladu čísel a a b určete $n(a,b)$, jestliže $a = 3^2 \cdot 5^4$, $b = 2^5 \cdot 3^3 \cdot 7^2$. Násobky čísla a mají tvar $3^2 \cdot 5^4 \cdot k_1$, kde $k_1 \in \mathbb{N}$. Násobky čísla b mají tvar $2^5 \cdot 3^3 \cdot 7^2 \cdot k_2$, kde $k_2 \in \mathbb{N}$. Společný násobek čísel a a b musí mít tvar

$$2^5 \cdot 3^3 \cdot 5^4 \cdot 7^2 \cdot k_3, \text{ kde } k_3 \in \mathbb{N}.$$

A které z těchto čísel je nejmenší? Přece to, kde $k_3 = 1$. Takže $n(a,b) = 2^5 \cdot 3^3 \cdot 5^4 \cdot 7^2$.

Příklad 1.43. Pomocí kanonického rozkladu čísel a a b určete $n(a,b)$, jestliže $a = 2^2 \cdot 5^3 \cdot 7^3$, $b = 3^2 \cdot 5^4 \cdot 7^2$. Podle předchozího příkladu je postup následující.

Nejprve sepíšeme do součinu všechny prvočísla, které se vyskytují v kanonických rozkladech čísel a a b. Pak k nim připíšeme nejvyšší mocniny, které se u nich vyskytly v kanonických rozkladech čísel a a b.

$$\left.\begin{array}{l} a \ = 2^2 \cdot 5^3 \cdot 7^3 \\ \\ b = 3^2 \cdot 5^4 \cdot 7^2 \end{array}\right\} \Rightarrow n(a,b) = 2^2 \cdot 3^2 \cdot 5^4 \cdot 7^3$$

Postup použitý ve výše uvedených příkladech můžeme formulovat jako lemma.

Lemma 1.44. *Nechť $a, b \in \mathbb{N}$, $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ a $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$, kde pro každé $i \in \{1, \ldots, n\}$ platí, že p_i je prvočíslo a $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$. Potom*

$$n(a,b) = p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}}.$$

Důkaz. Číslo $p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}}$ vyhovuje všem podmínkám kladeným na nejmenší společný násobek čísel a a b.

- Číslo $p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}}$ je jistě větší než nula.
- Číslo $p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}}$ je jistě násobkem čísla a i b.
- Každý společný násobek čísel a a b ve svém kanonickém rozkladu určitě obsahuje také prvočísla $p_1, \ldots, p_n$. Navíc se p_i v tomto kanonickém rozkladu musí vyskytovat nejméně v mocnině $\max\{\alpha_i, \beta_i\}$. Proto je každý společný násobek čísel a a b násobkem čísla $p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}}$.

□

V předcházejících třech příkladech jsme si ukázali dva postupy určování hodnoty $n(a,b)$. Postup využívající kanonických rozkladů je velmi elegantní, ale má velkou slabinu. Pokud nejsou zadány kanonické rozklady, pak je musíme nejprve najít. Není problém? Ale je! U „velkých“ čísel je to značný problém (využívá se toho v současných metodách šifrování - jak uvidíme později). Jen zkuste nalézt kanonický rozklad čísla $2^{2048} - 1$.

Proti tomu při prvním postupu určíme jen součin ab a nalezneme Euklidovým algoritmem hodnotu $\gcd(a,b)$. Pak tyto dvě hodnoty podělíme. Z výpočetního hlediska nejde o zvlášť náročné operace.

Z toho důvodu je třeba říci, že postup z Příkladu 1.41 je v praxi efektivnější.

1.4.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.1.3.

1. Nalezněte nejmenší společný násobek čísel 198 a 55.

2. Nalezněte nejmenší společný násobek čísel 198, 55 a 65.

3. Dokažte následující tvrzení. Nejmenším společným násobkem dvou navzájem nesoudělných přirozených čísel je součin těchto čísel.

Kapitola 2

Množina prvočísel

V této kapitole se budeme podrobněji věnovat množině prvočísel (viz Definice 1.25). Budeme ji označovat $\mathbb{P}$. Pokud nebude řečeno jinak, pak pod pojmem „číslo“ budeme rozumět **přirozené** číslo. Malými tiskacími písmeny, pokud nebude řečeno jinak, budeme v této kapitole označovat přirozená čísla. Pokud malé tiskací písmeno použijeme pro označení celého, nebo jiného čísla, bude to uvedeno.

Přirozeně vyvstávají otázky jako „Kolik je prvočísel?“ Ukážeme, že prvočísel je nekonečně mnoho. Přirozených čísel je také nekonečně mnoho. Můžeme říci, jak velkou část přirozených čísel tvoří prvočísla? V Kapitole 3 uvidíme, že z jistého úhlu pohledu tvoří jen zanedbatelnou část.

Dále bychom se mohli zajímat o rozložení prvočísel na číselné ose. Nejmenším prvočíslem je číslo 2. Následuje prvočíslo 3. Třetím prvočíslem je číslo 5 .... Dokážete najít sto třetí prvočíslo?

Bohužel neznáme žádný předpis, jak určit n-té prvočíslo. Pokusíme se alespoň o odhad počtu prvočísel menších, nebo rovných danému $n \in \mathbb{N}$.

Také rozhodnutí, zda dané číslo je prvočíslo, není u „velkých“ čísel nijak snadné. Kritéria prvočíselnosti sice existují, ale nejsou příliš vhodná pro praktické použití. To matematikům nedává spát a množina prvočísel je neustále intenzivně zkoumána.

2.1 Základní vlastnosti

Věta 2.1. (Euklidova prvočíselná) *Prvočísel je nekonečně mnoho.*

Důkaz. Důkaz provedeme sporem. Předpokládejme, že existuje jen konečně mnoho prvočísel a to čísla

$$p_1 < p_2 < \cdots < p_n.$$

Potom každé číslo větší než p_n musí být složené číslo, v jehož kanonickém rozkladu (viz Věta 1.29) se vyskytuje některé z prvočísel $p_1, p_2, \ldots, p_n$. To znamená, že každé číslo větší než p_n musí být dělitelné alespoň jedním z prvočísel $p_1, p_2, \ldots, p_n$. Vezměme třeba číslo $p_1 p_2 \cdots p_n + 1$. Zřejmě platí $p_1 p_2 \cdots p_n + 1 > p_n$. Proto musí existovat $p_i \in \{p_1, p_2, \ldots, p_n\}$ takové, že

$$p_1 p_2 \cdots p_n + 1 = p_i k,$$

kde $k \in \mathbb{N}$. Evidentně $\frac{p_1 p_2 \cdots p_n}{p_i} = m \in \mathbb{N}$. Proto

$$m p_i + 1 = p_i k,$$

$$1 = p_i (k - m). \tag{2.1}$$

Z (2.1) plyne, že $p_i \mid 1$. To je ale spor, neboť prvočíslo p_i je větší než 1. Předpoklad, že prvočísel je konečně mnoho, je tedy chybný. Musí jich proto být nekonečně mnoho. □

Dokázali jsme, že prvočísel je nekonečně mnoho. Teď se budeme zajímat o to, jak jsou rozložena na číselné ose. Nemůže být třeba každé páté přirozené číslo prvočíslem? Nesmysl! Číslo 5 je prvočíslo, ale $2 \cdot 5$, $3 \cdot 5$, $4 \cdot 5$ ... už evidentně prvočísla nejsou, neboť jde o čísla složená.

A co takhle čísla ve tvaru $5k + 2$, kde $k \in \mathbb{N} \cup \{0\}$? Bereme tedy na číselné ose zase každé páté číslo, ale začneme od čísla 2. Ze začátku to vypadá nadějně $5 \cdot 0 + 2 = 2$, což je prvočíslo, $5 \cdot 1 + 2 = 7$, což je zase prvočíslo! Ale už třetí pokus nás vyvede z omylu $5 \cdot 2 + 2 = 12$, a to prvočíslo není. Takže ne všechna přirozená čísla ve tvaru $5k + 2$ jsou prvočísla! Některá však ano, všimněme si:

$$2 = 5 \cdot 0 + 2$$

$$7 = 5 \cdot 1 + 2$$

$$17 = 5 \cdot 3 + 2$$

$$37 = 5 \cdot 7 + 2$$

$$\vdots$$

Můžeme se ptát, kolik prvočísel je v posloupnosti přirozených čísel ve tvaru $5k + 2$? Je jich nekonečně mnoho. Také prvočísel ve tvaru $5k + 3$ je nekonečně mnoho, i ve tvarech $6k + 1$, $134k + 5$, ... (všimněte si, $\gcd(5, 2) = 1$, $\gcd(5, 3) = 1$, $\gcd(6, 1) = 1$, $\gcd(134, 5) = 1$, ...). Obecně o tom pojednává věta z pera pana jménem Johann Peter Gustav Lejeune Dirichlet. Uvedeme ji bez důkazu.

Věta 2.2. (Dirichletova prvočíselná) *Nechť $a, b \in \mathbb{N}$, $\gcd(a, b) = 1$. Potom existuje nekonečně mnoho prvočísel p ve tvaru*

$$p = ak + b,$$

kde $k \in \mathbb{N}$. Navíc, řada převrácených hodnot těchto prvočísel diverguje. Tzn.

$$\sum_{\substack{p \in \mathbb{P} \\ p = ak+b}} \frac{1}{p} = \infty.$$

Poznámka 2.3. Požadavek $\gcd(a, b) = 1$ uvedený ve Větě 2.2 je důležitý! Pokud by $\gcd(a, b) = d > 1$, potom $a = dk_1$ a $b = dk_2$. Předpokládejme, že prvočíslo p můžeme psát ve tvaru $p = ak+b$, kde $k \in \mathbb{N}$. Po dosazení dostáváme $p = dk_1k+dk_2$ a odtud $p = d(k_1k + k_2)$. To by znamenalo, že $d \mid p$, přičemž $1 < d < p$. To je spor, neboť p je prvočíslo!

Můžeme proto říci, že **prvočíslo nikdy nemůže mít tvar $p = ak + b$, kde $a, b, k \in \mathbb{N}$,** $\gcd(a, b) > 1$.

Příklad 2.4. Pomocí předchozí Věty 2.2 a k ní se vztahující Poznámky 2.3 můžeme určit, jakou cifrou může končit zápis prvočísla v desítkové soustavě. Například obvyklý zápis $n = 524$ vlastně znamená, že $n = 5 \cdot 10^2 + 2 \cdot 10 + 4$, obdobně $2125 = 2 \cdot 10^3 + 1 \cdot 10^2 + 2 \cdot 10 + 5$. Obecně, používáme-li desítkovou soustavu, pak číslo zapsané pomocí cifer ve tvaru $a_n \ldots a_2a_1a_0$ je rovno $a_n10^n + \cdots + a_210^2 + a_110 + a_0$.

Vidíme, že číslo zapsané v desítkové soustavě má tvar

$$a_n10^n + \cdots + a_210^2 + a_110 + a_0 = 10 \underbrace{(a_n10^{n-1} + \cdots + a_210 + a_1)}_{k} + a_0 = 10k + a_0,$$

kde a_0 je poslední cifra v desítkovém zápisu a samozřejmě všechny cifry a_i patří do množiny $\{0, 1, \ldots, 9\}$.

Podle Věty 2.2 a Poznámky 2.3 může být číslo[1]

$$a_n \ldots a_2a_1a_0 = 10k + a_0, \text{ kde } k \geqq 1$$

prvočíslem pouze v případě, že čísla 10 a a_0 jsou navzájem nesoudělná, to jest, když $\gcd(10, a_0) = 1$. Platí to pouze pro $a_0 = 1$, $a_0 = 3$, $a_0 = 7$, nebo $a_0 = 9$.

To znamená, že číslo $n \geqq 10$, jehož poslední cifrou v desítkové soustavě je 1, 3, 7, nebo 9 může (ale nemusí!) být prvočíslo. Čísla $n \geqq 10$, končící na 0, 2, 4, 5, 6, nebo 8 nemohou být prvočísla.

Takže, bráno podle poslední cifry, například

- 24 nemůže být prvočíslo,

[1] Všimněte si, že uvažujeme nyní jen čísla větší, nebo rovná 10.

- $11, 13, 17$ mohou být prvočísla (a také jimi jsou)
- 27 může být prvočíslo (ale není, neboť $27 = 3 \cdot 9$)
- 135 nemůže být prvočíslo
- 109 může být prvočíslo (a také jím je)
- 121 může být prvočíslo (ale není, protože $121 = 11 \cdot 11$).

Jak uvidíme později (v Kapitole 3) vyloučili jsme tak „60% přirozených čísel“ z podezření, že jsou prvočísly.

Dokážete si rozmyslet, jak by to dopadlo, kdybychom obdobně použili zápis ve dvojkové soustavě (cifry jsou jen 0, nebo 1)? Správná odpověď je, že čísla ve tvaru $2k+1$, kde $k \in \mathbb{N}$ mohou (ale nemusí) být prvočísla a čísla ve tvaru $2k+0$, kde $k \in \mathbb{N} - \{1\}$ nemohou být prvočísla. Není to nijak zásadní zjištění. Jistě už jste slyšeli, nebo si sami rozmysleli, že kromě čísla 2 jsou všechna prvočísla lichá. Vyloučili jsme tak „jen 50% přirozených čísel.“

Obecný případ, kdy za základ číselné soustavy vezmeme číslo n vyřešíme ve Cvičení 6.1.1.

Dále ukážeme, že se prvočísla nevyskytují na číselné ose jako členy aritmetické posloupnosti. Věta 2.2 říká, že některá prvočísla určitě tvoří vybranou posloupnost aritmetické posloupnosti $\{ak + b\}_{k=1}^{\infty}$, kde $\gcd(a, b) = 1$. To jest, že mezi čísly ve tvaru $ak + b$, kde $\gcd(a, b) = 1$, je nekonečně mnoho prvočísel. Nicméně dokážeme, že ne všechny členy této posloupnosti jsou prvočísla - dokonce existuje nekonečně mnoho čísel ve tvaru $ak + b$, které nejsou prvočísly.

Věta 2.5. *Nechť $a, b \in \mathbb{N}$. Potom platí.*

1.) Jestliže $\gcd(a, b) = 1$, pak nekonečně mnoho členů aritmetické posloupnosti $\{ak + b\}_{k=1}^{\infty}$ patří do množiny prvočísel a nekonečně mnoho (jiných) členů aritmetické posloupnosti $\{ak + b\}_{k=1}^{\infty}$ nepatří do množiny prvočísel.

2.) Jestliže $\gcd(a, b) = d \geqq 2$, pak členy aritmetické posloupnosti $\{ak + b\}_{k=1}^{\infty}$ nepatří do množiny prvočísel.

Důkaz.

ad 1.) Jestliže $\gcd(a, b) = 1$, pak, podle Věty 2.2, existuje nekonečně mnoho členů aritmetické posloupnosti $\{ak + b\}_{k=1}^{\infty}$, které patří do množiny prvočísel. Ukážeme, že existuje také nekonečně mnoho prvků této posloupnosti, které prvočísly nejsou.

Nejprve uvažujme případ $b \geqq 2$. Potom pro $k = bn$, kde $n \in \mathbb{N}$, číslo $ak + b$ není prvočíslem, neboť v tom případě

$$ak + b = abn + b = b(an + 1).$$

Vidíme, že v případě kdy $k = bn$, je k-tý člen posloupnosti $\{ak + b\}_{k=1}^{\infty}$ číslem složeným. Nemůže proto být prvočíslem. Čísel k ve tvaru $k = bn$ je nekonečně mnoho, neboť za n si můžeme zvolit libovolné přirozené číslo. Proto také nekonečně mnoho členů posloupnosti $\{ak + b\}_{k=1}^{\infty}$ není prvočíslem.

Zbývá prověřit případ, kdy $b = 1$. Dokážeme, že nekonečně mnoho členů posloupnosti $\{ak + 1\}_{k=1}^{\infty}$ není prvočíslem.

Nejprve sporem dokážeme, že existují členy posloupnosti $\{ak+1\}_{k=1}^{\infty}$, které nejsou prvočíslem. Předpokládejme proto, že všechny prvky této posloupnosti jsou prvočísla. Vynásobíme-li

$$(ak_1 + 1)(ak_2 + 1),$$

obdržíme číslo složené (podle předpokladu jde o součin dvou prvočísel). Ale

$$(ak_1+1)(ak_2+1) = a^2k_1k_2+ak_1+ak_2+1 = a\underbrace{(ak_1k_2 + k_1 + k_2)}_{k\in\mathbb{N}}+1 = ak+1.$$

Vidíme, že číslo $(ak_1 + 1)(ak_2 + 1)$ je také členem posloupnosti $\{ak+1\}_{k=1}^{\infty}$, ale není prvočíslem! To je spor s předpokladem, že všechny členy této posloupnosti jsou prvočísla.

Znamená to, že musí existovat členy posloupnosti $\{ak+1\}_{k=1}^{\infty}$, které nejsou prvočísly. Možná je jich ale jen konečně mnoho, ne? Ne! A dokážeme to!

Opět sporem. Předpokládejme, že existuje jen konečně mnoho prvků posloupnosti $\{ak+1\}_{k=1}^{\infty}$, které nejsou prvočísly. Určitě existuje největší z nich[1]. Označme jej $s_{max} = ak_0 + 1$. Potom pro každé $k_1 \in \mathbb{N}$ platí

$$s_{max}(ak_1 + 1) = (ak_0 + 1)(ak_1 + 1) = a\underbrace{(ak_0k_1 + k_0 + k_1)}_{k\in\mathbb{N}}+1 = ak + 1.$$

Můžeme proto tvrdit, že číslo $s_{max}(ak + 1)$ je také prvkem posloupnosti $\{ak + 1\}_{k=1}^{\infty}$ a je evidentně číslem složeným, neboť $s_{max} = ak_0 + 1 \geqq 2$ a také $ak + 1 \geqq 2$ (viz Definice 1.26). Navíc

$$ak + 1 = s_{max}(ak_1 + 1) \geqq s_{max}\cdot 2 > s_{max}.$$

To je ovšem spor s předpokladem, že největším složeným číslem, které je prvkem posloupnosti $\{ak + 1\}_{k=1}^{\infty}$ je číslo s_{max}.

ad 2.) Jestliže $\gcd(a, b) = d \geqq 2$, pak členy aritmetické posloupnosti $\{ak + b\}_{k=1}^{\infty}$ nepatří do množiny prvočísel. Tuto skutečnost jsme dokázali v Poznámce 2.3.

[1] Konečná množina přirozených čísel má maximum.

□

Při hledání pravidelnosti ve výskytu prvočísel jsme zatím nebyli úspěšní. A nyní dokážeme výsledek, který také ukazuje na jistou nepravidelnost ve výskytu prvočísel. Máme na mysli nepravidelnost v tom smyslu, že se prvočísla na číselné ose nevyskytují ani přibližně v konstantních „rozestupech.“

Zamysleme se, jak velká „mezera“ může být mezi dvěma po sobě jdoucími prvočísly. Třeba rozdíl – „vzdálenost“ – mezi 5 a 7 je $7-5=2$. Rozdíl mezi 13 a 17 je $17-13=4$, atp. Může být rozdíl mezi po sobě jdoucími prvočísly libovolně velký? Ukážeme, že ano.

Věta 2.6. *Nechť $p_1 < p_2 < \dots$ je posloupnost všech prvočísel. Pro každé $n \in \mathbb{N}$ existují prvočísla p_k a p_{k+1} takové, že*

$$p_{k+1} - p_k \geqq n.$$

Důkaz. Uvažujme libovolné pevně zvolené přirozené číslo n a číslo $m=(n+1)!+1$. Protože

$$(n+1)! = 1\cdot 2\cdot \dots \cdot n\cdot (n+1),$$

je číslo $(n+1)!$ dělitelné čísly $2, 3, \dots, n, n+1$. A tak

$$m+1 = (n+1)!+1+1 = (n+1)!+2 = 2\Big(\underbrace{\frac{(n+1)!}{2}+1}_{=k_1\in\mathbb{N}}\Big) = 2k_1, \text{ kde } k_1 > 1.$$

Potom $m+1$ je číslo složené a nemůže být prvočíslem. Obdobně

$$m+2 = (n+1)!+3 = 3\Big(\underbrace{\frac{(n+1)!}{3}+1}_{k_2\in\mathbb{N}}\Big) = 3k_2, \text{ kde } k_2 > 1.$$

$$m+3 = (n+1)!+4 = 4\Big(\underbrace{\frac{(n+1)!}{3}+1}_{k_3\in\mathbb{N}}\Big) = 4k_3, \text{ kde } k_3 > 1.$$

$$\vdots$$

$$m+n = (n+1)!+n+1 = (n+1)\Big(\underbrace{\frac{(n+1)!}{n+1}+1}_{k_n\in\mathbb{N}}\Big) = (n+1)k_n, \text{ kde } k_n > 1.$$

Tím jsme dokázali, že čísla $m+1, m+2, \dots, m+n$ jsou čísla složená. A tak ani jedno z nich nemůže být prvočíslo.

Nyní již stačí jen najít vhodné p_k a p_{k+1}. Označme p_k největší z prvočísel, která jsou menší, nebo rovna m (takové určitě existují, neboť $m \geqq 3$). Tzn.

$$p_k = \max\{p \in \mathbb{P} \mid p \leqq m\}.$$

Znamená to, že mezi p_k a m nejsou žádná prvočísla (pokud m je prvočíslo, pak $m = p_k$). Dále víme, že $m + 1$, $m + 2$, ..., $m + n$ také nejsou prvočísla. Proto prvočíslo p_{k+1} následující po p_k musí být větší, než $m + n$. Dostáváme tak nerovnosti

$$p_k \leqq m \quad \text{a} \quad p_{k+1} \geqq m + n.$$

Odtud $p_{k+1} - p_k \geqq n$.

□

Nakonec uvedeme větu sice méně obecnou, než je Dirichletova prvočíselná věta, ale na rozdíl od od ní ji dokážeme. Konkrétně dokážeme, že řada převrácených hodnot prvočísel diverguje.

Věta 2.7. *Nechť $\{p_i\}_{i=1}^{\infty}$, je posloupnost všech prvočísel. Potom*

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty.$$

Důkaz. Důkaz provedeme sporem. Předpokládejme, že řada $\sum_{i=1}^{\infty} \frac{1}{p_i}$ konverguje. Prolistujete-li nějakou slušnější učebnici matematické analýzy, najdete tam informaci, že v takovém případě musí existovat libovolně malý (zvolme si třeba menší než $\frac{1}{2}$) zbytek této řady[1]. Jinak řečeno, musí existovat nějaké k takové, že

$$\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}. \tag{2.2}$$

Označme $P = p_1 p_2 \dots p_k$ a uvažujme čísla ve tvaru

$$k_n = 1 + nP = 1 + np_1 p_2 \dots p_k.$$

Ať zvolíme jakékoli n, nemůže být číslo k_n dělitelné ani jedním z prvočísel p_1, p_2, ..., p_k. Předpoklad, že nějaké p_i dělí k_n by, stejně jako v důkazu Euklidovy prvočíselné Věty 2.1, vedl ke sporu - k nepravdivému tvrzení, že p_i dělí jedničku. Proto můžeme tvrdit, že všichni prvočíselní dělitelé čísel ve tvaru $1 + nP$ jsou mezi prvočísly p_{k+1}, p_{k+2}, ...

Nyní zvolněme tempo a pro dobré pochopení věcí následujících prostudujme následující poznámku. Poté budeme pokračovat v důkazu Věty 2.7.

[1] Zbytek řady znamená, že nesčítáme všechny členy řady, ale prvních k členů vynecháme. Takže zbytkem řady $\sum_{i=1}^{\infty} \frac{1}{p_i}$ je řada $\sum_{i=k+1}^{\infty} \frac{1}{p_i}$.

Poznámka 2.8. Stejně jako v předcházejícím důkazu Věty 2.7 označme $k_n = 1 + nP = 1 + np_1p_2 \dots p_k$. Zjistili jsme, že všichni prvočíselní dělitelé čísel ve tvaru $1 + nP$ jsou mezi prvočísly p_{k+1}, p_{k+2}, ... Uvažujme dvě sumy

$$\sum_{n=1}^{r} \frac{1}{1+nP} \text{ a } \sum_{m=1}^{\infty} \left(\sum_{i=k+1}^{\infty} \frac{1}{p_i} \right)^m . \tag{2.3}$$

Jaký je mezi nimi vztah? Tvrdím, že libovolné číslo $\frac{1}{1+nP}$ je možné najít mezi sčítanci součtu $\sum_{m=1}^{\infty} \left(\sum_{i=k+1}^{\infty} \frac{1}{p_i} \right)^m$.

Ukažme si na příkladě. Pokud by platilo $k = 3$, potom $k_n = 1 + nP = 1 + np_1p_2p_3 = 1 + n2{\cdot}3{\cdot}5 = 1 + n30$. Zvolme si nějaké n, třeba $n = 3$. Potom

$$\frac{1}{1+nP} = \frac{1}{1+3{\cdot}30} = \frac{1}{91} = \frac{1}{7{\cdot}13}.$$

Vidíme, že všichni prvočíselní dělitelé čísla $k_3 = 91 = 7{\cdot}13$ jsou opravdu mezi prvočísly $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, ... Najdeme číslo $\frac{1}{1+nP} = \frac{1}{7\,13}$ mezi sčítanci součtu

$$\sum_{m=1}^{\infty} \left(\sum_{i=4}^{\infty} \frac{1}{p_i} \right)^m ? \tag{2.4}$$

Ale ano, uvažujme případ $m = 2$. Potom

$$\begin{aligned}
\left(\sum_{i=4}^{\infty} \frac{1}{p_i} \right)^2 &= \left(\frac{1}{7} + \frac{1}{11} + \frac{1}{13} \dots \right)^2 > \\
&> \left(\frac{1}{7} + \frac{1}{11} + \frac{1}{13} \right)^2 = \\
&= \left(\frac{1}{7} + \frac{1}{11} + \frac{1}{13} \right) \left(\frac{1}{7} + \frac{1}{11} + \frac{1}{13} \right) = \\
&= \frac{1}{7{\cdot}7} + \frac{1}{7{\cdot}11} + \frac{\mathbf{1}}{\mathbf{7{\cdot}13}} + \\
&+ \frac{1}{11{\cdot}7} + \frac{1}{11{\cdot}11} + \frac{1}{11{\cdot}13} + \frac{1}{13{\cdot}7} + \frac{1}{13{\cdot}11} + \frac{1}{13{\cdot}13}.
\end{aligned}$$

Obecně v případě $k_n = p_{i_1}^{\alpha_1} p_{i_2}^{\alpha_2} \cdots p_{i_k}^{\alpha_k}$ zvolíme $m = \sum_{j=1}^{k} \alpha_k$. Potom číslo $\frac{1}{k_n}$ je jistě jedním ze sčítanců součtu, který dostaneme po umocnění výrazu

$$\left(\sum_{i=k+1}^{K} \frac{1}{p_i} \right)^{\sum_{j=1}^{k} \alpha_k},$$

kde K zvolíme tak, aby $K \geqq \max\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$.

Nyní můžeme pokračovat v důkazu Věty 2.7. Z výše uvedené Poznámky 2.8 je zřejmé, že každý ze zlomků $\frac{1}{1+nP}$ se vyskytuje v součtu $\sum\limits_{m=1}^{\infty}\left(\sum\limits_{i=k+1}^{\infty}\frac{1}{p_i}\right)^m$. Proto pro každé $r \in \mathbb{N}$ platí

$$\sum_{n=1}^{r}\frac{1}{1+nP} \leqq \sum_{m=1}^{\infty}\left(\sum_{i=k+1}^{\infty}\frac{1}{p_i}\right)^m. \tag{2.5}$$

S využitím (2.2) dostáváme

$$\sum_{n=1}^{r}\frac{1}{1+nP} \leqq \sum_{m=1}^{\infty}\left(\frac{1}{2}\right)^m. \tag{2.6}$$

Protože $\sum\limits_{m=1}^{\infty}\left(\frac{1}{2}\right)^m$ je součet geometrické řady s prvním členem $\frac{1}{2}$ a kvocientem $\frac{1}{2}$, platí

$$\sum_{n=1}^{r}\frac{1}{1+nP} \leqq \frac{1}{2}\frac{1}{1-\frac{1}{2}} = 1. \tag{2.7}$$

Nerovnost (2.7) platí pro libovolné $r \in \mathbb{N}$. Proto docházíme k závěru, že

$$\sum_{n=1}^{\infty}\frac{1}{1+nP} \leqq 1. \tag{2.8}$$

To je ovšem spor! Dokážeme, že řada $\sum\limits_{n=1}^{\infty}\frac{1}{1+nP}$ je divergentní. Stačí si uvědomit platnost následujících nerovností

$$\sum_{n=1}^{\infty}\frac{1}{1+nP} \geqq \sum_{n=1}^{\infty}\frac{1}{n+nP} = \sum_{n=1}^{\infty}\frac{1}{1+P}\cdot\frac{1}{n} = \frac{1}{1+P}\sum_{n=1}^{\infty}\frac{1}{n} = \infty. \tag{2.9}$$

Poslední rovnost v (2.9) plyne z divergence řady $\sum\limits_{n=1}^{\infty}\frac{1}{n}$ (což snadno ověříme pomocí integrálního kritéria divergence řady).

□

2.1.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.2.1.

1. Nechť $\{p_n\}_{n=1}^{\infty}$ je rostoucí posloupnost všech prvočísel. Dokažte, že pro každé $n \in \mathbb{N}$ platí: $p_n > n$.

2.2 Eratosthenovo síto

Již dlouhá léta se lidé snaží najít nějaký způsob, jak snadno a rychle rozhodnout, zda dané číslo je, či není prvočíslo. U „malých“ čísel to není tak velký problém. Zjišťujeme například, zda číslo 29 je prvočíslo. Evidentně stačí uvažovat následovně. Je číslo 29 násobkem dvojky? Není! Je násobkem trojky? Není! Je násobkem čtyřky? Není! A tak dále, až dojdeme k tomu, že číslo 29 není, kromě jedničky, násobkem žádného čísla menšího než 29. Proto nemůže jít o číslo složené. Číslo 29 je proto určitě prvočíslo.

Výše uvedený postup můžeme ještě poněkud zjednodušit. Nemusíme projít všechna čísla od dvojky po 28. Stačí projít přirozená čísla od 2 do $\sqrt{29}$. Jak to? Ale to je jednoduché! Předpokládejme na chvíli, že číslo 29 je složené. Existovaly by tak čísla $k_1, k_2 > 1$ splňující rovnost $29 = k_1 k_2$ Může mít číslo 29 *všechny* své dělitele větší než $\sqrt{29}$? Pokud ano, pak by platilo

$$29 = k_1 k_2 > \sqrt{29}\sqrt{29} = 29.$$

To je ovšem spor, neboť nemůže platit $29 > 29$. A co jsme tím zjistili? No, pokud číslo 29 nějaké dělitele má, pak alespoň jeden z nich musí být menší, nebo roven $\sqrt{29}$.

V našem případě proto stačilo zjistit, zda číslo 29 je násobek nějakého přirozeného čísla, které leží mezi číslem 2 a $\sqrt{29} \doteq 5,4$. Takže, je 29 násobek dvojky? Ne! Je násobkem trojky? Není! Je násobkem čtyřky? Není! Je násobkem pětky? Ne! Už z toho můžeme dojít k závěru, že 29 je prvočíslo.

Svoje pozorování formulujeme následovně.

Lemma 2.9. *Jestliže $k = k_1 k_2$, pak $k_1 \leqq \sqrt{k}$, nebo $k_2 \leqq \sqrt{k}$.*

Důkaz. Důkaz provedeme sporem. Předpokládejme, že $k = k_1 k_2$ a zároveň $k_1 > \sqrt{k}$ a $k_2 > \sqrt{k}$. Potom platí

$$k = k_1 k_2 > \sqrt{k}\sqrt{k} = k.$$

A to není pravda! Jistě neplatí $k > k$. Proto je chybný náš předpoklad. Číslo k jistě můžeme napsat ve tvaru $k = k_1 k_2$. A tak musí být nepravdivý předpoklad, že $k_1 > \sqrt{k}$ a také $k_2 > \sqrt{k}$. Pravdivá je jeho negace, $k_1 \leqq \sqrt{k}$, nebo $k_2 \leqq \sqrt{k}$. □

Postup můžeme ještě poněkud zjednodušit. Předpokládejme, že číslo k má kanonický rozklad

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

kde $\alpha_1, \alpha_2 \cdots \alpha_n \in \mathbb{N}$

Mohou být všechna prvočísla v kanonickém rozkladu čísla k větší než $\sqrt{k}$? Můžeme to na chvíli předpokládat a uvidíme, že v případě, kdy k je složené číslo, dojdeme ke sporu.

Tak hurá do toho! Pokud k je složené číslo, jsou dvě možnosti

- $n > 1$, to jest, existují alespoň dvě různá prvočísla p_1 a p_2 která dělí číslo k.

  V tom případě

  $$k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \geqq p_1 p_2 > \sqrt{k}\sqrt{k} = k.$$

  To je spor! Není pravda, že $k > k$. Proto v tomto případě musí být nepravdivý náš předpoklad.

- $n = 1$, to jest, existuje jen jedno prvočíslo p_1 které dělí číslo k.

  V tom případě $k = p_1^{\alpha_1}$. Aby k bylo skutečně číslo složené, musí být $\alpha_1 \geqq 2$. Potom

  $$k = p_1^{\alpha_1} \geqq p_1^2 > (\sqrt{k})^2 = k.$$

  To je spor! Není pravda, že $k > k$. Proto také v tomto případě musí být nepravdivý předpoklad.

Tím jsme dokázali následující tvrzení

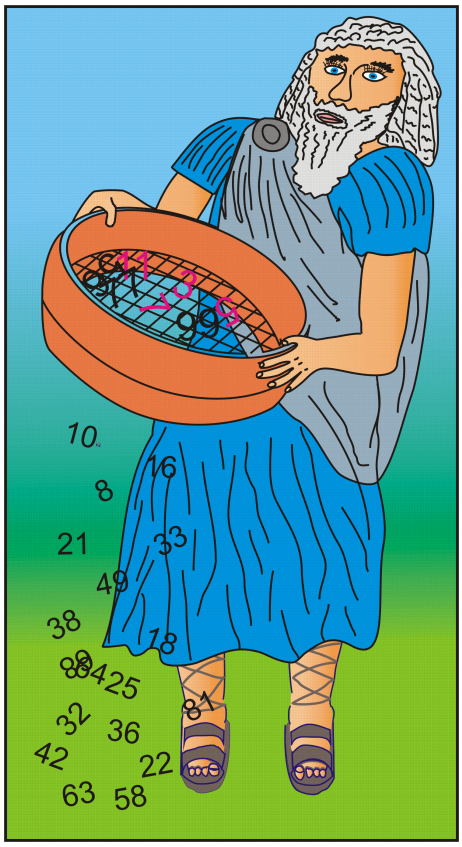
Lemma 2.10. *Nechť k je číslo složené. Potom existuje prvočíslo p, $p \leqq \sqrt{k}$, které je dělitelem čísla k.*

Vraťme se k našemu příkladu, kdy jsme zjišťovali, zda je číslo 29 prvočíslo. Pokud by to bylo číslo složené, muselo by být podle Lemmatu 2.10 dělitelné nějakým prvočíslem z intervalu $\langle 2, \sqrt{29}\rangle$. Jedná se o prvočísla 2, 3 a 5. Číslo 29 není násobkem ani jednoho z nich. Proto není číslem složeným, ale je prvočíslem. Tento postup je proti předchozímu jednodušší v tom, že jsme nemuseli kontrolovat, zda je 29 násobkem čísla 4.

V dalších úvahách využijeme následující triviální důsledek Lemmatu 2.10.

Důsledek 2.11. *Nechť k je číslo složené. Potom existuje prvočíslo p, $p < k$, které je dělitelem čísla k. To jest, každé složené číslo k je násobkem nějakého prvočísla p, které je menší, než k.*

A nyní se vraťme k samotnému nadpisu podkapitoly. Copak že to pan Eratosthenes prosíval ve svém sítu? Inu vzal si hromadu přirozených čísel a prosil z nich všechna čísla složená. Co mu v sítu zbylo? Nu? Ano správně, prvočísla! A jakpak to dělal? Pokusme se zrekonstruovat jeho myšlenkové pochody v den, kdy nutně potřeboval najít všechna prvočísla mezi jedničkou a stovkou. S trochou fantazie to mohlo býti nějak takto. Ten den jej postihl velký záchvat lenosti a nechtělo se mu kontrolovat jedno číslo po druhém. Pídil se proto po jednodušším způsobu hledání prvočísel!



Obr. 2.1 Eratosthenovo síto na prvočísla

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Obr. 2.2 Eratosthenovo síto na prvočísla - dvojka v podezření!

Nejprve si všechna čísla seřadil do tabulky. Čísla podezřelá z toho, že jsou prvočísla napsal modře. Jen o jedničce věděl, že to není prvočíslo. Proto je napsána černě (viz obrázek 2.2). A co dál? Následuje dvojka. Značně podezřelé číslo!

A opravdu, dvojka je prvočíslo, neboť je dělitelná jen jedničkou a sama sebou. Obarvíme ji na červeno! Všechny ostatní násobky dvojky jsou ale jistě čísla složená. Můžeme je proto z tabulky vyškrtnout, či obarvit je na černo. Jak je komu libo, my zde budeme přebarvovat.

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Obr. 2.3 Eratosthenovo síto na prvočísla - dvojka odhalena jako prvočíslo a její násobky vyškrtnuty!

Pak se podívejme na nejmenší modré číslo. Je jím číslo 3 (viz obrázek 2.3). Může jít o složené číslo? Kdepak, podle Důsledku 2.11 by musela být nějakým násobkem prvočísla, které je od něj menší - to by ovšem byla násobkem dvojky a tudíž by už byla černá, ne modrá! Takže trojka je prvočíslo a z tabulky můžeme vyškrtnout všechny její násobky (obarvíme na černo - obrázek 2.4).

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Obr. 2.4 Eratosthenovo síto na prvočísla - trojka odhalena jako prvočíslo a její násobky vyškrtnuty!

A tak pokračujeme stále dál. Jak? No v tuto chvíli je nejmenší modré číslo číslo 5. Kdyby to bylo číslo složené, muselo by být násobkem dvojky, nebo trojky.

Ale není jím, protože je zatím modré! Takže číslo 5 je prvočíslo. Obarvíme jej na červeno a vyškrtneme všechny násobky čísla 5 (obrázek 2.5).

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Obr. 2.5 Eratosthenovo síto na prvočísla - pětka odhalena jako prvočíslo a její násobky vyškrtnuty!

Obdobně dopadneme prvočíslo 7 a vyškrtneme jeho násobky (obrázek 2.6). Ppřesněji jen tři jeho násobky, a to čísla 49, 77 a 91, neboť ostatní byly vyškrtnuty už dříve.

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Obr. 2.6 Eratosthenovo síto na prvočísla - sedmička odhalena jako prvočíslo a její násobky vyškrtnuty!

V následujícím kroku Eratosthenes objevil, že číslo 11 je prvočíslem. Ale co to? Když se jal vyškrtávat z tabulky násobky čísla 11 (čísla 22, 33, 44, 55, 66, 77, 88 a 99), zjistil, že už jsou všechny pryč (jsou černé už na obrázku 2.6).

I hluboce se zamyslel. Jak se stalo, že nebylo co vyškrtnout? Po chvíli se blaženě usmál a zbývající modré čísla přebarvil na červeno.

Proč to udělal? Uvažoval asi nějak takhle. Které násobky čísla 11 by v tabulce byly ještě modré, kdyby tam tedy ještě nějaké byly? Určitě ne ty násobky

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Obr. 2.7 Eratosthenovo síto na prvočísla - jedenáctka odhalena jako prvočíslo a její násobky vyškrtnuty!

	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Obr. 2.8 Eratosthenovo síto na prvočísla - prvočísla menší, než 100

jedenáctky, které jsou také násobky některých prvočísel menších, než je sama jedenáctka (ty už přece obarvil na černo!). V modré barvě je proto nějaké číslo, které je násobkem jedenáctky a také nějakého prvočísla, které je větší, nebo rovno 11. Takže nejmenší násobek jedenáctky, který by ještě mohl být v modrý je číslo 11·11, ale to je číslo 121. A to už v tabulce nemáme! Proto už nebylo co vyškrtnout!

Ale to je přece báječné. Nebylo co vyškrtnout, protože číslo 11·11 přesáhlo číslo 99. No a? Co je na tom báječného? Tak podívejte. Jaké bude další prvočíslo? Kouknem do tabulky (obrázek 2.7). Nejmenší číslo v modrém je číslo 13. Je to proto prvočíslo. Které násobky čísla 13 ještě nejsou vyškrtnuty? Obdobná úvaha jako u jedenáctky. Nejmenší z nich je číslo 13·13. Ale když 11·11 bylo větší, než 99, pak 13·13 jistě také!

A stejně tomu musí být u dalších prvočísel, které se ještě v tabulce skrývají! Nebude již co vyškrtávat! Takže všechny zbývající modré čísla se přebarví na červeno. A jsme hotovi (obrázek 2.8)!

Nakonec poznamenejme, že Eratosthenovo síto je algoritmus poměrně efektivní pro hledání „malých“ prvočísel, řádově do 10 000 000. Složitost tohoto algoritmu je $O(N \log\log N)$, kde N je horní mez rozsahu „prosívaných“ čísel. Pro identifikaci větších prvočísel existují jiné testy prvočíselnosti. Některé jsou pravděpodobnostní, fungují tak, že určují pravděpodobnost s jakou je zkoumané číslo prvočíslo, jiné jsou deterministické. Ty s jistotou (pokud něco jako jistota existuje) určují, zda je zkoumané číslo prvočíslo. Velkým hitem je například AKS test, jehož matematické základy položili v roce 2002 M.Agrawal, N.Kayal a N.Saxena. Dosáhli složitosti $O(\log^{12} n)$, kde n je testované číslo. Algoritmus AKS byl poté ještě vylepšován a v roce 2005 C. Pomerance a H.W. Lenstra Jr, dosáhli složitosti $O(\log^6 n)$. To už je ale jiná kapitola ....

2.3 Prvočíselná funkce a prvočíselná věta

Zjistili jsme, že prvočísel je nekonečně mnoho. Kolik jich však může být v konečné podmnožině přirozených čísel? Nebo si položme otázku, kolik je prvočísel menších, nebo rovných deseti, dvaceti, nebo obecně nějakému číslu x? Počet čísel menších, nebo rovných danému číslu x se obvykle označuje $\pi(x)$. Například počet prvočísel menších než 10 je $\pi(10) = 4$, neboť jen čtyři prvočísla jsou menší, nebo rovny 10. Jsou to čísla 2, 3, 5 a 7.

Každému reálnému číslu x tak můžeme jednoznačně přiřadit hodnotu $\pi(x)$.

Definice 2.12. (*Prvočíselná funkce*) Funkci $\pi : \mathbb{R} \to \mathbb{N} \cup \{0\}$, danou pro každé $x \in \mathbb{R}$ předpisem

$$\pi(x) = \#\{p \in \mathbb{P} \mid p \leqq x\},$$

nazýváme prvočíselnou funkcí.[a]

[a] Vidíme, že $\pi(x)$ rovná se počtu prvočísel menších, nebo rovných x. Symbol $\#A$ označuje počet prvků množiny A. Viz zavedené označení $\#A$ v odstavci 0.2.

Bohužel nemáme k dispozici žádný předpis, do kterého by stačilo dosadit číslo x a výsledkem by byla hodnota $\pi(x)$ (alespoň pro všechna $x \geqq 2$ ne). Dokážeme ale chování této funkce alespoň přibližně odhadnout (viz podkapitola 2.4 a Lemma 2.13), případně známe chování funkce $\pi(x)$ při $x \to \infty$ (viz Věta 2.14).

Poznamenejme, že funkční hodnoty funkce π na množině $\langle 1, \infty)$ jsou určeny jejími funkčními hodnotami na množině $\mathbb{N}$, neboť $\forall x \in \mathbb{R}$, $x \in \langle n, n+1)$, kde $n \in \mathbb{N}$, platí $\pi(x) = \pi(n)$.

Lemma 2.13. *Pro každé $n \in \mathbb{N}$ platí*

$$\pi(n) \geqq \frac{\ln n}{2 \ln 2}.$$

Důkaz. Jestliže $n = 1$, pak podle Definice 2.12 je $\pi(n) = \pi(1) = 0$. A evidentně platí $0 \geqq \frac{\ln 1}{2 \ln 2} = 0$.

Nyní uvažujme případ $n \geqq 2$. Označme $p_1 < p_2 < \dots$ rostoucí posloupnost všech prvočísel. Protože $n \geqq 2$, musí existovat nějaká prvočísla, která jsou menší, nebo rovna číslu n. Která to jsou a kolik jich je? Podle Definice 2.12 jich je právě $\pi(n)$, takže to musí být prvočísla $p_1, p_2, \dots, p_{\pi(n)}$.

Dále uvažujme libovolné m takové, že $1 \leqq m \leqq n$. Takových čísel m je přesně n. My však jejich počet (z prozatím záhadných důvodů) pouze značně nepřesně odhadneme. Podle Lemmata 1.38 pro číslo m existují $a, b \in \mathbb{N}$ takové, že $m = a^2 b$ a číslo b ve svém kanonickém rozkladu obsahuje prvočísla pouze s mocninou rovnou jedné, nebo nule. Je jasné, že tato prvočísla musí být menší, nebo rovna n (jinak by muselo platit $m \leqq n < a^2 b = m$, což je nesmysl). Takže

$$b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{\pi(n)}^{\alpha_{\pi(n)}}, \tag{2.10}$$

kde $\alpha_1, \alpha_2, \dots, \alpha_{\pi(n)} \in \{0, 1\}$. Jednoduchou kombinatorickou úvahou[1] dospějeme k tomu, že čísel b ve tvaru (2.10) je celkem $2^{\pi(n)}$.

Nyní odhadneme, kolik různých čísel a může maximálně existovat takových, aby byly splněny předpoklady $1 \leqq m \leqq n$, $m = a^2 b$. Z rovnosti $m = a^2 b$ plyne $m \geqq a^2$ Odtud $\sqrt{m} \geqq a$. A protože $n \geqq m$, platí $\sqrt{n} \geqq \sqrt{m}$. A tak

$$\sqrt{n} \geqq a. \tag{2.11}$$

Přirozených čísel a splňujících (2.11) je celkem $[\sqrt{n}]$. Takže čísel a, splňujících $m = a^2 b$, $1 \leqq m \leqq n$, je nejvýše $\sqrt{n}$. Podle předchozího máme nejvýše $2^{\pi(n)}$ možností pro hodnotu čísla b. Proto číslo $m = a^2 b$ nemůže nabývat více než $\sqrt{n} \cdot 2^{\pi(n)}$ hodnot. Ale my víme, kolika hodnot může nabýt číslo m a to z nerovnosti $1 \leqq m \leqq n$. Je jich celkem n. Dostáváme tak nerovnost

$$n \leqq \sqrt{n} \cdot 2^{\pi(n)}.$$

Odtud

$$\begin{aligned}
\sqrt{n} &\leqq 2^{\pi(n)}, \\
\ln \sqrt{n} &\leqq \ln 2^{\pi(n)}, \\
\ln n^{\frac{1}{2}} &\leqq \pi(n) \ln 2, \\
\frac{1}{2} \ln n &\leqq \pi(n) \ln 2, \\
\pi(n) &\geqq \frac{1}{2} \frac{\ln n}{\ln 2}.
\end{aligned}$$

□

[1] Máme celkem $\pi(n)$ pozic (exponentů) a na každé z nich může být číslo (exponent) 0, nebo 1. Jedná se o variace $\pi(n)$-té třídy ze 2 prvků. Těch je $2^{\pi(n)}$.

Lemma 2.13 poskytuje dolní odhad hodnoty $\pi(n)$. Například

$$\pi(500) \geqq \frac{\ln 500}{2 \ln 2} \doteq 4,48.$$

Můžeme proto tvrdit, že prvočísel menších než 500 je nejméně 5. Jak vidno, jde ve své nepřesnosti o dost ubohý odhad. Nicméně nám může sloužit k elegantnímu důkazu Euklidovy prvočíselné věty (Věta 2.1):

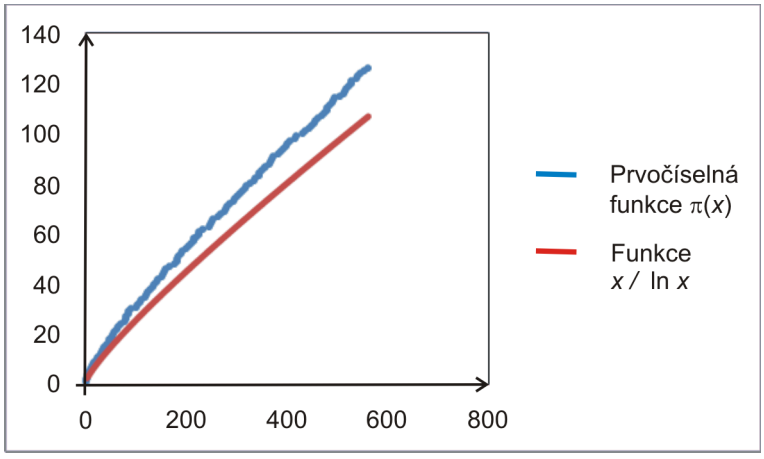
$$\pi(n) \geqq \frac{\ln n}{2 \ln 2} \tag{2.12}$$

Víme, že $\lim_{n\to\infty} \frac{\ln n}{2 \ln 2} = \infty$. Z nerovnosti (2.12) pak plyne $\lim_{n\to\infty} \pi(n) = \infty$. To ovšem znamená, že prvočísel je nekonečně mnoho.

Významným výsledkem v teorii čísel je takzvaná *prvočíselná věta*. Popisuje chování funkce $\pi(x)$ při $x \to \infty$. Prvočíselná věta je velice užitečná pro odvozování dalších teoretických výsledků. Také nám umožňuje odhadnout hodnotu $\pi(x)$ v případě, že x je „velké“ kladné číslo. V takovém případě je počet prvočísel nepřesahujících dané $x \in \mathbb{R}$ „srovnatelný“ s číslem $\frac{x}{\ln x}$. Důkaz prvočíselné věty zde pro jeho náročnost nebudeme provádět.

Věta 2.14. (Prvočíselná věta) *Platí rovnost*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$



Obr. 2.9 Porovnání hodnot funkce $\pi(x)$ a $\frac{x}{\ln x}$. Prvočíselná věta říká, že jejich poměr se blíží k jedné.

Poznámka 2.15. Pokud funkce f a g splňují podmínku

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

pak tuto skutečnost symbolicky zapisujeme $f(x) \sim g(x)$. V duchu této symboliky můžeme podle Věty 2.14 psát

$$\pi(x) \sim \frac{x}{\ln x}.$$

Ale pozor! Tento zápis není možné interpretovat tak, že pro „velká“ x jsou hodnoty $\pi(x)$ a $\frac{x}{\ln x}$ „téměř“ stejné. Informuje nás pouze o tom, že jejich poměr se blíží jedné. To není totéž? Ne, není! Ukažme si na jednoduchém příkladě. Uvažme, že

$$\lim_{x\to\infty} \frac{x^2+x}{x^2} = 1.$$

To znamená, že $x^2 + x \sim x^2$. Ale všimněme si, že $x^2 + x$ a x^2 se liší právě o x. Takže při $x \to \infty$ se rozdíl hodnot $x^2 + x$ a x^2 blíží nekonečnu! Nicméně v jistém úhlu pohledu můžeme říci, že vzhledem k velikosti hodnot $x^2 + x$ a x^2 je jejich rozdíl „zanedbatelný.“

Při studiu prvočísel je jedním ze základních cílů našeho zkoumání umožnit jejich identifikaci mezi ostatními přirozenými čísly. Představme si, že máme najít všechna prvočísla menší než 100 000. Dokázali byste si s takovým problémem poradit?

