

2. Počítání modulo

Hodiny ukazují devět a dali jsme se do přípravy lasagne, což trvá čtyři hodiny. Jako zkušený matematici hravě spočítáme, že budu hotovy ve 13 hodin, my ovšem víme, že v tu chvíli ručička na hodinách bude ukazovat na jedničku. Ve světě ručičkových hodin jsme zvyklí, že různá čísla dávají tutéž informaci, třeba 13 je 1, 18 je 6 a podobně. Platí to i pro počítání ve světě digitálu. Jestliže ve 23:00 spustí systém uprade, který trvá 5 hodin, tak nám konec vychází na 28:00, což pro nás znamená ve 4:00. Při určování denního času tedy můžeme čísla navzájem cyklicky nahrazovat.

Podobně to funguje třeba při určování azimutu, kdy vydat se ve směru 450 stupňů je totéž jako vydat se ve směru $450 - 360 = 90$ stupňů. To je samozřejmě jen aplikovaný pohled na měření úhlů v rovině, kde jsme také smíření s periodicitou 360 (popřípadě 2π).

V této kapitole pro to vytvoříme matematickou teorii. Je vysoce užitečná pro svět počítačů, například uvidíme, že se významně podílí na fungování Internetu.

2a. Kongruence, počítání modulo

Situace, kdy pro nás čísla periodicky opakují svůj praktický význam a jsou zaměnitelná, se matematicky zachycuje pomocí kongruence.



Definice.

Nechť $n \in \mathbb{N}$. Řekneme, že čísla $a, b \in \mathbb{Z}$ jsou **kongruentní modulo n** , značeno $a \equiv b \pmod{n}$, jestliže n dělí $a - b$.

Let $n \in \mathbb{N}$. We say that numbers $a, b \in \mathbb{Z}$ are **congruent modulo n** , denoted $a \equiv b \pmod{n}$, if $n \mid (a - b)$.

Číslu n se říká modul a jeho volbou vznikne konkrétní svět, ve kterém počítáme. Například volbou $n = 12$ vznikne svět ručičkových hodin. Nepředpokládá se, že by se v průběhu práce n měnilo. Je to tedy jakýsi základní parametr našeho pracovního světa.

Zvolené značení vyžaduje pozornost, protože zkratka „mod“ se teď objevuje ve dvou rozdílných kontextech. Když napíšeme $a \bmod n$, tak tím vyjadřujeme zbytek po dělení čísla a číslem n , třeba $15 \bmod 6 = 3$. Když napíšeme $a \equiv b \pmod{n}$, tak tím míníme kongruenci (neboli praktickou zaměnitelnost) dvou čísel a, b ve světě se zvoleným modulem n .

Někteří autoři používají v definici podmínku $n \mid (b - a)$. Nemá to žádný dopad na výslednou teorii, jen na důkazy. Ještě se k tomu vrátíme.

Příklad 2a.a: Pokud opravdu definice vystihuje náš hodinový příklad, tak by mělo novým jazykem platit, že $13 \equiv 1 \pmod{12}$. Zkouška podle definice: $13 - 1 = 12$, což je dělitelné dvanácti. Ano, souhlasí.

Jiný příklad: $3 \equiv 13 \pmod{5}$, protože $3 - 13 = -10$, což je dělitelné pěti.

Naopak neplatí $3 \equiv -3 \pmod{5}$, protože 5 nedělí $3 - (-3) = 6$.

△

Často se hodí poznávat kongruenci jinak než podle definice.



Věta 2a.1.

Nechť $n \in \mathbb{N}$. Pro čísla $a, b \in \mathbb{Z}$ jsou následující podmínky ekvivalentní:

(i) $a \equiv b \pmod{n}$,

(ii) existuje $k \in \mathbb{Z}$ takové, že $a = b + kn$,

(iii) $a \bmod n = b \bmod n$, tj. jsou si rovny zbytky čísel a, b po dělení číslem n .

Tato věta nabízí další dva způsoby, jak rozpoznat kongruenci. Odborně by se dalo říct, že nabízí charakterizace kongruence.

S Rozbor: Jak jsme již rozebrali v poznámce 1b.14, toto tvrzení v sobě zahrnuje tři ekvivalence, což se nejlépe dokáže uzavřeným cyklem implikací. Zde není důvod preferovat nějaký speciální průchod, tak to uděláme, jak to přišlo, tedy dokážeme implikace (i) \implies (ii), (ii) \implies (iii) a nakonec (iii) \implies (i), která uzavře cyklus.

Důkazy první a třetí implikace jsou přímočaré a snadné, stačí si u každé implikace napsat, co víme a co potřebujeme, a cesta by se měla nabídnout. Náročnější je přechod (ii) \implies (iii). Pro důkaz, že se dva zbytky po dělení rovnají, použijeme následující postup. Jeden ze zbytků vybereme a sepíšeme, co o něm z definice víme. Na základě toho pak ukážeme, že splňuje požadavky z definice i na ten druhý zbytek.

Poznamenejme, že v této sekci budeme zase nacházet především přímočaré důkazy, které lze použít k nácviu.

Důkaz (rutinní, poučný): Dány $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ libovolné.

1) (i) \implies (ii): Jestliže $a \equiv b \pmod{n}$, pak $n \mid (a - b)$. Proto existuje $k \in \mathbb{Z}$: $a - b = nk$, tedy $a = b + kn$.

2) (ii) \implies (iii): Předpokládejme, že $a = b + kn$ pro nějaké $k \in \mathbb{Z}$. Označme $r = a \bmod n$ (zbytek po dělení), tedy máme rozklad $a = qn + r$ splňující $q \in \mathbb{Z}$ a $0 \leq r < n$. Pak také máme $b = a - kn = (q - k)n + r$, kde $(q - k) \in \mathbb{Z}$ a $0 \leq r < n$, tedy jsou splněny podmínky z definice pro závěr $r = b \bmod n$.

3) (iii) \implies (i): Předpoklad: $a \bmod n = b \bmod n$, označme tento zbytek jako r . Pak existují $p, q \in \mathbb{Z}$ takové, že $a = pn + r$ a $b = qn + r$. Odtud $a - b = n(p - q)$ a $p - q \in \mathbb{Z}$, tedy $n \mid (a - b)$. Podle definice pak $a \equiv b \pmod{n}$.

Uzavřeli jsme kruh, proto jsou libovolná dvě z tvrzení (i) až (iii) spolu ekvivalentní. \square

Příklad 2a.b: Ověřme, že $21 \equiv 9 \pmod{6}$. Podle definice máme zkusit, zda 6 dělí $21 - 9 = 12$, což platí.

Podle podmínky (ii) to vidíme také, $21 = 9 + 2 \cdot 6$ a $2 \in \mathbb{Z}$.

Podmínka (iii): $21 \bmod 6 = 3$ a $9 \bmod 6 = 3$, zbytky se shodují.

\triangle

Poznámka: Algebraický zápis kongruence nabízí interpretaci, která je příjemná pro intuici: Výraz $b + kn$, $k \in \mathbb{Z}$ je možno vnímat jako zápis cesty z lokace b . Takže $a \equiv b \pmod{n}$ právě tehdy, pokud dokážeme z b doskákat do a jistým počtem kroků o velikosti n (celočíslným, nesmíme dělat půlkroky a podobně). Při počítání s menšími čísly je to efektivní způsob. Například snadno vidíme, že z 8 doskáceme pomocí pětky do -2 , a proto $-2 \equiv 8 \pmod{5}$. Je to také užitečná představa pro teoretické úvahy.

Pohled přes zbytky se hodí u modulů n , kde jsou zbytky hned patrné. Například ve světě modulu $n = 10$ vidíme zbytky po dělení jako poslední cifry čísel. Na první pohled je tak jasné, že číslo 1497853 je kongruentní s číslem 9628473, ale není kongruentní s číslem 2357652. Stejně tak snadno poznáme zbytky po dělení pěti, ovšem zrovna tyto příjemné moduly se v praxi moc nepoužívají.

\triangle

M Poznámka: V kapitole 1 se v důkazech osvědčilo přecházet od pojmu dělitelnosti k algebře. Pro kongruenci teď máme díky definici a větě dvě možnosti.

Vpravo vidíme, jak přechází data pro jistý zvolený modul $n \in \mathbb{N}$. Definice nám nabízí zápis kongruence (uprostřed) na dělitelnost (nahore), o které jsme již mnohé dokázali, takže se s ní dá v důkazech manipulovat. Nevýhody jsou, že každá taková manipulace musí být podepřena odkazem na konkrétní tvrzení a že dělitelnost nabízí v pravidlech menší flexibilitu než algebra. Jsou ale tvrzení, u kterých je v důkazu jazyk dělitelnosti velmi efektivní.

Přepis do tvaru algebraické rovnosti (dole) nabízí vysokou flexibilitu, takže se důkazy o kongruenci technicky velmi podobají důkazům o dělitelnosti a obvykle tento přístup preferujeme.

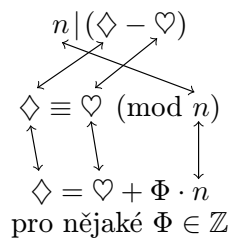
Jako obvykle je při přecházení mezi formulacemi nutno dodržovat formální strukturu, takže například od výrazu $a = b + 3n + 5n$ je ještě nutno přejít k $a = b + 8n$, než máme právo (po stejně tak povinné poznámce, že $8 \in \mathbb{Z}$) přejít ke kongruenci.

V této souvislosti poznamenejme, že někteří autoři v definici kongruence používají podmínku $n \mid (b - a)$. To znamená, že se v takové alternativní teorii v našem schématu výše v druhém a třetím vzorci prohodí pozice \diamond a \heartsuit . To se pak následně se stane i ve všech důkazech, ale samotná tvrzení a výsledky se nemění. Volba pořadí a, b v definici je tedy jen technická a záleží na vkusu autora. Ostatně jedna z verzí tohoto textu to také měla naopak, než se autor v této verzi rozhodl to přecvaknout zpět. Podstatné není pořadí, ale konzistence. Jakmile se jednou jedno pořadí zvolí, tak je třeba se jej důsledně držet.

Pohled na kongruenci přes zbytky bývá v náročnějších situacích nepraktický, takže se v důkazech a odvozeních příliš nepoužívá. Nicméně v jednodušších situacích někdy poslouží výborně, což hned uvidíme.

\triangle

V praxi pomocí kongruence často nahrazujeme velká čísla menšími, třeba $127 \equiv 7 \pmod{10}$. Charakterizaci $127 = 7 + k \cdot 10$ je pak zajímavé vidět jako vzorec pro nové číslo: $7 = 127 - k \cdot 10$. Stejný přístup k nalézání nového čísla posuny o velikosti n jsme již viděli v kapitole 1a při počítání zbytku po dělení. K tomu se od daného čísla a dostaneme stejnými posuny $a - kn$, jakými potvrzujeme kongruenci, takže každé číslo je kongruentní se svým zbytkem po dělení modulem n . Naopak pokud pomocí kongruence doskáceme na vhodné místo, dostaneme zbytek po dělení.



! Fakt 2a.2.

Nechť $n \in \mathbb{N}$, uvažujme $a \in \mathbb{Z}$.

(i) Jestliže $r = a \bmod n$, tedy r je zbytek po dělení a číslem n , pak $a \equiv r \pmod{n}$.

(ii) Jestliže $a \equiv r \pmod{n}$ a $0 \leq r < n$, pak $r = a \bmod n$.

Potkávají se nám tady dva významy symbolu mod. Tvrzení (i) lze vystihnout vzorcem

$$a \equiv a \pmod{n} \quad (\text{mod } n).$$

S Rozbor: Vlastnost $a \equiv r \pmod{n}$ má algebraický přepis $a = r + kn$, $k \in \mathbb{Z}$.

Číslo $r = a \pmod{n}$ má splňovat $a = qn + r$ pro $q \in \mathbb{Z}$ a $0 \leq r < n$.

Porovnáním vidíme, že přejít od jednoho k druhému by mělo být snadné.

Důkaz (rutinní): Dáno $n \in \mathbb{N}$, $a \in \mathbb{N}$.

(i): Uvažujme zbytek $r = a \pmod{n}$. Podle definice existuje $q \in \mathbb{Z}$ tak, aby $a = qn + r$. To přepíšeme jako $a = r + qn$ a díky $q \in \mathbb{Z}$ a větě 2a.1 máme $a \equiv r \pmod{n}$.

(ii): Opačný směr necháme čtenáři jako cvičení 2a.5. □

! Příklad 2a.c: Uvažujme případ $n = 2$. Pro $a = 1$ máme $1 \pmod{2} = 1$, podle věty 2a.1 je tedy kongruentní se všemi celými čísly, které mají také zbytek po dělení dvojkou rovný jedné, což jsou lichá čísla. Tato skupina zahrnuje i jedničku samotnou. Ovšem shodnost zbytků je vlastnost přirozeně symetrická, takže všechna lichá čísla jsou naopak kongruentní s jedničkou. Protože mají všechny stejný zbytek, jsou vlastně kongruentní všechna mezi sebou.

Množině všech čísel kongruentní modulo n s daným a se říká „zbytková třída“ a značí se $[a]_n$. Právě jsme zjistili, že $[1]_2$ je množina všech lichých čísel. Podle charakterizace (ii) bychom ke všem měli být schopni doskákat skoky o velikosti 2, což souhlasí, stejnými skoky umíme doskákat mezi prvky této třídy navzájem. To ostatně není překvapení, množina lichých čísel se tradičně zapisuje

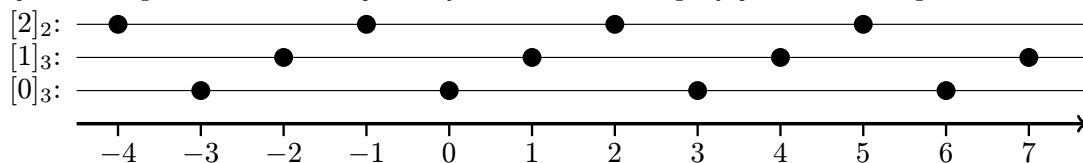
$$[1]_2 = \{1 + 2k; k \in \mathbb{Z}\}.$$

Pokud bychom nezačali jedničkou ale jiným lichým číslem, tak má také zbytek po dělení dvěma rovný jedné a je tedy zase kongruentní se všemi lichými čísly. Jinak řečeno, jeho zbytková třída (skupina kongruence) bude souhlasit s tou $[1]_2$. Můžeme tedy volit zástupce třídy dle libosti, třeba $[13]_2 = [1]_2$. To, že se prvky jedné kongruentní skupiny (zbytkové třídy) mohou vzájemně zastupovat, je jedním z klíčových témat této kapitoly.

Obdobně nahlédneme, že číslo 0 (nebo třeba 14) je kongruentní se všemi sudými čísly, a dostáváme druhou skupinu vytvořenou kongruencí, jmenovitě zbytkovou třídu $[0]_2$. Množina celých čísel se tak rozpadla na dvě podmnožiny. Ty jsou navzájem disjunktní. Aby totiž nějaké číslo leželo v obou, tak by muselo mít dva různé zbytky po dělení, což nejde.

Stejně úvahy samozřejmě platí i pro jiná $n \in \mathbb{N}$. Jakmile se rozhodneme vnímat \mathbb{Z} pohledem kongruence s jistým zvoleným modulem n , tak se celá čísla rozdělí do skupin podle zbytků. V každé skupině (zbytkové třídě) budou čísla se stejným zbytkem po dělení, tedy navzájem kongruentní, což znamená, že se liší posuny o n . Množiny tedy mají pravidelnou strukturu (korálky pravidelně rozmístěné na celočíselné ose) a konkrétní skupinu tak snadno vytvoříme z jednoho libovolného zástupce posuny o n . Jednotlivé množiny jsou navzájem disjunktní a je jich přesně n , protože tolik je možných zbytků při dělení číslem n .

Vzniká tak specifický rozklad množiny \mathbb{Z} , což je pojem, který jsme představili v sekci 1b po poznámce 1b.2. Obrázek ukazuje situaci pro $n = 3$. Vlevo jsme vybrali z každé skupiny jednoho zástupce.



△

V této sekci se zbytkovými třídami pracovat nebudeme, jen se občas budeme chtít odvolat na skupiny vytvořené kongruencí a je namístě použít správný název, když už existuje. Shrňme poznatky, které jsme v příkladě poznali.

! 2a.3 Poznámka: Uvažujme zvolený modul $n \in \mathbb{N}$. Množině $[a]_n$ všech celých čísel kongruentních s daným číslem $a \in \mathbb{Z}$ se říká zbytková třída. Platí následující:

- $[a]_n = \{a + kn; k \in \mathbb{Z}\}$.
- Pokud $a \equiv b \pmod{n}$, tak $[a]_n = [b]_n$.
- Pokud $b \in [a]_n$, tak $[a]_n = [b]_n$.
- Pro $a, b \in \mathbb{Z}$ je buď $[a]_n = [b]_n$ nebo $[a]_n \cap [b]_n = \emptyset$.
- $\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} [a]_n$.

Tyto vlastnosti se snadno dokážou pomocí charakterizace přes zbytky, viz také fakt 2c.1. Zároveň vyplývají z obecnějších principů, které potkáme v kapitole 5.

Je dobré mít na paměti, že jedna třída je speciální, jmenovitě $[0]_n = \{kn; k \in \mathbb{Z}\}$. Jinak řečeno, ve světě kongruence modulo n je samotné n (a také jeho násobky) vlastně nula (viz cvičení 2a.6).

Je také jeden speciální modul. V celých číslech modulo $n = 1$ je jen jedna zbytková třída, všechna čísla jsou navzájem kongruentní a vlastně jsou to všechno nuly. To je velmi exotický svět a občas jsou tam věci trochu jinak, na druhou stranu celá teorie je validní. Proto není zvykem hodnotu $n = 1$ zakazovat, ale v praxi se nepoužívá.

Zvídavého čtenáře napadne, zda lze modulo zavést také pro $n = 0$. Mohli bychom, ale je to trochu naopak než s $n = 1$. Museli bychom být ve střehu při budování teorie, ale výsledný svět by vůbec nebyl exotický, právě naopak. Každé celé číslo by modulo 0 bylo kongruentní jen se sebou samým, čili \mathbb{Z} modulo 0 by zase bylo \mathbb{Z} . Standardně tedy při budování teorie případ $n = 0$ nestojí za zahrnutí.

△

Představa zbytkové třídy coby pravidelně rozmístěných čísel vede na pozorování, které je snadné, ale zaslouží si vypíchnout, protože je občas užitečné.

Fakt 2a.4.

Nechť $n \in \mathbb{N}$, uvažujme $a, b \in \mathbb{Z}$. Jestliže $a \equiv b \pmod{n}$ a $|a - b| < n$, pak $a = b$.

Důkaz je snadný, když si předpoklad přepíšeme do řeči algebry a spojíme. Využijeme toho, že nerovnost aplikovaná na celá čísla má někdy specifické dopady, což je užitečné pozorování.

Důkaz (poučný): Dány $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Předpokládáme $|a - b| < n$ a $a \equiv b \pmod{n}$, což si přepíšeme jako $a = b + kn$, $k \in \mathbb{Z}$ neboli $a - b = kn$. To znamená, že $|kn| < n$, díky $n > 0$ je možné jej vytknout z absolutní hodnoty a pak zkrátit. Dostaneme $|k| < 1$, což pro celé číslo znamená $k = 0$ a tedy $a = b$. □

V předchozích úvahách jsme narazili na některé vlastnosti kongruence, které si zaslouží vyslovit. Jde totiž o stejné vlastnosti, které má běžná rovnost a které jsou klíčové pro její praktické používání, takže mají i speciální názvy (viz kapitola 4 o relacích).

! Věta 2a.5.

Nechť $n \in \mathbb{N}$. Pak platí:

(i) Pro každé $a \in \mathbb{Z}$ je $a \equiv a \pmod{n}$.

(ii) Pro každé $a, b \in \mathbb{Z}$ platí, že $a \equiv b \pmod{n}$ je ekvivalentní s $b \equiv a \pmod{n}$.

(iii) Pro každé $a, b, c \in \mathbb{Z}$ platí, že jestliže $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, pak také $a \equiv c \pmod{n}$.

S Rozbor: Každou ze tří částí dokážeme pomocí jedné z charakterizací kongruence. Podle definice dokážeme část (iii). Tam je následující situace:

- Máme: n dělí $a - b$
- Chceme: n dělí $a - c$
- n dělí $b - c$

Přechod zleva doprava je snadný, pokud si připomeneme vlastnosti dělitelnosti.

Pomocí rovností dokážeme tvrzení (ii). Tam máme následující situaci:

- Máme: $a = b + kn$, kde $k \in \mathbb{Z}$
- Chceme: $b = a + \Phi n$ pro nějaké $\Phi \in \mathbb{Z}$.

Upravit levou rovnost na pravou je snadné.

Tvrzení (i) není implikace, takže nemáme přirozený začátek odvození. Víme jen, k čemu chceme dojít, pomocí třetí charakterizace potřebujeme následující:

- Máme: ?
- Chceme: $a \bmod n = a \bmod n$.

Klíčem k úspěchu je uvědomit si, že se nepotřebujeme zabývat tím, co vlastně vzorec $a \bmod n$ dělá, podstatné je, že jeho výsledkem je konkrétní číslo.

Poznamenejme, že všechna tři tvrzení lze dokázat stejně snadno všemi třemi přístupy a je to dobrý nácvik, viz cvičení 2a.7.

Důkaz (rutinní, poučný): Dány $n \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$.

(i): Každé číslo je rovno samo sobě, platí to tedy i pro zbytek po dělení $a \bmod n$. Takže $a \bmod n = a \bmod n$, což podle věty 2a.1 znamená $a \equiv a \pmod{n}$.

(ii): Jestliže $a \equiv b \pmod{n}$, pak podle věty 2a.1 máme $a = b + kn$ pro nějaké $k \in \mathbb{Z}$. Odtud $b = a - kn$ neboli $b = a + (-k)n$ a $(-k) \in \mathbb{Z}$, tedy podle stejné věty $b \equiv a \pmod{n}$.

(iii): Jestliže $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, pak podle definice n dělí $a - b$ a také $b - c$. Podle faktu 1a.17 pak n dělí také číslo $(a - b) + (b - c) = a - c$ a tedy $a \equiv c \pmod{n}$. \square

M Poznámka: V poznámce po větě 2a.1 jsme upozornili na nutnost dodržovat schémata. Ve vzorci $\diamond = \heartsuit + \Phi \cdot n$ je důležité splnit části, které nejsou proměnné. Jde o pravou stranu, kde je znaménko plus a přítomnost modulu n v posunovém členu. To bylo důležité v důkazu výše. Když jsme se dostali k rovnosti $b = a - kn$, tak jsme ještě neměli právo přejít k závěru $b \equiv a \pmod{n}$, protože tato rovnost nemá správnou strukturu. Teprve ve tvaru $b = a + (-k)n$ splňuje požadavky.

S tím souvisí další důležitá poznámka. Začátečníci v situaci, kdy mají $b = a + (-k)n$, občas zapomenou udělat poznámku, že $(-k) \in \mathbb{Z}$. O její nutnosti jsme psali již v kapitole 1a. U kongruence se objevuje další začátečnická chyba, kdy se udělá poznámka $(-k)n \in \mathbb{Z}$. To ale není něco, co by nás zajímalo. Smyslem vzorce je ukázat, že se dá povoleným způsobem dojít od a k b . Na potvrzení potřebujeme vědět, kolik jsme udělali kroků velikosti n , a to najdeme právě v podobě $-k$, bez zahrnutí n .

\triangle

Tvrzení (i) nám říká, že například $15 \equiv 15 \pmod{7}$, ale ve skutečnosti je v něm schováno mnohem více. Vztahuje se také na situace, kdy neporovnáváme konkrétní číslo se sebou, ale dva na pohled různé vzorce, o kterých nicméně víme, že dávají totéž. Pak nám tvrzení zaručuje, že jsou i spolu kongruentní. Toto užitečné pozorování potvrdíme formálně.

Fakt 2a.6.

Nechť $n \in \mathbb{N}$, $x, y \in \mathbb{Z}$. Jestliže $x = y$, tak $x \equiv y \pmod{n}$.

Kongruence je tedy rozšířením rovnosti, jakousi její benevolentnější verzí.

S Rozbor: Rozmyslíme si situaci, závěr s kongruencí přepíšeme na odpovídající rovnost.

- Máme: $x = y$
- Chceme: $x = y + \Phi n$
pro nějaké $\Phi \in \mathbb{Z}$

Čtenář by měl vidět, jak se dostat k cíli, důkaz tedy necháme jako cvičení 2a.8.

\triangle

Vlastnosti z věty 2a.5 nám pomohou podepřít následující důležité pozorování.

Podobně jako rovnítko, také kongruenci v praxi používáme více způsoby. Zápis $a \equiv b$ lze vnímat jako potvrzení, že dvě čísla patří do stejné kongruentní skupiny, ale také jako vyjádření situace, že bylo dáno číslo a a my jsme se jej rozhodli nahradit kongruentním zástupcem b (například zbytkem po dělení).

Toto nahrazování provádíme zejména ve výpočtech, abychom si je zjednodušili. Počítání ve světě modulu je hlavním tématem této kapitoly a musíme začít tím, že se rozhodneme, jak vlastně budeme ve světě modulu počítat. Samozřejmě chceme, aby výpočty dávaly smysl, ale také vyžadujeme, aby se při výpočtech dala čísla zaměňovat v rámci kongruentních skupin, aniž by to ovlivnilo výsledek, který ovšem také chápeme očima kongruence.

Čtenář už něco podobného zná. Zlomky $\frac{1}{2}$ a $\frac{2}{4}$ jsou formálně různé, ale oba zastupují hodnotu 0.5 a jsou tedy ve výpočtech zaměnitelné. Pokud k oběma přičteme $\frac{1}{3}$, tak společný jmenovatel poskytne dva formálně různé výsledky:

$$\frac{1}{2} + \frac{1}{3} = \frac{5}{6}, \quad \frac{2}{4} + \frac{1}{3} = \frac{10}{12}.$$

Ty ale zase zastupují stejnou hodnotu, takže oba výpočty vlastně daly stejný výsledek. V praxi nám to umožňuje přejít od zadaných čísel k příjemnějším, například takto:

$$\frac{2}{4} + \frac{13}{39} = \frac{1}{2} + \frac{1}{3} = \frac{5}{6}.$$

Je užitečné si všimnout, že rovnosti v tomto zápisu vnímáme nikoliv symetricky, ale jako přechod od čísla vlevo k číslu vpravo, jak jsme diskutovali výše.

