7. Počítání modulo

V této kapitole se podíváme na téma, bez kterého se neobejde žádná diskuse o fungování počítačů, nakonec skončíme u Internetu. Tato látka je přirozené pokračování kapitoly 6.

7a. Kongruence, počítání modulo

V mnoha aplikacích se omezujeme na malou množinu čísel a při vyskočení se do ní vracíme cyklicky, tak jak to děláme běžně u hodin. Zde se na to podíváme pořádně a matematicky.

! **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 $n \mid (a-b)$.

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 $n \mid (a-b)$.

Příklad 7a.a: Z hodin víme, že $21 \equiv 9 \pmod{12}$. Zkouška podle definice: $21 - 9 = 12$, což je dělitelné dvanácti.
Jiný příklad: $(-2) \equiv 13 \pmod{5}$, protože $(-2) - 13 = -15$, což je dělitelné pěti.
△

Někdy se hodí poznávat kongruenci jinak než podle definice.

! **Věta 7a.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 po dělení číslem n.

Důkaz (rutinní, poučný)**:** (i)$\Longrightarrow$(ii): Jestliže $a \equiv b \pmod{n}$, pak $n \mid (a-b)$. Proto existuje $k \in \mathbb{Z}$: $(a-b) = kn$, tedy $a = b + kn$.

(ii)$\Longrightarrow$(iii): Předpokládejme, že $a = b + kn$ pro nějaké $k \in \mathbb{Z}$. Nechť $r = b \bmod n$ (zbytek po dělení), tedy máme rozklad $b = qn + r$ splňující $q \in \mathbb{Z}$ a $0 \leq r < n$. Pak $a = b + kn = (q+k)n + r$, kde $(q+k) \in \mathbb{Z}$ a $0 \leq r < n$, proto jde o rozklad z věty o dělení a $r = a \bmod n$.

(iii)$\Longrightarrow$(i): Nechť $a \bmod n = b \bmod n = r$. Pak existují $p, q \in \mathbb{Z}$ takové, že $a = pn + r$ a $b = qn + r$. Odtud $b - a = (q-p)n$ a $q - p \in \mathbb{Z}$, tedy $n \mid (b-a)$, což podle definice znamená $a \equiv b \pmod{n}$.

Uzavřeli jsme kruh, proto je libovolné z tvrzení (i) až (iii) ekvivalentní s libovolným jiným.

□

Zejména podmínka (ii) je příjemná pro rychlé počítání s malými čísly. Říká, že $a \equiv b \pmod{n}$, jestliže se od a k b (či naopak) dokážeme dostat opakovaným přičítáním/odčítáním čísla n.

! **Příklad 7a.b:** Tvrdíme, že $21 \equiv 9 \pmod{6}$. Podle definice máme ověřit, že 6 dělí $21 - 9 = 12$, což tedy platí.
Podle podmínky (ii) to vidíme také, dvojím přičtením 6 k 9 dostaneme 21. I zbytky po dělení hravě spočítáme, $21 \bmod 6 = 3$ a $9 \bmod 6 = 3$ se rovnají a podmínka (iii) dává $21 \equiv 9 \pmod{12}$.
Podmínka (ii) bývá pro mnohé pohodlná, když dojde na záporná čísla, nemusí si tolik dávat pozor na znaménka. Například dvojím odečtením trojky od -68 dostaneme -74, proto určitě $-68 \equiv -74 \pmod{3}$, mnoha lidem to přijde pohodlnější než odečítat $(-68) - (-74)$.
Podmínka (iii) se hodí v případech, kdy zbytky po dělení n vidíme hned, což je zejména případ $n = 5$. Například $37 \bmod 5 = 2$ a $12 \bmod 5 = 2$, proto určitě $37 \equiv 12 \pmod{5}$.
Jakmile si na tohle čtenář zvykne, tak hned vidí, že ve světě počítání modulo 5 je $3 \equiv 8 \equiv 13 \equiv 18 \equiv 23 \equiv \ldots$ a také $3 \equiv -2 \equiv -7 \equiv -12 \equiv -17 \equiv \ldots$.
△

Ze třetí podmínky okamžitě dostáváme následující.

! **Fakt 7a.2.**
Nechť $n \in \mathbb{N}$. Pak platí:
(i) Pro každé $c \in \mathbb{Z}$ je $c \equiv c \pmod{n}$.
(ii) Nechť $a \in \mathbb{Z}$. $a \equiv 0 \pmod{n}$ právě tehdy, když n dělí a.

Důkaz necháváme jako cvičení 7a.13.

Kongruence splňuje mnoho vlastností, které nám usnadňují práci. Přenesme se tedy do světa, kde vše funguje modulo nějaké konkrétní n. Všechna čísla se tam rozpadnou do skupin podle toho, které je s kterým kongruentní. Například ve světě modulo 2 to bude skupina zahrnující čísla $0, 2, -2, 4, -4, \ldots$ (všechna jsou navzájem kongruentní, lze se mezi nimi přesouvat přičítáním/odčítáním dvojky) a druhá skupina zahrnující čísla $1, -1, 3, -3, 5, -5, \ldots$ (i mezi těmi se lze přesunovat přičítáním/odčítáním dvojky). Formálně si to zavedeme později, nejprve si o takových skupinách něco ukážeme.

Důležité na těch skupinách je, že se v rámci jedné skupiny čísla mohou navzájem zastupovat. Jinak řečeno, pokud máme nějaké číslo a ono se nám nelíbí (třeba je moc velké a nám se s ním nechce počítat), tak si jej ve světě modulo můžeme v mnoha situacích nahradit libovolným jiným číslem z jeho skupiny a nic tím neovlivníme. To je klíčové tvrzení, které si zaslouží přesnější vyjádření a také důkaz.

! **Věta 7a.3.**
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) $ab \equiv uv \pmod{n}$.

Důkaz (poučný)**:** (iii): Podle předpokladu a Věty 7a.1 platí $a = u + kn$ a $b = v + ln$ pro nějaká $k, l \in \mathbb{Z}$. Pak máme také $ab = uv + uln + vkn + kln^2 = (uv) + (ul + vk + kln)n$ a $(ul + vk + kln) \in \mathbb{Z}$, závěr zase plyne z dotyčné Věty.

Důkazy (i) a (ii) necháme jako cvičení 7a.10, jsou obdobné.

□

! Díky této větě například ve světě modula 5 můžeme místo výpočtu $195376 \cdot 16239 + 32532675$ počítat $1 \cdot 4 + 0 = 4$ a výsledky se budou (modulo 5) rovnat. Zástupce jsme přitom našli velice snadno, již totiž víme, že se čísla ve skupinách modulo poznají podle zbytků a zbytek po dělení pěti určíme hravě podle poslední cifry v čísle.

Samozřejmě jsme mohli použít i jiné zástupce, například počítat $(-4) \cdot 114 + 290$, ale proč pracovat, když nemusíme. Potvrdíme si teď obecně, že ve světě modulo n můžeme každé číslo nahradit tím nejjednodušším kandidátem, tedy zbytkem po dělení.

! **Fakt 7a.4.**
Nechť $n \in \mathbb{N}$, uvažujme $a \in \mathbb{Z}$. Jestliže $r = a \bmod n$, tedy r je zbytek po dělení a číslem n, pak $a \equiv r \pmod{n}$.

Důkaz (rutinní)**:** Zbytek splňuje $a = qn + r$ pro jisté $q \in \mathbb{Z}$, proto $a - r = qn$, tedy n dělí $a - r$.

□

Poznamenejme nicméně, že ne vždy je zrovna zbytek po dělení ten nejlepší zástupce. Pokud potřebujeme spočítat $398 \cdot 1243$ modulo 100, pak přechod ke zbytkům dá $98 \cdot 43$, ale my určitě dáme přednost výpočtu $(-2) \cdot 43 = -86 \equiv 14 \pmod{100}$.

Čtenář jistě ví, že odčítání je vlastně přičítání opačného čísla, takže jsme vlastně ani nemuseli dokazovat speciální pravidlo (ii), stačilo by (i) a (iii). Ještě se k tomuto tématu vrátíme. Věta naopak neřešila komplikovanější algebraické výpočty, ale k těm se snadno dostaneme, protože je stejně vždy děláme postupně podle priorit. Můžeme tak princip zastupování rozšířit i na složitější výrazy standardním způsobem, například případ sčítání více čísel se jistě bude dělat indukcí.

Důsledek 7a.5.
Nechť $n \in \mathbb{Z}$.
(i) Uvažujme $a_1, u_1, \ldots, a_m, u_m \in \mathbb{Z}$ takové, že $a_i \equiv u_i \pmod{n}$ pro všechna $i = 1, \ldots, m$.
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 $a_1, b_1, u_1, v_1, \ldots, a_m, b_m, u_m, v_m \in \mathbb{Z}$ takové, že $a_i \equiv u_i \pmod{n}$ a $b_i \equiv v_i \pmod{n}$ pro všechna $i = 1, \ldots, m$. 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 7a.11.
(0) $m = 1$: Předpoklad $a_1 \equiv b_1 \pmod{n}$ je zároveň závěrem, tedy platí.

(1) Předpokládejme, že sčítací vzorec platí pro nějaké $m \in \mathbb{N}$ a všechna a_i, u_i. 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 7a.3 (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 7a.3 (iii) platí $a_i b_i \equiv u_i v_i \pmod n$ pro všechna i, na tyto čísla pak aplikujeme část (i) a sečteme je.

□

Stručně řečeno, v jakémkoliv algebraickém výrazu poskládaném ze sčítání (odčítání) a násobení, případně závorek lze zúčastněná čísla nahrazovat. Doplníme ještě jedno užitečné výpočetní pravidlo.

Fakt 7a.6.
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 $a^k \equiv u^k \pmod n$.

Důkaz (poučný)**:** Protože $a^k = a \cdot a \cdots a$, plyne to hned z (i) v Důsledku výše. Pro zajímavost ukážeme ještě jeden důkaz pro případ $k \geq 2$.

Předpoklad dává $m \in \mathbb{Z}$ takové, že $a - u = mn$. Pak

$$a^k - u^k = (a-u)(a^{k-1} + a^{k-2}u + \cdots + au^{k-2} + u^{k-1}) = m(a^{k-1} + a^{k-2}u + \cdots + au^{k-2} + u^{k-1})n,$$

kde $m(u^{k-1} + a^{k-2}u + \cdots + au^{k-2} + u^{k-1}) \in \mathbb{Z}$. Proto $n \,|\, (a^k - u^k)$ a závěr následuje.

Další alternativní důkaz (indukcí) najdete jako cvičení 7a.12.

□

Příklad 7a.c: Vypočítáme, čemu je kongruentní výraz $(3 \cdot 5 \cdot 17 + 6 \cdot 3 + 9)^8 \cdot (2 + 35 - 4 \cdot 5)$ modulo 6. Podle vět víme, že můžeme prakticky všechna čísla (kromě exponentu 8, pro ten jsme zatím pravidlo neměli) nahradit čísly příjemnějšími, čím menší tím určitě lépe. Proto podle Faktu 7a.4 zkusíme dávat rovnou zbytky po dělení šesti, ke kterým se často nejsnáze dostaneme odečítáním šestky.

$$(3 \cdot 5 \cdot 17 + 6 \cdot 3 + 10)^8 \cdot (2 + 35 - 4 \cdot 5) \equiv (3 \cdot 5 \cdot 5 + 0 \cdot 3 + 4)^8 \cdot (2 + 5 - 4 \cdot 5) \pmod 6.$$

Teď si započítáme obyčejným způsobem:

$$(3 \cdot 5 \cdot 5 + 0 \cdot 3 + 4)^8 \cdot (2 + 5 - 4 \cdot 5) = (15 \cdot 5 + 3)^8 \cdot (7 - 20) \pmod 6.$$

A zase můžeme nahradit, pak zase počítat, napíšeme celý výpočet.

$$\begin{aligned}(3 \cdot 5 \cdot 17 + 6 \cdot 3 + 10)^8 \cdot (2 + 35 - 4 \cdot 5) &\equiv (3 \cdot 5 \cdot 5 + 0 \cdot 3 + 4)^8 \cdot (2 + 5 - 4 \cdot 5) = (15 \cdot 5 + 4)^8 \cdot (7 - 20) \\ &\equiv (3 \cdot 5 + 4)^8 \cdot (1 - 2) = (15 + 4)^8 \cdot (-1) \\ &= (19)^8 \cdot (-1) \equiv 1^8 \cdot (-1) = 1 \cdot (-1) = -1 \pmod 6.\end{aligned}$$

Všimněte si, jak v postupu pečlivě rozlišujeme mezi běžnou algebrou s čísly (značenou rovnítkem) a místy, kde nahrazujeme pomocí rozličných pravidel pro kongruenci (značeno $\equiv$).

△

V aplikacích, kde se pracuje výhradně modulo nějaké konkrétní n, se takové pečlivé rozlišování už nedělá a zkušení lidé prostě píšou rovnítko. Například pokud bychom pracovali čistě s hodinami, tak namísto správného $3 \cdot 16 - 21 \equiv 3 \cdot 4 - 9 = 3 \pmod{12}$ prostě napíšeme $3 \cdot 16 - 21 = 3 \cdot 4 - 9 = 3$. Je to příjemné, ale tady zatím ještě tak zkušení nejsme a navíc se tu snažíme pochopit i teorii, takže budeme pečlivě psát kongruence, ať v tom není zmatek.