Asi by to nebylo zrovna jednoduché a určitě byste uvítali pomocnou ruku ve formě informace, kolik takových prvočísel přibližně je. S pomocí prvočíselné věty odhadneme, že prvočísel menších než 100 000 je něco kolem 8 686.[1]

To nám ale ke štěstí nemůže stačit. Jde jen o poměrně mlhavou informaci. Určitě by byl užitečný odhad, kolik je hledaných prvočísel nejméně a kolik nejvýše. Určitým návodem, jak k němu dojít, jsou Čebyševovy nerovnosti o kterých pojednává podkapitola 2.4. Ale, jak uvidíme, ani ty nejsou pro hledání „velkých“ prvočísel příliš efektivní.

2.3.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.2.2.

1. Odhadněte, kolik prvočísel je menších, nebo rovných číslu $n = 1\,000$, $n = 10\,000$, $n = 1\,000\,000$.

2. Odhadněte, kolik procent čísel menších, nebo rovných číslu $n = 1\,000$, $n = 10\,000$, $n = 1\,000\,000$ tvoří prvočísla.

3. Dokažte, že pro každé $x \in \mathbb{R}$, $x \geqq 2$ platí $\pi(x) \leqq x - 1$.

[1] Neboť $\frac{100\,000}{\ln 100\,000} \doteq 8\,686$

2.4 Čebyševovy nerovnosti

V předchozím textu jsme se seznámili s prvočíselnou větou. Ta říká, že srovnáme-li hodnoty prvočíselné funkce s hodnotami funkce $f(x) = \frac{x}{\ln x}$, pak se při $x \to \infty$ tyto dvě čísla sobě blíží. Zmíněné pozorování provedli již pan Johann Carl Friedrich Gauss a Adrien-Marie Legendre, když studovali tabulku hodnot těchto funkcí pro $x \leqq 10^6$. Pravdivost prvočíselné věty však neuměli dokázat.

V roce 1851 pan Pafnutij Lvovič Čebyšev odvodil odhady prvočíselné funkce, nerovnosti svírající funkci $\pi(x)$ shora i zdola. Jednalo se o odhady poněkud přesnější, než jaké v této podkapitole budeme vydávat za Čebyševovy nerovnosti a jejich důkaz je o to náročnější. Díky tomu však byl schopen dokázat, že $\lim\limits_{n\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$, za předpokladu, že tato limita existuje. Její existenci se mu však dokázat nepodařilo.

Důkaz prvočíselné věty si tak na pažby svých pušek mohli vyrýt až v roce 1896 pánové Jacques Salomon Hadamard a Charles-Jean Étienne Gustave Nicolas de la Vallée Poussin (nezávisle na sobě). Využili k tomu dřívějších prací pana George Friedricha Bernharda Riemanna, které spojovaly teorii čísel s komplexní analýzou.

Důkaz prvočíselné věty založený čistě na technikách a výsledcích z oblasti teorie čísel (poněkud zavádějícím způsobem se takto provedený důkaz označuje jako *elementární*) podali až v roce 1949 pánové Atle Selberg a Paul Erdős.

Vraťme se však k panu Čebyševovi. Čebyševovy nerovnosti jsou odhady počtu prvočísel nepřevyšujících dané $n \in \mathbb{N}$ (tj. odhady hodnot $\pi(n)$) a odhady hodnot $n-$tého prvočísla p_n.

První Čebyševova věta říká, že existují kladné konstanty $c_1, c_2 \in \mathbb{R}$ takové, že pro každé $x \in \mathbb{R}, x \geqq 2$ platí

$$c_1 \frac{x}{\ln x} < \pi(x) < c_2 \frac{x}{\ln x}.$$

Můžeme to interpretovat tak, že hodnoty $\pi(x)$ souvisí s hodnotami $\frac{x}{\ln x}$. Jestliže si věc představíme graficky, znamená to, že hodnoty $\pi(x)$ jsou „uvězněny“ v pásu ohraničeném grafy funkcí $c_1 \frac{x}{\ln x}$ a $c_2 \frac{x}{\ln x}$.

Bez znalosti prvočíselné věty[1] (viz Věta 2.14) by to však nebyla žádná velká výhra, neboť toto vězení není příliš těsné. Zmiňovaný pás se s rostoucím n rozšiřuje nade všechny meze. Snadno se o tom přesvědčíme[2]

$$\lim_{n\to\infty} \left(c_2 \tfrac{n}{\ln n} - c_1 \tfrac{n}{\ln n} \right) = \lim_{n\to\infty} \tfrac{n}{\ln n} \underbrace{(c_2 - c_1)}_{>0} \overset{\text{l'H}}{=} \lim_{n\to\infty} \tfrac{1}{\frac{1}{n}} (c_2 - c_1) =$$

$$= \lim_{n\to\infty} n(c_2 - c_1) = \infty.$$

[1] Ta říká, že se hodnoty $\pi(x)$ nejen drží mezi hodnotami $c_1 \frac{x}{\ln x}$ a $c_2 \frac{x}{\ln x}$, ale dokonce, že se s rostoucím $x \in \mathbb{R}$ velmi blíží hodnotě $\frac{x}{\ln x}$.

[2] Při výpočtu limity použijeme l' Hospitalovo pravidlo, což na příslušném místě naznačíme symbolem *l' H* nad rovnítkem.

Druhá Čebyševova věta říká, že existují kladné konstanty $k_1, k_2 \in \mathbb{R}$ takové, že pro každé $n \geqq 2$ platí

$$k_1 n \ln n < p_n < k_2 n \ln n.$$

Toto tvrzení je důsledkem první Čebyševovy věty. Jde o odhad intervalu, v němž se s jistotou nachází n-té prvočíslo. Velikost tohoto intervalu však s rostoucím n také roste nade všechny meze, neboť

$$\lim_{n\to\infty}(k_2 n \ln n - k_1 n \ln n) = \lim_{n\to\infty}(\underbrace{k_2 - k_1}_{>0})n \ln n = \infty.$$

Čebyševovy věty představují velice hezký teoretický výsledek. Bohužel, jak jsme viděli, s rostoucí hodnotou n ztrácí na užitečnosti. Odhady jsou stále méně přesné. Nicméně Čebyševovy věty budou ještě užitečné i jinak. Použijeme je v důkazu Bertrandova postulátu (viz podkapitola 2.5).

Poznámka 2.16. Ve výše uvedených Čebyševových nerovnostech se objevily blíže neurčené konstanty c_1 a c_2. Pokud bychom chtěli pro konkrétní $x \in \mathbb{R}$ odhadnout hodnotu $\pi(x)$, byl by to problém. Z níže uvedených textů této podkapitoly však lze vyčíst o něco méně elegantní, leč konkrétnější odhady hodnoty $\pi(x)$. Jsou to nerovnosti

$$(\ln 2)\frac{x}{\ln x} - \frac{\ln 4}{\ln x} - 1 < \pi(x) < 2(\ln 4)\frac{x}{\ln x} + \sqrt{x}. \tag{2.13}$$

Pomocí prvočíselné věty jsme odhadli, že prvočísel menších než 1 000 000 je přibližně 72 382 (viz podkapitola 2.3). [1] Pomocí nerovností (2.13) docházíme k tomu, že

$$(\ln 2)\frac{1\,000\,000}{\ln 1\,000\,000} - \frac{\ln 4}{\ln 1\,000\,000} - 1 < \pi(1\,000\,000) < 2(\ln 4)\frac{1\,000\,000}{\ln 1\,000\,000} + \sqrt{1\,000\,000},$$

$$50\,170 < \pi(1\,000\,000) < 201\,686.$$

Zatím jsme tedy schopni říci, že prvočísel menších než 1 000 000 je nejspíš něco kolem 72 tisíc, ale určitě více než 50 170 a méně než 201 686.

Zbývá jediné, a to Čebyševovy věty dokázat. Budeme k tomu potřebovat následující lemmata.

Lemma 2.17. *Pro každé přirozené číslo k platí*[2]

$$\binom{2k+1}{k+1} < 4^k.$$

[1] Neboť $\frac{1\,000\,000}{\ln 1\,000\,000} \doteq 72382,41$

[2] Obecně, $\binom{n}{k}$ (čteme „n nad k“) je tzv. kombinační číslo a platí $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Důkaz. Důkaz provedeme pomocí elementárních úvah a odhadů.

$$\binom{2k+1}{k+1} = \frac{(2k+1)!}{k!(k+1)!} = \frac{\overbrace{(2\cdot 4\cdot \cdots \cdot(2k))}^{\text{sudá čísla}}.\overbrace{(3\cdot 5\cdot \cdots \cdot(2k+1))}^{\text{lichá čísla}}}{(1\cdot 2\cdot \cdots \cdot k)(1\cdot 2\cdot \cdots \cdot(k+1))}$$

Z každého čísla v levé závorce v čitateli vytkneme číslo 2 a obdržíme

$$\binom{2k+1}{k+1} = \frac{2^k(1\cdot 2\cdot \cdots \cdot k)(3\cdot 5\cdot \cdots \cdot(2k+1))}{(1\cdot 2\cdot \cdots \cdot k)(1\cdot 2\cdot \cdots \cdot(k+1))} =$$

$$= \frac{2^k(3\cdot 5\cdot \cdots \cdot(2k+1))}{(1\cdot 2\cdot \cdots \cdot(k+1))} < \frac{2^k(4\cdot 6\cdot \cdots \cdot(2k+2))}{(1\cdot 2\cdot \cdots \cdot(k+1))}.$$

Opět vytkneme z čísel ze závorky v čitateli (je tam k sudých čísel, takže před závorkou bude 2^k). A tak

$$\binom{2k+1}{k+1} < \frac{2^k(4\cdot 6\cdot \cdots \cdot(2k+2))}{(1\cdot 2\cdot \cdots \cdot(k+1))} = \frac{2^k\cdot 2^k(2\cdot 3\cdot \cdots \cdot(k+1))}{(1\cdot 2\cdot \cdots \cdot(k+1))} = 2^k\cdot 2^k = 4^k.$$

□

Lemma 2.18. *Pro každé přirozené číslo k platí*

$$\prod_{\substack{p\in\mathbb{P}\\ k+1<p\leqq 2k+1}} p < 4^k.$$

Důkaz. Uvažujme kombinační číslo $K = \binom{2k+1}{k+1}$. Jak známo, kombinační čísla jsou přirozená čísla, takže $K \in \mathbb{N}$. Dále platí

$$K = \binom{2k+1}{k+1} = \frac{(2k+1)!}{k!(k+1)!} = \frac{(k+2)(k+3)\cdots(2k+1)}{k!}.$$

Odtud

$$(k+2)(k+3)\cdots(2k+1) = K\cdot k!$$

Všechna prvočísla p splňující $k+1 < p \leqq 2k+1$ se vyskytují v součinu $(k+2)(k+3)\cdots(2k+1)$. Proto všechna prvočísla p, kde $k+1 < p \leqq 2k+1$, dělí číslo $K\cdot k!$.

Všimněme si, že p, kde $k+1 < p \leqq 2k+1$, nemůže dělit číslo $k!$ (neboť $k!$ je součin čísel menších, nebo rovných číslu k).

Proto, podle Lemmata 1.23, musí všechna čísla p, kde $k+1 < p \leqq 2k+1$, dělit číslo K. Součin všech prvočísel p, splňujících $k+1 < p \leqq 2k+1$, pak musí také dělit číslo K. A tak

$$\prod_{\substack{p\in\mathbb{P}\\ k+1<p\leqq 2k+1}} p \leqq K = \binom{2k+1}{k+1}.$$

Podle Lemmata 2.17 je $\binom{2k+1}{k+1} < 4^k$. □

Lemma 2.19. *Pro každé přirozené číslo $n \geqq 2$ platí*

$$\prod_{p\in\mathbb{P},p\leqq n} p < 4^n.$$

Důkaz. Důkaz provedeme silnou matematickou indukcí podle n. Nejprve proto ověříme platnost tvrzení pro $n = 2$. A opravdu,

$$\prod_{p\in\mathbb{P},p\leqq 2} p = 2 < 4^2 = 16.$$

Indukčním předpokladem je, že tvrzení lemmata je pravdivé pro všechna $m < < n$, tj. předpokládáme, že

$$\prod_{p\in\mathbb{P},p\leqq m} p < 4^m \text{ pro všechna } m < n.$$

Na základě tohoto předpokladu dokážeme, že platí také $\prod_{p\in\mathbb{P},p\leqq n} p < 4^n$.

Mohou nastat dvě možnosti. Číslo n je buď sudé, a nebo liché. Probereme oba tyto případy.

Pokud je n sudé, pak $n = 2k$. V případě, že $k = 1$ je tvrzení lemmata pravdivé (případ $n = 2$ jsme již ověřili). V případě, že $k \geqq 2$, nemůže být číslo $n = 2k$ prvočíslem (jedná se o číslo složené!). Proto všechna prvočísla splňující podmínku $p \leqq n$ splňují také $p \leqq n - 1$. A tak

$$\prod_{p\in\mathbb{P},p\leqq n} p = \prod_{p\in\mathbb{P},p\leqq n-1} p.$$

Podle indukčního předpokladu platí

$$\prod_{p\in\mathbb{P},p\leqq n-1} p < 4^{n-1}.$$

Odtud dostáváme

$$\prod_{p\in\mathbb{P},p\leqq n} p = \prod_{\substack{p\in\mathbb{P}\\ p\leqq n-1}} p < 4^{n-1} < 4^n.$$

Takže, pokud je n sudé, pak je tvrzení lemmata pravdivé.

Zbývá prověřit případ, kdy n je liché. Potom $n = 2k + 1$, kde $k \geqq 1$ a díky indukčnímu předpokladu a Lemmata 2.18 můžeme psát

$$\prod_{p\in\mathbb{P},p\leqq n} p = \prod_{\substack{p\in\mathbb{P}\\ p\leqq 2k+1}} p = \underbrace{\left(\prod_{\substack{p\in\mathbb{P}\\ p\leqq k+1}} p\right)}_{<4^{k+1}} \underbrace{\left(\prod_{\substack{p\in\mathbb{P}\\ k+1<p\leqq 2k+1}} p\right)}_{<4^{k}} < 4^{2k+1} = 4^n.$$

podle ind. předp. podle Lemmatu 2.18

□

Důsledek 2.20. Pro každé reálné číslo $x \geqq 2$ platí

$$\prod_{p\in\mathbb{P},p\leqq x} p < 4^x.$$

Důkaz. Každé reálné $x \geqq 2$ můžeme psát ve tvaru $x = [x] + \varepsilon_x$, kde $[x] \in \mathbb{N}$, $[x] \geqq 2$, $0 \leqq \varepsilon_x < 1$.

Prvočísla p splňující $p \leqq x$ evidentně také splňují $p \leqq [x]$ (taková prvočísla p existují, neboť $[x] \geqq 2$). Proto, podle Lemmata 2.19 a protože $[x] \leqq x$, platí

$$\prod_{p\in\mathbb{P},p\leqq x} p = \underbrace{\prod_{p\in\mathbb{P},p\leqq[x]} p < 4^{[x]}}_{\text{podle Lemmatu 2.19}} < 4^x.$$

□

Lemma 2.21. *Nechť $n, p \in \mathbb{N}$. Potom počet přirozených čísel ve tvaru $p\cdot m$, kde $p\cdot m \leqq n$, $m \in \mathbb{N}$, je roven $\left[\frac{n}{p}\right]$.*

Důkaz. Nejprve připomeňme, že $[x]$ je označení pro celou část reálného čísla x (viz Definice 1.11).

Pokud $n < p$, pak čísla ve tvaru $p\cdot m$, kde $p\cdot m \leqq n$ ($m \in \mathbb{N}$), evidentně neexistují. A opravdu. V tomto případě je $0 < \frac{n}{p} < 1$, a tak $\left[\frac{n}{p}\right] = 0$.

V případě $n \geqq p$ čísla ve tvaru $p\cdot m$, kde $pm \leqq n$, existují (minimálně jedno: $p\cdot 1$). Dejme tomu, že čísla ve tvaru pm, která jsou menší, nebo rovna n, jsou čísla

$$p\cdot 1,\ p\cdot 2, \ldots,\ p\cdot m_0$$

(jejich počet je tedy roven m_0). Potom $p\cdot(m_0+1)$ již musí být větší než n. Dostáváme nerovnosti

$$p\cdot m_0 \leqq n < p\cdot(m_0+1).$$

Odtud

$$m_0 \leqq \frac{n}{p} < m_0 + 1.$$

Podle Definice 1.11 je $m_0 = \left[\frac{n}{p}\right]$.

□

Lemma 2.22. *Nechť $n \in \mathbb{N}$. Potom $n! = \prod_{p\in\mathbb{P},p\leqq n} p^{\alpha(p)}$, kde*

$$\alpha(p) = \sum_{k\in\mathbb{N},p^k\leqq n} \left[\frac{n}{p^k}\right].$$

Důkaz. Lema 2.22 říká, že v kanonickém rozkladu čísla $n! = 1\cdot 2\cdot\cdots\cdot n$ jsou zastoupena všechna prvočísla $p \leqq n$, a to s exponentem $\alpha(p)$.

Protože $n!$ je součin čísel menších, nebo rovných n, je zřejmé, že v jeho kanonickém rozkladu mohou vystupovat pouze prvočísla $p \leqq n$.

Uvažujme, čemu je roven exponent $\alpha(p)$. K jeho hodnotě mohou přispívat čísla vyskytující se v součinu $1\cdot 2\cdot\cdots\cdot n$, která mají tvar $p\cdot m$. [1]

Kolik čísel ve tvaru $p\cdot m$ se vyskytuje v součinu $1\cdot 2\cdot\cdots\cdot n$? Jsou to ty, které splňují $p\cdot m \leqq n$. Těch je podle Lemmata 2.21 celkem $\left[\frac{n}{p}\right]$ a každé z nich přispívá k hodnotě $\alpha(p)$ alespoň číslem 1.

Číslem 1 přispívají k hodnotě $\alpha(p)$ ty čísla, která mají tvar $p\cdot m \leqq n$, ale nemají tvar $p^2\cdot m$. Těch je podle Lemmata 2.21 celkem $\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]$.

Číslem 2 přispívají k hodnotě $\alpha(p)$ ty čísla, která mají tvar $p^2\cdot m \leqq n$, ale nemají tvar $p^3\cdot m$. Těch je podle Lemmata 2.21 celkem $\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]$.

$\vdots$

Číslem k přispívají k hodnotě $\alpha(p)$ ty čísla, která mají tvar $p^k\cdot m \leqq n$, ale nemají tvar $p^{k+1}\cdot m$. Těch je podle Lemmata 2.21 celkem $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$.

$\vdots$

Pokud $p^{k_0} > n$, pak se $p^{k_0}.m$ již nevyskytuje v součinu $1\cdot 2\cdot\cdots\cdot n$, a tak k hodnotě $\alpha(p)$ nepřispívá. Odpovídá to tomu, že v tom případě je čísel $p^{k_0}\cdot m \leqq n$ celkem $\left[\frac{n}{p^{k_0}}\right] = 0$. Označíme-li k_1 číslo splňující podmínku $p^{k_1} \leqq n$ a zároveň $p^{k_1+1} > n$, pak platí

$$\alpha(p) = 1\cdot\left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + 2\cdot\left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right) + \cdots + k_1\cdot\left(\left[\frac{n}{p^{k_1}}\right] - \underbrace{\left[\frac{n}{p^{k_1+1}}\right]}_{=0}\right).$$

Odtud pomocí vytýkání dostáváme

$$\alpha(p) = \left[\frac{n}{p}\right] + (2-1)\left[\frac{n}{p^2}\right] + (3-2)\left[\frac{n}{p^3}\right] + \cdots + (k_1 - (k_1-1))\cdot\left[\frac{n}{p^{k_1}}\right],$$

$$\alpha(p) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots + \left[\frac{n}{p^{k_1}}\right],$$

$$\alpha(p) = \sum_{k\in\mathbb{N}, p^k\leqq n}\left[\frac{n}{p^k}\right].$$

□

[1] Uvažme, že některá z čísel ve tvaru $p\cdot m$ mohou mít i tvar $p^2\cdot m$ ($p^2\cdot m = p\cdot p\cdot m = p\cdot m^*$). Dále, některá z čísel ve tvaru $p^2\cdot m$ mohou mít i tvar $p^3\cdot m$ ($p^3\cdot m = p^2\cdot p\cdot m = p\cdot m^*$). A tak dále. Samozřejmě se ale v úvahách stačí omezit jen na tvary $p^k.m$, kde $k\in\mathbb{N}, p^k \leqq n$.

Důsledek 2.23. Nechť $n \in \mathbb{N}$. Potom $n! = \prod\limits_{\substack{p \leqq n \\ p \in \mathbb{P}}} p^{\alpha(p)} = \prod_{p \in \mathbb{P}} p^{\alpha(p)}$, kde

$$\alpha(p) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

Důkaz. Podle Lemmata 2.22 je $n! = \prod_{p \in \mathbb{P}, p \leqq n} p^{\alpha(p)}$, kde $\alpha(p) = \sum\limits_{k \in \mathbb{N}, p^k \leqq n} \left[\frac{n}{p^k} \right]$.

Pro každé $k_0 \in \mathbb{N}$ takové, že $p^{k_0} > n$ zřejmě platí $\left[\frac{n}{p^{k_0}} \right] = 0$. Proto

$$\sum_{k \in \mathbb{N}, p^k \leqq n} \left[\frac{n}{p^k} \right] = \sum_{k \in \mathbb{N}} \left[\frac{n}{p^k} \right] = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

Pro $p > n$ evidentně platí $\left[\frac{n}{p^k} \right] = 0$ pro každé $k \in \mathbb{N}$. Proto pro $p > n$ je $\alpha(p) = \sum\limits_{k \in \mathbb{N}} \left[\frac{n}{p^k} \right] = 0$. A tak se v součinu $\prod_{p \in \mathbb{P}} p^{\alpha(p)}$ vyskytují s nenulovým exponentem pouze prvočísla $p \leqq n$. Odtud dostáváme

$$\prod_{p \in \mathbb{P}, p \leqq n} p^{\alpha(p)} = \prod_{p \in \mathbb{P}} p^{\alpha(p)}.$$

□

Lemma 2.24. *Nechť $n \in \mathbb{N}$. Potom*

$$\binom{2n}{n} = \prod_{\substack{p \leqq 2n \\ p \in \mathbb{P}}} p^{\beta(p)},$$

kde $\beta(p) = \sum\limits_{k=1}^{\infty} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right)$

Důkaz. Připomeňme, že hodnota kombinačního čísla je dána vztahem

$$\binom{r}{s} = \frac{r!}{s!(r-s)!}$$

Proto

$$\binom{2n}{n} = \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{n!n!} = \frac{(2n)!}{(n!)^2}.$$

Podle Věty 2.22 a Důsledku 2.23 můžeme psát

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{\prod_{\substack{p \leqq 2n \\ p \in \mathbb{N}}} p^{\alpha_1(p)}}{\left(\prod_{\substack{p \leqq n \\ p \in \mathbb{N}}} p^{\alpha_2(p)} \right)^2}, \tag{2.14}$$

kde $\alpha_1(p) = \sum_{k=1}^{\infty} \left[\frac{2n}{p^k}\right]$ a $\alpha_2(p) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$.

Z důkazu Důsledku 2.23 je patrné, že $\prod_{\substack{p\leqq n\\ p\in\mathbb{N}}} p^{\alpha_2(p)} = \prod_{\substack{p\leqq 2n\\ p\in\mathbb{N}}} p^{\alpha_2(p)}$. Dosadíme do vztahu (2.14) a obdržíme

$$\binom{2n}{n} = \frac{\prod_{\substack{p\leqq 2n\\ p\in\mathbb{N}}} p^{\alpha_1(p)}}{\left(\prod_{\substack{p\leqq 2n\\ p\in\mathbb{N}}} p^{\alpha_2(p)}\right)^2} = \frac{\prod_{\substack{p\leqq 2n\\ p\in\mathbb{N}}} p^{\alpha_1(p)}}{\prod_{\substack{p\leqq 2n\\ p\in\mathbb{N}}} p^{2\alpha_2(p)}} = \prod_{\substack{p\leqq 2n\\ p\in\mathbb{N}}} p^{\alpha_1(p)-2\alpha_2(p)} = \prod_{\substack{p\leqq 2n\\ p\in\mathbb{N}}} p^{\beta(p)},$$

kde $\beta(p) = \alpha_1(p) - 2\alpha_2(p) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right)$.

□

Lemma 2.25. *Nechť $n \in \mathbb{N}$, $n \geqq 2$. Potom*

$$\binom{2n}{n} > \frac{2^{2n}}{2n}.$$

Důkaz. Důkaz provedeme pomocí elementárních úprav a nerovností.

$$\binom{2n}{n} = \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{n!n!} = \frac{1\cdot 2\cdot 3\cdot \cdots \cdot 2n}{(1\cdot 2\cdot \cdots \cdot n)(1\cdot 2\cdot \cdots \cdot n)}$$

Součin v čitateli můžeme přeuspořádat tak, že nejprve vynásobíme sudá čísla a pak lichá. Proto

$$\binom{2n}{n} = \frac{(2\cdot 4\cdot \cdots \cdot 2n)(3\cdot 5\cdot \cdots \cdot (2n-1))}{(1\cdot 2\cdot \cdots \cdot n)(1\cdot 2\cdot \cdots \cdot n)}.$$

Sudých čísel v čitateli je celkem n a z každého můžeme vytknout číslo 2 před závorku (celkově proto vytkneme 2^n). A tak

$$\binom{2n}{n} = \frac{2^n(1\cdot 2\cdot \cdots \cdot n)(3\cdot 5\cdot \cdots \cdot (2n-1))}{(1\cdot 2\cdot \cdots \cdot n)(1\cdot 2\cdot \cdots \cdot n)}.$$

Lichých čísel v čitateli (jsou v pravé závorce) je celkem $n-1$ a platí $3 > 2$, $5 > 4$, $\ldots$, $2n-1 > 2(n-1)$. Odtud dostáváme odhad

$$\binom{2n}{n} = \frac{2^n(1\cdot 2\cdot \cdots \cdot n)(3\cdot 5\cdot \cdots \cdot (2n-1))}{(1\cdot 2\cdot \cdots \cdot n)(1\cdot 2\cdot \cdots \cdot n)} > \frac{2^n(1\cdot 2\cdot \cdots \cdot n)\Big(2\cdot 4\cdot \cdots \cdot (2(n-1))\Big)}{(1\cdot 2\cdot \cdots \cdot n)(1\cdot 2\cdot \cdots \cdot n)}.$$

V pravé závorce v čitateli je celkem $n-1$ a z každého můžeme vytknout číslo 2 před závorku (celkově proto vytkneme 2^{n-1}). Proto

$$\binom{2n}{n} > \frac{2^n(1\cdot 2\cdot \cdots \cdot n)\Big(2\cdot 4\cdot \cdots \cdot (2(n-1))\Big)}{(1\cdot 2\cdot \cdots \cdot n)(1\cdot 2\cdot \cdots \cdot n)} = \frac{2^n(1\cdot 2\cdot \cdots \cdot n)2^{n-1}(1\cdot 2\cdot \cdots \cdot (n-1))}{(1\cdot 2\cdot \cdots \cdot n)(1\cdot 2\cdot \cdots \cdot n)}.$$

Pouhým krácením ve zlomku vpravo obdržíme odhad

$$\binom{2n}{n} > \frac{2^n \cdot 2^{n-1}}{n} = \frac{2^{2n}}{2n}.$$

□

Nyní odvodíme horní odhad hodnoty $\pi(x)$.

Věta 2.26. *Pro každé $x \geqq 2$ platí*

$$\pi(x) < 2(\ln 4)\frac{x}{\ln x} + \sqrt{x}.$$

Důkaz. Zřejmě platí následující nerovnosti

$$\underbrace{4^x > \prod_{\substack{p\in\mathbb{P}\\ p\leqq x}} p}_{\text{podle Důsledku 2.20}} = \underbrace{\prod_{\substack{p\in\mathbb{P}\\ p\leqq\sqrt{x}}} p}_{\geqq 1} \prod_{\substack{p\in\mathbb{P}\\ \sqrt{x}<p\leqq x}} p \geqq \prod_{\substack{p\in\mathbb{P}\\ \sqrt{x}<p\leqq x}} p \tag{2.15}$$

Uvažme, kolik prvočísel p splňuje nerovnosti $\sqrt{x} < p \leqq x$. Od počtu prvočísel menších než x je třeba odečíst počet prvočísel menších než $\sqrt{x}$. Takže mezi $\sqrt{x}$ a x je celkem $\pi(x) - \pi(\sqrt{x})$. Navíc, každé z těchto prvočísel splňuje $p > \sqrt{x}$. Proto

$$\prod_{\substack{p\in\mathbb{P}\\ \sqrt{x}<p\leqq x}} p > (\sqrt{x})^{(\pi(x)-\pi(\sqrt{x}))} \geqq (\sqrt{x})^{(\pi(x)-\sqrt{x})}, \tag{2.16}$$

neboť[1] $\pi(\sqrt{x}) \leqq \sqrt{x}$.

Z (2.15) a (2.16) dostáváme

$$4^x > (\sqrt{x})^{(\pi(x)-\sqrt{x})}.$$

Odtud[2] dostáváme

$$\begin{aligned}
\ln(4^x) &> \ln(\sqrt{x})^{(\pi(x)-\sqrt{x})},\\
\ln(4^x) &> (\pi(x)-\sqrt{x})\ln(\sqrt{x}),\\
x(\ln 4) &> (\pi(x)-\sqrt{x})\frac{1}{2}\ln x,\\
2(\ln 4)\frac{x}{\ln x} &> (\pi(x)-\sqrt{x}).
\end{aligned}$$

□

[1] Prvočísel menších, než $\sqrt{x}$ je méně než $\sqrt{x}$ (nebo rovno). Jinak řečeno, $\pi(\sqrt{x}) \leqq \sqrt{x}$.

[2] Přirozený logaritmus je rostoucí funkce. Tj. v případě $a > b$ platí $\ln a > \ln b$

Následuje dolní dohad hodnoty $\pi(x)$.

Věta 2.27. *Pro každé reálné $x \geqq 2$ platí*

$$\pi(x) > \frac{x}{\ln x} \ln 2 - \frac{2 \ln 2}{\ln x} - 1.$$

Důkaz. Z Lemmat 2.24 a 2.25 plyne, že pro každé $n \in \mathbb{N}$ platí

$$\prod_{\substack{p \leqq 2n \\ p \in \mathbb{N}}} p^{\beta(p)} = \binom{2n}{n} > \frac{2^{2n}}{2n}, \tag{2.17}$$

kde $\beta(p) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right)$. Označíme-li m_p přirozené číslo takové, že

$$p^{m_p} \leqq 2n < p^{m_p+1}, \tag{2.18}$$

pak

$$\beta(p) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right) = \sum_{k=1}^{m_p} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right), \tag{2.19}$$

neboť pro $k > m_p$ platí $\left[\frac{2n}{p^k} \right] = 0 = \left[\frac{n}{p^k} \right]$.

V příkladě 1. ze Cvičení 1.2.1 jsme dokázali (viz řešení příkladů v Kapitole 8), že

$$\forall r \in \mathbb{R} : -1 = 2r - 1 - 2r < [2r] - 2[r] < 2r - 2(r-1) = 2.$$

Proto můžeme psát

$$-1 < \left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] < 2,$$

jinak řečeno

$$0 \leqq \left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \leqq 1. \tag{2.20}$$

Z (2.19) a (2.20) dostáváme odhad hodnoty $\beta(p)$.

$$0 = 0 \cdot m_p \leqq \beta(p) = \sum_{k=1}^{m_p} \Bigg(\underbrace{\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right]}_{0 \leqq \text{ a zároveň } \leqq 1} \Bigg) \leqq 1 \cdot m_p = m_p \tag{2.21}$$

Z (2.18) a (2.20) pak plyne, že pro každé $p \leqq 2n$ platí

$$p^{\beta(p)} \leqq p^{m_p} \leqq 2n. \tag{2.22}$$

Použijeme-li (2.17), (2.22) a fakt, že počet prvočísel p splňujících $p \leqq 2n$ je roven $\pi(2n)$, pak obdržíme nerovnosti

$$\frac{2^{2n}}{2n} < \prod_{\substack{p \leqq 2n \\ p \in \mathbb{N}}} p^{\beta(p)} \leqq \prod_{\substack{p \leqq 2n \\ p \in \mathbb{N}}} p^{m_p} \leqq (2n)^{\pi(2n)},$$

tj.

$$\frac{2^{2n}}{2n} < (2n)^{\pi(2n)} \tag{2.23}$$

Poštveme-li na (2.23) logaritmus, získáme

$$\ln\left(\frac{2^{2n}}{2n}\right) < \ln(2n)^{\pi(2n)},$$

$$\ln 2^{2n} - \ln(2n) < \pi(2n)\ln(2n),$$

$$\frac{\ln 2^{2n}}{\ln(2n)} - 1 < \pi(2n),$$

$$\frac{2n}{\ln(2n)}\ln 2 - 1 < \pi(2n). \tag{2.24}$$

Naším cílem ovšem není odhad hodnoty $\pi(2n)$, ale odhad $\pi(x)$. Provedeme proto substituci. Pro $x \geqq 2$ platí, že $\left[\frac{x}{2}\right] \in \mathbb{N}$. Proto si může dovolit provést substituci $n = \left[\frac{x}{2}\right]$. A tak z (2.24) dostáváme

$$\frac{2\left[\frac{x}{2}\right]}{\ln\left(2\left[\frac{x}{2}\right]\right)}\ln 2 - 1 < \pi\left(2\left[\frac{x}{2}\right]\right). \tag{2.25}$$

Platí $2\left[\frac{x}{2}\right] \leqq 2\frac{x}{2} = x$, proto $\pi\left(2\left[\frac{x}{2}\right]\right) \leqq \pi(x)$ a tak z (2.25) plyne

$$\pi(x) > \underbrace{\frac{2\left[\frac{x}{2}\right]}{\ln\left(2\left[\frac{x}{2}\right]\right)}\ln 2 - 1 \geqq \frac{2\left[\frac{x}{2}\right]}{\ln x}\ln 2 - 1}_{\text{neboť } \ln\left(2\left[\frac{x}{2}\right]\right) \leqq \ln x}. \tag{2.26}$$

A protože $2\left[\frac{x}{2}\right] \geqq 2\left(\frac{x}{2} - 1\right)$, musí podle (2.26) platit

$$\pi(x) > \frac{2\left(\frac{x}{2} - 1\right)}{\ln x}\ln 2 - 1 = \frac{x}{\ln x}\ln 2 - \frac{2\ln 2}{\ln x} - 1.$$

□

Nyní již disponujeme znalostmi postačujícími pro důkaz první Čebyševovy věty.

Věta 2.28. (První Čebyševova) *Existují reálné konstanty $c_1, c_2 > 0$ takové, že pro každé $x \geqq 2$ platí*

$$c_1 \frac{x}{\ln x} < \pi(x) < c_2 \frac{x}{\ln x}.$$

Důkaz. Vyjdeme z tvrzení vět 2.26 a 2.27. Ty říkají, že pro každé $x \geqq 2$ platí

$$\frac{x}{\ln x} \ln 2 - \frac{2 \ln 2}{\ln x} - 1 < \pi(x) < 2(\ln 4) \frac{x}{\ln x} + \sqrt{x}.$$

Odtud

$$\frac{x}{\ln x} \left(\ln 2 - \frac{2 \ln 2}{x} - \frac{\ln x}{x} \right) < \pi(x) < \frac{x}{\ln x} \left(2 \ln 4 + \frac{\ln x}{\sqrt{x}} \right). \tag{2.27}$$

Vzhledem k tomu, že $\lim\limits_{x \to \infty} \frac{2 \ln 2}{x} = 0$, $\lim\limits_{n \to \infty} \frac{\ln x}{x} = 0$ a také $\lim\limits_{x \to \infty} \frac{\ln x}{\sqrt{x}} = 0$,[1] musí existovat číslo $x_0 \in \mathbb{R}$, $x_0 > 2$ takové, že pro každé $x > x_0$ jsou splněny nerovnosti

$$\frac{2 \ln 2}{x} < \frac{1}{4} \ln 2 \text{ a zároveň } \frac{\ln x}{x} < \frac{1}{4} \ln 2 \text{ a zároveň } \frac{\ln x}{\sqrt{x}} < \ln 4. \tag{2.28}$$

Takže, podle nerovností (2.27) a (2.28), musí pro každé $x > x_0$ platit

$$\frac{x}{\ln x} \left(\ln 2 - \frac{1}{4} \ln 2 - \frac{1}{4} \ln 2 \right) < \frac{x}{\ln x} \left(\ln 2 - \frac{2 \ln 2}{x} - \frac{\ln x}{x} \right) < \pi(x) \tag{2.29}$$

a také

$$\pi(x) < \frac{x}{\ln x} \left(2 \ln 4 + \frac{\ln x}{\sqrt{x}} \right) < \frac{x}{\ln x} \left(2 \ln 4 + \ln 4 \right). \tag{2.30}$$

Z nerovností (2.29) a (2.30) dostáváme pro každé $x > x_0$ odhad

$$\frac{x}{\ln x} \left(\underbrace{\frac{1}{2} \ln 2}_{d_1} \right) < \pi(x) < \frac{x}{\ln x} (\underbrace{3 \ln 4}_{d_2}).$$

Dokázali jsme tak, že existují reálné konstanty $d_1, d_2 > 0$ takové, že pro každé $x > x_0$ platí

$$\frac{x}{\ln x} d_1 < \pi(x) < \frac{x}{\ln x} d_2. \tag{2.31}$$

[1] S využitím l'Hospitalova pravidla: $\lim\limits_{n \to \infty} \frac{\ln x}{x} = \lim\limits_{n \to \infty} \frac{\frac{1}{x}}{1} = 0$ a také $\lim\limits_{x \to \infty} \frac{\ln x}{\sqrt{x}} \overset{\text{l'H}}{=} \lim\limits_{x \to \infty} \frac{\frac{1}{x}}{\frac{1}{2} x^{-\frac{1}{2}}} =$
$= \lim\limits_{x \to \infty} \frac{2}{x^{\frac{1}{2}}} = 0.$

A co případ, kdy $x \leqq x_0$ (přičemž uvažujeme $x \geqq 2$)? Definujme $m(x) = \frac{x}{\pi(x)\ln x}d_1$ a $m_0 = \sup\limits_{x\leqq x_0}\{\frac{x}{\pi(x)\ln x}d_1\}$.[1] Potom pro každé $x \leqq x_0$ platí $m(x) \leqq m_0$ a jistě najdeme přirozené číslo k takové, že

$$\frac{m_0}{k} < 1.$$

Evidentně pak pro každé $x \geqq 2$, $x \leqq x_0$ platí

$$\frac{m(x)}{k} \leqq \frac{m_0}{k} < 1.$$

Odtud

$$\underbrace{\frac{x}{\pi(x)\ln x}\frac{d_1}{k}}_{\frac{m(x)}{k}} < 1,$$

$$\frac{x}{\ln x}\frac{d_1}{k} < \pi(x). \tag{2.32}$$

Číslo $k \in \mathbb{N}$ a $d_1 > 0$, proto pro každé $x \geqq 2$ platí $\frac{x}{\ln x}\frac{d_1}{k} \leqq \frac{x}{\ln x}d_1$. A tak z nerovností (2.31) a (2.32) můžeme usoudit, že pro každé $x \in \mathbb{R}$, $x \geqq 2$ platí

$$\frac{x}{\ln x}\frac{d_1}{k} < \pi(x). \tag{2.33}$$

Označíme-li $c_1 = \frac{d_1}{k}$, pak z (2.33) plyne, že existuje reálná konstanta $c_1 > 0$ taková, že pro každé $x \in \mathbb{R}$, $x \geqq 2$ platí

$$\frac{x}{\ln x}c_1 < \pi(x). \tag{2.34}$$

Odhad shora dokončíme obdobně. Definujme $M(x) = \frac{x}{\pi(x)\ln x}d_2$ a $M_0 = \inf\limits_{x\leqq x_0}\{\frac{x}{\pi(x)\ln x}d_2\}$. Potom pro každé $x \leqq x_0$ platí $M(x) \geqq M_0$ a jistě najdeme přirozené číslo K takové, že

$$1 < K\cdot M_0.$$

Evidentně pak pro každé $x \geqq 2$, $x \leqq x_0$ platí

$$1 < K\cdot M_0 \leqq K\cdot M(x).$$

Odtud

$$1 < \underbrace{\frac{x}{\pi(x)\ln x}K\cdot d_2}_{K\cdot M(x)},$$

[1] $m_0 = \sup\limits_{x\leqq x_0}\{\frac{x}{\pi(x)\ln x}d_1\}$ je supremum množiny $\{\frac{x}{\pi(x)\ln x}d_1 \mid x \in \mathbb{R}, x \leqq x_0\}$. Připomeňme, že supremum neprázdné množiny M je reálné číslo, nebo $\pm\infty$, které je větší, nebo rovno všem prvkům množiny M a navíc, v jeho libovolně malém okolí nalezneme nějaký prvek z M. Každá množina reálných čísel má své supremum.

$$\pi(x) < \frac{x}{\ln x} K \cdot d_2. \tag{2.35}$$

Číslo $K \in \mathbb{N}$ a $d_2 > 0$, proto pro každé $x \geqq 2$ platí $\frac{x}{\ln x} K \cdot d_2 \geqq \frac{x}{\ln x} d_2$. A tak z nerovností (2.31) a (2.35) můžeme usoudit, že pro každé $x \in \mathbb{R}$, $x \geqq 2$ platí

$$\pi(x) < \frac{x}{\ln x} K \cdot d_2. \tag{2.36}$$

Označíme-li $c_2 = K \cdot d_2$, pak z (2.36) plyne, že existuje reálná konstanta $c_2 > 0$ taková, že pro každé $x \in \mathbb{R}$, $x \geqq 2$ platí

$$\pi(x) < \frac{x}{\ln x} c_2. \tag{2.37}$$

Tím jsme dokázali tvrzení první Čebyševovy věty, neboť z (2.34) a (2.37) plyne existence reálných konstant $c_1, c_2 > 0$ takových, že

$$\frac{x}{\ln x} c_1 < \pi(x) < \frac{x}{\ln x} c_2.$$

□

Věta 2.29. (Druhá Čebyševova) *Nechť $p_1 < p_2 < \cdots < p_n < \cdots$ je posloupnost všech prvočísel. Potom existují kladné konstanty $k_1, k_2 \in \mathbb{R}$ takové, že pro každé $n \geqq 2$ platí*

$$k_1 n \ln n < p_n < k_2 n \ln n.$$

Důkaz. Vyjdeme ze znalosti první Čebyševovy věty, tj. Věty 2.28. Podle ní existují reálné konstanty $c_1, c_2 > 0$ takové, že vztah

$$c_1 \frac{x}{\ln x} < \pi(x) < c_2 \frac{x}{\ln x} \tag{2.38}$$

platí pro každé $x \geqq 2$. Musí tedy platit také pro libovolné $x = p_n$, $n \geqq 2$. Dosadíme-li $x = p_n$ do (2.38), obdržíme

$$c_1 \frac{p_n}{\ln p_n} < \pi(p_n) < c_2 \frac{p_n}{\ln p_n} \tag{2.39}$$

Prvočísel menších, nebo rovných n-tému prvočíslu p_n je evidentně celkem n. Proto $\pi(p_n) = n$. A tak z (2.28) plyne vztah

$$c_1 \frac{p_n}{\ln p_n} < n < c_2 \frac{p_n}{\ln p_n} \tag{2.40}$$

Nerovnost vpravo můžeme převést na tvar

$$p_n > \frac{1}{c_2} n \ln p_n$$

Dále využijeme toho, že n-té prvočíslo p_n je určitě větší než n. Symbolicky zapsáno $p_n > n$ (viz Cvičení 2.1.1 příklad 1. a jeho řešení v Kapitole 8). Protože logaritmus je rostoucí funkce, musí platit $\ln p_n > \ln n$. Proto

$$p_n > \frac{1}{c_2} n \ln p_n > \underbrace{\frac{1}{c_2}}_{k_1} n \ln n \tag{2.41}$$

Levou nerovnost v (2.40) můžeme převést na tvar

$$p_n < \frac{1}{c_1} n \ln p_n \tag{2.42}$$

a také

$$c_1 < \frac{n \ln p_n}{p_n} \tag{2.43}$$

Nyní uvažme, že $\lim_{x\to\infty} \frac{\ln x}{\sqrt{x}} = 0$.[1] To podle definice limity znamená, že existuje $x_0 \in \mathbb{R}$, $x_0 \geqq 3$ takové, že pro každé $p_n > x_0$ platí

$$\frac{\ln p_n}{\sqrt{p_n}} < c_1 \tag{2.44}$$

Spojením nerovností (2.43) a (2.44) dostáváme pro každé $p_n > x_0$

$$\frac{\ln p_n}{\sqrt{p_n}} < c_1 < \frac{n \ln p_n}{p_n},$$

$$\frac{\ln p_n}{\sqrt{p_n}} < \frac{n \ln p_n}{p_n}$$

$$\frac{1}{\sqrt{p_n}} < \frac{n}{p_n}$$

$$\sqrt{p_n} < n$$

$$p_n < n^2$$

$$\ln p_n < \ln n^2. \tag{2.45}$$

Z (2.42) a (2.45) plyne, že pro každé $p_n > x_0$ a $k \in \mathbb{N}$ platí

$$p_n < \frac{1}{c_1} n \ln p_n < \frac{1}{c_1} n \ln n^2 = \frac{2}{c_1} n \ln n \leqq \frac{2k}{c_1} n \ln n. \tag{2.46}$$

[1] S využitím l'Hospitalova pravidla: $\lim_{x\to\infty} \frac{\ln x}{\sqrt{x}} \overset{\text{l'H}}{=} \lim_{x\to\infty} \frac{\frac{1}{x}}{\frac{1}{2}x^{-\frac{1}{2}}} = \lim_{x\to\infty} \frac{2}{x^{\frac{1}{2}}} = 0.$

Zbývá prozkoumat případ, kdy $p_n \leqq x_0$, tj. případ kdy $2 \leqq n \leqq \pi(x_0)$. Definujme $m(n) = \frac{2}{c_1 p_n} n \ln n$ pro každé $n \in \{2, \ldots, \pi(x_0)\}$ a

$$m_0 = \min \left\{ \frac{2}{c_1 p_n} n \ln n \mid 2 \leqq n \leqq \pi(x_0) \right\}.$$

Potom platí $m_0 \leqq m(n)$ a jistě existuje $k \in \mathbb{N}$ takové, že $1 < k \cdot m_0$. Potom pro každé $n \in \{2, \ldots, \pi(x_0)\}$ platí

$$1 < k \cdot m_0 \leqq k \cdot m(n),$$

$$1 < \underbrace{\frac{2k}{c_1 p_n} n \ln n}_{k \cdot m(n)},$$

$$p_n < \frac{2k}{c_1} n \ln n. \tag{2.47}$$

Z nerovností (2.46) (platí pro $p_n > x_0$) a (2.47) (platí pro $3 \leqq p_n \leqq x_0$) plyne následující odhad platný pro každé $p_n \geqq 3$

$$p_n < \underbrace{\frac{2k}{c_1}}_{k_2} n \ln n. \tag{2.48}$$

Ze vztahů (2.41) a (2.48) plyne existence čísel $k_1, k_2 > 0$ takových, že pro každé $p_n \geqq 3$, tj. pro $n \geqq 2$ platí

$$k_1 n \ln n < p_n < k_2 n \ln n.$$

□

2.4.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.2.3.

1. Pomocí Lemmata 2.22 nalezněte kanonické rozklady čísel 7! a 20!.

2. Obdobně jako v Poznámce 2.16 odhadněte, kolik je prvočísel menších, nebo rovných 1 000.

3. Pokuste se vylepšit odhad $\pi(x) < 2(\ln 4)\frac{x}{\ln x} + \sqrt{x}$ uvedený ve Větě 2.26.

2.5 Bertrandův postulát

Bertrandův postulát je výsledek popisující jistou (byť nevalnou) pravidelnost ve výskytu prvočísel. Říká, že mezi číslem $n \in \mathbb{N}$, $n > 1$ a číslem $2n$ vždy existuje prvočíslo. Například zvolíme $n = 21$. Můžeme si pak být jisti, že existuje prvočíslo p splňující $21 < p < 42$.[1]

Zbytek této podkapitoly věnujeme důkazu Bertrandova postulátu. Pro ten budeme potřebovat následující lemmata.

Poznámka 2.30. V dalším textu této podkapitoly budeme používat označení

$$\beta(p) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right).$$

Lemma 2.31. *Pro každé $n > 1$ platí*

$$\prod_{\substack{p \in \mathbb{P} \\ p \leqq \sqrt{2n}}} p^{\beta(p)} \leqq (2n)^{(\sqrt{2n}-1)\frac{\ln 2n}{\ln 4}}.$$

Důkaz. Uvažujme $p \in \mathbb{P}$, $p \leqq \sqrt{2n}$. Nejprve zjistíme, pro která $k \in \mathbb{N}$ je $\left[\frac{2n}{p^k} \right] = 0$ (V tom případě je také $\left[\frac{n}{p^k} \right] = 0$, neboť $0 \leqq \left[\frac{n}{p^k} \right] \leqq \left[\frac{2n}{p^k} \right]$).

Snadno si rozmyslíme, že $\left[\frac{2n}{p^k} \right] = 0$ v případě, že $\frac{2n}{p^k} < 1$. A kdy je $\frac{2n}{p^k} < 1$? No určitě v případě, kdy $\frac{2n}{2^k} < 1$, neboť $p \geqq 2$. A tak

$$\frac{2n}{p^k} < \frac{2n}{2^k} < 1.$$

Hledáme tedy $k \in \mathbb{N}$ takové, aby platilo

$$\begin{aligned} \frac{2n}{2^k} &< 1, \\ 2n &< 2^k, \\ \ln(2n) &< \ln 2^k, \\ \ln(2n) &< k \ \ln 2, \\ k &> \frac{\ln(2n)}{\ln 2}. \end{aligned} \tag{2.49}$$

Můžeme si tak být jisti, že v případě, kdy k splňuje nerovnost (2.49), musí platit

$$\left[\frac{2n}{p^k} \right] = \left[\frac{n}{p^k} \right] = 0$$

[1] Snadno ověříme, že je jich dokonce pět. Jsou to prvočísla 23, 29, 31, 37 a 41.

A tak v případě $k > \frac{\ln(2n)}{\ln 2}$ je

$$\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] = 0.$$

Odtud dostáváme rovnost

$$\beta(p) = \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) = \sum_{k=1}^{\frac{\ln(2n)}{\ln 2}}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right).$$

Jak víme z příkladu 1. Cvičení 1.2.1 (viz jeho řešení v Kapitole 8), platí $0 \leqq \leqq \left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \leqq 1$. Proto

$$0 \leqq \beta(p) = \sum_{k=1}^{\frac{\ln(2n)}{\ln 2}}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) \leqq \frac{\ln(2n)}{\ln 2}. \tag{2.50}$$

Ze vztahu (2.50) plyne, že

$$\begin{aligned}\prod_{\substack{p\in\mathbb{P}\\ p\leqq\sqrt{2n}}} p^{\beta(p)} &\leqq \prod_{\substack{p\in\mathbb{P}\\ p\leqq\sqrt{2n}}} p^{\frac{\ln(2n)}{\ln 2}} \leqq \left((\sqrt{2n})^{\frac{\ln(2n)}{\ln 2}}\right)^{\pi(\sqrt{2n})} = \\ &= \left((2n)^{\frac{1}{2}\frac{\ln 2n}{\ln 2}}\right)^{\pi(\sqrt{2n})} = \left((2n)^{\frac{\ln 2n}{2.\ln 2}}\right)^{\pi(\sqrt{2n})}.\end{aligned} \tag{2.51}$$

Jak víme z příkladu 3. Cvičení 2.3.1, je $\pi(\sqrt{2n}) \leqq \sqrt{2n} - 1$. Z (2.51) pak plyne

$$\prod_{\substack{p\in\mathbb{P}\\ p\leqq\sqrt{2n}}} p^{\beta(p)} \leqq \left((2n)^{\frac{\ln 2n}{2.\ln 2}}\right)^{\pi(\sqrt{2n})} = (2n)^{\pi(\sqrt{2n})\frac{\ln 2n}{\ln 2^2}} \leqq (2n)^{(\sqrt{2n}-1)\frac{\ln 2n}{\ln 4}}.$$

□

Lemma 2.32. *Pro každé $n > 1$ platí*

$$\prod_{\substack{p\in\mathbb{P}\\ \sqrt{2n}<p\leqq\frac{2}{3}n}} p^{\beta(p)} < 4^{\frac{2}{3}n}.$$

Důkaz. Nejprve odhadneme hodnotu $\beta(p) = \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right)$.