Obdobné chování očekáváme od počítání, které zavedeme ve světě modulu. Přirozeným nápadem je vypůjčit si potřebné operace ze světa celých čísel. Vyzkoušíme to.

! Příklad 2a.d: Uvažujme celá čísla modulu $n = 10$. Mějme čísla $a = 3$, $b = 8$. Můžeme je sečíst pomocí standardního sčítání: $3 + 8 = 11$. Co se stane, když se tato čísla rozhodneme nahradit jinými zástupci z příslušných zbytkových tříd?

Máme například $3 \equiv 23 \pmod{10}$ a $8 \equiv -2 \pmod{10}$, takže namísto a, b budeme pracovat s čísly $u = 23$ a $v = -2$. Sečtením dostaneme $23 + (-2) = 21$. To je výsledek odlišný od předchozího výsledku 11, jenže ve světě modulu 10 dávají oba stejnou informaci, protože $21 \equiv 11 \pmod{10}$. Jde tedy vlastně o stejný výsledek a záměna

vstupních čísel neovlivnila výsledek sčítání. Kdybychom chtěli, můžeme tento výsledek nahradit ještě jiným, který nám bude třeba sympatičtější. Postup můžeme zapsat například takto:

$$3 + 8 \equiv 23 + (-2) = 21 \equiv 1 \pmod{10}.$$

Všimněte si, že při výpočtu pečlivě rozlišujeme mezi nahrazením pomocí kongruence (značeno \equiv) a standardní algebrou vypůjčenou od celých čísel (značeno $=$). Víme, že kongruence závisí na zvoleném modulu n . Čtenář by měl tedy vědět, s jakým modulem ty kongruence ve výpočtu pracují. Protože se modul v průběhu výpočtu zásadně nemění, nemusíme to psát u všech kongruencí, stačí to poznamenat na závěr výpočtu (což je standardní a budeme to vyžadovat).

Jako obvykle při zřetěženém výpočtu je jeho význam dán začátkem a koncem, takže jsme výpočtem zjistili, že $3 + 8 \equiv 1 \pmod{10}$ (viz poznámka 1a.10). Formálně to vyplývá z toho, že lze díky faktu 2a.6 výpočet přepsat jako

$$3 + 8 \equiv 23 + (-2) \equiv 21 \equiv 1 \pmod{10},$$

a vlastnosti (iii) ve větě 2a.5.

Podobně nám bude nahrazování fungovat i pro násobení.

$$3 \cdot 8 = 24, \quad 3 \cdot 8 \equiv 23 \cdot (-2) = -46 \equiv 24 \pmod{10}.$$

△

To samozřejmě mohla být náhoda, proto potvrdíme, že nahrazování ve sčítání a násobení opravdu funguje. V zásadě by to mělo stačit, protože víc operací vlastně nepotřebujeme. Například bez odečítání se obejdeme, protože se dá vnímat jako zápis pro přičtení opačného čísla: $a - b = a + (-b)$. Z pohledu teorie jde o preferovaný přístup, protože odčítání nesplňuje některé klíčové vlastnosti (například asociativitu, viz bonusová kapitola 19).

Na druhou stranu je v praxi pohodlné s odčítáním pracovat a zastupování pro něj funguje, takže jej také zahrneme.

! Věta 2a.7.

Nechť $n \in \mathbb{N}$, uvažujme $a, b, u, v \in \mathbb{Z}$ takové, že $a \equiv u \pmod{n}$ a $b \equiv v \pmod{n}$. Pak platí následující:

- (i) $a + b \equiv u + v \pmod{n}$;
- (ii) $a - b \equiv u - v \pmod{n}$;
- (iii) $ab \equiv uv \pmod{n}$.

S Rozbor: Větu lze interpretovat jako tři implikace, například tuto:

$$[a \equiv u \pmod{n} \wedge b \equiv v \pmod{n}] \implies a + b \equiv u + v \pmod{n}.$$

Nalevo vidíme předpoklady, napravo závěr, ke kterému se musíme dostat. Obvykle se doporučuje přejít k jednodušším pojmům, v tomto případě můžeme zkusit definici a dostáváme následující situaci:

- Máme: n dělí $a - u$
 n dělí $b - v$
- Chceme: n dělí $(a + b) - (u + v)$.

Je potřeba najít můstek vedoucí od poznatků nalevo k tomu napravo. Někomu může přijít jednodušší pracovat s rovnostmi než s pojmem dělitelnosti. Pomocí věty 2a.1 lze naši situaci přepsat takto:

- Máme: $a = u + k \cdot n$ pro nějaké $k \in \mathbb{Z}$
 $b = v + l \cdot n$ pro nějaké $l \in \mathbb{Z}$
- Chceme: $a + b = u + v + \Phi \cdot n$
pro nějaké $\Phi \in \mathbb{Z}$

Při pokusu o přímé odvození závěru bychom si teď položili otázku, jak z rovností nalevo dostat rovnost typu napravo. Při typu důkazu „závěr jako cesta“ (poznámka 1a.18) bychom si položili otázku, co na základě toho vlevo dokážeme říct o čísle $a + b$, přičemž bychom nakonec rádi napravo vytvořili $u + v$ a k tomu přičtené n násobené nějakým číslem.

Podobnou analýzu je možné provést pro další dvě tvrzení. Jeden důkaz ukážeme a ostatní dva (snažší) přepustíme čtenáři.

Důkaz (poučný): Dány $n \in \mathbb{N}$, $a, b, u, v \in \mathbb{Z}$. Předpoklad: $a \equiv u \pmod{n}$ a $b \equiv v \pmod{n}$. Podle věty 2a.1 pak platí $a = u + kn$ a $b = v + ln$ pro nějaká $k, l \in \mathbb{Z}$.

(iii): Pomocí rovností spočítáme $ab = (u + kn)(v + ln) = uv + uln + vkn + kln^2 = uv + (ul + vk + kln)n$, kde $(ul + vk + kln) \in \mathbb{Z}$. Proto podle věty 2a.1 máme $ab \equiv uv \pmod{n}$.

Důkazy (i) a (ii) jsou obdobné, viz cvičení 2a.9.

□

Teď už tedy můžeme s jistotou ve výpočtech nahrazovat, zatím ovšem jen v jednotlivých operacích. U složitějších výrazů by se nahrazování muselo dělat krok za krokem shlukováním pomocí závorek, což je zdouhavé. Proto si toto tvrzení zobecníme na komplikovanější výrazy, pak budeme moci nahrazovat hromadně.

Zobecnování pravidel ze dvou na více objektů se standardně dělá matematickou indukcí. Zatím jsme ji oficiálně neprobrali (čeká v kapitole 7), ale mnozí čtenáři ji znají a v tomto důkazu je použita dosti transparentním způsobem, takže by to nemělo vadit.

Důsledek 2a.8.

Nechť $n \in \mathbb{Z}$.

(i) Uvažujme $a_1, u_1, \dots, a_m, u_m \in \mathbb{Z}$ takové, že $a_i \equiv u_i \pmod{n}$ pro všechna $i = 1, \dots, m$.

Pak $\sum_{i=1}^m a_i \equiv \sum_{i=1}^m u_i \pmod{n}$ a $\prod_{i=1}^m a_i \equiv \prod_{i=1}^m u_i \pmod{n}$.

(ii) Uvažujme $a_1, b_1, u_1, v_1, \dots, a_m, b_m, u_m, v_m \in \mathbb{Z}$ takové, že $a_i \equiv u_i \pmod{n}$

a $b_i \equiv v_i \pmod{n}$ pro všechna $i = 1, \dots, m$. Pak $\sum_{i=1}^m a_i b_i \equiv \sum_{i=1}^m u_i v_i \pmod{n}$.

Důkaz (rutinní): (i): Dokážeme to indukcí na m pro sčítání, násobení necháme jako cvičení 2a.11.

(0) $m = 1$: Předpoklad $a_1 \equiv b_1 \pmod{n}$ je zároveň závěrem, tedy implikace platí.

(1) Předpokládejme, že sčítací vzorec platí pro nějaké $m \in \mathbb{N}$ a všechna $a_1 \equiv u_1, \dots, a_m \equiv u_m$. Mějme čísla $a_1, u_1, \dots, a_{m+1}, u_{m+1}$ splňující $a_i \equiv u_i \pmod{n}$ pro všechna i . Podle indukčního předpokladu pak máme

$\sum_{i=1}^m a_i \equiv \sum_{i=1}^m u_i \pmod{n}$, proto podle věty 2a.7 (i) také $\left(\sum_{i=1}^m a_i\right) + a_{m+1} \equiv \left(\sum_{i=1}^m u_i\right) + u_{m+1} \pmod{n}$ neboli

$\sum_{i=1}^{m+1} a_i \equiv \sum_{i=1}^{m+1} u_i \pmod{n}$, důkaz je hotov.

(ii): Podle věty 2a.7 (iii) platí $a_i b_i \equiv u_i v_i \pmod{n}$ pro všechna i , na tato čísla pak aplikujeme část (i) a sečteme je.

□

Lze dokázat i komplikovanější věty, v praxi lze čísla nahrazovat kongruentními zástupci v prakticky každém výrazu poskládaném z násobení, sčítání a odčítání a závorek.

Příklad 2a.e: Uvažujme výraz $195302 \cdot 16293 + 32532675$ ve světě modulu 100. Čísla můžeme nahradit jejich jinými zástupci modulu 100, třeba zbytky po dělení, viz fakt 2a.2, a počítat

$$195302 \cdot 16293 + 32532675 \equiv 2 \cdot 93 + 75 = 186 + 75 = 261 \equiv 61 \pmod{100}.$$

Výsledek 261 jsme mohli nechat, jako bonus jsme přechodem k ideálnímu zástupci díky faktu 2a.2 (ii) zjistili, že $(195302 \cdot 16293 + 32532675) \bmod 100 = 61$. Mohli jsme ovšem také jako výsledek dát libovolného jiného zástupce, třeba 1361.

Počítáči je to jedno, ale při ručním výpočtu je dobré mít na paměti také možnost záporných zbytků.

$$195302 \cdot 16293 + 32532675 \equiv 2 \cdot (-7) + 75 = 75 - 14 = 61 \pmod{100}.$$

Ve výpočtech opět značíme odlišně přechod kongruencí a přechod algebrou. V praxi lidé často píšou všude rovnítko, ale v učebnici bychom to flákat neměli.

Zajímavá finta je psát všude kongruence, je to totiž formálně správně, viz fakt 2a.6.

△

Čtvrtou algebraickou operací je dělení. To v oboru celých čísel můžeme používat jen občas, například $6 \div 2 = 3$, zatímco $6 \div 5$ se nepovede, s tím jsme smířeni. Bohužel si jej nemůžeme přímo vypůjčit do světa modulu jako ostatní operace.

! Příklad 2a.f: Potřebujeme vydělit $20 \div 5$ ve světě modulu $n = 10$. Návštěva ve světě reálných čísel naznačí, že 4 by mohl být rozumný výsledek. Teď zkusíme zúčastěná čísla nahradit kongruentními zástupci. Když ovšem posuneme dvacítku jednou o deset, dostaneme $30 \div 5 = 6$, a když teď zkusíme posunout pětku, dostaneme pro změnu $30 \div 15 = 2$. Protože ve světě modulu $n = 10$ nejsou výsledky 4, 6, 2 shodné (nejsou to čísla kongruentní mod 10), vidíme, že takovéto naivní dělení nedělá to, co od něj potřebujeme. Nemluvě o problému, že jiná volba zástupců promění úlohu $20 \div 5$ v úlohu $20 \div 15$, se kterou si v celých číslech neporadíme.

Mimočodem, ve světě modulu $n = 10$ jsou čísla 20 a 30 vlastně nuly, takže by výsledkem dělení měla být nula.

△

Budeme tedy muset dělení realizovat jinak. Necháme se inspirovat algebrou, protože ta se obejde i bez dělení podobně, jako se obejde bez odčítání. Ve skutečnosti je zápis $a \div d$ možno chápat jako pohodlnou zkratku pro výpočet $a \cdot \frac{1}{d} = a \cdot d^{-1}$. Například ve světě reálných čísel máme $6 \div 3 = 6 \cdot 3^{-1} = 2$. Pokud tedy potřebujeme nějakou kvantitu a vydělit číslem d , tak místo toho najdeme d^{-1} , tedy inverzní číslo k d , a tím vynásobíme.

My to teď napodobíme ve světě modulo. Nejprve se musíme zamyslet, co tím vlastně myslíme, když ve světě reálných (nebo třeba racionálních) čísel napíšeme d^{-1} . Je to jakési číslo, kvantita x , která má vlastnost, že $d \cdot x = 1$. To je něco, co se dá přenést také do světa modulo. Vyzkoušíme to.

Příklad 2a.g: Uvažujme příklad $6 \div 2$ ve světě modulo $n = 7$, myslíme si, že 3 by byla vhodná odpověď. Najdeme magické číslo x , které zastupuje inverzní číslo 2^{-1} neboli zlomek $\frac{1}{2}$, tedy splňuje $2x = 1$ ve světě modulo 7. Přesně řečeno, požadujeme $2x \equiv 1 \pmod{7}$.

Toto číslo najdeme zkusmo. Stačí otestovat například čísla 0 až 6, protože ostatní jsou s nimi kongruentní a proto podle věty 2a.7 dají ve výrazu $2x$ shodné výsledky. Zjistíme, že $2 \cdot 4 \equiv 1 \pmod{7}$. To znamená, že číslo $x = 4$ má ve světě modulo 7 stejnou funkci jako zlomek $\frac{1}{2}$ neboli 2^{-1} v \mathbb{R} . Ověříme:

$$6 \div 2 = 6 \cdot 4 = 24 \equiv 3 \pmod{7}.$$

To dává smysl. Stejný výsledek bychom dostali, pokud bychom místo $x = 4$ použili jiné s ním kongruentní číslo, třeba $x = -3$:

$$6 \div 2 = 6 \cdot (-3) = -18 \equiv 3 \pmod{7}.$$

Nás ale hlavně zajímá, zda s tímto přístupem k dělení funguje zaměnitelnost přímo ve vstupních datech. Zkusíme namísto $6 \div 2$ spočítat $13 \div 9$.

Na to potřebujeme y nahrazující číslo 9^{-1} ve světě modulo 7, tedy hledáme y splňující $9y \equiv 1 \pmod{7}$. Ovšem podle nahrazovací věty je $9y$ totéž co $2y$ a my už víme, že $2 \cdot 4 \equiv 1 \pmod{7}$, takže čtyřka bude fungovat i pro devítku. Vidíme, že jednou nalezené speciální číslo poslouží i pro kongruentního blízence. Proto počítáme

$$13 \div 9 = 13 \cdot 4 = 52 \equiv 3 \pmod{7},$$

tedy dostali jsme správný výsledek. Vidíme, že pokud definujeme dělení přes násobení, tak pro něj platí nahraditelnost (tedy, zatím to fungovalo jednou, obecně to ještě musíme ukázat).

Kongruence čísel platí či neplatí v závislosti na zvoleném modulu a platí to i pro to speciální číslo x . Zjistili jsme, že pro $d = 2$ máme ve světě modulo 7 číslo $x = 4$. Snadno ovšem ověříme, že ve světě modulo $n = 5$ už čtyřka nefunguje, protože $2 \cdot 4 \equiv 3 \not\equiv 1 \pmod{5}$. Zkusmo zjistíme, že tam funguje $x = 3$.

Ve světě modulo $n = 6$ pak budeme řešení úlohy $2x \equiv 1 \pmod{6}$ hledat marně. Muselo by totiž platit $2x = 1 + 6k$ pro nějaké $x, k \in \mathbb{Z}$, což lze přepsat na $2(x - 3k) = 1$. Protože je vlevo číslo sudé a vpravo číslo liché, toto se nikdy nepovede. To znamená, že ve světě modulo 6 prostě dělit dvojkou nejde. I to se stává.

△

Nyní tento nápad zavedeme oficiálně.

!

Definice.

Uvažujme $n \in \mathbb{N}$.

Nechť $d \in \mathbb{Z}$. Řekneme, že $x \in \mathbb{Z}$ je **inverzní číslo (inverse number) k d modulo n** , jestliže $d \cdot x \equiv 1 \pmod{n}$.

Z našeho experimentu už víme, že 4 i -3 jsou inverzní čísla k dvojce modulo 7, vlastně je jich nekonečně mnoho. V definici jsme pro inverzní číslo nezavedli značení. Není to zvykem; jedním důvodem může být právě to, že toto číslo není jediné, což by komplikovalo používání takového značení ve výpočtech. Když totiž napíšeme třeba značku π nebo $\sqrt{9}$, tak očekáváme, že to bude jedna hodnota, ne že budeme mít na výběr z více možností.

Náš speciální přístup k dělení je rozumný, protože dává očekávaný výsledek v případech, kdy lze v rámci celých čísel použít běžné dělení.

Fakt 2a.9.

Nechť $n \in \mathbb{N}$, $a, d \in \mathbb{Z}$, $d \neq 0$. Předpokládejme, že $d \mid a$ a tedy má smysl počítat $\frac{a}{d}$ v oboru celých čísel. Nechť x je inverzní číslo k d modulo n . Pak $\frac{a}{d} \equiv ax \pmod{n}$.

S Rozbor: Rozmyslíme si situaci.

• Máme: $d \mid a$, $dx \equiv 1 \pmod{n}$

• Chceme: $\frac{a}{d} \equiv ax \pmod{n}$

Informace přepíšeme do jazyka rovností:

- Máme: $a = dk, k \in \mathbb{Z}$
 $dx = 1 + ln, l \in \mathbb{Z}$
- Chceme: $\frac{a}{d} = ax + \Phi n$
pro nějaké $\Phi \in \mathbb{Z}$

Co lze na základě rovností vlevo říct o $\frac{a}{d}$? Máme $\frac{a}{d} = k$. Abychom mohli použít druhou rovnost, zlomek rozšíříme, tím zároveň v čitateli vznikne správný výraz:

$$\frac{a}{d} = \frac{ax}{dx} = \frac{ax}{1+ln}.$$

Bohužel, toto nelze algebraicky převést na tvar $ax + \Phi n$, takže je to slepá ulička. Tento důkaz není rutinní a vyžaduje inspiraci. Například nás napadne, že bývá užitečné zbavit se zlomků ve výrazech, což pro tu rovnost napravo („chceme“) znamená $a = dax + d\Phi n$. Když druhou rovnost nalevo vynásobíme áčkem, dva členy se budou shodovat, to vypadá nadějně.

Důkaz: Dáno $n \in \mathbb{N}$, $a, d, x \in \mathbb{Z}$, $d \neq 0$. Předpokládáme, že $d \mid a$ a $dx \equiv 1 \pmod{n}$. Pak existují $k, l \in \mathbb{Z}$ takové, že $a = dk$ a $dx = 1 + ln$. Z druhé rovnosti vynásobením číslem a vznikne $a = adx - aln$. Do členu napravo dosadíme $a = dk$ a dostáváme

$$a = adx - dkl n \quad \longrightarrow \quad \frac{a}{d} = ax + (-kl)n.$$

Protože $-kl \in \mathbb{Z}$, platí $\frac{a}{d} \equiv ax \pmod{n}$. □

Přístup přes násobení inverzním číslem nám dokonce umožňuje dělit v případě, že to ve světě celých čísel udělat nelze. Například ve světě modulu 7 můžeme počítat $5 \div 2 = 5 \cdot 4 = 20 \equiv 6 \pmod{7}$. Jaký má smysl tvrdit, že $5 \div 2 = 6$? Výsledkem dělení $\frac{a}{d}$ je podíl q , který má vlastnost, že $qd = a$. Náš podivný výsledek dělení $5 \div 2$ toto splňuje: $6 \cdot 2 = 12 \equiv 5 \pmod{7}$. Platí to také obecně.

Fakt 2a.10.

Nechť $n \in \mathbb{N}$, $a, d \in \mathbb{Z}$, $d \neq 0$. Nechť x je inverzní číslo k d modulo n , označme $q = ax$. Pak $dq \equiv a \pmod{n}$.

S Rozbor: Přejdeme-li od daných pojmů k rovnostem, je naše situace takováto:

- Máme: $dx = 1 + kn, k \in \mathbb{Z}$
 $q = ax$
- Chceme: $dq = a + \Phi n$
pro nějaké $\Phi \in \mathbb{Z}$

Pokud si v tomto případě odpovíme na otázku, co nám vstupní data říkají o výrazu dq , tak se již dostaneme bez nějakých triků k žádanému tvaru. Tento důkaz je tedy přímočarý, ale přece jen je třeba se trochu zamyslet nad správným dosazením.

Důkaz: Dáno $n \in \mathbb{N}$, $a, d, x \in \mathbb{Z}$, $d \neq 0$. Předpokládáme, že $dx \equiv 1 \pmod{n}$. Pak existuje $k \in \mathbb{Z}$ takové, že $dx = 1 + kn$. Označme $q = ax$. Pak

$$dq = dax = a(dx) = a(1 + kn) = a + (ak)n.$$

Protože $ak \in \mathbb{Z}$, platí $dq \equiv a \pmod{n}$. □

Náš speciální přístup k dělení tedy dává rozumné výsledky. Ještě ověříme, že umožňuje pro $a \div d$ zastupitelnost čísel. Protože se používá násobení $a \cdot x$, podle věty 2a.7 lze nahradit číslo a . Zbývá potvrdit totéž o d .

! Fakt 2a.11.

Nechť $n \in \mathbb{N}$, $d \in \mathbb{Z}$. Předpokládejme, že $x \in \mathbb{Z}$ je nějaké inverzní číslo k d modulo n . Jestliže $u \in \mathbb{Z}$ splňuje $d \equiv u \pmod{n}$, pak je x také inverzní číslo k u modulo n .

Důkaz je snadný a necháme jej jako cvičení 2a.12.

Vidíme tedy, že všechna čísla ze zbytkové třídy dané číslem d sdílí svá inverzní čísla, pokud tedy nějaká existují.

Asi nečekáme, že by byla inverzní čísla k nule. V případě $n = 1$ tedy ano, $0 \cdot 0 \equiv 1 \pmod{1}$, ale to je exot, v praxi se používá $n \geq 2$. Pak nelze rovnici $0x \equiv 1 \pmod{n}$ neboli $0 = 1 + kn$, $k \in \mathbb{Z}$ splnit a tedy nelze dělit nulou. Nelze pak dělit ani dalšími čísly s nulou kongruentními, což jsou násobky n . Ovšem jak jsme viděli, inverzní číslo nemusí existovat ani pro čísla, která s nulou kongruentní nejsou, jmenovitě jsme vyloučili existenci inverzního čísla k $d = 2$ modulo $n = 6$. Rádi bychom věděli, pro která čísla jejich inverze existují a pro která ne. Ukáže se, že je na to jednoduché kritérium.

**Věta 2a.12.**Nechť $n \in \mathbb{N}$.Pro $d \in \mathbb{Z}$ existuje inverzní číslo modulo n právě tehdy, když $\gcd(d, n) = 1$.

S Rozbor: Opět máme ekvivalenci a dokazujeme dvě implikace. Směr zleva doprava použije oblíbený postup, který jsme již viděli v kapitole 1b a ani jej nevidíme naposledy.

Opáčným směrem je typickou ukázkou existenčního důkazu. Hledané x opravdu najdeme, a to pomocí informace o $\gcd(d, n)$. Takovou informaci často zpracováváme ve formě Bezoutovy identity a i zde tento přístup zabere.

Důkaz (poučný): Dány $n \in \mathbb{N}$, $d \in \mathbb{Z}$.

1) \implies : Předpokládejme, že existuje $x \in \mathbb{Z}$ takové, že $dx \equiv 1 \pmod{n}$. Pak také existuje $k \in \mathbb{Z}$ takové, že $dx = 1 + kn$ neboli $1 = dx - kn$. Protože $\gcd(d, n)$ dělí čísla d a n , musí podle důsledku 1a.20 také dělit lineární kombinaci těchto čísel napravo v rovnosti a tedy také dělit číslo 1. Podle věty 1a.23 proto $\gcd(d, n) \leq 1$. Protože $n \neq 0$, platí také $\gcd(d, n) \geq 1$ a tedy $\gcd(d, n) = 1$.

2) \impliedby : Předpokládejme, že $\gcd(d, n) = 1$. Pak podle Bezoutovy identity 1b.15 existují čísla $A, B \in \mathbb{Z}$ taková, že $Ad + Bn = 1$ neboli $Ad = 1 + (-B)n$, kde $-B \in \mathbb{Z}$, tedy $Ad \equiv 1 \pmod{n}$. Zvolíme $x = A$ a důkaz je hotov. \square

Důkaz je důležitý, protože zároveň dává návod, jak existující inverzní čísla najít.

Příklad 2a.h: Rádi bychom spočítali $10 \div 5$ ve světě modulo $n = 12$. Protože je pětka nesoudělná s dvanáctkou, má inverzní číslo modulo 12.

Podle důkazu věty hledáme Bezoutovo vyjádření $1 = 5A + 12B$. Lze použít Euklidův algoritmus, nebo uhadneme $1 = 5 \cdot (-7) + 12 \cdot 3$. Přepíšeme to jako $5 \cdot (-7) = 1 + (-3) \cdot 12$, s poznámkou $-3 \in \mathbb{Z}$ nás to opravňuje napsat $5 \cdot (-7) \equiv 1 \pmod{12}$. Máme inverzní číslo $x = -7$ k pětku modulo 12, tedy jakoby $\frac{1}{5}$ nebo 5^{-1} , ale oficiálně jsme to nezavedli. Můžeme počítat

$$10 \div 5 = 10 \cdot (-7) = -70 \equiv 2 \pmod{12}.$$

Výsledek nás nepřekvapil.

Možná by se někomu více líbilo inverzní číslo $x = -7 + 12 = 5$. Číslo 5 je tedy ve světě modulo 12 samo sobě inverzí, což vypadá zvláště, ale není to výjimečné, viz $1^{-1} = 1$. Pro jistotu ověříme: $5 \cdot 5 = 25 \equiv 1 \pmod{12}$.