Jistě jste si všimli, že jsme zatím nezmínili některé operace. Asi to nebude náhoda.

• Nemáme pravidlo pro nahrazování v exponentu. Konkrétně, není obecně pravda, že když $k \equiv l \pmod n$, tak $a^k \equiv a^l \pmod n$. Například počítáme-li 2^4 modulo 3, pak by nahrazení v exponentu dalo $2^1 = 2$, což ale není správně, $2^4 = 16 \equiv 1 \pmod 3$.

Je to dáno tím, že mocnění ve skutečnosti není algebraická operace, ale zápis (zkratka) pro opakované násobení. Třeba $a^4 = a \cdot a \cdot a \cdot a$, zde jsou čísla a z určitého světa (ve kterém se počítá modulo n nebo i jinak, mocnina se zavádí mnohem obecněji), zatímco to 4 (obecně exponent) do toho světa nepatří, je vždy ze světa $\mathbb{N}$ a říká, kolik objektů násobíme. Nedá se proto čekat, že by pravidla ze světa, odkud bereme a, platila i pro exponent (pro exponenty máme jiná pravidla). Blíže se o tom dočteme v kapitole 8.

Přesto by se nám často hodilo umět zmenšovat exponenty, na to jsou triky jednoduché (viz následující příklad níže) i sofistikované, viz sekce o Eulerově větě.

• Nemáme pravidla pro dělení. My totiž dokonce ani nemáme dělení. Je to podobné jako s odčítáním, dělení je jen pohodlný převlek pro něco jiného. Tak jako je $5-2$ jen zkratka pro $5+(-2)$, je i $6/2$ jen příjemný způsob, jak napsat $6 \cdot \frac{1}{2}$. Takže by nám vlastně ani pravidla pro dělení neměla chybět, ale chybí, ona je to totiž moc příjemná zkratka. Budeme ale na to muset jít jinak, dáme se do toho za chvíli, až si k tomu připravíme podmínky. Jmenovitě si proces počítání modulo zachytíme pomocí speciální matematické struktury.

! Viděli jsme, že si ve světě modula n při počítání zahrnujícím operace sčítání a násobení (a taky to odčítání) vystačíme jen s malou množinou čísel, což je ohromně užitečné třeba pro počítače, které umí ukládat jen konečně mnoho dat. Nejtradičnější je pracovat čistě se zbytky, tedy s čísly z rozmezí 0 až $n-1$. Vzniká pak nový matematický svět.

!
Definice.
Nechť $n \in \mathbb{N}$. Symbolem $\mathbb{Z}_n$ značíme množinu $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$.
Pro všechna $a, b \in \mathbb{Z}_n$ definujme operace

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

Takže chceme-li sečíst/vynásobit dvě čísla ze $\mathbb{Z}_n$, tak začneme tím, že to uděláme normálně, čímž se ale můžeme dostat mimo tuto množinu. Vrátíme se do ní, když výsledek nahradíme oblíbeným zástupcem neboli zbytkem po dělení n.

! **Příklad 7a.d:** Nechť $n = 5$. Pak $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ a máme třeba $2 \oplus 1 = 3$, neboť $2 + 1 = 3$ a $3 \bmod 5 = 3$. Zajímavější je $3 \oplus 4 = 2$, neboť $3 + 4 = 7$ a $7 \bmod 5 = 2$. Máme také $1 \oplus 4 = 0$ (rozmyslete si) nebo třeba $3 \odot 4 = 2$, neboť $3 \cdot 4 = 12 \bmod 5 = 2$.
△

Čtenář se setkal s tím, že se třeba operace sčítání, což je určitý nápad, jak kombinovat čísla, dala používat v rozličných světech: Sčítali jsme ve světě přirozených čísel $\mathbb{N}$, reálných čísel $\mathbb{R}$ nebo třeba ve světě komplexních čísel. Nejde tedy o nic nového, teď používáme sčítání v dalším světě čísel $\mathbb{Z}_n$ (museli jsme jej na to trochu upravit). Posléze ukážeme, že i v tomto světě platí pro „sčítání“ stejná pravidla, na jaká jsme zvyklí, obdobně pro násobení.

! **Příklad 7a.e:** Chování operací u konečných množin se dá dobře zachytit tabulkou. Ukažme si tabulky pro operace $\oplus$ a $\odot$ v $\mathbb{Z}_6$.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\odot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Ověřte si, že se v tabulkách vyznáte, takže například umíte v levé najít, že $3 \oplus 4 = 1$, a v pravé $2 \odot 4 = 2$.
Vyzkoušejte si také, že takto umíte počítat, dokázali byste tu tabulku sami vyrobit?
△

Možná vás teď napadlo, jaký je vlastně rozdíl mezi počítáním modulo n a počítáním v prostoru $\mathbb{Z}_n$? V podstatě žádný, v obou případech lze zúčastněná čísla nahradit příjemnějšími a počítáme stejně, rozdíl je až na konci, kde si v případě počítání modulo můžeme pro výsledek vybrat libovolného zástupce, zatímco v případě počítání v $\mathbb{Z}_n$ si musíme vybrat zástupce z této množiny. Dá se říct, že při počítání v $\mathbb{Z}_n$ jsme vlastně počítání modulo pěkně zabalili.
Další drobný rozdíl je v tom, že některé malé triky bychom při práci v $\mathbb{Z}_n$ vlastně neměli používat, ale ony se tam dají udělat neoficiálně, jak hned uvidíme.

Příklad 7a.f: Hledáme výsledek výrazu $(7 + 3 \cdot 5)^{18}$ modulo 8. Počítáme

$$(7 + 3 \cdot 5)^{18} = (7 + 15)^{18} \equiv (7 + 7)^{18} = 14^{18} \equiv 6^{18} \pmod 8.$$

Již jsme diskutovali, že mocninu 18 nahradit lepším zástupcem nelze, a přímý výpočet také není nejlepší strategie. O zbytku po dělení totiž rozhoduje i poslední cifra, jinými slovy není možné pracovat se zaokrouhlenými čísly, musíme znát všechny cifry. Tím se u vyšších mocnin vylučuje použití kalkulačky, protože tradičně vycházejí čísla delší, než kalkulačka dokáže udržet. Nezbývá než použít nějaký trik, velice populární je postupné odebírání malých mocnin z exponentu, které pak snadno vypočítáme. Běžná pravidla pro práci s exponenty totiž platí i obecně.

$$(7 + 3 \cdot 5)^{18} \equiv 6^{18} = 6^{2 \cdot 9} = (6^2)^9 = 36^9 \equiv 4^9 \pmod 8.$$

Teď už dvojku oddělit neumíme. Mohli bychom oddělit trojku a počítat $4^9 = (4^3)^3 = \ldots$, ale druhá mocnina je přece jen hezčí, tak použijeme jiný způsob odebírání z exponentu.

$$(7 + 3 \cdot 5)^{18} \equiv 4^9 = 4^1 4^8 = 4 \cdot (4^2)^4 = 4 \cdot 16^4 \equiv 4 \cdot 0^4 = 0 \pmod 8.$$

Pomocí těchto dvou druhů odebírání dokážeme i velice vysokou mocninu zredukovat bez větších problémů, jen to někdy chvíli trvá.

Tento výpočet se dá ovšem také interpretovat jako počítání v prostoru $\mathbb{Z}_8$, kde operace už v sobě zahrnují jak běžný výpočet, tak okamžitý přechod k ideálním kongruentním zástupcům:

$$(7 \oplus 3 \odot 5)^{18} = (7 \oplus 7)^{18} = 6^{18} = (6^2)^9 = (6 \odot 6)^9 = 4^9 = 4 \odot 4^8 = 4 \odot (4^2)^4 = 4 \odot (4 \odot 4)^4 = 4 \odot 0^4 = 0.$$

Vidíme, že se to od výpočtu modulo opravdu liší jen zápisem.

Zkušení výpočetníci by při práci v $\mathbb{Z}_n$ psali obyčejné plus a krát, ale my si v této kapitole musíme dávat pozor na teorii, tak si budeme speciálním značením připomínat, že používáme speciální operace z prostoru $\mathbb{Z}_n$. Je to o to důležitější, že se nám vlastně budou míchat tři druhy operací: obyčejné, výpočty modulo a výpočty v $\mathbb{Z}_n$, rozličné značení nám pomůže, ať v tom není zmatek.

Teď si ukážeme příklad, kde již rozdíl mezi počítáním modulo a počítáním v $\mathbb{Z}_n$ bude. Pokud budeme chtít spočítat $147 \cdot 148$ modulo 150, můžeme to provést takto:

$$147 \cdot 148 = 21756 \equiv 6 \pmod{150}.$$

Výpočet v $\mathbb{Z}_{150}$ by se dělal stejně, $147 \odot 148 = 21756 \bmod 150 = 6$.

Jenže při výpočtu modulo 150 můžeme zkusit ještě něco jiného, co celý výpočet výrazně zjednoduší:

$$147 \cdot 148 \equiv (-3) \cdot (-2) = 6.$$

A tento trik v $\mathbb{Z}_{150}$ udělat nelze, protože tam žádná záporná čísla neexistují. Ale to není problém, v takových případech si prostě na chvíli odskočíme do počítání modulo n a pak výsledek nahradíme kongruentním číslem ze $\mathbb{Z}_n$.

△

7a.7 Další operace v $\mathbb{Z}_n$: Odčítání.

Na první pohled by se zdálo, že s odčítáním v $\mathbb{Z}_n$ nebude problém. Nabízí se definice $a \ominus b = (a - b) \bmod n$ a ani prakticky to nevypadá špatně. Například bychom si tipli, že v prostoru $\mathbb{Z}_6$ máme $5 \ominus 3 = 2$, což potvrdí i zkouška: $2 \oplus 3 = 5$. Aby to bylo zajímavější, zkusíme si $2 \ominus 5 = -3 \bmod 6 = 3$ a zkouška nám opět vyjde: $3 \oplus 5 = 2$ v $\mathbb{Z}_6$.

Nicméně se to takto nedělá. Již jsme se zmínili, že odčítání se nebere jako jedna ze základních algebraických operací, mimo jiné proto, že nesplňuje některé věci, které považujeme za zásadní, například asociativní zákon. Ve skutečnosti se odečítání bere jako příjemná zkratka pro přičítání opačného prvku. Například opačný prvek k 5 je -5, namísto $3 + (-5)$ píšeme $3 - 5$.

Proto se odčítání nezavádí ani ve světě modulo jako samostatná operace, místo toho se vytvoří pojem opačného čísla. Protože v $\mathbb{Z}_n$ záporná čísla nejsou, musíme na to trochu jinak. Začneme otázkou, co je to vlastně opačné číslo, jak jej známe. Co mají společná čísla 5 a -5? To, že se navzájem vynulují, tedy $5 + (-5) = 0$. Přesně toto nám může fungovat i v $\mathbb{Z}_n$.

Podívejme se třeba do světa $\mathbb{Z}_6$. Dokážeme najít číslo opačné k 5 neboli číslo takové, že po přičtení k 5 dostaneme nulu? Podíváme-li se do tabulky v příkladě 7a.e, zjistíme, že $5 \oplus 1 = 0$. Zkusmo tedy prohlašme, že opačné číslo k 5 je 1 v $\mathbb{Z}_6$, psáno $(-5) = 1$ modulo 6. Letmý pohled na tabulku sčítání v $\mathbb{Z}_6$ odhalí, že opačné číslo lze najít ke všem prvkům $\mathbb{Z}_6$, což je slibný začátek, čtenář již dokonce asi tuší, jak se ta čísla hledají a že se najdou obdobnou metodou v každém $\mathbb{Z}_n$.

Dobrá otázka je, zda nám tato opačná čísla opravdu dokážou nahradit odčítání modulo. Před chvílí jsme zkusili spočítat $2 - 5$ modulo 6, vyšlo $-3 \equiv 3 \pmod 6$. Pokud budeme počítat v prostoru $\mathbb{Z}_6$, musíme přejít k přičtení opačného čísla: $2 \ominus 5 = 2 \oplus (-5) = 2 \oplus 1 = 3$. Funguje to.

To samozřejmě mohla být náhoda, ale není, jsme na správné cestě. Další povzbuzení nám dodá, když se na opačný prvek podíváme trochu jinou cestou. Říkali jsme si, že někdy se vyplatí ze $\mathbb{Z}_n$ vyskočit k počítání modulo, tam dostat výsledek a nahradit jej správným zástupcem ze Z_n. Opačné číslo k 5 je -5, to platí i modulo 6, teď najdeme správného zástupce čísla -5 modulo 6, což je 1, souhlasí.

Než se dáme do formálních definic, poznamenejme, že modulo je zde stále zásadní. Pokud bychom chtěli počítat $2 - 5$ v $\mathbb{Z}_7$, tak musíme použít opačný prvek k 5 vzhledem k modulu 7, což je evidentně jiné číslo než ta 1 ze světa modulo 6.

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

Diskuse před definicí naznačila, jak opačné prvky v prostorech $\mathbb{Z}_n$ hledat v praxi, pro dané $a \in \mathbb{Z}_n$ začneme s $-a$ a najdeme si jeho zástupce ze $\mathbb{Z}_n$, což je $(-a) + n = n - a$. Možná. Rozmyslete si, že to neplatí úplně vždy, pak čtěte dál.