Uvažujeme $\sqrt{2n} < p$. Proto Pro každé $k \geqq 2$ platí

$$2n = \left(\sqrt{2n}\right)^2 < p^2 \leqq p^k.$$

Odtud dostáváme pro každé $k \geqq 2$ nerovnosti

$$\begin{aligned} 2n &< p^k \\ \frac{2n}{p^k} &< 1 \end{aligned} \tag{2.52}$$

a navíc

$$0 \leqq \frac{n}{p^k} \leqq \frac{2n}{p^k} < 1.$$

Můžeme proto říci, že pro $k \geqq 2$ je $\left[\frac{2n}{p^k}\right] = 0 = \left[\frac{n}{p^k}\right]$. Proto

$$\beta(p) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \right) = \sum_{k=1}^{1} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \right) = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right].$$

Jak už víme (viz příklad 1. Cvičení 1.2.1), je $0 \leqq \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] \leqq 1$. Proto

$$0 \leqq \beta(p) \leqq 1 \tag{2.53}$$

Díky (2.53) a Důsledku 2.20 dostáváme

$$\prod_{\substack{p\in\mathbb{P} \\ \sqrt{2n}<p\leqq\frac{2}{3}n}} p^{\beta(p)} \leqq \prod_{\substack{p\in\mathbb{P} \\ \sqrt{2n}<p\leqq\frac{2}{3}n}} p \leqq \underbrace{\prod_{\substack{p\in\mathbb{P} \\ p\leqq\frac{2}{3}n}} p < 4^{\frac{2}{3}n}}_{\text{podle Důsledku 2.20}} . \tag{2.54}$$

□

Lemma 2.33. *Pro každé $n > 1$ platí*

$$\prod_{\substack{p\in\mathbb{P} \\ \frac{2}{3}n<p\leqq n}} p^{\beta(p)} = 1.$$

Důkaz. Podle Lemmata 2.24 pro každé $n \in \mathbb{N}$ platí

$$\prod_{\substack{p\in\mathbb{P} \\ p\leqq 2n}} p^{\beta(p)} = \binom{2n}{n}. \tag{2.55}$$

Proto existuje $K \in \mathbb{N}$ takové, že

$$\prod_{\substack{p\in\mathbb{P} \\ p\leqq 2n}} p^{\beta(p)} = K. \prod_{\substack{p\in\mathbb{P} \\ \frac{2}{3}n<p\leqq n}} p^{\beta(p)} = \binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{(n+1)(n+2)\cdots(2n)}{1\cdot 2\cdot 3\cdot \cdots \cdot n} \tag{2.56}$$

Uvažujme prvočísla p splňující

$$\frac{2}{3}n < p \leqq n \tag{2.57}$$

V součinu $1{\cdot}2{\cdot}3{\cdot}\cdots{\cdot}n$ se pak určitě vyskytuje prvočíslo p. Z toho plyne, že

$$1{\cdot}2{\cdot}3{\cdot}\cdots{\cdot}n = p{\cdot}s, \text{ kde } s \in \mathbb{N}. \tag{2.58}$$

Nyní obraťme pozornost na čitatele v (2.56), tj. součin $(n{+}1)(n{+}2)\cdots(2n)$. Které násobky prvočísla p se v něm vyskytují? Číslo $1p$ určitě ne, neboť $p \leqq n < n+1$. Číslo $2p$ ano, neboť z (2.57) dostáváme

$$n < 2\frac{2}{3}n < 2p \leqq 2n.$$

Násobek $3p$, ani žádný větší násobek p se v součinu $(n+1)(n+2)\cdots(2n)$ nevyskytuje, neboť

$$3p > 3\frac{2}{3}n = 2n.$$

Z výše uvedeného plyne, že

$$(n+1)(n+2)\cdots(2n) = p{\cdot}r, \text{ kde } \gcd(r,p) = 1. \tag{2.59}$$

Jednoduchou úpravou (2.56) obdržíme

$$(1{\cdot}2{\cdot}3{\cdot}\cdots{\cdot}n)K \prod_{\substack{p\in\mathbb{P}\\ \frac{2}{3}n<p\leqq n}} p^{\beta(p)} = (n+1)(n+2)\cdots(2n).$$

S využitím (2.58) a (2.59) pak

$$p{\cdot}sK \prod_{\substack{p\in\mathbb{P}\\ \frac{2}{3}n<p\leqq n}} p^{\beta(p)} = p{\cdot}r, \text{ kde } \gcd(r,p) = 1.$$

$$sK \prod_{\substack{p\in\mathbb{P}\\ \frac{2}{3}n<p\leqq n}} p^{\beta(p)} = r, \text{ kde } \gcd(r,p) = 1. \tag{2.60}$$

Číslo r není dělitelné prvočíslem p, kde $\frac{2}{3}n < p \leqq n$. Z (2.60) pak plyne, že pro prvočísla p, kde $\frac{2}{3}n < p \leqq n$ je $\beta(p) = 0$. A tak

$$\prod_{\substack{p\in\mathbb{P}\\ \frac{2}{3}n<p\leqq n}} p^{\beta(p)} = \prod_{\substack{p\in\mathbb{P}\\ \frac{2}{3}n<p\leqq n}} p^0 = 1.$$

□

Lemma 2.34. *Pro každé $n > 1$ platí*

$$\prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p^{\beta(p)} = \prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p.$$

Důkaz. Uvažujeme-li $n < p \leqq 2n$, pak pro $k \geqq 2$ evidentně platí

$$\frac{n}{p^k} < \frac{2n}{p^k} \leqq \frac{2n}{p^2} \leqq \frac{2n}{2.p} = \frac{n}{p} < 1.$$

Proto pro $k \geqq 2$ je

$$\left[\frac{n}{p^k}\right] = \left[\frac{2n}{p^k}\right] = 0.$$

A tak

$$\beta(p) = \sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right) = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right].$$

Opět využijeme příkladu 1. Cvičení 1.2.1, podle nějž je $0 \leqq \underbrace{\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]}_{=\beta(p)} \leqq 1.$

Navíc $\frac{2n}{p} \geqq 1$ a $\frac{p}{n} < 1$. Proto

$$1 \geqq \beta(p) = \underbrace{\left[\frac{2n}{p}\right]}_{\geqq 1} - \underbrace{2\left[\frac{n}{p}\right]}_{=0} \geqq 1.$$

To znamená, že

$$\beta(p) = 1,$$
$$\prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p^{\beta(p)} = \prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p.$$

□

Věta 2.35. (Bertrandův postulát) *Pro každé $n > 1$ existuje prvočíslo p takové, že*

$$n < p < 2n.$$

Důkaz. Označme

$$\prod_{\substack{p\in\mathbb{P}\\ p\leqq 2n}} p^{\beta(p)} = \underbrace{\prod_{\substack{p\in\mathbb{P}\\ p\leqq\sqrt{2n}}} p^{\beta(p)}}_{A(n)} \underbrace{\prod_{\substack{p\in\mathbb{P}\\ \sqrt{2n}<p\leqq\frac{2}{3}n}} p^{\beta(p)}}_{B(n)} \underbrace{\prod_{\substack{p\in\mathbb{P}\\ \frac{2}{3}n<p\leqq n}} p^{\beta(p)}}_{C(n)} \underbrace{\prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p^{\beta(p)}}_{X(n)} = A(n)B(n)C(n)X(n). \tag{2.61}$$

Podle Lemmatu 2.24 a 2.25 pro každé $n \geqq 2$ platí

$$\prod_{\substack{p\in\mathbb{P}\\ p\leqq 2n}} p^{\beta(p)} = \binom{2n}{n} > \frac{2^{2n}}{2n}. \tag{2.62}$$

Vzhledem k (2.61) a (2.62) můžeme psát

$$A(n)B(n)C(n)X(n) > \frac{2^{2n}}{2n}. \tag{2.63}$$

Lemata 2.31, 2.32, 2.33, resp. 2.34 říkají, že

$$\begin{aligned} (2n)^{(\sqrt{2n}-1)\frac{\ln 2n}{\ln 4}} &\geqq A(n)\\ 4^{\frac{2}{3}n} &> B(n)\\ 1 &= C(n)\\ \textstyle\prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p &= X(n) \end{aligned} \tag{2.64}$$

Na tomto místě už můžeme říci, že se dále budeme snažit dokázat, že pro $n > n_0$ platí $X(n) > 1$. V tom případě je od nějakého n_0 mezi n a $2n$ jistě nějaké prvočíslo (viz poslední vztah v 2.64). Poté dokážeme, že to platí i pro $n \leqq n_0$.

Z (2.63) a (2.64) plynou nerovnosti

$$\begin{aligned} \prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p = X(n) &> \frac{2^{2n}}{2n}\frac{1}{A(n)B(n)C(n)} = \frac{2^{2n}}{2n}\frac{1}{A(n)B(n)} > \\ > \frac{2^{2n}}{2n}\frac{1}{((2n)^{(\sqrt{2n}-1)\frac{\ln 2n}{\ln 4}})(4^{\frac{2}{3}n})} &= \frac{2^{2n}}{((2n)^{1+(\sqrt{2n}-1)\frac{\ln 2n}{\ln 4}})(2^{\frac{4}{3}n})} \geqq {}^{1}\\ \geqq \frac{2^{2n}}{((2n)^{\frac{\ln 2n}{\ln 4}+(\sqrt{2n}-1)\frac{\ln 2n}{\ln 4}})(2^{\frac{4}{3}n})} &= \frac{2^{2n-\frac{4}{3}n}}{(2n)^{(\sqrt{2n})\frac{\ln 2n}{\ln 4}}} = \\ = \frac{2^{\frac{2}{3}n}}{(2n)^{(\sqrt{2n})\frac{\ln 2n}{2\ln 2}}} \end{aligned} \tag{2.65}$$

Provedeme substituci $2^z = \sqrt{2n}$, tj. $z = \frac{\ln 2n}{2\ln 2}$. Tak obdržíme

$$\begin{aligned} \prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p = X(n) &> \frac{2^{\frac{2}{3}n}}{(2n)^{(\sqrt{2n})\frac{\ln 2n}{2\ln 2}}} = \frac{2^{\frac{2^{2z}}{3}}}{(2^{2z})^{2^z z}} = \\ = 2^{\frac{1}{3}2^{2z}-2^z 2z^2} &= 2^{\frac{2^z}{3}(2^z-6z^2)} = 2^{\frac{\sqrt{2n}}{3}(2^z-6z^2)} \end{aligned} \tag{2.66}$$

[1] Protože pro $n \geqq 2$ je $1 \leqq \frac{\ln 2n}{\ln 4}$

Uvažme, že pro $n > 1$ je $a = 2^{\frac{\sqrt{2n}}{3}} > 1$. Potom $X(n)$ je určitě větší než jedna pokud $2^z - 6z^2 > 0$, neboť z (2.66) dostáváme odhad

$$\prod_{\substack{p\in\mathbb{P}\\ n<p\leqq 2n}} p = X(n) > 2^{\frac{\sqrt{2n}}{3}(2^z-6z^2)} = a^{(2^z-6z^2)}. \tag{2.67}$$

Musíme proto zjistit, kdy je $2^z - 6z^2 > 0$. Nebude to nijak obtížné. Snadno ověříme, že na intervalu $(7, \infty)$ je funkce $g(z) = 2^z - 6z^2$ rostoucí [1] a $g(9) = 26 > 0$.

Takže pro každé $z \geqq 9$ je $g(z) > 0$. Proto můžeme říci, že $X(n) > 1$ (viz 2.67) pro každé $n \in \mathbb{N}$ splňující

$$\sqrt{2n} = 2^z \geqq 2^9$$
$$2n \geqq 2^{18}$$
$$n \geqq 2^{17} = 131\,072.$$

To ovšem znamená, že tvrzení věty je pravdivé pro každé $n \geqq 131\,072$ (tj. hledané $n_0 = 131\,072$ - viz výše).

Zbývá dokázat, že pro každé $n \in \mathbb{N}$, $1 < n < 131\,072$ existuje prvočíslo p splňující $n < p < 2n$. Využijeme existence následujících prvočísel

2, 3 5, 7, 13, 23, 43, 83, 163, 317, 631, 1 259, 2 503, 4 993, 9 973, 19 937, 39 869, 79 699, 159 389.

Označme tyto prvočísla (ve stejném pořadí) $q_1, q_2, \ldots, q_{19}$. Všimněte si, že pro každé $i \in \{1, 2, \ldots, 18\}$ platí[2]

$$q_{i+1} < 2q_i.$$

Navíc pro každé $n \in \mathbb{N}$, $1 < n < 131\,072$ existuje q_i a q_{i+1} takové, že

$$q_i \leqq n < q_{i+1} < 2q_i \leqq 2n.$$

Z toho je patrné, že pro každé $n \in \mathbb{N}$, $1 < n < 131\,072$ existuje prvočíslo q_{i+1} splňující

$$n < q_{i+1} \leqq 2n.$$

Číslo $2n$ určitě není prvočíslo, a tak

$$n < q_{i+1} < 2n.$$

□

[1] Derivace funkce $g(z)$ je $g'(z) = 2^z \ln 2 - 12z$. Pokud $g'(z) = 2^z \ln 2 - 12z > 0$, je $g(z)$ rostoucí. Pro hledání z splňujících $g'(z) = 2^z \ln 2 - 12z > 0$ využijeme druhou derivaci $g(z)$, tj. $g''(z)$.

Pokud $g''(z) = 2^z (\ln 2)^2 - 12 > 0$, pak je $g'(z)$ rostoucí funkce. Snadno ověříme, že v případě $z \geqq 5$ je $g''(z) = 2^z (\ln 2)^2 - 12 > 0$. Takže na intervalu $(5, \infty)$ je $g'(z)$ rostoucí funkce a platí $g'(6,95) \doteq 2,3 > 0$. Proto pro každé $z \geqq 7$ je $g'(z) > g'(6,95) > 0$. To znamená, že na intervalu $(7, \infty)$ je $g(z)$ určitě rostoucí funkce.

[2] Každé z těchto prvočísel je menší než dvojnásobek předcházejícího.

2.6 Další vlastnosti

Zde odvodíme vlastnosti množiny prvočísel, které využijeme v Kapitole 3. Proto bude sestávat pouze z lemmat, jejichž konkrétní použití v teorii čísel bude čtenáři objasněno později. (Pokud nemáte rádi překvapení, pak se autor omlouvá za sníženou čtivost této podkapitoly.)

Dokážete určit součet čísel $\sum_{k=1}^{4} \frac{1}{k} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}$? Nic těžkého, že? Zvláště, je-li po ruce kalkulačka. Ale zkuste určit

$$\sum_{k=1}^{1\,000\,000} \frac{1}{k} = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{1\,000\,000}.$$

Asi to bude horší. Nebo ne? Od čeho máme výpočetní techniku! Ale i ta má své limity a i ona se začne psychicky hroutit, pokud po ní budeme chtít určit součet $\sum_{k \leqq x} \frac{1}{k}$ pro stále větší a větší x. A co kdybychom po ní chtěli nějaký, poměrně jednoduchý, předpis, jak určit hodnotu

$$f(x) = \sum_{k \leqq x} \frac{1}{k}?$$

a nedali jí **žádný** konkrétní návod, jak na to!

V blízké budoucnosti zřejmě žalostně zklame. Proto nezbývá, než dát prostor starému dobrému lidskému intelektu a dokázat následující lemma. Neurčíme pomocí něj hodnotu $f(x) = \sum_{k \leqq x} \frac{1}{k}$ přesně, ale získáme s její pomocí poměrně slušný odhad, jak se tento součet chová při $x \to \infty$. Zjistíme, že pro „velká“ x je hodnota $f(x) = \sum_{k \leqq x} \frac{1}{k}$ přibližně rovna $\ln x + \gamma$.

Lemma 2.36. *Pro každé $x \in \mathbb{R}$, $x \geqq 1$ platí*

$$f(x) = \sum_{\substack{k \leqq x \\ k \in \mathbb{N}}} \frac{1}{k} = \ln x + \gamma + O\left(\frac{1}{x}\right),$$

kde $\gamma \in (0,1)$ je takzvaná Eulerova konstanta (její přibližná hodnota je $0,577\,215$).[1]

[1] Tj. $f(x) = \sum_{k \leqq x} \frac{1}{k} = \ln x + \gamma + g(x)$, kde $g(x) = O\left(\frac{1}{x}\right)$. To znamená, že $\limsup_{x \to \infty} \frac{|g(x)|}{\frac{1}{x}} =$ konstanta. Odtud $\lim_{x \to \infty} |g(x)| = \lim_{x \to \infty} \frac{1}{x} \frac{|g(x)|}{\frac{1}{x}} = 0$. A tak $O\left(\frac{1}{x}\right) = o(1)$. Tj. pro „velká“ x dostáváme odhad $f(x) = \sum_{k \leqq x} \frac{1}{k} = \ln x + \gamma +$ *zanedbatelně malé číslo.* $O\left(\frac{1}{x}\right)$, viz též podkapitola 0.2.

Důkaz. Připomeneme-li si definici Riemannova integrálu, jsou pro každé $k \in \mathbb{N}$ zřejmé nerovnosti

$$\frac{1}{k+1} < \int_k^{k+1} \frac{1}{t}\mathrm{d}t < \frac{1}{k},$$

z nichž jednoduchými úpravami dostaneme

$$0 < \frac{1}{k} - \int_k^{k+1} \frac{1}{t}\mathrm{d}t < \frac{1}{k} - \frac{1}{k+1}. \tag{2.68}$$

Proto pro každé $n \in \mathbb{N}$ platí

$$0 < \sum_{k \leqq n} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\mathrm{d}t \right) < \sum_{k \leqq n} \left(\frac{1}{k} - \frac{1}{k+1} \right). \tag{2.69}$$

Protože

$$\sum_{k \leqq n} \left(\frac{1}{k} - \frac{1}{k+1} \right) = \left(\frac{1}{1} - \frac{1}{2} \right) + \left(\frac{1}{2} - \frac{1}{3} \right) + \cdots + \left(\frac{1}{n} - \frac{1}{n+1} \right) = \frac{1}{1} - \frac{1}{n+1}, \tag{2.70}$$

dostáváme z (2.69) pro každé $n \in \mathbb{N}$

$$0 < \sum_{k \leqq n} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\mathrm{d}t \right) < 1 - \frac{1}{n+1}. \tag{2.71}$$

Označme $\gamma = \sum\limits_{k \leqq \infty} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\mathrm{d}t \right)$. Využijeme-li srovnávacího kritéria, pak je z (2.69), (2.70) a (2.71) zřejmé, že tento součet řady opravdu existuje a platí

$$0 < \gamma = \sum_{k \leqq \infty} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\mathrm{d}t \right) < \lim_{n \to \infty} \left(1 - \frac{1}{n+1} \right) = 1.$$

Tj. $0 < \gamma < 1$. Podle výše uvedeného označení je

$$\gamma = \sum_{k \leqq \infty} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\mathrm{d}t \right) = \sum_{k \leqq n} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\mathrm{d}t \right) + \underbrace{\sum_{k=n+1}^{\infty} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\mathrm{d}t \right)}_{\text{označme } f(n)}. \tag{2.72}$$

Nyní odhadneme hodnotu $f(n)$. Vzhledem k (2.68) je $f(n) > 0$ pro každé $n \in \mathbb{N}$ a navíc

$$\begin{aligned} f(n) &= \sum_{k=n+1}^{\infty} \left(\tfrac{1}{k} - \int_k^{k+1} \tfrac{1}{t}\mathrm{d}t \right) < \sum_{k=n+1}^{\infty} \left(\tfrac{1}{k} - \tfrac{1}{k+1} \right) = \\ &= \left(\tfrac{1}{n+1} - \tfrac{1}{n+2} \right) + \left(\tfrac{1}{n+2} - \tfrac{1}{n+3} \right) + \cdots + \left(\tfrac{1}{n+m} - \tfrac{1}{k+m+1} \right) + \cdots = \\ &= \lim_{m \to \infty} \left(\tfrac{1}{n+1} - \tfrac{1}{k+m+1} \right) = \tfrac{1}{n+1}. \end{aligned}$$

Proto $f(n) = O\left(\frac{1}{n}\right)$. Dosadíme-li do (2.72), musí pro každé $n \in \mathbb{N}$ platit

$$\begin{aligned}
\gamma &= \sum_{k\leqq n}\left(\tfrac{1}{k} - \int_k^{k+1}\tfrac{1}{t}\mathrm{d}t\right) + O\left(\tfrac{1}{n}\right) = \\
&= \sum_{k\leqq n}\left(\tfrac{1}{k}\right) - \sum_{k\leqq n}\left(\int_k^{k+1}\tfrac{1}{t}\mathrm{d}t\right) + O\left(\tfrac{1}{n}\right) = \\
&= \sum_{k\leqq n}\tfrac{1}{k} - \int_{k=1}^{n+1}\tfrac{1}{t}\mathrm{d}t + O\left(\tfrac{1}{n}\right) = \\
&= \sum_{k\leqq n}\tfrac{1}{k} - \ln(n+1) - \underbrace{\ln 1}_{0} + O\left(\tfrac{1}{n}\right) = \\
&= \sum_{k\leqq n}\tfrac{1}{k} - (\ln(n+1) - \ln n) - \ln n + O\left(\tfrac{1}{n}\right) = \\
&= \sum_{k\leqq n}\tfrac{1}{k} - \ln\tfrac{n+1}{n} - \ln n + O\left(\tfrac{1}{n}\right).
\end{aligned} \tag{2.73}$$

Uvažme, že

$$\lim_{n\to\infty}\frac{-\ln\frac{n+1}{n}}{\frac{1}{n}} = \lim_{n\to\infty} -n\ln\left(1+\frac{1}{n}\right) = \lim_{n\to\infty} -\ln\left(1+\frac{1}{n}\right)^n = -\ln\mathrm{e} = -1.$$

Proto je $-\ln\frac{n+1}{n} = O\left(\frac{1}{n}\right)$. Dosadíme-li do (2.73), obdržíme vztah[1]

$$\gamma = \sum_{k\leqq n}\frac{1}{k} - \ln n + O\left(\frac{1}{n}\right).$$

A odtud jednoduchou úpravou[2] odvodíme, že pro každé $n \in \mathbb{N}$ platí

$$\sum_{k\leqq n}\frac{1}{k} = \ln n + \gamma + O\left(\frac{1}{n}\right). \tag{2.74}$$

My však potřebujeme dokázat, že pro každé $x \in \mathbb{R}$ platí $\sum_{k\leqq x}\frac{1}{k} = \ln x + \gamma + O\left(\frac{1}{x}\right)$. To nebude těžké. označme $n = [x]$ a $\varepsilon_x = x - [x]$. Potom evidentně $0 \leqq \varepsilon_x < 1$

[1] Je třeba si uvědomit, že $-\ln\frac{n+1}{n} + O\left(\frac{1}{n}\right) = O\left(\frac{1}{n}\right) + O\left(\frac{1}{n}\right) = O\left(\frac{1}{n}\right)$, neboť $O\left(\frac{1}{n}\right)$ není konkrétní funkce (posloupnost), ale symbol zastupující funkci (posloupnost) splňující určitou podmínku (viz podkapitola 0.2).

[2] Uvažte, že $-O\left(\frac{1}{n}\right) = O\left(\frac{1}{n}\right)$

a podle (2.74) platí[1]

$$\begin{aligned}
\sum_{k\leqq x}\tfrac{1}{k} &= \sum_{k\leqq [x]}\tfrac{1}{k} = \sum_{k\leqq n}\tfrac{1}{k} = \ln n + \gamma + O\left(\tfrac{1}{n}\right) = \\
&= \ln n + \ln x - \ln x + \gamma + O\left(\tfrac{1}{x}\right) = \\
&= \ln x - (\ln x - \ln [x]) + \gamma + O\left(\tfrac{1}{x}\right) = \\
&= \ln x - (\ln ([x] + \varepsilon_x) - \ln [x]) + \gamma + O\left(\tfrac{1}{x}\right) = \\
&= \ln x - \ln \tfrac{([x]+\varepsilon_x)}{[x]} + \gamma + O\left(\tfrac{1}{x}\right) = \\
&= \ln x - \underbrace{\ln\left(1 + \frac{\varepsilon_x}{[x]}\right)}_{=O\left(\frac{1}{x}\right)} + \gamma + O\left(\tfrac{1}{x}\right) = \\
&= \ln x + \gamma + O\left(\tfrac{1}{x}\right)
\end{aligned} \tag{2.75}$$

□

Obdobným způsobem odhadneme hodnotu $\sum_{k\leqq x} \ln k = \ln 1 + \ln 2 + \cdots + \ln [x]$.

Lemma 2.37. *Pro každé $x \in \mathbb{R}$, $x \geqq 2$ platí*

$$\sum_{k\leqq x} \ln k = x \ln x - x + O(\ln x)$$

Důkaz. Z definice Riemannova integrálu a vlastností funkce $f(t) = \ln t$ plyne, že pro libovolné $k \in \mathbb{N}$, $k \geqq 2$ jsou splněny nerovnosti

$$\int_{k-1}^{k} \ln t \,\mathrm{d}t \leqq \ln k \leqq \int_{k}^{k+1} \ln t \,\mathrm{d}t.$$

Označíme-li $[x] = n$, pak musí platit

$$\sum_{k=2}^{n} \left(\int_{k-1}^{k} \ln t \,\mathrm{d}t\right) \leqq \sum_{k=2}^{n} \ln k \leqq \sum_{k=2}^{n} \left(\int_{k}^{k+1} \ln t \mathrm{d}t\right). \tag{2.76}$$

[1] Využijeme toho, že $0 \leqq \limsup_{x\to\infty} \frac{\ln\left(1+\frac{\varepsilon_x}{[x]}\right)}{\frac{1}{x}} \leqq \lim_{x\to\infty} \ln\left(1+\frac{1}{x-1}\right)^x = 1$. Proto $\ln\left(1+\frac{\varepsilon_x}{[x]}\right) = O\left(\frac{1}{x}\right)$.

Protože $\ln 1 = 0$, je $\sum\limits_{k\leqq x} \ln k = \sum\limits_{k=1}^{n} \ln k = \sum\limits_{k=2}^{n} \ln k$. A tak z (2.76) plyne odhad

$$\int_1^n \ln t \,\mathrm{d}t \leqq \sum_{k\leqq x} \ln k \leqq \int_2^{n+1} \ln t \,\mathrm{d}t.$$

$$\int_1^n \ln t \,\mathrm{d}t \leqq \sum_{k\leqq x} \ln k \leqq \int_1^{n+1} \ln t \,\mathrm{d}t. \tag{2.77}$$

Z (2.77) dostáváme

$$0 \leqq \sum_{k\leqq x} \ln k - \int_1^n \ln t \,\mathrm{d}t \leqq \int_1^{n+1} \ln t \,\mathrm{d}t - \int_1^n \ln t \,\mathrm{d}t = \int_n^{n+1} \ln t \,\mathrm{d}t. \tag{2.78}$$

Funkce $\ln t$ je rostoucí a na intervalu $(n, n+1)$ nabývá kladných hodnot. A tak platí (viz Cvičení podkapitoly 0.2)

$$\int_n^{n+1} \ln t \,\mathrm{d}t \leqq \ln(n+1) \leqq \ln(x+1) = O(\ln x). \tag{2.79}$$

Z (2.78) proto plyne

$$\sum_{k\leqq x} \ln k - \int_1^n \ln t \,\mathrm{d}t = O(\ln x)$$

$$\sum_{k\leqq x} \ln k = \int_1^n \ln t \,\mathrm{d}t + O(\ln x) \tag{2.80}$$

Uvažme, že $n \leqq x < n+1$ a tak, podle (2.79), musí platit

$$0 \leqq \int_n^x \ln t \,\mathrm{d}t \leqq \int_n^{n+1} \ln t \,\mathrm{d}t = O(\ln x). \tag{2.81}$$

Z (2.80) a (2.81) vyplývá (viz též cvičení Podkapitoly 0.2), že

$$\sum_{k\leqq x} \ln k \underbrace{=}_{\text{podle (2.80)}} \int_1^n \ln t \,\mathrm{d}t + O(\ln x) =$$

$$= \int_1^x \ln t \,\mathrm{d}t - \underbrace{\int_n^x \ln t \,\mathrm{d}t}_{=O(\ln x)\ \text{podle (2.81)}} + O(\ln x) =$$

$$= \int_1^x \ln t \,\mathrm{d}t + \underbrace{O(\ln x) + O(\ln x)}_{=O(\ln x)} =$$

$$= x \ln x - x \underbrace{-(1.\ln 1 - 1)}_{O(\ln x)} + O(\ln x) =$$

$$= x \ln x - x + O(\ln x).$$

□

Lemma 2.38. (Mertensova první věta) *Nechť $x \geqq 2$. Potom platí*

$$\sum_{\substack{p \leqq x \\ p \in \mathbb{P}}} \frac{\ln p}{p} = \ln x + O(1).$$

Důkaz. Označme $n = [x]$. Podle Důsledku 2.23 platí

$$n! = \prod_{p \leqq n} p^{\alpha(p)}, \text{ kde } \alpha(p) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]. \tag{2.82}$$

Navíc pro každé $x \in \mathbb{R}$, $p \in \mathbb{P}$ a $k = 1, 2, \ldots$ platí (viz Cvičení 1.2.1)

$$\left[\frac{x}{p^k} \right] = \left[\frac{n}{p^k} \right]. \tag{2.83}$$

Proto (podle (2.82) a (2.83)) je v případě $n = [x]$ splněna rovnost

$$n! = \prod_{p \leqq n} p^{\alpha(p)}, \text{ kde } \alpha(p) = \sum_{k=1}^{\infty} \left[\frac{x}{p^k} \right]. \tag{2.84}$$

Uvažme, že

$$\ln n! = \ln(1 \cdot 2 \cdot \cdots n) = \ln 1 + \ln 2 + \cdots + \ln n = \sum_{k \leqq n} \ln k \tag{2.85}$$

a

$$\ln \left(\prod_{p \leqq n} p^{\alpha(p)} \right) = \sum_{p \leqq n} \ln p^{\alpha(p)} = \sum_{p \leqq n} \alpha(p) \ln p = \sum_{p \leqq n} \underbrace{\left(\sum_{k=1}^{\infty} \left[\frac{x}{p^k} \right] \right)}_{\alpha(p)} \ln p. \tag{2.86}$$

Z (2.84) plyne, že

$$\ln n! = \ln \left(\prod_{p \leqq n} p^{\alpha(p)} \right).$$

A tak, podle (2.85) a (2.86) musí platit

$$\sum_{k\leqq n}\ln k=\sum_{p\leqq n}\left(\sum_{k=1}^{\infty}\left[\frac{x}{p^k}\right]\right)\ln p.$$

$$\sum_{k\leqq n}\ln k=\sum_{p\leqq n}\left(\sum_{\substack{k\in\mathbb{N}\\ p^k\leqq x}}\left[\frac{x}{p^k}\right]\right)\ln p.$$

$$\sum_{k\leqq n}\ln k=\sum_{p\leqq n}\left(\left[\frac{x}{p}\right]+\left[\frac{x}{p^2}\right]+\left[\frac{x}{p^3}\right]+\cdots\right)\ln p.$$

$$\sum_{p\leqq n}\left[\frac{x}{p}\right]\ln p=\sum_{k\leqq n}\ln k-\sum_{p\leqq n}\left(\left[\frac{x}{p^2}\right]+\left[\frac{x}{p^3}\right]+\cdots\right)\ln p.$$

$$\frac{1}{x}\sum_{p\leqq n}\left[\frac{x}{p}\right]\ln p=\frac{1}{x}\sum_{k\leqq n}\ln k-\frac{1}{x}\sum_{p\leqq n}\left(\left[\frac{x}{p^2}\right]+\left[\frac{x}{p^3}\right]+\cdots\right)\ln p. \tag{2.87}$$

Podle Lemmatu 2.37 je $\sum\limits_{k\leqq n}\ln k=x\ln x-x+O(\ln x)$. Dosadíme-li do (2.87), obdržíme

$$\frac{1}{x}\sum_{p\leqq n}\left[\frac{x}{p}\right]\ln p=\frac{1}{x}\left(x\ln x-x+O(\ln x)\right)-\frac{1}{x}\sum_{p\leqq n}\left(\left[\frac{x}{p^2}\right]+\left[\frac{x}{p^3}\right]+\cdots\right)\ln p,$$

$$\frac{1}{x}\sum_{p\leqq n}\left[\frac{x}{p}\right]\ln p=\ln x-1+\frac{1}{x}O(\ln x)-\frac{1}{x}\sum_{p\leqq n}\left(\left[\frac{x}{p^2}\right]+\left[\frac{x}{p^3}\right]+\cdots\right)\ln p. \tag{2.88}$$

Protože $-1+\frac{1}{x}O(\ln x)=O(1)$ (viz Cvičení 0.2.1) můžeme psát

$$\frac{1}{x}\sum_{p\leqq n}\left[\frac{x}{p}\right]\ln p=\ln x+O(1)-\underbrace{\frac{1}{x}\sum_{p\leqq n}\left(\left[\frac{x}{p^2}\right]+\left[\frac{x}{p^3}\right]+\cdots\right)\ln p}_{\text{označme A}}. \tag{2.89}$$

Nyní odhadneme hodnotu A [1] .

$$\begin{aligned} A &= \frac{1}{x}\sum_{p\leqq n}\left(\left[\frac{x}{p^2}\right]+\left[\frac{x}{p^3}\right]+\cdots\right)\ln p \quad \leqq \\ &\leqq \sum_{p\leqq n}\left(\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)\ln p \qquad \leqq \\ &\leqq \sum_{p\leqq n}\underbrace{\left(\frac{1}{p}+\frac{1}{p^2}+\cdots\right)}_{\text{součet geometrické řady}}\ln p \qquad = \\ &= \sum_{p\leqq n}\frac{\ln p}{p(p-1)} \leqq \sum_{k=2}^{\infty}\frac{\ln k}{k(k-1)} \qquad = \underbrace{O(1)}_{\text{viz 2.6.1 Cvičení}} \end{aligned} \tag{2.90}$$

A tak $A = O(1)$. Dosazením do (2.89) obdržíme ($O(1) - O(1) = O(1)$)

$$\frac{1}{x}\sum_{p\leqq n}\left[\frac{x}{p}\right]\ln p = \ln x + O(1) \tag{2.91}$$

Jak víme, dané číslo (např. α) je součtem jeho celé a zlomkové části (tj. $\alpha = [\alpha] + \{\alpha\}$). proto.

$$\frac{1}{x}\sum_{p\leqq n}\frac{x}{p}\ln p = \frac{1}{x}\sum_{p\leqq n}\left[\frac{x}{p}\right]\ln p + \frac{1}{x}\sum_{p\leqq n}\left\{\frac{x}{p}\right\}\ln p. \tag{2.92}$$

Z (2.91) pak plyne

$$\frac{1}{x}\sum_{p\leqq n}\frac{x}{p}\ln p = \ln x + O(1) + \underbrace{\frac{1}{x}\sum_{p\leqq n}\left\{\frac{x}{p}\right\}\ln p}_{\text{označme } B}. \tag{2.93}$$

Dokážeme, že $B = O(1)$ (připomeňme, že $n = [x]$).

$$\begin{aligned} B &= \frac{1}{x}\sum_{p\leqq n}\underbrace{\left\{\frac{x}{p}\right\}}_{<1}\ln p \leqq \frac{1}{x}\sum_{p\leqq n}\ln p \leqq \frac{1}{x}\sum_{p\leqq x}\ln x = \\ &= \frac{1}{x}\left(\underbrace{\ln x + \ln x + \cdots + \ln x}_{\pi(x)\text{- krát}}\right) = \frac{1}{x}\pi(x)\ln x. \end{aligned} \tag{2.94}$$

[1] První nerovnost plyne z toho, že $\frac{1}{x}\left[\frac{x}{p^k}\right] \leqq \frac{1}{p^k}$, viz Cvičení 1.2.1

Podle Věty 2.28 (Čebyševova) existuje $c_2 \in \mathbb{R}^+$ takové, že

$$\pi(x) < c_2 \frac{x}{\ln x}.$$

Tzn.

$$\frac{1}{x}\pi(x) \ln x < c_2.$$

Ze vztahu (2.94) tak dostáváme

$$B = \frac{1}{x} \sum_{p \leqq n} \left\{ \frac{x}{p} \right\} \ln p \leqq c_2$$

A proto $B = O(1)$. Dosazením do (2.93) obdržíme rovnost

$$\frac{1}{x} \sum_{p \leqq n} \frac{x}{p} \ln p = \ln x + \underbrace{O(1) + O(1)}_{=O(1)}.$$

Krácením x a protože $n = [x]$, dostáváme dokazované tvrzení Lemmatu

$$\sum_{p \leqq x} \frac{1}{p} \ln p = \ln x + O(1).$$

□

2.6.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.2.4.

1. Dokažte, že $\sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} = O(1)$. (Návod: Dokažte existenci čísla $c \in \mathbb{R}$ takového, že $\sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} \leqq c = konst. \in \mathbb{R}$. Použijte myšlenku integrálního kritéria konvergence řady. Integrujte per partes.)

2. Dokažte, že pro každé $n \in \mathbb{N}$ platí

$$\sum_{k \leqq n} \frac{1}{k} = \ln(n+1) + \gamma + g(n),$$

kde $\gamma \in (0,1)$ je Eulerova konstanta, a $g(n)$ je funkce splňující pro každé $n \in \mathbb{N}$ nerovnosti

$$-\frac{1}{n+1} < g(n) < 0.$$

Kapitola 3

Hustoty množin

Co je to hustota množiny? Význam tohoto pojmu si předvedeme na konkrétním příkladě.

Uvažujme množinu všech sudých přirozených čísel. Jak hustě jsou její prvky rozloženy v množině všech přirozených čísel? Vážený čtenář si jistě dokáže odpovědět sám. Sudé číslo je každé druhé mezi všemi přirozenými čísly. To nás vede k intuitivnímu závěru, že sudé čísla tvoří 50% všech přirozených čísel.

Další příklad? Uvažujeme všechny násobky čísla 3. Na číselné ose představují každé třetí přirozené číslo. Docházíme intuitivně k závěru, že násobky trojky tvoří $33,\overline{3}\%$ přirozených čísel. [1]

U ostatních množin $A \subseteq \mathbb{N}$ si můžeme položit obdobnou otázku, a to jak velkou část množiny všech přirozených čísel tvoří. A přesně to by měla vystihovat hustota množiny A.

Způsobů, jak tento poměr odhadnout, je více, a tak existují různé hustoty množin. My se v dalším textu budeme zabývat *asymptotickou*, *logaritmickou* a *Schnirelmannovou hustotou* množiny $A \subseteq \mathbb{N}$.

Definice 3.1. V dalším textu bude symbol $A(n)$ označovat počet prvků množiny $A \subseteq N$, které jsou menší, nebo rovny n, tzn.

$$A(n) = \sum_{a \in A, a \leq n} 1$$

Například, je-li A množina všech lichých čísel, pak právě čtyři prvky z A jsou menší, nebo rovny 7. Proto je v tomto případě $A(7) = 4$.

[1] Vidíme, že násobků trojky je v jistém smyslu méně než sudých čísel, ač obě množiny jsou nekonečné!

3.1 Asymptotická hustota

Zamysleme se, jak určit poměr počtu prvků množiny $A \subseteq \mathbb{N}$ ku počtu prvků množiny $\mathbb{N}$. Pokud je A konečná množina, je to triviální. Počet prvků A je zanedbatelný vzhledem k počtu prvků $\mathbb{N}$.

Co však v případě, kdy je množina A nekonečná? Tento poměr nemůžeme určit jako podíl dvou čísel[1], ale můžeme se k němu limitně přibližovat! Jak? Pro libovolné $n \in \mathbb{N}$ můžeme určit poměr

$$\frac{A(n)}{n}.$$

Ten označuje (viz Definice 3.1) poměr počtu prvků množiny A ku počtu prvků množiny $\mathbb{N}$, ale uvažujeme pouze ty prvky z A a $\mathbb{N}$, které jsou menší, nebo rovny n.[2] Pokud chceme odhadnout poměr počtu všech prvků množiny A ku počtu všech prvků množiny $\mathbb{N}$, musíme zvětšovat n nade všechny meze. To jest, hledáme hodnotu

$$\lim_{n\to\infty} \frac{A(n)}{n}.$$

Jak víme z matematické analýzy, limita dané posloupnosti nemusí nutně existovat, ale určitě existuje limes superior a limes inferior dané posloupnosti. A tedy i posloupnosti $d_n = \frac{A(n)}{n}$. Proto asymptotickou hustotu množiny A definujeme následovně.

[1] $\frac{\infty}{\infty}$ není definováno!

[2] Počet prvků množiny A, které jsou menší, nebo rovny n je $A(n)$. Počet prvků množiny $\mathbb{N}$, které jsou menší, nebo rovny n je n.

Definice 3.2. (*Asymptotická hustota*) Nechť $A \subseteq N$. Horní asymptotickou hustotou[a] množiny A nazýváme číslo

$$\bar{d}(A) = \limsup_{n\to\infty} \frac{A(n)}{n}.$$

Dolní asymptotickou hustotou množiny A nazýváme číslo

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{A(n)}{n}.$$

Jestliže $\bar{d}(A) = \underline{d}(A)$, pak hodnotu

$$d(A) = \bar{d}(A) = \underline{d}(A) = \lim_{n\to\infty} \frac{A(n)}{n}.$$

nazýváme asymptotickou hustotou množiny A.

[a]Připomeňme, že limes superior posloupnosti d_n značíme $\limsup_{n\to\infty} d_n$ a jedná se o největší hromadný bod posloupnosti d_n. Například, vezmeme-li posloupnost $-1+\frac{1}{2}, 0+\frac{1}{2}, 1+\frac{1}{2}, -1+\frac{1}{3}, 0+\frac{1}{3}, 1+\frac{1}{3}, \ldots, -1+\frac{1}{n}, 0+\frac{1}{n}, 1+\frac{1}{n}, \ldots$, pak hromadnými body této posloupnosti jsou body 0, 1 a -1, neboť v jejich (i libovolně malém) okolí se nachází nekonečně mnoho prvků dané posloupnosti. Proto je limes superior této posloupnosti rovno 1 a limes inferior (nejmenší hromadný bod posloupnosti) je rovno -1.

Uvedeme některé vlastnosti asymptotické hustoty množiny (tyto vlastnosti budou dokázány v rámci cvičení). $A \subseteq \mathbb{N}$.

1. Pro každou množinu $A \subseteq \mathbb{N}$ existuje její horní a dolní asymptotická hustota $\bar{d}(A)$, respektive $\underline{\mathrm{d}}(A)$, ale nemusí existovat asymptotická hustota $d(A)$.

2. Pro každou množinu $A \subseteq \mathbb{N}$ platí, že $0 \leqq \underline{\mathrm{d}}(A) \leqq \bar{d}(A) \leqq 1$.

3. Existují množiny, jejichž asymptotická hustota splňuje $d(A) = 1$ a přesto $A \neq \mathbb{N}$. Jde například o množiny typu $A = \mathbb{N} - K$, kde K je neprázdná konečná podmnožina množiny přirozených čísel.

4. Existují nekonečné množiny, jejichž asymptotická hustota splňuje $d(A) = 0$. Například množina $A = \{n^2 \mid n \in \mathbb{N}\}$, nebo množina všech prvočísel.

5. Přidáme-li, nebo odebereme-li z dané množiny A konečný počet prvků, pak asymptotická hustota výsledné množiny je stejná jako asymptotická hustota množiny A. Tj. pokud $A, K \subseteq \mathbb{N}$, K je konečná množina, pak $d(A \cup K) = d(A)$ a také $d(A - K) = d(A)$.

Příklad 3.3. Nalezněte asymptotickou hustotu množiny $A = \{4k - 1 \mid k \in \mathbb{N}\}$.

Řešení:

Podle zadání množina A obsahuje čísla 3, 7, 11, 15, ... Abychom určili $d(A)$, musíme znát $A(n)$. Tj. musíme určit, kolik prvků množiny A je menších, nebo rovných n. Jinak řečeno, hledáme odpověď na otázku, pro která $k \in \mathbb{N}$ platí

$$4k - 1 \leqq n.$$

Úpravami této nerovnosti dostáváme

$$4k \leqq n + 1,$$

$$k \leqq \frac{n}{4} + \frac{1}{4}. \tag{3.1}$$

Pokud si situaci představíme na číselné ose, je zřejmé, že čísel $k \in \mathbb{N}$ splňujících nerovnost (3.1) je právě $\left[\frac{n}{4} + \frac{1}{4}\right]$.[1] Proto

$$A(n) = \left[\frac{n}{4} + \frac{1}{4}\right] = \frac{n}{4} + \frac{1}{4} - \varepsilon_n,$$

kde $0 \leqq \varepsilon_n < 1$ pro každé $n \in \mathbb{N}$.

Odtud dostáváme

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = \lim_{n\to\infty} \frac{\frac{n}{4} + \frac{1}{4} - \varepsilon_n}{n} = \lim_{n\to\infty} \left(\frac{1}{4} + \frac{1}{4n} - \frac{\varepsilon_n}{n}\right) = \frac{1}{4}.$$

Výsledek můžeme interpretovat tak, že čísla ve tvaru $4k - 1$, kde $k \in \mathbb{N}$ tvoří jednu čtvrtinu všech přirozených čísel.

Nyní pomocí dříve nabytých vědomostí dokážeme, že asymptotická hustota množiny všech prvočísel je rovna nule. Znamená to, že prvočísel je mezi všemi přirozenými čísly zanedbatelně málo.

Věta 3.4. *Nechť $\mathbb{P}$ je množina všech prvočísel. Potom $d(\mathbb{P}) = 0$.*

Důkaz. Podle Definice 2.12 a 3.1 je $\mathbb{P}(n) = \pi(n)$. Navíc podle první Čebyševovy věty existuje $c_2 > 0$ takové, že pro každé $n \geqq 2$ je

$$\pi(n) < c_2 \frac{n}{\ln n}.$$

Proto

$$0 \leqq \underline{d}(\mathbb{P}) \leqq \overline{d}(\mathbb{P}) = \limsup_{n\to\infty} \frac{\pi(n)}{n} \leqq \lim_{n\to\infty} \frac{c_2 \frac{n}{\ln n}}{n} = \lim_{n\to\infty} \frac{c_2}{\ln n} = 0,$$

[1] $[x]$ je celá část čísla x.

$$0 \leqq \underline{\mathrm{d}}(\mathbb{P}) \leqq \bar{d}(\mathbb{P}) \leqq 0.$$

Proto

$$d(\mathbb{P}) = \underline{\mathrm{d}}(\mathbb{P}) = \bar{d}(\mathbb{P}) = 0.$$

□

Dále dokážeme, že ne u každé množiny $A \subseteq \mathbb{N}$ můžeme určit její asymptotickou hustotu. Je to dáno tím, že pro některé množiny A limita $\lim\limits_{n\to\infty} \frac{A(n)}{n}$ neexistuje. V takovém případě říkáme, že množina A nemá asymptotickou hustotu, nebo že $d(A)$ neexistuje.

Věta 3.5. *Existují množiny $A \subseteq \mathbb{N}$ takové, že asymptotická hustota $d(A)$ neexistuje. Například množina přirozených čísel, které ve svém dekadickém zápisu začínají cifrou* 1 *nemá asymptotickou hustotu.*

Důkaz. Pro každé přirozené číslo k existuje $m \in \mathbb{N} \cup \{0\}$ takové, že k můžeme zapsat ve tvaru[1]

$$k = a_m 10^m + \cdots + a_1 10 + a_0,$$

kde $a_m, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$, $a_m \neq 0$.[2] Označme A množinu přirozených čísel k takových, že

$$k = 1.10^m + \cdots + a_1 10 + a_0.$$

Tj. jde o množinu

$$A = \{1, 10, 11, \ldots, 19, 100, 101, \ldots, 199, 1\,000, 1\,001, \ldots, 1\,999, \ldots\}.$$

Nejprve určíme $A(10-1)$, $A(10^2-1)$, $A(10^3-1)$, …, $A(10^m-1)$.

$$\begin{aligned} &A(10-1) = 1 \\ &A(10^2-1) = 1 + 10 \\ &A(10^3-1) = 1 + 10 + 100 \\ &\vdots \\ &A(10^m-1) = 1 + 10 + 100 + \cdots + 10^{m-1} \end{aligned} \tag{3.2}$$

Nyní určíme $A(2.10-1)$, $A(2.10^2-1)$, $A(2.10^3-1)$, …, $A(2.10^m-1)$.

$$\begin{aligned} &A(2.10-1) = 1 + 10 \\ &A(2.10^2-1) = 1 + 10 + 100 \\ &A(2.10^3-1) = 1 + 10 + 100 + 1000 \\ &\vdots \\ &A(2.10^m-1) = 1 + 10 + 100 + \cdots + 10^m \end{aligned} \tag{3.3}$$

[1] Například $k = 3\,637 = 3.10^3 + 6.10^2 + 3.10 + 7$.

[2] V dekadickém zápisu k pak píšeme $k = a_m \cdots a_1 a_0$. Například $k = 2.10^3 + 1.10^2 + 0.10 + 3$ zapisujeme jako $k = 2\,103$.

Z (3.2) a (3.3) dostáváme pro každé $m \in \mathbb{N}$ platnost vztahů[1]

$$\begin{aligned} A(10^m - 1) &= 1 + 10 + 100 + \cdots + 10^{m-1} = \sum_{i=1}^{m} 10^{i-1} = \tfrac{10^m - 1}{10 - 1} \\ A(2.10^m - 1) &= 1 + 10 + 100 + \cdots + 10^{m} = \sum_{i=1}^{m+1} 10^{i-1} = \tfrac{10^{m+1} - 1}{10 - 1} \end{aligned} \tag{3.4}$$

Pokud by asymptotická hustota $d(A)$ existovala, pak by muselo platit[2]

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = \lim_{m\to\infty} \frac{A(10^m - 1)}{10^m - 1} = \lim_{m\to\infty} \frac{A(2.10^m - 1)}{2.10^m - 1}. \tag{3.5}$$

To ovšem neplatí, neboť

$$\lim_{m\to\infty} \frac{A(10^m - 1)}{10^m - 1} = \lim_{m\to\infty} \frac{\frac{10^m - 1}{10 - 1}}{10^m - 1} = \frac{1}{9} \tag{3.6}$$

a

$$\lim_{m\to\infty} \frac{A(2.10^m - 1)}{2.10^m - 1} = \lim_{m\to\infty} \frac{\frac{10^{m+1} - 1}{10 - 1}}{2.10^m - 1} = \lim_{m\to\infty} \frac{1}{9} \frac{10.10^m - 1}{2.10^m - 1} = \frac{1}{9}\frac{10}{2} = \frac{5}{9}. \tag{3.7}$$

Vidíme, že (3.6) a (3.7) je ve sporu s předpokladem (3.5). Z toho plyne, že asymptotická hustota $d(A)$ neexistuje.

□

Nakonec poznamenejme, že asymptotickou hustotu lze použít nejen k charakterizaci „velikosti“ množin, ale také při zkoumání vlastností aditivních bází, r-hustých množin a podobně.

3.1.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.3.1.

1. Ověřte, že pro každou množinu $A \subseteq \mathbb{N}$ existuje její horní a dolní asymptotická hustota $\bar{d}(A)$, respektive $\underline{\mathrm{d}}(A)$, ale nemusí nutně existovat asymptotická hustota $d(A)$.