\triangle

Poznámka: Zatím jsme od rovnosti $a = b + kn$, $k \in \mathbb{Z}$ přecházeli ke kongruenci $a \equiv b \pmod{n}$ pomocí věty 2a.1. Díky poznatkům to teď dokážeme i jinak. Začneme tím, že podle faktu 2a.6 lze rovnost napsat jako kongruenci:

$$a \equiv b + kn \pmod{n}.$$

Ve výpočtu napravo nahradíme n jeho zástupcem nulou. Dostáváme

$$a \equiv b + k \cdot 0 \pmod{n} \implies a \equiv b \pmod{n}.$$

Tento přístup je užitečný při praktickém počítání. Například v příkladu výše se na obdrženu Bezoutovu identitu $1 = 5 \cdot (-7) + 12 \cdot 3$ podíváme očima kongruence modulo 12 a rovnou vidíme $1 \equiv 5 \cdot (-7) + 0$, tedy -7 je hledané číslo. Nemusíme identitu přepisovat do žádaného tvaru.

\triangle

S Algoritmus 2a.13.

pro nalezení inverzního čísla k d modulo n .

0. Jestliže snadno vidíme, že $\gcd(a, n) > 1$, tak inverzní prvek k d modulo n neexistuje.

Jinak například pomocí rozšířeného Euklidova algoritmu najdeme $\gcd(a, n) = Aa + Bn$.

1. Jestliže $\gcd(d, n) > 1$, pak inverzní číslo k d modulo n neexistuje.

2. Jestliže $\gcd(d, n) = 1$, pak A je inverzní číslo k d modulo n .

\triangle

Mimochodem, někdy se dá snadno všimnout, že čísla d, n mají nějakého společného dělitele většího než 1. Pak nic nemusíme počítat a rovnou víme, že inverzní číslo k d modulo n neexistuje. To je třeba případ, kdy jsou n i d sudá čísla.

Pokud inverzní číslo x k danému d existuje, pak díky pravidlu o nahrazování budou inverzními čísla i jeho kongruentní zástupci získaní posuny. Nabízí se otázka, jestli d nemá ještě jiná inverzní čísla, která by nevznikla posunem x . Ukáže se, že ne.

**Věta 2a.14.**

Nechť $n \in \mathbb{N}$. Předpokládejme, že $d, x \in \mathbb{Z}$ a x je inverzní číslo k d modulo n . Pak $y \in \mathbb{Z}$ je inverzní číslo k d modulo n právě tehdy, když $y \equiv x \pmod{n}$.

Důkaz (poučný): Dány $n \in \mathbb{N}$, $d, x, y \in \mathbb{Z}$.

1) \Leftarrow : Nejprve předpokládejme, že $y \equiv x \pmod{n}$. Pak podle věty 2a.7 máme $dy \equiv dx \equiv 1 \pmod{n}$, tedy y je inverzní číslo k d modulo n .

2) \Rightarrow : Nechť jsou $x, y \in \mathbb{Z}$ oba inverzní čísla k d modulo n . Pak existují $k, l \in \mathbb{Z}$ takové, že $dx = 1 + kn$ a $dy = 1 + ln$. Odečtením získáme $dx - dy = kn - ln$, tedy $d(x - y) = (k - l)n$, tedy n dělí $d(x - y)$. Protože d má inverzní číslo modulo n , musí být podle věty 2a.12 tato čísla nesoudělná, tudíž podle Euklidova lemmatu 1b.23 musí n dělit $x - y$, tedy $x \equiv y \pmod{n}$. □

Situace je tedy jasná. Inverzní číslo k danému d buď není žádné, nebo je jich nekonečně mnoho a je to přesně jedna zbytková třída daná nějakým inverzním číslem x . Podíváme se teď na reprezentativnější příklad.

! Příklad 2a.i: Najdeme inverzní číslo k 23 modulo 169.

Pomocí Euklidova algoritmu najdeme Bezoutovu identitu pro čísla $n = 169$ a $d = 23$. Protože vyšlo $\gcd(169, 23) = 1$, inverzní číslo k 23 modulo 169 existuje. U takto pěkných čísel jsme si toho ostatně mohli všimnout rovnou.

Bezoutova identita je $1 = 3 \cdot 169 - 22 \cdot 23$. Můžeme ji formálně přepsat jako $23 \cdot (-22) = 1 + (-3) \cdot 169$, nebo se v souladu s poznámkou výše na tuto rovnost podíváme očima kongruence a díky $169 \equiv 0 \pmod{169}$ hned dostáváme $1 \equiv 23 \cdot (-22) \pmod{169}$. Nalezli jsme inverzní číslo $x = -22$.

a, b	(169)	(23)
169	1	0
23	0	1
8	1	-7
7	-2	15
1	3	-22
0		

Někomu se možná bude více líbit zástupce $-22 + 169 = 147$. Můžete si ověřit (já jsem to udělal), že také $23 \cdot 147 \equiv 1 \pmod{169}$.

Jako úplnou odpověď můžeme uživateli nabídnout informaci, že množina všech inverzních čísel modulo 169 k číslu 23 je $\{147 + 169k; k \in \mathbb{Z}\}$.

Z praktického pohledu je užitečné si všimnout, že pokud v Euklidovské tabulce najdeme jedničku coby $\gcd(d, n)$, tak v dotyčném řádku rovnou najdeme inverzní číslo k d v pomocném sloupci příslušném tomuto vstupu. Můžeme si také všimnout, že pomocný sloupec pro $n = 169$ vlastně vůbec nepotřebujeme. Hledání inverzního čísla se tedy dá oproti tomuto příkladu ještě zestručnit.

△

Některé postupy fungují tak, že když uspějí, tak dají hledaný objekt, ale v případě neúspěchu ještě nevíme, zda daný objekt opravdu neexistuje, nebo existuje, ale daný postup jej neuměl najít. To je v praxi nepříjemné. Hledání inverzního čísla našťstí tuto komplikaci nemá. Pokud v Euklidovské tabulce vyjde jako $\gcd(a, b)$ jednička, tak si inverzní číslo přímo přečteme, v opačném případě máme jistotu, že hledané inverzní číslo neexistuje.

S Algoritmus 2a.15.

pro nalezení inverzního čísla k d modulo n Euklidovým algoritmem.

0. Jestliže snadno vidíme, že $\gcd(a, n) > 1$, tak inverzní prvek k d modulo n neexistuje.

Jinak sestavíme tabulku se dvěma sloupci: Do levého sloupce dáme čísla n a d , do pomocného sloupce dáme čísla 0 a 1. Aplikujeme Euklidův algoritmus.

1. Jestliže $\gcd(d, n) > 1$, pak inverzní číslo k d modulo n neexistuje.

2. Jestliže $\gcd(d, n) = 1$, inverzní číslo x k d modulo n je v pomocném sloupci v řádku s jedničkou nalevo.

Množina všech inverzních čísel k d modulo n je

$$\{x + kn; k \in \mathbb{Z}\}.$$

△

S Poznámka: Algoritmy, zejména ty zefektivněné, mají jednu nevýhodu: Pokud se je naučíme čistě jako postup, tak je snadné (zejména pokud je nepoužíváme často) zapomenout či v paměti zkreslit nějaký klíčový detail. Proto je dobré vědět, na čem jsou založeny, protože souvislosti se v paměti udrží lépe než mechanické postupy. My bychom v příkladě výše mohli prostě mechanicky nasadit algoritmus s jedním pomocným sloupcem a z tabulky vyčíst odpověď.

Měli bychom ale také vědět, že vlastně hledáme číslo x splňující $23x \equiv 1 \pmod{169}$ neboli $23x + 169k = 1$. To by v naší paměti mělo vyvolat souvislost s Bezoutovou identitou a Euklidovým algoritmem. Znalost pozadí je

tedy pojistkou proti zapomenutí a může proto být bezpečnější používat o něco méně efektivní algoritmus, který má ale blíže k souvislostem.

Samozřejmě nejlepší je znát efektivní algoritmus a k tomu rozumět souvislostem.

△

Inverzní čísla modulo splňují běžné vlastnosti, viz cvičení 2a.14.

Podmínka pro existenci inverzních čísel nás přivádí k zajímavému případu: Pokud by modul byl nějaké prvočíslo p , tak jediná čísla, která s p nejsou nesoudělná, jsou jeho násobky, viz fakt 1b.20. Tato čísla jsou ovšem kongruentní s nulou modulo p . To znamená, že ve světě modulo prvočíslo najdeme inverzní čísla ke všem číslům, která nejsou ztotožněná s nulou, což je úplný luxus, vlastně v takovém světě můžeme dělit vším kromě nuly. K tomuto pozorování se dostaneme ještě jednou, v trochu jiném převleku (sekce 2b a 2c), a je to jeden z důvodů, proč lidé pracující ve světě modulo preferují mít jako modul prvočíslo.

2a.16 Poznámka: Když máme v nějakém (matematickém) světě pojem rovnosti, tak můžeme sestavovat a řešit rovnice.

Představme si, že na hodinách hodinová ručička ukazuje na jedničku a nás zajímá, zda existuje nějaký časový interval (v celých hodinách), který když necháme proběhnout pětkrát, tak bude ručička ukazovat na čtyřku. Zapsáno pomocí kongruence, chceme vyřešit rovnici

$$1 + 5x \equiv 4 \pmod{12}.$$

Kdyby to byla normální rovnice, tak bychom neprve odečetli od obou stran jedničku a pak vydělili pěti a dostali $x = (4-1) \div 5$. Zkusíme to ve světě kongruence. Tam se dělení nahrazuje násobením, naštěstí jsme již v příkladě 2a.h pro svět modulo $n = 12$ našli inverzní číslo $x = -7$ k číslu $d = 5$. Můžeme tedy napodobit postup řešení:

$$x = (4 - 1) \div 5 = 3 \cdot (-7) \equiv 3 \pmod{12}.$$

Je opravdu $x = 3$ řešením naší rovnice? Uděláme zkoušku:

$$1 + 5 \cdot 3 = 16 \equiv 4 \pmod{12}.$$

Vidíme, že naše speciální dělení také funguje pro řešení lineárních rovnic.

Vlastně jsme již rovnice ve světě modulo neoficiálně řešili, protože inverzní číslo k d získáme jako řešení rovnice $dx \equiv 1 \pmod{n}$.

Je možné řešit rovnice ve světě kongruence běžnými úpravami? Podívejme se na tvrzení věty 2a.7 a představme si, že zápisy $a \equiv u$ a $b \equiv v$ jsou vlastně rovnosti či rovnice. Věta nám říká, že dvě rovnice ve světě modulo je možné sčítat, odečítat a násobit přesně tak, jak jsme zvyklí ze světa reálných čísel.

Přepíšme první kongruenci jako $x \equiv y$ a druhou pro speciální případ $c \equiv c$ (což platí vždy podle věty 2a.5). Pak nám věta 2a.7 říká následující:

- Jestliže ve světě modulo n máme platnou rovnici $x \equiv y$, pak platí i rovnice $x \pm c \equiv y \pm c$ a $cx \equiv cy$.

Máme tedy také pro svět modulo potvrzena pravidla o rozšiřování rovnic, na která běžně spoléháme. Při bližším pohledu se ovšem ukáže, že tento přístup pomocí úprav rovnice má ve světě modulo určitá zásadní omezení, například pokud potřebujeme dělit a dotyčné číslo nemá k sobě číslo inverzní. Proto v kapitole 3 vyvineme jiný postup řešení rovnic.

Pro zájemce o klasický postup nabízíme cvičení 2a.15, kde přímo potvrdíme známá pravidla pro rozšiřování rovnic a podíváme se i na oblíbená pravidla pro krácení.

△

Ted' ukážeme jednu zajímavou aplikaci.

Příklad 2a.j: Úzký vztah mezi kryptografií a počítáním modulo jde zpět minimálně ke starým Římanům. Takzvanou Césarovu šifru nejlépe představíme takto: Máme dva soustředné kruhy, jeden menší než druhý, a po obvodu napíšeme na oba písmena, vždy stejná proti sobě. Pak jeden kruh otočíme o tři pozice a vzniká tím šifra, kdy namísto A píšeme D , namísto B píšeme E a tak dále, třeba Y přejde na B .

Vytvoříme matematický model. Nahradíme písmena čísly $0, \dots, 25$. Protože jsou na kruhu, vnímáme je cyklicky, tedy pracujeme s čísly modulo 26. Původní šifrování se změní v přiřazování čísel, tedy máme $0 \mapsto 3, 1 \mapsto 4$, a třeba $24 \mapsto 27 \equiv 1$. Tím vlastně vzniká funkce, kterou lze vyjádřit vzorcem $T(m) = (m + 3) \pmod{26}$, tedy výsledek přičtení nahradíme zbytkem po dělení (proměnnou zde tradičně značíme m jako message).

Obecně lze posouvat také o jiné číslo než o tu Césarovu trojku. Zvolíme si nějaké e (tradiční značení z anglického encode) mezi 1 a 25 a dostáváme „šifrování posunem“: $T(m) = (m + e) \pmod{26}$.

Dešifrování probíhá opačným přiřazením, čemuž v matematice odpovídá pojem inverzní funkce. Jestliže šifrovací funkce T šifruje $T(m) = c$ (c jako code), pak inverzní funkce T^{-1} dešifruje $T^{-1}(c) = m$, tedy u Césarovy šifry očekáváme $T^{-1}(3) = 0, T^{-1}(4) = 1$ atd.

Pro šifrování máme vzorec $c = (m + 3) \pmod{26}$, takže snadno usoudíme, že dešifrování probíhá pomocí inverzní funkce $m = (c - 3) \pmod{26}$. Obecně pro šifrování s posunem e máme $T^{-1}(c) = (c - e) \pmod{26}$.

Je ovšem užitečnější používat vzorec stejného typu, tedy přepíšeme to jako $T^{-1}(c) = (m + (-e)) \pmod{26}$. Zde je $-e$ opačné číslo k e , které si označíme tradičním názvem d (jako decoding) a získáme jej například jako $d = -e + 26$.

Máme tedy praktickou situaci, kdy k šifrování i dešifrování používáme stejný vzorec (přístroj), jen měníme nastavení: máme šifrovací konstantu e (vzorec $(a+e) \pmod{26}$) a dešifrovací konstantu d (vzorec $(a+d) \pmod{26}$). Zajímavá volba je $e = 13$, pak také $d = 13$ a $T^{-1} = T$, tedy vysílání i příjem se dějí stejným způsobem.

Jak víme, že dešifrování opravdu probíhá správně? Musíme ukázat, že když na číslo m aplikujeme šifrování a dešifrování, tak se zase vrátíme k m . Matematicky: $T^{-1}(T(m)) = m$. Chceme tedy ukázat, že

$$m = (T(m) + (-e)) \pmod{26} = ((m + e) \pmod{26} + (-e)) \pmod{26}.$$

Nejraději bychom zkrátili e a $-e$, ale v cestě stojí operace zbytku. Obvyklý postup je, že se využije fakt 2a.2, podle jeho části (ii) stačí ukázat, že

$$m \equiv (m + e) \pmod{26} + (-e) \pmod{26}.$$

Při počítání ve světě modulo lze čísla nahrazovat, obvykle se od daného čísla přechází ke zbytku, zde to uděláme naopak a místo $(m + e) \pmod{26}$ použijeme zástupce $m + e$. Dostáváme pak

$$(m + e) \pmod{26} + (-e) \equiv (m + e) + (-e) = m + e - e = m \pmod{26}.$$

Tím je správnost dešifrovací funkce potvrzena.

Tato šifra není příliš bezpečná. Protože se dané písmeno vždy šifruje stejně, je vysoce náchylná na frekvenční analýzu, kdy si prostě spočítáme, který znak se v zašifrované zprávě vyskytuje nejčastěji, a je vysoce pravděpodobné, že odpovídá nejčastějšímu písmenu daného jazyka. Velice pěkně toto popsal E.A. Poe v povídce *Zlatý skarabeus*.

Podobně zranitelný je nápad nahradit posun násobením. Uvažujme číslo e , které je nesoudělné s $n = 26$, a uvažujme šifrování $T(m) = (em) \pmod{26}$. Dá se ukázat, že díky nesoudělnosti je zaručeno, že se různá písmena zobrazí zase na různá písmena, viz důkaz věty 2a.21. Zejména ale víme, že e má inverzní číslo modulo n , označme jej d , které prakticky realizuje dělení číslem e . Dá se tedy očekávat, že dešifrování proběhne pomocí funkce $T^{-1}(c) = (dc) \pmod{26}$. Abychom to potvrdili, opět se zbavíme zbytků ve vzorci

$$T^{-1}(T(m)) = (d[(em) \pmod{26}]) \pmod{26} \equiv d(em) = (ed)m \equiv 1 \cdot m = m \pmod{26}$$

a tedy podle faktu 2a.2 platí $T^{-1}(T(m)) = m$.

Vyzkoušíme to. Zvolme třeba $e = 7$. Pak potřebujeme vyřešit rovnici $7x \equiv 1 \pmod{26}$, buď Euklidovým algoritmem nebo to zkusíme uhádnout. Vyjde například $x = -11$. Tradičně se bere kladný zástupce, zvolíme tedy $d = 15$.

Ted' zašifrujeme písmeno C odpovídající hodnotě $m = 2$, takže vyšleme zprávu $T(2) = (7 \cdot 2) \pmod{26} = 14$ neboli písmeno O . Příjemce na zprávu aplikuje T^{-1} :

$$T^{-1}(14) = (15 \cdot 14) \pmod{26} = 210 \pmod{26} = 2.$$

Dostává C .

V tomto příkladě jsme se podívali na základní principy, které po doplnění nástrojů rozvineme v pořádné šifrování. \triangle

Pravidla světa modulo nám umožňují nahrazovat čísla menšími zástupci. Slovo „menší“ je ovšem velmi relativní. Jak brzy uvidíme, existují aplikace, kde se běžně pracuje s moduly n , které jsou třeba dvěstémístné, ale i významně větší. Podotkněme, že dvěstémístný modul má řádově velikost 10^{200} , zatímco standardní vědecká kalkulačka je omezena na čísla nejvýše řádu 10^{99} a není mi známo, že by to někdy inženýrům přišlo málo. Jinak řečeno, výpočty ve světě modulo mohou být monstrózní.

Naštěstí existují postupy, jak si pomoci v případě, kdy je modul součinem faktorů, které jsou nesoudělné. Pro začátek ukážeme, že se pak dá kongruence testovat „po částech“.

Lemma 2a.17.

Nechť $p, q \in \mathbb{N}$ jsou nesoudělná, označme $n = pq$. Pak pro čísla $a, b \in \mathbb{Z}$ platí, že $a \equiv b \pmod{n}$ právě tehdy, když $a \equiv b \pmod{p}$ a $a \equiv b \pmod{q}$.

S Rozbor: Jde o ekvivalenci, tedy potřebujeme dokázat dva směry. Jeden je velmi snadný, po přechodu od kongruencí k rovnostem máme následující:

- Máme: $a = b + kpq$ pro jisté $k \in \mathbb{Z}$
- Chceme: $a = b + \Phi p$ pro nějaké $\Phi \in \mathbb{Z}$.
- $\gcd(p, q) = 1$
- $a = b + \Xi q$ pro nějaké $\Xi \in \mathbb{Z}$.

Čtenář by měl vidět, jak z rovnosti nalevo vyrobit rovnost napravo, dokonce k tomu ani nepotřebuje předpoklad o nesoudělnosti. Necháme obecnější formulaci jako cvičení 2a.16.

Opačný směr je náročnější. Ze znalosti kongruence vůči p a q potřebujeme získat informaci o kongruenci vzhledem k pq . Jak to uděláme?

Pro kongruenci máme tři ekvivalentní vyjádření, obvykle nám dobře poslouží vyjádření pomocí rovnic:

- Máme: $a = b + kp$ pro jisté $k \in \mathbb{Z}$
- Chceme: $a = b + \Phi pq$ pro nějaké $\Phi \in \mathbb{Z}$.
- $a = b + lq$ pro jisté $l \in \mathbb{Z}$
- $\gcd(p, q) = 1$

Zde není zcela zjevné, jak sloučit ta dvě známá vyjádření do tvaru, který potřebujeme. Podívejme se tedy na situaci pomocí definice kongruence:

- Máme: p dělí $a - b$
- Chceme: pq dělí $a - b$.
- q dělí $a - b$
- $\gcd(p, q) = 1$

Přesně tuto situaci jsme již (úspěšně) zkoumali v kapitole 1.

Důkaz (poučný): Nechtě $p, q \in \mathbb{N}$ splňují $\gcd(p, q) = 1$. Dány $a, b \in \mathbb{Z}$.

1) \implies : Z předpokladu $a \equiv b \pmod{n}$ máme $a = b + kpq$, $k \in \mathbb{Z}$. Pak $a = b + (kq)p$, kde $kq \in \mathbb{Z}$, proto $a \equiv b \pmod{p}$. Důkaz druhé kongruence je obdobný.

2) \impliedby : Předpoklady $a \equiv b \pmod{p}$ a $a \equiv b \pmod{q}$ dávají $p \mid (a - b)$ a $q \mid (a - b)$. Protože $\gcd(p, q) = 1$, podle lemma 1b.24 máme $(pq) \mid (a - b)$ neboli $a \equiv b \pmod{n}$. □

V cvičení 2a.17 se podíváme na případ, kdy m, n nejsou nesoudělná.

Lemma 2a.17 se dá snadno zobecnit také na vyšší počet činitelů modulu.

Lemma 2a.18.

Nechtě $n_1, n_2, \dots, n_m \in \mathbb{N}$ jsou po dvou nesoudělná. Označme $n = n_1 \cdot n_2 \cdots n_m$.

Čísla $a, b \in \mathbb{Z}$ splňují $a \equiv b \pmod{n}$ právě tehdy, když $a \equiv b \pmod{n_i}$ pro všechna $i = 1, \dots, m$.

Důkaz (poučný): 1) \implies : Důkaz je stejný jako dříve, využije faktu, že $n_i \mid n$.

2) \implies : Předpoklad říká, že $n_i \mid (a - b)$ pro všechna i . Protože jsou n_i navzájem nesoudělná, podle lemma 1b.26 číslo $n = n_1 n_2 \cdots n_m$ dělí $a - b$, tedy $a \equiv b \pmod{n}$. □

Jako cvičení 7a.17 nabízíme alternativní důkaz indukcí, který může čtenáři přijít stravitelnější (nebo také ne).

Příklad 2a.k: Dokážeme, že $337 \cdot 675 \equiv 105 \pmod{165}$.

Je možné spočítat to přímo, ale to dá hodně práce. Místo toho si všimneme, že $165 = 3 \cdot 5 \cdot 11$, a potvrdíme kongruenci vůči navzájem nesoudělným složkám 3, 5, 11:

$$n_1 = 3: 337 \cdot 675 \equiv 1 \cdot 0 = 0 \equiv 105 \pmod{3};$$

$$n_2 = 5: 337 \cdot 675 \equiv 2 \cdot 0 = 0 \equiv 105 \pmod{5};$$

$$n_3 = 11: 337 \cdot 675 \equiv 7 \cdot 4 = 28 \equiv 105 \pmod{11}.$$

Výsledek je potvrzen.

Zvídavého čtenáře teď možná napadlo, že je sice pěkné umět ověřit platnost výsledku, ale kde jsme ten výsledek 105 vlastně vzali, když se nám nechtělo počítat $337 \cdot 675$ a pak hledat zbytek? To je pro některé aplikace naprosto zásadní otázka a dostaneme se k ní, až si vyrobíme pokročilejší nástroje, jmenovitě v kapitole 3e.

△

Práce s velkými moduly je komplikována ještě jedním faktorem. Běžné výpočty v počítači a kalkulačce jsou cíleny na vědu a techniku. Proto se při nich čísla zaokrouhlují, což je v pořádku, protože cifry nižších řádů nejsou pro tyto obory podstatné. Například moje kalkulačka si z každého čísla pamatuje prvních 13 cifer.

Počítání modulu to má jinak. Význam čísla je dán jeho celým zápisem, první i poslední cifra jsou stejně důležité, v mnoha případech je dokonce cifra jednotek ta nejdůležitější. Například při počítání modulu 100 je význam čísla dán čistě posledními dvěma ciframi, ty ostatní nejsou důležité. To znamená, že pro výpočty v celých číslech je třeba používat speciální procedury, které si pamatují všechny cifry. Pokud bych například chtěl zjistit, kolik je 11^{13} modulu 37, tak bych nemohl nejprve celou mocninu jednoduše spočítat na kalkulačce, protože výsledek má 14 míst, ale moje kalkulačka si pamatuje jen 13 a nejnižší cifru zahodí. To se dá vyřešit tak, že bychom postupně násobili jedenáctky a velké mezivýsledky nahrazovali menšími kongruentními zástupci, ale to je pro velké mocniny příliš pracné. Budeme tedy potřebovat vyvinout sofistikovanější postupy pro práci s mocninami ve světě modulu.

2a.19 Mocniny a kongruence

Protože je mocnina a^k jen zkratkou pro opakované násobení $a \cdot a \cdots a$, dává nám důsledek 2a.8 pravidlo pro nahrazování v základu.

!

Fakt 2a.20.

Nechť $n \in \mathbb{N}$, uvažujme $a, u \in \mathbb{Z}$ takové, že $a \equiv u \pmod{n}$.
Pak pro všechna $k \in \mathbb{N}$ platí $a^k \equiv u^k \pmod{n}$.

S Rozbor: Toto se často dokazuje indukcí, viz cvičení 7a.16. Zde ukážeme zajímavý alternativní důkaz. Jsme v situaci, kdy z předpokladu máme informaci $a - u = nl$ pro nějaké $l \in \mathbb{Z}$. Potřebujeme se pomocí tohoto faktu dozvědět něco o čísle $a^k - b^k$. Zde by se čtenáři mohl vybavit vzorec $a^2 - u^2 = (a - u)(a + u)$ či dokonce $a^3 - u^3 = (a - u)(a^2 + au + u^2)$, který přivádí do hry právě výraz $a - u$. Obdobné vzorce platí i pro vyšší mocniny, čímž je plán důkazu hotov.

Důkaz (poučný): Nechť $n \in \mathbb{N}$, dány $a, u \in \mathbb{Z}$. Předpoklad: $a \equiv u \pmod{n}$. Pak existuje $l \in \mathbb{Z}$ takové, že $a - u = nl$.

Pokud $k = 1$, tak máme dokázat, že n dělí $a - u$, což je vlastně totéž co předpoklad, tedy důkaz je hotov.