Fakt 7a.8.
Nechť $n \in \mathbb{N}$.
(i) $(-0) = 0$.
(ii) Jestliže $a \in \mathbb{Z}_n$ a $a \neq 0$, pak $(-a) = n - a$.

Důkaz je snadný, necháme jej jako cvičení 7a.14.

S opačnými prvky jsme se setkali i při práci s běžnými čísly například při řešení rovnic.

Příklad 7a.g: Uvažujme rovnici $x \oplus 5 = 2$ v $\mathbb{Z}_6$. Kdyby to byla rovnice „normální“, tak bychom prostě od obou stran odečetli 5 neboli přičetli -5. V $\mathbb{Z}_6$ je to stejné, jen musíme hledat opačný prvek jinak. Víme už, že v $\mathbb{Z}_6$ je $(-5) = 6 - 5 = 1$, takže upravujeme:

$$x \oplus 5 = 2 \implies (x \oplus 5) \oplus 1 = 2 \oplus 1 \implies x \oplus (5 \oplus 1) = 3 \implies x \oplus 0 = 3 \implies x = 3.$$

Postup je delší, protože jsme schválně zdůraznili klíčové kroky při řešení. Viděli jsme tak, že toto řešení závisí na možnosti změnit pozici závorek na levé straně neboli na platnosti tzv. asociativního zákona. Jak víme, že v prostoru $\mathbb{Z}_6$ platí? To je dobrá otázka a brzy se k ní vrátíme.
△

7a.9 Další operace v $\mathbb{Z}_n$: Dělení.

Zde je obdobná situace jako u odčítání. U reálných čísel bychom výpočet $4/2$ přepsali jako $4 \cdot \frac{1}{2}$, kde souvislost mezi 2 a $\frac{1}{2}$ je zjevná, $2 \cdot \frac{1}{2} = 1$. Vztah $x \cdot \frac{1}{x} = 1$ lze zkoumat i ve světě $\mathbb{Z}_n$, třeba si můžeme všimnout, že $3 \cdot 7 = 1 \pmod{10}$, tudíž bychom ve světě $\mathbb{Z}_{10}$ mohli psát, že $\frac{1}{3} = 7$.

To se zase hodí třeba při řešení rovnic. V prostoru $\mathbb{Z}_{10}$ lze rovnici $3x = 4$ řešit tímto postupem:

$$3 \odot x = 4 \implies 3^{-1} \odot (3 \odot x) = 3^{-1} \odot 4 \implies (7 \odot 3) \odot x = 7 \odot 4 \implies 1 \odot x = 8 \implies x = 8.$$

Zkuste si ale rozmyslet, že k číslu 4 nenajdete žádné x, aby platilo $4 \cdot x = 1 \pmod{10}$, stačí projít všechna čísla 0 až 9 a vyloučit je. To ukazuje, že tentokráte bude situace poněkud jiná než u opačných čísel.

Definice.
Uvažujme $n \in \mathbb{N}$.
Nechť $a \in \mathbb{Z}$. Řekneme, že $b \in \mathbb{Z}$ je **inverzní prvek** (**inverse element**) k a **modulo** n, jestliže $a \cdot b \equiv 1 \pmod{n}$.
Nechť $a \in \mathbb{Z}_n$. Řekneme, že $b \in \mathbb{Z}_n$ je **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**) modulo n, resp. v $\mathbb{Z}_n$.

Jako obvykle platí, že nalezený inverzní prvek v $\mathbb{Z}_n$ již dává inverzní prvek modulo n dle první definice, naopak libovolný inverzní prvek modulo n nám okamžitě dá i inverzní prvek z prostoru $\mathbb{Z}_n$, když jej nahradíme vhodným kongruentním zástupcem. Jde tedy opět o stejnou myšlenku, jen trochu jinak oblečenou.

Podobně jako u opačného prvku, i zde na modulu záleží, například v $\mathbb{Z}_{10}$ jsme uhodli $3^{-1} = 7$, ale v $\mathbb{Z}_8$ již je $3^{-1} = 3$ (ověřte). A stejně jako u opačného prvku se modulo ze značení nepozná, což je ze striktně matematického pohledu nešťastné, ale z praktického pohledu to zase takový problém není, protože používané modulo je vždy jasné z kontextu, prakticky nikdy nepracujeme s více moduly najednou.

V této chvíli čtenáři doporučíme, aby si přečetl kapitolu 8, přinejmenším část 8a. Pochopí, proč byla u definice opačného prvku zrovna nula a u invezního zrovna jednička, a vůbec celou tuto partii uvidí v trochu jiném světle.

Invertibilní a inverzní prvky jsou velice užitečné a musíme se je naučit hledat, příklad výše ovšem ukazuje, že někdy to je nemožné. To vlastně není nic nového, v prostoru $\mathbb{R}$ také neumíme najít inverzní prvek k nule, ale v $\mathbb{Z}_n$ těchto nepříjemných situací může být víc.

Příklad 7a.h: Podíváme se na několik tabulek násobení v zajímavých $\mathbb{Z}_n$. Prvky, které mají inverzi (jsou invertibilní), poznáme podle toho, že se v jejich řádku vyskytne výsledek jedna, v příslušném sloupci pak nahoře dohledáme onen inverzní prvek.

Nejprve si připomeneme případ $(\mathbb{Z}_6, \odot)$.

$\odot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Zde vidíme, že jediné invertibilní prvky jsou 1 a 5, platí $1^{-1} = 1$ a $5^{-1} = 5$.
Zato tu máme „dělitele nuly“, třeba $2 \odot 3 = 0$ či $3 \odot 4 = 0$.
Na to nejsme zvyklí a má to zase dopady na řešení rovnic. Zatímco v $\mathbb{Z}$ (a v $\mathbb{R}$ atd.) má rovnice $2x = 0$ automaticky jediné řešení $x = 0$, v $\mathbb{Z}_6$ už je i řešení $x = 3$. Z toho někdy plynou zajímavé komplikace.

Toto byl asi extrémně pesimistický případ. Teď si ukážeme naopak nejlepší možný případ, zastoupený příkladem $(\mathbb{Z}_5, \odot)$.

$\odot$	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

Vidíme, že v $\mathbb{Z}_5$ jsou všechny prvky kromě nuly invertibilní, máme $1^{-1} = 1$, $2^{-1} = 3$ a $3^{-1} = 2$ neboť $2 \odot 3 = 1$, $4^{-1} = 4$ neboť $4 \odot 4 = 1$.
Zde by tedy mnohé věci měly fungovat dost podobně jako ve světě reálných čísel a dokonce někdy lépe než ve světě $\mathbb{Z}$. Například rovnici $3x = 4$ nedokážeme ve světě $\mathbb{Z}$ vyřešit, zatímco v $\mathbb{Z}_5$ stačí rovnici vynásobit číslem $3^{-1} = 2$ a dostáváme $x = 3$, což je opravdu řešení dané rovnice.
Jen pro úplnost, $(-0) = 0$, $(-1) = 4$, $(-2) = 3$, $(-3) = 2$ a $(-4) = 1$.

Na takovéto výrazně příjemné případy se brzy podíváme blíže. Typický prostor $\mathbb{Z}_n$ je nicméně někde mezi právě předvedenými extrémy, pěkně to ukazuje třeba $\mathbb{Z}_{14}$.

$\odot$	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 $13^{-1} = 13$.

△

Jak se pozná, které prvky v $\mathbb{Z}_n$ jsou invertibilní? Pokud vám příklady nenapověděly, tady je odpověď. Opět poskytneme dvě verze, jednu pro počítání modulo a jednu pro počítání v prostoru $\mathbb{Z}_n$, jako obvykle půjde o stejnou věc, jen jinak vyjádřenou.

! **Věta 7a.10.**
Nechť $n \in \mathbb{N}$.
(i) Nechť $a \in \mathbb{Z}$. Existuje $x \in \mathbb{Z}$ takové, že $ax \equiv 1 \pmod{n}$, právě tehdy, když $\gcd(a, n) = 1$.
Pak je toto x určeno jednoznačně až na modulo n a všechna y s x kongruentní také splňují $ay \equiv 1 \pmod{n}$.
(ii) Nechť $a \in \mathbb{Z}_n$. Inverzní prvek a^{-1} v $\mathbb{Z}_n$ existuje právě tehdy, když $\gcd(a, n) = 1$. Pak je tento prvek jediný.

Důkaz (poučný)**:** (i): 1) Takové x existuje právě tehdy, když existuje $k \in \mathbb{Z}$ takové, že $1 - ax = kn$. Jinými slovy, nalezení prvku x je ekvivalentní tomu, že umíme najít řešení $x, k \in \mathbb{Z}$ rovnice $1 = ax + kn$. To je ale diofantická rovnice, kterou jsme se už naučili řešit, a podle Věty 6c.1 to lze právě tehdy, když je 1 násobkem $\gcd(a, n)$. Takže řešení existuje právě tehdy, když $\gcd(a, n) = 1$. Důkaz ekvivalence je hotov.

2) Jednoznačnost: Nechť $x, y \in \mathbb{Z}$ obě splňují dotyčnou podmínku. Pak existují $k, l \in \mathbb{Z}$ takové, že $1 = ax + kn$ a $1 = ay + ln$. Odečtením získáme $ax - ay = kn - ln$, tedy $a(x - y) = (k - l)n$. To znamená, že n dělí $a(x - y)$, a protože je n nesoudělné s a, musí podle Lemma 6a.23 n dělit $x - y$, tedy $x \equiv y \pmod{n}$.

3) $y \equiv x \bmod n$ dává $k \in \mathbb{Z}$ tak, aby $y = x + kn$. Pak $ay = a(x + kn) = ax + (ak)n \equiv 1 + 0 = 1 \pmod{n}$, použili jsme Fakt 7a.2 (ii) na násobek $(ak)n$.

(ii): Číslo $x \in \mathbb{Z}_n$ splňuje $a \odot x = 1$ právě tehdy, když $ax \bmod n = 1$, což je právě tehdy, když $ax \equiv 1 \pmod{n}$, což je podle (i) právě tehdy, když $\gcd(a, n) = 1$.

Jednoznačnost plyne buď z (i), nebo také z Faktu 8a.5.

□

Vlastně jsme v bodě (i) dokázali, že jakmile je nějaký prvek a invertibilní modulo n, tak množina všech jeho inverzních čísel je přesně množina všech čísel kongruentních s nějakým konkrétním inverzním číslem x.

Už umíme poznat, kdy a^{-1} existuje, ale jak jej najdeme? Úplně snadné to není, žádný vzoreček totiž neexistuje. Jediný rozumný postup vychází z důkazu Věty 7a.10, přes řešení příslušné diofantické rovnice. Na to máme Algoritmus 6c.6, postup lze ale zjednodušit, protože teď nás vlastně jedna neznámá nezajímá.

S **Algoritmus 7a.11.** pro hledání inverzního prvku k a vzhledem k násobení modulo n, popřípadě pro hledání inverzního prvku k a v $\mathbb{Z}_n$.
0. Například pomocí rozšířeného Euklidova algoritmu najděte $\gcd(a,n) = Aa + Bn$.
1. Jestliže $\gcd(a,n) > 1$, pak inverzní prvek k a v $\mathbb{Z}_n$ neexistuje.
Pokud umíte $\gcd(a,n)$ získat snadněji než Euklidovým algoritmem (třeba pohledem) a vyjde číslo větší než 1, je možné krok **0** přeskočit.
2. Jestliže $\gcd(a,n) = 1$, pak Bezoutova identita dává $1 = a \cdot A + B \cdot n$. To znamená, že $a \cdot A \equiv 1 \bmod n$ a $x = A$ je hledaný inverzní prvek.
Pokud hledáte inverzní prvek v $\mathbb{Z}_n$, pak najděte vhodného zástupce x z rozmezí $1, 2, \ldots, n-1$ buď přičtením/odečtením vhodného násobku n, nebo dělením se zbytkem.
△

! **Příklad 7a.i:** Najdeme inverzní prvek k $a = 36$ modulo 175.

Nejprve si to přeložíme: Hledáme x splňující $36x \equiv 1 \pmod{175}$ neboli x takové, aby pro nějaké $m \in \mathbb{Z}$ bylo $36x + 175m = 1$.

Není jasné, zda vidíme bez větší práce, kolik je $\gcd(36, 175)$, tak rovnou zkusíme rozšířený Euklidův algoritmus pro jeho nalezení.

175		1	0
36	4	0	1
31	1	1	-4
5	6	-1	5
1•	5	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 $36 \cdot (-34) + 0 \cdot 7 \equiv 1$, tedy $36 \cdot (-34) \equiv 1 \pmod{175}$. Proto $36^{-1} = -34$ vzhledem k počítání modulo 175.

Čtenář si samořejmě může vybrat i jiného zástupce dle osobní preference, například $-34 \equiv 316 \pmod{175}$.

Pokud bychom hledali inverzní prvek k 36 v $\mathbb{Z}_{175}$, pak bychom také nejprve přeložili zadání: Hledáme x splňující $36 \odot x = 1$ neboli $36x \equiv 1 \pmod{175}$ neboli $36x + 175m = 1$ pro nějaké $m \in \mathbb{Z}$.