2. Dokažte, že pro každou množinu $A \subseteq \mathbb{N}$ platí, že $0 \leqq \underline{\mathrm{d}}(A) \leqq \bar{d}(A) \leqq 1$.

[1] Pro součet geometrické řady $a_i = a_1 q^{i-1}$ platí vztah $\sum_{i=1}^{r} a_1 q^{i-1} = a_1 \frac{q^r - 1}{q - 1}$. V našem případě je $a_1 = 1$ a $q = 10$.

[2] Jak známo, jestliže posloupnost reálných čísel konverguje, pak její vybraná posloupnost konverguje k téže hodnotě.

3. Dokažte, že existují množiny, jejichž asymptotická hustota splňuje $d(A) = 1$ a přesto $A \neq \mathbb{N}$. (Jde například o množiny typu $A = \mathbb{N} - K$, kde K je neprázdná konečná podmnožina množiny přirozených čísel.)

4. Ověřte, že existují nekonečné množiny, jejichž asymptotická hustota splňuje $d(A) = 0$. (Například množina $A = \{n^2 \mid n \in \mathbb{N}\}$, nebo množina všech prvočísel.)

5. Přidáme-li, nebo odebereme-li z dané množiny A konečný počet prvků, pak asymptotická hustota výsledné množiny je stejná jako asymptotická hustota množiny A (za předpokladu, že $d(A)$ existuje). Tj. pokud $A, K \subseteq \mathbb{N}$, K je konečná množina, pak $d(A \cup K) = d(A)$ a také $d(A - K) = d(A)$. Dokažte.

6. Dokažte, že neexistuje asymptotická hustota množiny $A = \cup_{n\in\mathbb{N}}\{6^n+1, 6^n+ + 2, \ldots, 2.6^n\}$

3.2 Logaritmická hustota

Jak jsme viděli v předcházející podkapitole, je „nejpřirozenější“ charakterizovat velikost množiny $A \subseteq \mathbb{N}$ pomocí asymptotické hustoty. Velkou slabinou ovšem je, že tuto hodnotu nejsme schopni určit u libovolné množiny $A \subseteq \mathbb{N}$.

Dále uvidíme, že logaritmická hustota tento nedostatek neodstraňuje zcela (existují množiny, které nemají ani logaritmickou hustotu). Nicméně každá množina, která má asymptotickou hustotu, má také logaritmickou hustotu (a jsou si rovny) a hlavně, existují množiny, které nemají asymptotickou hustotu, ale logaritmickou hustotu mají.

Můžeme proto říci, že zavedením logaritmické hustoty jsme rozšířili naše schopnosti charakterizovat velikosti množin $A \subseteq \mathbb{N}$. Pojem logaritmické hustoty je zobecněním pojmu asymptotické hustoty množin.

A jaká je myšlenka logaritmické hustoty? U asymptotické hustoty jsme se snažili určit limitu poměru počtu prvků množiny A (menších, nebo rovných n) ku počtu prvů množiny $\mathbb{N}$ (menších, nebo rovných n). Tj. hledali jsme hodnotu

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} 1}{\sum\limits_{\substack{k\in\mathbb{N}\\ k\leqq n}} 1}.$$

U logaritmické hustoty srovnáváme velikosti součtů převrácených hodnot prvků z A a $\mathbb{N}$. Tj. hledáme hodnotu

$$\delta(A) = \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{\substack{k\in\mathbb{N}\\ k\leqq n}} \frac{1}{k}}.$$

S odkazem na znalosti z matematické analýzy můžeme říci, že tato limita nemusí nutně existovat, ale určitě existuje limes superior a limes inferior posloupnosti $\delta_n = \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{\substack{k\in\mathbb{N}\\ k\leqq n}} \frac{1}{k}}$. Proto logaritmickou hustotu množiny A definujeme následovně.

Definice 3.6. (*Logaritmická hustota*) Nechť $A \subseteq N$. Horní logaritmickou hustotou množiny A nazýváme číslo

$$\overline{\delta}(A) = \limsup_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{\substack{k\in\mathbb{N}\\ k\leqq n}} \frac{1}{k}}.$$

Dolní logaritmickou hustotou množiny A nazýváme číslo

$$\underline{\delta}(A) = \liminf_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{\substack{k\in\mathbb{N}\\ k\leqq n}} \frac{1}{k}}.$$

Jestliže $\overline{\delta}(A) = \underline{\delta}(A)$, pak hodnotu

$$\delta(A) = \overline{\delta}(A) = \underline{\delta}(A) = \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{\substack{k\in\mathbb{N}\\ k\leqq n}} \frac{1}{k}}.$$

nazýváme logaritmitickou hustotou množiny A. V případě, že $\overline{\delta}(A) \neq \underline{\delta}(A)$ říkáme, že $\delta(A)$ neexistuje, nebo že A nemá logaritmickou hustotu.

Čtenáře možná napadla otázka, proč se v názvu logaritmické hustoty vyskytlo slovíčko „logaritmická,“ když v její definici není po logaritmu ani stopy. Odpověď skrývá následující lema[1].

[1]Jde o to, že součet $\sum\limits_{k=1}^{n} \frac{1}{k}$ při velkých hodnotách n nabývá hodnot „téměř stejných“ jako funkce $\ln n + \gamma$, kde $\gamma \doteq 0,577\,215$ je konstanta (a tedy pro velká n také zanedbatelná položka). Hodnotu součtu převrácených hodnot čísel patřících do množiny A, $\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}$, proto můžeme porovnávat s hodnotou $\ln n$. Čím „hustější“ je množina A (tzn. jen „málo“ přirozených čísel do ní nepatří), tím více se k sobě tyto dvě hodnoty blíží

Lemma 3.7. *Nechť $A \subseteq \mathbb{N}$ a $\delta(A)$ existuje. Potom platí*

$$\delta(A) = \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{\substack{k\in\mathbb{N}\\ k\leqq n}} \frac{1}{k}} = \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n}.$$

Důkaz. Podle Lemmatu 2.36 (viz též poznámka pod čarou k Lemmatu 2.36) pro každé $x \in \mathbb{R}$, $x \geqq 1$ platí

$$\sum_{\substack{k\leqq n\\ k\in\mathbb{N}}} \frac{1}{k} = \ln n + \gamma + o(1),$$

kde γ je takzvaná Eulerova konstanta (její přibližná hodnota je $0,577\,215$). Proto[1]

$$\begin{aligned}
\delta(A) &= \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{\substack{k\in\mathbb{N}\\ k\leqq n}} \frac{1}{k}} = \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n + \gamma + o(1)} = \\
&= \lim_{n\to\infty} \left(\frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} \underbrace{\frac{\ln n}{\ln n + \gamma + o(1)}}_{\to 1} \right) = \\
&= \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n}.
\end{aligned}$$

□

Nyní ukážeme, že každá množina, která má asymptotickou hustotu má i logaritmickou a jsou si rovny.

Věta 3.8. *Nechť $A \subseteq \mathbb{N}$. Potom platí*

$$\underline{d}(A) \leqq \underline{\delta}(A) \leqq \overline{\delta}(A) \leqq \overline{d}(A).$$

[1] Využijeme toho, že pokud $\lim\limits_{n\to\infty} f(n)g(n) = \delta(A) \in \mathbb{R}$ a $\lim\limits_{n\to\infty} g(n) = 1$, pak $\lim\limits_{n\to\infty} f(n) = \delta(A)$.

Důkaz. Vezměme libovolné $m, n \in \mathbb{N}$, $n > 1$ a $m < n$. Potom platí[1]

$$\begin{aligned}
\sum_{\substack{a\in A\\ m\leqq a\leqq n}} \frac{1}{a} &= \sum_{k=m}^{n} \frac{A(k)-A(k-1)}{k} = \\
&= \frac{A(m)-A(m-1)}{m} + \frac{A(m+1)-A(m)}{m+1} + \cdots + \\
&\quad + \frac{A(n-1)-A(n-2)}{n-1} + \frac{A(n)-A(n-1)}{n} = \\
&= -\frac{A(m-1)}{m} + A(m)\left(\frac{1}{m}-\frac{1}{m+1}\right) + A(m+1)\left(\frac{1}{m+1}-\frac{1}{m+2}\right) + \\
&\quad + \cdots + A(n-1)\left(\frac{1}{n-1}-\frac{1}{n}\right) + \frac{A(n)}{n} = \\
&= -\frac{A(m-1)}{m} + A(m)\frac{1}{m(m+1)} + A(m+1)\frac{1}{(m+1)(m+2)} + \\
&\quad + \cdots + A(n-1)\frac{1}{(n-1)n} + \frac{A(n)}{n} = \\
&= \frac{A(n)}{n} - \frac{A(m-1)}{m} + \sum_{k=m}^{n-1} \frac{A(k)}{k}\frac{1}{k+1}. \qquad (3.8)
\end{aligned}$$

Označme $Q_m = \{\frac{A(m)}{m}, \frac{A(m+1)}{m+1}, \dots\}$ a supremum[2] této množiny označíme $\sup\limits_{k\geqq m} \frac{A(k)}{k}$. Potom z (3.8) plyne, že pro každé $m, n \in \mathbb{N}$, $m \leqq n$ platí

$$\begin{aligned}
\sum_{\substack{a\in A\\ m\leqq a\leqq n}} \frac{1}{a} &= \frac{A(n)}{n} - \frac{A(m-1)}{m} + \sum_{k=m}^{n-1} \frac{A(k)}{k}\frac{1}{k+1} \leqq \\
&\leqq \frac{A(n)}{n} - \frac{A(m-1)}{m} + \sum_{k=m}^{n-1} \sup_{k\geqq m} \frac{A(k)}{k}\frac{1}{k+1} = \\
&= \frac{A(n)}{n} - \frac{A(m-1)}{m} + \sup_{k\geqq m} \frac{A(k)}{k} \sum_{k=m+1}^{n} \frac{1}{k} \leqq \\
&\leqq \frac{A(n)}{n} - \frac{A(m-1)}{m} + \sup_{k\geqq m} \frac{A(k)}{k} \sum_{k=1}^{n} \frac{1}{k}. \qquad (3.9)
\end{aligned}$$

[1] Všimněte si, že pokud číslo k patří do množiny A, je $A(k) - A(k-1) = 1$, pokud ne, je $A(k) - A(k-1) = 0$.

[2] Připomeňme, že k supremu množiny se svou hodnotou prvky této množiny mohou libovolně blížit, ale nikdy nemohou být větší!

Proto (viz (3.8)) pro libovonné $m \in \mathbb{N}$ a pro všechna $n \geqq m$ platí

$$\sum_{\substack{a\in A\\ m\leqq a\leqq n}} \frac{1}{a} + \frac{A(m-1)}{m} - \frac{A(n)}{n} \leqq \sup_{k\geqq m} \frac{A(k)}{k} \sum_{k=1}^{n} \frac{1}{k},$$

$$\sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} - \sum_{\substack{a\in A\\ a\leqq m-1}} \frac{1}{a} + \frac{A(m-1)}{m} - \frac{A(n)}{n} \leqq \sup_{k\geqq m} \frac{A(k)}{k} \sum_{k=1}^{n} \frac{1}{k}.$$

Celou nerovnici podělíme výrazem $\sum_{k=1}^{n} \frac{1}{k}$ a obdržíme tak pro libovonné $m \in \mathbb{N}$ a pro všechna $n \geqq m$ nerovnost

$$\frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{k=1}^{n} \frac{1}{k}} \underbrace{- \frac{\sum\limits_{\substack{a\in A\\ a\leqq m-1}} \frac{1}{a}}{\sum\limits_{k=1}^{n} \frac{1}{k}} + \frac{\frac{A(m-1)}{m}}{\sum\limits_{k=1}^{n} \frac{1}{k}} - \frac{\frac{A(n)}{n}}{\sum\limits_{k=1}^{n} \frac{1}{k}}}_{\to 0 \text{ při } n\to\infty} \leqq \sup_{k\geqq m} \frac{A(k)}{k} \tag{3.10}$$

Při $n \to \infty$ pak podle definice horní logaritmické hustoty pro libovonné $m \in \mathbb{N}$ z (3.10) dostáváme[1]

$$\overline{\delta}(A) = \limsup_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{k=1}^{n} \frac{1}{k}} \leqq \sup_{k\geqq m} \frac{A(k)}{k}. \tag{3.11}$$

A protože vztah (3.11) je splněn pro každé $m \in \mathbb{N}$, platí také

$$\overline{\delta}(A) \leqq \lim_{m\to\infty} \left(\sup_{k\geqq m} \frac{A(k)}{k} \right). \tag{3.12}$$

Ve Cvičení 3.2.1 je dokázáno (viz řešení), že

$$\lim_{m\to\infty} \left(\sup_{k\geqq m} \frac{A(k)}{k} \right) = \limsup_{k\to\infty} \frac{A(k)}{k}.$$

Proto

$$\overline{\delta}(A) \leqq \limsup_{k\to\infty} \frac{A(k)}{k} = \overline{d}(A). \tag{3.13}$$

[1] Uvažte, že pro dané m jsou $\sum\limits_{\substack{a\in A\\ a\leqq m-1}} \frac{1}{a}$ a $\frac{A(m-1)}{m}$ konstanty, pro každé $n \in \mathbb{N}$ je $0 \leqq \frac{A(n)}{n} \leqq 1$ a $\sum\limits_{k=1}^{n} \frac{1}{k} \to \infty$ při $n \to \infty$.

Zbývá dokázat,že $\underline{d}(A) \leqq \underline{\delta}(A)$. Označme symbolem $\inf\limits_{k\geqq m} \frac{A(k)}{k}$ infimum množiny $Q_m = \{\frac{A(m)}{m}, \frac{A(m+1)}{m+1}, \dots\}$. Ze vztahu (3.8) pak plyne, že pro každé $m, n \in \mathbb{N}$, $m \leqq n$ platí

$$\begin{aligned}\sum_{\substack{a\in A\\ m\leqq a\leqq n}} \frac{1}{a} &= \frac{A(n)}{n} - \frac{A(m-1)}{m} + \sum_{k=m}^{n-1} \frac{A(k)}{k}\frac{1}{k+1} \geqq \\ &\geqq \frac{A(n)}{n} - \frac{A(m-1)}{m} + \sum_{k=m}^{n-1} \inf_{k\geqq m} \frac{A(k)}{k}\frac{1}{k+1} = \\ &= \frac{A(n)}{n} - \frac{A(m-1)}{m} + \inf_{k\geqq m} \frac{A(k)}{k} \sum_{k=m+1}^{n} \frac{1}{k}\end{aligned} \tag{3.14}$$

A tak

$$\sum_{\substack{a\in A\\ m\leqq a\leqq n}} \frac{1}{a} \geqq \frac{A(n)}{n} - \frac{A(m-1)}{m} + \inf_{k\geqq m} \frac{A(k)}{k} \sum_{k=1}^{n} \frac{1}{k} - \inf_{k\geqq m} \frac{A(k)}{k} \sum_{k=1}^{m} \frac{1}{k}. \tag{3.15}$$

Označme $c(m) = -\frac{A(m-1)}{m} - \inf\limits_{k\geqq m} \frac{A(k)}{k} \sum\limits_{k=1}^{m} \frac{1}{k}$. Při tomto značení můžeme (3.15) přepsat do tvaru[1]

$$\sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} - \sum_{\substack{a\in A\\ a<m}} \frac{1}{a} \geqq \frac{A(n)}{n} + c(m) + \inf_{k\geqq m} \frac{A(k)}{k} \sum_{k=1}^{n} \frac{1}{k}.$$

Tato nerovnice je splněna pro libovolné $m \in \mathbb{N}$ a pro libovolné $n \in \mathbb{N}$, $n > m$. Obě její strany podělíme $\sum\limits_{k=1}^{n} \frac{1}{k}$ a obdržíme tak[2]

$$\frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\sum\limits_{k=1}^{n} \frac{1}{k}} - \underbrace{\frac{\sum\limits_{\substack{a\in A\\ a<m}} \frac{1}{a}}{\sum\limits_{k=1}^{n} \frac{1}{k}}}_{\to 0 \text{ při } n\to\infty} - \underbrace{\frac{\frac{A(n)}{n} + c(m)}{\sum\limits_{k=1}^{n} \frac{1}{k}}}_{\to 0 \text{ při } n\to\infty} \geqq \inf_{k\geqq m} \frac{A(k)}{k}. \tag{3.16}$$

[1] Pro dané m jsou $\frac{A(m-1)}{m}$ i $\inf\limits_{k\geqq m} \frac{A(k)}{k} \sum\limits_{k=1}^{m} \frac{1}{k}$ konstanty.

[2] $\sum\limits_{\substack{a\in A\\ a<m}} \frac{1}{a}$ a $c(m)$ jsou pro dané m konstanty, navíc $0 \leqq \frac{A(n)}{n} \leqq 1$ pro každé $n \in \mathbb{N}$.

Při pevně zvoleném m a $n \to \infty$ z (3.16) dostáváme

$$\underline{\delta}(A) = \liminf_{n\to\infty} \frac{\sum\limits_{\substack{a\in A \\ m\leqq a\leqq n}} \frac{1}{a}}{\sum\limits_{k=1}^{n} \frac{1}{k}} \geqq \inf_{k\geqq m} \frac{A(k)}{k}.$$

Tato nerovnost platí pro každé $m \in \mathbb{N}$. A tak, při $m \to \infty$ dostáváme

$$\underline{\delta}(A) \geqq \lim_{m\to\infty} \left(\inf_{k\geqq m} \frac{A(k)}{k} \right). \tag{3.17}$$

Obdobně jako ve Cvičení 3.2.1 bychom mohli dokázat, že

$$\lim_{m\to\infty} \left(\inf_{k\geqq m} \frac{A(k)}{k} \right) = \liminf_{k\to\infty} \frac{A(k)}{k} = \underline{d}(A).$$

Z (3.17) pak plyne

$$\underline{\delta}(A) \geqq \underline{d}(A). \tag{3.18}$$

Spojením nerovnic (3.13) a (3.18) obdržíme dokazované tvrzení[1]

$$\underline{d}(A) \leqq \underline{\delta}(A) \leqq \overline{\delta}(A) \leqq \overline{d}(A).$$

□

Věta 3.9. *Nechť $A \subseteq \mathbb{N}$. Jestliže existuje asymptotická hustota množiny A, pak existuje i logaritmická hustota množiny A a platí*

$$d(A) = \delta(A).$$

Důkaz. Tvrzení této věty je důsledkem Věty 3.8. Jestliže existuje asymptotická hustota množiny A, znamená to, že se její horní a dolní asymptotická hustota rovnají a jejich společná hodnota je rovna $d(A)$, tj.

$$\underline{d}(A) = \overline{d}(A) = d(A).$$

Věta 3.8 říká, že $\underline{d}(A) \leqq \underline{\delta}(A) \leqq \overline{\delta}(A) \leqq \overline{d}(A)$. V tomto případě[2] proto platí

$$d(A) \leqq \underline{\delta}A \leqq \overline{\delta}A \leqq d(A).$$

A proto není jiná možnost, než že se rovná také horní a dolní logaritmická hustota a jsou rovny $d(A)$. Podle definice logaritmické hustoty je však jejich společná hodnota rovna $\delta(A)$. Proto musí platit $d(A) = \delta(A)$.

□

[1] Vždy platí $\underline{\delta}(A) \leqq \overline{\delta}(A)$.

[2] Tj. v případě, že existuje $d(A)$.

V předchozí podkapitole věnované asymptotické hustotě jsme viděli, že existují množiny, které nemají asymptotickou hustotu. Jako příklad byla uvedena množina přirozených čísel, které ve svém dekadickém zápisu začínají jedničkou. Z následující věty plyne, že logaritmická hustota této množiny existuje a je rovna $\log_{10} 2 \doteq 0,301$.

Množinu přirozených čísel, které ve svém dekadickém zápise začínají číslem $c \in \{1, 2, \ldots, 9\}$ označme M_c. Tj.

$$M_c = \{c.10^j + a_{j-1}.10^{j-1} + \cdots + a_1.10 + a_0 \mid j \in \mathbb{N} \cup \{0\}, a_{j-1}, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}\}.$$

Věta 3.10. *Pro každé $c \in \{1, 2, \ldots, 9\}$ platí*

$$\delta(M_c) = \log_{10}\left(\frac{c+1}{c}\right).$$

Důkaz. Potřebujeme určit hodnotu limity (viz Lema 3.7)

$$\delta(M_c) = \lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in M_c \\ a\leqq n}} \frac{1}{a}}{\ln n}.$$

Je proto třeba určit hodnotu součtu $\sum\limits_{\substack{a\in M_c \\ a\leqq n}} \frac{1}{a}$ v závislosti na n.

Množina M_c obsahuje přirozená čísla ve tvaru $c.10^j + a_{j-1}.10^{j-1} + \cdots + a_1.10 + + a_0$. Uvažujme, která přirozená čísla a patří do množiny M_c a splňují podmínku $10^j \leqq a < 10^{j+1}$. Nejmenší takové číslo a je rovno $c.10^j$ a největší je rovno $c.10^j + 9.10^{j-1} + \cdots + 9.10 + 9 = (c+1)10^j - 1$. A všechna přirozená čísla mezi nimi také patří do množiny M_c. Proto, označíme-li pro každé $j = 0, 1, \ldots$

$$L_j = \sum_{\substack{a\in M_c \\ 10^j\leqq a<10^{j+1}}} \frac{1}{a}, \tag{3.19}$$

je

$$L_j = \sum_{c.10^j\leqq a\leqq(c+1)10^j-1} \frac{1}{a} = \sum_{a\leqq(c+1)10^j-1} \frac{1}{a} - \sum_{a\leqq c.10^j-1} \frac{1}{a}. \tag{3.20}$$

Pro každé $n \in \mathbb{N}$ platí (viz Cvičení 2.6.1) $\sum\limits_{a\leqq n} \frac{1}{a} = \ln(n+1) + \gamma + g(n)$, kde γ je konstanta, a $g(n)$ splňuje nerovnosti $-\frac{1}{n+1} < g(n) < 0$. Proto

$$\begin{aligned} L_j &= \ln\left((c+1)10^j\right) - \ln\left(c.10^j\right) + \underbrace{g((c+1)10^j - 1) - g(c.10^j - 1)}_{\alpha(j)}, \\ L_j &= \ln\left(\frac{(c+1)10^j}{c.10^j}\right) + \alpha(j), \\ L_j &= \ln\left(\frac{c+1}{c}\right) + \alpha(j), \end{aligned} \tag{3.21}$$

kde

$$\begin{aligned} -\tfrac{1}{(c+1)10^j} \;<\; g\left((c+1)10^j - 1\right) \;<\; 0, \\ 0 \;<\; -g(c.10^j - 1) \;<\; \tfrac{1}{c.10^j}. \end{aligned} \tag{3.22}$$

A tak $\alpha(j) = g\left((c+1)10^j - 1\right) - g(c.10^j - 1)$ splňuje pro každé $j = 0, 1, \ldots$ podmínku

$$-\frac{1}{(c+1)10^j} < \alpha(j) < \frac{1}{c.10^j}. \tag{3.23}$$

Nyní už můžeme snadno odhadnout hodnotu součtu $\sum\limits_{\substack{a \in M_c \\ a \leqq n}} \frac{1}{a}$. Pro dané n jistě existuje $j_n \in \mathbb{N}$ takové, že

$$10^{j_n} \leqq n < 10^{j_n+1}. \tag{3.24}$$

Podle (3.19) a (3.24) platí

$$\sum_{j=0}^{j_n-1} L_j \leqq \sum_{\substack{a \in M_c \\ a \leqq n}} \frac{1}{a} < \sum_{j=0}^{j_n+1} L_j, \tag{3.25}$$

dosazením (3.21) do (3.25) obdržíme

$$\sum_{j=0}^{j_n-1} \left(\ln\left(\frac{c+1}{c}\right) + \alpha(j)\right) \leqq \sum_{\substack{a \in M_c \\ a \leqq n}} \frac{1}{a} < \sum_{j=0}^{j_n+1} \left(\ln\left(\frac{c+1}{c}\right) + \alpha(j)\right),$$

$$\sum_{j=0}^{j_n-1} \ln\left(\frac{c+1}{c}\right) + \sum_{j=0}^{j_n-1} \alpha(j) \leqq \sum_{\substack{a \in M_c \\ a \leqq n}} \frac{1}{a} < \sum_{j=0}^{j_n+1} \ln\left(\frac{c+1}{c}\right) + \sum_{j=0}^{j_n+1} \alpha(j),$$

$$j_n \ln\left(\frac{c+1}{c}\right) + \sum_{j=0}^{j_n-1} \alpha(j) \leqq \sum_{\substack{a\in M_c \\ a\leqq n}} \frac{1}{a} < (j_n+2)\ln\left(\frac{c+1}{c}\right) + \sum_{j=0}^{j_n+1} \alpha(j). \quad (3.26)$$

S využitím (3.23) dostaneme odhady

$$\sum_{j=0}^{j_n-1} \alpha(j) \geqq \sum_{j=0}^{j_n-1} \frac{-1}{(c+1)10^j} \geqq \sum_{j=0}^{\infty} \frac{-1}{(c+1)10^j} = \frac{-10}{9(c+1)} \quad (3.27)$$

a

$$\sum_{j=0}^{j_n+1} \alpha(j) \leqq \sum_{j=0}^{j_n+1} \frac{1}{c.10^j} \leqq \sum_{j=0}^{\infty} \frac{1}{c.10^j} = \frac{10}{9c}. \quad (3.28)$$

Použijeme odhady (3.27) a (3.28) v nerovnostech (3.26) a obdržíme

$$j_n \ln\left(\frac{c+1}{c}\right) - \frac{10}{9(c+1)} \leqq \sum_{\substack{a\in M_c \\ a\leqq n}} \frac{1}{a} < (j_n+2)\ln\left(\frac{c+1}{c}\right) + \frac{10}{9c}. \quad (3.29)$$

Z nerovností (3.24) určíme hodnotu j_n

$$\begin{aligned} 10^{j_n} &\leqq n &< 10^{j_n+1}, \\ \ln 10^{j_n} &\leqq \ln n &< \ln 10^{j_n+1}, \\ j_n \ln 10 &\leqq \ln n &< (j_n+1)\ln 10, \\ j_n &\leqq \tfrac{\ln n}{\ln 10} &< j_n + 1 \end{aligned}$$

To znamená, že $j_n = \left[\frac{\ln n}{\ln 10}\right]$. Z nerovností (3.29) plynou následující odhady:

$$\begin{aligned} \liminf_{n\to\infty} \frac{\sum\limits_{\substack{a\in M_c \\ a\leqq n}} \frac{1}{a}}{\ln n} &\geqq \lim_{n\to\infty} \frac{j_n \ln\left(\frac{c+1}{c}\right) - \frac{10}{9(c+1)}}{\ln n} = \\ &= \lim_{n\to\infty} \frac{j_n \ln\left(\frac{c+1}{c}\right)}{\ln n} - \underbrace{\lim_{n\to\infty} \frac{10}{9(c+1)\ln n}}_{=0} = \\ &= \lim_{n\to\infty} \frac{\left[\frac{\ln n}{\ln 10}\right] \ln\left(\frac{c+1}{c}\right)}{\ln n} = \\ &= \frac{\ln\left(\frac{c+1}{c}\right)}{\ln 10}. \end{aligned} \quad (3.30)$$

a

$$\begin{aligned}\limsup_{n\to\infty}\frac{\sum\limits_{\substack{a\in M_c\\ a\leqq n}}\frac{1}{a}}{\ln n} &\leqq \lim_{n\to\infty}\frac{(j_n+2)\ln\left(\frac{c+1}{c}\right)+\frac{10}{9c}}{\ln n}= \\ &= \lim_{n\to\infty}\frac{(j_n+2)\ln\left(\frac{c+1}{c}\right)}{\ln n}+\underbrace{\lim_{n\to\infty}\frac{10}{9c\ln n}}_{=0}= \\ &= \lim_{n\to\infty}\frac{\left(\left[\frac{\ln n}{\ln 10}\right]+2\right)\ln\left(\frac{c+1}{c}\right)}{\ln n}= \\ &= \frac{\ln\left(\frac{c+1}{c}\right)}{\ln 10}. \end{aligned} \tag{3.31}$$

Proto

$$\frac{\ln\left(\frac{c+1}{c}\right)}{\ln 10}\leqq\liminf_{n\to\infty}\frac{\sum\limits_{\substack{a\in M_c\\ a\leqq n}}\frac{1}{a}}{\ln n}\leqq\limsup_{n\to\infty}\frac{\sum\limits_{\substack{a\in M_c\\ a\leqq n}}\frac{1}{a}}{\ln n}\leqq\frac{\ln\left(\frac{c+1}{c}\right)}{\ln 10}.$$

To znamená, že

$$\liminf_{n\to\infty}\frac{\sum\limits_{\substack{a\in M_c\\ a\leqq n}}\frac{1}{a}}{\ln n}=\limsup_{n\to\infty}\frac{\sum\limits_{\substack{a\in M_c\\ a\leqq n}}\frac{1}{a}}{\ln n}=\lim_{n\to\infty}\frac{\sum\limits_{\substack{a\in M_c\\ a\leqq n}}\frac{1}{a}}{\ln n}=\frac{\ln\left(\frac{c+1}{c}\right)}{\ln 10}.$$

A tak (viz Lema 3.8)

$$\delta(M_c)=\lim_{n\to\infty}\frac{\sum\limits_{\substack{a\in M_c\\ a\leqq n}}\frac{1}{a}}{\ln n}=\frac{\ln\left(\frac{c+1}{c}\right)}{\ln 10}=\log_{10}\left(\frac{c+1}{c}\right).$$

□

3.2.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.3.2.

1. Nalezněte logaritmickou hustotu množiny přirozených čísel, které ve svém dekadickém zápisu začínají ciframi 11. Tzn. jde o množinu $A = \{11, 110, 111, \ldots, 119, 1100, 1101, \ldots, 1199, \ldots\}$.
2. Nalezněte logaritmickou hustotu množiny $A = \bigcup_{j\in\mathbb{N}}\{6^j+1, 6^j+2, \ldots, 2.6^j\}$.
3. Nechť $A \subseteq \mathbb{N}$. Dokažte, že $\lim\limits_{m\to\infty}\left(\sup\limits_{k\geqq m}\frac{A(k)}{k}\right)=\limsup\limits_{k\to\infty}\frac{A(k)}{k}$.

3.3 Schnirelmannova hustota

Asymptotickou i logaritmickou hustotou dané množiny A se snažíme vystihnout poměr velikosti množiny A a velikosti množiny přirozených čísel $\mathbb{N}$. Schnirelmannova hustota, kterou se budeme v této části textu zabývat, má poněkud jiný význam. Předvedeme na konkrétním příkladě.

Uvažujme množinu A, která obsahuje všechny přirozené čísla, kromě čísla 2. Tj.

$$A = \{1, 3, 4, 5, \dots\}.$$

Prozkoumejme posloupnost čísel $\frac{A(n)}{n}$. Pokud se omezíme pouze na prvních n přirozených čísel[1], pak toto číslo udává poměr počtu prvků množiny A mezi těmito čísly ku počtu všech těchto čísel. U výše uvedené množiny A tak dostáváme

$$\begin{aligned} \frac{A(1)}{1} &= \frac{1}{1} \\ \frac{A(2)}{2} &= \frac{1}{2} \\ \frac{A(3)}{3} &= \frac{2}{3} \\ &\vdots \\ \frac{A(n)}{n} &= \frac{n-1}{n} = 1 - \frac{1}{n}, \text{ pro } n \geqq 2. \\ &\vdots \end{aligned} \tag{3.32}$$

A tak, označíme-li $R = \{\frac{A(n)}{n} \mid n \in \mathbb{N}\}$, je zřejmé, že

$$R = \left\{1, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots\right\}$$

a

$$\inf_{n\in\mathbb{N}} \frac{A(n)}{n} = \frac{1}{2}. \tag{3.33}$$

Posledně uvedená hodnota $\inf_{n\in\mathbb{N}} \frac{A(n)}{n}$ vyjadřuje, k jaké nejmenší hodnotě se přiblížily (či jí dosáhly) hodnoty $\frac{A(n)}{n}$ pro všechna $n \in \mathbb{N}$. U námi zvolené množiny A jsme zjistili (viz rovnice (3.32) a (3.33)), že mezi čísly $1, 2, ..., n$ je nejméně jedna polovina čísel patřících do množiny A (tento krajní případ nastal pro $n = 2$.)

Číslo $\inf_{n\in\mathbb{N}} \frac{A(n)}{n}$ tedy svým způsobem také charakterizuje velikost množiny A. Říkejme mu Schnirelmannova hustota množiny A. Nejde však, tak jako u asympto-

[1] Tím je míněno na čísla $1, 2, \dots, n$.

tické a logaritmické hustoty, o pokus o odpověď na otázku, jak velkou část z přirozených čísel tvoří množina A. Jde o odpověď na otázku, jakou nejmenší část z čísel $1, 2, \ldots, n$ tvoří prvky množiny A (a to pro všechna možná n).

Z toho také plyne, možná na první pohled poněkud zarážející, vlastnost Schnirelmannovy hustoty. Spočívá v tom, že když do dané množiny A nepatří číslo 1, pak její Schnirelmannova hustota je rovna nule (viz následující Lema 3.12). A to i v případě, že množina A obsahuje třeba všechny zbývající přirozená čísla. Nicméně na tom vlastně není nic zarážejícího, neboť mezi čísly $1, \ldots, n$ pro $n = 1$ není ani jeden prvek z množiny A. Proto je Schnirelmannova hustota množiny A nutně rovna 0.[1]

Dost bylo úvodu, přistupme k definici Schnirelmannovy hustoty.

Definice 3.11. (*Schnirelmannova hustota*) Nechť $A \subseteq N$. Schnirelmannovou hustotou množiny A nazýváme číslo

$$\sigma(A) = \inf_{n \in N} \frac{A(n)}{n}.$$

Základní vlastnosti Schnirelmannovy hustoty shrnuje následující lema.

Lemma 3.12. *Nechť $A \subseteq \mathbb{N}$ potom platí:*

1. *Schnirelmannova hustota $\sigma(A)$ existuje pro každou množinu $A \subseteq \mathbb{N}$.*
2. *Pro každou množinu $A \subseteq \mathbb{N}$ platí $0 \leqq \sigma(A) \leqq 1$.*
3. *Platí, že $\sigma(A) = 1$ právě tehdy, když $A = \mathbb{N}$.*
4. *Jestliže $1 \notin A$, pak $\sigma(A) = 0$.*
5. *Pro každé $n \in \mathbb{N}$ platí, že $A(n) \geqq n\sigma(A)$.*

Důkaz. 1. Jak bylo již nejednou řečeno, množina reálných čísel má vždy své infimum. A tak musí existovat i

$$\sigma(A) = \inf_{n \in N} \frac{A(n)}{n},$$

neboť symbolický zápis $\inf_{n \in N} \frac{A(n)}{n}$ neznamená nic jiného, než infimum množiny $\{\frac{A(n)}{n} \mid n \in \mathbb{N}\}$.

2. Pro každou množinu $A \subseteq \mathbb{N}$ a pro každé $n \in \mathbb{N}$ platí[2]

$$0 \leqq \frac{A(n)}{n} \leqq 1.$$

[1] A stojí za povšimnutí fakt, že asymptotická i logaritmická hustota této množiny je rovna 1.

[2] Neboť $0 \leqq A(n) \leqq n$.

Proto $\{\frac{A(n)}{n} \mid n \in \mathbb{N}\} \subseteq \langle 0, 1\rangle$. A tak

$$0 \leqq \underbrace{\inf_{n\in N} \frac{A(n)}{n}}_{=\sigma(A)} \leqq 1.$$

3. Nejprve dokážeme implikaci:

$$(A = \mathbb{N}) \Rightarrow (\sigma(A) = 1)\,.$$

To ovšem není nikterak složité. Podle předpokladu je $A = \mathbb{N}$. Proto pro každé $n \in \mathbb{N}$ platí $A(n) = n$. A tak

$$\left\{\frac{A(n)}{n} \mid n \in \mathbb{N}\right\} = \{1\}.$$

Proto

$$\sigma(A) = \inf_{n\in\mathbb{N}} \frac{A(n)}{n} = 1.$$

Nyní provedeme důkaz opačné implikace, tj.

$$(\sigma(A) = 1) \Rightarrow (A = \mathbb{N})\,.$$

Dokážeme větu obměněnou (viz Nepřímý důkaz v kapitole 0.4). To jest, dokážeme pravdivost ekvivalentního tvrzení:

$$(A \neq \mathbb{N}) \Rightarrow (\sigma(A) \neq 1)\,.$$

Podle předpokladu je $A \neq \mathbb{N}$. Znamená to, že nějaké přirozené číslo, označme jej k, nepatří do množiny A. Proto je počet prvků množiny A, které jsou menší, nebo rovny k, nejvýše roven $k - 1$. Symbolicky zapsáno,

$$A(k) \leqq k - 1.$$

A tak

$$\frac{A(k)}{k} \leqq \frac{k-1}{k} = 1 - \frac{1}{k} < 1.$$

Infimum množiny je menší (nebo rovno), než její libovolný prvek. Proto

$$\sigma(A) = \inf_{n\in\mathbb{N}} \frac{A(n)}{n} \leqq \frac{A(k)}{k} < 1.$$

Triviálním důsledkem je, že $\sigma(A) \neq 1$.

4. Je zřejmé (viz výše), že $\{\frac{A(n)}{n} \mid n \in \mathbb{N}\} \subseteq \langle 0, 1\rangle$. Proto[1]

$$0 \leqq \inf_{n\in\mathbb{N}} \frac{A(n)}{n}. \tag{3.34}$$

Podle předpokladu $1 \notin A$. Potom $A(1) = 0$, a tak

$$\frac{A(1)}{1} = 0.$$

Podle definice infima množiny musí platit, že všechny prvky množiny $R = \{\frac{A(n)}{n} \mid n \in \mathbb{N}\}$ musí být větší, nebo rovny infimu množiny R. A protože jedním z prvků R je $\frac{A(1)}{1}$, můžeme tvrdit, že

$$\inf_{n\in\mathbb{N}} \frac{A(n)}{n} \leqq \frac{A(1)}{1} = 0. \tag{3.35}$$

Z nerovností (3.34) a (3.35) pak plyne

$$0 \leqq \inf_{n\in\mathbb{N}} \frac{A(n)}{n} \leqq 0.$$

To ovšem znamená, že

$$\sigma(A) = \inf_{n\in\mathbb{N}} \frac{A(n)}{n} = 0.$$

□

[1]Infimum množiny $R = \{\frac{A(n)}{n} \mid n \in \mathbb{N}\}$ nemůže být menší, než 0, neboť na infimum množiny je kladen požadavek, aby se v jeho libovolně malém okolí vyskytoval nějaký prvek z této množiny. To nesplňuje žádné číslo menší než 0, protože všechny prvky množiny R jsou větší, nebo rovny 0.

Kapitola 4

Kongruence na množině celých čísel

4.1 Relace kongruence na množině celých čísel

Vraťme se k úvahám o dělení se zbytkem. Na základní škole jsme se naučili, že když podělíme číslo 11 číslem 4, je vyjde 2 se zbytkem 3. Neznamená to nic jiného než fakt, že

$$\mathbf{11} = 2{\cdot}\mathbf{4} + \mathbf{3}.$$

Co když k číslu 11 přičteme čtyřku, bude zbytek po dělení čtyřmi stejný? No?! No jistě, neboť

$$\mathbf{15} = 3{\cdot}\mathbf{4} + \mathbf{3}.$$

Chcete další příklad, no prosím, přičteme ještě čtyřku a vidíme, že

$$\mathbf{19} = 4{\cdot}\mathbf{4} + \mathbf{3}.$$

Opět stejný zbytek po dělení! Nyní už je snad jasné, že všechna celá čísla, která můžeme zapsat ve tvaru

$$\mathbf{z} = k{\cdot}\mathbf{4} + \mathbf{3}, \text{ kde } k \in \mathbb{Z},$$

dávají při dělení číslem 4 zbytek 3. Všechna tato čísla tvoří množinu, kterou později nazveme zbytkovou třídou modulo 4.

Proto, pokud dělíme číslem 4, rozpadá se množina celých čísel na čtyři[1] zbyt-

[1] Můžeme obdržet pouze zbytek, 0, 1, 2, nebo 3 a žádný jiný!

kové třídy modulo 4, které budeme označovat následovně:[1]

$$\begin{aligned} \overline{0} &= \{k{\cdot}4 \mid k \in \mathbb{N}\} \\ \overline{1} &= \{k{\cdot}4+1 \mid k \in \mathbb{N}\} \\ \overline{2} &= \{k{\cdot}4+2 \mid k \in \mathbb{N}\} \\ \overline{3} &= \{k{\cdot}4+3 \mid k \in \mathbb{N}\} \end{aligned} \tag{4.1}$$

Výše uvedené úvahy provedené na konkrétním příkladě můžeme zobecnit. Všechna čísla $\mathbf{z} \in \mathbb{Z}$ ve tvaru

$$\mathbf{z} = k\mathbf{m} + \mathbf{a}, \text{ kde } k \in \mathbb{Z}, 0 \leqq \mathbf{a} < \mathbf{m},$$

dávají při dělení číslem m zbytek a. Mají tedy něco společného (jsou v relaci). Říkáme, že jsou navzájem kongruentní modulo m.

Uvažme, co se stane, když od sebe odečteme dvě čísla z_1 a z_2 patřící stejné zbytkové třídy? No pokud opravdu z_1 a z_2 patří do stejné zbytkové třídy, musí mít tvar $z_1 = k_1m+a$ a $z_2 = k_2m+a$. Jejich rozdílem je pak $z_1-z_2 = (k_1-k_2)m = km$, kde $k \in \mathbb{Z}$. Výsledkem je tedy číslo dělitelné číslem m. A naopak, pokud je rozdíl dvou celých čísel dělitelný číslem m, musí tato čísla patřit do stejné zbytkové třídy modulo m.[2] Nyní už snad bude zřejmý význam následující definice.

Definice 4.1. (*Kongruence na množině* $\mathbb{Z}$) Nechť $z, a \in \mathbb{Z}$, $m \in \mathbb{N}$. Čísla z a a jsou kongruentní modulo m, právě když $z - a = km$, kde $k \in \mathbb{Z}$. Značíme

$$z \equiv a (\mathrm{mod}\, m).$$

Definici máme za sebou. Nyní dokážeme, že relace kongruence na $\mathbb{Z}$, tak jak jsme ji definovali, je relace ekvivalence na množině $\mathbb{Z}$. Česky to znamená, že kongruence má tři vlastnosti. Za prvé, každé celé číslo je kongruentní samo se sebou (jde o relaci reflexivní). Za druhé, když a je kongruentní s číslem b, pak také b je kongruentní s a (jde o relaci symetrickou). A za třetí, když a je kongruentní s číslem b a b je kongruentní s číslem c, pak a je také kongruentní s číslem c (jde o relaci tranzitivní).

Věta 4.2. *Relace kongruence modulo m je relací ekvivalence na množině celých čísel. To jest, pro každé $a, b, c \in \mathbb{Z}$ a pro každé $m \in \mathbb{N}$ platí:*

1. $a \equiv a (\mathrm{mod}\, m)$,
2. $a \equiv b (\mathrm{mod}\, m) \Rightarrow b \equiv a (\mathrm{mod}\, m)$,
3. $(a \equiv b (\mathrm{mod}\, m) \wedge b \equiv c (\mathrm{mod}\, m)) \Rightarrow a \equiv c (\mathrm{mod}\, m)$.

[1] Navíc každé celé číslo patří právě do jedné z těchto tříd. Tj. nemůže patřit do dvou různých zbytkových tříd zároveň - viz Věta 1.12.

[2] Dokažte! Viz cvičení.

Důkaz. 1. Pro každé $a \in \mathbb{Z}$ platí $a - a = 0 = 0 \cdot m$. Podle Definice 4.1 to znamená, že $a \equiv a (\mathrm{mod}\, m)$.

2. Jestliže $a \equiv b (\mathrm{mod}\, m)$ potom (viz Definice 4.1) je $a - b = km$, kde $k \in \mathbb{Z}$. A tak $b - a = -km = k^* m$, kde $k^* \in \mathbb{Z}$. Podle Definice 4.1 to znamená, že $b \equiv a (\mathrm{mod}\, m)$.

3. Předpokládejme, že $a \equiv b (\mathrm{mod}\, m) \wedge b \equiv c (\mathrm{mod}\, m)$. Z definice kongruence dostáváme

$$\left.\begin{array}{rcl} a - b & = & k_1 m \\ b - c & = & k_2 m \end{array}\right\} \Rightarrow {}^{1} \quad a - c = (k_1 - k_2)m = km, \text{ kde } k \in \mathbb{Z}. \qquad (4.2)$$

Z Definice 4.1 a (4.2) plyne, že $a \equiv c (\mathrm{mod}\, m)$. □

Ač jsme již několikrát použili pojem zbytková třída modulo m, pracovali jsme s ním zatím jen intuitivně - neuvedli jsme definici tohoto pojmu. Tento hrubý nedostatek nyní odstraníme.

Definice 4.3. (*Zbytková třída*) Nechť $r \in \mathbb{Z}$, $m \in \mathbb{N}$. Potom zbytkovou třídou modulo m nazveme množinu

$$\overline{r}_m = \{z \in \mathbb{Z} \mid z \equiv r (\mathrm{mod}\, m)\}.$$

V případě, kdy je jasné, že jde o zbytkovou třídu modulo m, použijeme místo označení $\overline{r}_m$ pouze označení $\overline{r}$.

Z Definice 4.3 a Věty 4.2 je zřejmé, že v případě, kdy číslo k patří do zbytkové třídy $\overline{r}$ modulo m (tj. $k \equiv r (\mathrm{mod}\, m)$), pak $\overline{k} = \overline{r}$, neboť

$$\overline{k}_m = \underbrace{\{z \in \mathbb{Z} \mid z \equiv k (\mathrm{mod}\, m)\} = \{z \in \mathbb{Z} \mid z \equiv r (\mathrm{mod}\, m)\}}_{\begin{array}{c}[z \equiv k (\mathrm{mod}\, m) \wedge k \equiv r (\mathrm{mod}\, m)] \;\Rightarrow\; z \equiv r (\mathrm{mod}\, m) \\ \text{proto } \overline{k}_m \subseteq \overline{r}_m, \text{ navíc} \\ \\ [z \equiv r (\mathrm{mod}\, m) \wedge k \equiv r (\mathrm{mod}\, m)] \;\Rightarrow\; z \equiv k (\mathrm{mod}\, m) \\ \text{proto } \overline{k}_m \supseteq \overline{r}_m\end{array}} = \overline{r}_m.$$

Tak například, uvažujme zbytkové třídy modulo 5. Potom platí

$$\overline{0} = \overline{5} = \overline{10} = \overline{15} = \ldots,$$
$$\overline{1} = \overline{6} = \overline{11} = \overline{16} = \ldots,$$
$$\overline{2} = \overline{7} = \overline{12} = \overline{17} = \ldots,$$

[1] Stačí sečíst uvedené dvě rovnice.

$$\overline{3} = \overline{8} = \overline{13} = \overline{18} = \dots,$$
$$\overline{4} = \overline{9} = \overline{14} = \overline{19} = \dots.$$

Jinak řečeno, nezáleží na výběru reprezentanta dané zbytkové třídy.

A ještě uvedeme v soulad Definici 4.3 s motivací uvedenou v úvodu této podkapitoly.

Lemma 4.4. *Pro každé $r \in \mathbb{Z}$, a pro každé $m \in \mathbb{N}$ platí*

$$\overline{r}_m = \{z \in \mathbb{Z} \mid z \equiv r (\mathrm{mod}\, m)\} = \{km + r \mid k \in \mathbb{Z}\}.$$

Důkaz. Důkaz tohoto lemmatu plyne přímo z definice relace kongruence na $\mathbb{Z}$. Podle ní každé číslo z splňuje kongruenci $z \equiv r (\mathrm{mod}\, m)$ právě tehdy když $z - r = k.m$ a to nastane právě tehdy když $z = km + r$. Proto číslo z patří do množiny $\{z \in \mathbb{Z} \mid z \equiv r (\mathrm{mod}\, m)\}$ právě tehdy když patří do množiny $\{km + r \mid k \in \mathbb{Z}\}$. Proto $\{z \in \mathbb{Z} \mid z \equiv r (\mathrm{mod}\, m)\} = \{km + r \mid k \in \mathbb{Z}\}$. □

Každá relace ekvivalence na dané množině rozkládá tuto množinu na takzvané třídy ekvivalence. Jedná se o množiny obsahující navzájem ekvivalentní prvky. V našem případě relace kongruence modulo m rozkládá množinu $\mathbb{Z}$ na třídy ekvivalence, které nazýváme *zbytkovými třídami modulo m* .

Toto tvrzení formulujeme jako větu.

Věta 4.5. *Označme $\overline{r} = \{z \in \mathbb{Z} \mid z \equiv r (\mathrm{mod}\, m)\}$, pro $r = 0, 1, \dots, m-1$. Potom*

1. $\mathbb{Z} = \bigcup_{r=0}^{m-1} \overline{r}$,
2. *Jestliže $r_1, r_2 \in \{0, 1, \dots, m-1\}$, $r_1 \neq r_2$, pak $\overline{r}_1 \cap \overline{r}_2 = \emptyset$.*

Důkaz. 1. Důkaz tvrzení $\mathbb{Z} = \bigcup_{r=0}^{m-1} \overline{a}$ okamžitě plyne z Věty 1.12. Podle ní pro každé $z \in \mathbb{Z}$ a pro každé $m \in \mathbb{N}$ existuje právě jedno $k \in \mathbb{Z}$ a právě jedno $r \in \mathbb{N}$, $0 \leqq r < m$ takové, že

$$z = km + r.$$

Tuto rovnost upravíme na tvar $z - r = km$. To ovšem, podle Definice 4.1, znamená, že $z \equiv r (\mathrm{mod}\, m)$. A tak $z \in \overline{r}$.

Můžeme proto tvrdit, že pro každé $z \in \mathbb{Z}$ existuje zbytková třída $\overline{r}$ do níž patří. Libovolný prvek množiny celých čísel $\mathbb{Z}$ je tedy také prvkem sjednocení množin $\bigcup_{r=0}^{m-1} \overline{r}$. Symbolicky zapsáno,

$$\mathbb{Z} \subseteq \bigcup_{r=0}^{m-1} \overline{r}. \tag{4.3}$$

Navíc, pro každé $\overline{r}$, kde $r = 0, 1, \ldots m-1$, platí $\overline{r} \subseteq \mathbb{Z}$. Musí proto být splněn vztah

$$\mathbb{Z} \supseteq \bigcup_{r=0}^{m-1} \overline{r}. \tag{4.4}$$

Z platnosti (4.3) a (4.4) pak plyne

$$\mathbb{Z} = \bigcup_{r=0}^{m-1} \overline{r}.$$

2. Provedeme důkaz sporem. Předpokládejme, že $r_1 \neq r_2$ a zároveň $\overline{r}_1 \cap \overline{r}_2 \neq \emptyset$.

   Protože $\overline{r}_1 \cap \overline{r}_2 \neq \emptyset$, musí existovat celé číslo $z \in \overline{r}_1 \cap \overline{r}_2$ To jest, $z \in \overline{r}_1$ a zároveň $z \in \overline{r}_2$. Proto

$$\begin{aligned} r_1 &\equiv z (\mathrm{mod}\, m), \\ z &\equiv r_2 (\mathrm{mod}\, m). \end{aligned} \tag{4.5}$$

   Z tranzitivnosti relace kongruence (viz Věta 4.2) pak plyne

$$r_1 \equiv r_2 (\mathrm{mod}\, m). \tag{4.6}$$

   Podle předpokladu je $0 \leqq r_1 \leqq m-1$ a také $0 \leqq r_2 \leqq m-1$. Proto

$$\begin{array}{rcccl} 0 & \leqq & r_1 & \leqq & m-1, \\ -(m-1) & \leqq & -r_2 & \leqq & 0. \end{array} \tag{4.7}$$

   Sečtením nerovnic v (4.7) obdržíme

$$-(m-1) \leqq r_1 - r_2 \leqq m-1. \tag{4.8}$$

   Z definice relace kongruence na $\mathbb{Z}$ a (4.6) plyne, že existuje $k \in \mathbb{Z}$ splňující rovnici

$$r_1 - r_2 = km. \tag{4.9}$$

   Tvrzení (4.8) a (4.9) mohou být obě pravdivá pouze v případě, že $k = 0$. Potom (viz (4.9)) platí $r_1 - r_2 = 0$, což je ekvivalentní tvrzení $r_1 = r_2$. To je ovšem spor s předpokladem $r_1 \neq r_2$.