Pokud $k \geq 2$, můžeme počítat takto:

$$a^k - u^k = (a - u)(a^{k-1} + a^{k-2}u + \cdots + au^{k-2} + u^{k-1}) = n \left[l \sum_{i=0}^{k-1} a^{k-1-i} u^i \right],$$

přičemž číslo v hranaté závorce je zjevně celé. Proto $n \mid (a^k - u^k)$ a závěr následuje. □

Příklad 2a.1: Vypočítáme, jaký je zbytek výrazu $(80 \cdot 70 - 7)^8 \cdot (14 + 69)$ po dělení šesti. Podle faktu 2a.2 stačí tento výraz vypočítat modulo 6 a najít vhodného zástupce. Výpočet nám usnadní to, že díky větám lze prakticky všechna čísla (kromě exponentu 8, pro ten jsme zatím pravidlo neměli) nahradit čísly příjemnějšími, takže snadno počítáme:

$$\begin{aligned} (80 \cdot 70 - 7)^8 \cdot (14 + 69) &\equiv (2 \cdot (-2) - 1)^8 \cdot (2 + 3) \\ &= (-5)^8 \cdot 5 \equiv 1^8 \cdot (-1) = -1 \equiv 5 \pmod{6}. \end{aligned}$$

Zjistili jsme, že dané číslo je modulo 6 kongruentní s číslem 5, které splňuje $0 \leq 5 < 6$ a proto je to zbytek po dělení, tedy $[(80 \cdot 70 - 7)^8 \cdot (14 + 69)] \pmod{6} = 5$.

△

V příkladu jsme poznamenali, že nám zatím chybí pravidlo nahrazování v exponentu. Líbilo by se nám, kdyby platilo něco takového: Když $k \equiv l \pmod{n}$, tak $a^k \equiv a^l \pmod{n}$. Máme ale smůlu, není to pravda. Pro protipříklad si zajdeme do světa modulo $n = 3$, kde máme $2^4 = 16 \equiv 1 \pmod{3}$. Když se ale pokusíme nahradit v exponentu, dostáváme $2^1 = 2$, což není kongruentní jedničce modulo 3.

Je to dáno tím, že mocnění ve skutečnosti není algebraická operace, ve které je k jedním ze vstupů, ale speciální zápis (zkratka) pro opakované násobení, přičemž čísla a mohou být z různých světů (čísla reálná, celá, celá modulo n). Dokonce to ani nemusí být čísla, opakovaně násobit (a tedy mocnit) umíme třeba i matice či funkce. Exponent mocniny je ale vždy ze světa \mathbb{N} a není důvod, proč by pro něj měla platit pravidla ze světa, odkud bereme a , exponenty mají svá vlastní pravidla. Blíže se o tom dočteme v bonusové kapitole 19.

Mý se ale mocniny s velkými exponenty potřebujeme naučit efektivně počítat. Najít a^n postupným násobením číslem a vyžaduje $n - 1$ operací, což je pro velké exponenty nepraktické. Existuje standardní postup, který vyžaduje typicky výrazně méně násobení; je založen na postupném redukování exponentu pomocí dvou pravidel podle jeho parity:

- $a^{2k} = (a^2)^k$,
- $a^{k+1} = a \cdot a^k$.

Opakovanou aplikací těchto pravidel se nakonec dostaneme k mocnině tak malé, že ji již dokážeme snadno spočítat, a při každém kroku máme příležitost zmenšit zúčastněná čísla volbou lepšího zástupce.

! Příklad 2a.m: Spočítáme 136^{182} modulo 13. Nejprve nahradíme v základu: $136^{182} \equiv 6^{182} \pmod{13}$. Víc nám zatím známá pravidla neumožňují, začneme tedy s redukcí mocniny. Nejprve budeme postupovat krok za krokem,

aby byla vidět aplikace pravidel, později budeme kroky slučovat kvůli urychlení.

$$\begin{aligned} 6^{182} &= 6^{2 \cdot 91} = (6^2)^{91} = 36^{91} \equiv (-3)^{91} = (-3) \cdot (-3)^{90} = -3 \cdot ((-3)^2)^{45} = -3 \cdot 9^{45} \\ &\equiv -3 \cdot (-4)^{45} = -3 \cdot (-4) \cdot (-4)^{44} = 12 \cdot ((-4)^2)^{22} \equiv (-1) \cdot 16^{22} \equiv -3^{22} \\ &= -(3^2)^{11} = -9^{11} \equiv -(-4) \cdot (-4)^{10} = 4 \cdot ((-4)^2)^5 = 4 \cdot 16^5 \equiv 4 \cdot 3 \cdot 3^4 \\ &= 12 \cdot (3^2)^2 \equiv (-1) \cdot 9^2 \equiv -(-4)^2 = -16 \equiv -3 \pmod{13}. \end{aligned}$$

Pro počítač je efektivní pracovat se dvěma pravidly, při ručním výpočtu bychom si občas mohli troufnout i na vyšší mocninu, což by postup urychlilo, například

$$6^{182} \equiv \dots \equiv -3 \cdot (-4)^{45} = -3 \cdot (-4)^{3 \cdot 15} = -3 \cdot ((-4)^3)^{15} = -3 \cdot (-64)^{15} \equiv -3 \cdot 1^{15} = -3 \cdot 1 = -3 \equiv 10 \pmod{13}.$$

Ať už volíme cestu automatickou či chytrou, určitě jsme ani jednou nemuseli provést 181 násobení, takže jsme výrazně ušetřili.

△

Máme tedy postup na počítání vysokých mocnin, který funguje obecně a snadno se algoritmizuje. Pro počítač je navíc snazší díky tomu, že se nemusí zdržovat hledáním pohodlnějších zástupců, protože má prostě zadržováno, že ve světě modulo 13 je $9^2 = 3$.

Tento postup je skoro neefektivnější, ale pořád ještě plytvá, protože některé mocniny jsme počítali vícekrát, třeba zrovna 9^2 . Existuje postup, jak mocnění reorganizovat tak, abychom se opakování vyhnuli. Je založen na pozorování, že nejnáze se počítají mocniny s exponentem typu 2^k , protože pak se nemusíme zdržovat snižováním lichého exponentu o jedničku.

! Příklad 2a.n: Ještě jednou $6^{182} \pmod{13}$. Nejprve si exponent vyjádříme pomocí mocnin dvojky, tedy vlastně jde o převod do binárního tvaru, na který máme algoritmus v příkladě 15.d. Vyjde $182 = 128 + 32 + 16 + 4 + 2$, proto $6^{182} = 6^{128+32+16+4+2} = 6^{128} \cdot 6^{32} \cdot 6^{16} \cdot 6^4 \cdot 6^2$. Jednotlivé mocniny lze spočítat odebráním dvojky jako výše, ale pokud začneme od největší, budeme nižší počítat vícekrát. Neefektivnější je tedy začít naopak od nejmenších a pomocí nich se propracovat k vyšším. Například známe-li a^4 , tak umocněním tohoto známého čísla na druhou získáme $a^{4 \cdot 2} = a^8$, pak umocněním tohoto čísla na druhou získáme a^{16} a tak dále. Potřebné mocniny si připravíme ve sloupci nalevo, počítáme modulo 13:

$$\begin{array}{ll} 6^2 = 36 \equiv -3 & \text{To bylo snadné, zejména zacyklení ušetřilo práci, to byl takový bonus. Pak už to jen} \\ 6^4 = (6^2)^2 \equiv (-3)^2 = 9 & \text{dáme dohromady:} \\ 6^8 = (6^4)^2 \equiv 9^2 = 81 \equiv 3 & 6^{182} = 6^{128} \cdot 6^{32} \cdot 6^{16} \cdot 6^4 \cdot 6^2 \equiv 3 \cdot 3 \cdot 9 \cdot 9 \cdot (-3) \\ 6^{16} = (6^8)^2 \equiv 3^2 = 9 & = 9 \cdot 81 \cdot (-3) \equiv (-4) \cdot 3 \cdot (-3) = 36 \equiv 10 \pmod{13}. \\ 6^{32} = (6^{16})^2 \equiv 9^2 \equiv 3 & \\ 6^{64} = (6^{32})^2 \equiv 3^2 = 9 & \\ 6^{128} = (6^{64})^2 \equiv 9^2 \equiv 3 & \end{array}$$

Tento postup vychází v průměru jako jeden z neefektivnějších a je široce používán počítači pro počítání mocniny ve světě celých čísel či celých čísel modulo n . Vrátime se k němu ve cvičení 10c.4. Vyžaduje ale přípravné výpočty, pro běžné ruční počítání bývá redukce mocniny z předchozího příkladu často pohodlnější.

Výpočet se dá ještě mírně urychlit tím, že se spojí umocňování s rozkladem exponentu do jednoho kroku, zájemci si mohou najít algoritmus zvaný „square and multiply“.

△

Nyní pokročíme od metody univerzální k metodě speciální, která v příznivé situaci dokáže proces mocnění významným způsobem zkrátit. Je založena na následujícím tvrzení.

! Věta 2a.21. (malá Fermatova věta)

Nechť $n \in \mathbb{N}$ je prvočíslo.

(i) Je-li $a \in \mathbb{Z}$ nesoudělné s n , pak platí $a^{n-1} \equiv 1 \pmod{n}$.

(ii) Pro každé $a \in \mathbb{Z}$ platí $a^n \equiv a \pmod{n}$.

S Rozbor: Důkaz využívá zajímavé pozorování z obecné algebry. Ukážeme jej na příkladě.

Uvažujme modul $n = 7$. Pak existuje v podstatě jen šest nenulových čísel (kongruentních skupin) zastupovaných čísly z množiny $M = \{1, 2, 3, 4, 5, 6\}$. Co se stane, když všechny členy této množiny vynásobíme nenulovým číslem, řekněme $a = 3$? Protože jsme ve světě modulo 7, máme

$$\{1 \cdot 3, 2 \cdot 3, 3 \cdot 3, 4 \cdot 3, 5 \cdot 3, 6 \cdot 3\} = \{3, 6, 9, 12, 15, 18\} \equiv \{3, 6, 2, 5, 1, 4\} = M.$$

Dostali jsme zase původní množinu, jen s jiným pořadím, což ale u množin nehraje roli. Čtenář si může vyzkoušet, že to dopadne obdobně s libovolným jiným nenulovým číslem a . V důkazu tento jev potvrdíme pro všechna n, a splňující předpoklady věty. Z toho pak odvodíme žádaný vzorec. Důkaz tedy rozhodně není rutinní.

Poznamenejme, že podmínka $\gcd(a, n) = 1$ je pro toto chování klíčová. Například pro $n = 6$ máme množinu $\{1, 2, 3, 4, 5\}$. Když ji vynásobíme pětkou nesoudělnou s $n = 6$, dostaneme $\{5, 4, 3, 2, 1\}$, tedy přerovnění původní množiny, ale násobení čtyřkou dá $\{4, 2, 0, 4, 2\}$.

Důkaz (dobrý, poučný): Nechť $n \in \mathbb{N}$ je prvočíslo, $a \in \mathbb{Z}$.

(i): Předpokládejme, že $\gcd(a, n) = 1$. Nejprve ukážeme, že čísla $a, 2a, \dots, (n-1)a$ nejsou navzájem kongruentní modulo n . Když totiž $ia \equiv ja \pmod{n}$, pak n dělí $a(i-j)$, ale n je nesoudělné s a , proto (lemma 1b.23) n dělí $i-j$. Nicméně $|i-j| < n$, proto $i-j = 0$, tedy $i = j$.

Žádné z těchto čísel také není kongruentní s nulou. Protože n je prvočíslo a čísla $i \in \{1, \dots, n-1\}$ splňují $1 \leq i < n$, musejí být podle faktu 1b.20 nesoudělná s n . Také $\gcd(a, n) = 1$, proto podle lemma 1b.25 také $\gcd(ia, n) = 1$ a tedy n nedělí ia .

Když tedy vezmeme čísla $a, 2a, \dots, (n-1)a$ a přejdeme ke zbytkům modulo n , dostaneme $n-1$ různých nenulových zbytků, tedy všechna čísla $1, 2, \dots, n-1$ (nejspíše v jiném pořadí).

Uvažujme součin

$$\prod_{i=1}^{n-1} (ia) = (1a) \cdot (2a) \cdots ((n-1)a).$$

Podle důsledku 2a.8 můžeme každý z činitelů nahradit zbytkem modulo n a podle našeho pozorování dostaneme součin čísel 1 až $n-1$ neboli číslo $(n-1)!$. Máme

$$(1a) \cdot (2a) \cdots ((n-1)a) \equiv (n-1)! \pmod{n}.$$

My ovšem můžeme v součinu nalevo přesunout násobky $1, 2, \dots$, dopředu, dostáváme pak

$$1 \cdot 2 \cdots (n-1)a^{n-1} \equiv (n-1)! \pmod{n},$$

tedy $(n-1)!a^{n-1} \equiv (n-1)! \pmod{n}$. To znamená, že n dělí číslo

$$(n-1)!a^{n-1} - (n-1)! = (n-1)![a^{n-1} - 1].$$

Protože je n větší než čísla $1, 2, \dots, n-1$, nemůže je dělit, tudíž je s nimi coby prvočíslo nesoudělné (fakt 1b.20). Podle lemma 1b.27 tedy platí $\gcd((n-1)!, n) = 1$ a proto podle lemma 1b.23 n dělí $a^{n-1} - 1$ neboli $a^{n-1} \equiv 1 \pmod{n}$.

(ii): Nechť $a \in \mathbb{Z}$. Příklad $\gcd(a, n) = 1$: Pak lze aplikovat (i) a dostaneme $a^{n-1} \equiv 1 \pmod{n}$, takže podle věty 2a.7 (iii) je $a^n = a \cdot a^{n-1} \equiv a \cdot 1 = a \pmod{n}$.

Příklad $\gcd(a, n) > 1$: Pak coby prvočíslo (viz fakt 1b.20) n dělí a . Proto $a \equiv 0 \pmod{n}$, tedy podle faktu 2a.20 $a^n \equiv 0^n = 0 = a \pmod{n}$. □

Alternativní důkaz se najde jako Poznámka 18a.21xxx.

Čtenáře možná napadne, proč jsme vlastně uváděli (i), když je verze (ii) obecnější a možná i elegantnější. Důvod je jednoduchý, verze (i) je tradiční a rovněž v praktických výpočtech užitečnější, protože do dalšího výpočtu posílá jedničku, zatímco verze (ii) nechává a . Proto všichni za „malou Fermatovu větu“ považují tvrzení (i), budeme to tak dělat i my.

! Příklad 2a.o: Spočítáme zase 6^{182} modulo 13. Protože je 13 prvočíslo nesoudělné s šestkou, můžeme použít malého Fermata. K tomu musíme výraz upravit, aby se v něm objevilo číslo $6^{13-1} = 6^{12}$, což se dělá trikem: na exponent aplikujeme dělení číslem dvanáct se zbytkem a poté standardní identitu pro mocninu:

$$6^{182} = 6^{12 \cdot 15 + 2} = (6^{12})^{15} \cdot 6^2.$$

Podle malé Fermatovy věty pak máme $6^{12} \equiv 1 \pmod{13}$, proto

$$136^{182} \equiv 6^{182} = (6^{12})^{15} \cdot 6^2 \equiv 1^{15} \cdot 36 = 36 \equiv 10 \pmod{13}.$$

Je to jistě snazší než náš předchozí pokus pomocí redukce exponentu.

Všimněte si, že pokud bychom chtěli použít tvrzení (ii) výše, dostali bychom

$$6^{182} = 6^{13 \cdot 14} = (6^{13})^{14} \equiv 6^{14} \pmod{13}$$

a čekala by nás další práce.

△

Ve výpočtu jsme použili postup, který lze vyjádřit obecně a je užitečný při práci s velkými čísly.

Fakt 2a.22.

Nechť $n \in \mathbb{N}$ je prvočíslo a $a \in \mathbb{Z}$ není dělitelné n .

Pak pro každé $k \in \mathbb{N}$ platí $a^k \equiv a^{k \bmod (n-1)} \pmod{n}$.

Pro obecnější pohled viz cvičení 2a.18.

Malá Fermatova věta se tedy dokáže postarat o velké exponenty. Její nevýhodou je, že platí jen pro prvočíselné moduly. Podmínka $\gcd(a, n)$ ve skutečnosti není omezující. Jak jsme již rozebrali výše, pro prvočíslo n a číslo a jsou jen dvě možnosti. Buď $\gcd(a, n) = 1$ a malá Fermatova věta se dá aplikovat, nebo n dělí a , ale pak $a^k \equiv 0^k = 0$.

Hlavní omezení malé Fermatovy věty je, že po rozkladu exponentu typicky zůstává zbytková mocnina, která nepřekročí $n - 1$, ale i to může být dosti velké číslo. Pak nezbyvá než použít univerzální postup pomocí redukce exponentu, například ve formě rychlého mocnění z příkladu 2a.n. Tato věta pro nás tedy problém mocnění zcela neřeší, ale dokáže jej významně redukovat a má také významná použití v teorii.

Přirozená otázka je, zda něco jako malá Fermatova věta existuje i pro n , která nejsou prvočísla. Odpověď je kladná, ale dá to víc práce.

Definice.

Pro $n \in \mathbb{N}$ je **Eulerova funkce (Euler function or totient)** $\varphi(n)$ definována jako počet přirozených čísel, která jsou menší než n a nesoudělná s n .

Kolik je třeba $\varphi(6)$? Snadno nahlédneme, že z množiny $\{1, 2, 3, 4, 5\}$ jsou jen čísla 1, 5 nesoudělná s šestkou, proto $\varphi(6) = 2$. S devítkou jsou v množině $\{1, 2, 3, 4, 5, 6, 7, 8\}$ nesoudělná čísla 1, 2, 4, 5, 7, 8, proto $\varphi(9) = 6$. Tato funkce je známá v teorii čísel a dá se použít k redukci mocniny.

Věta 2a.23. (Eulerova věta)

Nechť $n \in \mathbb{N}$. Jestliže je $a \in \mathbb{Z}$ nesoudělné s n , pak $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Snadno si rozmyslíme, že pro prvočíslo n je $\varphi(n) = n - 1$, protože nesoudělná s prvočíslem n jsou všechna čísla $1, 2, \dots, n - 1$. Pak Eulerova věta říká $a^{n-1} \equiv 1 \pmod{n}$. Je to tedy zobecnění malé Fermatovy věty, či jinak nahlíženo, malá Fermatova věta je jen speciální případ Eulerovy věty.

Důkaz (poučný): Nechť $n \in \mathbb{N}$, dáno $a \in \mathbb{Z}$ nesoudělné s n . Označme

$$M = \{b \in \{1, 2, \dots, n - 1\}; \gcd(b, n) = 1\}.$$

Pak M má $N = \varphi(n)$ prvků, lze ji tedy napsat jako

$$M = \{a_1, \dots, a_N\}.$$

Podobně jako v důkazu malé Fermatovy věty dokážeme, že pro $a_i \neq a_j$ jsou čísla $a_i a, a_j a$ nekongruentní modulo n . Totéž proto platí i pro čísla $a_i a \pmod{n}$ a zase jde o čísla nesoudělná s n a z množiny $\{1, \dots, n - 1\}$. Máme tedy

$$\{a_1 a \pmod{n}, \dots, a_N a \pmod{n}\} \equiv \{a_1, \dots, a_N\} = M.$$

Musí se tedy (v kongruenci modulo n) shodovat i součiny prvků množiny vlevo a množiny vpravo, tedy

$$(a_1 a) \cdot (a_2 a) \cdots (a_N a) \equiv a_1 \cdot a_2 \cdots a_N.$$

Stejně jako v důkazu malé Fermatovy věty pak dovedíme, že $a^N \equiv 1 \pmod{n}$. □

Tato věta se aplikuje stejně jako malá Fermatova věta a obdobně také dostáváme následující fakt:

Důsledek 2a.24.

Nechť $n \in \mathbb{N}$, uvažujme $a \in \mathbb{Z}$ nesoudělné s n .

Pak pro všechna $k \in \mathbb{N}$ platí $a^k \equiv a^{k \bmod \varphi(n)} \pmod{n}$.

Pro obecnější pohled viz cvičení 2a.19.

Nabízí se otázka, proč jsme se zdržovali malou Fermatovou větou a nešli rovnou k Eulerově větě. Jsou dva hlavní důvody. První je, že Eulerova věta je sice aplikovatelná na neprvočíselné moduly n , ale v takovém případě se stává nespolehlivou, protože mezi čísly 1 až $n - 1$ může být velké množství čísel a soudělných s n , se kterými nám vzorec nepomůže. Ten druhý předpoklad $\gcd(a, n) = 1$, který nám v případě malé Fermatovy věty nevadil, se zde tedy stává značně omezující.

Druhým důvodem je, že nalezení hodnoty funkce $\varphi(n)$ pro velká čísla n není snadné. V praxi se preferuje práce s prvočíselnými moduly a malou Fermatovou větou.

Jako ukázkou použití malé Fermatovy věty se vrátíme k šifrování.

Příklad 2a.p (pokračování 2a.j): Původní násobící šifru vylepšíme dvěma způsoby. Za prvé, nebudeme šifrovat jednotlivá písmena, ale budeme je spojovat do bloků určité délky, například tak, že každé písmeno ze zprávy nahradíme dvoučíslím od 00 do 25 a dáme je za sebe. Každý blok pak zašifrujeme. Chceme tedy vytvořit metodu, která umí šifrovat celá čísla.

Druhá modifikace spočívá v nahrazení násobení mocněním. Nejprve odvodíme fungování pro celá čísla. Zvolíme $e \in \mathbb{N}$. Zprávu $m \in \mathbb{N}$ zašifrujeme jako $T(m) = m^e$. Jak se dostaneme k původnímu textu? Inverzním zobrazením $T^{-1}(c) = \sqrt[e]{c} = c^{1/e}$. Vzorec naznačuje, že bychom ve světě celých čísel mohli zkusit dekódovat pomocí vzorce c^d , kde d je inverzní číslo k e modulo n , ale to nefunguje, protože jak jsme již viděli, na exponenty se nevztahují pravidla pro kongruenci. Je tedy potřeba tuto základní myšlenku upravit.

Zvolíme nějaké hodně velké prvočíslo n . Budeme pak posílat zprávy menší než n , čímž zajistíme jejich nesoudělnost s číslem n a tedy aplikovatelnost malé Fermatovy věty (delší zprávy rozdělíme na vhodně malé úseky).

Zvolme libovolné číslo $e \in \mathbb{N}$ nesoudělné s $n - 1$, pak podle věty 2a.12 k němu existuje inverzní číslo $d \in \mathbb{N}$, tedy platí $ed \equiv 1 \pmod{n - 1}$ neboli $ed = 1 + k(n - 1)$ pro nějaké $k \in \mathbb{Z}$. Máme pak k dispozici následující způsob šifrování.

Předpokládejme, že m je zpráva splňující $m < n$. Zašifrujeme ji zobrazením $T(m) = m^e \pmod{n}$. Tvrdíme, že dešifrování dělá zobrazení $T^{-1}(c) = c^d \pmod{n}$. Podobně jako v příkladě 2a.j stačí k potvrzení rovnosti $T^{-1}(T(m)) = m$ ukázat, že $T^{-1}(T(m)) \equiv m$, kdy ve výpočtu vynecháme přechody ke zbytkům. Protože je n prvočíslo a m je s ním nesoudělné, bude možné aplikovat malou Fermatovu větu:

$$T^{-1}(T(m)) = [(m^e) \pmod{n}]^d \pmod{n} \equiv (m^e)^d = m^{ed} = m^{1+k(n-1)} = m \cdot (m^{n-1})^k \equiv m \cdot 1^k = m.$$

Toto šifrování je výrazně bezpečnější než posun či násobení.

Obecným problémem všech šifer je bezpečné doručení klíče druhému účastníkovi, protože dokud jej nedoručíme, tak nemůžeme komunikovat. Představme si případ, kdy chceme, aby nám někdo poslal soukromou informaci, například heslo k platební kartě (jsme banka). Když zákazníkovi sdělíme údaje pro zašifrování, tedy n a e , a někdo je zachytí, tak si snadno rozšířeným Euklidem dopočítá inverzní číslo d a zákazníkovo heslo rozluští.

Zlatým hřeben naší procházky šifrováním je tedy úprava mocnicí šifry tak, abychom mohli informace z zašifrování (n, e) veřejně sdílet, ale dokud si hlídáme tajemství čísla d , tak je takto zašifrovaná zpráva bezpečná.

△

Příklad 2a.q (pokračování 2a.p): Jedním z nejrozšířenějších veřejných šifrovacích schémat na Internetu je v současnosti takzvané **RSA šifrování** (nazvané podle autorů jménem Rivest, Shamir a Adleman, nápad publikovali v roce 1978, i když v tajných službách byl znám dříve, ale patrně nebyl použit). Na začátku zvolíme dvě prvočísla p, q (typicky o 200 a více cifrách). Nechť $n = pq$. Zvolíme $e \in \mathbb{N}$ tak, aby bylo nesoudělné s $(p - 1)(q - 1)$, pak najdeme (rozšířeným Euklidovým algoritmem) $d \in \mathbb{N}$ tak, aby $de \equiv 1 \pmod{(p - 1)(q - 1)}$, tj. d je inverzní prvek k e vzhledem k násobení modulo $(p - 1)(q - 1)$. Dvojici (n, e) sdělíme tomu, kdo nám má zprávy posílat, je to tzv. „veřejný klíč“. Sami si schováme „soukromý klíč“ (n, d) .

Zpráva $m \in \mathbb{N}$ splňující $m < \min(p, q)$ se zašifruje pomocí zobrazení $T(m) = m^e \pmod{n}$. Tvrdíme, že ji lze dešifrovat pomocí zobrazení $T^{-1}(c) = c^d \pmod{n}$.

Opravdu? Protože je p prvočíslo a díky $m < p$ je s ním m nesoudělné, podle malé Fermatovy věty platí

$$T^{-1}(T(m)) \equiv (m^e)^d = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1^{k(q-1)} = m \pmod{p}.$$

Číslo q má ovšem stejné vlastnosti, proto stejně ukážeme $(m^e)^d \equiv m \pmod{q}$. Protože jsou p, q coby různá prvočísla nesoudělná, použijeme lemma 2a.17 a dostáváme $(m^e)^d \equiv m \pmod{n}$ neboli $T^{-1}(T(m)) = m$.