Pak bychom postupovali stejně jako výše, ale na konci bychom pro -34 museli najít zástupce ze $\mathbb{Z}_{175}$, nejsnáze přičtením čísla 175.

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

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

△

Všimněte si, že pokud je n prvočíslo, tak vlastně všechny nenulové prvky $\mathbb{Z}_n$ jsou nesoudělné s n a tudíž mají inverzi. To už je jako u reálných čísel. V mnoha aplikacích skutečně úspěšně nahrazujeme svět $\mathbb{R}$ světem $\mathbb{Z}_p$ pro p prvočíslo.

Teď si ukážeme jednu zajímavou aplikaci počítání modulo.

! **Příklad 7a.j:** Úzký vztah mezi kryptografií a počítáním modulo jde zpět minimálně ke starým Římanům. Takzvanou Césarovu šifru si 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, namísto A píšeme D, namísto B píšeme E a tak dále, třeba Y přejde na B.

Matematicky se to simuluje jednoduše, nahradíme písmena čísly $1, \ldots, 26$ a pak používáme jako šifru bijekci $T(a) = (a+3) \bmod 26$.

Obecně lze posouvat i o jiné číslo než o tu Césarovu trojku. Zvolíme si nějaké k mezi 1 a 25 a dostáváme „šifrování posunem“: $T(a) = (a+k) \bmod 26$. Toto se snadno dešifruje, $T^{-1}(b) = (b-k) \bmod 26$, a pokud nechceme odečítat, tak si najdeme opačný prvek $(-k)$ a máme $T^{-1}(b) = (b + (-k)) \bmod 26$.

Například pokud zvolíme číslo $k = 8$, tak písmeno 20 zašifrujeme jako $T(20) = (20+8) \bmod 26 = 28 \bmod 26 = 2$. Opačný prvek ke $k = 8$ modulo 26 je 18 (zkouška: $8 + 18 = 26 \equiv 0 \pmod{26}$), proto bychom se posunem o 18 měli zase dostat zpět: $T^{-1}(2) = (2 + 18) \bmod 26 = 20 \bmod 26 = 20$. Zajímavá volba je $k = 13$, pak $T^{-1} = T$.

Tato šifra není příliš bezpečná. Protože se dané písmeno vždy kóduje stejně, je vysoce náchylná na frekvenční analýzu, kdy si prostě spočítáme, které písmeno 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*.

Lépe vypadá šifrování dané předpisem $T(a) = (ea + k) \bmod 26$, kde e je zvoleno tak, aby T bylo prosté (tedy je třeba zvolit něco nesoudělného s 26). Jak se takový vzkaz dekóduje? Zvolili jsme e nesoudělné s 26, pak už víme (Věta 7a.10), že k němu existuje inverzní prvek d modulo 26, tedy prvek splňující $ed \bmod 26 = 1$. Ukážeme, že $T^{-1}(b) = d(b + (-k))$ dekóduje zprávu:

$$T^{-1}(T(a)) = d(T(a) + (-k)) \equiv d((ea + k) + (-k)) \equiv d(ea + 0) = (de)a \equiv 1 \cdot a = a \pmod{26}.$$

Zvolme třeba $e = 7$ a $k = 3$. Pak $-k = 23$ a ještě potřebujeme vyřešit rovnici $7x + 26m = 1$, buď algoritmem nebo to zkusíme uhádnout. Vyjde například $x = -11$ a $m = 3$, nás zajímá x, ale z prostoru $\mathbb{Z}_{26}$, dostáváme tedy $d = 15$.

Teď zakódujeme třeba písmeno B odpovídající hodnotě $a = 2$, takže vyšleme zprávu $T(2) = 7{\cdot}2{+}3 \mod 26 = 17$ neboli písmeno Q. Příjemce na zprávu aplikuje T^{-1}:

$$T^{-1}(17) = 15(17 + 23) = 15 \cdot 40 \equiv 15 \cdot 14 = 210 \equiv 2 \pmod{26}.$$

Vyšlo to.

Ale lépe tato šifra jen vypadá, pořád je to dětská šifra zranitelná přes frekvenční analýzu. Zajímavé zobecnění je použít modulární aritmetiku na bloky číslic, nikoliv jednotlivé číslice, tam už frekvence nepomohou. Přesto jsou ale šifry tohoto typu pořád zranitelné díky své pravidelnosti. K lepším šifrám se dostaneme brzy.

△

Problém inverzních prvků jsme vyřešili tak dobře, jak jen to jde. Vrátíme se ještě k problematice umocňování. Sice jsme vyvinuli metodu postupné redukce exponentu, ale počítat tak třeba 13^{1946} modulo 17 nezní moc lákavě. Pokud je n prvočíslo (a už víme, že to je velice příjemný případ), naskýtá se ještě jiná zajímavá metoda snižování mocniny.

! **Věta 7a.12.** (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 $a \in \mathbb{Z}$ pak platí $a^n \equiv a \pmod{n}$.

Důkaz (poučný)**:** (i) Nejprve ukážeme, že čísla a, $2a$, ... , $(n-1)a$ 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 6a.23) n dělí $i - j$. Nicméně $|i - j| < n$, proto $i - j = 0$, tedy $ia = ja$.

Když tedy vezmeme $a, 2a, \dots, (n-1)a$ modulo n, dostaneme v nějakém pořadí všechna čísla $1, 2, \dots, n-1$. Když je všechny spolu vynásobíme, což lze psát jako $\prod_{i=1}^{n-1} (ia) \bmod n$, dostaneme $(n-1)!$. Upravením toho součinu máme $(n-1)! \equiv a^{n-1}(n-1)! \pmod{n}$. Protože $\gcd((n-1)!, n) = 1$, je prvek $(n-1)!$ invertibilní v $\mathbb{Z}_n$, proto vynásobením obou stran kongruence jeho inverzí dostaneme $1 \equiv a^{n-1} \pmod{n}$.

(ii) Nechť $a \in \mathbb{Z}$, rozebereme dva případy. Jestliže $\gcd(a, n) = 1$, tak lze aplikovat a) a dostaneme $a^{n-1} \equiv 1 \pmod{n}$, takže podle Věty 7a.3 (iii) je $a^n = a \cdot a^{n-1} \equiv a \cdot 1 = a \pmod{n}$.

Jestliže $\gcd(a, n) > 1$, pak existuje společný dělitel $d > 1$. Jenže n je prvočíslo, takže jediný jeho dělitel (kromě 1) je $d = n$. Takže vlastně $n \mid a$, pak $a \equiv 0 \pmod{n}$, tedy podle Faktu 7a.6 $a^n \equiv 0^n = 0 = a \pmod{n}$.

□

Alternativní důkaz se najde jako Poznámka 7a.21.

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 praktických výpočtech užitečnější. Proto všichni za „malou Fermatovu větu“ považují tvrzení (i), budeme to tak dělat i my.

! **Příklad 7a.k:** Spočítáme 136^{182} modulo 13. Nejprve použijeme nahrazení v základu: $136^{182} \equiv 6^{182} \pmod{13}$. Poznamenejme, že číslo 6^{182} má 142 cifer, takže by nám v této fázi kalkulačka rozhodně nepomohla. Musíme redukovat exponent, a protože je 13 prvočíslo, můžeme na to použít malého Fermata. Na to si tam ale musíme vyrobit mocninu $13 - 1 = 12$, což je snadné, $6^{182} = 6^{12 \cdot 15 + 2}$. Podle malé Fermatovy věty pak máme $6^{12} \equiv 1 \pmod{13}$, tedy

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

Je to rozhodně lepší, než snižování mocniny po dvou, což by vypadalo nějak takto:

$$6^{182} = (6^2)^{91} \equiv 10 \cdot 10^{90} = 10 \cdot (10^2)^{45} \equiv 10 \cdot 9 \cdot 9^{44} = \dots$$

Chytřejší by bylo použít $10 \equiv -3 \pmod{13}$ a při umocňování na sudý exponent se dá znaménko ignorovat, tedy

$$6^{182} = (6^2)^{91} \equiv 10 \cdot (-3)^{90} = 10 \cdot (3^2)^{45} = 10 \cdot 9 \cdot 9^{44} \equiv 10 \cdot 9 \cdot (-4)^{44} = \dots$$

I tak by to bylo na dlouhé zimní večery, ten Fermat byl výrazně kratší.

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

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

Čekala nás další práce, ta jednička coby výsledek u verze (i) je příjemnější.

△

Pro další podobný příklad a poznámku s úderným trikem viz příklad 7a.o.

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

Fakt 7a.13.
Nechť $n \in \mathbb{N}$ je prvočíslo a $a \in \mathbb{Z}$ není dělitelné n. Pak pro každé $k \in \mathbb{N}_0$ platí $a^k \equiv a^r \pmod{n}$, kde $r = k \bmod (n-1)$ neboli zbytek po dělení k číslem $n-1$.

V zásadě se dá říct, že už ve světě $\mathbb{Z}_n$ umíme počítat. Teď se podíváme na další aplikaci.

Příklad 7a.l (pokračování 7a.j)**:** Vrátíme se k problému šifrování. Pro zjednodušení každou zprávu převedeme na jedno číslo v zásadě libovolným způsobem, třeba se rozhodneme, že každé písmeno ze zprávy nahradíme dvoučíslím od 00 do 26 a dáme je za sebe. Chceme tedy vytvořit metodu, která umí kódovat celá čísla.

Jako inspiraci si představme následující kód. Zvolíme $e \in \mathbb{N}$. Zprávu $M \in \mathbb{N}$ zašifrujeme jako $T(M) = M^e$. Jak se dostaneme k původnímu textu? Zobrazením $T^{-1}(C) = \sqrt[e]{C}$. Tato šifra je již výrazně lepší než predchozí pokusy, protože se maskují frekvence a má obecně méně vnitřních pravidelností, čímž se protivníkovi ztěžuje protiútok.

Její nevýhodou je, že výpočet mocniny i odmocniny je velice náročná operace, zejména výpočet odmocniny znamená, že metoda je v praxi nepoužitelná. Proto si teď nápad vylepšíme.

Zvolíme nějaké prvočíslo n strašlivě velké, aby byly zprávy vždy o hodně menší (dlouhé zprávy můžeme sekat). Zvolme libovolné číslo $e \in \mathbb{N}$ nesoudělné s $n-1$, pak podle Věty 7a.10 existuje také $d \in \mathbb{N}$ takové, že $de \equiv 1 \pmod{n-1}$, tedy $ed = 1 + k(n-1)$ pro nějaké $k \in \mathbb{Z}$. Máme pak k dispozici následující způsob šifrování.

Předpokládejme, že M je zpráva splňující $M < n$. Zakódujeme ji zobrazením $T(M) = M^e \pmod{n}$ (proto jsme volili zkratku e jako „encode“). Jak se dělá dešifrování? Tvrdíme, že to dělá zobrazení $T^{-1}(C) = C^d \pmod{n}$ (proto d jako „decode“). Důkaz plyne z malé Fermatovy věty, zde je dobré si uvědomit, že n je prvočíslo, proto jej číslo $1 < M < n$ nemůže dělit a jsou tedy nesoudělná. Máme pak (počítáme modulo n)

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

A je to. Nemusíme odmocňovat, navíc na mocnění modulo máme pěkné triky. Největší slabina této metody je v praktickém provedení, což je mimochodem velkou slabinou většiny šifrovacích schémat. Odesílatel musí nějak dopravit dekódovací klíč d příjemci zprávy, jakákoliv cesta je zranitelná a hrozí tak nebezpečí, že si naši zprávu někdo po zachycení klíče přečte.

Šifra je zranitelná i opačným směrem. Řekněme, že chceme, aby nám někdo poslal tajnou zprávu. Pošleme mu šifrovací klíč e a číslo n nutné k operaci modulo, sami si schováme dešifrovací klíč d. Jenže pokud někdo naši zprávu odesílateli zachytí, tak si z hodnot e a n hravě náš dešifrovací klíč d spočítá, protože najít inverzi k e modulo $n-1$ je pro rozšířeného Euklida relativně snadný úkol.

Výrazné zvýšení bezpečnosti se dá dosáhnout, pokud nějakou fintou znemožníme, aby odposlouchávač dokázal z hodnot e a n odvodit náš dešifrovací klíč d. Tím se dostáváme ke zlatému hřebu naší procházky kódováním.

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 i dříve, ale patrně nebyl použit). Na začátku zvolíme dvě prvočísla p, q (typicky o 200 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).

Kódování: Zprávu $M \in \mathbb{N}$ splňující $M < p, q$ zašifrujeme 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

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

Číslo q má ovšem stejné vlastnosti, proto stejně ukážeme $(M^e)^d \equiv M \pmod{q}$. Podle Cvičení 7a.16 tudíž musí platit $(M^e)^d \equiv M \pmod{\operatorname{lcm}(p,q)}$, a protože jsou p, q coby různá prvočísla nesoudělná, máme dle Cvičení 6a.15 také $(M^e)^d \equiv M \pmod{n}$. Tím jsme dokázali, že ze zprávy M^e dalším umocněním na d a přechodem ke zbytku po dělení modulo n dostáváme původní text M.