   Předpoklad učiněný na začátku je proto nepravdivý. Pravdivá je jeho negace: Jestliže $r_1 \neq r_2$, pak $\overline{r}_1 \cap \overline{r}_2 = \emptyset$.

□

Z Věty 4.2 plyne, že množina celých čísel $\mathbb{Z}$ se rozpadá na celkem m zbytkových tříd modulo m. Jde o množiny $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

Věta 4.6. *Nechť* $a_1 \equiv b_1 (\mathrm{mod}\, m)$ *a* $a_2 \equiv b_2 (\mathrm{mod}\, m)$. *Potom*

1. $a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod}\, m)$,
2. $a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\, m)$,
3. $a_1 - a_2 \equiv b_1 - b_2 (\mathrm{mod}\, m)$.

Důkaz. 1. Předpokládejme, že $a_1 \equiv b_1 (\mathrm{mod}\, m)$ a $a_2 \equiv b_2 (\mathrm{mod}\, m)$. Potom, podle Definice 4.1 existují čísla k_1 a k_2 takové, že

$$a_1 - b_1 = k_1 m \qquad \text{a} \qquad a_2 - b_2 = k_2 m.$$

Sečtením těchto dvou rovnic obdržíme

$$(a_1 + a_2) - (b_1 + b_2) = \underbrace{(k_1 + k_2)}_{=k \in \mathbb{Z}} m.$$

To, podle Definice 4.1 znamená, že $a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod}\, m)$.

2. Jak jsme zjistili výše, předpoklady $a_1 \equiv b_1 (\mathrm{mod}\, m)$ a $a_2 \equiv b_2 (\mathrm{mod}\, m)$ říkají, že existují čísla k_1 a k_2 tak, že

$$a_1 - b_1 = k_1 m \qquad \text{a} \qquad a_2 - b_2 = k_2 m.$$

Proto

$$\begin{aligned} a_1 a_2 &= (k_1 m + b_1)(k_2 m + b_2) = \\ &= b_1 b_2 + k_1 k_2 m^2 + k_1 b_2 m + b_1 k_2 m = \\ &= b_1 b_2 + m(k_1 k_2 m + k_1 b_2 + b_1 k_2) = \\ &= b_1 b_2 + mk. \end{aligned} \tag{4.10}$$

A tak $a_1 a_2 - b_1 b_2 = km$, kde $k \in \mathbb{Z}$. Z Definice 4.1 pak plyne

$$a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\, m).$$

3. Předpokládejme, že $a_1 \equiv b_1 (\mathrm{mod}\, m)$ a $a_2 \equiv b_2 (\mathrm{mod}\, m)$. Relace kongruence je reflexivní (viz Věta 4.2), a tak $-1 \equiv -1 (\mathrm{mod}\, m)$. Užijeme výše dokázaných bodů této věty. Protože $a_2 \equiv b_2 (\mathrm{mod}\, m)$ a $-1 \equiv -1 (\mathrm{mod}\, m)$, platí, podle druhého bodu, že $-a_2 \equiv -b_2 (\mathrm{mod}\, m)$. A protože $a_1 \equiv b_1 (\mathrm{mod}\, m)$ a $-a_2 \equiv -b_2 (\mathrm{mod}\, m)$, platí, podle bodu prvního, že $a_1 + (-a_2) \equiv b_1 + (-b_2) (\mathrm{mod}\, m)$. To jest, $a_1 - a_2 \equiv b_1 - b_2 (\mathrm{mod}\, m)$.

□

Jak je možné využít poznatky Věty 4.2 a 4.6? Předvedeme na konkrétním příkladě.

Příklad 4.7. Vezměme $a = 3\,284$, $b = 2\,333$ Jaký zbytek dává $a + b$ po dělení číslem 2 a jaký zbytek dává ab po dělení číslem 3?
Řešení: Příklad bychom mohli vyřešit „hrubou silou," to jest, sečíst a a b, vynásobit a a b a pak dělením příslušným číslem zjistit, jaký dávají zbytek. Nicméně máme elegantnější řešení, neboť nebudeme muset dělit tak velká čísla, jaká bychom obdrželi při sčítání a násobení čísel a a b. Nebudeme muset čísla a a b ani sčítat ani násobit.

Uvažme, že $3\,284 \equiv 0 (\mathrm{mod}\, 2)$ ($3\,284$ je sudé, a tak po dělení číslem 2 dostaneme zbytek 0) a $2\,333 \equiv 1 (\mathrm{mod}\, 2)$ (je to číslo liché). Proto, podle Věty 4.6 platí

$$3\,284 + 2\,333 \equiv 0 + 1 (\mathrm{mod}\, c),$$

$$3\,284 + 2\,333 \equiv 1 (\mathrm{mod}\, c).$$

Znamená to, že číslo $3\,284 + 2\,333$ patří do zbytkové třídy $\overline{1}$ modulo 2, tzn. číslo $a + b$ dává po dělení číslem 2 zbytek 1.

Obdobně u součinu ab. Zjistíme, do jakých zbytkových tříd modulo 3 patří čísla a a b. Můžeme od nich postupně odečítat či přičítat násobky čísla 3 (tím dostaneme číslo menší, ale patřící do stejné zbytkové třídy), až dojdeme k číslu menšímu než 3.

$$3\,284 \equiv 3\,284 - 3\,300 \equiv -16 \equiv -16 + 18 \equiv 2 (\mathrm{mod}\, 3)$$

Obdobně,

$$2\,333 \equiv 2\,333 - 2\,100 \equiv 233 \equiv 233 - 210 \equiv 23 \equiv 2 (\mathrm{mod}\, 3).$$

Obě čísla, $3\,284$ a $2\,333$, patří do zbytkové třídy $\overline{2}$ modulo 3 (plyne to z tranzitivnosti relace kongruence a výše uvedených kongruencí. Viz Věta 4.2). Proto, podle Věty 4.6 platí

$$3\,284 \cdot 2\,333 \equiv 2 \cdot 2 (\mathrm{mod}\, 3),$$

$$3\,284 \cdot 2\,333 \equiv 4 (\mathrm{mod}\, 3),$$

$$3\,284 \cdot 2\,333 \equiv 1 (\mathrm{mod}\, 3).$$

To znamená, že když podělíme číslo $3\,284 \cdot 2\,333$ číslem 3, dostaneme zbytek 1. Jinak řečeno, číslo $3\,284 \cdot 2\,333$ ($= 7\,661\,572$) patří do zbytkové třídy $\overline{1}$ modulo 3.

Přímým důsledkem Věty 4.6 je skutečnost, že kongruence můžeme, obdobně jako rovnice, „násobit číslem." Formulujeme tento poznatek jako větu a dokážeme jej bez použití Věty 4.6.

Věta 4.8. *Nechť* $a \equiv b (\mathrm{mod}\, m)$, $c \in \mathbb{Z}$. *Potom* $ac \equiv bc (\mathrm{mod}\, m)$.

Důkaz. Podle předpokladu je $a \equiv b (\mathrm{mod}\, m)$. A tak, podle definice relace kongruence, existuje $k \in \mathbb{Z}$ takové, že $a - b = km$. Pokud obě strany rovnice vynásobíme číslem c, zůstane rovnost zachována. To jest, platí rovnost

$$ca - cb = \underbrace{ck}_{=k_1 \in \mathbb{Z}} m.$$

Z definice relace kongruence pak dostáváme $ca \equiv cb (\mathrm{mod}\, m)$. □

Věta 4.9. *Nechť* $ac \equiv bc (\mathrm{mod}\, m)$ *a* $\gcd(m, c) = 1$. *Potom* $a \equiv b (\mathrm{mod}\, m)$.

Důkaz. Z tvrzení $ac \equiv bc (\mathrm{mod}\, m)$ plyne existence celého čísla k takového, že

$$ac - bc = km.$$

Vytknutím obdržíme

$$c(a - b) = km. \tag{4.11}$$

To znamená, že číslo c dělí číslo $k.m$. A protože $\gcd(m, c) = 1$, musí číslo c dělit číslo k (viz Lema 1.23). Číslo k proto můžeme psát ve tvaru $k = ck_1$, kde $k_1 \in \mathbb{Z}$. Dosazením do (4.11) obdržíme

$$\begin{aligned} c(a - b) &= ck_1 m, \\ a - b &= k_1 m. \end{aligned} \tag{4.12}$$

Poslední rovnice je ekvivalentní s tvrzením $a \equiv b (\mathrm{mod}\, m)$ (viz Definice 4.1). □

Příklad 4.10. Předpokládejme, že celé číslo x splňuje kongruenci

$$3x \equiv 15 (\mathrm{mod}\, 7). \tag{4.13}$$

Protože $(3, 7) = 1$, můžeme kongruenci „podělit" číslem 3. Obdržíme

$$x \equiv 5 (\mathrm{mod}\, 7).$$

Je proto zřejmé, že kongruenci (4.13) splňuje každé $x \in \overline{5}_7$, tzn. každé celé číslo ve tvaru $z = k \cdot 7 + 5$ (viz Lema 4.4).

4.1.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.4.1.

1. Dokažte následující tvrzení. Pokud je rozdíl dvou celých čísel dělitelný číslem m, musí tato čísla patřit do stejné zbytkové třídy modulo m.

4.2 Lineární kongruence

Zajisté by jste bez větších problémů vyřešili lineární rovnici $3x = 6$. Obdobně bychom se mohli zamyslet, pro která celá čísla x platí $3x \equiv 5(\mathrm{mod}\, 7)$.[1] Nebo obecně, hledejme všechna $x \in \mathbb{Z}$ splňující vztah

$$ax \equiv b(\mathrm{mod}\, m), \tag{4.14}$$

kde a, b jsou daná celá čísla, $a \neq 0$.

Matematicky řečeno, lineární kongruencí s neznámou x nazveme výrokovou funkci (4.14) definovanou na množině $\mathbb{Z}$.

Ukážeme, že když celé číslo x_1 vyhovuje vztahu (4.14), pak také všechna celá čísla patřící do zbytkové třídy $\overline{x_1}$ (tj. celá čísla x_2 ve tvaru $x_2 = x_1 + km$, kde $k \in \mathbb{Z}$) vyhovují vztahu (4.14).

Věta 4.11. *Nechť a, b, x_1 jsou celá čísla a platí $ax_1 \equiv b(\mathrm{mod}\, m)$. Potom pro každé $x_2 \in \mathbb{Z}$, kde $x_1 \equiv x_2(\mathrm{mod}\, m)$, platí $ax_2 \equiv b(\mathrm{mod}\, m)$.*

Důkaz. Předpokládejme, že $x_1 \equiv x_2(\mathrm{mod}\, m)$. Podle Věty 4.8 můžeme vynásobit obě strany kongruence číslem a. Obdržíme tak kongruenci

$$ax_1 \equiv ax_2(\mathrm{mod}\, m). \tag{4.15}$$

Navíc, podle předpokladu Věty je

$$ax_1 \equiv b(\mathrm{mod}\, m). \tag{4.16}$$

Podle Věty 4.2 je relace kongruence tranzitivní. A tak z (4.15) a (4.16) plyne, že

$$ax_2 \equiv b(\mathrm{mod}\, m).$$

□

Rozmysleme si podrobně význam Věty 4.11. Příklad s čísly?

Tak tedy vezměme kongruenci $2x \equiv -2(\mathrm{mod}\, 3)$. Dosaďme za x číslo 2. Bude kongruence $4 \equiv -2(\mathrm{mod}\, 3)$ splněna? Ale ovšem, neboť $4 - (-2) = 6 = 2.3$ (vzpomeňte na definici relace kongruence).

Podle Věty 4.11 bude kongruence splněna také v případě, že za x dosadíme libovolné jiné číslo patřící do zbytkové třídy $\overline{2}_3$. To jest, čísla $\ldots, -1, 2, 5, 8, \ldots$.

Zkusit? No prosím, tak třeba $2.5 \equiv -2(\mathrm{mod}\, 3)$. Platí tato kongruence? Jistě, $10 - (-2) = 12 = 4.3$.

[1] Pak říkáme, že řešíme lineární kongruenci $3x \equiv 5(\mathrm{mod}\, 7)$

A tak docházíme k definici *řešení lineární kongruence.*

Definice 4.12. (*Řešení lineární kongruence*) Nechť jsou dána celá čísla a, b a x_0. Jestliže $ax_0 \equiv b(\mathrm{mod}\, m)$, potom zbytkovou třídu $\overline{x_0}_m$ nazveme řešením lineární kongruence $ax \equiv b(\mathrm{mod}\, m)$.

Ale dost příkladů. Naskýtá se otázka, kolik různých řešení má daná lineární kongruence.[1]

Věta 4.13. *Nechť* $\gcd(a, m) = 1$. *Potom lineární kongruence* $ax \equiv b(\mathrm{mod}\, m)$ *má jediné řešení.*

Důkaz. Nejprve ukážeme, že existuje alespoň jedno řešení kongruence

$$ax \equiv b(\mathrm{mod}\, m), \tag{4.17}$$

kde $\gcd(a, m) = 1$.

Podle předpokladu je $\gcd(a, m) = 1$. A tak existují čísla $x_0, y_0 \in \mathbb{Z}$ splňující rovnost (vizLema 1.22)

$$ax_0 + my_0 = 1.$$

Tuto rovnici vynásobíme číslem b.

$$abx_0 + mby_0 = b,$$

$$abx_0 - b = -mby_0.$$

Označme $bx_0 = x_1$ a $-by_0 = k$, potom

$$ax_1 - b = km.$$

Podle definice relace kongruence to znamená, že $ax_1 \equiv b(\mathrm{mod}\, m)$. Můžeme proto tvrdit, že zbytková třída $\overline{x_1}_m$ je řešením lineární kongruence (4.18).

Nyní ukážeme, že jde o jediné řešení. Předpokládejme, že

$$ax_1 \equiv b(\mathrm{mod}\, m) \tag{4.18}$$

a také

$$ax_2 \equiv b(\mathrm{mod}\, m). \tag{4.19}$$

Dokážeme, že v tom případě x_1 a x_2 patří do stejné zbytkové třídy modulo m, tj. $x_1 \equiv x_2(\mathrm{mod}\, m)$. Prostým odečtením kongruencí[2] obdržíme

$$ax_1 - ax_2 \equiv 0(\mathrm{mod}\, m),$$

[1] Dvě čísla patřící do téže zbytkové třídy nepovažujeme za různá řešení! Jedním řešením je celá zbytková třída.

[2] To opravdu můžeme udělat. Podle Věty 4.8 můžeme obě strany kongruence (4.19) vynásobit mínus jedničkou a takto upravenou ji podle Věty 4.6 můžeme přičíst ke kongruenci (4.18).

a přičtením ax_2 k oběma stranám kongruence dostaneme

$$ax_1 \equiv ax_2 (\mathrm{mod}\, m). \tag{4.20}$$

Podle předpokladu je $(a, m) = 1$. Můžeme proto kongruenci (4.20) podělit číslem a (viz Věta 4.9). Odtud $x_1 \equiv x_2 (\mathrm{mod}\, m)$.

□

Dále objasníme řešitelnost lineární kongruence $ax \equiv b (\mathrm{mod}\, m)$, kde $\gcd(a, m)$ je nějaké přirozené číslo d (předchozí věta řešila jen případ $d = 1$).

Věta 4.14. *Nechť $a, b \in \mathbb{Z}$, $\gcd(a, m) = d$. Lineární kongruence*

$$ax \equiv b (\mathrm{mod}\, m) \tag{4.21}$$

má řešení právě tehdy, když $d \mid b$. V případě, že d dělí číslo b, má lineární kongruence (4.21) právě d řešení.

Důkaz. Případ, kdy $\gcd(a, m) = d = 1$ je již dokázán (viz Věta 4.13). Proto dále budeme předpokládat, že $d > 1$.

Nejprve dokážeme pravdivost implikace: $ax \equiv b (\mathrm{mod}\, m)$ má řešení $\Rightarrow d \mid b$.
Předpokládejme, že $\overline{x_0}$ je řešením kongruence $ax \equiv b (\mathrm{mod}\, m)$. Potom

$$ax_0 - b = km, \tag{4.22}$$

kde $k \in \mathbb{Z}$. Podle předpokladu věty je $\gcd(a, m) = d$. Proto $a = da_1$ a $m = dm_1$, kde $a_1, m_1 \in \mathbb{Z}$. Dosazením do (4.22) obdržíme

$$da_1 x_0 - b = kdm_1,$$

$$d(a_1 x_0 - km_1) = b. \tag{4.23}$$

Rovnost (4.23) znamená, že $d \mid b$.

Nyní dokážeme pravdivost implikace: $d \mid b \Rightarrow ax \equiv b (\mathrm{mod}\, m)$ má právě d různých řešení.

Předpokládejme, že $d \mid b$. Potom $b = db_1$, kde $b_1 \in \mathbb{Z}$. Protože $d = \gcd(a, m)$, je $a = da_1$, $m = dm_1$, kde $\gcd(a_1, m_1) = 1$. Proto (viz Věta 4.13) má kongruence

$$a_1 x \equiv b_1 (\mathrm{mod}\, m_1) \tag{4.24}$$

právě jedno řešení. Řekněme, že tímto řešením je zbytková třída $\overline{x_0}_{m_1}$. Znamená to, že

$$a_1 x_0 \equiv b_1 (\mathrm{mod}\, m_1),$$

$$a_1x_0 - b_1 = km_1,$$

kde $k \in \mathbb{Z}$. Posledně uvedenou rovnici vynásobíme číslem d a obdržíme

$$da_1x_0 - db_1 = kdm_1,$$

$$ax_0 - b = km. \tag{4.25}$$

Rovnost (4.25) je ekvivalentní tvrzení

$$ax_0 \equiv b(\mathrm{mod}\, m)$$

.

Znamená to, že zbytková třída $\overline{x_0}_m$ je řešením kongruence (4.21).

Zbývá dokázat, že v případě, kdy řešení kongruence (4.21) existuje, tj. v případě $d \mid b$, existuje právě d navzájem různých zbytkových tříd modulo m, jejichž prvky splňují (po dosazení za x) kongruenci (4.21).

Jak jsme ukázali výše, existuje zbytková třída $\overline{x_0}$ modulo m_1, která je řešením kongruence $a_1x \equiv b_1(\mathrm{mod}\, m_1)$. Podle Věty 4.11 můžeme za x v kongruenci $a_1x \equiv b_1(\mathrm{mod}\, m_1)$ dosadit libovolné číslo ze zbytkové třídy $\overline{x_0}$ modulo m_1, a obdržíme pravdivý výrok. Zbytková třída $\overline{x_0}_{m_1}$ obsahuje celá čísla ve tvaru $x_0 + jm_1$, kde $j \in \mathbb{Z}$. A tak musí pro každé $j \in \mathbb{Z}$ platit

$$a_1(x_0 + jm_1) \equiv b_1(\mathrm{mod}\, m_1).$$

Podle definice relace kongruence existuje celé číslo k takové, že

$$a_1(x_0 + jm_1) - b_1 = km_1.$$

Tuto rovnici vynásobíme číslem d

$$da_1(x_0 + jm_1) - db_1 = kdm_1,$$

$$a(x_0 + jm_1) - b = km,$$

což znamená, že

$$a(x_0 + jm_1) \equiv b(\mathrm{mod}\, m). \tag{4.26}$$

Z (4.26) plyne, že pro libovolné $j \in \mathbb{Z}$ je zbytková třída $\overline{x_0 + jm_1}$ řešením kongruence $ax \equiv b(\mathrm{mod}\, m)$. Čísla j jsou celá čísla a těch je nekonečně mnoho. Znamená to, že jsme našli nekonečně mnoho řešení kongruence $ax \equiv b(\mathrm{mod}\, m)$? Ale vůbec ne! Ve skutečnosti jsme jich našli právě d. Jak to?

Čísla j nabývají následujících tvarů a v každém z uvedených tvarů je jich nekonečně mnoho[1]:

$$j = rd + 0,$$
$$j = rd + 1,$$
$$j = rd + 2,$$
$$\vdots$$
$$j = rd + (d-1),$$

kde $r \in \mathbb{Z}$.

A tak pro zbytkovou třídu $\overline{x_0 + jm_1}$ modulo m nastávají (a určitě nastanou všechny) následující možnosti:

$$j = rd + 0 \;\Rightarrow\; \overline{x_0 + jm_1} = \overline{x_0 + r\underbrace{dm_1}_{=m}} = \overline{x_0 + rm} = \overline{x_0}$$

$$j = rd + 1 \;\Rightarrow\; \overline{x_0 + jm_1} = \overline{x_0 + r\underbrace{dm_1}_{=m} + m_1} = \overline{x_0 + rm + m_1} = \overline{x_0 + m_1}$$

$$j = rd + 2 \;\Rightarrow\; \overline{x_0 + jm_1} = \overline{x_0 + r\underbrace{dm_1}_{=m} + 2m_1} = \overline{x_0 + rm + 2m_1} = \overline{x_0 + 2m_1}$$

$$\vdots$$

$$j = rd + (d-1) \;\Rightarrow\; \overline{x_0 + jm_1} = \overline{x_0 + r\underbrace{dm_1}_{=m} + (d-1)m_1} = \overline{x_0 + (d-1)m_1}$$

Každá ze zbytkových tříd $\overline{x_0 + jm_1}$ modulo m, kde $j \in \mathbb{Z}$, tedy představuje jednu ze zbytkových tříd

$$\overline{x_0},\ \overline{x_0 + m_1},\ \overline{x_0 + 2m_1}, \ldots, \overline{x_0 + (d-1)m_1}.$$

A tyto zbytkové třídy jsou navzájem různé, neboť $0 < m_1 < 2m_1 < \cdots < (d-1)m_1 < dm_1 = m$.

Prokázali jsme, že zbytkové třídy $\overline{x_0}$, $\overline{x_0 + m_1}$, $\overline{x_0 + 2m_1}$ …, $\overline{x_0 + (d-1)m_1}$ jsou řešeními kongruence $ax \equiv b (\mathrm{mod}\, m)$ (je jich d). Zbývá dokázat, že žádná jiná řešení kongruence $ax \equiv b (\mathrm{mod}\, m)$ neexistují.

Předpokládejme, že zbytková třída $\overline{x_1}$ je, stejně jako $\overline{x_0}$ řešením kongruence $ax \equiv b (\mathrm{mod}\, m)$. Tzn.

$$ax_1 \equiv b (\mathrm{mod}\, m)$$

[1] Množina celých čísel se rozpadá na d zbytkových tříd modulo d. Viz Věta 4.5.

A tak existuje celé číslo k_1 takové, že

$$ax_1 - b = k_1 m,$$

$$da_1 x_1 - db_1 = k_1 d m_1,$$

$$a_1 x_1 - b_1 = k_1 m_1.$$

Posledně uvedená rovnice znamená, že

$$a_1 x_1 \equiv b_1 (\mathrm{mod}\, m_1).$$

Můžeme proto tvrdit, že zbytková třída $\overline{x_1}$ modulo m_1 je řešením kongruence $a_1 x \equiv b_1 (\mathrm{mod}\, m_1)$. Jak jsme viděli výše, zbytková třída $\overline{x_0}$ modulo m_1 je také řešením kongruence $a_1 x \equiv b_1 (\mathrm{mod}\, m_1)$. Ale tato kongruence má jen jediné řešení, neboť $\gcd(a_1, m_1) = 1$ (viz Věta 4.13). A tak musí platit

$$x_1 \equiv x_0 (\mathrm{mod}\, m_1).$$

To jest, musí existovat $j \in \mathbb{Z}$ takové, že $x_1 - x_0 = j m_1$. A tak

$$x_1 = x_0 + j m_1.$$

Ale my již víme, že zbytková tříd $\overline{x_0 + j m_1}$ modulo m, kde $j \in \mathbb{Z}$, tedy představuje jednu z následujících zbytkových tříd (modulo m):

$$\overline{x_0},\ \overline{x_0 + m_1},\ \overline{x_0 + 2m_1}, \ldots, \overline{x_0 + (d-1)m_1}. \tag{4.27}$$

Tím jsme ověřili, že libovolné řešení kongruence $ax \equiv b (\mathrm{mod}\, m)$ je jednou ze zbytkových tříd (4.27). Jinak řečeno, jiná řešení neexistují. Dokázali jsme tak, že kongruence $ax \equiv b (\mathrm{mod}\, m)$ má právě d řešení. □

Tak jsme určili kdy a kolik řešení má zadaná lineární kongruence. Zbývá už jen vymyslet nějaký postup, jak spolehlivě a co nejsnadněji tato řešení nalézt. Okamžitě se nabízí dosadit za x do kongruence $ax \equiv b (\mathrm{mod}\, m)$ postupně všechna celá čísla od 0 do $m - 1$ a zjistit, která vyhovují. Tento postup je však pro velká m poměrně pracný. V následující poznámce popíšeme efektivnější způsob řešení lineárních kongruencí.

Poznámka 4.15. Je zadána lineární kongruence $ax \equiv b (\mathrm{mod}\, m)$. Postup při jejím řešení může být následující.

1. Určíme číslo $d = \gcd(a, m)$ (Euklidův algoritmus).

2. Rozhodneme o řešitelnosti zadané kongruence.

- Kongruence **nemá řešení** $\Leftrightarrow$ d nedělí b.
- Kongruence **má d různých řešení** $\Leftrightarrow$ d dělí b.

3. V případě, kdy d dělí b, podělíme všechna čísla (tj. čísla a, b, m) v zadané kongruenci $ax \equiv b(\mathrm{mod}\, m)$ číslem d. Obdržíme tak kongruenci

$$a_1 x \equiv b_1(\mathrm{mod}\, m_1), \tag{4.28}$$

která má jediné řešení, neboť $\gcd(a_1, m_1) = 1$.

4. Nalezneme celá čísla x_0 a y_0 tak, aby

$$x_0 a_1 + y_0 m_1 = \gcd(a_1, m_1) = 1 \tag{4.29}$$

Taková čísla existují, viz Lemma 1.22. Určit je můžeme zpětným vyjádřením $\gcd(a_1, m_1)$ z Euklidova algoritmu. Rovnici (4.33) vynásobíme číslem b_1. Dojdeme tak k rovnosti

$$x_0 b_1 a_1 + y_0 b_1 m_1 = b_1 \tag{4.30}$$

5. Místo b_1 dosadíme do (4.32) číslo $x_0 b_1 a_1 + y_0 b_1 m_1$ (viz (4.33)). Obdržíme tak kongruence

$$a_1 x \equiv x_0 b_1 a_1 + y_0 b_1 \underbrace{m_1}_{\equiv 0}(\mathrm{mod}\, m_1),$$

$$a_1 x \equiv x_0 b_1 a_1(\mathrm{mod}\, m_1),$$

$$x \equiv x_0 b_1(\mathrm{mod}\, m_1).$$

Nalezli jsme tak číslo $x_1 = x_0 b_1$ (vyhovuje kongruenci (4.32))

6. Všechna řešení zadané kongruence $ax \equiv b(\mathrm{mod}\, m)$ pak jsou zbytkové třídy

$$\overline{x_1},\ \overline{x_1 + m_1},\ \overline{x_1 + 2m_1}, \ldots, \overline{x_1 + (d-1)m_1}. \tag{4.31}$$

A teď by to chtělo konkrétní příklad. Takže hurá na to.

Příklad 4.16. Vyřešte lineární kongruenci $646x \equiv 68(\mathrm{mod}\, 782)$.

1. Určíme číslo $d = \gcd(646, 782)$. Euklidův algoritmus:

$$\begin{aligned} 782 &= 1 \cdot 646 + 136 \\ 646 &= 4 \cdot 136 + 102 \\ 136 &= 1 \cdot 102 + \mathbf{34} \\ 102 &= 3 \cdot 34 + 0 \end{aligned}$$

Proto $d = \gcd(646, 782) = 34$.

2. Rozhodneme o řešitelnosti zadané kongruence.

   Zadaná kongruence má 34 různých řešení, protože $d = 34$ dělí 68.

3. Podělíme všechna čísla v zadané kongruenci $646x \equiv 68 (\mathrm{mod}\, 782)$ číslem 34. Obdržíme tak kongruenci

$$19x \equiv 2 (\mathrm{mod}\, 23), \tag{4.32}$$

   která má jediné řešení, neboť $\gcd(19, 23) = 1$.

4. Nalezneme celá čísla x_0 a y_0 tak, aby

$$x_0 19 + y_0 23 = \gcd(19, 23) = 1 \tag{4.33}$$

   Taková čísla existují, viz Lemma 1.22. Určit je můžeme zpětným vyjádřením $\gcd(19, 23)$ z Euklidova algoritmu. Provedeme proto nejprve Euklidův algoritmus:

$$\begin{aligned} 23 &= 1 \cdot 19 + 4 && (4.34)\\ 19 &= 4 \cdot 4 + 3 && (4.35)\\ 4 &= 1 \cdot 3 + \mathbf{1} && (4.36)\\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

   Odtud dokážeme vyjádřit $\gcd(19, 23)$, tj. číslo 1, jako lineární kombinaci (součet násobků) čísel 19 a 23. Z rovnice (4.36) vyjádříme číslo 1.

$$1 = 4 - 3 \tag{4.37}$$

   Z rovnice (4.35) vyjádříme číslo $3 = 19 - 4 \cdot 4$ a dosadíme do (4.37).

$$1 = 4 - (19 - 4 \cdot 4) \tag{4.38}$$

   Z rovnice (4.34) vyjádříme číslo $4 = 23 - 19$ a dosadíme do (4.38).

$$1 = (23 - 19) - (19 - 4 \cdot (23 - 19)) \tag{4.39}$$

   Odtud

$$\begin{aligned} 1 &= 23 - 19 - 19 + 4 \cdot (23 - 19) \\ 1 &= 23 - 2 \cdot 19 + 4 \cdot 23 - 4 \cdot 19 \\ 1 &= 5 \cdot 23 - 6 \cdot 19 \end{aligned} \tag{4.40}$$

Rovnici (4.40) vynásobíme číslem 2. Dojdeme tak k rovnosti

$$2 = 10 \cdot 23 - 12 \cdot 19. \tag{4.41}$$

5. Místo čísla 2 dosadíme do (4.32) číslo $10 \cdot 23 - 12 \cdot 19$ (viz (4.41)). Obdržíme tak kongruence

$$19x \equiv 10 \cdot \underbrace{23}_{\equiv 0} - 12 \cdot 19 (\mathrm{mod}\, 23),$$

$$19x \equiv -12 \cdot 19 (\mathrm{mod}\, 23),$$

$$x \equiv -12 (\mathrm{mod}\, 23),$$

$$x \equiv 11 (\mathrm{mod}\, 23),$$

Nalezli jsme tak číslo $x_1 = 11$, které vyhovuje kongruenci (4.32).

6. Všechna řešení zadané kongruence $646x \equiv 68 (\mathrm{mod}\, 782)$ pak jsou zbytkové třídy modulo 782

$$\overline{11}, \overline{11 + 23}, \overline{11 + 46}, \ldots, \overline{11 + (34 - 1)23}.$$

To jest, zbytkové třídy

$$\overline{11}_{782}, \overline{34}_{782}, \overline{57}_{782}, \ldots, \overline{770}_{782}.$$

4.2.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.4.2.

1. Nalezněte všechna řešení lineární kongruence $14x \equiv 5 (\mathrm{mod}\, 23)$.

2. Nalezněte všechna řešení lineární kongruence $3x \equiv 15 (\mathrm{mod}\, 6)$.

3. Nalezněte všechna řešení lineární kongruence $32x \equiv 10 (\mathrm{mod}\, 46)$.

4.3 Fermatova - Eulerova věta

Fermatova - Eulerova věta je významný výsledek teorie čísel. Má nejen teoretické, ale, jak uvidíme později, i praktické využití a to při šifrování. Než budeme moci přistoupit k samotné formulaci a důkazu Fermatovy - Eulerovy věty, budeme se muset vyzbrojit řadou poznatků. Takže mějte trpělivost!

Nejprve uvažujme nějaké konkrétní m a zbytkovou třídu $\overline{a}$ modulo m. Například vezměme zbytkovou třídu $\overline{4}$ modulo 6. Je zřejmé, že $\gcd(4,6) = 2$. A jaký je největší společný dělitel ostatních čísel patřících do zbytkové třídy $\overline{4}_6$ a čísla 6? Všimněme si několika čísel patřících do $\overline{4}_6$ Vidíme, že čísla 4, 10, 16 i 22 mají všechny stejný největší společný dělitel s číslem 6 a je jím číslo 2. Je to náhoda? A jak to bude u ostatních čísel ze zbytkové třídy $\overline{4}_6$?

V následujícím Lemmatu 4.17 ukážeme obecně, že to náhoda není. Uvažujeme-li konkrétní m a zbytkovou třídu $\overline{a}$ modulo m, pak všechny čísla patřící do zbytkové třídy mají stejný největší společný dělitel s číslem m a je jím číslo $\gcd(a, m)$.

Lemma 4.17. *Nechť* $\gcd(a, m) = d$. *Potom pro každé* $x \in \overline{a}_m$ *platí* $\gcd(x, m) = d$.

Důkaz. Uvažujme libovolné $x \in \overline{a}_m$. Jak víme (Lemma 4.4), můžeme číslo x zapsat ve tvaru

$$x = km + a. \tag{4.42}$$

Ukážeme, že číslo $d = \gcd(a, m)$ je společným dělitelem čísel m a x.

Protože $d = \gcd(a, m)$, je d dělitelem čísla m i čísla a. Z toho plyne, že $m = k_1 d$ a $a = k_2 d$, kde $k_1, k_2 \in \mathbb{Z}$. Dosazením do (4.42) obdržíme

$$x = kk_1 d + k_2 d. \tag{4.43}$$

To však znamená, že

$$x = (\underbrace{kk_1 + k_2}_{k_3 \in \mathbb{Z}})d \tag{4.44}$$

a ukázali jsme tak, že d je dělitelem čísla m i čísla x. Je však d největším společným dělitelem čísel m a x? Sporem dokážeme, že ano.

Předpokládejme, že číslo D, $D > d$ je největším společným dělitelem čísel m a x, to jest $D = \gcd(x, m)$. To by znamenalo, že $m = z_1 D$ a $x = z_2 D$. Dosazením do (4.42) obdržíme

$$z_2 D = kz_1 D + a. \tag{4.45}$$

Odtud $a = z_2 D - kz_1 D = (z_2 - kz_1)D$. To by ovšem znamenalo, že číslo D je dělitelem čísla a a také musí být dělitelem čísla m (protože $D = \gcd(x, m)$). Číslo

D by pak bylo společným dělitelem čísel a a m. Ale to je spor, protože D je podle předpokladu větší, než největší společný dělitel čísel a a m!

Znamená to tedy, že číslo $d = \gcd(a, m)$ je *největším* společným dělitelem čísla x a m. To jest,

$$d = \gcd(a, m) = \gcd(x, m).$$

□

Z Lemmatu 4.17 pak plyne, že když je číslo a nesoudělné s číslem m, pak také všechny čísla ze zbytkové třídy $\overline{a}_m$ jsou nesoudělná s číslem m.

Nyní zavedeme pojem *redukovaný systém zbytkových tříd*. Nejde o nic složitého, jen ze systému všech zbytkových tříd modulo m odstraníme zbytkové třídy, které obsahují čísla soudělná[1] s číslem m.

Definice 4.18. (*Redukovaný systém zbytkových tříd*) Redukovaným systémem zbytkových tříd modulo m nazveme systém množin

$$R_m = \{\overline{a}_m \mid a \in \mathbb{Z}, \gcd(a, m) = 1\}$$

Poznámka 4.19. Počet zbytkových tříd v redukovaném systému zbytkových tříd modulo m je rovno počtu přirozených čísel menších, nebo rovných číslu m, která jsou s m nesoudělná. Toto číslo značíme $\varphi(m)$. Například $\varphi(6) = 2$, neboť mezi čísly 1, 2, 3, 4, 5, 6 jsou jen dvě, která jsou s číslem 6 nesoudělná (jsou to čísla 1 a 5).

Funkce $\varphi(m)$, která číslu m přiřazuje počet přirozených čísel menších, nebo rovných m nesoudělných s m, se nazývá *Eulerova funkce*. Blíže se s ní seznámíme v podkapitole 6.1

Dále dokážeme, že vynásobením dvou čísel nesoudělných s číslem m obdržíme opět číslo nesoudělné s m.

Lemma 4.20. *Nechť* $a, b \in \mathbb{Z}$. *Jestliže* $\gcd(a, m) = \gcd(b, m) = 1$, *potom* $\gcd(ab, m) = 1$.

Důkaz. Podle předpokladu věty je $\gcd(a, m) = \gcd(b, m) = 1$. Podle Lemmatu 1.22 existují $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ takové, že

$$ax_1 + my_1 = 1 \text{ a také } bx_2 + my_2 = 1$$

Odtud

$$\begin{aligned}(ax_1 + my_1)(bx_2 + my_2) &= 1\\ ax_1bx_2 + ax_1my_2 + my_1bx_2 + my_1my_2 &= 1\\ abx_1x_2 + m(ax_1y_2 + y_1bx_2 + y_1my_2) &= 1\end{aligned}$$

[1] To jest čísla, jejichž největší společný dělitel s číslem m je větší než 1.

Vidíme, že existují $x, y \in \mathbb{Z}$ takové, že $abx + my = 1$. Jestliže $d = \gcd(ab, m)$, pak $ab = k_1 d$ a $m = k_2 d$, kde k_1, k_2 jsou nějaká celá čísla a platí

$$\begin{aligned} abx + my &= 1 \\ k_1 dx + k_2 dy &= 1 \\ d(k_1 x + k_2 y) &= 1. \end{aligned}$$

Z poslední rovnosti vyplývá, že číslo d dělí jedničku. Proto d může být jen 1, nebo -1. Ale $d = \gcd(ab, m)$ a největší společný dělitel dvou celých čísel je z definice nezáporný. Proto $d = \gcd(ab, m) = 1$. □

Důsledek 4.21. Důsledek Lemmatu 4.20 je následující. Jestliže $\overline{a}_m$ a $\overline{b}_m$ jsou zbytkové třídy, které patří do redukovaného systému zbytkových tříd modulo m, pak také zbytková třída $\overline{ab}_m$ patří do redukovaného systému zbytkových tříd modulo m.

Jednoduše a elegantně je tento poznatek možno matematicky zapsat následujícím způsobem

$$\forall\, \overline{a}_m, \overline{b}_m \in R_m : \overline{ab}_m \in R_m.$$

Příklad 4.22. Nyní provedeme jedno malé, ale snad zajímavé pozorování. Vezměme si zbytkové třídy modulo 8 :

$$\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{7}.$$

Vyškrtneme ty zbytkové třídy, které obsahují čísla soudělná[1] s číslem 8 a zůstane nám redukovaný systém zbytkových tříd modulo 8:

$$R_8 = \left\{\overline{1},\ \overline{3},\ \overline{5},\ \overline{7}\right\}.$$

Vybereme si libovolnou z těchto zbytkových tříd. Třeba $\overline{3}$. Do to této zbytkové třídy patří například číslo tři (říkáme, že je jejím reprezentantem). Vynásobme postupně číslo 3 reprezentanty všech zbytkových tříd z R_8, to jest například čísly 1, 3, 5 a 7. Do jakých zbytkových tříd budou patřit výsledky? Jednoduše to zjistíme z následujících kongruencí

$$\begin{array}{rcrcl} \mathbf{1}\cdot 3 & = & 3 & \equiv & \mathbf{3} \pmod 8 \\ \mathbf{3}\cdot 3 & = & 9 & \equiv & \mathbf{1} \pmod 8 \\ \mathbf{5}\cdot 3 & = & 15 & \equiv & \mathbf{7} \pmod 8 \\ \mathbf{7}\cdot 3 & = & 21 & \equiv & \mathbf{5} \pmod 8 \end{array} \tag{4.46}$$

[1] Jsou to zbytkové třídy $\overline{0}$, $\overline{2}$, $\overline{4}$, a $\overline{6}$, protože $\gcd(0,8) = 8$, $\gcd(2,8) = 2$, $\gcd(4,8) = 4$ a $\gcd(6,8) = 2$.

Všimněme si čísel na pravých stranách uvedených kongruenci! Jsou zde opět reprezentanti všech zbytkových tříd z R_8, tj. čísla 3, 1, 7 a 5.

Náhoda! Náhoda? Nu což, zkusme totéž ale místo trojky budeme násobit třeba číslo 5. Obdržíme kongruence

$$\begin{array}{rcrcl} \mathbf{1}\cdot 5 & = & 5 & \equiv & \mathbf{5} (\mathrm{mod}\, 8), \\ \mathbf{3}\cdot 5 & = & 15 & \equiv & \mathbf{7} (\mathrm{mod}\, 8), \\ \mathbf{5}\cdot 5 & = & 25 & \equiv & \mathbf{1} (\mathrm{mod}\, 8), \\ \mathbf{7}\cdot 5 & = & 35 & \equiv & \mathbf{3} (\mathrm{mod}\, 8). \end{array} \tag{4.47}$$

Jak vidno, na pravých stranách kongruencí jsou opět reprezentanti všech zbytkových tříd z R_8, tj. čísla 5, 7, 1 a 3. Uvidíme, že se o náhodu nejedná. Naopak, jde o schwerpunkt důkazu Eulerovy věty! Ukažme si na konkrétním příkladu, že na pravých stranách nemohou vyjít dvě stejná čísla. Nemůže náhodou $\mathbf{3}\cdot 5$ vyjít stejně jako $\mathbf{2}\cdot 5$? Potom by muselo platit

$$\mathbf{3}\cdot 5 \equiv \mathbf{2}\cdot 5 (\mathrm{mod}\, 8). \tag{4.48}$$

Číslo 5 patří do redukovaného systému zbytkových tříd modulo 8, to znamená, že $\gcd(5, 8) = 1$ a můžeme proto v kongruenci (4.48) krátit číslem 5. Obdržíme vztah

$$\mathbf{3} \equiv \mathbf{2} (\mathrm{mod}\, 8). \tag{4.49}$$

To je ovšem spor, čísla 3 a 2 jistě nejsou kongruentní modulo 8, neboť jde o navzájem různá čísla mezi 0 a 8. Obecně pro každé $\overline{r_1}, \overline{r_2} \in R_8$, $\overline{r_1} \neq \overline{r_2}$ musí platit

$$\overline{r_1 \cdot 5}_8 \neq \overline{r_2 \cdot 5}_8.$$

Právě proto jsou všechna čísla na pravých stranách kongruencí (4.47) navzájem různá.

Dále si všimněme, že kongruencí (4.47) je přesně tolik, kolik je zbytkových tříd v R_m. Podle Poznámky 4.19 je jich $\varphi(8) = 4$. Navíc, podle Věty 4.6, můžeme čísla na levých a pravých stranách kongruencí vynásobit. Z (4.47) pak plyne

$$\begin{array}{rcl} \mathbf{1}\cdot\mathbf{3}\cdot\mathbf{5}\cdot\mathbf{7}\cdot 5^4 & \equiv & \mathbf{5}\cdot\mathbf{7}\cdot\mathbf{1}\cdot\mathbf{3} (\mathrm{mod}\, 8), \\ \mathbf{1}\cdot\mathbf{3}\cdot\mathbf{5}\cdot\mathbf{7}\cdot 5^{\varphi(8)} & \equiv & \mathbf{5}\cdot\mathbf{7}\cdot\mathbf{1}\cdot\mathbf{3} (\mathrm{mod}\, 8), \end{array} \tag{4.50}$$

Číslo $1\cdot 3\cdot 5\cdot 7$ je s číslem 8 (podle Lemmatu 4.20) nesoudělné. Proto můžeme obě strany kongruence (4.50) podělit číslem $1\cdot 3\cdot 5\cdot 7$ (Věta 4.9). Výsledný vztah má tvar

$$5^{\varphi(8)} \equiv 1 (\mathrm{mod}\, 8). \tag{4.51}$$

Obdobně bychom z kongruencí (4.46) mohli odvodit vztah

$$3^{\varphi(8)} \equiv 1 (\mathrm{mod}\, 8). \tag{4.52}$$

Vztahy (4.51) a (4.52) zobecňuje Fermatova - Eulerova věta.

Věta 4.23. (Fermatova - Eulerova) *Nechť* $\gcd(a, m) = 1$. *Potom*

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

Důkaz. Označme (viz 4.19) prvky redukovaného systému zbytkových tříd modulo m následovně

$$R_m = \{\overline{r_1}, \overline{r_2}, \ldots, \overline{r_{\varphi(m)}}\},$$

kde $1 \leqq r_i \leqq m$ pro všechna $i \in \{1, 2, \ldots, \varphi(m)\}$.

Podle předpokladu věty je číslo a nesoudělné s m a také všechna čísla r_i, $i \in \{1, 2, \ldots, \varphi(m)\}$ jsou nesoudělná s m. Proto, podle Lemmatu 4.20, je číslo ar_i nesoudělné s m. A tak můžeme říci, že $\overline{ar_i}$ je některá ze zbytkových tříd z R_m. Nevíme v tuto chvíli která, ale to nevadí, označme ji $\overline{z_i}$, kde $1 \leqq z_i \leqq m$ pro všechna $i \in \{1, 2, \ldots, \varphi(m)\}$.

Dostáváme tak soustavu kongruencí

$$\begin{aligned} ar_1 &\equiv z_1 (\mathrm{mod}\, m), \\ ar_2 &\equiv z_2 (\mathrm{mod}\, m), \\ &\vdots \\ ar_{\varphi(m)} &\equiv z_{\varphi(m)} (\mathrm{mod}\, m). \end{aligned} \tag{4.53}$$

Jejich vynásobením obdržíme

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv z_1 z_2 \cdots z_{\varphi(m)} (\mathrm{mod}\, m). \tag{4.54}$$

Čísla $z_1, z_2, \ldots, z_{\varphi(m)}$ na pravých stranách kongruencí (4.53) jsou navzájem různá, neboť ze vztahu

$$z_i \equiv z_j (\mathrm{mod}\, m)$$

okamžitě plyne

$$ar_i \equiv ar_j (\mathrm{mod}\, m)$$

a odtud[1]

$$r_i \equiv r_j (\mathrm{mod}\, m).$$

Pro $r_i \neq r_j$ proto dostáváme $z_i \neq z_j$. Je tedy zřejmé, že každé z čísel z_i je rovno některému z čísel r_i, kde $i \in \{1, 2, \ldots, \varphi(m)\}$. Proto

$$r_1 r_2 \cdots r_{\varphi(m)} = z_1 z_2 \cdots z_{\varphi(m)} \tag{4.55}$$

Dosaďíme z (4.55) do (4.54) a obdržíme tak

$$r_1 r_2 \cdots r_{\varphi(m)} a^{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} (\mathrm{mod}\, m). \tag{4.56}$$

[1] $\gcd(a, m) = 1$, v dané kongruenci proto můžeme krátit číslem a.

Číslo $r_1 r_2 \cdots r_{\varphi(m)}$ je jistě s číslem m nesoudělné, neboť všechna čísla r_1, r_2, $\ldots$, $r_{\varphi(m)}$ jsou s m nesoudělné. Můžeme proto v kongruenci (4.56) krátit číslem $r_1 r_2 \cdots r_{\varphi(m)}$. Odtud

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

□

Poznámka 4.24. Můžete si klást otázku, jak vypadá situace v případě, kdy předpoklad Frematovy - Eulerovy věty $\gcd(a, m) = 1$ není splněn. Nebylo by přesto tvrzení Fermatovy - Eulerovy věty pravdivé?

Ukážeme protipříklad! Uvažme případ, kdy $m = 6$, $a = 4$. Potom $\varphi(m) = = \varphi(6) = 2$, neboť z čísel 1, 2, 3, 4, 5, 6 jsou jen dvě nesoudělná s číslem 6. Navíc platí

$$a^{\varphi(m)} = 4^{\varphi(6)} = 4^2 = 16 \equiv 4 (\mathrm{mod}\, 6).$$

Vidíme, že v tomto případě není splněno $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

V případě, že $m = p$, kde p je prvočíslo, dostáváme speciální případ Fermatovy - Eulerovy věty, který je znám jako Malá Fermatova věta.

Věta 4.25. (Malá Fermatova) *Nechť p je prvočíslo a* $\gcd(a, p) = 1$. *Potom*

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p). \tag{4.57}$$

Důkaz. Malá Fermatova věta je přímým důsledkem obecnější Fermatovy - Eulerovy Věty 4.23. Podle ní, v případě, že $\gcd(a, p) = 1$, musí platit

$$a^{\varphi(p)} \equiv 1 (\mathrm{mod}\, p). \tag{4.58}$$

Nyní si stačí jen uvědomit, že $\varphi(p)$ je počet čísel nesoudělných s číslem p, které vybíráme z množiny $\{1, 2, \ldots, p-1, p\}$. Ale p je prvočíslo, proto jsou všechny čísla z této množiny s p nesoudělná – kromě jediného, a to čísla p. Proto $\varphi(p) = p - - 1$. Nyní jen stačí dosadit za $\varphi(p)$ do kongruence (4.58). Obdržíme toužebně očekávaný vztah

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

□

Poznámka 4.26. Můžete si klást otázku, zda je předpoklad $\gcd(a, p) = 1$ v Malé Fermatově větě nutný. V případě obecnější Fermatovy - Eulerovy Věty 4.23 předpoklad $\gcd(a, m) = 1$ nutný byl, jak jsme viděli v Poznámce 4.24. U speciálního tvrzení by však možná nebyl nepostradatelný, ne?

Ne! Požadavek $\gcd(a, p) = 1$ v Malé Fermatově větě nutný opravdu je. Uvažme, že p je prvočíslo. Potom v případě, kdy $\gcd(a, p) \neq 1$, je jediná možnost $\gcd(a, p) = = p$. Znamená to, že a je násobkem čísla p. Proto

$$a \equiv 0 (\mathrm{mod}\, p),$$

a odtud

$$a^{p-1} \equiv 0 (\mathrm{mod}\, p).$$

Tvrzení Malé Fermatovy věty by bez předpokladu $\gcd(a, p) = 1$ nebylo pravdivé. Někdy ale bývá Malá Fermatova věta formulována ve tvaru, kde se obejdeme bez tohoto předpokladu:

Věta 4.27. (Malá Fermatova) *Nechť p je prvočíslo. Potom*

$$a^p \equiv a (\mathrm{mod}\, p).$$

Tvrzení v tomto tvaru je pravdivé jak v případě $\gcd(a, p) = 1$ (plyne pak přímo z Malé Fermatovy věty, vynásobíme-li kongruenci (4.57) číslem a), tak v případě $\gcd(a, p) \neq 1$. To jest, v případě $\gcd(a, p) = p$, kdy kongruence

$$\underbrace{a^p}_{\equiv 0} \equiv \underbrace{a}_{\equiv 0} (\mathrm{mod}\, p)$$

říká jen to, že

$$0 \equiv 0 (\mathrm{mod}\, p).$$

4.3.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.4.3.

1. V Poznámce 4.24 bylo ukázáno, že kongruence $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ nemusí být splněna v případě, kdy $\gcd(a, m) \neq 1$. Existují nějaká čísla a a m, taková, že $\gcd(a, m) \neq 1$ a přitom platí $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$?

2. Pomocí Fermatovy věty nalezněte $x \in \{0, 1, \ldots, 6\}$ splňující kongruenci $x \equiv 2^3 28 (\mathrm{mod}\, 7)$.