Jak bezpečná je tato metoda? Aby zprávu někdo rozšifroval, musel by najít d , k tomu ale potřebuje znát $(p - 1)(q - 1)$. Takže šifra RSA je tak bezpečná, jako je číslo $(p - 1)(q - 1)$. To se dá z veřejného klíče (n, e) získat jedině nalezením příslušné faktorizace n na $p \cdot q$, což je pro velká čísla velmi obtížná úloha. Náročnost faktorizačních algoritmů roste exponenciálně s délkou kódu, přibližně řečeno pokud prvočísla p, q uděláme o jeden bit delší, tak se délka faktorizace zdvojnásobí. To je pro praktické počítání smrtící (viz kapitola 8d). Odhaduje se, že nejvýkonnější dešifrovací centra světových tajných služeb dokážou dnes požívané RSA metody zlomit po několika desetiletích práce, což se považuje za akceptovatelné. V okamžiku, kdy se díky pokroku ve výpočetní technice tato doba nebezpečně zkrátí, stačí díky prudkému růstu náročnosti zvolit o něco větší p, q , což už se několikrát stalo. Mimochodem, očekává se, že kvantové počítače by si s úlohou faktorizace poradily efektivněji, čtenář si může tipnout, kdo sponzoruje jejich vývoj.

Poznamenejme, že existují efektivní metody pro určité kombinace, například když jsou p, q dosti blízké nebo když je d relativně malé číslo. Je tedy potřeba p, q dobře vybrat.

Mimochodem, pokud bychom prozradili zároveň n a $m = (p - 1)(q - 1)$, tak už nejen může kdokoliv zjistit d řešením $ed \equiv 1 \pmod{m}$, ale dokonce snadno zjistí naši faktorizaci: Máme $m = pq - p - q + 1 = n - p - q + 1$, čísla p, q tedy řeší rovnice $pq = n$, $p + q = n - m + 1$, což je snadná algebraická úloha.

Máme tedy kvalitní šifrování, ale také nový problém: Kde vezmeme prvočísla o 200 cifrách? To je hodně dobrá otázka, na kterou určitě nezapomeneme v kapitole o prvočíslech, viz poznámka 13.9.

△

2a.25 Poznámka (kritéria dělitelnosti): V kapitole 1 jsme se zmínili o existenci kritérií dělitelnosti, ale pořádně se na ně podíváme až zde, protože počítání modulo nabídne pohodlný zápis. Mějme tedy číslo d a chceme najít nějaký pohodlný způsob, jak rozpoznat čísla dělitelná tímto d . Lidé obvykle znají kritéria pro několik menších čísel, relativně populární bývají testy pro dělitelnost čísly 2, 3, 4, 5, 6 (použijí se testy pro 2 a 3), 8, 9, 10 a 11. Dostí nápadně v tomto seznamu chybí sedmička.

Známa kritéria se dají rozdělit do skupin podle toho, z jaké myšlenky vycházejí. Ukážeme několik populárních nápadů, nejprve na kritériích, která známe, a pak se podíváme, jestli bychom dostali něco rozumného pro sedmičku. V úvahách využijeme to, že d dělí a právě tehdy, pokud $a \equiv 0 \pmod{d}$, popřípadě to, že když jsou dvě čísla kongruentní modulo d , tak dávají na otázku dělitelnosti číslem d stejnou odpověď.

1. Jedna skupina kritérií vychází z oddělení koncové cifry (či více cifer). Matematicky oddělíme poslední cifru tak, že dané číslo a napíšeme jako $a = 10A + r$, kde $r = a \bmod 10$. Při pohledu vzhledem k počítání modulo d občas objevíme zajímavé věci. Jako ukázkou dokážeme kritérium dělitelnosti dvojkou. Modulo 2 totiž máme

$$a = 10A + r \equiv 0A + r = r \pmod{2}.$$

Vidíme, že $a \equiv 0 \pmod{2}$ právě tehdy, když $r \equiv 0 \pmod{2}$, jinak řečeno, dělitelnost čísla dvojkou se pozná podle poslední číslice, což samozřejmě známe. Je také vidět, že tento výpočet bude fungovat pro libovolné d , které dělí desítku, čímž dostaneme kritéria pro dělitelnost pěti a deseti.

Oddělení poslední dvojice číslic je dáno vzorcem $a = 100A + r$, kde $r = a \bmod 100$. Pak máme třeba

$$a = 100A + r \equiv 0A + r = r \pmod{4}$$

a vidíme, že poslední dvojčíslí rozhoduje o dělitelnosti čísla čtyřkou, viz také cvičení 1a.13. Podobně se dokazuje kritérium pro $d = 25$. Můžete zkusit oddělit poslední trojčíslí a zamyslet se, jakými zajímavými čísly je dělitelné číslo 1000, viz cvičení 2a.20.

Co dostaneme, když počítáme modulo 7? Nevypadá to moc dobře, protože žádné z čísel typu 10^k není dělitelné sedmi. Například oddělení poslední cifry dává $a = 10A + r \equiv 3A + r \pmod{7}$. Číslo a je tedy dělitelné sedmi právě tehdy, je-li sedmi dělitelné číslo, které vznikne přičtením poslední cifry k trojnásobku toho, co zbylo po odříznutí poslední číslice.

Příklad: Otestujeme dělitelnost čísla $a = 87654$. Předchozí odstavec nabízí testovat místo toho číslo $3 \cdot 8765 + 4$, to se mi ani nechce počítat.

Trochu lépe vypadá oddělení trojčíslí, protože $1000A + r \equiv -A + r \pmod{7}$. Protože dělitelnost nezáleží na znaménku, lze testovat $A - r$, což se trochu lépe pamatuje. Máme tedy následující test:

- Odděl od čísla poslední trojčíslí a odečti jej od toho, co po odříznutí zbylo. Toto nové číslo je dělitelné sedmi právě tehdy, když je dělitelné původní číslo.

Zpět k příkladu: Místo $a = 87654$ otestujeme $87 - 654 = -567$. Zkusíme vydělit, jde to. Číslo 87654 je dělitelné sedmi.

Pokud by po odříznutí a odečtení zbylo velké číslo, je možné použít tento test opakovaně, dokud nezbyde třiciferné číslo. Není to úplně marná metoda.

2. Další populární rodinka kritérií vychází z dekadického rozvoje čísla. Jako inspiraci ukážeme, proč funguje kritérium dělitelnosti trojkou. Když se na dané číslo v dekadickém tvaru $a = \sum_k a_k 10^k$ podíváme modulo 3, můžeme podle věty o kongruenci a operacích nahrazovat jednotlivé části.

$$a = \sum_k a_k 10^k \equiv \sum_k a_k \cdot (10 \bmod 3)^k = \sum_k a_k \cdot 1^k = \sum_k a_k \pmod{3}.$$

Vidíme, že číslo a je dělitelné třemi právě tehdy, pokud je dělitelný jeho ciferný součet. Podobný důkaz ukáže také známá kritéria pro dělitelnost devíti a jedenácti, viz cvičení 2a.20. Dokonce bychom mohli aplikovat modulo i na cifry samotné, tedy $a = \sum_k (a_k \bmod 3)$. Je tedy možné rovnou sčítat namísto cifer jejich zbytky po dělení třemi.

Pomohlo by to se sedmičkou? Modulo 7 dostáváme $a = \sum_k a_k \cdot (10 \bmod 7)^k = \sum_k a_k \cdot 3^k$. Namísto čísla $a = 87654$ bychom mohli testovat číslo $8 \cdot 3^4 + 7 \cdot 3^3 + 6 \cdot 3^2 + 5 \cdot 3^1 + 4$, ani to se mi nechce počítat. Přesto to není zcela slepá ulička. Pokud se podíváme, jaké jsou zbytky čísel 10^k po dělení sedmi, dostáváme cyklickou posloupnost 1, 3, 2, 6, 4, 5, 1, 3, 2... Můžeme tedy sčítat cifry daného a (bráno zprava) násobené těmito váhami. Takže namísto $a = 87654$ lze testovat číslo $4 \cdot 1 + 5 \cdot 3 + 6 \cdot 2 + 7 \cdot 6 + 8 \cdot 4 = 105$. To dělitelné sedmi je, což nám potvrzuje, že opravdu $7 \mid 87654$. Toto kritérium je asi méně příjemné než předchozí algoritmus, ale také se používá.

Velice rozumné kritérium dostaneme, pokud se na tu sumu podíváme podobným způsobem, jako se počítá Hornerovo schéma. Máme-li číslo zapsané číslicemi $(a_n a_{n-1} \dots a_1 a_0)_{10}$, pak bychom kvůli dělitelnosti sedmi měli

testovat číslo

$$\sum_{k=0}^n 3^k a_k = 3^n a_n + 3^{n-1} a_{n-1} + \cdots + 3^1 a_1 + a_0 = 3 \cdot (3 \cdots 3 \cdot (3 \cdot (3 \cdot a_n + a_{n-1}) + a_{n-2}) + \cdots + a_1) + a_0.$$

Toto se dá vyjádřit rozumně slovy.

• Vezmi levou cifru, vynásob třemi a přičti druhou cifru zleva. Výsledné číslo vynásob třemi a přičti třetí cifru zleva, to vynásob třemi a přičti čtvrtou cifru zleva atd., dokud se nedojde k poslední (pravé) cifře. Výsledné číslo je dělitelné sedmi přesně tehdy, když to původní. Vždy po ukončení kroku (přičtení, před násobením třemi) je možné přejít ke zbytku modulo 7.

Ukážeme pro $a = 87654$. Nejprve $3 \cdot 8 + 7 = 31$, zbytek je 3. Pak $3 \cdot 3 + 6 = 15$, zbytek je 1. Pak $3 \cdot 1 + 5 = 8$, pak $3 \cdot 8 + 4 = 28$. Toto je výsledné číslo. Je dělitelné sedmi, proto je i $a = 87654$ dělitelné sedmi.

3. Číslo je možné rozdělovat na skupiny číslic, tedy zapsat je jako $a = \sum_k A_k 100^k$ pro $0 \leq A_k < 100$ (dvojice), $a = \sum_k A_k 1000^k$ pro $0 \leq A_k < 1000$ (trojčísli) atd. Pro rozumné kritérium dělitelnosti číslem d potřebujeme, aby $100 \bmod d$, $1000 \bmod d$ atd. bylo příjemné číslo.

Například $100 \bmod 33 = 1$, proto $\sum_k A_k 100^k \equiv \sum_k A_k \pmod{33}$ a o dělitelnosti daného čísla číslem 33 rozhoduje součet jeho dvojčísli (bráno zprava).

Lze takto dostat něco rozumného pro sedmičku? Ta stovka moc nadějně nevypadá, ale $1000 \bmod 7 = -1$. Máme pak

$$a \equiv \sum (A_k \bmod 7) \cdot (-1)^k \pmod{7}.$$

Dostáváme tak další možné kritérium.

• Dané číslo rozděl zprava na trojčísli a ta postupně sčítej a odčítej, při tomto procesu je možné čísla kdykoliv nahrazovat zbytky po dělení sedmi. Výsledné číslo je dělitelné sedmi právě tehdy, když je dělitelné původní číslo.

Opět zpět k příkladu: Místo $a = 87654$ otestujeme $87 - 654 = -567$. To už tu bylo, toto nové kritérium vlastně vznikne opakováním onoho prvního kritéria.

Neodpustím si poznámku, že také $1000 \bmod 13 = -1$, takže máme obdobné kritérium pro třináctku.

4. Velice zajímavá rodinka kritérií funguje ještě jinak. Zajímá nás dělitelnost číslem d . Začneme tím, že najdeme číslo c tak, aby bylo nesoudělné s d , ale aby d dělilo $10c + 1$.

Uvažujme teď číslo $a = 10A + r$. Protože jsou d, c nesoudělná, tak platí $d \mid a$ právě tehdy, když $d \mid (ca)$. Pak si šikovně napíšeme

$$ca = 10Ac + cr = (10c + 1)A - (A - cr).$$

Výraz nalevo je násobkem d právě tehdy, pokud je jím výraz napravo. Protože ale podle předpokladu d dělí $(10c + 1)A$, tak o všem rozhodne výraz $A - cr$.

Jako ukázkou se opět podíváme na případ $d = 7$. Hledáme c tak, aby nebylo dělitelné sedmi, ale $7 \mid (10c + 1)$. Zkusmo najdeme $c = 2$. Číslo a je tedy dělitelné sedmi právě tehdy, je-li dělitelné číslo $A - 2r$. Tento test lze znovu opakovat na číslo $A - 2r$, takže dostáváme menší a menší čísla, dokud nejsme spokojeni.

• Odřízni pravou cifru, vynásob dvěma a odečti od toho, co zbylo. Opakuj, kolikrát chceš. Výsledné číslo je dělitelné sedmi právě tehdy, když je dělitelné původní číslo.

Výhodou oproti prvnímu přístupu je, že zde nenásobíme A , ale r , což je jednociferné číslo.

Obvyklá ukáзка: Chceme znát dělitelnost čísla $a = 87654$, místo toho koukneme na $8765 - 2 \cdot 4 = 8757$, pak na $875 - 2 \cdot 7 = 861$, pak na $86 - 2 \cdot 1 = 84$ a zde již vidíme, že jde o číslo dělitelné sedmičkou.

Podobně lze vytvořit kritéria pro dělitelnost třinácti, sedmnácti a další zajímavá čísla.

△

Cvičení

Cvičení 2a.1 (rutinní): Spočítejte následující výrazy (zbytky po dělení), tedy ideální zástupce v kongruenci modulo dané číslo:

- | | | | |
|--------------------|---------------------|--------------------|--------------------|
| a) $81 \bmod 11$; | c) $3 \bmod 11$; | e) $48 \bmod 8$; | g) $-8 \bmod 4$; |
| b) $-1 \bmod 7$; | d) $-14 \bmod 13$; | f) $-37 \bmod 5$; | h) $-15 \bmod 6$. |

Cvičení 2a.2 (rutinní): Rozhodněte, které dvojice čísel z následujícího seznamu jsou kongruentní modulo 7: $-13, -4, 0, 1, 3, 7, 9, 17, 28$.

Cvičení 2a.3 (rutinní): Pro daná n spočítejte dané výrazy modulo n tak, aby výsledkem bylo číslo z rozmezí $0, 1, \dots, n - 1$:

- a) $n = 6, (3 \cdot 13 + 11)^4 \cdot (37 + 14 \cdot 5)$;
 b) $n = 5, (13 - 39) \cdot 37 \cdot (-14)^2$;
 c) $n = 8, (24 \cdot 135 + 9)^7 \cdot 15 \cdot 18$.

Cvičení 2a.4 (rutinní): Použijte malou Fermatovu větu k výpočtu následujících výrazů modulo zadané n . Očekávají se výsledky z $\{0, 1, \dots, n-1\}$.

a) 3^{33} modulo $n = 11$;

b) 4^{44} modulo $n = 13$;

c) 5^{55} modulo $n = 23$.

Cvičení 2a.5 (rutinní):

Nechť $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Dokažte, že jestliže $r \in \mathbb{Z}$ splňuje $a \equiv r \pmod{n}$ a $0 \leq r < n$, pak $r = a \bmod n$.

Cvičení 2a.6 (rutinní): Nechť $n \in \mathbb{N}$. Dokažte, že pro každé $a \in \mathbb{Z}$ platí: $a \equiv 0 \pmod{n}$ právě tehdy, když $n|a$.

Cvičení 2a.7 (rutinní): Nechť $n \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$. Pomocí všech tří charakterizací kongruence (dělitelnost, rovnost, zbytky) dokažte, že platí:

a) $a \equiv a \pmod{n}$.

b) Jestliže $a \equiv b \pmod{n}$, pak $b \equiv a \pmod{n}$.

c) Jestliže $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, pak $a \equiv c \pmod{n}$.

Viz věta 2a.5.

Cvičení 2a.8 (rutinní, poučné): Nechť $n \in \mathbb{N}$, $x, y \in \mathbb{Z}$. Dokažte, že jestliže $x = y$, pak $x \equiv y \pmod{n}$.

Cvičení 2a.9 (rutinní, poučné): Nechť $n \in \mathbb{N}$, uvažujme $a, b, u, v \in \mathbb{Z}$ takové, že $a \equiv u \pmod{n}$ a $b \equiv v \pmod{n}$. Dokažte, že pak $a + b \equiv u + v \pmod{n}$ a $a - b \equiv u - v \pmod{n}$ (viz věta 2a.7).

Cvičení 2a.10 (rutinní): Dokažte, že jestliže je $n \in \mathbb{N}$ liché, pak $n^2 \equiv 1 \pmod{4}$.

Dokonce platí $n^2 \equiv 1 \pmod{8}$, ale to už chce nápad.

Cvičení 2a.11 (poučné): Nechť $n \in \mathbb{Z}$, uvažujme $a_1, u_1, \dots, a_m, u_m \in \mathbb{Z}$ takové, že $a_i \equiv u_i \pmod{n}$ pro všechna $i = 1, \dots, m$. Dokažte, že pak $\prod_{i=1}^m a_i \equiv \prod_{i=1}^m u_i \pmod{n}$, viz důsledek 2a.8.

Důkaz používá indukci. Pokud si s ní čtenář ještě nerozumí, může se k tomuto cvičení vrátit po kapitole 7.

Cvičení 2a.12 (poučné): Nechť $n \in \mathbb{N}$. Dokažte, že pro každé $a, u, x \in \mathbb{Z}$ platí: Jestliže je x inverzní číslo k a modulo n a $a \equiv u \pmod{n}$, pak je x inverzní číslo k u modulo n .

Cvičení 2a.13 (rutinní): Nechť $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Dokažte, že b je inverzní číslo k a modulo n právě tehdy, když a je inverzní číslo k b modulo n .

Cvičení 2a.14 (rutinní, poučné): Nechť $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Uvažujme \mathbb{Z} modulo n . Dokažte následující:

a) Jestliže je a invertibilní a x je inverzní číslo k a modulo n , tak je také x invertibilní a a je inverzní číslo k x .

Poznámka: Jde o obdobu vzorce $(a^{-1})^{-1} = a$.

b) Jestliže jsou čísla a a b invertibilní a jejich inverzní čísla modulo n jsou x a y , pak je také ab invertibilní a yx je inverzní číslo k ab modulo n .

Poznámka: Jde o obdobu vzorce $(ab)^{-1} = b^{-1}a^{-1}$.

c) Jestliže a je invertibilní a x je jeho inverzní číslo modulo n , tak je také $-a$ invertibilní a $-x$ je jeho inverzní číslo modulo n .

Poznámka: Jde o obdobu vzorce $(-a)^{-1} = -a^{-1}$.

Nápověda: Ověřte, že kandidáti dělají, co mají.

Cvičení 2a.15 (poučné, dobré): V tomto cvičení budeme považovat kongruenci za zápis rovnice a ověříme, které s obvyklých postupů řešení jsou použitelné.

Nechť $n \in \mathbb{N}$, $x, y, c \in \mathbb{Z}$. Ukažte následující:

a) Jestliže $x \equiv y \pmod{n}$, pak $x + c \equiv y + c \pmod{n}$ a $x - c \equiv y - c \pmod{n}$.

(přičtení k rovnici, odečtení)

b) Jestliže $x + c \equiv y + c \pmod{n}$, pak $x \equiv y \pmod{n}$.

(krácení v rovnici)

c) Jestliže $x \equiv y \pmod{n}$, pak $cx \equiv cy \pmod{n}$.

(vynásobení rovnice)

d) Jestliže $cx \equiv cy \pmod{n}$ a $\gcd(c, n) = 1$, pak $x \equiv y \pmod{n}$.

(krácení v rovnici podruhé, s výhradou)

Vlastně tady dokazujeme, že ve světě modulo lze v rovnicích krátit, ale jen invertibilními čísly. To odpovídá zkušenostem s rovnicemi v reálném světě, kde také lze krátit jen invertibilními (tedy nenulovými) čísly.

Nápověda: Kongruenci přepište pomocí dělitelnosti a pak použijte Euklidovo lemma 1b.23. Nebo využijte právě dokázané (iii) a větu 2a.12.

e) Jestliže $\gcd(c, n) > 1$, pak existují $x, y \in \mathbb{Z}$ takové, že $cx \equiv cy \pmod{n}$, ale neplatí $x \equiv y \pmod{n}$.

Nápověda: Jako y lze zvolit cokoliv, docela šikovná je volba $y = 0$. Využijte přístup z bodu (iv).

Může pomoci, když nejdříve vymyslíte konkrétní protipříklad, zkuste například najít x takové, aby $4x \equiv 0 \pmod{6}$, ale neplatilo $x \equiv 0 \pmod{6}$.

Cvičení 2a.16 (poučné): Necht' $m, n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$. Dokažte, že jestliže $a \equiv b \pmod{n}$ a m dělí n , pak $a \equiv b \pmod{m}$.

Viz lemma 2a.17.

Cvičení 2a.17 (poučné): Necht' $m, n \in \mathbb{N}$. Dokažte, že pro každé $a, b \in \mathbb{Z}$ platí: Jestliže $a \equiv b \pmod{m}$ a $a \equiv b \pmod{n}$, pak $a \equiv b \pmod{\text{lcm}(m, n)}$.

Viz lemma 2a.17.

Cvičení 2a.18 (rutinní, poučné): Dokažte: Necht' $n \in \mathbb{N}$ je prvočíslo a $a \in \mathbb{Z}$ nesoudělné s n . Pro všechna $k, l \in \mathbb{N}$ pak platí: Jestliže $k \equiv l \pmod{n-1}$, pak $a^k \equiv a^l \pmod{n}$.

Viz věta 2a.21.

Cvičení 2a.19 (rutinní, poučné): Dokažte: Necht' $n \in \mathbb{N}$ je prvočíslo a $a \in \mathbb{Z}$ nesoudělné s n . Pro všechna $k, l \in \mathbb{N}$ pak platí: Jestliže $k \equiv l \pmod{\varphi(n)}$, pak $a^k \equiv a^l \pmod{n}$.

Viz věta 2a.23.

Cvičení 2a.20 (rutinní, poučné): Necht' $a = \sum_{i=0}^m a_i 10^i$. Dokažte následující:

- a je dělitelné osmi právě tehdy, když je dělitelné osmi poslední trojčíslí.
- a je dělitelné třemi právě tehdy, když je ciferný součet a (daný $\sum a_i$) dělitelný třemi.
- a je dělitelné devíti právě tehdy, když je ciferný součet a dělitelný devíti.
- a je dělitelné jedenácti právě tehdy, když je jedenácti dělitelné číslo, které získáme sečtením sudých cifer a a odečtením lichých cifer a .

Nápověda: Viz poznámka 2a.25.

Řešení:

Připomínáme, že zde v řešeních symbol \longrightarrow znamená, že z toho nalevo vyplývá to napravo.

2a.1: a) $4 = 81 - 7 \cdot 11$. b) $6 = -1 + 7 = -1 - (-1) \cdot 7$. c) 3. d) $12 = -14 + 13 + 13 = -14 - (-2) \cdot 13$. e) 0 neboť $8 \mid 48$. f) $3 = -37 + 8 \cdot 5 = -37 - (-8) \cdot 5$. g) 0 neboť $4 \mid (-8)$. h) $3 = -15 + 6 + 6 + 6 = -15 - (-3) \cdot 6$.

2a.2: $0 \equiv 7 \equiv 28 \pmod{7}$, $-4 \equiv 3 \equiv 17 \pmod{7}$, $-13 \equiv 1 \pmod{7}$, číslo 9 není kongruentní s nikým v seznamu. Mimochodem, právě jsme viděli rozklad dané množiny na zbytkové třídy.

2a.3: a) $(3 \cdot 13 + 11)^4 \cdot (37 + 14 \cdot 5) \equiv (3 \cdot 1 + (-1))^4 \cdot (1 + 2 \cdot (-1)) = 2^4 \cdot (-1) = -16 \equiv 2 \pmod{6}$.

b) $(13 - 39) \cdot 37 \cdot (-14)^2 \equiv (3 - 4) \cdot 2 \cdot 1^2 = (-1) \cdot 2 = -2 \equiv 3 \pmod{5}$.

c) $(24 \cdot 135 + 9)^7 \cdot 15 \cdot 18 \equiv (0 \cdot 135 + 1)^7 \cdot (-1) \cdot 2 = 1^7 \cdot (-2) = -2 \equiv 6 \pmod{8}$.

Mimochodem, kdyby v tom prvním součinu nevyšla nula, museli bychom nahradit i 135. Standardně bychom počítali $q = \lfloor \frac{135}{8} \rfloor = \lfloor 16.875 \rfloor = 16$, $135 - 16 \cdot 8 = 135 - 128 = 7$. Proto $135 \equiv 7 \pmod{8}$. Nebo bychom odebrali desetkrát osm a dostali 55, od toho odebereme $7 \cdot 8$ a máme -1 .

2a.4: a) $= 3^{3 \cdot 10 + 3} = (3^{10})^3 \cdot 3^3 \equiv 1^3 \cdot 3^3 = 27 \equiv 5 \pmod{11}$. Výpočet je platný, protože 11 je prvočíslo a $\text{gcd}(3, 11) = 1$.

b) $= 4^{3 \cdot 12 + 8} = (4^{12})^3 \cdot 4^8 \equiv 1^3 \cdot (4^2)^4 = 16^4 \equiv 3^4 = 81 \equiv 3 \pmod{13}$. Výpočet je platný, protože 13 je prvočíslo a $\text{gcd}(4, 13) = 1$.

c) $= 5^{2 \cdot 22 + 11} = (5^{22})^2 \cdot 5^{11} \equiv 1^2 \cdot 5 \cdot (5^2)^5 = 5 \cdot 25^5 \equiv 5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 9 = 45 \equiv 22 \pmod{23}$. Výpočet je platný, protože 23 je prvočíslo a $\text{gcd}(5, 23) = 1$.

2a.5: Předp.: $a = r + kn$ pro $k \in \mathbb{Z}$, $0 \leq r < n$. Pak $a = kn + r$ a $0 \leq r < n$, tedy r splňuje požadavky na zbytek po dělení.

2a.6: $a \equiv 0 \pmod{n} \iff n \mid (a - 0) \iff n \mid a$.

2a.7: Dělitelnost: a) $a - a = 0$, proto $n \mid (a - a) \longrightarrow a \equiv a \pmod{n}$. b) $a \equiv b \pmod{n} \longrightarrow n \mid (b - a) \longrightarrow n \mid -(b - a) \longrightarrow n \mid (a - b) \longrightarrow b \equiv a \pmod{n}$. c) viz důkaz věty 2a.5.