Jak bezpečná je tato metoda? Aby zprávu někdo rozšifroval, musel by najít d, k tomu ale potřebuje znát $(p-1)(q-1)$. Takže RSA kód je tak bezpečný, jako je číslo $(p-1)(q-1)$. To se dá získat jedině nalezením příslušné faktorizace n na $p \cdot q$, což už jsme zde několikrát zmiňovali jako pořádný problém. Existují efektivní metody pro určité kombinace, například když jsou p, q dosti blízké nebo když je d relativně malé číslo, ale pro dobře vybrané p, q se odhadovaný čas faktorizace blíží tomu nejhoršímu scénáři, náročnost faktorizačních algoritmů je horší než mocniny, patří do skupiny a^n, což už je hodně (viz kapitola 9b).

Mimochodem, pokud bychom prozradili zároveň n a $m = (p-1)(q-1)$, tak už nejen může kdokoliv zjistit e 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. Například z druhé rovnice vyjádříme q, dáme do první a dostáváme $p^2 - (n - m + 1)p + n = 0$.

△

Máme tedy kvalitní kódování, ale také nový problém: Kde vezmeme prvočísla o 200 cifrách?

Příklad 7a.m: Zde se vrátíme k problému, jak poznat, zda je nějaké $n \in \mathbb{N}$ prvočíslo. Již jsme diskutovali, že zkoušet dělit čísly mezi 1 a $\sqrt{n}$ je extrémně časově náročné, je načase zapřemýšlet nad lepšími alternativami.

Malá Fermatova věta nabízí následující zajímavou obměnu:

Jestliže jsou čísla $a \in \mathbb{Z}$ a n nesoudělná a neplatí $a^{n-1} \equiv 1 \pmod{n}$, pak už n nemůže být prvočíslo.

Toto může sloužit jako test prvočíselnosti. Vezměme libovolné liché $n > 2$, chceme vědět, zda je to prvočíslo. použijeme $a = 2$, protože pro liché číslo určitě $\gcd(2, n) = 1$. Jestliže $2^{n-1} \not\equiv 1 \pmod{n}$, pak podle malé Fermatovy věty n určitě není prvočíslo.

Bohužel, malá Fermatova věta je jen implikace. Takže pokud by platilo $2^{n-1} \equiv 1 \pmod{n}$, pak n prvočíslo být může, ale nemusí. Jsou zvláštní čísla, která $2^{n-1} \equiv 1 \pmod{n}$ splňují, ale jsou složená, říkáme jim **pseudoprvočísla**. Dobrá zpráva je, že pseudoprvočísel je velice málo, například mezi prvními 10^{10} přirozenými čísly je cca 450,000,000 prvočísel, ale jen cca 15,000 pseudoprvočísel. To znamená, že tento test je vysoce účinný při vyřazování čísel, která prvočísly nejsou, a pokud už nějaké n tímto testem projde, tak je vysoká pravděpodobnost, že jsme opravdu ulovili prvočíslo, a vyplatí se investovat další námahu na skutečné potvrzení této skutečnosti.

Tato myšlenka se dá samozřejmě rozvést dále. Řekneme, že n je pseudoprvočíslo vzhledem k základu a, jestliže $a^{n-1} \equiv 1 \pmod{n}$. Takže pokud nějaké pseudoprvočíslo přežije první test, zvolíme nějaké nesoudělné a, například další prvočíslo $a = 3$, a zkusíme, zda neplatí $a^{n-1} \equiv 1 \pmod{n}$. To při troše štěstí zase vyřadí neprvočíslo.

Řekneme, že n je Carmichaelovské číslo, jestliže $a^{n-1} \equiv 1 \pmod{n}$ pro všechna $a \in \mathbb{N}$ s $\gcd(a, n) = 1$. Např. 561 je takové číslo. Těchto je sice nekonečně mnoho, ale zase hrozně málo, čili když začneme s n a protestujeme jej pro hodně a, tak v případě úspěchu už je skoro jisté, že n je prvočíslo.

Je to dobrá strategie pro hledání velkých prvočísel, například pro kódování RSA. Dělá se to tak, že si prostě zvolíme nějaké vhodně dlouhé číslo (liché a nekončící pětkou, samozřejmě). Testovat přímo dělením, zda je to prvočíslo, by trvalo strašně dlouho (mluvíme zde o desítkách let na těch nejvýkonnějších počítačích). Místo toho jej rychle proženeme testy popsanými výše a ono asi vypadne jako složené číslo. Tak zkusíme jiné velké číslo (třeba přičteme 2 k tomu neúspěšnému) a jedeme znovu. Nakonec nějaké číslo těmi testy projde, pak je téměř jisté, že je to prvočíslo. Tak prostě z takového čísla zkusíme RSA kódování udělat, zkusmo něco zakódujeme a rozkódujeme a pokud to vyjde, tak jsme našli, co jsme potřebovali.

△

7a.14 Poznámka (kritéria dělitelnosti): V kapitole 6 jsme se zmínili o existenci kritérií dělitelnosti, ale pořádně se na ně podíváme až zde, protože počítání modulo občas nabídne pohodlný zápis. Využijeme pak toho, že n dělí a právě tehdy, pokud $a \equiv 0 \pmod{n}$. Známá kritéria se dají rozdělit do skupin podle toho, z jaké myšlenky vycházejí. Ukážeme si několik populárních myšlenek, obvykle nejprve na kritériu známém a pak se pokusíme zjistit něco o dělitelnosti sedmičkou.

Jedna skupina kritérií vychází z toho, že si dané číslo a napíšeme jako $a = 100A + r$, kde $r = a \bmod 100$. Při pohledu vzhledem k počítání modulo d občas objevíme zajímavé věci. Jako ukázku dokážeme kritérium dělitelnosti čtyřkou, viz 6a.11. Modulo 4 totiž máme

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

Vidíme, že $a \equiv 0 \pmod 4$ právě tehdy, když $r \equiv 0 \pmod 4$, jinak řečeno, číslo a je dělitelné čtyřkou právě tehdy, když je čtyřkou dělitelné r neboli poslední dvojčíslí čísla a. Podobně se dokazuje kritérium pro $d = 25$, pomocí rozpisu $a = 10A + r$ takto snadno dokážeme kritérium pro dělitelnost dvojkou nebo pětkou.

Co dostaneme, když počítáme modulo 7? $a = 10A + r \equiv 3A + r$. Chceme-li tedy vědět, zda je číslo dělitelné sedmičkou, oddělíme poslední cifru a přičteme ji k trojnásobku „začátku“, pak otestujeme nové. To zní pěkně, ale je to pracné. Pokud bychom potřebovali znát dělitelnost čísla $a = 87654$, toto kritérium nabízí testovat místo toho číslo $3 \cdot 8765 + 4$, to se mi ani nechce počítat. Je to ale východisko k zajímavému algoritmu. Číslo se dá totiž probírat principem $10x + y \mapsto 3x + y$ postupně zleva (detaily raději vynecháme), čímž vznikne tento postup:

• 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.

Další populární rodinka kritérií vychází z dekadického rozvoje čísla. Jako inspiraci si 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 ciferný součet. Podobný důkaz ukáže i známá kritéria pro dělitelnost devíti a jedenácti. 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.

Lepší trik dostaneme, když dané číslo nebudeme dělit na cifry, ale na větší skupiny cifer. Dvojice ještě moc nepomohou, vedou na $a \equiv \sum (a_k \bmod 7) \cdot 2^k \pmod 7$. Když dané číslo rozložíme na trojčíslí, $a = \sum_k a_k 1000^k$, dostáváme modulo 7 rovnost

$$a \equiv \sum (a_k \bmod 7) \cdot (1000 \bmod 7)^k = \sum (a_k \bmod 7) \cdot (-1)^k \pmod 7.$$

Chceme-li tedy vědět, zda je číslo a dělitelné sedmi, tak místo toho můžeme testovat číslo vytvořené takto: první trojčíslí zprava nahradíme zbytkem po dělení sedmi a vezmeme se znaménkem plus. Od toho odečteme zbytek po dělení druhého trojčíslí zprava sedmi. K tomu přičteme zbytek po dělení třetího trojčíslí zprava sedmi atd. V případě $a = 87654$ bychom místo toho testovali číslo $(654 \bmod 7) - (87 \bmod 7) = 3 - 3 = 0$, to je dělitelné sedmi a potvrzujeme nezávisle, že 87654 je dělitelné sedmičkou.

Asi nejpoužívanější kritérium pro dělitelnost sedmi vypadá ještě jinak. Zapišme zase $a = 10A + r$. Tvrdíme, že je dělitelné sedmi právě tehdy, pokud je sedmi dělitelné číslo $A - 2r$. Důkaz by vypadal třeba takto. Protože je 2 nesoudělná se sedmi, pak má číslo $2a$ stejnou dělitelnost sedmi jako a. Když od čísla odečteme násobek sedmičky, také jeho dělitelnost sedmi nezměníme, takže číslo $2a - 21A = 2r - A$ má zase stejnou dělitelnost jako a. Z praktického důvodu je pak lepší ještě změnit znaménko.

Obvyklá ukázka: 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.

Toto kritérium má obdobu i pro dělitelnost třinácti, sedmnácti a podobně, tak si ukážeme obecný mustr.

Odvodíme kritérium pro dělitelnost $a = 10A + r$ číslem $d \in \mathbb{N}$. Začneme tím, že najdeme číslo c tak, aby bylo nesoudělné s d, ale aby d dělilo $10c + 1$. Díky nesoudělnosti víme, že $d \mid a$ 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 $A - cr$.

Volba $c = 2$ dá již výše zmíněné kritérium pro sedmičku, $c = -4$ zase vede na kritérium pro třináctku a podobně.

Poněkud jednodušší a známá kritéria připomínáme ve cvičení 7a.4.

△

7a.15 Strukturální teoretický pohled na počítání modulo

Existují dva pohledy na svět zvaný $\mathbb{Z}_n$, každý má své výhody a nevýhody a autoři si volí ten, který se jim lépe hodí do koncepce knihy. Zatím jsme představili definici, která je praktičtější, dá se říct, že pokud člověk počítání modulo používá při práci, tak je tento pohled na $\mathbb{Z}_n$ ten pravý.

Existuje ještě pohled jiný, který je teoretičtější (pro mnohé zbytečně), ale zase toho o množině $\mathbb{Z}_n$ více řekne, občas ušetří trochu práce a přednost mu dávají autoři, kteří se na $\mathbb{Z}_n$ dívají jako na zajímavou matematickou strukturu. Teď si jej představíme, myslím, že pro pokročilejšího čtenáře to může být zajímavá alternativa, ale pro ty, kteří mají méně vyvinutý smysl pro abstrakci, to může být spíš matoucí. Pokud by čtenář při četbě začínal mít pocit, že se topí (pokud jej už tedy nemá), nic se nestane, když skočí buď k Eulerově větě 7a.22, nebo dokonce rovnou na cvičení. Přesto doporučuji, aby se alespoň zastavil u Věty 7a.19.

Jdeme na to.

! **Fakt 7a.16.**
Pro každé $n \in \mathbb{N}$ je relace „být kongruentní modulo n“ ekvivalence na $\mathbb{Z}$.

Důkaz (rutinní)**:** Reflexivitu a symetrii necháme jako cvičení 7a.31, zde ukážeme tranzitivitu.

Jestliže $a \equiv b \pmod n$ a $b \equiv c \pmod n$, pak $a = b + kn$ pro nějaké $k \in \mathbb{Z}$ a $b = c + ln$ pro nějaké $l \in \mathbb{Z}$. Odtud $a = c + (k + l)n$ a $(k + l) \in \mathbb{Z}$, tedy $a \equiv c \pmod n$.

□

Můžeme teď aplikovat teorii z kapitoly 4a a vidíme, že se nám množina $\mathbb{Z}$ rozpadne na třídy ekvivalence, kterým říkáme **zbytkové třídy**. Zbytkovou třídu čísla a vzhledem k relaci kongruence modulo n budeme značit $[a]_n$.

Například při volbě $n = 4$ máme třeba $[1]_4 = [5]_4 = [-3]_4 = \cdots = \{\dots, -7, -3, 1, 5, 9, \dots\}$. Obecně samozřejmě $[a]_n = \{a + kn;\ k \in \mathbb{Z}\}$, mimo jiné vždy $a \in [a]_n$. Výsledky z kapitoly 4a říkají, že je úplně jedno, kterého zástupce si vybereme, také víme, že $[a]_n = [b]_n$ právě tehdy, když $a \equiv b \pmod n$ neboli když dají stejný zbytek při dělení n neboli když je $a - b$ dělitelné n neboli když se od a k b dokážeme dostat opakovaným přičítáním/odčítáním n.

Množina $\mathbb{Z}$ se nám rozpadla na přesně n zbytkových tříd, čímž nám vznikl nový objekt, množina těchto zbytkových tříd. Naším cílem je s touto množinou normálně pracovat, tedy brát zbytkové třídy jako objekty, se kterými normálně manipulujeme, jako jsme to zvyklí dělat s čísly. To je oblíbená matematická věc, vezme se nějaký třeba i dosti komplikovaný objekt (v našem případě nekonečná množina navzájem kongruentních čísel) a ten se vhodně zabalí a označí písmenkem, takže se navenek tváří jako nějaká obyčejná věc, se kterou pak v pohodě manipulujeme pomocí odvozených pravidel.