3. Pomocí Fermatovy věty nalezněte $x \in \{0, 1, 2\}$ splňující kongruenci $5x \equiv 1 (\mathrm{mod}\, 3)$.

4. Pomocí Fermatovy věty nalezněte $x \in \{0, 1, 2\}$ splňující kongruenci $2x^2 + 5x + 1 \equiv 0 (\mathrm{mod}\, 3)$.

Kapitola 5

Operace na $\mathbb{Z}_n$

V algebře se zavádí obecné pojmy *inverzní prvek* a *neutrální prvek*. Jejich význam objasníme nejprve na konkrétních příkladech a poté definujeme pojem inverzního a neutrálního prvku pouze pro náš konkrétní případ.

Takže nejprve pár příkladů. Vždy budeme potřebovat nějakou množinu a na ní definovanou operaci. Nejprve něco ze základní školy. Vezměme množinu všech celých čísel $\mathbb{Z}$. A operaci *sčítání celých čísel*. Neutrálním prvkem vzhledem ke sčítání celých čísel je číslo 0, neboť ať vezmu jakékoli číslo $z \in \mathbb{Z}$, a přičtu k němu nulu, vůbec nic se nestane, to jest $a + 0 = 0 + a = a$ (přesně to požadujeme od neutrálního prvku). Inverzní prvek k číslu $a \in \mathbb{Z}$ je to číslo $x \in \mathbb{Z}$ splňující rovnost $a + x = x + a = 0$. To jest, sečtením prvku a jeho prvku inverzního vzhledem ke sčítání musí vyjít neutrální prvek vzhledem ke sčítání. Příklad s konkrétními čísly:

$$3 + (-3) = 0.$$

Proto číslo -3 je prvkem inverzním k číslu 3 vzhledem ke sčítání celých čísel. Obdobně číslo -5 je prvkem inverzním k číslu 5 vzhledem ke sčítání celých čísel a tak dále.

Nicméně nemusíme se omezit pouze na operaci sčítání celých čísel. Jako další příklad vezměme operaci násobení celých čísel. Neutrálním prvkem vzhledem k násobení celých čísel je číslo 1, neboť pro libovolné $a \in \mathbb{Z}$ platí $a \cdot 1 = 1 \cdot a = a$.

Dokážete nalézt prvek inverzní k prvku -1 vzhledem k násobení celých čísel? No ano, výborně, je jím samo číslo -1, neboť $(-1)\cdot(-1) = 1$. Vynásobením prvku a jeho inverze vzhledem k násobení musí vyjít prvek neutrální vzhledem k násobení. Dokážeme najít prvek inverzní vzhledem k násobení celých čísel k prvku 3? Ne, nenajdeme! Neexistuje celé číslo x, které by splňovalo $x \cdot 3 = 1$. Takové x sice známe, je jím číslo $\frac{1}{3}$, ale to není číslo celé! Je to číslo racionální. Proto můžeme říci, že číslo 3 nemá inverzní prvek vzhledem k násobení celých čísel. Ale má inverzní prvek $\frac{1}{3}$ vzhledem k násobení racionálních čísel (trojka je celé, ale i racionální číslo).

Nu a jakou my si zvolíme množinu a operaci pro další zkoumání? Označme $\mathbb{Z}_n$ množinu všech zbytkových tříd modulo n. To bude množina našeho zájmu.

A operace? Budeme násobit zbytkové třídy. To jde? Ale ano, fantazii se meze nekladou, klidně můžeme vymyslet násobení prasátek v chlívku. Stačilo by definovat, které prasátko má vyjít pokud vynásobíme Pašíka s Mařenkou, které vyjde po vynásobení Aleška s Karlem a tak dál. My se ale vraťme k násobení zbytkových tříd. V definici popíšeme jak na to.

Definice 5.1. Operaci $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ (násobení zbytkových tříd modulo n) definujeme pro každé $\overline{a}_n, \overline{b}_n \in \mathbb{Z}_n$ předpisem

$$\overline{a}_n \cdot \overline{b}_n = \overline{ab}_n$$

Pro jednoduchost budeme místo zápisu $\overline{a}_n \cdot \overline{b}_n$ používat zápis $\overline{a}_n\overline{b}_n$. V případě, kdy je jasné, že jde o zbytkové třídy modulo n, budeme zápis $\overline{a}_n \cdot \overline{b}_n$ zkracovat na $\overline{a}\overline{b}$.

Jak vidno z Věty 4.6, nezáleží na výběru reprezentantů ze zbytkových tříd $\overline{a}$ a $\overline{b}$, proto je naše definice násobení zbytkových tříd modulo n korektní[1].

Příklad 5.2. Uvažujme množinu zbytkových tříd modulo 6. To jest, množinu $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Podle definice $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$, $\overline{2} \cdot \overline{5} = \overline{10} = \overline{4}$ a tak dále. Všechny možné součiny v $\mathbb{Z}_6$ můžeme znázornit v Tabulce 5.1. Pro přehlednost zápisu v tabulce pro označení zbytkové třídy $\overline{a}$ použijeme pouze a. Například místo $\overline{2}$ napíšeme pouze číslo 2. Chceme-li v tabulce nalézt součin zbytkových tříd $\overline{3}$ a $\overline{4}$, stačí se podívat na číslo, které je v řádku nadepsaném číslem **3** a v sloupci nadepsaném číslem **4**. Je jím číslo 0, což znamená, že $\overline{3} \cdot \overline{4} = \overline{0}$.

Tab. 5.1 Tabulka násobení v $\mathbb{Z}_6$.

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

[1] Výběr reprezentantů by obecně vzato mohl být problém. Ukážeme si na konkrétních číslech. Vezměme zbytkové třídy modulo 5. Podle Definice 5.1 platí $\overline{3}_5\overline{4}_5 = \overline{12}_5$. My však víme, že $\overline{3}_5 = \overline{8}_5$ a také $\overline{4}_5 = \overline{9}_5$. Potom ale $\overline{3}_5\overline{4}_5 = \overline{8}_5\overline{9}_5 = \overline{72}_5$. Dospěli jsme tak zdánlivě ke dvěma různým výsledkům $\overline{3}_5\overline{4}_5 = \overline{12}_5$ a $\overline{3}_5\overline{4}_5 = \overline{72}_5$. Problém by nastal, kdyby $\overline{12}_5 \neq \overline{72}_5$. My ale díky Větě 4.6 víme, že když $3 \equiv 8 (\mathrm{mod}\, 5)$ a také $4 \equiv 9 (\mathrm{mod}\, 5)$, pak $3 \cdot 4 \equiv 8 \cdot 9 (\mathrm{mod}\, 5)$. To jest, $12 \equiv 72 (\mathrm{mod}\, 5)$. To ale znamená, že $\overline{12}_5 = \overline{72}_5$. A opravdu, $\overline{12}_5 = \overline{72}_5 = \overline{2}_5$.

Věta 5.3. *Operace $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, násobení zbytkových tříd modulo n, je komutativní. To jest, pro každé $\overline{a}_n, \overline{b}_n \in \mathbb{Z}_n$ platí*

$$\overline{a}_n \cdot \overline{b}_n = \overline{b}_n \cdot \overline{a}_n$$

Důkaz. Důkaz je založen na komutativnosti operace násobení celých čísel. Potom

$$\overline{a}_n \cdot \overline{b}_n = \overline{ab}_n = \overline{ba}_n = \overline{b}_n \cdot \overline{a}_n.$$

□

Poznamenejme, že v Tabulce 5.1 se komutativnost násobení zbytkových tříd projeví v její symetričnosti podle diagonály. Dále definujeme neutrální prvek vzhledem k násobení zbytkových tříd.

Definice 5.4. Neutrálním prvkem vzhledem k operaci $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ (násobení zbytkových tříd modulo n) je zbytková třída $\overline{i}_n \in \mathbb{Z}_n$ splňující pro každé $\overline{a}_n \in \mathbb{Z}_n$ rovnosti

$$\overline{i}_n \cdot \overline{a}_n = \overline{a}_n$$

Zbytková třída $\overline{i}_n$ z Definice 5.4, jež má býti neutrálním prvkem vzhledem k násobení zbytkových tříd, je poněkud záhadná. V tuto chvíli nevíme konkrétně, která to je. Odhalme její totožnost!

Věta 5.5. *Neutrálním prvkem vzhledem k operaci $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ (násobení zbytkových tříd modulo n) je zbytková třída $\overline{1}_n \in \mathbb{Z}_n$.*

Důkaz. Důkaz je založen na poznatku, že číslo 1 je neutrálním prvkem vzhledem k operaci násobení celých čísel. Potom je zřejmé, že pro každé $\overline{a}_n \in \mathbb{Z}_n$ jsou splněny rovnosti

$$\overline{1}_n \cdot \overline{a}_n = \overline{1 \cdot a}_n = \overline{a}_n.$$

□

Konečně se dostáváme k definici pojmu inverzního prvku vzhledem k násobení zbytkových tříd.

Definice 5.6. Zbytkovou třídu $\overline{x}_n$ nazveme inverzním prvkem k prvku $\overline{a}_n$ vzhledem k operaci násobení zbytkových tříd modulo n, právě když platí

$$\overline{x}_n \cdot \overline{a}_n = \overline{1}_n.$$

Značíme $\overline{x}_n = {\overline{a}_n}^{-1}$. V případě, kdy je jasné, že jde o zbytkové třídy modulo n, budeme zápis $\overline{x}_n = {\overline{a}_n}^{-1}$ zkracovat na $\overline{x} = \overline{a}^{-1}$. Zbytkovou třídu ${\overline{a}_n}^{-1}$ též nazýváme multiplikativní inverzí k $\overline{a}_n$.

Definici máme za sebou. Vyvstává problém jak k zadané zbytkové třídě najít její inverzi? A existuje ke každé zbytkové třídě inverze?

Příklad 5.7. Zjistíme, které zbytkové třídy modulo 9 mají vzhledem k násobení inverzi. Prozkoumejme Tabulku 5.2, kde je popsáno násobení zbytkových tříd modulo 9.

Tab. 5.2 Tabulka násobení v $\mathbb{Z}_9$.

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8
2	0	2	4	6	8	**1**	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	**1**	5
5	0	5	**1**	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	**1**	8	6	4	2
8	0	8	7	6	5	4	3	2	**1**

Je z ní patrno, že

$$\overline{1}\cdot\overline{1} = \overline{1} \Rightarrow \overline{1}^{-1} = \overline{1},$$

$$\overline{2}\cdot\overline{5} = \overline{1} \Rightarrow \overline{2}^{-1} = \overline{5},$$

$$\overline{4}\cdot\overline{7} = \overline{1} \Rightarrow \overline{4}^{-1} = \overline{7},$$

$$\overline{5}\cdot\overline{2} = \overline{1} \Rightarrow \overline{5}^{-1} = \overline{2},$$

$$\overline{7}\cdot\overline{4} = \overline{1} \Rightarrow \overline{7}^{-1} = \overline{4}.$$

$$\overline{8}\cdot\overline{8} = \overline{1} \Rightarrow \overline{8}^{-1} = \overline{8}.$$

Zjistili jsme tak, že inverzi vzhledem k násobení v $\mathbb{Z}_9$ mají pouze zbytkové třídy $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{7}$ a $\overline{8}$, neboť nikdy jindy při násobení zbytkových tříd modulo 9 nevyjde číslo 1. Všimněme si, že $\gcd(1,9) = 1$, $\gcd(2,9) = 1$, $\gcd(4,9) = 1$, $\gcd(5,9) = 1$ a také $\gcd(7,9) = 1$. Proti tomu $\gcd(0,9) = 9 > 1$, $\gcd(3,9) = 3 > 1$, $\gcd(6,9) = 3 > 1$. V dalším textu ukážeme, že to není náhoda.

Dále si všimněme, že ty zbytkové třídy, k nimž existuje inverzní prvek, mají jediný inverzní prvek.

Věta 5.8. *Zbytková třída $\overline{x}_n \in \mathbb{Z}_n$ je multiplikativní inverzí zbytkové třídy $\overline{a}_n \in \mathbb{Z}_n$ právě tehdy, když*

$$ax \equiv 1 (\mathrm{mod}\, n).$$

Důkaz. Tvrzení Věty 5.8 je přímým důsledkem Definice 5.6 (definice inverzního prvku), neboť rovnost $\overline{x}_n \cdot \overline{a}_n = \overline{1}_n$ je splněna právě tehdy (viz Definice 5.1) když $\overline{xa}_n = \overline{1}_n$. To je ovšem ekvivalentní s tvrzením $ax \equiv 1 (\mathrm{mod}\, n)$. □

Věta 5.9. *Zbytková třída $\overline{a}_n \in \mathbb{Z}_n$ má multiplikativní inverzi právě tehdy, když*

$$\gcd(a, n) = 1.$$

Pokud multiplikativní inverze existuje, pak je jediná.

Důkaz. Podle Věty 5.8 má zbytková třída $\overline{a}_n \in \mathbb{Z}_n$ multiplikativní inverzi $\overline{x}_n \in \mathbb{Z}_n$ právě tehdy, když

$$ax \equiv 1 (\mathrm{mod}\, n). \tag{5.1}$$

Kongruence (5.1) má však řešení právě tehdy, když $\gcd(a, n) = 1$ a toto řešení je jediné (viz Věta 4.14). □

5.0.2 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.5.1.

1. Věta 5.5 říká, že neutrálním prvkem vzhledem k operaci násobení zbytkových tříd modulo n je zbytková třída $\overline{1}_n$. Nemůže ale roli neutrálního prvku hrát i jiná zbytková třída ze Z_n? Dokažte, že ne, že existuje pouze jediný neutrální prvek vzhledem k operaci násobení zbytkových tříd (Definice 5.1).

2. Dokažte, že ke každému prvku v $Z_n - \{\overline{0}_n\}$ existuje jeho prvek inverzní (vzhledem k násobení) právě tehdy, když n je prvočíslo.

3. Vytvořte tabulku násobení zbytkových tříd modulo 7.

4. Pomocí tabulky násobení v Z_7 vyřešte lineární kongruence $3x \equiv 2 (\mathrm{mod}\, 7)$ a $-5x \equiv -2 (\mathrm{mod}\, 7)$.

Kapitola 6

Aritmetické funkce

Jako aritmetické funkce označujeme ty reálné, či komplexní funkce, jejichž definičním oborem je množina přirozených čísel. Za aritmetickou funkci tak vlastně můžeme považovat libovolnou posloupnost reálných, nebo komplexních čísel. Nicméně zajímavé pro nás budou v dalším textu jen nemnohé z nich.

Například nás bude zajímat, kolik různých dělitelů má číslo 6. Snadno zjistíme, že děliteli šestky jsou čísla 1, 2, 3 a 6. Jsou tedy celkem čtyři. Jak ale jistě tušíte, bude nás zajímat, jak určit počet dělitelů obecně pro nějaké číslo n. Použijeme standardní matematickou fintu. Označme pro každé přirozené číslo n počet jeho dělitelů jako $\sigma_0(n)$. Vytvořili jsme tak funkci[1], která číslu n přiřazuje počet jeho dělitelů $\sigma_0(n)$. Zbývá již jen drobnost - prozkoumat vlastnosti této funkce a pravým splněním snu by byl objev nějakého jednoduchého předpisu[2] umožňujícího určit hodnotu $\sigma_0(n)$ pro zadané n.

Podobně můžeme definovat funkci σ_1, kde $\sigma_1(n)$ označuje součet dělitelů[3] čísla n. Našemu zájmu se ovšem jako první bude těšit takzvaná Eulerova funkce φ, kde $\varphi(n)$ označuje počet čísel menších, nebo rovných n, která jsou s n nesoudělná.

6.1 Eulerova funkce

Nejprve uvedeme definici Eulerovy funkce

Definice 6.1. (*Eulerova funkce*) Eulerova funkce φ je dána předpisem

$$\varphi(n) = \#\left\{k \in \{1, 2, \ldots, n\} \mid \gcd(k, n) = 1\right\}.$$

To jest, $\varphi(n)$ je počet čísel menších, nebo rovných n, která jsou s n nesoudělná.

[1] A již jsme určili i jednu z jejích nekonečně mnoha funkčních hodnot: $\sigma_0(6) = 4$:) !

[2] Je tu samozřejmě možnost projít všechna čísla menší, nebo rovná n a zjistit, která jsou děliteli čísla n. Nicméně tento postup je pracný a neuspokojuje naši potřebu nalézt nějaké vychytrale jednoduché řešení zadaného problému.

[3] Například $\sigma_1(6) = 1 + 2 + 3 + 6 = 12$.

Poznámka 6.2. Vzhledem k tvrzení Lemmatu 4.17 můžeme tvrdit, že $\varphi(n)$ má též význam počtu zbytkových tříd modulo n, které obsahují čísla nesoudělná s n. To jest, počet prvků redukovaného systému zbytkových tříd modulo n je roven $\varphi(n)$.

Nyní si položme otázku, jak určit hodnotu $\varphi(n)$ pro zadané n. Všimněme si, že v případě, kdy n je rovno nějakému prvočíslu p, je to jednoduché. S prvočíslem p jsou nesoudělná všechna čísla menší než p a je jich $p-1$. Například s prvočíslem 5 jsou nesoudělná čísla 1, 2, 3 a 4. Proto $\varphi(5) = 4$ Tento náš první objev můžeme zformulovat následovně.

Věta 6.3. *Pro každé prvočíslo p platí*

$$\varphi(p) = p - 1.$$

Jak však určíme $\varphi(n)$ v případě, že n není prvočíslo? Pro tento účel je možné využít znalosti kanonického rozkladu čísla n. Než tak ale učiníme, vydáme se ve studiu zdánlivě jiným směrem. Prostudujme nejprve jeden konkrétní příklad.

Příklad 6.4. Uvažujme dvě nesoudělná čísla, například 4 a 3. A dále vypočtěme všechna čísla ve tvaru $a4 + b3$, kde za a budeme dosazovat čísla z množiny $\{0, 1, \ldots, 3-1\}$ a za b čísla z množiny $\{0, 1, \ldots, 4-1\}$. Pro přehlednost uvedeme výsledky v tabulce

$a\backslash b$	0	1	2	3
0	$0\cdot4+0\cdot3=0$	$0\cdot4+1\cdot3=3$	$0\cdot4+2\cdot3=6$	$0\cdot4+3\cdot3=9$
1	$1\cdot4+0\cdot3=4$	$1\cdot4+1\cdot3=7$	$1\cdot4+2\cdot3=10$	$1\cdot4+3\cdot3=13$
2	$2\cdot4+0\cdot3=8$	$2\cdot4+1\cdot3=11$	$2\cdot4+2\cdot3=14$	$2\cdot4+3\cdot3=17$

Nic zajímavého? Možná na první pohled, ale zkuste si určit, do jakých zbytkových tříd modulo $4\cdot3 = 12$ obdržené výsledky patří. Tabulka pak bude vypadat takto:

$a\backslash b$	0	1	2	3
0	$0\cdot4+0\cdot3\equiv$ **0**	$0\cdot4+1\cdot3\equiv$ **3**	$0\cdot4+2\cdot3\equiv$ **6**	$0\cdot4+3\cdot3\equiv$ **9**
1	$1\cdot4+0\cdot3\equiv$ **4**	$1\cdot4+1\cdot3\equiv$ **7**	$1\cdot4+2\cdot3\equiv$ **10**	$1\cdot4+3\cdot3\equiv$ **1**
2	$2\cdot4+0\cdot3\equiv$ **8**	$2\cdot4+1\cdot3\equiv$ **11**	$2\cdot4+2\cdot3\equiv$ **2**	$2\cdot4+3\cdot3\equiv$ **5**

Už je to překvapivější? V tabulce se objevily všechny zbytky modulo 12. Každé ze zkoumaných čísel ve tvaru $a4+b3$, kde za a budeme dosazovat čísla z množiny $\{0, 1, \ldots, 3-1\}$ a za b čísla z množiny $\{0, 1, \ldots, 4-1\}$ tak patří do jiné zbytkové

třídy modulo 12. A protože takových čísel je právě 12, jsou tato čísla reprezentanty *všech* zbytkových tříd modulo 12.

Výsledek předchozího příkladu není náhodný. Zobecníme jej pro libovolná nesoudělná čísla m a n (v Příkladu 6.4 bylo $m = 4$ a $n = 3$.).

Lemma 6.5. *Nechť jsou dána čísla* m, n, *kde* $\gcd(m, n) = 1$. *Potom*

$$\left\{\overline{am + bn}_{mn} \mid a \in \{0, 1, \ldots, n-1\}, b \in \{0, 1, \ldots, m-1\}\right\} = \mathbb{Z}_{mn}$$

Důkaz. Co že to vlastně máme dokázat?! Vytvořme všechna čísla ve tvaru $am+bn$, kde m a n jsou zadaná nesoudělná čísla. Kolik takových čísel je? To je jednoduché! Za a dosazujeme čísla z množiny $\{0, 1, \ldots, n-1\}$. Máme proto n možností pro a. Obdobně, za b dosazujeme čísla z množiny $\{0, 1, \ldots, m-1\}$. Máme proto m možností pro b. Máme tak mn možností jak zvolit dvojici čísel (a, b).

Celkový počet čísel v požadovaném tvaru $am + bn$ je tedy mn. Vidíme, že je jich právě tolik, kolik je zbytkových tříd modulo mn, to jest prvků množiny $\mathbb{Z}_{mn}$. Čísla v uvažovaném tvaru $am+bn$ by tak možná mohly patřit každé do jiné zbytkové třídy modulo mn. Ale je tomu skutečně tak? Patří čísla $am + bn$ každé do jiné zbytkové třídy modulo mn? Cílem je ukázat, že ano, že pro různé dvojice (a, b) vycházejí čísla $am + bn$, která nejsou kongruentní modulo mn.

Vezmeme dvě čísla $a_1m + b_1n$ a $a_2m + b_2n$ a zjistíme, kdy jsou kongruentní modulo mn. Řešíme proto kongruenci

$$a_1m + b_1n \equiv a_2m + b_2n (\mathrm{mod}\, mn). \tag{6.1}$$

Podle Definice 4.1 (relace kongruence) vztah (6.1) znamená, že existuje $k \in \mathbb{Z}$ takové, že

$$(a_1m + b_1n) - (a_2m + b_2n) = kmn.$$

Po úpravě obdržíme

$$m(a_1 - a_2 - kn) = n(b_2 - b_1)$$

Čísla m a n jsou nesoudělná, musí proto platit, že

$$m \mid (b_2 - b_1) \text{ a zároveň } n \mid (a_1 - a_2 - kn). \tag{6.2}$$

Vztahy (6.2) můžeme zapsat ve tvaru

$$b_2 \equiv b_1 (\mathrm{mod}\, m) \text{ a zároveň } a_1 \equiv a_2 + \underbrace{kn}_{\equiv 0} (\mathrm{mod}\, n).$$

Odtud

$$b_2 \equiv b_1 (\mathrm{mod}\, m) \text{ a zároveň } a_1 \equiv a_2 (\mathrm{mod}\, n). \tag{6.3}$$

Čísla b_2, b_1 patří do množiny $\{0, 1, \ldots, m-1\}$. Mají-li být kongruentní modulo m, jak je uvedeno v (6.3), není jiná možnost, než že jsou si rovny.

Také čísla $a_2, a_1 \in \{0, 1, \ldots, n-1\}$. Proto, mají-li být kongruentní modulo n, jak je uvedeno v (6.3),musí si být rovny.

Dospěli jsme tak k závěru, že $a_1 = a_2$ a také $b_1 = b_2$. A to jsme potřebovali! Proč? Tak si to shrňme. Dokázali jsme implikaci

$$a_1 m + b_1 n \equiv a_2 m + b_2 n (\mathrm{mod}\, mn) \Rightarrow (a_1, b_1) = (a_2, b_2). \tag{6.4}$$

Výrok logicky ekvivalentní s (6.4) je věta obměněná (viz metoda nepřímého důkazu 0.4). A tak můžeme říci, že pro různé dvojice $(a_1, b_1) \neq (a_2, b_2)$ patří čísla $a_1 m + b_1 n$ a $a_2 m + b_2 n$ do různých zbytkových tříd. A to jsme chtěli dokázat.

□

Výsledek je to pěkný, což o to, ale k čemu nám bude?! Vydržte, včas se dozvíte! Uděláme ještě jednu odbočku, a to k definici multiplikativní funkce.

Definice 6.6. (Multiplikativní funkce) Aritmetickou funkci f nazveme multiplikativní funkcí, právě když pro každé m, n, kde $\gcd(m, n) = 1$ platí

$$f(mn) = f(m)f(n).$$

Celkem snadno zjistíme, že ne každá funkce je multiplikativní. Vezměme například aritmetickou funkci danou předpisem $f(n) = 3n$. Můžeme zvolit například $m = 2$, $n = 3$, což jsou nesoudělná čísla, ale

$$f(2{\cdot}3) = f(6) = 3{\cdot}6 = 18 \neq f(2)f(3) = 3{\cdot}2{\cdot}3{\cdot}3 = 54.$$

Existují ale nějaké funkce, které multiplikativní jsou? Ano, tušíte správně! Dokážeme, že námi zkoumaná funkce φ je multiplikativní.

Věta 6.7. *Eulerova funkce φ je multiplikativní. To jest, pro každé m, n, kde* $\gcd(m, n) = 1$ *platí*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Důkaz. Určíme hodnotu $\varphi(mn)$. Využijeme poznatku Lemmatu 6.5. To říká, že do každé ze zbytkových tříd modulo mn patří právě jedno z čísel ve tvaru $am+bn$, kde m a n jsou zadaná nesoudělná čísla, $a \in \{0, 1, \ldots, n-1\}$, $b \in \{0, 1, \ldots, m-1\}$. Zjistíme, kolik z těchto čísel je nesoudělných s číslem mn. To jest, zajímá nás, kdy platí

$$\gcd(am + bn, mn) = 1 \tag{6.5}$$

Rovnost nastane právě tehdy, když platí[1]

$$\gcd(am + bn, m) = 1 \text{ a zároveň } \gcd(am + bn, n) = 1 \tag{6.6}$$

[1]Je nutné a postačuje, aby $am + bn$ bylo nesoudělné jak s m, tak s n.

Dále uvažme, že rovnosti (6.6) nastanou právě tehdy, když platí

$$\gcd(bn, m) = 1 \text{ a zároveň } \gcd(am, n) = 1 \tag{6.7}$$

Protože $\gcd(m, n) = 1$ (předpoklad věty), nastanou rovnosti (6.7) právě když

$$\gcd(b, m) = 1 \text{ a zároveň } \gcd(a, n) = 1 \tag{6.8}$$

Dospěli jsme tak k závěru, že číslo $am + bn$ je nesoudělné s číslem mn (rovnost 6.5) právě když b je nesoudělné s m a a je nesoudělné s n (rovnosti 6.8). Takových čísel b nalezneme v množině $\{0, 1, \ldots, m-1\}$ právě $\varphi(m)$ a čísel a nesoudělných s n nalezneme v množině $\{0, 1, \ldots, n-1\}$ právě $\varphi(n)$. Počet dvojic čísel a a b, kde $\gcd(b, m) = 1$ a $\gcd(a, n) = 1$ je proto roven $\varphi(m)\varphi(n)$.

Existuje proto právě $\varphi(m)\varphi(n)$ čísel $am + bn$, kde $a \in \{0, 1, \ldots, n-1\}$, $b \in \{0, 1, \ldots, m-1\}$, která jsou nesoudělná s mn. Existuje proto právě $\varphi(m)\varphi(n)$ zbytkových tříd modulo mn, které obsahují čísla nesoudělná[1] s mn. Jinak řečeno, počet prvků redukovaného systému zbytkových tříd modulo mn je roven $\varphi(m)\varphi(n)$. Podle Poznámky 6.2 to ale znamená, že

$$\varphi(mn) = \varphi(m)\varphi(n).$$

□

Výborně, tak jsme dokázali, že Eulerova funkce je multiplikativní! Světový mír tento výsledek asi nezajistí, ale my jsme již připraveni najít předpis pro nalezení hodnoty $\varphi(n)$ v případě, že známe kanonický rozklad čísla n. Dokonce bude stačit ještě méně, a to znalost všech prvočísel, která dělí n a čísla n samotného.

Věta 6.8. *Nechť $n > 1$ a $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, kde p_1, p_2, …, p_k jsou navzájem různá prvočísla. Potom*

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Důkaz. Nejprve zjistíme, jaká je funkční hodnota Eulerovy funkce v nějaké mocnině prvočísla. To jest, hledáme $\varphi(p^\alpha)$, v případě, že p je prvočíslo, $\alpha \in \mathbb{N}$. Zjišťujeme počet přirozených čísel menších, nebo rovných p^α, nesoudělných s p^α. Uděláme to tak, že od počtu všech přirozených čísel menších, nebo rovných p^α odečteme počet čísel soudělných s p^α.

Která čísla jsou ale soudělná s p^α? No jen ty, která ve svém kanonickém rozkladu mají prvočíslo p. Jde tedy o všechny násobky prvočísla p, které jsou mezi jedničkou a p^α:

$$1p, 2p, \ldots, p^{\alpha-1}p = p^\alpha.$$

[1] Jsou to právě ty zbytkové třídy, které obsahují číslo v uvažovaném tvaru $am + bn$, které je nesoudělné s mn. Viz Lemma 4.17

Vidíme, že takových násobků je právě $p^{\alpha-1}$. Proto

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right). \tag{6.9}$$

Nyní využijeme Větu 6.7, která říká, že funkce φ je multiplikativní. Čísla $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}$ a $p_k^{\alpha_k}$ jsou zcela jistě nesoudělná, neboť $p_1, p_2, \ldots, p_k$ jsou navzájem různá prvočísla. Proto podle Věty 6.7 můžeme psát

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}})\varphi(p_k^{\alpha_k}). \tag{6.10}$$

Obdobně $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-2}^{\alpha_{k-2}}$ a $p_{k-1}^{\alpha_{k-1}}$ jsou zcela jistě nesoudělná. Proto podle Věty 6.7 a předchozí rovnosti (6.10) můžeme psát

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}})\varphi(p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-2}^{\alpha_{k-2}})\varphi(p_{k-1}^{\alpha_{k-1}})\varphi(p_k^{\alpha_k}).$$

Stejným způsobem můžeme pokračovat dál a dál až dospějeme ke vztahu

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}). \tag{6.11}$$

Podle (6.9) je $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$ dosazením do (6.11) obdržíme

$$\varphi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right),$$

$$\varphi(n) = \underbrace{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}_{n} \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right),$$

$$\varphi(n) = n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

□

Příklad 6.9. A opravdu to funguje? Zkusme a potěšme se výsledkem. Tak třeba $\varphi(24)$? Nejprve to zkusme hrubou silou. Mezi čísly 1 až 24 najdeme čísla nesoudělná s 24. Jsou to čísla

$$1, 5, 7, 11, 13, 17, 19, 23$$

a je jich celkem 8. Proto $\varphi(24) = 8$.

Nyní to zkusme s využitím Věty 6.8. Nalezneme kanonický rozklad čísla 24.

$$24 = 3{\cdot}8 = 3{\cdot}2^3.$$

Proto ($p_1 = 3$, $p_2 = 2$)

$$\varphi(24) = 24\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{2}\right) = 24\frac{2}{3}\frac{1}{2} = 24\frac{1}{3} = \mathbf{8}.$$

Zázrak! Zázrak? Ne! Vždyť jsme to dokázali!

Dlužno poznamenat, že Věta 6.8 umožňuje jednoduše určit $\varphi(n)$ jen v případě „malých“ čísel, nebo u „velkých“ n, jejichž kanonické rozklady známe. Je tomu tak proto, že nalezení kanonických rozkladů „velkých“ čísel je „velký“ problém.

6.1.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.6.1.

1. Vyřešte Příklad 2.4 pro libovolnou číselnou soustavu. Kolik procent přirozených čísel můžeme vyloučit v případě použití číselné soustavy o základu n?

2. Jaké n je třeba v předchozím příkladě zvolit, abychom maximalizovali procento přirozených čísel u kterých můžeme vyloučit podezření z prvočíselnosti?

3. Označme $n_k = \prod_{i=1}^{k} p_i$, kde $\{p_i\}_{i=1}^{\infty}$ je posloupnost všech prvočísel. Dále označme $\alpha_k = 1 - \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$. Dokažte, že $\lim_{k\to\infty} \alpha_k \cdot 100\% = 100\%$. To jest, dokažte, že postupem popsaným v řešeních předchozích příkladů je možné při volbě dostatečně velkého n_k vyloučit z podezření, že jde o prvočísla, libovolně velké procento čísel.

6.2 Funkce sigma

V úvodu této kapitoly jsme již zmínili funkce σ_0 a σ_1. V této podkapitole nejprve uvedeme definici funkce σ_α pro libovolné $\alpha \in \mathbb{R}$.

Definice 6.10. (*Funkce σ_α*) Funkce σ_α je dána pro každé $\alpha \in \mathbb{R}$ předpisem

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha,$$

kde $d \geqq 1$. To jest, $\sigma_\alpha(n)$ je součet kladných dělitelů čísla n umocněných na α.

Poznámka 6.11. Poznamenejme, že i v této kapitole se budeme držet následující úmluvy. Malými písmeny budeme označovat čísla z množiny přirozených čísel. Pokud tomu bude jinak, například uvažujeme-li čísla z množiny celých čísel, bude to uvedeno. Proto zápis v Definici 6.10

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha,$$

znamená totéž co

$$\sigma_\alpha(n) = \sum_{d|n, d\geqq 1} d^\alpha.$$

Pro jednoduchost a vzhledem k výše popsané úmluvě budeme i nadále používat zápis $\sum_{d|n}$ místo zápisu $\sum_{d|n, d\geqq 1}$.

V Definici 6.10 jsme nedefinovali jedinou funkci, ale nekonečně mnoho různých funkcí. Pro každé α dostáváme jinou funkci. V případě, kdy zvolíme $\alpha = 0$ dostáváme:

Definice 6.12. (*Funkce* σ_0) Funkce σ_0 je dána předpisem

$$\sigma_0(n) = \sum_{d|n} d^0 = \sum_{d|n} 1.$$

To jest, $\sigma_0(n)$ je součet jedniček. A kolik těch jedniček je? No přece tolik, kolik je dělitelů čísla n. Proto $\sigma_0(n)$ je rovno počtu dělitelů čísla n.

Příklad 6.13. Vzhledem k úmluvě popsané v Poznámce 6.11 platí

$$\sigma_0(6) = \sum_{d|6} d^0 = 1^0 + 2^0 + 3^0 + 6^0 = 1 + 1 + 1 + 1 = 4,$$

Neboť čísla 1, 2, 3 a 6 jsou jedinými děliteli čísla 6.

Jak určit hodnotu $\sigma_0(n)$ pro dané n? V případě, kdy známe kanonický rozklad čísla n to není nic těžkého.

Věta 6.14. *Nechť* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, *kde* p_1, p_2, ...,p_k *jsou navzájem různá prvočísla. Potom pro každé* $n > 1$ *platí*

$$\sigma_0(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

Pro $n = 1$ *platí* $\sigma_0(1) = 1$.

Příklad 6.15. Díky Větě 6.14 můžeme tvrdit, že číslo $n = 3^4 \cdot 5^6 \cdot 7^3$ má

$$\sigma_0(n) = (1 + 4)(1 + 6)(1 + 3) = 5 \cdot 7 \cdot 4 = 140$$

různých kladných dělitelů.

Důkaz. Dokažme nyní tvrzení Věty 6.14. Číslo 1 má jediného dělitele (a to číslo 1). Proto $\sigma_0(1) = 1$.

Dále uvažujme $n > 1$. Důkaz je v tomto případě kombinatorické povahy. Nechť tedy $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, kde p_1, p_2, ...,p_k jsou navzájem různá prvočísla. Otázka zní, kolik má číslo $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ různých dělitelů? Uvažme, že každé číslo d, $d = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$, kde $c_1 \in \{0, 1, \ldots, \alpha_1\}$, $c_2 \in \{0, 1, \ldots, \alpha_2\}$, ..., $c_k \in \{0, 1, \ldots, \alpha_k\}$, je dělitelem čísla n a žádní jiní dělitelé čísla n neexistují. A kolik takových čísel d je? Pro volbu c_1 máme $(\alpha_1 + 1)$ možností[1]. Obdobně pro volbu c_2 máme $(\alpha_2 + 1)$ možností. A tak dále. Celkový počet možností jak zvolit hodnotu koeficientů c_1, c_2, ...,c_k je proto roven

$$(\alpha_1 + 1)\,(\alpha_2 + 1) \cdots (\alpha_k + 1)\,.$$

Nyní si už jen stačí uvědomit, že pro různé volby hodnot koeficientů c_1, c_2, ...,c_k dostáváme různé dělitele čísla n. Proto

$$\sigma_0(n) = (\alpha_1 + 1)\,(\alpha_2 + 1) \cdots (\alpha_k + 1)\,.$$

□

Z Věty 6.14 plyne, že funkce σ_0 je multiplikativní

Věta 6.16. *Funkce σ_0 je multiplikativní. To jest, pro každé m, n, kde $\gcd(m, n) = 1$ platí*

$$\sigma_0(mn) = \sigma_0(m)\sigma_0(n).$$

Důkaz. Vezměme dvě čísla m, n, kde $\gcd(m, n) = 1$. Zcela jistě je možné tyto dvě čísla napsat ve formě kanonického rozkladu. Řekněme

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \text{ a } n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}.$$

Odtud s využitím Věty 6.14 dostáváme

$$\sigma_0(m) = (\alpha_1 + 1)\,(\alpha_2 + 1) \cdots (\alpha_r + 1) \tag{6.12}$$

a

$$\sigma_0(n) = (\beta_1 + 1)\,(\beta_2 + 1) \cdots (\beta_s + 1) \tag{6.13}$$

Protože čísla m a n jsou nesoudělná ($\gcd(m, n) = 1$), jsou jistě prvočísla $p_1, p_2, \ldots, p_r$ a $q_1, q_2, \ldots, q_s$ navzájem různá. Proto

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

je kanonický rozklad čísla mn. Podle Věty 6.14 platí

$$\sigma_0(mn) = (\alpha_1 + 1)\,(\alpha_2 + 1) \cdots (\alpha_s + 1)\,(\beta_1 + 1)\,(\beta_2 + 1) \cdots (\beta_s + 1)\,. \tag{6.14}$$

Srovnáním (6.12), (6.13) a (6.14) zjistíme, že

$$\sigma_0(mn) = \sigma_0(m)\sigma_0(n).$$

□

[1] Neboť $c_1 \in \{0, 1, \ldots, \alpha_1\}$.

Příklad 6.17. Čísla 4 a 7 jsou nesoudělná, přičemž $\sigma_0(4) = 3$ (1, 2 a 4 jsou všichni kladní dělitelé čísla 4) a $\sigma_0(7) = 2$ (1 a 7 jsou všichni kladní dělitelé čísla 7). Díky Větě 6.16 můžeme tvrdit, že číslo $n = 4 \cdot 7 = 28$ má

$$\sigma_0(28) = \sigma_0(4)\sigma_0(7) = 3 \cdot 2 = 6$$

různých kladných dělitelů. A opravdu, čísla 1, 2, 4, 7, 14 a 28 jsou jediní kladní dělitelé čísla 28.

Nyní se vraťme k Definici 6.10, kde jsou definovány funkce σ_α. Zvolíme-li $\alpha = 1$, obdržíme definici funkce σ_1.

Definice 6.18. (*Funkce* σ_1) Funkce σ_1 je dána předpisem

$$\sigma_1(n) = \sum_{d|n} d.$$

To jest, $\sigma_1(n)$ je součet všech kladných dělitelů čísla n.

Příklad 6.19. Děliteli čísla 10 jsou čísla 1, 2, 5 a 10. Proto

$$\sigma_1(n) = \sum_{d|n} d = 1 + 2 + 5 + 10 = 18.$$

Obdobně jako u funkce σ_0 si můžeme položit otázku, zda je možné nějakým způsobem určit hodnotu $\sigma_1(n)$ ze znalosti kanonického rozkladu čísla n. Odpověď dává následující věta.

Věta 6.20. *Nechť* $n > 1$ *a* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, *kde* $p_1, p_2, \ldots, p_k$ *jsou navzájem různá prvočísla a* $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$. *Potom*

$$\sigma_1(n) = \frac{\left(p_1^{\alpha_1+1} - 1\right)}{p_1 - 1} \frac{\left(p_2^{\alpha_2+1} - 1\right)}{p_2 - 1} \cdots \frac{\left(p_k^{\alpha_k+1} - 1\right)}{p_k - 1}.$$

Příklad 6.21. Dříve než Větu 6.20 dokážeme, ukážeme si, jak s její pomocí vyřešit Příklad 6.19. Hledáme součet dělitelů čísla 10. Kanonický rozklad čísla 10 má tvar $10 = 2^1 5^1$. Proto

$$\sigma_1(n) = \sum_{d|n} d = \underbrace{\frac{2^2 - 1}{2 - 1}}_{3} \underbrace{\frac{5^2 - 1}{5 - 1}}_{6} = 18.$$

Důkaz. Důkaz Věty 6.20 začíná obdobně jako Důkaz Věty 6.14. Nechť $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, kde p_1, p_2, …,p_k jsou navzájem různá prvočísla. Uvažme, že každé číslo d,

$$d = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k},$$

kde $c_1 \in \{0, 1, \ldots, \alpha_1\}$, $c_2 \in \{0, 1, \ldots, \alpha_2\}$, $\ldots$, $c_k \in \{0, 1, \ldots, \alpha_k\}$, je dělitelem čísla n a žádní jiní dělitelé čísla n neexistují. Součet všech dělitelů čísla n, tj. hodnotu $\sigma_1(n)$, proto dostaneme roznásobením závorek na pravé straně následující rovnosti:

$$\begin{aligned}\sigma_1(n) &= \left(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}\right)\cdots \\ &\quad \cdots\left(1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k}\right).\end{aligned} \tag{6.15}$$

Nyní vzpomeňme na vzorec známý již od střední školy. Pro $\alpha \in \mathbb{N}$ platí

$$(p^{\alpha+1} - 1) = (p - 1)(1 + p + p^2 + \cdots + p^{\alpha}),$$

z čehož plyne

$$\frac{(p^{\alpha+1} - 1)}{p - 1} = (1 + p + p^2 + \cdots + p^{\alpha}).$$

Pak je již zřejmé, že rovnici (6.15) můžeme přepsat do tvaru

$$\sigma_1(n) = \frac{\left(p_1^{\alpha_1+1} - 1\right)}{p_1 - 1}\frac{\left(p_2^{\alpha_2+1} - 1\right)}{p_2 - 1}\cdots\frac{\left(p_k^{\alpha_k+1} - 1\right)}{p_k - 1}.$$

□

Obdobně jako u funkce σ_0 dokážeme, že i funkce σ_1 je multiplikativní.

Věta 6.22. *Funkce σ_1 je multiplikativní. To jest, pro každé m, n, kde* $\gcd(m, n) = 1$ *platí*

$$\sigma_1(mn) = \sigma_1(m)\sigma_1(n).$$

Důkaz. Vezměme dvě čísla m, n, kde $\gcd(m, n) = 1$. Zcela jistě je možné tyto dvě čísla napsat ve formě kanonického rozkladu. Řekněme

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \text{ a } n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}.$$

Odtud s využitím Věty 6.20 dostáváme

$$\sigma_1(m) = \frac{\left(p_1^{\alpha_1+1} - 1\right)}{p_1 - 1}\frac{\left(p_2^{\alpha_2+1} - 1\right)}{p_2 - 1}\cdots\frac{\left(p_r^{\alpha_r+1} - 1\right)}{p_r - 1} \tag{6.16}$$

a

$$\sigma_1(n) = \frac{\left(q_1^{\beta_1+1} - 1\right)}{q_1 - 1}\frac{\left(q_2^{\beta_2+1} - 1\right)}{q_2 - 1}\cdots\frac{\left(q_s^{\beta_s+1} - 1\right)}{q_s - 1} \tag{6.17}$$

Protože čísla m a n jsou nesoudělná ($\gcd(m, n) = 1$), jsou jistě prvočísla $p_1, p_2, \ldots, p_r$ a $q_1, q_2, \ldots, q_s$ navzájem různá. Proto

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

je kanonický rozklad čísla mn. Podle Věty 6.14 platí

$$\begin{aligned}\sigma_1(mn) &= \frac{\left(p_1^{\alpha_1+1}-1\right)}{p_1-1}\frac{\left(p_2^{\alpha_2+1}-1\right)}{p_2-1}\cdots\frac{\left(p_r^{\alpha_r+1}-1\right)}{p_r-1} \\ &\quad \frac{\left(q_1^{\beta_1+1}-1\right)}{q_1-1}\frac{\left(q_2^{\beta_2+1}-1\right)}{q_2-1}\cdots\frac{\left(q_s^{\beta_s+1}-1\right)}{q_s-1}.\end{aligned} \tag{6.18}$$

Srovnáním (6.16), (6.17) a (6.18) zjistíme, že

$$\sigma_1(mn) = \sigma_1(m)\sigma_1(n).$$

□

6.2.1 Cvičení

Výsledky, návody k řešení a řešení příkladů tohoto cvičení naleznete v odstavci 8.6.2.

1. Dokažte, že číslo p je prvočíslo právě tehdy, když $\sigma_0(p) = 2$.
2. Dokažte, že oborem hodnot funkce σ_0 je množina $\mathbb{N}$.
3. Dokažte, že $\liminf_{n\to\infty} \sigma_0(n) = 2$.
4. Dokažte, že $\limsup_{n\to\infty} \sigma_0(n) = \infty$.

Kapitola 7

Aplikace teorie čísel v kryptografii

Ač se může zdát, že celá teorie čísel je jen v praxi nepoužitelné hraní s čísly, není tomu tak. I pro výsledky našich hrátek s čísly se našly aplikace. Především v kódování a šifrování. Například takové čárové kódy. Nejde jen o to přidělit určitému druhu zboží číslo. Co když se nějakým řízením osudu jedno z čísel smaže, nebo při zpracování dojde k chybě a dvě čísla si vymění pozici? Je možné tyto chyby detekovat a opravit? Obdobné otázky vyvstávají při používání kódu ISBN pro identifikaci knih. Nejvíce se ale teorie čísel vyznamenala v šifrování. S její pomocí je dnes možné velice dobře ochránit soukromí v komunikaci (například mezi zákazníkem a bankou).

7.1 Šifrování s veřejným klíčem

Představme si hypotetickou situaci. Zlý Gargamel pochytal všechny malé Šmoulíky a zavřel je do svého hradu, pouze Taťka Šmoula unikl. Taťka Šmoula dlouho uvažoval, jak své Šmoulíky vysvobodit. Zjistil, že existuje pouze jediná útěková cesta z jinak útěkuvzdorného a nedobytného hradu. Pomocí svého poštovního holuba by mohl Šmoulíkům předat zprávu s plánem útěku. Hrozí však nebezpečí, že Gargamel zprávu zachytí a poslední slabinu svého hradu odstraní. Šmoulíci by pak již nikdy nemohli býti vysvobozeni. Taťka Šmoula se přesto rozhodl poslat zprávu Koumákovi, ale je třeba ji zašifrovat!

Pro tyto příležitosti se jako neocenitelný jeví šifrovací systém s následujícími vlastnostmi

- Každý Šmoula (a tedy i Taťka Šmoula) ví, jak poslat Koumákovi šifrovanou zprávu. Koumák zveřejnil svůj *veřejný klíč* - způsob, jak zprávu pro něj zašifrovat.

- Pouze Koumák (Gargamel ne a ani Taťka Šmoula by to neuměl!) umí takto

zašifrovanou zprávu dešifrovat. Pouze on disponuje svým *soukromým klíčem*, kterým odemkne tajemství zašifrované zprávy.

Naštěstí Šmoulové tak úžasným šifrovacím systémem disponují! Je jím RSA algoritmus.

7.2 Algoritmus RSA

Název algoritmu RSA vznikl z počátečních písmen jmen jeho objevitelů,[1] jimiž byli pánové Rivest, Shamir a Adelman. Jedná se o kryptosystém pracující s veřejným klíčem. Odolnost šifrování pomocí RSA algoritmu je založena na naší neschopnosti rozložit velká čísla na součin prvočísel, neboť tato úloha je nesmírně výpočetně náročná. A jak to funguje?

Nejprve pro Koumáka vytvoříme veřejný a soukromý klíč. Vezměme dvě prvočísla p a q. Jejich vynásobením obdržíme $n = pq$. Podle Věty 6.7 a Věty 6.3 platí $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Vybereme *šifrovací exponent* $\mathrm{e} \in \mathbb{N}$ tak, aby platilo $\gcd(\mathrm{e}, \varphi(n)) = 1$. Dvojice čísel n a e bude tvořit Koumákův *veřejný klíč* - budou (a musí) jej znát všichni, kdo mu chtějí poslat šifrovanou zprávu.

Koumákovým *soukromým klíčem* bude číslo $d \in \{1, \ldots, \varphi(n) - 1\}$ splňující kongruenci

$$\mathrm{e} \cdot d \equiv 1 (\mathrm{mod}\, \varphi(n)) \tag{7.1}$$

Takové číslo d určitě existuje a je jediné - tvrdí to Věta 4.13.

Postup při šifrování je pak následující. Text převedeme na sekvenci čísel. Každé číslo m z této sekvence musí splňovat podmínku $m < n$. Číslo m pak zašifrujeme jeho umocněním na e mnodulo n. To jest, zašifrovaný text m je číslo $c \in \{0, \ldots, n-1\}$ splňující kongruenci

$$c \equiv m^{\mathrm{e}} (\mathrm{mod}\, n). \tag{7.2}$$

Tatka Šmoula pošle Koumákovi v dopise číslo c. Koumák použije svůj soukromý klíč d tak, že obdržené číslo c umocní na d a k výsledku nalezne jeho zbytek po dělení číslem n. Jaké číslo obdrží? Tušíte správně, bude to číslo m (pouze ve výjimečných případech se tak nestane - uvidíme později), které už jen znovu převede do řeči písmen. Plyne to z následujících kongruencí

[1] Pro přesnost je třeba uvést, že zmiňovaní pánové jsou prvními, kdo svůj objev RSA algoritmu z roku 1976 publikovali. Nicméně Britská bezpečnostní služba GCHQ (Government Communications Headquarters) tento šifrovací systém objevila pravděpodobně již v roce 1973. Americká NSA dokonce tvrdí, že myšlenka RSA jí byla známa již v 60-tých letech 20. století. Obě zmiňované organizace ovšem svůj objev z pochopitelných důvodů tajily až do doby, kdy byl veřejně znám vinou pánů Rivesta, Shamira a Adelmana.

$$c^d \equiv (m^{\mathrm{e}})^d \equiv m^{\mathrm{e}d} \equiv m^{k\varphi(n)+1} \equiv \left(m^{\varphi(n)}\right)^k \cdot m \equiv m(\mathrm{mod}\, n). \tag{7.3}$$

Třetí z výše uvedených kongruencí plyne z toho, že $\mathrm{e}d \equiv 1(\mathrm{mod}\, \varphi(n))$ (viz (7.1)). Proto $\mathrm{e}d = k\varphi(n) + 1$, kde $k \in \mathbb{Z}$. Poslední kongruence je splněna s jistotou - využijeme-li Eulerovu větu - pouze za předpokladu $\gcd(m, n) = 1$, potom $m^{\varphi(n)} \equiv 1(\mathrm{mod}\, n)$ (viz Věta 4.23).

Co se však stane, když $\gcd(m, n) \neq 1$?! Pro „velké“ hodnoty čísel n, p a q je tato situace velice nepravděpodobná. Uvažme, že $n = pq$. Proto mezi čísly $0, 1, \ldots, n-1$ jsou s číslem n soudělná jen ta, která jsou násobkem čísla p, nebo q. Proto dešifrování může selhat pouze v případě, pokud Taťka Šmoula pošle číslo $c = 1p, 2p, \ldots, (q-1)p$, nebo $c = 1q, 2q, \ldots, (p-1)q$. Jde tedy o $p+q-2$ různých čísel z $n = pq$ čísel. Klasická pravděpodobnost takové události je potom rovna $\frac{1}{q} + \frac{1}{p} - \frac{2}{pq}$. Pro „velké“ hodnoty p a q se hodnota této pravděpodobnosti blíží nule.