Rovnost: a) $a = a + 0 = a + 0 \cdot n$ a $0 \in \mathbb{Z}$, proto $a \equiv a \pmod{n}$. b) viz důkaz věty 2a.5. c) Předp. dají $a = b + kn$ a $b = c + ln$, $k, l \in \mathbb{Z}$. Pak $a = (c + ln) + kn = c + (l + k)n$ a $k + l \in \mathbb{Z}$, tedy $a \equiv c \pmod{n}$.

Zbytky: a) viz důkaz věty 2a.5. b) Předp. dá $a \bmod n = b \bmod n$. V rovnost dvou čísel na pořadí nezáleží, proto $b \bmod n = a \bmod n \longrightarrow b \equiv a \pmod{n}$. c) Podle předp. se rovnají čísla $a \bmod n, b \bmod n$ a také se rovnají čísla $b \bmod n, c \bmod n$. Takže jsou tato tři čísla stejná, tudíž $a \bmod n = c \bmod n \longrightarrow a \equiv c \pmod{n}$.

2a.8: $x = y \longrightarrow x = y + 0 \cdot n$, $0 \in \mathbb{Z} \longrightarrow x \equiv y \pmod{n}$.

2a.9: $u = a + kn$, $v = b + ln$ pak $u + v = (a + b) + (k + l)n$ a $u - v = (a - b) + (k - l)n$, kde $k + l, k - l \in \mathbb{Z}$.

2a.10: $n = 2k + 1 \longrightarrow n^2 = 4k^2 + 4k + 1 = 1 + k(k + 1) \cdot 4$ a $k(k + 1) \in \mathbb{Z}$.

Ovšem jedno z čísel $k, k + 1$ musí být sudé, takže se dá ze členu $4k(k + 1)$ dokonce vytknout osmička.

2a.11: Indukcí. (0) $m = 1$ dává $a_1 \equiv u_1 \pmod{n}$, což platí dle předpokladu.

(1) Nechť $m \in \mathbb{N}$. Indukční předpoklad je $\prod_{i=1}^m a_i \equiv \prod_{i=1}^m u_i \pmod{n}$ pro všechna $a_i \equiv u_i$.

Mějme a_1, \dots, a_{m+1} a u_1, \dots, u_{m+1} po dvou kongruentní. Předpoklad dává $\prod_{i=1}^m a_i \equiv \prod_{i=1}^m u_i \pmod{n}$, také $a_{m+1} \equiv u_{m+1} \pmod{n}$, proto dle věty 2a.7 (iii) platí $\left(\prod_{i=1}^m a_i\right) \cdot a_{m+1} \equiv \left(\prod_{i=1}^m u_i\right) \cdot u_{m+1} \pmod{n}$ neboli $\prod_{i=1}^{m+1} a_i \equiv \prod_{i=1}^{m+1} u_i \pmod{n}$.

2a.12: x je inverzní číslo k a modulo n , tedy $ax \equiv 1 \pmod{n}$, podle $a \equiv u \pmod{n}$ a věty 2a.7 pak také $ux \equiv 1 \pmod{n}$ a x je inverzní číslo k u modulo n .

2a.13: b inv. č. k a mod $n \rightarrow ab \equiv 1 \pmod{n} \rightarrow ba \equiv 1 \pmod{n} \rightarrow a$ inv. č. k b mod n .

2a.14: a) $x \cdot a = a \cdot x \equiv 1 \pmod{n}$ tedy a splňuje podmínku na inverzi k x .

b) $(ab) \cdot (yx) = (a \cdot x) \cdot (b \cdot y) \equiv 1 \cdot 1 = 1 \pmod{n}$ tedy yx splňuje podmínku na inverzi k ab .

c) $(-a) \cdot (-x) = a \cdot x \equiv 1 \pmod{n}$.

2a.15: a) Předp. $x \equiv y \pmod{n} \rightarrow x = y + kn, k \in \mathbb{Z}$. Pak $x \pm c = (y \pm c) + kn, k \in \mathbb{Z}$, tedy $x \pm c \equiv y \pm c \pmod{n}$.

b) Předp. $x + c \equiv y + c \pmod{n} \rightarrow x + c = y + c + kn, k \in \mathbb{Z}$. Pak $x = y + kn, k \in \mathbb{Z}$, tedy $x \equiv y \pmod{n}$.

c) Předp. $x \equiv y \pmod{n} \rightarrow x = y + kn, k \in \mathbb{Z}$. Pak $cx = cy + (ck)n, ck \in \mathbb{Z}$, tedy $cx \equiv cy \pmod{n}$.

d) Předp. $cx \equiv cy \pmod{n} \rightarrow n \mid (cx - cy)$ neboli $n \mid c(x - y)$. Protože $\gcd(c, n) = 1$, podle 1b.23 musí $n \mid (x - y)$ neboli $x \equiv y \pmod{n}$.

Nebo: Máme $cx \equiv cy$, podle (iii) to vynásobíme d , což je inverzní číslo k c (existuje díky nesoudělnosti c, n), dostaneme $dcx \equiv dcy$ a $(dc) \equiv 1$, takže nahradíme: $1x \equiv 1y$.

Nebo: $x = 1x \equiv (dc)x = d(cx) \equiv d(cy) = (dc)y \equiv 1y = y \pmod{n}$.

e) Příklad: $4 \cdot 3 \equiv 4 \cdot 0 \pmod{6}$, ale neplatí $3 \equiv 0 \pmod{6}$.

Jestliže $\gcd(c, n) > 1$, pak existuje celé $d > 1$ takové, že $c = dk$ a $n = dl$ pro nějaké $k, l \in \mathbb{Z}$, přičemž $1 < l < n$. Zvolme $x = l, y = 0$. Pak $c(x - y) = dl$, tedy n dělí $c(x - y) = cx - cy$. Proto $cx \equiv cy \pmod{n}$.

Ale $x - y = l < n$, proto n nedělí $x - y$ a tedy neplatí $x \equiv y \pmod{n}$.

2a.16: Předpoklad $m \mid n$ dává $n = km$ pro nějaké $k \in \mathbb{Z}$. Předpoklad $a \equiv b \pmod{n}$ dává $b = a + ln$ pro nějaké $l \in \mathbb{Z}$. Pak $b = a + (kl)m$ a $kl \in \mathbb{Z}$.

2a.17: Předpoklad dává $m \mid (x - y)$ a $n \mid (x - y)$, takže číslo $x - y$ je společný násobek m, n , tudíž podle faktu 1b.11 také $\text{lcm}(m, n) \mid (x - y)$.

2a.18: Předpoklad dává $k = l + (n - 1)m$ pro $m \in \mathbb{Z}$. Pak podle malé Fermatovy věty $a^k = a^{l+(n-1)m} = a^l (a^{n-1})^m \equiv a^l \cdot 1^m = a^l$.

2a.19: Předpoklad dává $k = l + \varphi(n)m$ pro $m \in \mathbb{Z}$. Pak podle Eulerovy věty $a^k = a^{l+\varphi(n)m} = a^l (a^{\varphi(n)})^m \equiv a^l \cdot 1^m = a^l$.

2a.20: a) $a = 1000A + r \rightarrow a - r = 1000A$ a $8 \mid 1000$, proto $8 \mid (a - r) \rightarrow a \equiv r \pmod{8}$.

b) $10 \equiv 1 \pmod{3}$, proto $a = \sum a_k 10^k \equiv \sum a_k \cdot 1^k = \sum a_k \pmod{3}$.

c) $10 \equiv 1 \pmod{9}$, proto $a = \sum a_k 10^k \equiv \sum a_k \cdot 1^k = \sum a_k \pmod{9}$.

d) $10 \equiv (-1) \pmod{11}$, proto $a = \sum a_k 10^k \equiv \sum a_k \cdot (-1)^k = \sum a_{2i} - \sum a_{2i+1} \pmod{11}$.

2b. Prostor \mathbb{Z}_n

Při práci ve světě celých čísel modulo n můžeme čísla nahrazovat kongruentními zástupci. Pokud se domluvíme, že každé číslo okamžitě nahradíme jeho zbytkem, tak bychom v zásadě ani nepotřebovali jiná čísla než $0, 1$ až $n - 1$. My jsme tedy ve výpočtech pracovali také s čísly jinými, ale to je do značné míry dáno naší pohodlností. Například ve světě modulo $n = 5$ jsme odvodili $3 \cdot 4 \equiv 2$ pomocí $3 \cdot 4 = 12 \equiv 2$. To jsme ale dělali jen proto, že jsme chtěli využít naší znalosti malé násobilky, místo abychom se naučili novou malou násobilku pro svět modulo 5 , kde je prostě $3 \cdot 4 = 2$.

Ovšem pro počítač není problém se takové malé násobilky (a sčítací tabulky) naučit, čímž vzniknou nové operace s čísly, které zde budeme značit \oplus a \odot . Pak si počítač opravdu vystačí s omezenou množinou čísel, což je pro něj výhodné, protože stejně nedokáže obsáhnout všech nekonečně mnoho celých čísel. Z pohledu teoretického tak vznikne nový a zajímavý matematický svět.

**Definice.**

Nechť $n \in \mathbb{N}$. Symbolem \mathbb{Z}_n značíme množinu $\{0, 1, 2, \dots, n-1\}$ spolu s následujícími operacemi:
Pro všechna $a, b \in \mathbb{Z}_n$ definujeme

$$a \oplus b = (a + b) \bmod n,$$

$$a \odot b = (a \cdot b) \bmod n.$$

Pro usnadnění zápisu i zde přiřadíme násobení vyšší prioritu než sčítání, což umožní vynechat některé závorky. Množinu čísel jsme naznačili výčtem, což je zde pro pohodlí čtenáře lepší, ale korektní verze zní $\{a \in \mathbb{Z}; 0 \leq a < n\}$. Pak je jasné, že $\mathbb{Z}_1 = \{0\}$, což se mimochodem v praxi nepoužívá, protože to není užitečné, spíš je to taková kuriozita. Naopak velmi užitečný pro počítačové vědy je prostor $\mathbb{Z}_2 = \{0, 1\}$.

! **Příklad 2b.a:** Nechť $n = 5$. Pak $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ a už jsme viděli, že v tomto světě platí $3 \odot 4 = 2$. Máme tam třeba $1 \oplus 3 = 4$ (což nepřekvapuje), ale také $2 \oplus 3 = 0$ a $3 \oplus 4 = 2$.

Všimněte si, že píšeme rovnítka. Přechody ke zbytkům pomocí kongruence jsou skryty ve značení pro operace, takže máme skutečnou rovnost čísel v \mathbb{Z}_n .

Chování operací u konečných množin se dá dobře zachytit tzv. „Cayleyho tabulkou“. Vpravo vidíme tabulky pro operace \oplus a \odot v \mathbb{Z}_5 .

Ověřte si, že se v tabulkách vyznáte, takže například umíte v levé najít, že $1 \oplus 4 = 0$, a v pravé $2 \odot 4 = 3$.

Pokud bychom si tyto tabulky zapamatovali, tak už při výpočtech ve světě \mathbb{Z}_5 opravdu nepotřebujeme žádná jiná čísla, zejména když za chvíli vyřešíme otázku odčítání, třeba $2 - 4$.

\oplus	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

\odot	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Když máme násobení, tak máme i mocninu. Protože je značení a^k univerzální, neupozorní nás, jaká mocnina to vlastně je. Proto je nutno si hlídat, v jakém světě zrovna umocňujeme. Pro prostor \mathbb{Z}_5 nemáme $4^2 = 16$ (což by ostatně ani nešlo), ale $4^2 = 4 \odot 4 = 1$. Obdobně $2^3 = (2 \odot 2) \odot 2 = 4 \odot 2 = 3$.

△

Operace v prostoru \mathbb{Z}_n jsou nově definovány, takže potřebujeme vědět, jak fungují. V ideálním případě by pro ně platila stejná pravidla jako pro běžné sčítání a násobení, takže bychom při počítání v \mathbb{Z}_n nemuseli přemýšlet jinak. Pokud se například podíváme na sčítací a násobící tabulku v příkladě 2b.a, tak si hned všimneme, že jsou symetrické, což ukazuje na komutativitu. Také si všimneme, že nula a jednička fungují obvyklým způsobem. Není to náhoda, ukážeme, že operace v prostorech \mathbb{Z}_n splňují to, co známe u standardního sčítání a násobení.

**Věta 2b.1.**

Nechť $n \in \mathbb{N}$. Pro všechna $a, b, c \in \mathbb{Z}_n$ platí následující:

- (i) $a \oplus b = b \oplus a$ (komutativita);
- (ii) $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ (asociativita);
- (iii) $a \oplus 0 = 0 \oplus a = a$ (nulový/neutrální prvek);
- (iv) $a \odot b = b \odot a$ (komutativita);
- (v) $a \odot (b \odot c) = (a \odot b) \odot c$ (asociativita);
- (vi) $1 \odot a = a \odot 1 = a$ (jednotkový prvek);
- (vii) $0 \odot a = a \odot 0 = 0$;
- (viii) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ (distributivní zákon).

V důkazech se odvoláme na definice operací, což nás zavede k přístupům známým z důkazů o kongruenci.

Důkaz: (i): Protože $a + b = b + a$, musejí se rovnat i jejich zbytky, tedy $a + b \bmod n = b + a \bmod n$, což podle definice znamená $a \oplus b = b \oplus a$.

Obdobně se dokazuje část (iv).

(ii): Začneme nalevo. Výsledkem operace $b \oplus c$ je číslo $r \in \mathbb{Z}_n$ takové, že $b + c = r + kn$ pro $k \in \mathbb{Z}$. Levá strana dokazované rovnosti je nalezena jako zbytek čísla $a + r = a + (b + c - kn) = a + b + c - kn$, což je díky $k \in \mathbb{Z}$ podle věty 2a.1 totéž jako zbytek s ním kongruentního čísla $a + b + c$.

Napravo: Výsledkem operace $a \oplus b$ je číslo $s \in \mathbb{Z}_n$ takové, že $a + b = s + ln$ pro $l \in \mathbb{Z}$. Pravá strana je pak nalezena jako zbytek čísla $s + c = (a + b - ln) + c = a + b + c - ln$, což je ale totéž jako zbytek čísla $a + b + c$ a tedy totéž jako levá strana.

Obdobně se dokazuje část (v).

(iii): $0 \oplus a = (0 + a) \bmod n = a \bmod n = a$, protože a jakožto číslo z $\{0, 1, \dots, n-1\}$ je samo sobě zbytkem modulo n . Vzorec pro $a \oplus 0$ se dokáže obdobně, popřípadě se použije (i).

Obdobně se dokážou části (vi) a (vii).

(viii): Nalevo: Výsledkem operace $b \oplus c$ je číslo $r \in \mathbb{Z}_n$ takové, že $b + c = r + kn$ pro $k \in \mathbb{Z}$. Levá strana je tedy zbytek čísla $ar = a(b + c - kn) = ab + ac - akn$, což je díky $ak \in \mathbb{Z}$ totéž jako zbytek s ním kongruentního čísla $ab + ac$.

Na pravé straně nejprve spočítáme $a \odot b = r$ a $a \odot c = s$, kde $ab = r + kn$ a $ac = s + ln$. Celkový výsledek pak najdeme jako zbytek čísla

$$r + s = (ab - kn) + (ac - ln) = ab + ac - (k + l)n,$$

což je díky $k + l \in \mathbb{Z}$ stejně jako zbytek čísla $ab + ac$, tedy vyjde to stejně jako nalevo. □

Závěr je, že při úpravách výrazů v \mathbb{Z}_n postupujeme stejně jako u běžných operací.

Protože jsou přechody ke zbytkům a kongruence skryty v definicích operací, v řadě situací nabízí \mathbb{Z}_n efektivnější zápis a díky právě dokázaným vlastnostem také pohodlnější práci, viz třeba příklad 2b.e. Ovšem v okamžiku, kdy něco dokazujeme (či počítáme rukou), tak nám naopak nucené přechody ke zbytkům komplikují situaci. Například v části (viii) potřebujeme podle definice operací dokázat

$$[a \cdot ((b + c) \bmod n)] \bmod n = [(ab) \bmod n + (ac) \bmod n] \bmod n.$$

V důkazu výše jsme se s tím vypořádali mimo jiné odkazem na fakt, že kongruentní čísla a výrazy mají stejný zbytek po dělení n . Souvislost mezi počítáním v \mathbb{Z}_n a kongruencí se vyplatí prozkoumat.

Protože prvky $x, y \in \mathbb{Z}_n$ jsou běžná čísla a porovnávají se standardní rovností, platí pro ně fakt 2a.6. Také ale splňují $|x - y| < n$ a tudíž je možné aplikovat fakt 2a.4. Dostáváme tak následující tvrzení.

Fakt 2b.2.

Nechť $n \in \mathbb{N}$. Čísla $x, y \in \mathbb{Z}_n$ splňují $x = y$ právě tehdy když $x \equiv y \pmod{n}$.

Obdobné tvrzení platí také v případě, kdy x, y jsou algebraické výrazy, ale tam je to poněkud komplikovanější. Výrazy z prostoru \mathbb{Z}_n používají vlastní operace, například $x = 2 \odot 3 \oplus 1$, takže na ně nelze nahlížet jako na výrazy z prostoru \mathbb{Z} a aplikovat kongruenci, jak to děláme v tvrzení. Můžeme se ale dohodnout, že při přechodu od \mathbb{Z}_n do \mathbb{Z} budeme operace nahrazovat podle definice příslušnými operacemi, které už dávají smysl v celých číslech (a poskytují stejnou hodnotu), v našem příkladě by to bylo $x = ((2 \cdot 3) \bmod n + 1) \bmod n$. V této interpretaci už má fakt 2b.2 smysl a platí.

Je ale možné zajít ještě dále. Výraz, který vznikne přepisem speciálních operací, zahrnuje přechody ke zbytkům a je tedy přirozené jej vnímat jako výraz ze světa modulo n , kde je přechod k zástupcům povolen. Je tam také povoleno přejít k jiným zástupcům s tím, že hodnota výrazu se sice změní, ale zůstane s původní hodnotou kongruentní. Klíčovým nápadem je, že jednou z povolených možností je nepřecházet vůbec, tedy ignorovat všechny přechody ke zbytkům v původním výrazu. Dostaneme tak výraz $v = 2 \cdot 3 + 1$, který vznikl prostým nahrazením speciálních operací těmi standardními a s původním výrazem souvisí kongruencí, tedy $x \equiv v \pmod{n}$. Tento nápad nabízí možnost provádět efektivně ruční výpočty.

! **Příklad 2b.b:** Hledáme výsledek výrazu $(9 \odot 5 \oplus 21)^2$ v prostoru \mathbb{Z}_{23} .

Nejprve předvedeme oficiální výpočet v \mathbb{Z}_{23} .

$$(9 \odot 5 \oplus 21)^2 = (22 \oplus 21)^2 = 20^2 = 20 \odot 20 = 9.$$

Coby počítač bychom si jednotlivé výsledky operací pamatovali, jako lidé bychom museli nejprve počítat běžnou algebrou a výsledky hned nahrazovat zbytky.

Nyní se podíváme na alternativu: Namísto výrazu $(9 \odot 5 \oplus 21)^2$ budeme počítat výraz $(9 \cdot 5 + 21)^2$. Vyhodnotíme jej a víme už, že výsledná hodnota bude s tou původní kongruentní. Protože jsme od rovnosti přešli ke kongruenci, můžeme ji rovnou využít také k usnadnění výpočtu.

$$(9 \odot 5 \oplus 21)^2 \equiv (9 \cdot 5 + 21)^2 = (45 + 21)^2 \equiv ((-1) + (-2))^2 = (-3)^2 = 9 \pmod{23}.$$

Zjistili jsme, že $(9 \odot 5 \oplus 21)^2 \equiv 9$. Protože jsou obě čísla ze \mathbb{Z}_{23} , podle faktu 2b.2 musí platit $(9 \odot 5 \oplus 21)^2 = 9$.

Poznamenejme, že abychom mohli tento poslední krok udělat, musíme při kongruentním výpočtu na závěr najít výsledek z množiny $\{0, \dots, n-1\}$, což ale není problém.

△

Toto přenesení práce do světa modulo lze realizovat také ve výrazech s proměnnými, protože všechny argumenty aplikované výše jsou platné i pro ně. Protože jde o důležité pozorování, uděláme na to poznámku.

! 2b.3 Poznámka o výrazech v \mathbb{Z}_n a kongruenci: Odvodili jsme následující postup.

• Mějme výraz x z prostoru \mathbb{Z}_n . Když všechny operace \oplus , \odot nahradíme sčítáním a násobením, dostaneme výraz v , který splňuje $x \equiv v \pmod{n}$. Pokud jeho výpočtem ve světě modulo získáme hodnotu y , tedy $v \equiv y \pmod{n}$, a platí $0 \leq y < n$, pak $x = y$.

Souvislost ale funguje i naopak, protože pravidla pro počítání ve světě kongruence umožňují přechody ke zbytkům přidat všude, kde jsou potřeba pro vznik speciálních operací.

• Mějme algebraický výraz v , který je sestaven pomocí operací sčítání a násobení a ve kterém se vyskytují pouze čísla z množiny $\{0, \dots, n-1\}$ či proměnné s hodnotami tamtéž. Pokud sčítání a násobení nahradíme operacemi \oplus a \odot , tak vznikne výraz x z prostoru \mathbb{Z}_n a platí $x \equiv v \pmod{n}$.

Spojením těchto myšlenek získáme pozorování, které je velmi užitečné v důkazech.

• Uvažujme výrazy x, y v prostoru \mathbb{Z}_n a algebraické výrazy v, w , přičemž x a v se liší pouze záměnou operací \oplus, \odot a $+, \cdot$, stejně tak výrazy y, w . Pak platí, že $x = y$ právě tehdy, když $v \equiv w \pmod{n}$.

Ukažme si, proč tomu tak je. O výrazech víme, že díky spárování splňují $x \equiv v \pmod{n}$ a $y \equiv w \pmod{n}$.

Pokud by platilo $x = y$, tak také $x \equiv y \pmod{n}$ a dostáváme řetízek

$$v \equiv x \equiv y \equiv w \pmod{n}.$$

Naopak pokud by platilo $v \equiv w$, tak dostáváme řetízek

$$x \equiv v \equiv w \equiv y \pmod{n}.$$

K rovnosti se pak dostaneme díky faktu 2b.2, protože výrazy x, y reprezentují nějaké hodnoty ze \mathbb{Z}_n .

Ukažme si, jak se to dá aplikovat na důkaz distributivního zákona (viii). Namísto rovnosti

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

stačí dokázat $a(b+c) \equiv ab+ac \pmod{n}$, což je pravda, protože pro celá čísla máme dokonce přímo rovnost.

△

Nyní se podíváme na odčítání. Z pohledu praktického by bylo užitečné formálně zavést $a \ominus b = (a - b) \pmod{n}$ a vytvořit tabulku pro odčítání, což je pro počítač legitimní volba, ale v teorii se preferuje pracovat pouze s operacemi sčítání a násobení. Ostatně věta 2b.1 ukazuje, proč je máme rádi, při pokusu o obdobnou větu pro odčítání a dělení by v ní to podstatné chybělo.

Jak jsme již zmínili v sekci 2a, odčítání se bere jako příjemná zkratka pro přičítání opačného prvku. Například $2 - 4$ je symbol pro $2 + (-4)$, kde -4 je číslo opačné ke čtyřce. Při pokusu přenést tuto myšlenku do světa \mathbb{Z}_n ovšem narážíme na drobný problém, že tam záporná čísla nemáme.

Abychom jej vyřešili, zamysleme se, co je to vlastně opačný prvek. Co mají společná čísla 4 a -4 ? To, že se navzájem vynulují, tedy $4 + (-4) = 0$. Hledáme tedy řešení rovnice $4 \oplus x = 0$, jinak řečeno hledáme nulu v řádku čtyřky ve sčítací tabulce pro \mathbb{Z}_5 výše. Našli jsme $x = 1$.

Rovnou si všimneme, že nulu najdeme v každém řádku, tedy opačné číslo lze najít ke všem prvkům \mathbb{Z}_5 , což je slibný začátek. Čtenář již dokonce asi tuší, jak se ta čísla hledají a že se najdou obdobnou metodou v každém \mathbb{Z}_n .

Než se dáme do formálních definic, poznamenejme, že modul je zde stále zásadní. Pokud bychom chtěli počítat $2 - 4$ v \mathbb{Z}_9 , tak musíme použít opačný prvek k 4 vzhledem k modulu 9, což je evidentně jiné číslo než ta 1 ze světa modulo 5.

!

Definice.

Nechť $n \in \mathbb{N}$, nechť $a \in \mathbb{Z}_n$. Řekneme, že $b \in \mathbb{Z}_n$ je **opačné číslo** či **opačný prvek** k a v \mathbb{Z}_n , jestliže $a \oplus b = 0$ v \mathbb{Z}_n .
Pak značíme $b = (-a)$.

Protože je \oplus komutativní, opačné číslo automaticky splňuje nejen $a \oplus (-a) = 0$, ale také $(-a) \oplus a = 0$.

Když se na požadavek $a \oplus x = 0$ podíváme očima modulo, viz poznámka 2b.3, tak dostaneme rovnici $a + x \equiv 0$, kterou splníme triviálně volbou $x = -a$. Aby ale byla platná pro prostor \mathbb{Z}_n , musíme namísto $-a$ vzít zbytek po dělení neboli najít vhodného kongruentního zástupce. Vyzkoušíme to.

Příklad 2b.c: Rádi bychom v prostoru \mathbb{Z}_5 odečetli čtyřku od dvojky, tedy spočítali $2 \oplus (-4)$. Označme jako x opačné číslo k číslu 4 v \mathbb{Z}_5 , je to řešení rovnice $4 \oplus x = 0$. Z tabulky jsme našli, že $x = 1$ vyhovuje.

Podívejme se na alternativní přístup přes kongruenci naznačený před příkladem. Evidentně $4 + (-4) = 0$, přechodem k lepšímu zástupci $-4 + 5 = 1$ dostáváme $4 + 1 \equiv 0$ a tedy $x = 1$ je kandidát na opačné číslo k číslu 4 v \mathbb{Z}_5 . Souhlasí to.

Odečteme: $2 \oplus (-4) = 2 \oplus 1 = 3$. Dává to smysl? Výsledek rozdílu $2 - 4 = r$ by měl splňovat $r + 4 = 2$. Kontrola: $3 \oplus 4 = 2$, to souhlasí.