V tomto případě bychom se zbytkovými třídami rádi prováděli běžné algebraické operace. K tomu využijeme, že na každou zbytkovou třídu se lze odvolat nějakým zástupcem. Je čas zadefinovat hlavní pojmy.

! **Definice.**
Prostor $\mathbb{Z}_n$ definujeme jako množinu všech tříd ekvivalence v $\mathbb{Z}$ vzhledem k relaci být kongruentní modulo n, tedy $\mathbb{Z}_n = \{[a]_n;\ a \in \mathbb{Z}\}$.
Pro $[a]_n, [b]_n \in \mathbb{Z}_n$ definujeme

$$[a]_n \oplus [b]_n = [a + b]_n,$$
$$[a]_n \odot [b]_n = [a \cdot b]_n.$$

Další časté značení pro tuto množinu tříd ekvivalence je $\mathbb{Z}/n\mathbb{Z}$. Je lepší z hlediska formálního, protože je to obecné značení pro faktorovou množinu (což zde vlastně děláme), na druhou stranu je delší. Nakonec jsme zvolili pohodlnější verzi $\mathbb{Z}_n$, zejména proto, že záhy ukážeme, že je to vlastně naše stará dobrá $\mathbb{Z}_n$ v jiném převleku.

Než začneme s touto definicí pracovat, je třeba hned vyjasnit jeden potencionální problém. Není totiž vůbec jasné, jestli jsme operace na zbytkových třídách definovali tak, aby to mělo smysl. Například umíme vypočítat $[5]_8 \odot [6]_8 = [30]_8$, ale víme, že třeba $[5]_8 = [13]_8$, je to tentýž objekt, tatáž třída. Co kdybychom tedy ve výpočtu použili 13 namísto 5? Bude $[13]_8 \odot [6]_8$ dávat stejný výsledek, tedy stejnou třídu jako původní výpočet? Ano, protože $[13]_8 \odot [6]_8 = [78]_8 = [30]_8$, neboť $8 \mid (78 - 30)$. Takže to vyšlo, ale to byl jen jeden příklad. Aby byla definice korektní, musíme ukázat obecně, že konkrétní volba zástupce nemá vliv na výsledek operace.

Věta 7a.17.
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)**:** $[a]_n = [u]_n$ znamená $a \equiv u \pmod n$, podobně pro b a v, pak nám Věta 7a.3 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 není sporná, zkusíme si to.

! **Příklad 7a.n:** 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 $-[8]_{13} = [5]_{13}$.
△

! Máme teď zajímavou situaci, množina $\mathbb{Z}_n$ je definována dvakrát. Samozřejmě se ukáže, že vlastně jde o totéž. Začneme tím, že každá zbytková třída je dána nějakým svým zástupcem. Můžeme se rozhodnout, že budeme jako zástupce zásadně vybírat právě zbytky po dělení číslem n, pak dostáváme $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$. Kdybychom zavedli „$k$“ jako symbol pro $[k]_n$, tak máme přesně množinu $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$. Je to ale zatím jen podobnost vizuální. Abychom ukázali, že jde opravdu o zcela stejné struktury, musíme ještě ukázat, že si odpovídají i operace.

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, popř. násobení, a ukážeme, že to v obou světech dopadne stejně.

Podle první definice dostáváme $a \oplus b = (a+b) \bmod n$ a $a \odot b = (ab) \bmod n$. Když totéž provedeme v nové definici přes třídy, dostáváme výsledky $[a]_n \oplus [b]_n = [a+b]_n$ a $[a]_n \odot [b]_n = [ab]_n$. My jsme se ale rozhodli třídy zastupovat vždy zbytky po dělení n, tudíž $[a]_n \oplus [b]_n = [(a+b) \bmod n]_n$ a dostáváme stejný výsledek jako u první definice, podobně $[a]_n \odot [b]_n = [(ab) \bmod n]_n$ a zase máme stejný výsledek.

Takže se dá říct, že nová definice vlastně znamená, že kolem prvků z první definice $\mathbb{Z}_n$ nakreslíme ohrádky, operace děláme v zásadě stejně. Původní definice nás ještě nutí po provedení výpočtu přejít ke zbytkům coby zástupcům ze $\mathbb{Z}_n$, zatímco nová definice ne, to je jedna z jejích výhod. Nechává nám svobodu vybírat si zástupce tak, aby se nám co nejlépe počítalo. Například opačný prvek k 5 v $\mathbb{Z}_{137}$ najdeme dle nové definice jako $[-5]_{137}$, nemusíme používat 132 podle první definice $\mathbb{Z}_{137}$.

Všechny výpočty modulo z předchozích příkladů o $\mathbb{Z}_n$ by se proto daly přepsat jako výsledky o třídách, třeba v příkladě 7a.i jsme nalezli inverzní prvek k $a = 36$ v monoidu $\mathbb{Z}_{175}$, $36^{-1} = 141$. 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.

Všechny dosavadní výsledky o $\mathbb{Z}_n$ bychom teď mohli přepsat do nového jazyka, ale nestojí to za to, uveďme jen jedno klíčové tvrzení.

!

Důsledek 7a.18.
Nechť $n \in \mathbb{N}$, uvažujme $[a]_n \in \mathbb{Z}_n$.
(i) Vždy existuje prvek opačný $-[a]_n = [n-a]_n$.
(ii) $[a]_n$ je invertibilní vůči $\odot$ právě tehdy, když jsou a a n nesoudělné.

Přímý důkaz vzorce pro opačný prvek: $[a]_n \oplus [n-a]_n = [a + (n-a)]_n = [n]_n = [0]_n$, neboť $n \equiv 0 \pmod n$.

Takže například $-[3]_7 = [4]_7$ a $-[3]_{13} = [10]_{13}$. Všimněte si, že na rozdíl od počítání v $\mathbb{Z}_n$ podle té první definice si teď nemusíme dělat speciální případ pro inverzní prvek k nule. Vzorec dává výsledek $[n]_n$, což je správně, neboť $[n]_n = [0]_n$.

Inverzní prvky hledáme stejně jako předtím. Od inverzního prvku $[x]_n$ k prvku $[a]_n$ očekáváme, že $[a]_a \cdot [x]_n = [1]_n$ neboli $[ax]_n = [1]_n$ neboli $ax \equiv 1 \pmod n$ neboli $ax + kn = 1$ pro nějaké $k \in \mathbb{Z}$. Zase tedy přijde ke slovu rozšířený Euklidův algoritmus, který rovnou dá správnou třídu $[x]_n$, protože nemusíme hledat zbytek po dělení n coby vzorového zástupce. Pokud to ale uděláme, dopadne to přesně jako u $\mathbb{Z}_n$ podle první definice. Dostáváme se zpět k tomu, že jde vlastně o tutéž věc.

Zatím to vypadá, že vlastně jen dokreslujeme symboly kolem čísel, což vypadá jako zbytečná práce. Má to nějaké výhody? Jednu už jsme viděli, nenutí nás to hledat správné zástupce. Hlavní výhoda je ale ještě jinde. Protože nová definice používá pokročilejší matematické struktury, můžeme využívat rozličné nástroje, které nám byly u původního přístupu inspirovaného zejména praktickým počítáním nepřístupné.

První ukázkou je splacení dluhu, který máme. Již jsme ve výpočtech v $\mathbb{Z}_n$ použili běžná pravidla, na která jsme zvyklí od reálných čísel, jenže jsme ještě nepotvrdili, že opravdu platí. V původní definici by to dalo trochu práce, v té nové je „zdědíme“ téměř bez práce.

! **Věta 7a.19.**
Nechť $n \in \mathbb{N}$. Pak platí následující:
(i) pro všechna $a, b \in \mathbb{Z}$ platí $[a]_n \oplus [b]_n = [b]_n \oplus [a]_n$,
(ii) pro všechna $a, b, c \in \mathbb{Z}$ platí $[a]_n \oplus ([b]_n \oplus [c]_n) = ([a]_n \oplus [b]_n) \oplus [c]_n$,
(iii) pro všechna $a \in \mathbb{Z}$ platí $[a]_n \oplus [0]_n = [a]_n$,
(iv) pro každé $a \in \mathbb{Z}$ platí $[a]_n \oplus [-a]_n = [0]_n$,
(v) pro všechna $a, b \in \mathbb{Z}$ platí $[a]_n \odot [b]_n = [b]_n \odot [a]_n$,
(vi) pro všechna $a, b, c \in \mathbb{Z}$ platí $[a]_n \odot ([b]_n \odot [c]_n) = ([a]_n \odot [b]_n) \odot [c]_n$,
(vii) pro všechna $a \in \mathbb{Z}$ platí $[a]_n \odot [1]_n = [a]_n$,
(viii) pro všechna $a, b, c \in \mathbb{Z}$ platí $[a]_n \odot ([b]_n \oplus [c]_n) = ([a]_n \odot [b]_n) \oplus ([a]_n \odot [c]_n)$.

Důkaz (poučný)**:** Všechny vlastnosti platí pro počítání na $\mathbb{Z}$ a díky chytré definice operací v $\mathbb{Z}_n$ 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):

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

□

To znamená, že množina $\mathbb{Z}_n$ je velice příjemná z abstraktního pohledu an operace, viz kapitola 8, kterou by už bylo opravdu dobré si teď přečíst. Konkrétně tato Věta ukazuje, že $(\mathbb{Z}_n, \oplus, [0]_n)$ je komutativní grupa a $(\mathbb{Z}_n, \odot, [1]_n)$ je komutativní monoid, $(\mathbb{Z}_n, \oplus, \odot)$ je pak komutativní okruh (viz kapitola 8c). Díky tomu automaticky dostáváme spoustu vlastností, které jsme předtím museli dokazovat, například jednoznačnost inverzního prvku (pokud existuje).

Přeložíme do jazyka algebry ještě další poznatek, který plyne z Důsledku 7a.18.

! **Věta 7a.20.**
Nechť $n \in \mathbb{N}$, uvažujme $\mathbb{Z}_n$. Jestliže je n prvočíslo, tak je každý prvek $[a]_n \in \mathbb{Z}_n$ splňující $[0]_n \neq [a]_n$ invertibilní. To znamená, že pro prvočíslo n je $(\mathbb{Z}_n, \oplus, \odot)$ těleso.

Jinak řečeno, pro prvočísla n se v $\mathbb{Z}_n$ pracuje prakticky stejně jako v reálných číslech, všechno funguje báječně, dokonce můžeme dělit nenulovými prvky.

7a.21 Poznámka: Kombinací chytré nové definice $\mathbb{Z}_n$ a obecných poznatků o množinách s operacemi z kapitoly 8b dostáváme také zajímavý důkaz malé Fermatovy věty 7a.12.

Nejprve si ale musíme rozmyslet, co je to $[a]_n^k$. To je zkratka pro $[a]_n \odot [a]_n \odot \cdots \odot [a]_n$, což je podle definice násobení rovno $[a \cdot a \cdots a]_n = [a^k]_n$. Rovnost $a^{n-1} \equiv 1 \pmod n$ tedy znamená, že v řeči zbytkových tříd máme $[a^{n-1}]_n = [1]_n$ neboli $[a]_n^{n-1} = [1]_n$. Jsme připraveni.

Dokážeme, že když je n prvočíslo a a je nesoudělné s n, pak $[a]_n^{n-1} = [1]_n$.

Podle Věty 7a.20 je množina všech invertibilních prvků $\mathbb{Z}_n$ rovna $G = \{[1]_n, \ldots, [n-1]_n\}$. Podle Věty 8b.4 je $(G, \odot)$ grupa. Její mohutnost je $n-1$, tudíž podle Důsledku 8b.7 platí pro každý prvek $[a]_n \in G$, že $[a]_n^{n-1} = [1]_n$.

Hotovo.

Důkaz byl tedy kratší a zdánlivě snažší než ten první, což je způsobeno tím, že využívá spousty práce, která byla udělána v kapitole 8.

△

Eulerova věta.

Tím končí hlavní blok této kapitoly, pro pokročilé přidáme ještě část další, která se pokusí pomoci s následujícím problémem: Umíme už efektivně počítat mocniny pro případ, že je n prvočíslo. Co dělat v případě, kdy n prvočíslo není? Jinými slovy, co se pak stane s malou Fermatovou větou?

Na to budeme muset hlouběji zabrousit do teorie čísel, jmenovitě se pořádněji podívat na otázku, kolik je v množině $\{1, 2, \ldots, n\}$ čísel nesoudělných s n. Nejprve si to nazveme.

Definice.
Eulerova funkce (**Euler function** or **totient**) φ je definována takto: Pro $n \in \mathbb{N}$ je $\varphi(n)$ rovno počtu 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 $\varphi(6) = 2$. Z množiny $\{1, 2, 3, 4, 5, 6, 7, 8\}$ jsou s devítkou nesoudělná čísla $1, 2, 4, 5, 7, 8$, proto $\varphi(9) = 6$. Snadno si

rozmyslíme, že pro prvočíslo p je $\varphi(p) = p-1$, protože nesoudělná s prvočíslem p jsou všechna čísla $1, 2, \dots, p-1$. K čemu tato Eulerova funkce je? Díky ní hravě dokážeme zobecnění malé Fermatovy věty.