Tak s tímto vysvětlením se možná v některých publikacích spokojí (viz [3]). Nás by však čekaly bezesné noci. Co když RSA algoritmus selže právě v okamžiku bankovní transakce po které by na našem kontě měla přistát tučná suma peněz?! Pro klid své duše dokážeme, že se tak nestane. Budeme potřebovat následující lemma.

Lemma 7.1. *Nechť p, q jsou dvě navzájem nesoudělná čísla. Potom pro každé $k \in \mathbb{N}$ platí*

$$p^{k\varphi(pq)+1} \equiv p(\mathrm{mod}\, pq).$$

Důkaz. Podle předpokladu věty je $\gcd(p, q) = 1$. Podle Věty 4.23 pak platí

$$p^{\varphi(q)} \equiv 1(\mathrm{mod}\, q).$$

Umocněním obou stran kongruence číslem $k\varphi(p)$ obdržíme

$$p^{k\varphi(p)\varphi(q)} \equiv 1(\mathrm{mod}\, q). \tag{7.4}$$

Z definice relace kongruence na $\mathbb{Z}$ snadno odvodíme, že v případě platnosti vztahu $a \equiv b(\mathrm{mod}\, m)$ platí také $pa \equiv pb(\mathrm{mod}\, pm)$. Z kongruence (7.4) pak plyne

$$p \cdot p^{k\varphi(p)\varphi(q)} \equiv p(\mathrm{mod}\, pq)$$

a odtud (funkce φ je multiplikativní, proto $\varphi(p)\varphi(q) = \varphi(pq)$ - viz Věta 6.7)

$$p^{k\varphi(pq)+1} \equiv p(\mathrm{mod}\, pq).$$

□

Poznámka 7.2. Všimněme si, že Lemma 7.1 má v předpokladech pouze to, že $\gcd(p, q) = 1$. To bude splněno i pokud je zaměníme, neboť $\gcd(p, q) = \gcd(q, p)$. A tak musí platit nejenom vztah $p^{k\varphi(pq)+1} \equiv p(\mathrm{mod}\, pq)$, ale i vztah $q^{k\varphi(pq)+1} \equiv q(\mathrm{mod}\, pq)$.

Pomocí Fermatovy - Eulerovy věty (Věta 4.23), Lemmatu 7.1 a Poznámky 7.2 odvodíme, že i v případě, kdy šifrovaná zpráva je násobek čísla p, nebo q, bude RSA fungovat tak jak má.

Nechť tedy $m = zp^r q^s$, kde $\gcd(z, pq) = 1$. Potom šifrovaná zpráva je $c \equiv m^{\mathrm{e}} (\mathrm{mod}\, pq)$. Dešifrovanou zprávu bychom měli dostat jako $m \equiv c^d (\mathrm{mod}\, pq)$. A opravdu

$$\begin{aligned} c^d &\equiv (m^{\mathrm{e}})^d (\mathrm{mod}\, pq) \\ c^d &\equiv m^{\mathrm{e}d} (\mathrm{mod}\, pq) \\ c^d &\equiv (zp^r q^s)^{k\varphi(pq)+1} (\mathrm{mod}\, pq) \\ c^d &\equiv z^{k\varphi(pq)+1} (p^{k\varphi(pq)+1})^r (q^{k\varphi(pq)+1})^s (\mathrm{mod}\, pq) \\ c^d &\equiv zp^r q^s (\mathrm{mod}\, pq) \\ c^d &\equiv m (\mathrm{mod}\, pq) \end{aligned} \tag{7.5}$$

Příklad 7.3. Vytvořte pro Koumáka jeho veřejný a soukromý klíč pro RSA algoritmus!

Řešení: Pro jednoduchost vezmeme dvě poměrně malá prvočísla $p = 31$ a $q = 37$. Potom $n = 31 \cdot 37 = 1147$. První část veřejného klíče máme. Zbývá najít číslo $\mathrm{e} \in \{1, \ldots, \varphi(n)\}$ tak, aby $\gcd(\mathrm{e}, \varphi(n)) = 1$. Protože

$$\varphi(n) = \varphi(31 \cdot 37) = 30 \cdot 36 = 1080,$$

hledáme $\mathrm{e} \in \mathbb{N}$ v intervalu $(1, 1080)$. Jeho hodnotu zvolíme náhodně, například vezměme $\mathrm{e} = 11$, ale musíme, nejlépe pomocí Euklidova algoritmu, ověřit, zda $\gcd(\mathrm{e}, \varphi(n)) = \gcd(11, 1080) = 1$.

$$\begin{aligned} 1080 &= 98 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + \mathbf{1}. \end{aligned} \tag{7.6}$$

Vidíme, že největším společným dělitelem čísel $\mathrm{e} = 11$ a $\varphi(n) = 1080$ je číslo 1. Můžeme proto použít $\mathrm{e} = 11$ jako šifrovací exponent. Veřejný klíč máme hotov, je jím dvojice čísel $\mathbf{n} = \mathbf{1147}$ a $\mathrm{e} = 11$.

Nyní nalezneme soukromý klíč $d \in \{1, \ldots, \varphi(n)\}$ tak, aby vyhovoval kongruenci

$$\mathrm{e} \cdot d \equiv 1 (\mathrm{mod}\, \varphi(n)). \tag{7.7}$$

V našem případě do (7.7) dosadíme $\mathrm{e} = 11$ a $\varphi(n) = 1080$. Řešíme tak kongruenci

$$11 \cdot d \equiv 1 (\mathrm{mod}\, 1080). \tag{7.8}$$

K vyřešení této kongruence využijeme zpětné vyjádření $\gcd(11, 1080)$ z rovnic Euklidova algoritmu (7.6).

Z poslední rovnice (7.6) dostáváme

$$1 = 11 - 2 \cdot 5. \tag{7.9}$$

Z první rovnice (7.6) vyjádříme $2 = 1080 - 98 \cdot 11$ a dosadíme do (7.9). Obdržíme

$$1 = 11 - (1080 - 98 \cdot 11) \cdot 5 = (-5) \cdot 1080 + 11 \cdot 491$$

Odtud plyne, že $11 \cdot 491 = 5 \cdot 1080 + 1$. Proto

$$11 \cdot 491 \equiv 1 (\mathrm{mod}\, 1080).$$

Ze srovnání s (7.7) je jasné, že hledaný soukromý klíč je $d = 491$.

Příklad 7.4. Pomozte zašifrovat Taťkovi Šmoulovi jeho geniální plán k útěku! Vzkaz je určen pro Koumáka, jehož veřejný klíč je $\mathbf{n} = \mathbf{1147}$, $e = 11$ a text zprávy zní: „UTEČTE DVEŘE NEJSOU ZAMČENÉ“.

Řešení: Nejprve převedeme vzkaz na sekvenci čísel, která jsou menší, než $\mathbf{n} = \mathbf{1147}$. Vidíme, že stačí napsat vzkaz jako sekvenci trojciferných čísel[1] Můžeme postupovat následovně. Každý ze znaků vzkazu (písmena i mezery) nahradíme jednoznačně dvojciferným číslem. Vzniklou posloupnost čísel rozdělíme na trojčíslí.

U	T	E	Č	T	E		D	V	E	Ř	E	
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
10	11	12	13	11	12	14	15	16	12	17	12	14

N	E	J	S	O	U		Z	A	M	Č	E	N	É
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
18	12	19	20	21	10	14	22	23	24	13	12	18	25

Slovo „UTEČTE“ tak představuje sekvence trojčíslí 101 112 131 112. Zašifrujeme tato čísla pomocí veřejného klíče $\mathbf{n} = \mathbf{1147}$, $e = 11$.

Nejprve potřebujeme nalézt zbytek po dělení čísla $(101)^e = (101)^{11}$ číslem $\mathbf{n} = \mathbf{1147}$. Hledáme tedy $c \in \{1, \ldots, 1147\}$ splňující kongruenci

$$c \equiv (101)^{11} (\mathrm{mod}\, \mathbf{1147})$$

[1] Každé tojciferné číslo $ABC < 1000 < \mathbf{1147} = \mathbf{n}$.

Umocněním $(101)^{11}$ bychom dostali poměrně velké číslo. Můžeme postupovat chytřeji.

$$(101)^2 \equiv 10\,201 \equiv 1\,025 (\mathrm{mod}\, \mathbf{1147}). \tag{7.10}$$

Proto

$$(101)^4 \equiv (1\,025)^2 \equiv 1\,050\,625 \equiv 1\,120 (\mathrm{mod}\, \mathbf{1147}). \tag{7.11}$$

A tak

$$(101)^8 \equiv (1\,120)^2 \equiv 1\,254\,400 \equiv 729 (\mathrm{mod}\, \mathbf{1147}). \tag{7.12}$$

Z kongruencí (7.10), (7.11) a (7.12) pak plyne

$$c \equiv (101)^{11} \equiv (101)^8 \cdot (101)^2 \cdot 101 \equiv 729 \cdot 1\,025 \cdot 101 \equiv 75\,469\,725 \equiv 566 (\mathrm{mod}\, \mathbf{1147}).$$

Text 101 zašifrujeme jako 566. Obdobně zjistíme, že

$$(112)^{11} \equiv 630 (\mathrm{mod}\, \mathbf{1147}),$$

$$(131)^{11} \equiv 671 (\mathrm{mod}\, \mathbf{1147})$$

a

$$(112)^{11} \equiv 630 (\mathrm{mod}\, \mathbf{1147}).$$

Slovo „UTEČTE“ = 101 112 131 112 proto zašifrujeme jako 566 630 671 630. Obdobným způsobem je možné zašifrovat i zbytek zprávy.

Příklad 7.5. Pomozte Koumákovi dešifrovat vzkaz od Taťky Šmouly :

„ 566 630 671 630 . . . “.

Řešení: Koumák použije svůj soukromý klíč $d = 491$ a hodnotu $\mathbf{n} = \mathbf{1147}$. Hledáme v množině $\{1, \ldots, \mathbf{1147}\}$ čísla kongruentní s čísly 566^{491}, 630^{491}, 671^{491}, 630^{491} . . . modulo **1147**. To jest, hledáme ? v kongruencích

$$\begin{aligned} (566)^{491} &\equiv ? (\mathrm{mod}\, \mathbf{1147}) \\ (630)^{491} &\equiv ? (\mathrm{mod}\, \mathbf{1147}) \\ (671)^{491} &\equiv ? (\mathrm{mod}\, \mathbf{1147}) \\ (630)^{491} &\equiv ? (\mathrm{mod}\, \mathbf{1147}) \\ &\vdots \end{aligned} \tag{7.13}$$

Z výpočetního hlediska není výhodné umocňovat čísla šifrovaného textu rovnou na 491. Budeme postupovat obdobně jako v Příkladě 7.4. Předvedeme postup názorně na kongruenci $(566)^{491} \equiv ?(\mathrm{mod}\,\mathbf{1147})$.

$$\begin{aligned}
(566)^2 &\equiv 320356 \equiv 343(\mathrm{mod}\,\mathbf{1147}) \\
&\Downarrow \\
(566)^4 &\equiv 343^2 \equiv 655(\mathrm{mod}\,\mathbf{1147}) \\
&\Downarrow \\
(566)^8 &\equiv 655^2 \equiv 47(\mathrm{mod}\,\mathbf{1147}) \\
&\Downarrow \\
(566)^{16} &\equiv 47^2 \equiv 1062(\mathrm{mod}\,\mathbf{1147}) \\
&\Downarrow \\
(566)^{32} &\equiv 1062^2 \equiv 343(\mathrm{mod}\,\mathbf{1147}) \\
&\Downarrow \\
(566)^{64} &\equiv 343^2 \equiv 655(\mathrm{mod}\,\mathbf{1147}) \\
&\Downarrow \\
(566)^{128} &\equiv 655^2 \equiv 47(\mathrm{mod}\,\mathbf{1147}) \\
&\Downarrow \\
(566)^{256} &\equiv 47^2 \equiv 1062(\mathrm{mod}\,\mathbf{1147})
\end{aligned} \tag{7.14}$$

Odtud

$$(566)^{491} \equiv (566)^{256+128+64+32+8+2+1} \equiv 1062 \cdot 47 \cdot 655 \cdot 343 \cdot 47 \cdot 343 \cdot 566(\mathrm{mod}\,\mathbf{1147}). \tag{7.15}$$

Odtud již snadno určíme hledanou hodnotu.

$$\begin{aligned}
1062 \cdot 47 &\equiv 49\,914 \equiv 593(\mathrm{mod}\,\mathbf{1147}), \\
593 \cdot 655 &\equiv 388\,415 \equiv 729(\mathrm{mod}\,\mathbf{1147}), \\
729 \cdot 343 &\equiv 250\,047 \equiv 1(\mathrm{mod}\,\mathbf{1147}), \\
1 \cdot 47 &\equiv 47 \equiv 47(\mathrm{mod}\,\mathbf{1147}), \\
47 \cdot 343 &\equiv 16\,121 \equiv 63(\mathrm{mod}\,\mathbf{1147}), \\
63 \cdot 566 &\equiv 35\,658 \equiv 101(\mathrm{mod}\,\mathbf{1147})
\end{aligned} \tag{7.16}$$

Proto

$$(566)^{491} \equiv 101(\mathrm{mod}\,\mathbf{1147}). \tag{7.17}$$

Stejným způsobem zjistíme, že

$$\begin{aligned} (630)^{491} &\equiv 112 (\mathrm{mod}\, \mathbf{1147}) \\ (671)^{491} &\equiv 131 (\mathrm{mod}\, \mathbf{1147}) \\ (630)^{491} &\equiv 112 (\mathrm{mod}\, \mathbf{1147}) \\ &\vdots \end{aligned} \tag{7.18}$$

Z (7.17) a (7.18) plyne, že zprávu „ 566 630 671 630 . . . “ dešifrujeme jako „ 101 112 131 112 . . . “. Této sekvenci čísel nakonec přiřadíme příslušná písmena

10	11	12	13	11	12	. . .
↓	↓	↓	↓	↓	↓	
U	T	E	Č	T	E	. . .

Kapitola 8

Výsledky cvičení

8.1 Dělitelnost na množině přirozených čísel

8.1.1 Výsledky Cvičení 1.2.1

Cvičení k podkapitole *Největší společný dělitel*.

1. Dokažte, že $\forall r \in \mathbb{R} : 2r - 1 - 2r < [2r] - 2[r] < 2r - 2(r-1)$.

   Řešení:

   Jednoduchou úpravou můžeme zadané nerovnosti převést na tvar

   $$-1 < [2r] - 2[r] < 2.$$

   Platnost těchto nerovností snadno dokážeme, uvědomíme-li si, že každé $r \in \mathbb{R}$ můžeme psát ve tvaru $r = [r] + \varepsilon$, kde $0 \leqq \varepsilon < 1$. Proto

   $$[2r] - 2[r] = [2[r] + 2\varepsilon] - 2[r] = 2[r] + [2\varepsilon] - 2[r] = [2\varepsilon].$$

   Evidentně platí:

   $$[2\varepsilon] \geqq [2.0] = 0.$$

   A také

   $$[2\varepsilon] < [2.1] = 2.$$

   Proto $2r - 1 - 2r = -1 < [2r] - 2[r] < 2 = 2r - 2(r-1)$.

2. Dokažte, že $\forall x \in \mathbb{R}$ a $\forall p, k \in \mathbb{N}$ platí $\left[\frac{x}{p^k}\right] = \left[\frac{n}{p^k}\right]$, kde $n = [x]$.

   Řešení:
   Označme $x - n = x - [x] = \varepsilon_x \in \langle 0, 1)$, $m_1 = \left[\frac{x}{p^k}\right]$ a $m_2 = \left[\frac{n}{p^k}\right]$. Cílem je

dokázat, že $m_1 = m_2$. Čísla m_1 a m_2 splňují nerovnosti $m_1 \leqq \frac{x}{p^k} < m_1 + 1$ a $m_2 \leqq \frac{n}{p^k} < m_2 + 1$ Odtud

$$m_1 \leqq \frac{x}{p^k} < m_1 + 1 \text{ a také } -m_2 \geqq -\frac{n}{p^k} > -m_2 - 1$$

Odtud dostáváme

$$\begin{aligned} m_1 - m_2 - 1 &< \tfrac{x}{p^k} - \tfrac{n}{p^k} < m_1 - m_2 + 1 \\ m_1 - m_2 &\leqq \tfrac{\varepsilon_x}{p^k} < m_1 - m_2 + 1 \end{aligned}$$

To ale znamená, že celá část čísla $\frac{\varepsilon_x}{p^k}$ je rovna číslu $m_1 - m_2$, to jest,

$$\left[\frac{\varepsilon_x}{p^k}\right] = m_1 - m_2. \tag{8.1}$$

Uvažme, že $0 \leqq \varepsilon_x < 1$ a $p \geqq 1$. Proto $0 \leqq \frac{\varepsilon_x}{p^k} < \frac{1}{1}$. Odtud je jasné, že

$$\left[\frac{\varepsilon_x}{p^k}\right] = 0. \tag{8.2}$$

Srovnáním (8.1) a (8.2) zjistíme, že $m_1 - m_2 = 0$.

3. Dokažte, že pro každé $x \in \mathbb{R}^+$ a $p \in \mathbb{N}$ platí $\frac{1}{x}\left[\frac{x}{p^k}\right] \leqq \frac{1}{p^k}$.

   Řešení:
   Označme $x - [x] = \varepsilon_x \in \langle 0, 1)$. Potom

$$\frac{1}{x}\left[\frac{x}{p^k}\right] = \frac{1}{x}\frac{x}{p^k} - \frac{1}{x}\frac{\varepsilon_x}{p^k} \leqq \frac{1}{p^k}$$

4. Nalezněte celá čísla x_0 a y_0 tak, aby $\gcd(36, 14) = x_0 36 + y_0 14$. Tj. vyjádřete největšího společného dělitele čísel 36 a 14 jako jejich lineární kombinaci.

   Řešení:

   Nejprve pomocí Euklidova algoritmu nalezneme $\gcd(36, 14)$.

$$\begin{aligned} 36 &= 2 \cdot 14 + 8 && (8.3) \\ 14 &= 1 \cdot 8 + 6 && (8.4) \\ 8 &= 1 \cdot 6 + 2 && (8.5) \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

A tak jsme zjistili, že $\gcd(36, 14) = 2$. Nyní budeme postupovat opačným směrem. Nejprve z rovnice (8.5) vyjádříme $\gcd(36, 14)$, tj. číslo 2.

$$2 = 8 - 6 \tag{8.6}$$

Poté z rovnice (8.4) vyjádříme zbytek 6 ($6 = 14 - 8$) a dosadíme do (8.6). Obdržíme

$$2 = 8 - (14 - 8). \tag{8.7}$$

Z rovnice (8.3) vyjádříme zbytek 8 ($8 = 36 - 2.14$) a dosadíme do (8.7). Obdržíme

$$2 = (36 - 2 \cdot 14) - (14 - (36 - 2 \cdot 14)). \tag{8.8}$$

Posledně uvedenou rovnici už jen stačí upravit.

$$\begin{aligned} 2 &= 36 - 2 \cdot 14 - 14 + 36 - 2 \cdot 14 \\ 2 &= 2 \cdot 36 - 5 \cdot 14 \end{aligned}$$

Můžeme proto psát $2 = \gcd(36, 14) = 2 \cdot 36 - 5 \cdot 14$. Hledaná čísla tedy jsou $x_0 = 2$ a $y_0 = -5$.

5. Nalezněte největšího společného dělitele čísel 2 328 a 3 581

   Řešení:
   Použijeme Euklidův algoritmus

$$\begin{aligned} 3\,581 &= 1 \cdot 2\,328 + 1\,253 \\ 2\,328 &= 1 \cdot 1\,253 + 1\,075 \\ 1\,253 &= 1 \cdot 1\,075 + 178 \\ 1\,075 &= 6 \cdot 178 + 7 \\ 178 &= 25 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + \mathbf{1} \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

   Proto $\gcd(2\,328, 3\,581) = 1$.

8.1.2 Výsledky Cvičení 1.3.1

Cvičení k podkapitole *Kanonický rozklad*.

1. Nalezněte kanonický rozklad čísla 196.

   Řešení:
   $$196 = 2 \cdot 98 = 2 \cdot 2 \cdot 49 = 2^2 7^2.$$

2. Nalezněte kanonický rozklad čísla $(196)^3$.

   Řešení:
   $$(196)^3 = (2^2 7^2)^3 = 2^6 7^6.$$

3. Nalezněte kanonický rozklad čísla $(567)^2(196)^3$.

   Řešení:

   $(567)^2 = (3{\cdot}189)^2 2^6 7^6 = (3^2{\cdot}63)^2 2^6 7^6 = (3^3{\cdot}21)^2 2^6 7^6 = (3^4{\cdot}7)^2 2^6 7^6 = 2^6 3^8 7^8.$

4. Nalezněte kanonický rozklad čísel $(180)^2$, $(250)^3$ a určete $\gcd((180)^2, (250)^3)$.

   Řešení:
   $$\begin{aligned} (180)^2 &= (9 \cdot 20)^2 = (9 \cdot 4 \cdot 5)^2 = (3^2 \cdot 2^2 \cdot 5)^2 = 2^4 3^4 5^2, \\ (250)^3 &= (10 \cdot 25)^3 = (2 \cdot 5^3)^3 = 2^3 \cdot 5^9. \end{aligned}$$

   Proto $\gcd((180)^2, (250)^3) = 2^3 5^2 = 8 \cdot 25 = 200$.

5. Nalezněte kanonický rozklad čísla 99 221.

   Řešení:
   $$99\,221 = 313 \cdot 317.$$

8.1.3 Výsledky Cvičení 1.4.1

Cvičení k podkapitole *Nejmenší společný násobek*.

1. Nalezněte nejmenší společný násobek čísel 198 a 55.

   Řešení:
   $$\begin{aligned} 198 &= 3 \cdot 66 = 3 \cdot 3 \cdot 22 = 3 \cdot 3 \cdot 2 \cdot 11 = 2^1 3^2 11^1 \\ 55 &= 5^1 11^1. \end{aligned}$$

   Proto $n(198, 55) = 2^1 3^2 5^1 11^1 = 90 \cdot 11 = 990$.

2. Nalezněte nejmenší společný násobek čísel 198, 55 a 65.

   Řešení:

   $$\begin{aligned} 198 &= 3 \cdot 66 = 3 \cdot 3 \cdot 22 = 3 \cdot 3 \cdot 2 \cdot 11 = 2^1 3^2 11^1 \\ 55 &= 5^1 11^1. \\ 65 &= 5 \cdot 13 = 5^1 13^1. \end{aligned}$$

   Proto

   $$\begin{aligned} n(198, 55, 65) &= 2^{\max\{1,0,0\}} 3^{\max\{2,0,0\}} 5^{\max\{0,1,1\}} 11^{\max\{1,1,0\}} 13^{\max\{0,0,1\}} \\ &= 2^1 3^2 5^1 11^1 13^1 = \\ &= 12\,870. \end{aligned}$$

3. Dokažte následující tvrzení. Nejmenším společným násobkem dvou navzájem nesoudělných přirozených čísel je součin těchto čísel.

   Řešení: Snažíme se dokázat implikaci: $\gcd(a, b) = 1 \Rightarrow n(a, b) = ab$. To ale okamžitě plyne z Věty 1.40, která říká, že

   $$n(a, b) = \frac{|ab|}{\gcd(a, b)} = \frac{ab}{\gcd(a, b)}.$$

   Po dosazení $\gcd(a, b) = 1$ obdržíme

   $$n(a, b) = ab.$$

8.2 Množina prvočísel

8.2.1 Výsledky Cvičení 2.1.1

Cvičení k podkapitole *Základní vlastnosti*.

1. Dokažte, že pro každé $n \in \mathbb{N}$ platí: $p_n > n$.

   Řešení:

   Toto tvrzení je poměrně zřejmé, nicméně z cvičných důvodů provedeme jeho detailní důkaz. Můžeme si jej nejprve rozmyslet na několika konkrétních příkladech. Evidentně platí:

   $$p_1 = 2 > 1, \quad p_2 = 3 > 2, \quad p_3 = 5 > 3, \quad p_4 = 7 > 4 \quad \text{atd.}$$

Důkaz provedeme matematickou indukcí. Pro $n = 1$ a $n = 2$ je tvrzení pravdivé (viz výše). Můžeme proto přistoupit k indukčnímu kroku. Předpokládáme pro $n \geqq 2$ platnost nerovnosti $p_n > n$ a musíme dokázat, že pak také platí $p_{n+1} > n + 1$.

Vezměme prvočíslo p_n, kde $n \geqq 2$. Pouze $p_1 = 2$ je sudé prvočíslo a každé další je liché. Takže p_n musí být liché číslo a za ním následující číslo $p_n + 1$ je tedy sudé číslo větší než 2. Proto $p_n + 1$ nemůže být prvočíslo. Z toho je zřejmé, že

$$p_{n+1} > p_n + 1$$

Indukčním předpokladem je, že $p_n > n$. A tak

$$p_{n+1} > p_n + 1 > n + 1.$$

8.2.2 Výsledky Cvičení 2.3.1

Cvičení k podkapitole *Prvočíselná funkce a prvočíselná věta.*

1. Odhadněte, kolik prvočísel je menších, nebo rovných číslu $n = 1\,000$, $n = 10\,000$, $n = 1\,000\,000$.

   Řešení:
   Pomocí prvočíselné věty odhadujeme:

$$\begin{aligned}
\pi(1\,000) &\doteq \tfrac{1\,000}{\ln 1\,000} \doteq 144,76 && \text{skutečnost: } 168\\
\pi(10\,000) &\doteq \tfrac{10\,000}{\ln 10\,000} \doteq 1\,085,74 && \text{skutečnost: } 1\,229\\
\pi(1\,000\,000) &\doteq \tfrac{1\,000\,000}{\ln 1\,000\,000} \doteq 72382,41 && \text{skutečnost: } 78\,498
\end{aligned}$$

2. Odhadněte, kolik procent čísel menších, nebo rovných číslu $n = 1\,000$, $n = 10\,000$, $n = 1\,000\,000$ tvoří prvočísla.

   Řešení:
   Podle předchozího příkladu odhadujeme

$$\begin{aligned}
\tfrac{\pi(1\,000)}{1\,000} &\doteq \tfrac{144,76}{1\,000} = 0,144\,76 && \text{skutečnost: } 0,168\\
\tfrac{\pi(10\,000)}{10\,000} &\doteq \tfrac{1085,74}{10\,000} = 0,108\,74 && \text{skutečnost: } 0,122\,9\\
\tfrac{\pi(1\,000\,000)}{1\,000\,000} &\doteq \tfrac{1085,74}{1\,000\,000} \doteq 0,072\,382\,41 && \text{skutečnost: } 0,078\,498
\end{aligned}$$

3. Dokažte, že pro každé $x \in \mathbb{R}$, $x \geqq 2$ platí $\pi(x) \leqq x - 1$.

   Řešení:
   Počet přirozených čísel menších, nebo rovných x je roven $[x]$ a alespoň jedno z nich není prvočíslo (a to číslo 1). Proto $\pi(x) \leqq [x] - 1 \leqq x - 1$.

8.2.3 Výsledky Cvičení 2.4.1

Cvičení k podkapitole *Čebyševovy nerovnosti*.

1. Pomocí Lemmatu 2.22 nalezněte kanonické rozklady čísel 7! a 20!.

   Řešení:

   Zmíněné lema říká, že pro každé $n \in \mathbb{N}$ platí $n! = \prod_{p\in\mathbb{P}, p\leqq n} p^{\alpha(p)}$, kde

   $$\alpha(p) = \sum_{k\in\mathbb{N}, p^k\leqq n} \left[\frac{n}{p^k}\right].$$

   Musíme proto najít všechna prvočísla p splňující $p \leqq n$. V případě $n = 7$ jsou to prvočísla 2, 3, 5 a 7.

   Nyní určíme, jaké mocniny budou mít tato prvočísla v kanonickém rozkladu čísla 7!.

   $$\begin{aligned}
   \alpha(2) &= \sum_{k\in\mathbb{N}, 2^k\leqq 7} \left[\tfrac{7}{2^k}\right] = \left[\tfrac{7}{2}\right] + \left[\tfrac{7}{2^2}\right] = [3,5] + [1,75] = 3 + 1 = 4,\\
   \alpha(3) &= \sum_{k\in\mathbb{N}, 3^k\leqq 7} \left[\tfrac{7}{3^k}\right] = \left[\tfrac{7}{3}\right] = [2,\overline{3}] = 2,\\
   \alpha(5) &= \sum_{k\in\mathbb{N}, 5^k\leqq 7} \left[\tfrac{7}{5^k}\right] = \left[\tfrac{7}{5}\right] = [1,4] = 1,\\
   \alpha(7) &= \sum_{k\in\mathbb{N}, 7^k\leqq 7} \left[\tfrac{7}{7^k}\right] = \left[\tfrac{7}{7}\right] = [1] = 1.
   \end{aligned} \tag{8.9}$$

   Potom

   $$7! = \prod_{p\in\mathbb{P}, p\leqq 7} p^{\alpha(p)} = 2^4.3^2.5^1.7^1$$

   V případě $n = 20$ postupujeme analogicky. Prvočísla menší než 20 jsou 2, 3, 5, 7, 11, 13, 17 a 19. Pak určíme hodnoty $\alpha(p)$:

$$\alpha(2) = \sum_{k\in\mathbb{N},2^k\leqq 20} \left[\tfrac{20}{2^k}\right] = \left[\tfrac{20}{2}\right] + \left[\tfrac{20}{2^2}\right] + \left[\tfrac{20}{2^3}\right] + \left[\tfrac{20}{2^4}\right] = 18.$$

$$\alpha(3) = \sum_{k\in\mathbb{N},3^k\leqq 20} \left[\tfrac{20}{3^k}\right] = \left[\tfrac{20}{3}\right] + \left[\tfrac{20}{9}\right] = 8.$$

$$\alpha(5) = \sum_{k\in\mathbb{N},5^k\leqq 20} \left[\tfrac{20}{5^k}\right] = \left[\tfrac{20}{5}\right] = 4.$$

$$\vdots$$

Odtud

$$20! = \prod_{p\in\mathbb{P},p\leqq 20} p^{\alpha(p)} = 2^{18}.3^8.5^4.7^2.11^1.13^1.17^1.19^1$$

2. Obdobně jako v Poznámce 2.16 odhadněte, kolik je prvočísel menších, nebo rovných 1 000.

   Řešení:

   Dosadíme $x = 1\,000$ do nerovností $(\ln 2)\frac{x}{\ln x} - \frac{\ln 4}{\ln x} - 1 < \pi(x) < 2(\ln 4)\frac{x}{\ln x} + + \sqrt{x}$ a odhadu $\pi(x) \sim \frac{x}{\ln x}$. Obdržíme

   $$99,14\cdots < \pi(x) < 432,996\ldots$$

   $$\pi(x) \sim 144,76\ldots$$

   Což interpretujeme tak, že prvočísel menších, nebo rovných 1 000 je něco kolem 145 a z nerovností je patrné, že jich je alespoň 100, ale nejvýše 432. Poznamenejme, že ve skutečnosti je jich 168.

3. Pokuste se vylepšit odhad $\pi(x) < 2(\ln 4)\frac{x}{\ln x} + \sqrt{x}$ uvedený ve Větě 2.26.

   Řešení:

   Důkaz Věty 2.26 se odvíjel od následujícího rozdělení součinu $\prod_{\substack{p\in\mathbb{P}\\ p\leqq x}} p$

   $$\prod_{\substack{p\in\mathbb{P}\\ p\leqq x}} p = \prod_{\substack{p\in\mathbb{P}\\ p\leqq\sqrt{x}}} p \prod_{\substack{p\in\mathbb{P}\\ \sqrt{x}<p\leqq x}} p.$$

   Najdeme jiné rozdělení tohoto součinu. Hledejme $h \in (0,1)$ takové, aby rozdělení součinu

   $$\prod_{\substack{p\in\mathbb{P}\\ p\leqq x}} p = \prod_{\substack{p\in\mathbb{P}\\ p\leqq x^h}} p \prod_{\substack{p\in\mathbb{P}\\ x^h<p\leqq x}} p$$

vedlo k co nejlepšímu odhadu $\pi(x)$ pro dané x. Analogicky jako v důkazu Věty 2.26 vyjdeme z nerovnosti

$$4^x > \prod_{\substack{p\in\mathbb{P}\\ p\leqq x}} p = \prod_{\substack{p\in\mathbb{P}\\ p\leqq x^h}} p \prod_{\substack{p\in\mathbb{P}\\ x^h<p\leqq x}} p \geqq \prod_{\substack{p\in\mathbb{P}\\ x^h<p\leqq x}} p \geqq \left(x^h\right)^{\pi(x)-\pi(x^h)} \geqq \left(x^h\right)^{\pi(x)-x^h}.$$

Odtud máme $4^x > \left(x^h\right)^{\pi(x)-x^h}$ a stejnými úpravami jako v důkazu Věty 2.26 dojdeme k nerovnosti

$$\pi(x) < \frac{\ln 4}{h}\frac{x}{\ln x} + x^h = g(x,h). \tag{8.10}$$

Hledejme minimum funkce $g(x,h)$ pro pevně zvolené x (hledáme tedy minimum funkce $g(h)$, x považujeme za konstantu). Z rovnic

$$\frac{\partial g(x,h)}{\partial h} = -\frac{\ln 4}{h^2}\frac{x}{\ln x} + x^h \ln x = 0$$

plyne, že pro dané x je odhad (8.10) nejlepší[1], splňuje-li h rovnici

$$-\frac{\ln 4}{h^2}\frac{x}{\ln x} + x^h \ln x = 0. \tag{8.11}$$

V důkazu Věty 2.26 bylo zvoleno $h = \frac{1}{2}$. Vidíme, že to nemusí vést k nejlepšímu odhadu, jaký jsme tímto způsobem schopni odvodit.

Vezměme konkrétní příklad $x = 1\,000$. Potom h splňující podmínku (8.11) je přibližně rovno $0,62418$. V tom případě je

$$\pi(x) < \frac{\ln 4}{h}\frac{x}{\ln x} + x^h = \frac{\ln 4}{0,62418}\frac{1000}{\ln 1000} + 1000^{0,62418} \doteq 396,086.$$

(Srovnej s předchozím odhadem $\pi(x) < 432,996$ v příkladu 2.)

8.2.4 Výsledky Cvičení 2.6.1

Cvičení k podkapitole *Další vlastnosti* (množiny prvočísel).

1. Dokažte, že $\sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} = O(1)$. (Návod: Dokažte existenci čísla $c \in \mathbb{R}$ takového, že $\sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} \leqq c = konst. \in \mathbb{R}$. Použijte myšlenku integrálního kritéria konvergence řady. Integrujte per partes.)

[1] Ověřte, že $\frac{\partial^2 g(x,h)}{\partial h^2} > 0$, tj., že $g(h)$ opravdu nabývá svého minima pro dané $x \geqq 2$!

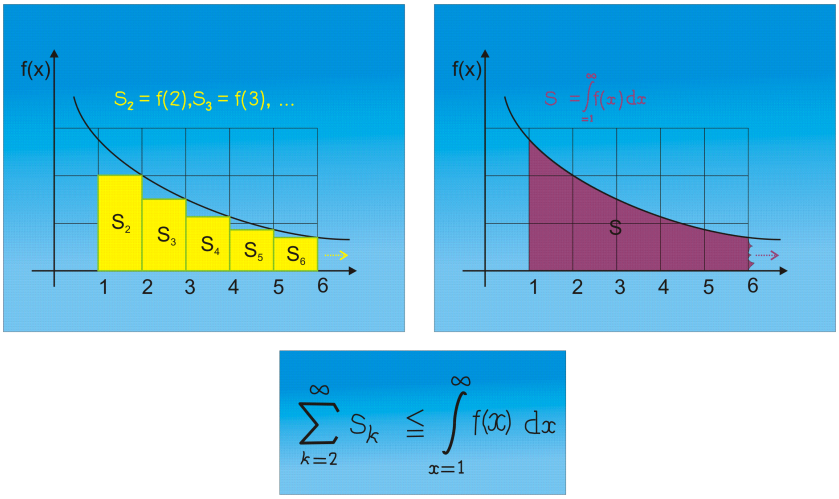
Řešení:

Snadno se přesvědčíme, že $\forall k \in \mathbb{N}, k \geqq 2$ platí nerovnost $k(k-1) \geqq \frac{1}{2}k^2$, neboť $\forall k \in \mathbb{N}, k \geqq 2$ jistě platí

$$\begin{aligned} k \ -2 &\geqq 0 \quad &| \cdot k \\ k^2 - 2k &\geqq 0 \quad &| +k^2 \\ 2k^2 - 2k &\geqq k^2 \quad &| : 2 \\ k^2 - k &\geqq \tfrac{1}{2}k^2 \\ k(k-1) &\geqq \tfrac{1}{2}k^2 \end{aligned}$$

Proto

$$\sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} \leqq \sum_{k=2}^{\infty} \frac{\ln k}{\frac{1}{2}k^2} = \sum_{k=2}^{\infty} 2\frac{\ln k}{k^2}. \tag{8.12}$$



Obr. 8.1 Součet ploch S_k je jistě menší, než plocha pod křivkou $y = f(x)$ na intervalu $(1, \infty)$.

Z definice Riemannova integrálu plyne[1], že

[1]Integrál $\int_1^{\infty} f(x)\,\mathrm{d}x$ vyjadřuje plochu pod grafem funkce $f(x)$ (a nad osou x) na intervalu $(1, \infty)$, zatímco $\sum_{k=2}^{\infty} f(k)$ představuje součet ploch obdélníků uvnitř této plochy (viz obr.8.1)

$$\sum_{k=2}^{\infty} 2\frac{\ln k}{k^2} \leqq \int_{x=1}^{\infty} 2\frac{\ln x}{x^2}\,\mathrm{d}x. \tag{8.13}$$

A tak, podle (8.12) a (8.13), platí nerovnost

$$\sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} \leqq \int_{x=1}^{\infty} 2\frac{\ln x}{x^2}\,\mathrm{d}x. \tag{8.14}$$

Označíme-li $u = \ln x$, $v' = \frac{1}{x^2}$, pak $u' = \frac{1}{x}$, $v = \frac{-1}{x}$ a integrací per partes[1] dostáváme

$$\begin{aligned}
\int_1^{\infty} \frac{\ln x}{x^2}\,\mathrm{d}x &= \left[\frac{-\ln x}{x}\right]_1^{\infty} + \int_1^{\infty} \frac{1}{x^2}\,\mathrm{d}x = \\
&= \left[\frac{-\ln x}{x} - \frac{1}{x}\right]_1^{\infty} = \\
&= \lim_{x\to\infty} \left(\underbrace{\frac{-\ln x}{x}}_{\to 0 (\mathrm{l'H.})} - \underbrace{\frac{1}{x}}_{\to 0} \right) - \left(\underbrace{\frac{-\ln 1}{1}}_{=0} - \frac{1}{1} \right) = \\
&= 1.
\end{aligned} \tag{8.15}$$

Podle (8.14) to znamená, že

$$0 \leqq \sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} \leqq 2 \cdot \int_{x=1}^{\infty} \frac{\ln x}{x^2}\,\mathrm{d}x = 2 = konst. \in \mathbb{R}. \tag{8.16}$$

Proto

$$\limsup_{x\to\infty} \left| \sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} \right| < 2.$$

To (viz definice $O(1)$ v podkapitole 0.2) znamená, že

[1] Podle vzorce $\int u.v'\,\mathrm{d}x = u.v - \int u'.v\,\mathrm{d}x$.

$$\sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)} = O(1).$$

2. Dokažte, že pro každé $n \in \mathbb{N}$ platí

$$\sum_{k \leqq n} \frac{1}{k} = \ln(n+1) + \gamma + g(n),$$

kde $\gamma \in (0,1)$ je Eulerova konstanta, a $g(n)$ je funkce splňující pro každé $n \in \mathbb{N}$ nerovnosti

$$-\frac{1}{n+1} < g(n) < 0.$$

Řešení:

Vyjdeme z důkazu Lemmatu 2.36, konkrétně ze vztahu (2.72), který říká, že

$$\gamma = \sum_{k \leqq n} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\,\mathrm{d}t \right) + \underbrace{\sum_{k=n+1}^{\infty} \left(\frac{1}{k} - \int_k^{k+1} \frac{1}{t}\,\mathrm{d}t \right)}_{\text{označme f(n)}}. \tag{8.17}$$

A navíc je zde dokázáno, že $f(n) < \frac{1}{n+1}$ pro každé $n \in \mathbb{N}$, a je zřejmé, že $0 < f(n)$. Proto

$$0 < f(n) < \frac{1}{n+1},$$
$$-\frac{1}{n+1} < -f(n) < 0.$$

Označíme-li $g(n) = -f(n)$, pak podle výše uvedeného pro každé $n \in \mathbb{N}$ platí

$$-\frac{1}{n+1} < g(n) < 0.$$

Jednoduchou úpravou[1] vztahu (8.17) obdržíme rovnici

$$\gamma = \sum_{k \leqq n} \frac{1}{k} - \int_1^{n+1} \frac{1}{t}\,\mathrm{d}t + f(n). \tag{8.18}$$

[1] Sečteme integrály, tzn. $\sum_{k \leqq n} \left(\int_k^{k+1} \frac{1}{t}\,\mathrm{d}t \right) = \int_1^{k+1} \frac{1}{t}\mathrm{d}t.$

Odtud

$$\begin{aligned}
\sum_{k\leqq n}\frac{1}{k} &= \gamma+\int_1^{n+1}\frac{1}{t}\,\mathrm{d}t - f(n)\\
\sum_{k\leqq n}\frac{1}{k} &= \gamma+\int_1^{n+1}\frac{1}{t}\,\mathrm{d}t + g(n)\\
\sum_{k\leqq n}\frac{1}{k} &= \gamma+\ln(n+1)-\underbrace{\ln 1}_{=0}+g(n)\\
\sum_{k\leqq n}\frac{1}{k} &= \gamma+\ln(n+1)+g(n),
\end{aligned} \tag{8.19}$$

kde (viz výše) $-\frac{1}{n+1} < g(n) < 0$.

8.3 Hustoty množin

8.3.1 Výsledky Cvičení 3.1.1

Cvičení k podkapitole *Asymptotická hustota*.

1. Ověřte, že pro každou množinu $A \subseteq \mathbb{N}$ existuje její horní a dolní asymptotická hustota $\overline{d}(A)$, respektive $\underline{\mathrm{d}}(A)$, ale nemusí nutně existovat asymptotická hustota $d(A)$.

   Řešení:

   Důkaz tohoto tvrzení naleznete v učebnicích matematické analýzy. Je tam (alespoň v těch lepších - náročnějších) ukázáno, že limita dané posloupnosti reálných čísel nemusí existovat. Ve Větě 3.5 je popsána množina přirozených čísel, která nemá asymptotickou hustotu. Ale každá posloupnost má své limes inferior a limes superior. A tak musí existovat i limes superior a limes inferior posloupnosti $\frac{A(1)}{1}, \frac{A(2)}{2}, \ldots$. Tj. existují hodnoty

   $$\overline{d}(A) = \limsup_{n\to\infty}\frac{A(n)}{n}$$

   a

   $$\underline{d}(A) = \liminf_{n\to\infty}\frac{A(n)}{n}.$$

2. Dokažte, že pro každou množinu $A \subseteq \mathbb{N}$ platí, že $0 \leqq \underline{d}(A) \leqq \bar{d}(A) \leqq 1$.

   Řešení:

   Čísel menších, nebo rovných n, které patří do množiny A je nejvýše n a nejméně 0. Symbolicky zapsáno

   $$0 \leqq A(n) \leqq n.$$

   Odtud dostáváme pro každé $n \in \mathbb{N}$ odhady

   $$0 \leqq \frac{A(n)}{n} \leqq 1.$$

   Proto

   $$0 \leqq \liminf_{n\to\infty} \frac{A(n)}{n} \leqq \limsup_{n\to\infty} \frac{A(n)}{n} \leqq 1.$$

   Podle definice horní a dolní asymptotické hustoty množiny A to znamená, že $0 \leqq \underline{d}(A) \leqq \bar{d}(A) \leqq 1$.

3. Dokažte, že existují množiny, jejichž asymptotická hustota splňuje $d(A) = 1$ a přesto $A \neq \mathbb{N}$. (Jde například o množiny typu $A = \mathbb{N} - K$, kde K je neprázdná konečná podmnožina množiny přirozených čísel.)

   Řešení:

   Dokážeme, že množina $A = \mathbb{N} - K$, kde K je neprázdná konečná podmnožina množiny přirozených čísel má asymptotickou hustotu rovnu 1. Předpokládejme, že množina K má celkem k prvků, tj.

   $$K = \{n_1, n_2, \ldots, n_k\}.$$

   Proto pro každé $n > n_k$ platí[1]

   $$A(n) = n - k.$$

   A tak

   $$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = \lim_{n\to\infty} \frac{n-k}{n} = \lim_{n\to\infty} \underbrace{\frac{n}{n}}_{=1} - \lim_{n\to\infty} \underbrace{\frac{k}{n}}_{\to 0} = 1.$$

[1] Mezi čísly $1, 2, \ldots, n$ pouze čísla $n_1, n_2, \ldots, n_k$ nepatří do množiny A. Tzn. mezi čísly $1, 2, \ldots, n$ je celkem $n - k$ čísel, které patří do množiny A.

4. Ověřte, že existují nekonečné množiny, jejichž asymptotická hustota splňuje $d(A) = 0$. (Například množina $A = \{n^2 \mid n \in \mathbb{N}\}$.)

   Řešení:

   Množina A obsahuje druhé mocniny přirozených čísel, tj. $A = \{1^2, 2^2, 3^2, \dots\}$. Abychom mohli určit $d(A)$, musíme znát závislost $A(n)$ na n, jinak řečeno, musíme vědět, kolik prvků množiny A je menších, nebo rovných danému n.

   Předpokládejme, že je jich celkem m. To znamená, že předpokládáme $A(n) = m$ a platí

   $$1^2 < 2^2 < \cdots < m^2 \leqq n < (m+1)^2.$$

   Musíme určit hodnotu m v závislosti na n. Z nerovností $m^2 \leqq n < (m+1)^2$ plyne, že

   $$\sqrt{m^2} \leqq \sqrt{n} < \sqrt{(m+1)^2},$$

   $$m \leqq \sqrt{n} < m + 1.$$

   Proto $m = [\sqrt{n}]$.[1] Znamená to, že pro každé $n \in \mathbb{N}$ jsou splněny nerovnosti

   $$0 \leqq \frac{A(n)}{n} = \frac{[\sqrt{n}]}{n} \leqq \frac{\sqrt{n}}{n} \tag{8.20}$$

   a evidentně platí

   $$\lim_{n\to\infty} \frac{\sqrt{n}}{n} = \lim_{n\to\infty} \frac{1}{\sqrt{n}} = 0.$$

   Proto z (8.20) plyne

   $$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = 0.$$

5. Přidáme-li, nebo odebereme-li z dané množiny A konečný počet prvků, pak asymptotická hustota výsledné množiny je stejná jako asymptotická hustota množiny A (za předpokladu, že $d(A)$ existuje). Tj. pokud $A, K \subseteq \mathbb{N}$, K je konečná množina, pak $d(A \cup K) = d(A)$ a také $d(A - K) = d(A)$. Dokažte.

   Řešení:

   Podle předpokladu je množina K konečná. Předpokládejme, že má k prvků. Množina $A - K$ je množina A, ze které jsme odebrali ty její prvky, které

[1] Viz Definice 1.11.

patří také do množiny K (obsahovala-li jaké). Je proto zřejmé, že odebereme nejméně 0 a nejvýše k prvků. Tzn. pro každé $n \in \mathbb{N}$ existuje k_n takové, že[1]

$$(A - K)(n) = A(n) - k_n,$$

kde $0 \leqq k_n \leqq k$.

Proto

$$d(A-K) = \lim_{n\to\infty} \frac{(A-K)(n)}{n} = \lim_{n\to\infty} \frac{A(n)-k_n}{n} = \lim_{n\to\infty} \frac{A(n)}{n} - \underbrace{\lim_{n\to\infty} \frac{k_n}{n}}_{=0} = d(A).$$

Vztah $d(A \cup K) = d(A)$ obdržíme analogicky, stačí si uvědomit, že $(A \cup \cup K)(n) = A(n) + k_n$, kde $0 \leqq k_n \leqq k$.

6. Dokažte, že neexistuje asymptotická hustota množiny $A = \cup_{n\in\mathbb{N}}\{6^n+1, 6^n+ + 2, \ldots, 2.6^n\}$.

Řešení:

Podle zadání je

$$\begin{aligned} A \;=\; & \{6+1, 6+2, \ldots, 2.6\} \cup \{6^2+1, 6^2+2, \ldots, 2.6^2\} \cup \\ & \cup \{6^3+1, 6^3+2, \ldots, 2.6^3\} \cup \cdots \end{aligned} \tag{8.21}$$

Z toho je patrné, že pro každé $n \in \mathbb{N}$, $n \geqq 2$ platí

$$A(6^n) \leqq 2.6^{n-1} \text{ a zároveň } A(2.6^n) \geqq 2.6^n - 6^n \tag{8.22}$$

Pokud by existovala asymptotická hustota $d(A)$, muselo by platit

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = \lim_{n\to\infty} \frac{A(6^n)}{6^n} \leqq \lim_{n\to\infty} \frac{2.6^{n-1}}{6.6^{n-1}} = \frac{2}{6} = \frac{1}{3}, \tag{8.23}$$

a zároveň

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = \lim_{n\to\infty} \frac{A(2.6^n)}{2.6^n} \geqq \lim_{n\to\infty} \frac{2.6^n - 6^n}{2.6^n} = 1 - \frac{1}{2} = \frac{1}{2}. \tag{8.24}$$

Z předpokladu, že asymptotická hustota $d(A)$ existuje, jsme dospěli k výroku (viz (8.23) a (8.24)), že $d(A) \leqq \frac{1}{3}$ a zároveň $d(A) \geqq \frac{1}{2}$. To je spor! Proto $d(A)$ nemůže existovat.

[1] $(A - K)(n)$ je počet prvků množiny $A - K$, které jsou menší, nebo rovny n.

8.3.2 Výsledky Cvičení 3.2.1

Cvičení k podkapitole *Logaritmická hustota*.

1. Nalezněte logaritmickou hustotu množiny přirozených čísel, které ve svém dekadickém zápisu začínají ciframi 11. Tzn. jde o množinu $A = \{11, 110, 111, \dots, 119, 1100, 1101, \dots, 1199, \dots\}$.