△

Víme tedy, že opačné číslo k číslu $a \in \mathbb{Z}_n$ hledáme nalezením lepšího zástupce čísla $-a$. Vypadá to, že jej získáme přičtením n , ale je tu jedna výjimka.

!

Fakt 2b.4.

Nechť $n \in \mathbb{N}$.

(i) $(-0) = 0$.

(ii) Jestliže $a \in \mathbb{Z}_n$ a $a \neq 0$, pak $(-a) = -a + n$.

Důkaz je snadný, necháme jej jako cvičení 2b.3. Tento fakt mimo jiné potvrzuje, že každé $a \in \mathbb{Z}_n$ má k sobě opačné číslo. Mohlo by jich být víc?

!

Věta 2b.5.

Nechť $n \in \mathbb{N}$. Pak má každé $a \in \mathbb{Z}_n$ právě jeden opačný prvek.

S Rozbor: Jednoznačnost se standardně ukazuje následovně: Předpokládáme, že máme dva kandidáty na dotyčný objekt, a ukážeme, že je vlastně jeden.

Důkaz (poučný): Dány $n \in \mathbb{N}$, $a \in \mathbb{Z}_n$. Předpokládejme, že b_1, b_2 jsou opačné prvky k a , tedy mimo jiné $a \oplus b_1 = 0$ a $b_2 \oplus a = 0$. Pomocí pravidel z věty 2b.1 proto

$$b_2 = b_2 \oplus 0 = b_2 \oplus (a \oplus b_1) = (b_2 \oplus a) \oplus b_1 = 0 \oplus b_1 = b_1.$$

Platí tedy $b_1 = b_2$.

□

Zajímavé je, že jsme v důkazu nikde nepracovali s tím, jak se vlastně v \mathbb{Z}_n sčítá, stačily odvolávky na pravidla. To ukazuje, že opačný prvek bude jednoznačný u každé operace, která splňuje dotyčná pravidla. Takto obecně se operace studují v oboru zvaném algebra, viz kapitola 19.

Pojem opačného prvku splňuje pravidla, na která jsme zvyklí.

Fakt 2b.6.

Nechť $n \in \mathbb{N}$, $a, b \in \mathbb{Z}_n$. Platí:

(i) $-(-a) = a$.

(ii) $-(a \oplus b) = (-a) \oplus (-b)$.

S Rozbor: Ukážeme, že navržená čísla splňují požadavky. V těchto vzorcích se nejedná o nějaké roznásobení mínus jedničkou, protože ta v \mathbb{Z}_n neexistuje. Musíme při důkazu pracovat s pojmem opačného prvku.

Důkaz (poučný): Nechť $n \in \mathbb{N}$, $a, b \in \mathbb{Z}_n$.

(i): Opačné číslo $(-a)$ k $a \in \mathbb{Z}_n$ splňuje $a \oplus (-a) = 0$. Díky (i) z věty 2b.1 také $(-a) \oplus a = 0$, tedy a splňuje požadavky na opačné číslo k $(-a)$.

(ii): Uvažujme výraz $(a \oplus b) \oplus ((-a) \oplus (-b))$. Opakovanou aplikací asociativního a komutativního zákona, předpokladu a dalších pravidel odvodíme následující:

$$\begin{aligned} (a \oplus b) \oplus ((-a) \oplus (-b)) &= (b \oplus a) \oplus ((-a) \oplus (-b)) = b \oplus (a \oplus ((-a) \oplus (-b))) = b \oplus ((a \oplus (-a)) \oplus (-b)) \\ &= b \oplus (0 \oplus (-b)) = b \oplus (-b) = 0. \end{aligned}$$

Takže $(-a) \oplus (-b)$ splňuje požadavky na opačné číslo k $a \oplus b$.

□

Rovněž dělení budeme realizovat pomocí násobení inverzním číslem, ostatně jsme to již udělali v sekci 2a.

!

Definice.

Nechť $n \in \mathbb{N}$, uvažujme $a \in \mathbb{Z}_n$.

Řekneme, že $b \in \mathbb{Z}_n$ je **inverzní číslo** či **inverzní prvek** k a v \mathbb{Z}_n , jestliže $a \odot b = 1$ v \mathbb{Z}_n .

Pokud takovýto prvek b existuje, pak jej značíme $b = a^{-1}$ a řekneme, že a je **invertibilní (invertible)** v \mathbb{Z}_n .

Pohledem do tabulky násobení v příkladě 2b.a odhalíme, že v tomto prostoru je $2^{-1} = 3$ a $3^{-1} = 2$. Také $4^{-1} = 4$. My jsme zvyklí, že $1^{-1} = 1$ a $(-1)^{-1} = -1$, ale tady máme další číslo, které je inverzní samo sobě. Není to zase tak překvapivé, protože ve světě modulo je $4 \equiv -1 \pmod{5}$. Obecněji viz cvičení 2b.6. Ovšem stává se to i pro čísla, která nejsou zástupci čísel 1 nebo -1 , například $5^{-1} = 5$ v \mathbb{Z}_{12} . Poznamenejme, že to sice vypadá zajímavě, ale nějaké významné dopady na chování těchto čísel to nemá.

Díky poznámce 2b.3 máme spojení mezi rovnostmi v \mathbb{Z}_n a kongruencí modulo n . To nám umožní přenést poznatky o inverzním číslu modulo do nového jazyka.



Věta 2b.7.

Nechť $n \in \mathbb{N}$, $a \in \mathbb{Z}_n$. Inverzní prvek a^{-1} v \mathbb{Z}_n existuje právě tehdy, když $\gcd(a, n) = 1$. Pokud existuje, tak je tento prvek jediný.

Důkaz: 1) \implies : Pokud $b = a^{-1}$ existuje, tak splňuje $a \odot b = 1$ a tedy také $ab \equiv 1 \pmod{n}$. Proto je b inverzní číslo modulo n k a a jeho existence podle věty 2a.12 implikuje $\gcd(a, n) = 1$.

2) \impliedby : Nechť $\gcd(a, n) = 1$. Pak podle věty 2a.12 existuje $x \in \mathbb{Z}$ splňující $ax \equiv 1 \pmod{n}$. Zvolme $b = x \pmod{n}$. Pak také b splňuje $a \cdot b \equiv 1 \pmod{n}$ a díky $a, b, 1 \in \mathbb{Z}_n$ platí i $a \odot b = 1$ v \mathbb{Z}_n , tedy $b = a^{-1}$.

3) Jednoznačnost: Nechť $x, y \in \mathbb{Z}_n$ splňují $x = a^{-1}$ a $y = a^{-1}$. Pak jsou to inverzní čísla k a modulo n , tudíž podle věty 2a.14 platí $x \equiv y \pmod{n}$ a proto podle faktu 2b.2 platí $x = y$. □

V kapitole uvidíme, že jednoznačnost inverzního prvku ve skutečnosti plyne z obecnějších zákonitostí (viz fakt 19b.2). Pokročilejší matematické knihy jsou psány tak, že se nejprve udělá co nejobecnější teorie, pak se přechází na speciálnější oblasti a spousta tvrzení se rovnou zdědí z obecně platných principů. V takto napsané knize o diskrétní matematice by přišla kapitola 19 dříve než tato, takže bychom si mohli část práce ušetřit. My se ale v této knize chceme dostat k obtížnějším partiím postupně a dozrát k nim, takže občas děláme práci navíc. Určitě to není na škodu.

Důkaz také ukázal, jak se inverzní čísla v \mathbb{Z}_n hledají.

S Algoritmus 2b.8.

pro nalezení inverzního prvku k a v \mathbb{Z}_n .

0. Jestliže snadno vidíme, že $\gcd(a, n) > 1$, tak inverzní prvek k a v \mathbb{Z}_n neexistuje.

Jinak například pomocí rozšířeného Euklidova algoritmu najdeme $\gcd(a, n) = Aa + Bn$.

1. Jestliže $\gcd(a, n) > 1$, pak inverzní prvek k a v \mathbb{Z}_n neexistuje.

2. Jestliže $\gcd(a, n) = 1$, pak v \mathbb{Z}_n máme $a^{-1} = A \pmod{n}$.

△

! **Příklad 2b.d:** Najdeme opačný prvek a inverzní prvek k $a = 36$ v \mathbb{Z}_{175} .

Opačný prvek: $(-36) \pmod{175}$ je $-36 + 175 = 139$.

Inverzní prvek: Hledáme x splňující $36x = 1$ v \mathbb{Z}_{175} neboli $36x \equiv 1 \pmod{175}$ neboli x takové, aby pro nějaké $m \in \mathbb{Z}$ bylo $36x + 175m = 1$. To nás inspiruje k nalezení Bezoutovy identity.

175	1	0
36	0	1
31	1	-4
5	-1	5
1●	7●	-34●
0		

Dostáváme $\gcd(175, 36) = 1 = 7 \cdot 175 + (-34) \cdot 36$. Když se na obě strany Bezoutovy rovnosti podíváme modulo 175, dostáváme $36 \cdot (-34) + 0 \cdot 7 \equiv 1 \pmod{175}$, tedy $36 \cdot (-34) \equiv 1 \pmod{175}$. Číslo -36 je proto inverzním číslem k 36 modulo 175. Přechodem k zástupci ze \mathbb{Z}_{175} získáme odpověď.

Závěr: 36 je v \mathbb{Z}_{175} invertibilní a $36^{-1} = -36 + 175 = 141$.

Zkouška: $36 \cdot 141 = 5076 \equiv 1 \pmod{175}$, neboť $5076 = 29 \cdot 175 + 1$.

Nalezení inverzního čísla lze zefektivnit tím, že bychom v tabulce měli jen druhý pomocný sloupec a pamatovali si, že výsledek získáme nalezením vhodného zástupce k číslu -34 v „jedničkovém“ řádku. Opět je na čtenáři, jestli si chce pamatovat myšlenku nebo mechanický postup (nejlépe obojí).

△

S Algoritmus 2b.9.

pro nalezení inverzního prvku k a v \mathbb{Z}_n Euklidovým algoritmem.

0. Jestliže snadno vidíme, že $\gcd(a, n) > 1$, tak inverzní prvek k a v \mathbb{Z}_n neexistuje.

Jinak sestavíme tabulku se dvěma sloupci: Do levého sloupce dáme čísla n a a , do pomocného sloupce dáme čísla 0 a 1. Aplikujeme Euklidův algoritmus.

1. Jestliže $\gcd(a, n) > 1$, pak inverzní číslo k a v \mathbb{Z}_n neexistuje.

2. Jestliže $\gcd(a, n) = 1$, najdeme číslo x v pomocném sloupci v řádku s jedničkou nalevo. Pak $a^{-1} = x \bmod n$.
 \triangle

Inverzní čísla ve světě \mathbb{Z}_n mají obvyklé vlastnosti.

Fakt 2b.10.

Nechť $n \in \mathbb{N}$, $a, b \in \mathbb{Z}_n$. Platí:

- (i) Jestliže je a invertibilní, tak je také a^{-1} invertibilní a platí $(a^{-1})^{-1} = a$.
- (ii) Jestliže jsou a, b invertibilní, tak je také $a \odot b$ invertibilní a platí $(a \odot b)^{-1} = b^{-1} \odot a^{-1}$.
- (iii) Jestliže je a invertibilní, tak je také $(-a)$ invertibilní a platí $(-a)^{-1} = (-a^{-1})$.

Důkazy jsou podobné jako u obdobného tvrzení pro opačná čísla a necháváme je jako cvičení 2b.5.

I v prostoru \mathbb{Z}_n je potřeba umět počítat efektivně mocniny neboli opakované násobení jako $a^3 = (a \odot a) \odot a$.

!

Věta 2b.11. (malá Fermatova věta)

Nechť $n \in \mathbb{N}$ je prvočíslo a $a \in \mathbb{Z}_n$ je nesoudělné s n .

- (i) Platí $a^{n-1} = 1$.
- (ii) Jestliže $k, l \in \mathbb{N}$ splňují $k \equiv l \pmod{n-1}$, pak $a^k = a^l$.

Platnost vyplývá z klasické malé Fermatovy věty a cvičení 2a.18 přenosem kongruence na rovnost v \mathbb{Z}_n podle poznámky 2b.3.

Jsou situace, kde je prostředí prostoru \mathbb{Z}_n přirozené.

Příklad 2b.e: Vrátime se k příkladu 2a.j. K šifrování a dešifrování jsme tam používali zobrazení, jejichž vzorce zahrnovaly předchod ke zbytkům. Je tedy přirozené řešit toto v prostoru \mathbb{Z}_{26} , kde se zbytky schovávají ve značení.

K šifrování posunem použijeme zobrazení $T(m) = m \oplus e$ pro zvolenou šifrovací konstantu $e \in \mathbb{Z}_n$. Tvrdíme, že dešifrování provede zobrazení $T^{-1}(c) = c \oplus d$, kde $d = (-e)$. Důkaz provedeme pomocí pravidel z věty 2b.1.

$$T^{-1}(T(m)) = (m \oplus e) \oplus d = m \oplus (e \oplus d) = m \oplus 0 = m.$$

Postupně jsme aplikovali asociativní zákon (přemístění závorek), existenci opačného prvku a pravidlo o nule.

K šifrování násobením použijeme zobrazení $T(m) = e \odot m$, tentokrát potřebujeme, aby $\gcd(e, n) = 1$. Tvrdíme, že dešifrování provede zobrazení $T^{-1}(c) = d \odot c$, kde $d = e^{-1}$. Důkaz:

$$T^{-1}(T(m)) = d \odot (e \odot m) = (d \odot e) \odot m = 1 \odot m = m.$$

Důkazy správnosti byly výrazně snazší, než když jsme toto řešili v jazyce kongruencí. Všechnu práci jsme totiž odvedli v důkazu věty o vlastnostech operací.

Jednoduchá mocninová šifra se definuje pro prvočíslo n a je dána zobrazením $T(m) = m^e$. Tentokrát už nevyžadujeme $e \in \mathbb{Z}_n$, ale chceme, aby $e \in \mathbb{N}$ bylo nesoudělné s $n-1$. Pak existuje $d \in \mathbb{N}$ splňující $ed \equiv 1 \pmod{n-1}$. Díky (ii) věty 2b.11 dokážeme, že zobrazení $T^{-1}(c) = c^d$ dešifruje:

$$T^{-1}(T(m)) = (m^e)^d = m^{ed} = m^1 = m.$$

I zde byly zápis a výpočty znatelně elegantnější než při práci s kongruencí. Bohužel pro RSA už důkaz správnosti dešifrovací funkce tak jednoduše nepůjde, protože jsme nevybudovali potřebné nástroje spojující \mathbb{Z}_p a \mathbb{Z}_{pq} .

\triangle

Pravidla z věty 2b.1 používáme v běžné matematické práci běžně a často si to ani neuvědomujeme. Zviditelníme to při pokusu o řešení jednoduché rovnice.

Příklad 2b.f: Uvažujme rovnici $5 \odot x \oplus 1 = 4$ v \mathbb{Z}_8 . Napodobíme postup, kterým bychom řešili rovnici $5x + 1 = 4$ v oboru reálných čísel.

Nejprve bychom od obou stran odečetli jedničku, což zde nahradíme přičtením (zprava) opačného čísla $(-1) = 7$. Při běžné práci bychom na levé straně prostě napsali $5x + 1 + 7$ či rovnou $5x + 8$, ale ve skutečnosti je potřeba nejprve přesunout závorek asociativním pravidlem a pak využít vlastnosti opačného prvku a nuly.

$$\begin{aligned} (5 \odot x \oplus 1) \oplus 7 &= 4 \oplus 7 \\ (5 \odot x) \oplus (1 \oplus 7) &= 3 \\ (5 \odot x) \oplus 0 &= 3 \\ 5 \odot x &= 3 \end{aligned}$$

8	0
5	1
3	-1
2	2
1•	-3•
0	

Teď bychom rádi rovnici dělili pětkou, což napodobíme tak, že rovnici vynásobíme (zleva) číslem 5^{-1} . Pomocí Euklidova algoritmu zjistíme, že $-3 \equiv 5$ je inverzní číslo k 5 modulo 8, tedy v \mathbb{Z}_8 je $5^{-1} = 5$. Rovnici tímto číslem vynásobíme zleva, opět musíme být opatrní a dojde na asociativitu, tentokrát násobením.

$$\begin{aligned} 5 \odot (5 \odot x) &= 5 \odot 3 \\ (5 \odot 5) \odot x &= 7 \\ 1 \odot x &= 7 \\ x &= 7 \end{aligned}$$

Našli jsme řešení, udělejte si zkoušku (já jsem si ji udělal).

Tento postup bohužel není univerzální. Uvažujme rovnici $6x + 1 = 3$ v \mathbb{Z}_8 . Tato rovnice má řešení, dokonce dvě ($x = 3$ a $x = 7$), ale tímto postupem je nenajdeme, protože $\gcd(6, 8) = 2 > 1$ a tedy neexistuje 6^{-1} . Standardní postup řešení takovýchto rovnic je tedy odlišný, viz kapitola 3.

Když už někdy chceme takto s rovnicemi pracovat, tak bychom ocenili pravidla pro rozšiřování a krácení, která by nám ušetřila ty technické komplikace. Necháme je jako cvičení 2b.8. U pravidel pro krácení existuje zajímavé odvození, která využívá dokázaná pravidla pro operace. Jako nápovědu ukážeme důkaz toho, že když $c \odot x = c \odot y$ v \mathbb{Z}_n a $\gcd(c, n) = 1$, pak $x = y$.

$$\begin{aligned} x &= 1 \odot x = (c^{-1} \odot c) \odot x = c^{-1} \odot (c \odot x) \\ &= c^{-1} \odot (c \odot y) = (c^{-1} \odot c) \odot y = 1 \odot y = y. \end{aligned}$$

△

Tento příklad připomněl, jak užitečné je mít co nejvíce invertibilních čísel. To nás znovu přivádí k prvočíselným modulům.

!

Fakt 2b.12.

Je-li p prvočíslo, pak jsou všechna $a \in \mathbb{Z}_p \setminus \{0\}$ invertibilní.

Důkaz (poučný): Nechť p je prvočíslo, $a \in \mathbb{Z}_p$, $a \neq 0$. Podle faktu 1b.20 jsou dvě možnosti: Buď p dělí a nebo $\gcd(a, p) = 1$.

Ovšem $a \neq 0$ znamená, že by $p|a$ dávalo (věta 1a.23) $p \leq a$, což pro $a \in \mathbb{Z}_p$ není možné. Musí tedy nastat $\gcd(a, p) = 1$ a proto je a invertibilní v \mathbb{Z}_p . □

Pro prvočíslo p se tedy prostor \mathbb{Z}_p chová jako reálná čísla, kde můžeme dělit všemi čísly kromě nuly. Můžeme si v příkladu 2b.a všimnout, že v tabulce pro násobení je v každém řádku jednička a tudíž pro dané číslo existuje číslo inverzní.

→ Z abstraktního pohledu (viz kapitola 19) teď můžeme říct, že $(\mathbb{Z}_n, \oplus, 0)$ je komutativní grupa a $(\mathbb{Z}_n, \odot, 1)$ je komutativní monoid, $(\mathbb{Z}_n, \oplus, \odot)$ je pak komutativní okruh. Pokud je n prvočíslo, pak $(\mathbb{Z}_n, \oplus, \odot)$ je těleso.

Pokud modul n není prvočíslo, tak některé prvky \mathbb{Z}_n nejsou invertibilní. To komplikuje dělení, ale ve skutečnosti to má řadu dalších dopadů na to, co se v takovém prostoru děje. Podíváme se na příklad.

Příklad 2b.g: Podíváme se na násobení v \mathbb{Z}_{14} .

\odot	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
2	0	2	4	6	8	10	12	0	2	4	6	8	10	12
3	0	3	6	9	12	1	4	7	10	13	2	5	8	11
4	0	4	8	12	2	6	10	0	4	8	12	2	6	10
5	0	5	10	1	6	11	2	7	12	3	8	13	4	9
6	0	6	12	4	10	2	8	0	6	12	4	10	2	8
7	0	7	0	7	0	7	0	7	0	7	0	7	0	7
8	0	8	2	10	4	12	6	0	8	2	10	4	12	6
9	0	9	4	13	8	3	12	7	2	11	6	1	10	5
10	0	10	6	2	12	8	4	0	10	6	2	12	8	4
11	0	11	8	5	2	13	10	7	4	1	12	9	6	3
12	0	12	10	8	6	4	2	0	12	10	8	6	4	2
13	0	13	12	11	10	9	8	7	6	5	4	3	2	1

Vidíme, že máme invertibilní prvky 1, kde $1^{-1} = 1$, dále $3^{-1} = 5$ (kontrola: $3 \cdot 5 = 15$, modulo 14 to dává opravdu $15 - 14 = 1$), dále $5^{-1} = 3$, $9^{-1} = 11$ (kontrola: $9 \cdot 11 = 99$, modulo 14 to dává opravdu $99 - 7 \cdot 14 = 1$), dále $11^{-1} = 9$ a nakonec $13^{-1} = 13$.

V tabulce vidíme jednu zvláštnost. V prvním řádku a sloupci samozřejmě nuly očekáváme, ale my je vidíme i jinde. Například $4 \odot 7 = 0$. Nejsme zvyklí, aby se nenulová čísla násobila na nulu. Takovýmto číslům se v algebře (tedy teorii zabývající se operacemi) říká „dělitelé nuly“, což není zrovna šťastný název vzhledem k tomu, že nulu dělí každé celé číslo, ale je to tradice.

Můžete si v tabulce všimnout, že nenulové číslo je vždy buď invertibilní nebo dělitel nuly. Uděláme z toho cvičení 2b.7.

Přítomnost dělitelů nuly má zásadní dopady na to, jak fungují výpočty. V běžném matematickém počítání máme velmi rádi rovnice, kdy je na jedné straně nula a na druhé součin. Například z rovnice $0 = (x - 1)(x + 2)$ rovnou vidíme řešení, $x = 1$ nebo $x = -2$. Ovšem pokud by to byla rovnice v \mathbb{Z}_{14} , tak se také nabízí řada dalších možností, třeba $x - 1 = 4$, $x + 2 = 7$ neboli $x = 5$. To je velmi nepříjemné.

△

Cvičení

Cvičení 2b.1 (rutinní): Pro daná n a a najděte opačný prvek $(-a)$ a inverzní prvek a^{-1} v prostoru \mathbb{Z}_n .

- a) $n = 35$, $a = 12$;
b) $n = 36$, $a = 15$;

- c) $n = 42$, $a = 25$;
d) $n = 146$, $a = 75$.

Cvičení 2b.2 (rutinní): Spočítejte následující výrazy v daném \mathbb{Z}_n . Nejprve převedte odčítání na sčítání s opačnými prvky.

a) $(7 + 8)^{146} - 1, n = 13;$

c) $(31 \cdot 4 - 1)^{192}, n = 20;$

b) $(11 \cdot 27 - 14)^{116}, n = 23;$

d) $(30 + 31)^{108} - 2, n = 53.$

Pokud čtenář není počítač, tak by mohl preferovat alternativní postup z příkladu 2b.b.

Cvičení 2b.3 (rutinní): Nechť $n \in \mathbb{N}$. Dokažte, že pro $a \in \mathbb{Z}_n, a \neq 0$ platí $(-a) = n - a$. (Viz fakt 2b.4.)

Cvičení 2b.4 (poučné): Nechť $n \in \mathbb{N}$. Dokažte, že pro $a, b \in \mathbb{Z}_n$ platí následující: $(-a \odot b) = a \odot (-b) = (-a) \odot b$.
Nápověda: Označíme-li $x = (-a \odot b)$, tak má tento prvek něco splňovat. Stačí ověřit, že to další dva kandidáti dělají.

Cvičení 2b.5 (rutinní, poučné): Nechť $n \in \mathbb{N}, a, b \in \mathbb{Z}$. Dokažte následující:

a) Jestliže je a invertibilní, tak je také a^{-1} invertibilní a platí $(a^{-1})^{-1} = a$.

b) Jestliže jsou a, b invertibilní, tak je také $a \odot b$ invertibilní a platí $(a \odot b)^{-1} = b^{-1} \odot a^{-1}$.

c) Jestliže je a invertibilní, tak je také $(-a)$ invertibilní a platí $(-a)^{-1} = -a^{-1}$.

Nápověda: Ověřte, že kandidáti dělají, co mají, viz cvičení 2b.4.

Cvičení 2b.6: Dokažte, že pro každé $n \in \mathbb{N}, n > 1$ platí $(n - 1)^{-1} = (n - 1)$ v \mathbb{Z}_n .

Cvičení 2b.7 (poučné): Nechť $n \in \mathbb{N}$. Dokažte, že pro každé $a \in \mathbb{Z}_n \setminus \{0\}$ platí, že buď je a invertibilní, nebo je to dělitel nuly, tedy existuje $b \in \mathbb{Z}_n \setminus \{0\}$ takové, že $a \odot b = 0$.

Cvičení 2b.8 (poučné): Nechť $n \in \mathbb{N}, x, y, c \in \mathbb{Z}_n$. Dokažte následující pravidla pro práci s rovnicemi.

a) Jestliže $x = y$, pak $x \oplus c = y \oplus c$ a $c \odot x = c \odot y$.

b) Jestliže $x \oplus c = y \oplus c$, pak $x = y$.

c) Jestliže $c \odot x = c \odot y$ a $\gcd(c, n) = 1$, pak $x = y$.

Řešení:

2b.1:

a) $(-a) = -12 + 35 = 23,$

35	1	0
12	0	1
11	1	-2
1●	-1●	3●
0		

nebo

35	0
12	1
-1	-3
1●	3●
0	

b) $(-a) = -15 + 36 = 21,$

36	1	0
15	0	1
6	1	-2
3●	-2●	5●
0		

$12^{-1} = 3$ v \mathbb{Z}_{35} .

$\gcd(15, 36) > 1$ tedy 15^{-1} v \mathbb{Z}_{36} neex.

c) $(-a) = -25 + 42 = 17,$

42	1	0
25	0	1
17	1	-1
8	-1	2
1●	3●	-5●
0		

nebo

42	0
25	1
-8	-2
1●	-5●
0	

$25^{-1} = -5 \pmod{42} = 37$ v \mathbb{Z}_{42} .

d) $(-a) = -75 + 146 = 71,$

146	1	0
75	0	1
71	1	-1
4	-1	2
3	18	-35
1●	-19●	37●
0		

nebo

146	0
75	1
-4	-2
-1	-37
1●	37●
0	

$75^{-1} = 37$ v \mathbb{Z}_{146} .