Věta 7a.22. (Eulerova věta)
Nechť $n \in \mathbb{N}$. Jestliže je $a \in \mathbb{N}$ nesoudělné s n, pak $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Důkaz (poučný)**:** Uvažujme $G = \{[a]_n;\ [a]_n \text{ invertibilní v } \mathbb{Z}_n\}$. Podle Důsledku (ii) víme, že $[a]_n \in G$ právě tehdy, když je a nesoudělné s n. To znamená, že G je dána těmi $a \in \{1, 2, \dots, n-1\}$, které jsou nesoudělné s n, proto $|G| = \varphi(n)$.

Podle Věty 8b.4 je $(G, \odot)$ grupa, tudíž podle Důsledku 8b.7 platí pro každý prvek $[a]_n \in G$, že $[a]_n^{\varphi(n)} = [1]_n$. Jinými slovy, pro každé a nesoudělné s n platí $a^{\varphi(n)} \equiv 1 \pmod{n}$.

□

Tato věta nám tedy umožňuje efektivně umocňovat i při práci v $\mathbb{Z}_n$ pro n neprvočíselné, jen je třeba umět nacházet $\varphi(n)$. Už víme, že pro prvočíslo n máme $\varphi(n) = n-1$, takže z této věty dostáváme jako důsledek malou Fermanovu větu.

Mimochodem, někdy se dá najít i menší číslo než $\varphi(n)$ tak, aby umocnilo a na jedničku. Například pro prvočíslo $n = 31$ nám malý Fermat i Euler zaručí, že $2^{30} \equiv 1 \pmod{31}$, ale máme i $2^5 \equiv 1 \pmod{31}$. To není v rozporu s Eulerovou větou, ta jen zaručí existenci vhodné mocniny a nikde netvrdí, že našla tu nejlepší.

Hledání hodnot Eulerovy funkce také není zrovna snadné a odložíme to na konec kapitoly, abychom čtenáře předčasně nevyčerpali. Teď si ukážeme pár aplikací.

Příklad 7a.o: Vypočítáme $6^{1040} \bmod 91$. Již tradičně nejde použít kalkulačku, toto číslo má totiž 810 cifer, takže by udolalo i vše, co má typický počítač k dispozici. Nadšenci si napíšou vlastní rutiny na operace s takto dlouhými čísly, my raději zkusíme redukovat zlomek. Začneme pokročilými nástroji.

Protože 91 není prvočíslo, nelze použít malou Fermatovu větu, ale je třeba použít Eulerovu větu 7a.22, což možné je, protože 6 je nesoudělné s 91. Podle Věty 7a.29 a definice spočítáme $\varphi(91) = \varphi(7\cdot 13) = \varphi(7)\cdot\varphi(13) = 6\cdot 12 = 72$. Ještě si spočítáme $q = \left\lfloor \frac{1040}{72} \right\rfloor = \lfloor 14.44.. \rfloor = 14$ a můžeme počítat modulo 91.

$$6^{1040} = 6^{14\cdot 72+32} = (6^{72})^{14} \cdot 6^{32} \equiv 1 \cdot 6^{32}.$$

To pořád není žádná sranda (25 cifer, moje kalkulačka nemá se svými 13 pamatovanými ciframi šanci), Euler už nepomůže, takže je čas na jednoduché metody, jmenovitě postupné snižování mocniny. Umíme relativně snadno mocnit $6^4 = 36^2 = 1296 \equiv 22 \pmod{91}$, díky čemuž

$$6^{1040} \equiv \cdots \equiv 6^{32} = (6^4)^8 \equiv 22^8 \pmod{91}.$$

Toto je desetimístné číslo, to už kalkulačka zvládne, vydělením, zaokrouhledním podílu dolů a odečtením příslušného násobku konečně nacházíme zbytek 27.3. To nevypadá moc dobře, je to tím, že jsme použili funkci mocninu, tedy zmáčknuli jsme 22, pak „x^y“ a pak 8, takové obecné mocniny počítá kalkulačka přes logaritmy a chybky se projevují. Zkusíme to znovu pomocí klávesy „x^2“, která opravdu násobí čísla, pak $((22^2)^2)^2 - 603031577\cdot 91 = 29$. Dostáváme celé číslo, ale raději ještě kalkulačce pomůžeme.

$22^2 = 484 \equiv 29 \pmod{91}$, proto $6^{1040} \equiv \cdots \equiv 22^8 = (22^2)^4 \equiv 29^4 \pmod{91}$. Tohle už na kalkulačce bezpečně utlučeme, $6^{1040} \equiv 29^4 = 707281 \equiv 29 \pmod{91}$. Takže těm 29 věříme.

Pro alternativní způsob výpočtu se podívejte na příklad 7b.f.

△

Poznámka: Díky rozličným trikům (redukce mocniny oddělováním dvojky, malým Fermatem, Eulerovinami) je umocňování modulo mnohem příjemnější než umocňování běžné. Navíc se dá jakékoliv umocňování velice zrychlit následující fintou pro nalezení a^b:

Díky opakovanému násobení umíme rychle najít mocniny $a^1 = a$, a^2, $(a^2)^2 = a^4$, $(a^4)^2 = a^8$, $(a^8)^2 = a^{16}$ atd., tedy mocniny typu a^{2^i}. Stačí si tedy vyjádřit b v dvojkové soustavě, $b = \sum_{i=0}^{m} b_i 2^i$, viz příklad 6a.d, a dostáváme $a^b = \prod (a^{2^i})^{b_i}$. To vypadá komplikovaně, ale b_i nabývá pouze hodnot 0 či 1, takže $a^b = \prod_{b_i=1} a^{2^i}$.

Například $a^{21} = a^{16+4+1} = a^{16}a^4a^1 = (((a^2)^2)^2)^2(a^2)^2a^1$. Takovéto mocnění je velice rychlé, viz cvičení 10c.4. Při počítání modulo se navíc při všech krocích přechází k příjemnějším zástupcům, takže díky kombinaci všech triků se z mocniny stává relativně nenáročná operace.

△

Na začátku této kapitoly jsme ukázali, že při výpočtech modulo n lze v běžných algebraických operacích a v základu mocniny čísla nahrazovat jejich kongruentními bratříčky. Pomocí Eulerovy věty se ukáže, že to lze dělat i s exponentem, ale musí se použít jiný modulus.

Důsledek 7a.23.
Nechť $n \in \mathbb{N}$, uvažujme $a \in \mathbb{N}$ nesoudělné s n. Pak pro všechna $x, y \in \mathbb{N}$ platí: Jestliže $x \equiv y \pmod{\varphi(n)}$, pak $a^x \equiv a^y \pmod{n}$.

Důkaz (rutinní)**:** $x \equiv y \pmod{\varphi(n)}$ znamená, že $x = y + k\varphi(n)$ pro nějaké $k \in \mathbb{Z}$.
Pak $a^x = a^{y+k\varphi(n)} = a^y(a^{\varphi(n)})^k \equiv a^y 1^k = a^y \pmod{n}$.

□

Ve zbytku kapitoly se podíváme na výpočet $\varphi(n)$, což je mimochodem dost náročná úloha. Dělat si seznam čísel a hledat v něm ta nesoudělná s n rozhodně není pro větší n vhodnou metodou, raději bychom nějaké vzorečky. Jeden už jsme odvodili pro prvočísla, $\varphi(p) = p - 1$, teď se podíváme na další.

Fakt 7a.24.
Nechť p je prvočíslo. Pak pro všechna $k \in \mathbb{N}$ platí $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$.

Důkaz (poučný)**:** Která čísla menší než p^k mají netriviálního společného dělitele s p^k? Jestliže je d dělitel p^k, tak podle Lemma 6b.5 musí být ve tvaru $d = p^i$, tudíž čísla, která mají netriviálního společného dělitele s p^k, jsou přesně čísla dělitelná nějakou mocninou p^k. Rozmyslete si, že to jsou všechny násobky p. Kolik takových čísel je? Jsou to čísla $p, 2p, 3p, \ldots, (p^{k-1}-1)p$, protože další násobek je $p^{k-1}p = p^k$, ten už je moc velký. Je tedy $p^{k-1} - 1$ čísel menších než p^k a soudělných s p^k. Celkem je $p^k - 1$ přirozených čísel menších než p^k, proto těch nesoudělných je $(p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1}$.

□

Abychom našli vzorec pro všechna čísla, musíme si nejprve připravit půdu.

Lemma 7a.25.
Nechť $n \in \mathbb{N}$. Pak pro každé $a \in \mathbb{Z}$ platí $\gcd(a, n) = \gcd(a \bmod n, n)$.

Toto lemma je vlastně jen přepsané Lemma 6a.15 s volbou $b = n$, neboť pak $r = a \bmod n$.

Lemma 7a.26.
Nechť $m, n \in \mathbb{N}$ a $a \in \mathbb{N}$. Pak $\gcd(a, mn) = 1$ právě tehdy, když $\gcd(a \bmod m, m) = 1$ a $\gcd(a \bmod n, n) = 1$.

Důkaz: Jde jen o Lemma 6b.3 přepsané pomocí předchozího lemmatu.

□

Potřebujeme ještě jedno lemma, tentokráte poněkud vydatné. Abychom usnadnili jeho strávení, uvedeme nejprve inspirační podobenství.

7a.27 Souřadnice. Čtenář jistě zná pojem souřadnicového systému v $\mathbb{R}^2$. Je-li dán vektor $\vec{u} = (x, y)$, tak jej dokážeme rozložit do základních směrů $\vec{e} = (1, 0)$, $\vec{f} = (0, 1)$ a naopak jej z těch složek zase poskládat zpět, $\vec{u} = x \cdot \vec{e} + y \cdot \vec{f}$. Čísla x a y nám říkají, jak velká část z vektoru $\vec{u}$ působí ve směrech $\vec{e}$ a $\vec{f}$.

Toto funguje zcela obecně, můžeme si v rovině zvolit i jiné dva vektory $\vec{e}, \vec{f}$ (nesmí být rovnoběžné) a stejný postup bude fungovat, jen už velikost působení $\vec{u}$ v těchto dvou směrech nebude rovna souřadnicím x, y, ale nějakým jiným číslům, kterým zcela přirozeně říkáme souřadnice $\vec{u}$ vůči těmto novým vektorům $\vec{e}, \vec{f}$. Podstatné je, že pak libovolný vektor $\vec{u}$ dokážeme kódovat pomocí souřadnic, přičemž toto kódování je jednoznačné. Ještě užitečnější je, že takovéto souřadnice nám umožňují provádět snadno vektorové operace. Máme-li najít součet dvou vektorů, je možné začít rýsovat a odměřovat, nebo prostě sečteme jejich souřadnice a dostaneme tak hledaný vektor.

Teď si zavedeme něco obdobného, ale v úplně jiné situaci. Uvažujme dvě čísla $m, n \in \mathbb{N}$ větší než 1. To budou jakoby základní směrové vektory. Pro jiná čísla a se pak můžeme ptát, jak veliká je jakási „složka vzhledem k m“ a „složka vzhledem k n“. Není jasné, co to vůbec znamená, ale tato kapitola je o modulu, tak můžeme zkusit $x = a \bmod m$ a $y = a \bmod n$.

Příklad to vysvětlí nejlépe. Zvolíme základní směry $m = 3$, $n = 5$, a vyzkoušíme si vytváření „souřadnic“. Například pro číslo $a = 10$ dostáváme „souřadnice“ $(10 \bmod 3, 10 \bmod 5) = (1, 0)$, pro $a = 7$ je to $(1, 2)$, pro

$a = 13$ je to $(1, 3)$. Vidíme, že pro různá čísla dostáváme různé souřadnice, což vypadá vysoce nadějně. Je nicméně jasné, že to je jen díky tomu, že jsme si hráli s malými čísly, například pro $a = 13 + 3 \cdot 5 = 28$ dostáváme zase $(1, 3)$. To by byl probém, pokud bychom si nevšimli, že se mu jednoduše vyhneme, když se omezíme na relativně malá čísla.

Snadno si rozmyslíme, že pokud se podíváme na číslo větší než $m \cdot n$, tak dostaneme stejné „souřadnice" jako u nějakého menšího (nezáporného) čísla. V následujícím tvrzení ukážeme, že to funguje i naopak, pokud zůstaneme u čísel menších než mn, tak již ke každému číslu náleží unikátní „souřadnice".

Lemma 7a.28.
Nechť $m, n \in \mathbb{N}$ jsou nesoudělná. Definujme zobrazení T: $\{0, 1, \dots, mn-1\} \mapsto \{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\}$ předpisem $T(a) = (a \bmod m, a \bmod n)$. Toto zobrazení je bijekce.

Důkaz (poučný)**:** Definice je evidentně korektní, pro libovolné $a \in \mathbb{Z}$ platí
$(a \bmod m, a \bmod n) \in \{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\}$.