   Řešení:

   Jak vidno,

   $$\begin{aligned} A &= \{11, 110, 111, \dots, 119, 1100, 1101, \dots, 1199, \dots\} = \\ &= \bigcup_{j=0}^{\infty} \left\{11.10^j, 11.10^j + 1, \dots, 11.10^j + 10^{j-1} - 1\right\}. \end{aligned} \tag{8.25}$$

   Označme

   $$L_j = \sum_{\substack{a \in A \\ 11.10^j \leqq a < 11.10^{j+1}}} \frac{1}{a}.$$

   Potom (viz (8.25)) platí

   $$L_j = \sum_{11.10^j \leqq k \leqq 11.10^j + 10^{j-1} - 1} \frac{1}{k} = \sum_{k \leqq 11.10^j + 10^{j-1} - 1} \frac{1}{k} - \sum_{k \leqq 11.10^j - 1} \frac{1}{k}.$$

   Nyní využijeme toho, že pro každé $n \in \mathbb{N}$ platí (viz Cvičení 2.6.1) $\sum_{k \leqq n} \frac{1}{k} =$ $= \ln(n+1) + \gamma + g(n)$, kde γ je konstanta, a $g(n)$ splňuje nerovnosti $-$ $-\frac{1}{n+1} < g(n) < 0$. Proto

   $$\begin{aligned} L_j &= \ln(11.10^j + 10^{j-1}) + \gamma + g(11.10^j + 10^{j-1} - 1) - \\ &\quad - \ln(11.10^j) - \gamma - g(11.10^j - 1) = \\ &= \ln\left(\frac{11.10^j + 10^{j-1}}{11.10^j}\right) + g(11.10^j + 10^{j-1} - 1) - \\ &\quad - g(11.10^j - 1) = \\ &= \ln\left(1 + \frac{1}{110}\right) + \alpha(j), \end{aligned} \tag{8.26}$$

kde $\alpha(j) = g(11.10^j + 10^{j-1} - 1) - g(11.10^j - 1)$. Navíc (viz Cvičení 2.6.1)

$$-\frac{1}{11.10^j + 10^{j-1}} < \alpha(j) < \frac{1}{11.10^j}.$$

A protože $\frac{1}{11.10^j+10^{j-1}} < \frac{1}{11.10^j}$, platí nerovnosti

$$-\frac{1}{11.10^j} < \alpha(j) < \frac{1}{11.10^j}. \tag{8.27}$$

Uvažujme libovolné pevné $n \in \mathbb{N}$. Jistě existuje $j_n \in \mathbb{N}$ takové, že $11.10^{j_n} \leqq$ $\leqq n < 11.10^{j_n+1}$. Hodnotu j_n určíme snadno:

$$\begin{aligned}
11.10^{j_n} &\leqq n &&< 11.10^{j_n+1} \\
\ln(11.10^{j_n}) &\leqq \ln n &&< \ln(11.10^{j_n+1}) \\
\ln 11 + j_n \ln(10) &\leqq \ln n &&< \ln 11 + (j_n+1)\ln(10) \\
j_n \ln(10) &\leqq \ln n - \ln 11 &&< (j_n+1)\ln(10) \\
j_n &\leqq \tfrac{\ln n - \ln 11}{\ln(10)} &&< j_n + 1.
\end{aligned} \tag{8.28}$$

A tak existuje jediná možnost, a to[1]

$$j_n = \left[\frac{\ln n - \ln 11}{\ln(10)}\right].$$

Protože $11.10^{j_n} \leqq n < 11.10^{j_n+1}$, platí odhady

$$\sum_{j=0}^{j_n-1} L_j \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < \sum_{j=0}^{j_n+1} L_j. \tag{8.29}$$

Využijeme (8.26) a (8.27) a obdržíme tak

$$\begin{aligned}
\sum_{j=0}^{j_n-1} L_j &\geqq \sum_{j=0}^{j_n-1} \ln\left(1+\frac{1}{110}\right) - \sum_{j=0}^{j_n-1} \frac{1}{11.10^j} \geqq \\
&\geqq \sum_{j=0}^{j_n-1} \ln\left(1+\frac{1}{110}\right) - \sum_{j=0}^{\infty} \frac{1}{11.10^j} = \\
&= j_n \ln\left(1+\frac{1}{110}\right) - \frac{10}{99}.
\end{aligned} \tag{8.30}$$

[1] $[x]$ označuje celou část čísla x.

Obdobně

$$\begin{aligned}\sum_{j=0}^{j_n+1} L_j &< \sum_{j=0}^{j_n+1} \ln\left(1+\frac{1}{110}\right) + \sum_{j=0}^{j_n+1} \frac{1}{11.10^j} < \\ &< \sum_{j=0}^{j_n-1} \ln\left(1+\frac{1}{110}\right) + \sum_{j=0}^{\infty} \frac{1}{11.10^j} = \\ &= j_n \ln\left(1+\frac{1}{110}\right) + \frac{10}{99}. \end{aligned} \tag{8.31}$$

Pomocí (8.30) a (8.29) a Věty 3.10 odhadneme dolní logaritmickou hustotu množiny A:

$$\begin{aligned}\liminf_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} &\geqq \lim_{n\to\infty} \frac{\sum\limits_{j=0}^{j_n-1} L_j}{\ln n} \geqq \\ &\geqq \lim_{n\to\infty} \left(\frac{j_n}{\ln n} \ln\left(1+\frac{1}{110}\right) - \underbrace{\frac{10}{99\ln n}}_{\to 0} \right) = \\ &= \lim_{n\to\infty} \frac{\left[\frac{\ln n - \ln 11}{\ln(10)}\right]}{\ln n} \ln\left(1+\frac{1}{110}\right) = \\ &= \frac{\ln\left(1+\frac{1}{110}\right)}{\ln 10}. \end{aligned} \tag{8.32}$$

Analogicky bychom mohli (pomocí (8.31) a (8.29)) odvodit nerovnost

$$\limsup_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} \leqq \frac{\ln\left(1+\frac{1}{110}\right)}{\ln 10}. \tag{8.33}$$

Z (8.32) a (8.33) plyne

$$\frac{\ln\left(1+\frac{1}{110}\right)}{\ln 10} \leqq \liminf_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} \leqq \limsup_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} \leqq \frac{\ln\left(1+\frac{1}{110}\right)}{\ln 10}.$$

A tak existuje limita $\lim\limits_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n}$ a platí (viz Věta 3.8)

$$\lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} = \frac{\ln\left(1+\frac{1}{110}\right)}{\ln 10} = \log_{10}\left(1+\frac{1}{110}\right) = \delta(A).$$

2. Nalezněte logaritmickou hustotu množiny $A = \bigcup_{j\in\mathbb{N}}\{6^j+1, 6^j+2, \ldots, 2.6^j\}$.

   Řešení:

   Řešení je obdobné jako v předchozím příkladu. Definujme

$$L_j = \sum_{\substack{a\in A\\ 6^j\leqq a<6^{j+1}}} \frac{1}{a}. \tag{8.34}$$

   Potom (viz Cvičení 2.6.1)

$$\begin{aligned}
L_j &= \sum_{6^j+1\leqq k\leqq 2.6^j} \frac{1}{k} = \\
&= \sum_{k\leqq 2.6^j} \frac{1}{k} - \sum_{k\leqq 6^j} \frac{1}{k} = \\
&= \frac{1}{2.6^j} + \sum_{k\leqq 2.6^j-1} \frac{1}{k} - \frac{1}{6^j} - \sum_{k\leqq 6^j-1} \frac{1}{k} = \\
&= \frac{-1}{2.6^j} + \ln 2.6^j + g(2.6^j-1) - \ln 6^j - g(6^j-1) = \\
&= \ln\left(\frac{2.6^j}{6^j}\right) - \frac{1}{2.6^j} + g(2.6^j-1) - g(6^j-1) = \\
&= \ln 2 + \alpha(j), \qquad (8.35)
\end{aligned}$$

   kde $\alpha(j) = -\frac{1}{2.6^j} + g(2.6^j-1) - g(6^j-1)$ a platí (viz Cvičení 2.6.1)

$$\begin{aligned}
-\frac{1}{2.6^j} - \frac{1}{2.6^j} &< \alpha(j) < -\frac{1}{2.6^j} + \frac{1}{6^j} \\
-\frac{1}{6^j} &< \alpha(j) < \frac{1}{2.6^j}
\end{aligned}$$

Uvažujme libovolné $n \in \mathbb{N}$ a najděme $j_n \in \mathbb{N} \cup \{0\}$ tak, aby $6^{j_n} \leqq n < 6^{j_n+1}$.

$$\begin{aligned} 6^{j_n} &\leqq n &< 6^{j_n+1} \\ j_n \ln 6 &\leqq \ln n &< (j_n+1)\ln 6 \\ j_n &\leqq \frac{\ln n}{\ln 6} &< (j_n+1) \end{aligned}$$

Proto

$$j_n = \left[\frac{\ln n}{\ln 6}\right]. \tag{8.36}$$

Platí nerovnosti $6^{j_n} \leqq n < 6^{j_n+1}$. Ze vztahu (8.34) proto plyne, že

$$\sum_{j=0}^{j_n-1} L_j \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < \sum_{j=0}^{j_n+1} L_j.$$

Dále využijeme (8.35) a obdržíme tak

$$\sum_{j=0}^{j_n-1} (\ln 2 + \alpha(j)) \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < \sum_{j=0}^{j_n+1} (\ln 2 + \alpha(j)),$$

$$\sum_{j=0}^{j_n-1} \ln 2 + \sum_{j=0}^{j_n-1} \alpha(j) \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < \sum_{j=0}^{j_n+1} \ln 2 + \sum_{j=0}^{j_n+1} \alpha(j),$$

$$j_n \ln 2 + \sum_{j=0}^{j_n-1} \alpha(j) \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < (j_n+2)\ln 2 + \sum_{j=0}^{j_n+1} \alpha(j).$$

Ze vztahů (8.36) pak plynou nerovnosti

$$j_n \ln 2 - \sum_{j=0}^{j_n-1} \frac{1}{6^j} \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < (j_n+2)\ln 2 + \sum_{j=0}^{j_n+1} \frac{1}{2.6^j},$$

$$j_n \ln 2 - \sum_{j=0}^{\infty} \frac{1}{6^j} \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < (j_n+2)\ln 2 + \sum_{j=0}^{\infty} \frac{1}{2.6^j},$$

$$j_n \ln 2 - \frac{6}{5} \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < (j_n+2)\ln 2 + \frac{3}{5},$$

Nyní dosadíme za j_n - viz (8.36)

$$\left[\frac{\ln n}{\ln 6}\right]\ln 2 - \frac{6}{5} \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < \left(\left[\frac{\ln n}{\ln 6}\right]+2\right)\ln 2 + \frac{3}{5}. \tag{8.37}$$

Díky nerovnostem (8.37) můžeme odhadnout horní a dolní logaritmickou hustotu množiny A.[1]

Nejprve odhadneme zdola dolní logaritmickou hustotu. Protože

$$\forall n \in \mathbb{N} : \left[\frac{\ln n}{\ln 6}\right]\ln 2 - \frac{6}{5} \leqq \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a},$$

musí platit

$$\lim_{n\to\infty} \frac{\left[\frac{\ln n}{\ln 6}\right]\ln 2 - \frac{6}{5}}{\ln n} \leqq \liminf_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n}. \tag{8.38}$$

Limitu vlevo v nerovnosti (8.38) určíme snadno:[2]

$$\begin{aligned}
\lim_{n\to\infty} \frac{\left[\frac{\ln n}{\ln 6}\right]\ln 2 - \frac{6}{5}}{\ln n} &= \lim_{n\to\infty} \frac{\left[\frac{\ln n}{\ln 6}\right]\ln 2}{\ln n} - \underbrace{\lim_{n\to\infty} \frac{\frac{6}{5}}{\ln n}}_{=0} = \\
&= \lim_{n\to\infty} \frac{\left(\frac{\ln n}{\ln 6} - \varepsilon_n\right)\ln 2}{\ln n} = \\
&= \lim_{n\to\infty} \frac{\ln n \ln 2}{\ln 6 \ln n} - \underbrace{\lim_{n\to\infty} \frac{\varepsilon_n \ln 2}{\ln n}}_{=0} = \\
&= \frac{\ln 2}{\ln 6}.
\end{aligned} \tag{8.39}$$

Dosadíme-li (8.39) do (8.38), obdržíme

$$\frac{\ln 2}{\ln 6} \leqq \liminf_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n}. \tag{8.40}$$

Obdobně, (viz nerovnosti (8.37))

$$\forall n \in \mathbb{N} : \sum_{\substack{a\in A\\ a\leqq n}} \frac{1}{a} < \left(\left[\frac{\ln n}{\ln 6}\right]+2\right)\ln 2 + \frac{3}{5},$$

[1] Uvidíme, že horní a dolní logaritmická hustota se rovnají. A tak existuje i logaritmická hustota množiny A a je rovna téže hodnotě.

[2] Číslem ε_n označme zlomkovou část čísla $\frac{\ln n}{\ln 6}$. A tak pro každé $n \in \mathbb{N}$ platí $0 \leqq \varepsilon_n < 1$.

proto musí platit

$$\limsup_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} \leqq \lim_{n\to\infty} \frac{\left(\left[\frac{\ln n}{\ln 6}\right]+2\right)\ln 2+\frac{3}{5}}{\ln n}. \tag{8.41}$$

Limitu vpravo v nerovnosti (8.41) určíme snadno:

$$\begin{aligned}\lim_{n\to\infty} \frac{\left(\left[\frac{\ln n}{\ln 6}\right]+2\right)\ln 2+\frac{3}{5}}{\ln n} &= \lim_{n\to\infty} \frac{\left[\frac{\ln n}{\ln 6}\right]\ln 2}{\ln n} + \\ &\quad + \underbrace{\lim_{n\to\infty} \frac{2\ln 2}{\ln n}}_{=0} - \underbrace{\lim_{n\to\infty} \frac{\frac{3}{5}}{\ln n}}_{=0} = \\ &= \frac{\ln 2}{\ln 6}. \end{aligned} \tag{8.42}$$

Dosazením (8.42) do (8.41) obdržíme

$$\limsup_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} \leqq \frac{\ln 2}{\ln 6}. \tag{8.43}$$

Spojením nerovností (8.40) a (8.43) obdržíme

$$\frac{\ln 2}{\ln 6} \leqq \liminf_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} \leqq \limsup_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} \leqq \frac{\ln 2}{\ln 6}.$$

Proto můžeme tvrdit, že existuje limita $\lim\limits_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n}$ a je rovna

$$\lim_{n\to\infty} \frac{\sum\limits_{\substack{a\in A\\ a\leqq n}} \frac{1}{a}}{\ln n} = \frac{\ln 2}{\ln 6}.$$

Podle Věty 3.8 to znamená, že

$$\delta(A) = \frac{\ln 2}{\ln 6}.$$

3. Nechť $A \subseteq \mathbb{N}$. Dokažte, že $\lim\limits_{m\to\infty} \left(\sup\limits_{k\geqq m} \frac{A(k)}{k}\right) = \limsup\limits_{k\to\infty} \frac{A(k)}{k}$.

Řešení:

Uvažme, že $\sup\limits_{k\geqq m}\frac{A(k)}{k}$ je supremum množiny

$$Q_m = \left\{\frac{A(m)}{m}, \frac{A(m+1)}{m+1}, \frac{A(m+2)}{m+2}, \dots\right\}$$

a $\limsup\limits_{k\to\infty}\frac{A(k)}{k}$ je největší hromadný bod množiny

$$Q = \left\{\frac{A(1)}{1}, \frac{A(2)}{2}, \frac{A(3)}{3}, \dots, \frac{A(m)}{m}, \dots\right\},$$

a tedy i množiny Q_m (množina Q_m vznikne odebráním pouze konečně mnoha prvků z množiny Q, a tak musí mít stejné hromadné body[1]).

Supremum množiny Q_m je bod (číslo), který je (kromě jiného) větší, nebo roven libovolnému bodu množiny Q_m. Hromadný bod množiny Q_m je limitou nějaké posloupnosti prvků z Q_m, proto i on je menší, nebo roven supremu množiny Q_m. Symbolicky zapsáno:

$$\forall m \in \mathbb{N} : \sup_{k\geqq m}\frac{A(k)}{k} \geqq \limsup_{k\to\infty}\frac{A(k)}{k} \tag{8.44}$$

Označíme-li $s = \limsup\limits_{k\to\infty}\frac{A(k)}{k}$, pak podle (8.44) musí pro každé $m \in \mathbb{N}$ platit

$$\sup_{k\geqq m}\frac{A(k)}{k} - s \geqq 0,$$

a tak

$$\sup_{k\geqq m}\frac{A(k)}{k} - s = \left|\sup_{k\geqq m}\frac{A(k)}{k} - s\right| \tag{8.45}$$

Číslo s je největší hromadný bod množiny Q. Znamená to, že pro libovolné $\frac{\varepsilon}{2} > 0$ existuje jen konečně mnoho prvků množiny Q větších než $s + \frac{\varepsilon}{2}$.

[1]Hromadný bod množiny Q si můžete představit jako puntík na reálné ose, kolem kterého se „hromadí“ prvky (čísla) z množiny Q a to tak, že v libovolně malém okolí tohoto bodu vždy najdeme nekonečně mnoho prvků z množiny Q. Proto, odebereme-li z množiny Q konečný počet prvků, nic se nezmění - hromadný bod zůstane hromadným bodem.

Abychom všechny takové prvky odstranili, stačí zvolit dostatečně velké m (označme jej m_0) tak, aby množina Q_{m_0} tyto prvky neobsahovala[1]. (Množiny Q_m, kde $m \geqq m_0$ pak takové prvky také neobsahují.) Symbolicky zapsáno[2]:

$$\forall \varepsilon > 0 \exists m_0 \in \mathbb{N} : \forall k \geqq m_0 : \frac{A(k)}{k} \leqq s + \frac{\varepsilon}{2}.$$

Prvky všech množin Q_m, kde $m \geqq m_0$ splňují, že jsou menší, než $s + \frac{\varepsilon}{2}$. A tak suprema těchto množin mohou být nejvýše rovna $s + \frac{\varepsilon}{2}$ a určitě jsou menší, než $s + \varepsilon$. Symbolicky zapsáno:

$$\forall \varepsilon > 0 \exists m_0 \in \mathbb{N} : \forall m \geqq m_0 : \sup_{k \geqq m} \frac{A(k)}{k} < s + \varepsilon,$$

po drobné úpravě nerovnosti dostaneme

$$\forall \varepsilon > 0 \exists m_0 \in \mathbb{N} : \forall m \geqq m_0 : \sup_{k \geqq m} \frac{A(k)}{k} - s < \varepsilon$$

a s využitím (8.45)

$$\forall \varepsilon > 0 \exists m_0 \in \mathbb{N} : \forall m \geqq m_0 : \left| \sup_{k \geqq m} \frac{A(k)}{k} - s \right| < \varepsilon \tag{8.46}$$

Tvrzení (8.46) je ekvivalentní (viz definice limity posloupnosti) s tvrzením

$$\lim_{m \to \infty} \left(\sup_{k \geqq m} \frac{A(k)}{k} \right) = s.$$

Nyní si stačí jen vzpomenout, že $\limsup\limits_{k \to \infty} \frac{A(k)}{k} = s$.

8.4 Kongruence na množině celých čísel

8.4.1 Výsledky Cvičení 4.1.1

Cvičení k podkapitole *Relace kongruence na množině cělých čísel.*

[1] Nezajímá nás konkrétní hodnota čísla m_0, stačí nám ke štěstí vědomí, že takové m_0 určitě existuje!

[2] Tento zápis znamená, že pro dané ϵ najdeme Q_{m_0} neobsahující prvky, které by byly větší, či rovny $s + \frac{\varepsilon}{2}$.

1. Dokažte následující tvrzení. Pokud je rozdíl dvou celých čísel dělitelný číslem m, musí tato čísla patřit do stejné zbytkové třídy modulo m.

   Řešení:

   Uvažujme čísla $x_1, x_2 \in \mathbb{Z}$ jejichž rozdíl je dělitelný číslem m. To jest, existuje $k \in \mathbb{Z}$ takové, že

   $$x_1 - x_2 = km$$

   Máme za úkol dokázat, že x_1 a x_2 v takovém případě patří do stejné zbytkové třídy modulo m. To nastane, pokud $x_1 \equiv x_2 (\mathrm{mod}\, m)$. Ale pravdivost vztahu $x_1 \equiv x_2 (\mathrm{mod}\, m)$ okamžitě plyne z Definice 4.1 :). Ta říká, že

   $$x_1 \equiv x_2 (\mathrm{mod}\, m) \Leftrightarrow x_1 - x_2 = km$$

8.4.2 Výsledky Cvičení 4.2.1

Cvičení k podkapitole *Lineární kongruence.*

1. Nalezněte všechna řešení lineární kongruence $14x \equiv 5 (\mathrm{mod}\, 23)$.

   Řešení:
   Jde o lineární kongruenci $ax \equiv b (\mathrm{mod}\, m)$, kde $a = 14$, $b = 5$ a $m = 23$, $\gcd(a, m) = \gcd(14, 23) = 1$. Podle Věty 4.14 můžeme tvrdit, že řešení bude jediné.

   Jak jej nalézt? Existuje jen dvacettři různých zbytkových tříd modulo 23, a tak by nebyl problém vzít jednu po druhé a vyzkoušet prostým dosazením do kongruence, která vyhovuje. Nicméně tento postup je vhodný jen pro malá m. Proto, z cvičných důvodů, najdeme řešení postupem uvedeným v důkazu Věty 4.14.

   Největším společným dělitelem čísel 23 a 14 je číslo 1. Postupem uvedeným ve Cvičení 1.2.1 vyjádříme $\gcd(23, 14)$ jako lineární kombinaci čísel 23 a 14. To jest, potřebujeme nalézt celá čísla x_0 a y_0 tak, aby $1 = x_0 23 + y_0 14$.

   Nejprve použijeme Euklidův algoritmus.

$$\begin{aligned} 23 &= 1.14 + 9 && (8.47)\\ 14 &= 1.9 + 5 && (8.48)\\ 9 &= 1.5 + 4 && (8.49)\\ 5 &= 1.4 + 1 && (8.50)\\ 4 &= 4.1 + 0 \end{aligned}$$

Z rovnice (8.50) vyjádříme $\gcd(23, 14)$, tj. číslo 1.

$$1 = 5 - 4 \tag{8.51}$$

Z rovnice (8.49) vyjádříme zbytek 4 ($4 = 9 - 5$) a dosadíme do rovnice (8.51). Obdržíme

$$1 = 5 - (9 - 5). \tag{8.52}$$

Z rovnice (8.48) vyjádříme zbytek 5 ($5 = 14 - 9$) a dosadíme do rovnice (8.52). Obdržíme

$$1 = 14 - 9 - (9 - (14 - 9)). \tag{8.53}$$

Z rovnice (8.47) vyjádříme zbytek 9 ($9 = 23 - 14$) a dosadíme do rovnice (8.53). Obdržíme

$$1 = 14 - (23 - 14) - ((23 - 14) - (14 - (23 - 14))). \tag{8.54}$$

Tuto rovnici ještě upravíme:

$$\begin{aligned} 1 &= 14 - 23 + 14 - (23 - 14) + (14 - (23 - 14))\\ 1 &= 14 - 23 + 14 - 23 + 14 + 14 - 23 + 14\\ 1 &= \underbrace{-3}_{=x_0}.23 + \underbrace{5}_{=y_0}.14 && (8.55) \end{aligned}$$

V zadané kongruenci $14x \equiv 5 (\mathrm{mod}\, 23)$ potřebujeme vyjádřit číslo 5 pomocí lineární kombinace čísel 14 a 23. Proto rovnici (8.55) vynásobíme číslem 5. Obdržíme tak rovnost $5 = -15.23 + 25.14$. Dosadíme do zadané kongruence:

$$\begin{aligned} 14x &\equiv 5 (\mathrm{mod}\, 23)\\ 14x &\equiv -15.\underbrace{23}_{\equiv 0 (\mathrm{mod}\, 23)} + \underbrace{25}_{\equiv 2 (\mathrm{mod}\, 23)}.14 (\mathrm{mod}\, 23)\\ 14x &\equiv 2.14 (\mathrm{mod}\, 23)\\ x &\equiv 2 (\mathrm{mod}\, 23) && (8.56) \end{aligned}$$

Z (8.56) plyne, že hledaným řešením kongruence $14x \equiv 5(\mathrm{mod}\,23)$ je zbytková třída $\overline{2}_{23}$

2. Nalezněte všechna řešení lineární kongruence $3x \equiv 15(\mathrm{mod}\,6)$.

   Řešení:

   Přidržíme-li se označení užívaného ve Větě 4.14, pak řešíme lineární kongruenci $ax \equiv b(\mathrm{mod}\,m)$, kde $a = 3$, $b = 15$ a $m = 6$. Protože $\gcd(a, m) = = \gcd(3, 6) = 3$ dělí číslo $b = 15$, má tato kongruence právě tři různá řešení.

   Jak je nalézt?

   Všechna čísla vyskytující se v kongruenci $3x \equiv 15(\mathrm{mod}\,6)$ podělíme číslem $\gcd(a, m) = \gcd(3, 6) = 3$. Obdržíme tak kongruenci $x \equiv 5(\mathrm{mod}\,2)$. Ta má již jen jediné řešení (neboť $\gcd(1, 2) = 1$). A evidentně jím je zbytková třída

   $$\overline{x_0}_2 = \overline{5}_2.$$

   Řešení zadané kongruence $3x \equiv 15(\mathrm{mod}\,6)$ pak dostaneme tak, že přičítáme násobky čísla 2. Víme, že řešení jsou právě tři, proto hledaná řešení najdeme jako

   $$\overline{x_0}_6,\ \overline{x_0 + 2}_6,\ \overline{x_0 + 4}_6.$$

   $$\overline{5}_6,\ \overline{5 + 2}_6,\ \overline{5 + 4}_6.$$

   Tzn., jde o zbytkové třídy $\overline{5}_6$, $\overline{7}_6$ a $\overline{9}_6$. Tento výsledek ještě můžeme upravit. Jde o zbytkové třídy $\overline{5}_6$, $\overline{1}_6$ a $\overline{3}_6$.

3. Nalezněte všechna řešení lineární kongruence $32x \equiv 10(\mathrm{mod}\,46)$.

   Řešení:
   Budeme postupovat obdobně jako v předchozím příkladu. Nejprve všechna čísla vyskytující se v kongruenci $32x \equiv 10(\mathrm{mod}\,46)$ podělíme největším společným dělitelem čísel 32 a 46, tj. číslem 2. Obdržíme

   $$16x \equiv 5(\mathrm{mod}\,23).$$

   Nalezneme řešení této kongruence (bude jediné, neboť $\gcd(16, 23) = 1$). Budeme postupovat stejně jako v prvním příkladě tohoto cvičení. Nejprve Euklidovým algoritmem nalezneme $\gcd(23, 16)$.

$$\begin{aligned} 23 &= 1.16 + 7 && (8.57)\\ 16 &= 2.7 + 2 && (8.58)\\ 7 &= 3.2 + 1 && (8.59)\\ 2 &= 2.1 + 0 \end{aligned}$$

Z rovnice (8.59) vyjádříme $\gcd(23, 16)$, tj. číslo 1.

$$1 = 7 - 3.2 \tag{8.60}$$

Z rovnice (8.58) vyjádříme zbytek 2 ($2 = 16 - 2.7$) a dosadíme do rovnice (8.60). Obdržíme

$$1 = 7 - 3.(16 - 2.7). \tag{8.61}$$

Z rovnice (8.57) vyjádříme zbytek 7 ($7 = 23 - 16$) a dosadíme do rovnice (8.61). Obdržíme

$$1 = (23 - 16) - 3.(16 - 2.(23 - 16)). \tag{8.62}$$

Odtud dokážeme vyjádřit $\gcd(23, 16)$, tj. číslo 1, jako lineární kombinaci (součet násobků) čísel 23 a 16.

$$\begin{aligned} 1 &= 23 - 16 - 3.(16 - 2.(23 - 16))\\ 1 &= 23 - 16 - 3.16 + 6(23 - 16)\\ 1 &= 23 - 16 - 3.16 + 6.23 - 6.16\\ 1 &= \underbrace{7}_{=x_0}.23 - \underbrace{10}_{=y_0}.16 && (8.63) \end{aligned}$$

V řešené kongruenci $16x \equiv 5 (\mathrm{mod}\, 23)$ potřebujeme vyjádřit číslo 5 jako lineární kombinaci čísel 23 a 16. Proto vynásobíme rovnici (8.63) číslem 5. Obdržíme tak

$$5 = 35.23 - 50.16.$$

Po dosazení do $16x \equiv 5 (\mathrm{mod}\, 23)$ řešíme kongruenci

$$\begin{aligned} 16x &\equiv 35.23 - 50.16 (\mathrm{mod}\, 23)\\ 16x &\equiv 35.\underbrace{23}_{\equiv 0 (\mathrm{mod}\, 23)} - \underbrace{50}_{\equiv 4 (\mathrm{mod}\, 23)}.16 (\mathrm{mod}\, 23)\\ 16x &\equiv -4.16 (\mathrm{mod}\, 23)\\ x &\equiv \underbrace{-4}_{\equiv 19 (\mathrm{mod}\, 23)} (\mathrm{mod}\, 23) && (8.64) \end{aligned}$$

Můžeme proto tvrdit, že $\overline{19}_{23}$ je řešením kongruence $16x \equiv 5(\mathrm{mod}\,23)$. Všechna řešení zadané kongruence $32x \equiv 10(\mathrm{mod}\,46)$ proto dostaneme jako

$$\overline{19}_{46}\,, \overline{19+23}_{46}.$$

To jest, hledanými řešeními zadané kongruence $32x \equiv 10(\mathrm{mod}\,46)$ jsou zbytkové třídy $\overline{19}_{46}$ a $\overline{42}_{46}$.

8.4.3 Výsledky Cvičení 4.3.1

Cvičení k podkapitole *Fermatova - Eulerova věta.*

1. V Poznámce 4.24 bylo ukázáno, že kongruence $a^{\varphi(m)} \equiv 1(\mathrm{mod}\,m)$ nemusí být splněna v případě, kdy $\gcd(a,m) \neq 1$. Existují nějaká čísla a a m, taková, že $\gcd(a,m) \neq 1$ a přitom platí $a^{\varphi(m)} \equiv 1(\mathrm{mod}\,m)$?

   Řešení:
   Žádná taková čísla a a m neexistují. Dokážeme to sporem. Předpokládejme, že $\gcd(a,m) = d > 1$ a platí

   $$a^{\varphi(m)} \equiv 1(\mathrm{mod}\,m). \tag{8.65}$$

   Podle definice kongruence je vztah (8.65) ekvivalentní s tvrzením

   $$a^{\varphi(m)} - 1 = km, \tag{8.66}$$

   kde k je nějaké celé číslo.

   Protože $\gcd(a,m) = d$, existují čísla a_1 a m_1 tak, že $a = da_1$ a $m = dm_1$. Dosazením do (8.66) obdržíme

   $$d^{\varphi(m)}a_1^{\varphi(m)} - 1 = kdm_1$$

   a po jednoduché úpravě

   $$d\left(d^{\varphi(m)-1}a_1^{\varphi(m)} - km_1\right) = 1. \tag{8.67}$$

   Z rovnice (8.67) pak plyne, že d je dělitelem čísla 1. To je ovšem spor s předpokladem $\gcd(a,m) = d > 1$.

   Ukázali jsme tak, že v případě, kdy $\gcd(a,m) = d > 1$, nemůže nastat $a^{\varphi(m)} \equiv 1(\mathrm{mod}\,m)$.

2. Pomocí Fermatovy věty nalezněte $x \in \{0,1,\ldots,6\}$ splňující kongruenci $x \equiv 2^{328}(\mathrm{mod}\,7)$.

Řešení:
Protože $\gcd(2,7)=1$, platí $2^{\varphi(7)}=2^6\equiv 1(\mathrm{mod}\,7)$. Proto

$$x\equiv 2^{328}=2^{324}2^4\equiv(2^6)^{54}2^4\equiv 1^{54}2^4\equiv 2^4\equiv 16\equiv 2(\mathrm{mod}\,7).$$

Řešením je tedy číslo $x=2$.

3. Pomocí Fermatovy věty nalezněte $x\in\{0,1,2\}$ splňující kongruenci $5x\equiv 1(\mathrm{mod}\,3)$.

   Řešení:
   Hledané číslo x jistě nepatří do zbytkové třídy $\overline{0}$, neboť po dosazení bychom obdrželi $0\equiv 1(\mathrm{mod}\,3)$ (a to není pravda). Proto $x\in\{1,2\}$. A tak $\gcd(x,3)=$ $=1$. Podle Fermatovy věty je $x^2\equiv 1(\mathrm{mod}\,3)$. Vynásobením obou stran zadané kongruence číslem x obdržíme kongruenci

   $$5\underbrace{x^2}_{\equiv 1}\equiv x(\mathrm{mod}\,3).$$

   Odtud je jasné, že $5\equiv x(\mathrm{mod}\,3)$ a tak $x=2$.

4. Pomocí Fermatovy věty nalezněte $x\in\{0,1,2\}$ splňující kongruenci $2x^2+$ $+5x+1\equiv 0(\mathrm{mod}\,3)$.

   Řešení:
   Hledané číslo x jistě nepatří do zbytkové třídy $\overline{0}$, neboť po dosazení bychom obdrželi $1\equiv 0(\mathrm{mod}\,3)$ (a to není pravda). Stejně jako v předchozím příkladě pak musí platit, že $x^2\equiv 1(\mathrm{mod}\,3)$. Dosazením do zadané kvadratické kongruence obdržíme $2+5x+1\equiv 0(\mathrm{mod}\,3)$. A tak

   $$5x\equiv -3(\mathrm{mod}\,3),$$

   $$5x\equiv 0(\mathrm{mod}\,3),$$

   $$x\equiv 0(\mathrm{mod}\,3).$$

   To by ovšem znamenalo, že $x=0$. Tuto možnost jsme však vyloučili. Z toho plyne, že zadaná kongruence nemá řešení.

8.5 Operace na $\mathbb{Z}_n$

8.5.1 Výsledky Cvičení 5.0.2

Cvičení ke kapitole *Operace na $\mathbb{Z}_n$*.

1. Věta 5.5 říká, že neutrálním prvkem vzhledem k operaci násobení zbytkových tříd modulo n je zbytková třída $\overline{1}_n$. Nemůže ale roli neutrálního prvku hrát i jiná zbytková třída ze Z_n? Dokažte, že ne, že existuje pouze jediný

neutrální prvek vzhledem k operaci násobení zbytkových tříd (Definice 5.1).

Řešení:
Podle Věty 5.5 je $\overline{1}_n$ neutrálním prvkem vzhledem k násobení na $\mathbb{Z}_n$. A tak víme, že neutrální prvek vzhledem k násobení na $\mathbb{Z}_n$ existuje. Předpokládejme nyní, že $\overline{e_{1}}_n$ a také $\overline{e_{2}}_n$ jsou neutrální prvky vzhledem k násobení na $\mathbb{Z}_n$ (a ukážeme, že ve skutečnosti jde o tentýž prvek a ne o dva různé). Podle definice neutrálního prvku, musí platit:

$$\overline{e_{1}}_n = \overline{e_{1}}_n\overline{e_{2}}_n = \overline{e_{2}}_n.$$

První rovnost nastane, neboť $\overline{e_{2}}_n$ je neutrální prvek a druhá rovnost platí, neboť $\overline{e_{1}}_n$ je neutrální prvek. Odtud vidíme že nemohou existovat dva různé neutrální prvky.

2. Dokažte, že ke každému prvku v $Z_n - \{\overline{0}_n\}$ existuje jeho prvek inverzní (vzhledem k násobení) právě tehdy, když n je prvočíslo.

Řešení:
Uvažme, že $Z_n - \{\overline{0}_n\} = \{\overline{1}_n, \overline{2}_n, \ldots, \overline{n-1}_n\}$. Podle Věty 5.9 mají všechny zbytkové třídy z $Z_n - \{\overline{0}_n\}$ multiplikativní inverzi právě tehdy, když

$$\forall a \in \{1, 2, \ldots, n-1\} \,:\, \gcd(a, n) = 1. \tag{8.68}$$

Když n je prvočíslo, je výrok (8.68) jistě pravdivý. Pokud n není prvočíslo, je n jistě dělitelné nějakým číslem a, které splňuje nerovnosti $2 \leqq a < n$. Potom by ale $\gcd(a, n) = a \neq 1$. Pro n, které není prvočíslo tedy (8.68) není pravdivý výrok. Proto (8.68) je pravda právě tehdy, když n je prvočíslo.

3. Vytvořte tabulku násobení zbytkových tříd modulo 7.

Řešení:
Viz tabulka 8.1.

4. Pomocí tabulky násobení v Z_7 (Tabulka 8.1)vyřešte lineární kongruence $3x \equiv 2 (\mathrm{mod}\, 7)$ a $-5x \equiv -2 (\mathrm{mod}\, 7)$.

Řešení:

- Řešíme kongruenci $3x \equiv 2 (\mathrm{mod}\, 7)$. V Tabulce 8.1 nalezneme multipli-

Tab. 8.1 Tabulka násobení v $\mathbb{Z}_7$.

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6
2	0	2	4	6	**1**	3	5
3	0	3	6	2	5	**1**	4
4	0	4	**1**	5	2	6	3
5	0	5	3	**1**	6	4	2
6	0	6	5	4	3	2	**1**

kativní inverzi ke zbytkové třídě $\overline{3}$ - je to zbytková třída $\overline{5}$. Proto:

$$\begin{aligned} 3x &\equiv 2 (\mathrm{mod}\, 7) \quad | \cdot 5 \\ \underbrace{5 \cdot 3}_{\equiv 1} x &\equiv 10 (\mathrm{mod}\, 7) \\ x &\equiv 3 (\mathrm{mod}\, 7) \end{aligned}$$

Řešením zadané kongruence je proto zbytková třída $\overline{3}_7$.

Zkouška: $3x \equiv 3 \cdot 3 \equiv 9 \equiv 2 (\mathrm{mod}\, 7)$.

- Řešíme kongruenci $-5x \equiv -2 (\mathrm{mod}\, 7)$. To je ekvivalentní řešení kongruence $2x \equiv 5 (\mathrm{mod}\, 7)$. V Tabulce 8.1 proto nalezneme multiplikativní inverzi ke zbytkové třídě $\overline{2}$ - je to zbytková třída $\overline{4}$. Proto:

$$\begin{aligned} -5x &\equiv -2 (\mathrm{mod}\, 7) \quad | +7 \\ 2x &\equiv 5 (\mathrm{mod}\, 7) \quad | \cdot 4 \\ \underbrace{4 \cdot 2}_{\equiv 1} x &\equiv 20 (\mathrm{mod}\, 7) \\ x &\equiv 6 (\mathrm{mod}\, 7) \end{aligned}$$

Řešením zadané kongruence je proto zbytková třída $\overline{6}_7$.

Zkouška: $-5x \equiv -5 \cdot 6 \equiv 2 \cdot 6 \equiv 12 \equiv 5 \equiv -2 (\mathrm{mod}\, 7)$.

8.6 Aritmetické funkce

8.6.1 Výsledky Cvičení 6.1.1

Cvičení k podkapitole *Eulerova funkce*.

1. Vyřešte Příklad 2.4 pro libovolnou číselnou soustavu. Kolik procent přirozených čísel můžeme vyloučit v případě použití číselné soustavy o základu n?

   Řešení:

   Pomocí Věty 2.2 a k ní se vztahující Poznámky 2.3 můžeme určit, jakou cifrou může končit zápis prvočísla v číselné soustavě o základu n. V takové soustavě zápis $z = 325$ vlastně znamená, že $z = 3n^2 + 2n + 5$, obdobně $2125 = 2n^3+1n^2+2n+5$. Obecně, používáme-li číselnou soustavu o základu n, pak číslo zapsané pomocí cifer ve tvaru $a_m \dots a_2 a_1 a_0$ je rovno $a_m n^m + + \cdots + a_2 n^2 + a_1 n + a_0$.

   Vidíme, že číslo zapsané v číselné soustavě o základu n má tvar

   $$a_m n^m + \cdots + a_2 n^2 + a_1 n + a_0 = n \underbrace{(a_m n^{m-1} + \cdots + a_2 n + a_1)}_{k} + a_0 = nk + a_0,$$

   kde a_0 je poslední cifra v ciferném zápisu a samozřejmě všechny cifry $a_i \in \{0, 1, \dots, n-1\}$.

   Podle Věty 2.2 a Poznámky 2.3 může být číslo

   $$z = a_m \dots a_2 a_1 a_0 = nk + a_0, \text{ kde } k \geqq 1$$

   (Všimněte si, že uvažujeme nyní jen čísla větší, nebo rovná n) prvočíslem pouze v případě, že čísla n a a_0 jsou navzájem nesoudělná, to jest, když $\gcd(n, a_0) = 1$.

   To znamená, že číslo $z \geqq n$, jehož poslední cifrou v soustavě o základu n je a_0, kde $\gcd(n, a_0) = 1$ může (ale nemusí!) být prvočíslo. Ostatní čísla nejsou prvočísla. Takových cifer je mezi čísly $1, 2, \dots, n-1$ (těchto hodnot může nabývat a_0) celkem $\varphi(n)$.

   Z podezření, že jsou prvočísly, jsme tak vyloučili všechna čísla k ve tvaru

   $$k = nk + a_0, \text{ kde } \gcd(n, a_0) > 1.$$

   Vylučujeme proto všechna čísla ze zbytkových třídy $\overline{a_0}$ modulo n, kde $\gcd(n, a_0) > 1$. Těch je celkem $n - \varphi(n)$ (všechny zbytkové třídy minus ty z redukovaného systému zbytkových tříd modulo n).

Na základě výsledků Kapitoly 3 můžeme poněkud nepřesně říci, že jsme vyloučili

$$\frac{n-\varphi(n)}{n}\cdot 100\% = \left(1-\frac{\varphi(n)}{n}\right)100\%$$

přirozených čísel z podezření, že jsou prvočísly.

2. Jaké n je třeba v předchozím příkladě zvolit, abychom maximalizovali procento přirozených čísel u kterých můžeme vyloučit podezření z prvočíselnosti?

Řešení:

Předem řekněme, že odpověď na otázku není zcela jednoznačná. Prostudujeme-li předchozí příklad, je zřejmé, že hledáme číslo n tak, aby hodnota $\frac{n-\varphi(n)}{n}$ byla co největší. Uvažme, že

$$\frac{n-\varphi(n)}{n} = 1-\frac{\varphi(n)}{n}.$$

Úlohu proto můžeme přeformulovat. Hledáme n tak, aby hodnota $\frac{\varphi(n)}{n}$ byla co nejmenší. Využijeme Větu 6.8. Podle ní pro $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, kde p_1, p_2, …, p_k jsou navzájem různá prvočísla, platí

$$\frac{\varphi(n)}{n} = \frac{n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)}{n} = \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

Hledáme proto $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ takové, aby hodnota součinu

$$\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \tag{8.69}$$

byla co nejmenší. Všimněme si, že hodnota součinu (8.69) nezávisí na hodnotách exponentů $\alpha_1, \alpha_2, \ldots, \alpha_k$ v kanonickém rozkladu n. Uvažujme proto co nejmenší n. Je jím $n = p_1p_2\cdots p_k$. Jaké zvolit k? To jest, kolik prvočísel by mělo být v kanonickém rozkladu $n = p_1p_2\cdots p_k$, aby hodnota součinu

(8.69) byla co nejnižší? Evidentně jsou splněny nerovnosti

$$\begin{aligned} 2 &\leqq p_i \\ \frac{1}{2} &\geqq \frac{1}{p_i} \\ -\frac{1}{2} &\leqq -\frac{1}{p_i} \\ 1-\frac{1}{2} &\leqq 1-\frac{1}{p_i} \\ \frac{1}{2} &\leqq 1-\frac{1}{p_i} \end{aligned} \tag{8.70}$$

A odtud snadno domyslíme, že

$$\frac{1}{2} \leqq 1-\frac{1}{p_i} < 1.$$

Chceme-li co nejmenší součin (8.69), měl by proto mít co nejvíce činitelů[1]. To jest, k by mělo být co největší. Jaké prvočísla p_i však zvolit? Malé? Velké? Snadno odvodíme, že pro $p_i < p_I$ platí

$$\begin{aligned} p_i &< p_I \\ \frac{1}{p_i} &> \frac{1}{p_I} \\ -\frac{1}{p_i} &< -\frac{1}{p_I} \\ 1-\frac{1}{p_i} &< 1-\frac{1}{p_I} \end{aligned}$$

Je tedy v našem zájmu, aby prvočísla p_i byla co nejmenší. Zvolíme proto $p_1 = 2$, $p_2 = 3$, ... To jest, posloupnost p_i je posloupnost *všech* prvočísel – nebudeme žádné přeskakovat.

Nalezenými adepty pro základ číselné soustavy jsou proto následující čísla

[1]Násobíme-li kladné číslo x kladným číslem $a = 1 - \frac{1}{p_i}$, které je menší než jedna, dozajista bude výsledek menší, než x.

(uvedeme i kolik procent čísel vyloučíme z podezření, že jde o prvočísla)

$$\begin{aligned}
n_1 = 2 &\Rightarrow \text{vyloučíme} \quad \left(1-\left(1-\tfrac{1}{2}\right)\right)\cdot 100\% = \tfrac{1}{2}\cdot 100\% \\
n_2 = 2\cdot 3 &\Rightarrow \text{vyloučíme} \quad \left(1-\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{3}\right)\right)\cdot 100\% = \tfrac{2}{3}\cdot 100\% \\
n_3 = 2\cdot 3\cdot 5 &\Rightarrow \text{vyloučíme} \quad \left(1-\prod_{i=1}^{3}\left(1-\tfrac{1}{p_i}\right)\right)\cdot 100\% = \tfrac{11}{15}\cdot 100\% \\
&\vdots \\
n_k = \prod_{i=1}^{k} p_i &\Rightarrow \text{vyloučíme} \quad \left(1-\prod_{i=1}^{k}\left(1-\tfrac{1}{p_i}\right)\right)\cdot 100\% = \alpha_k\cdot 100\% \\
&\vdots
\end{aligned} \tag{8.71}$$

S rostoucím k roste α_k. Měli bychom za základ číselné soustavy proto zvolit co největší n_k. Posloupnost čísel n_k však evidentně roste nade všechny meze. Nemůžeme proto vybrat *největší* číslo n_k. Vždy musíme zvážit, s jakou nejvyšší hodnotou n_k a tím pádem i α_k se spokojíme.

3. Označme $n_k = \prod_{i=1}^{k} p_i$, kde $\{p_i\}_{i=1}^{\infty}$ je posloupnost všech prvočísel. Dále označme $\alpha_k = 1 - \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$. Dokažte, že $\lim_{k\to\infty} \alpha_k\cdot 100\% = 100\%$. To jest, dokažte, že postupem popsaným v řešeních předchozích příkladů je možné při volbě dostatečně velkého n_k vyloučit z podezření, že jde o prvočísla, libovolně velké procento čísel.

Řešení:

Naším cílem je dokázat, že $\lim_{k\to\infty} \alpha_k = 1$, kde $\alpha_k = 1 - \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$. To je logicky ekvivalentní s tvrzením, že

$$\lim_{k\to\infty} \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) = 0. \tag{8.72}$$

Rovnost (8.72) nyní dokážeme. Pro libovolné prvočíslo p_i snadno ověříme pravdivost následujících nerovností

$$\begin{aligned}
-1 &< 0 \\
p_i^2 - 1 &< p_i^2 \\
(p_i-1)(p_i+1) &< p_i p_i \\
\tfrac{p_i-1}{p_i} &< \tfrac{p_i}{p_i+1}.
\end{aligned} \tag{8.73}$$

Proto pro každé $k \in \mathbb{N}$ platí

$$\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)=\prod_{i=1}^{k}\left(\frac{p_i-1}{p_i}\right)<\prod_{i=1}^{k}\left(\frac{p_i}{p_i+1}\right)=\frac{1}{\prod_{i=1}^{k}\left(1+\frac{1}{p_i}\right)}<\frac{1}{\sum\limits_{i=1}^{k}\frac{1}{p_i}}. \tag{8.74}$$

A tak

$$0 \leqq {}^{1}\liminf_{k\to\infty}\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \leqq \limsup_{k\to\infty}\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \leqq \lim_{k\to\infty}\frac{1}{\sum\limits_{i=1}^{k}\frac{1}{p_i}}, \tag{8.75}$$

pokud limita $\lim\limits_{k\to\infty}\frac{1}{\sum\limits_{i=1}^{k}\frac{1}{p_i}}$ existuje. My však víme že ano! Podle Věty 2.7 platí $\lim\limits_{k\to\infty}\sum\limits_{i=1}^{k}\frac{1}{p_i}=\infty$. Proto

$$\lim_{k\to\infty}\frac{1}{\sum\limits_{i=1}^{k}\frac{1}{p_i}}=0.$$

Dosazením do 8.75 obdržíme

$$0 \leqq \liminf_{k\to\infty}\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \leqq \limsup_{k\to\infty}\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \leqq 0. \tag{8.76}$$

Proto

$$\lim_{k\to\infty}\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)=0.$$

8.6.2 Výsledky Cvičení 6.2.1

Cvičení k podkapitole *Funkce sigma*.

1. Dokažte, že číslo p je prvočíslo právě tehdy, když $\sigma_0(p)=2$.

   Řešení:

   Je zřejmé, že p je prvočíslo právě tehdy, když má právě dva dělitele (číslo 1 a p). Jinak řečeno, p je prvočíslo právě tehdy, když $\sigma_0(p)=2$.

[1] Neboť v součinu $\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$ násobíme samé kladné čísla.

2. Dokažte, že oborem hodnot funkce σ_0 je množina $\mathbb{N}$.

   Řešení:

   Uvažme, že platí

$$\begin{aligned} n = 1 &\Rightarrow \sigma_0(n) = 1 \,(\text{ dělitelé } n : 1) \\ n = 2 &\Rightarrow \sigma_0(n) = 2 \,(\text{ dělitelé } n : 1, 2) \\ n = 2^2 &\Rightarrow \sigma_0(n) = 3 \,(\text{ dělitelé } n : 1, 2, 2^2) \\ &\vdots \\ n = 2^{m-1} &\Rightarrow \sigma_0(n) = m \,(\text{ dělitelé } n : 1, 2, \ldots, 2^{m-1}) \\ &\vdots \end{aligned}$$

3. Dokažte, že $\liminf_{n\to\infty} \sigma_0(n) = 2$.

   Řešení:

   Nejprve si všimněme, že

$$\forall n \in \mathbb{N}, n > 1 : \sigma_0(n) \geqq 2, \tag{8.77}$$

   neboť každé přirozené číslo $n > 1$ má alespoň dva různé dělitele, a to čísla 1 a n. Podle prvního příkladu tohoto cvičení navíc víme, že pro posloupnost všech prvočísel $\{p_i\}_{i=1}^{\infty}$ platí

$$\forall i \in \mathbb{N} : \sigma_0(p_i) = 2. \tag{8.78}$$

   Proto

$$\lim_{i\to\infty} \sigma_0(p_i) = 2. \tag{8.79}$$

   Z rovnice (8.79) plyne, že číslo 2 je hromadným bodem posloupnosti $\{\sigma_0(n)\}_{n=1}^{\infty}$. Z (8.77) pak plyne, že 2 je nejmenším hromadným bodem posloupnosti $\{\sigma_0(n)\}_{n=1}^{\infty}$. Symbolicky zapsáno

$$\liminf_{n\to\infty} \sigma_0(n) = 2.$$

4. Dokažte, že $\limsup_{n\to\infty} \sigma_0(n) = \infty$.

   Řešení:

Uvažujme posloupnost čísel $\{2^k\}_{k=1}^{\infty}$. Jak jsme viděli výše, $\sigma_0(2^k) = k + 1$. Proto

$$\lim_{k\to\infty} \sigma_0(2^k) = \lim_{k\to\infty} k + 1 = \infty. \tag{8.80}$$

Z (8.80) vidíme, že ∞ je hromadným bodem posloupnosti $\{\sigma_0(n)\}_{n=1}^{\infty}$. Žádný větší hromadný bod posloupnost $\{\sigma_0(n)\}_{n=1}^{\infty}$ mít nemůže. Nekonečno je proto největším hromadným bodem posloupnosti $\{\sigma_0(n)\}_{n=1}^{\infty}$. Symbolicky zapsáno

$$\limsup_{n\to\infty} \sigma_0(n) = \infty.$$

Literatura

[1] Hardy, G.H. – Wright, E.M. *Theory of Numbers*. 6. vydání. Great Britain: Oxford University Press, 2008. 595 s. ISBN 978-0-19-921986-5.

[2] Apostol, T.M. *Introduction to Analytic Number Theory*. New York: Springer, 328 s. ISBN 978-0-387-90163-3.

[3] Pommersheim, J.E. – Marks, T.K. – Flapan E.L. *Number theory*. USA: Wiley, 2010. 753 s. ISBN 978-0-470-42413-1.

[4] Burian, K. *Kapitoly z geometrie II*. Ostrava: Ostravská univerzita, 1996. 287 s. ISBN 80-7042-732-9.

[5] Kolibiar, M. a kol. *Algebra a príbuzné disciplíny*. Bratislava: Alfa, 1983

[6] Blažek, J. – Koman, M. – Vojtášková, B. *Algebra a teoretická aritmetika 2*. Praha: SPN, 1985