2b.2:

a) $(7 \oplus 8)^{146} \oplus (-1) \equiv (7 + 8)^{146} + 12 = 15^{146} + 12 \equiv 2^{146} + 12 = 2^{12 \cdot 12 + 2} + 12 = (2^{12})^{12} \cdot 2^2 + 12 \stackrel{\text{mF}}{\equiv} 1^{12} \cdot 4 + 12 = 16 \equiv 3 \pmod{13}$. Výpočet je platný, protože 13 je prvočíslo a $\gcd(2, 13) = 1$.

Při výpočtu v \mathbb{Z}_{13} bychom psali $(7 \oplus 8)^{146} \oplus (-1) = 2^{146} \oplus 12 = 2^{12 \cdot 12 + 2} \oplus 12 = (2^{12})^{12} \odot 2^2 \oplus 12 \stackrel{\text{mF}}{\equiv} 1^{12} \odot 4 \oplus 12 = 4 \oplus 12 = 3$.

b) $(11 \odot 4 \oplus (-14))^{116} \equiv (11 \cdot 4 + 9)^{116} = 53^{116} \equiv 7^{116} = 7^{22 \cdot 5 + 6} = (7^{22})^5 \cdot 7^6 \stackrel{\text{mF}}{\equiv} 1^5 \cdot 7^6 = 7^6 = (7^2)^3 = 49^3 \equiv 3^3 = 27 \equiv 4 \pmod{23}$.

Výpočet je platný, protože 23 je prvočíslo a $\gcd(7, 23) = 1$.

c) $(31 \odot 4 \oplus (-1))^{192} \equiv (31 \cdot 4 + 19)^{192} \equiv (11 \cdot 4 + 19)^{192} = (44 + 19)^{192} \equiv (4 + 19)^{192} = 23^{192} \equiv 3^{192} \pmod{20}$.

Nelze použít malého Fermata (20 není prvočíslo). Tři možnosti.

Redukce mocniny: $3^{192} = 3^{3 \cdot 64} = (3^3)^{64} = 27^{64} \equiv 7^{64} = (7^2)^{32} \equiv 9^{32} = (9^2)^{16} \equiv 1^{16} = 1 \pmod{20}$.

Chytré mocnění: $3^2 = 9, 3^4 = 9^2 = 81 \equiv 1, 3^8 \equiv 1^2 = 1$ atd., $3^{192} = 3^{128} \cdot 3^{64} \equiv 1 \cdot 1 = 1 \pmod{20}$.

Euler: $\varphi(20) = \varphi(2^2 \cdot 5) = 20(1 - \frac{1}{2})(1 - \frac{1}{5}) = 8$, dále $\gcd(3, 20) = 1$, proto $3^{192} = 3^{8 \cdot 24} = (3^8)^{24} \equiv 1^{24} = 1 \pmod{20}$.

d) $(30 \oplus 31)^{108} \oplus (-2) \equiv (30 + 31)^{108} + 51 = 61^{146} + 51 \equiv 8^{108} + 51 = 2^{52 \cdot 2 + 4} + 51 = (8^{52})^2 \cdot 8^4 + 51 \equiv 1^2 \cdot (8^2)^2 + 51 = 64^2 + 51 \equiv 11^2 + 51 = 121 + 51 \equiv 13 \pmod{53}$.

Výpočet je platný, protože 53 je prvočíslo a $\gcd(8, 53) = 1$.

2b.3: $0 \leq n - a \leq n - 1$, proto $n - a \in \mathbb{Z}_n$. Platí $a \oplus (n - a) = (a + (n - a)) \pmod n = n \pmod n = 0$.

2b.4: $x = (-a \odot b)$ musí splňovat $(a \odot b) \oplus x = 0$. Otestujeme $x = (-a) \odot b$: $(a \odot b) \oplus ((-a) \odot b) = (a \oplus (-a)) \odot b = 0 \odot b = 0$. Otestujeme $x = a \odot (-b)$: $(a \odot b) \oplus (a \odot (-b)) = a \odot (b \oplus (-b)) = a \odot 0 = 0$.

2b.5: a) $a^{-1} \odot a = a \odot a^{-1} = 1 \rightarrow (a^{-1})^{-1} = a$.

b) $(a \odot b) \odot (b^{-1} \odot a^{-1}) = (a \odot a^{-1}) \odot (b \odot b^{-1}) = 1 \odot 1 = 1 \rightarrow (a \odot b)^{-1} = b^{-1} \odot a^{-1}$.

c) Zde je třeba nejprve přejít k výpočtu modulo. $(-a) \cdot (-a^{-1}) = a \cdot a^{-1} \equiv 1 \pmod n$, také $a, a^{-1} \in \mathbb{Z}_n$, proto dle faktu 2b.2 $(-a) \odot (-a^{-1}) = 1$ a tedy $(-a)^{-1} = (-a^{-1})$ v \mathbb{Z}_n .

2b.6: $(n - 1)^2 = n^2 - 2n + 1 = 1 + n(n - 2)$ a $n - 2 \in \mathbb{Z}$, tedy $(n - 1)^2 \equiv 1 \pmod n$.

2b.7: Pokud je a invertibilní, máme hotovo. Jinak $\gcd(a, n) = d > 1$, tedy $a = dk$ pro nějaké $k \in \mathbb{N}$ a $n = db$ pro $b \in \mathbb{N}$. Tvrdíme, že b funguje. Z rovnosti $n = db$ a $d > 1$ máme $b < n$, také $b \neq 0$, tedy $b \in \mathbb{Z}_n$. Dále $ab = dkb = k(db) = kn$ a $k \in \mathbb{Z}$, proto $ab \equiv 0 \pmod n$, tedy $a \odot b = 0$.

2b.8: a) $x = y$ znamená, že daná čísla či hodnoty dané výrazy x, y jsou totožné, takže v algebraických výrazech lze jedno nahradit druhým. To mimo jiné platí i pro výrazy $x \oplus c$ a $c \odot x$.

b) Předp. $x \oplus c = y \oplus c$. Pak $x = x \oplus 0 = x \oplus (c \oplus (-c)) = (x \oplus c) \oplus (-c) = (y \oplus c) \oplus (-c) = y \oplus (c \oplus (-c)) = y \oplus 0 = y$.

c) Viz poznámka v příkladě 2b.f.

2c. Prostor zbytkových tříd \mathbb{Z}_n

Prostor \mathbb{Z}_n jsme zavedli způsobem, který je intuitivní, ale matematici často preferují abstraktnější přístup. Ten je založen na zbytkových třídách, proto je uvedeme oficiálně.

! Definice.

Nechť $n \in \mathbb{N}$. Pro $a \in \mathbb{Z}$ definujeme **zbytkovou třídu** čísla a (modulo n) jako

$$[a]_n = \{b; a \equiv b \pmod n\} = \{a + kn; k \in \mathbb{Z}\}.$$

Dokážeme klíčovou vlastnost zbytkových tříd.

Fakt 2c.1.

Nechť $n \in \mathbb{N}$. Pro $a, b \in \mathbb{Z}$ platí: $[a]_n = [b]_n$ právě tehdy, když $a \equiv b \pmod n$,

Důkaz: poučný 1) \implies : Předpoklad: $[a]_n = [b]_n$. Protože $b \equiv b \pmod n$ (věta 2a.5), je $b \in [b]_n = [a]_n$. Podle definice $[a]_n$ tedy $a \equiv b \pmod n$.

2) \impliedby : Předpoklad $a \equiv b \pmod n$ Uvažujme nějaké $c \in [a]_n$. Pak $a \equiv c \pmod n$. Podle předpokladu a věty 2a.5 pak $b \equiv a \pmod n$. Máme tedy $b \equiv a \equiv c \pmod n$ a tatáž věta dává $b \equiv c \pmod n$ a tedy $c \in [b]_n$. Proto $[a]_n \subseteq [b]_n$.

Obdobně ukážeme, že $[b]_n \subseteq [a]_n$, a máme rovnost množin. □

Další vlastnosti jsme viděli v poznámce 2a.3. Obecnější pohled na vznik zbytkových tříd přijde v kapitole 5.

Nyní se vrátíme k tomu, jak jsme počítali v sekci 2a, a podíváme se na to novým pohledem. Například násobení spojuje určitým způsobem čísla a vytvoří nové, třeba $3 \cdot 4 = 12$. Ovšem ve světě modulo n je možné čísla 3 a 4 a také výsledek 12 nahradit kongruentními zástupci dle libosti. Vlastně jsme tak nespojovali konkrétní čísla, ale jejich kongruentní skupiny neboli zbytkové třídy. Dá se říct, že jsme vytvořili operaci násobení pro třídy, která dala $[3]_n \cdot [4]_n = [12]_n$.

Při tomto novém pohledu tak sčítáme a násobíme nikoliv čísla, ale množiny, pracujeme tedy s nimi jako celky namísto s jednotlivými čísly. Vzniká tak nová matematická struktura.

! Definice.

Nechť $n \in \mathbb{N}$. Symbolem \mathbb{Z}_n značíme množinu $\{[a]_n; a \in \mathbb{Z}\}$ spolu s následujícími operacemi:

Pro všechna $[a]_n, [b]_n \in \mathbb{Z}_n$ definujeme

$$[a]_n \oplus [b]_n = [a + b]_n,$$

$$[a]_n \odot [b]_n = [a \cdot b]_n.$$

Tato definice potřebuje vyjasnit. Za prvé, do \mathbb{Z}_n vkládáme nekonečně mnoho zbytkových tříd. Ve skutečnosti ale většina z nich souhlasí, což znamená, že se tam objeví jen jako jeden prvek množiny. Víme už, že ve skutečnosti existuje jen n různých zbytkových tříd, takže jsme mohli napsat například toto:

$$\mathbb{Z}_n = \{[1]_n, [2]_n, \dots, [n]_n\}.$$

Protože $n \equiv 0 \pmod{n}$, mohli jsme namísto $[n]_n$ napsat $[0]_n$. To je jedna z výhod tohoto přístupu, máme svobodu vybírat zástupce.

Ovšem tím hlavním problémem je definice operací. Když jsme tam napsali $[a]_n \oplus [b]_n$, tak jsme definovali výsledek sčítání pro dvě konkrétní třídy $[a]_n$ a $[b]_n$ se zástupci a, b . My ovšem víme, že stejné třídy lze získat pomocí jiných zástupců, třeba $[u]_n$ a $[v]_n$. V definici se ale pro tyto dvě třídy definuje sčítání znovu, protože jde formálně o jiné třídy (jiní zástupci). Například pro $n = 2$ se součet zbytkových tříd $\{2k; k \in \mathbb{Z}\}$ a $\{1 + 2k; k \in \mathbb{Z}\}$ definuje v podobě $[0]_2 \oplus [1]_2$, ale také třeba $[-6]_2 \oplus [13]_2$. Dostáváme výsledky $[1]_2$ a $[7]_2$, což je ale zase reálně totéž. Nicméně to byl jen jeden příklad, jak je to obecně?

Bylo by velmi nemilé, kdyby se stalo, že by pro reálně stejné ale formálně různé situace definice nabídla rozdílné výsledky, to by pak byla takzvaně nekonzistentní a šlo by o logickou chybu, kterou není možné připustit. Je tedy potřeba se ujistit, že k tomu nedochází a operace jsou definovány korektně.

!

Věta 2c.2.

Nechť $n \in \mathbb{N}$. Uvažujme $a, b, u, v \in \mathbb{Z}$ takové, že $[a]_n = [u]_n$ a $[b]_n = [v]_n$. Pak $[a + b]_n = [u + v]_n$ a $[a \cdot b]_n = [u \cdot v]_n$.

Důkaz (rutinní): Podle faktu 2c.1 $[a]_n = [u]_n$ znamená $a \equiv u \pmod{n}$, podobně pro b a v , pak nám Věta 2a.7 dává $a + b \equiv u + v \pmod{n}$ neboli $[a + b]_n = [u + v]_n$.

Důkaz pro součin je obdobný. □

Takže už víme, že definice je korektní, a můžeme bez obav počítat.

! **Příklad 2c.a:** Například v \mathbb{Z}_5 máme $[3]_5 \odot [4]_5 = [3 \cdot 4]_5 = [12]_5$. Komu se nelíbí tento zástupce, může udělat třeba $[3]_5 \odot [4]_5 = [12]_5 = [2]_5 = [-3]_5 = [127]_5 = \dots$

Nebo třeba v \mathbb{Z}_{13} je $[8]_{13} \oplus [5]_{13} = [13]_{13} = [0]_{13}$, tohle mimochodem ukazuje, že $-[8]_{13} = [5]_{13}$.

△

Pro pokročilejší počítání se hodí vědět, že tyto nové operace splňují obvyklá pravidla. Obdobně jako v předchozí sekci je to pravda.

!

Věta 2c.3.

Nechť $n \in \mathbb{N}$. Pak všechna $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$ platí následující:

- (i) $[a]_n \oplus [b]_n = [b]_n \oplus [a]_n$;
- (ii) $[a]_n \oplus ([b]_n \oplus [c]_n) = ([a]_n \oplus [b]_n) \oplus [c]_n$;
- (iii) $[a]_n \oplus [0]_n = [0]_n \oplus [a]_n = [a]_n$;
- (iv) $[a]_n \odot [b]_n = [b]_n \odot [a]_n$;
- (v) $[a]_n \odot ([b]_n \odot [c]_n) = ([a]_n \odot [b]_n) \odot [c]_n$;
- (vi) $[1]_n \odot [a]_n = [a]_n \odot [1]_n = [a]_n$;
- (vii) $[0]_n \odot [a]_n = [a]_n \odot [0]_n = [0]_n$;
- (viii) $[a]_n \odot ([b]_n \oplus [c]_n) = ([a]_n \odot [b]_n) \oplus ([a]_n \odot [c]_n)$.

Důkaz (poučný): Všechny vlastnosti platí pro operace na \mathbb{Z} a díky chytré definice operací pro třídy se přenesou na operace \oplus a \odot . Ukážeme to pro komutativitu neboli (i): $[a]_n \oplus [b]_n = [a + b]_n = [b + a]_n = [b]_n \oplus [a]_n$. Jen mírně komplikovanější je třeba (viii):

$$[a]_n \odot ([b]_n \oplus [c]_n) = [a]_n \odot [b + c]_n = [a(b + c)]_n = [ab + ac]_n = [ab]_n \oplus [ac]_n = ([a]_n \odot [b]_n) \oplus ([a]_n \odot [c]_n).$$

Další důkazy viz cvičení 2c.1. □

Další dvě operace řešíme stejným přístupem jako v sekci 2b.

**Definice.**

Nechť $n \in \mathbb{N}$, nechť $[a]_n \in \mathbb{Z}_n$.

Řekneme, že $[b]_n \in \mathbb{Z}_n$ je **opačný prvek** k $[a]_n$, značeno $[b]_n = (-[a]_n)$, jestliže $[a]_n \oplus [b]_n = [0]_n$.

Řekneme, že $[b]_n \in \mathbb{Z}_n$ je **inverzní prvek** k $[a]_n$, značeno $[b]_n = [a]_n^{-1}$, jestliže $[a]_n \odot [b]_n = [1]_n$.

Podle definice sčítání je podmínka $[a]_n \oplus [b]_n = [0]_n$ totéž co $[a + b]_n = [0]_n$, což díky faktu 2c.1 je totéž jako $a + b \equiv 0 \pmod{n}$. Neboli $[b]_n$ je opačné číslo k $[a]_n$ přesně tehdy, když b je opačné číslo k a modulo n . Obdobně $[b]_n$ je inverzní číslo k $[a]_n$ přesně tedy, když b je inverzní číslo k a modulo n .

Poznatky o opačných a inverzních číslech včetně postupu jejich získání se tedy přímo převezmou z výpočtů modulo.

Jak si čtenář jistě všiml, prostor \mathbb{Z}_n je teď zaveden dvakrát, jednou jako obyčejná množina čísel $\{0, 1, \dots, n-1\}$ se speciálními operacemi a podruhé jako množina zbytkových tříd se speciálními operacemi. Možná také čtenář napadlo, že operace v zásadě fungují stejně, například v předchozí sekci jsme pro \mathbb{Z}_5 viděli příklad $3 \oplus 4 = 2$, zatímco teď máme

$$[3]_5 \oplus [4]_5 = [8]_5 = [2]_5.$$

Ve skutečnosti jsou tyto dvě verze \mathbb{Z}_n stejné, liší se jen značením. Kdybychom chtěli zjednodušit značení pro zbytkové třídy, tak bychom si pro každou mohli zvolit nějaký symbol. Nabízí se zvolit symbol „0“ pro $[0]_n$, „1“ pro $[1]_n$ až po „ $n-1$ “ pro $[n-1]_n$. Množina \mathbb{Z}_n se pak pomocí těchto zkratků dá napsat jako $\{0, 1, \dots, n-1\}$, přičemž teď to nejsou čísla, ale zkratky pro zbytkové třídy. Nicméně to vypadá stejně jako \mathbb{Z}_n podle první definice.

Dá se ukázat, že když v kterémkoliv výpočtu se zbytkovými třídami vzhledem k jistému $n \in \mathbb{N}$ nahradíme symboly tříd těmito novými zkratkami, tak to bude vypadat jako platný výpočet ze \mathbb{Z}_n podle první definice. Naopak, také se dá ukázat, že když v jakémkoliv výpočtu ve světě \mathbb{Z}_n podle první definice, například $3 \cdot 4 = 2$ v \mathbb{Z}_5 , přikouzlíme kolem každého čísla hranatou závorku a správné indexy $_5$, tedy v našem příkladě $[3]_5 \cdot [4]_5 = [2]_5$, tak dostaneme platný výpočet pro svět zbytkových tříd.

Ukažme to pro sčítání. Vezměme $a, b \in \mathbb{Z}_n$ (dle staré definice) a uvažujme $[a]_n, [b]_n$ jako prvky z nového \mathbb{Z}_n . Ve starém i novém \mathbb{Z}_n provedeme operace sčítání a ukážeme, že to v obou světech dopadne stejně.

Podle první definice dostáváme $a \oplus b = (a + b) \bmod n$, označme tento zbytek jako r , tedy v původním \mathbb{Z}_n máme $a \oplus b = r$. To ale znamená, že $a + b \equiv r \pmod{n}$. Proto také $[a + b]_n = [r]_n$, což podle definice operací pro zbytkové třídy znamená $[a]_n \oplus [b]_n = [r]_n$. Vychází to stejně.

Uvažujme naopak $[a]_n, [b]_n \in \mathbb{Z}$. Díky svobodě volby zástupců můžeme předpokládat, že $0 \leq a < n$ a $0 \leq b < n$, takže jsme pro tyto dvě zbytkové třídy vytvořili zkratky „ a “ a „ b “. Podle definice $[a]_n \oplus [b]_n = [a + b]_n$. Tato výsledná třída má oficiálně zavedenou zkratku „ r “, což je vhodný zástupce, tedy $a + b \equiv r \pmod{n}$ a r je z rozmezí $0, \dots, n-1$. To ale znamená, že $r = (a + b) \bmod n$, tedy v původním \mathbb{Z}_n platí $a \oplus b = r$, což je totéž jako výpočet ve světě tříd psaný zkratkami.

Shrnuto, dá se dokázat, že jde v podstatě o zcela stejný prostor, se stejnými pravidly a fungováním, liší se jen značkami pro jednotlivé prvky množiny \mathbb{Z}_n a mechanismem, pole kterého počítáme (oba ale fungují stejně).

Existuje matematický jazyk, který umí zachytit a rozpoznat, že dva na pohled rozdílné světy jsou ve skutečnosti stejný svět, jen jinak pojmenovaný. Zájemci se mohou podívat do bonusové kapitoly 20.

Nabízí se otázka, proč je svět \mathbb{Z}_n vytvořen dvakrát.

První definice má půvab jednoduchosti při vytváření i zápisu výpočtů. \mathbb{Z}_n je prostě jen konečná množina vybraných celých čísel, se kterými počítáme operacemi, které jsou založeny na jednoduchém mechanismu přechodu ke zbytku. Je to tedy konceptuálně jednodušší pohled.

Nevýhodou je, že dokazování pravidel v tomto světě je poněkud náročnější a jsme nuceni stále vybírat vhodné zástupce, což například komplikuje pravidlo pro opačné číslo.

Definice přes zbytkové třídy je konceptuálně náročnější, protože si uživatel musí zvyknout, že vlastně manipuluje s množinami. Odpovídá tomu i poněkud otravnější značení.

Výhodou je, že ze značení prvků rovnou vidíme použitý modul n , takže to nemusíme pořád někde poznamenávat. Další výhodou je, že mnohé důkazy jsou snadné, protože operace de facto dědíme z celých čísel, viz důkazy vět 2b.1 a 2c.3. Při práci s třídami také nejsme omezovali na specifický rozsah čísel, což není zajímavé pro počítače, ty ocení omezenost světa \mathbb{Z}_n podle původní definice, ale zjednodušuje to občas teoretické věci. Máme například toto:

**Fakt 2c.4.**

Nechť $n \in \mathbb{N}$. Pro každé $[a]_n \in \mathbb{Z}_n$ existuje opačný prvek $-[a]_n = [n - a]_n$.

Viz cvičení 2c.2. Nemuseli jsme řešit zvlášť případ $a = 0$, protože $[n]_n = [0]_n$.

Všechny výpočty modulo z předchozích příkladů o \mathbb{Z}_n by se proto daly přepsat jako výsledky o třídách, třeba v příkladě 2b.d jsme našli inverzní prvek k $a = 36$ v \mathbb{Z}_{175} , $36^{-1} = 141$. V novém znění můžeme říct, že $[36]_{175}^{-1} = [141]_{175}$. Opravdu, $[36]_{175} \cdot [141]_{175} = [36 \cdot 141]_{175} = [5076]_{175} = [1]_{175}$, protože $5076 \equiv 1 \pmod{175}$. Krásně to souhlasí.

Poznámka: Aby tato kapitola nebyla tak krátká, zamysleme se nad přirozenou otázkou. Inverzní čísla v \mathbb{Z}_n hledáme pomocí Euklidova algoritmu. Nedávalo by smysl, aby se i tento algoritmus prováděl pomocí operací z prostoru \mathbb{Z}_n ?

Bohužel to nepůjde, protože v prostorech \mathbb{Z}_n neplatí některé základní poznatky, na které jsme zvyklí z oboru celých čísel a které jsou pro fungování Euklidova algoritmu klíčové.

Začneme už tím, že při hledání inverzního čísla k a a v \mathbb{Z}_n Euklidův algoritmus začíná s čísly n a a , ale v prostoru \mathbb{Z}_n číslo n neexistuje. Je tam ovšem reprezentované číslem 0 . Pokud bychom zkusili začít Euklidův algoritmus s čísly 0 , d , tak okamžitě skončí a jako výsledek dá d bez ohledu na to, jaké je. Takže se neumíme dostat k jedničce a d^{-1} nenajdeme.

To souvisí s tím, že v prostoru \mathbb{Z}_n nefunguje rozumně pojem dělitelnosti. Pokud jej zavedeme stejnou definicí, tedy podmínkou $a = b \cdot k$ pro $k \in \mathbb{Z}_n$, pak nastanou nečekané jevy. Pokud je b invertibilní, tak dělí všechna $a \in \mathbb{Z}_n$. To znamená, že pro prvočíselné n se všechna nenulová čísla dělí navzájem. To je nezvyklé, nicméně smířit bychom se s tím asi uměli. Ale také to znamená, že dělitelnost nesouvisí s velikostí čísel, například v \mathbb{Z}_5 dělí 4 trojku ($3 = 4 \cdot 2$), ačkoliv je větší. To už je podstatný problém.

Jedním z důsledků je, že pokud je n prvočíselo, tak pro libovolná $a, b \in \mathbb{Z}_n$ je vždy číslo $n - 1$ jejich společným dělitelem, tedy v případě použití stejné definice jako u celých čísel bychom dostali $\gcd(a, b) = n - 1$. To ale znamená, že nám $\gcd(a, b)$ dá vždy stejný výsledek pro všechna a, b a tak nám o nich nic nevypovídá.

Jak vidíme, i kdybychom pojmy z kapitoly 1 zavedli v \mathbb{Z}_n , tak by nám to mnoho nepomohlo, proto se to nedělá.

Tedy k původní otázce: I když hledáme inverzní číslo v \mathbb{Z}_n , tak výpočty v Euklidově algoritmu děláme běžnými operacemi v celých číslech.

△

Cvičení

Cvičení 2c.1: .

Nechť $n \in \mathbb{N}$, $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$. Dokažte následující:

- $[a]_n \oplus ([b]_n \oplus [c]_n) = ([a]_n \oplus [b]_n) \oplus [c]_n$;
- $[a]_n \oplus [0]_n = [a]_n$;
- $[a]_n \odot [b]_n = [b]_n \odot [a]_n$;
- $[a]_n \odot ([b]_n \odot [c]_n) = ([a]_n \odot [b]_n) \odot [c]_n$;
- $[1]_n \odot [a]_n = [a]_n$;
- $[0]_n \odot [a]_n = [0]_n$.

Viz věta 2c.3.

Cvičení 2c.2: . Nechť $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Dokažte, že $-[a]_n = [n - a]_n$.

Řešení:

2c.1: a) $[a]_n \oplus ([b]_n \oplus [c]_n) = [a]_n \oplus [b + c]_n = [a + (b + c)]_n = [(a + b) + c]_n = [a + b]_n \oplus [c]_n = ([a]_n \oplus [b]_n) \oplus [c]_n$.

b) $[a]_n \oplus [0]_n = [a + 0]_n = [a]_n$. c) $[a]_n \odot [b]_n = [ab]_n = [ba]_n = [b]_n \odot [a]_n$.

d) $[a]_n \odot ([b]_n \odot [c]_n) = [a]_n \odot [bc]_n = [a(bc)]_n = [(ab)c]_n = [ab]_n \odot [c]_n = ([a]_n \odot [b]_n) \odot [c]_n$.

e) $[1]_n \odot [a]_n = [1 \cdot a]_n = [a]_n$. f) $[0]_n \odot [a]_n = [0 \cdot a]_n = [0]_n$.

2c.2: $[a]_n \oplus [n - a]_n = [a + (n - a)]_n = [n]_n = [0]_n$, neboť $n \equiv 0 \pmod{n}$.