Máme $|\{0, 1, \dots, mn-1\}| = mn = |\{0, 1, \dots, m-1\}| \cdot |\{0, 1, \dots, n-1\}| = |\{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\}|$, jinými slovy mohutnosti definičního oboru a cílové množiny se shodují (a jsou konečné). Podle Faktu 2b.13 proto stačí ukázat, že je T prosté. Mějme tedy $a, b \in \mathbb{Z}$ takové, že $T(a) = T(b)$. To znamená, že $a \bmod m = b \bmod m$ a $a \bmod n = b \bmod n$, takže dle Věty 7a.1 platí $m \mid (a-b)$ a $n \mid (a-b)$. Podle Faktu 6a.11 pak $\operatorname{lcm}(m, n) \mid (b-a)$, a jelikož jsou m, n nesoudělné, pak už nutně $(mn) \mid (a-b)$. Proto existuje $k \in \mathbb{Z}$ takové, že $(a-b) = kmn$. Jenže $a, b \in \{0, 1, \dots, mn-1\}$, tedy $|a-b| < mn$, což je možné jen pro $k = 0$, tedy $a = b$. Prostota a tudíž i bijektivita T jsou dokázány.

□

Toto nám ukazuje dvě věci. První je, že opravdu pro čísla z množiny $\{0, 1, \dots, mn-1\}$ jsou ony „souřadnice" jednoznačně dány. Druhá věc je, že se takto dají dostat všechny možné souřadnice. Jinými slovy, kdykoliv si zvolíme nějaké $x \in \{0, 1, \dots, m-1\}$ a $y \in \{0, 1, \dots, n-1\}$, tak už musí existovat $a \in \{0, 1, \dots, mn-1\}$ takové, že $a \bmod m = x$ a $a \bmod n = y$.

Jak se ale takové a najde? Bohuže důkaz věty není konstruktivní, tedy nedává návod, jak takové a identifikovat. Čtenář si může zkusit uhodnout třeba takové a, aby $a \bmod 101 = 13$ a $a \bmod 103 = 17$, aby docenil, jak obtížný problém to je. Naštěstí na to existuje metoda, viz Soustavy lineárních kongruencí 7b.8.

Je zajímavé, že se tam vrátíme k našim „souřadnicím", dokonce tam dokážeme, že se operace mezi čísly dají převést na operace s jejich „souřadnicemi", přesně jako v případě vektorů. To je ale budoucnost, teď si ukážeme, co vyplyne z našeho posledního lemmatu.

! **Věta 7a.29.**
Nechť $m, n \in \mathbb{N}$ jsou nesoudělná. Pak $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Důkaz (poučný)**:** Zavedeme si množiny, které je třeba znát při výpočtu Eulerových čísel. Nechť B je množina přirozených čísel menších než m a nesoudělných s m, C je množina přirozených čísel menších než n a nesoudělných s n a nechť A je množina přirozených čísel menších než mn, která jsou s mn nesoudělná. Pak podle definice Eulerovy funkce je $\varphi(mn) = |A|$, $\varphi(m) = |B|$ a $\varphi(n) = |C|$.

Z definice množin máme $A \subseteq \{0, 1, \dots, mn-1\}$, $B \subseteq \{0, 1, \dots, m-1\}$ a $C \subseteq \{0, 1, \dots, n-1\}$. Uvažujme zobrazení S dané jako restrikce T z Lemmatu 7a.28 na množinu A. Tvrdíme, že je to bijekce $A \mapsto B \times C$.

Jestliže $a \in A$, pak $\gcd(a, mn) = 1$, proto je podle Lemmatu 7a.26 první složka $T(a)$ nesoudělná s m a druhá nesoudělná s n, tedy platí $T(a) \in B \times C$. S je opravdu zobrazení do $B \times C$. Protože je to restrikce prostého zobrazení T, musí být prosté.

Zbývá ukázat, že je to zobrazení na. Nechť $(x, y) \in B \times C$. Z předchozího Lemmatu plyne, že existuje číslo $a \in \{0, 1, \dots, mn-1\}$ takové, že $T(a) = (x, y)$. Ovšem z definice B a C máme $\gcd(x, m) = 1$ a $\gcd(y, n) = 1$, tudíž podle definice T platí i $\gcd(a \bmod m, m) = 1$ a $\gcd(a \bmod n, n) = 1$, proto podle Lemmatu 7a.26 máme $\gcd(a, mn) = 1$ a $a \in A$.

Ukázali jsme, že restrikce T je bijekce z A na $B \times C$, proto $|A| = |B| \cdot |C|$.

□

Důsledek 7a.30.
Nechť $n \in \mathbb{N}$ má prvočíselný rozklad $n = p_1^{k_1} \cdots p_m^{k_m}$, kde $p_1 < \cdots < p_m$ jsou prvočísla. Pak

$$\varphi(n) = p_1^{k_1}\Big(1 - \frac{1}{p_1}\Big) \cdots p_m^{k_m}\Big(1 - \frac{1}{p_m}\Big) = n \prod_{p \mid n}\Big(1 - \frac{1}{p}\Big).$$

Důkaz (rutinní)**:** Podle předchozí věty a Faktu 7a.24 máme

$$\varphi(n) = \prod_{i=1}^{m} \varphi(p_i^{k_i}) = \prod_{i=1}^{m} (p_i^{k_i} - p_i^{k_i-1}) = \prod_{i=1}^{m} p_i^{k_i}(1 - \frac{1}{p_i}) = \prod_{i=1}^{m} p_i^{k_i} \cdot \prod_{i=1}^{m} (1 - \frac{1}{p_i}) = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big).$$

□

Příklad 7a.p: Platí $\varphi(36) = \varphi(2^2 3^2) = 2^2\big(1 - \frac{1}{2}\big)3^2\big(1 - \frac{1}{3}\big) = 36\big(1 - \frac{1}{2}\big)\big(1 - \frac{1}{3}\big) = 12.$
△

Získaný vzorec lze pro jeden speciální případ zajímavě přeorganizovat.

Důsledek 7a.31.
Pro všechna $n, N \in \mathbb{N}$ platí $\varphi(n^N) = n^{N-1}\varphi(n)$.

Důkaz (rutinní, poučný)**:** Rozložme si $n = p_1^{k_1} \cdots p_m^{k_m}$, kde $p_1 < \cdots < p_m$ jsou prvočísla. Pak také máme $n^N = p_1^{Nk_1} \cdots p_m^{Nk_m}$, tudíž

$$\varphi(n^N) = \prod_{i=1}^{m} p_i^{Nk_i} \cdot \prod_{i=1}^{m} (1 - \tfrac{1}{p_i}) = n^N \prod_{p|n} (1 - \tfrac{1}{p}) = n^{N-1} n \prod_{p|n} (1 - \tfrac{1}{p}) = n^{N-1}\varphi(n).$$

□

Naším cílem bylo vyhnout se pracnému procházení množiny a zjišťování, kdo je soudělný a kdo ne, abychom zjistili φ. Teď máme vzorec pro obecné n, což zní nadějně, ale ve skutečnosti to také není žádná výhra. Vyžaduje totiž najít prvočíselný rozklad čísla, což je výpočetně vysoce náročná úloha. Proto je vhodné hledat alternativy ke zjišťování $\varphi(n)$. Tato funkce byla a je v teorii čísel pilně studována a už se toho o ní spoustu ví, ukažme si pro zajímavost bez důkazu některé věci:

- Pro všechna $n \in \mathbb{N}$ platí $n = \sum_{d|n} \varphi(d)$.
- Schrammův vzorec: $\varphi(n) = \sum_{k=1}^{n} \gcd(k, n) e^{-2\pi i k/n}$.
- $\varphi(n)$ roste skoro tak rychle jako n. Přesně:
  Pro každé $n \in \mathbb{N}$ platí $\sqrt{\frac{n}{2}} \leq \varphi(n) \leq n - 1$.
  Pro každé $\varepsilon > 0$ existuje $N(\varepsilon) \in \mathbb{N}$ takové, že $n^{1-\varepsilon} < \varphi(n) < n$ pro všechna $n > N(\varepsilon)$.

Cvičení

Cvičení 7a.1 (rutinní)**:** Spočítejte následující výrazy (zbytky po dělení), tedy ideální zástupce v kongruenci modulo dané číslo:

(i) 81 mod 11; (iii) 3 mod 11; (v) 48 mod 8; (vii) -8 mod 4;
(ii) -1 mod 7; (iv) -14 mod 13; (vi) -37 mod 5; (viii) -15 mod 6.

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

Cvičení 7a.3 (rutinní, zkouškové)**:** Pro daná n spočítejte dané výrazy modulo n tak, aby výsledkem bylo číslo z rozmezí $0, 1, \ldots, n-1$:
(i) $n = 6$, $(3 \cdot 13 + 11)^4 \cdot (37 + 14 \cdot 5)$;
(ii) $n = 5$, $(13 - 39) \cdot 37 \cdot (-14)^2$;
(iii) $n = 8$, $(24 \cdot 135 + 9)^7 \cdot 15 \cdot 18$.

Cvičení 7a.4 (rutinní, poučné)**:** Nechť $a = \sum_{i=0}^{m} a_i 10^i$. Dokažte následující:
(i) a je dělitelné třemi právě tehdy, když je ciferný součet a (daný $\sum a_i$) dělitelný třemi.
(ii) a je dělitelné devíti právě tehdy, když je ciferný součet a dělitelný devíti.
(iii) a je dělitelné jedenácti právě tehdy, když je jedenácti dělitelné číslo, které získáme sečtením sudých cifer a a odečtením lichých cifer a.
Nápověda: $n \,|\, a$ právě tehdy, když $a \equiv 0 \pmod{n}$.
Viz poznámka 7a.14.

Cvičení 7a.5 (rutinní)**:** Pro daná n a a najděte opačný prvek $(-a)$ a inverzní prvek a^{-1} v prostoru $\mathbb{Z}_n$, tedy prvky z množiny $\{0, 1, \dots, n-1\}$ takové, že $a + (-a) \equiv 0 \pmod{n}$ a $a^{-1} \cdot a \equiv 1 \pmod{n}$:
(i) $n = 35$, $a = 12$; (iii) $n = 42$, $a = 25$;
(ii) $n = 36$, $a = 15$; (iv) $n = 146$, $a = 75$.

Cvičení 7a.6 (rutinní, zkouškové)**:** Použijte malou Fermatovu větu k výpočtu následujících výrazů modulo zadané n. Očekávají se výsledky z $\{0, 1, \dots, n-1\}$.
(i) 3^{33} modulo $n = 11$; (ii) 4^{44} modulo $n = 13$; (iii) 5^{55} modulo $n = 23$.

Cvičení 7a.7 (rutinní, zkouškové)**:** Spočítejte následující výrazy v daném $\mathbb{Z}_n$. Nejprve převeďte odčítání na sčítání s opačnými prvky.
(i) $(7 + 8)^{146} - 21$ modulo $n = 13$; (ii) $(31 \cdot 4 - 1)^{192}$ modulo $n = 20$.

Cvičení 7a.8 (dobré)**:** Dokažte, že jestliže je $n \in \mathbb{N}$ liché, pak $n^2 \equiv 1 \pmod{8}$.

Cvičení 7a.9 (rutinní, poučné)**:** Která pseudonáhodná posloupnost je generována pomocí $x_{k+1} = (4x_k + 1) \bmod 7$ při $x_0 = 3$?

Cvičení 7a.10 (rutinní, poučné, zkouškové)**:** Nechť $n \in N$, 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 7a.3).

Cvičení 7a.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 7a.5.

Cvičení 7a.12 (rutinní, poučné, zkouškové)**:** Nechť $n \in \mathbb{N}$. Dokažte matematickou indukcí na k, že když $a, u \in \mathbb{Z}$ splňují $a \equiv u \pmod{n}$, pak pro libovolné $k \in \mathbb{N}$ platí $a^k \equiv u^k \pmod{n}$ (viz Fakt 7a.6).

Cvičení 7a.13 (rutinní, zkouškové)**:** Nechť $n \in \mathbb{N}$. Dokažte, že
(i) pro každé $a \in \mathbb{Z}$ platí $a \equiv a \pmod{n}$;
(ii) pro každé $a \in \mathbb{Z}$ platí: $a \equiv 0 \pmod{n}$ právě tehdy, když $n \mid a$.
(Viz Fakt 7a.2.)

Cvičení 7a.14 (rutinní, zkouškové)**:** Nechť $n \in \mathbb{N}$. Dokažte, že pro $a \in \mathbb{Z}_n$, $a \neq 0$ platí $(-a) = n - a$.
(Viz Fakt 7a.8.)

Cvičení 7a.15 (rutinní, zkouškové)**:** Nechť $n \in \mathbb{N}$. Dokažte, že pro každé $a, b \in \mathbb{Z}$ platí: $a \equiv b \pmod{n}$ právě tehdy, když $b \equiv a \pmod{n}$.
(Viz Věta 7a.16.)

Cvičení 7a.16 (poučné)**:** Nechť $m, n \in \mathbb{N}$. Dokažte, že pro každé $a, b \in \mathbb{Z}$ platí: Jestliže $a \equiv b \pmod{m}$ a $a \equiv b \pmod{n}$, pak $a \equiv b \pmod{\operatorname{lcm}(m, n)}$.

Řešení:
7a.1: (i): $\left\lfloor \frac{81}{11} \right\rfloor = \lfloor 7.4... \rfloor = 7$, proto $81 \bmod 11 = 81 - 7 \cdot 11 = 4$; (ii): $\left\lfloor \frac{-1}{7} \right\rfloor = \lfloor -0.14... \rfloor = -1$, proto $-1 \bmod 7 = -1 - (-1) \cdot 7 = 6$, nebo prostě $-1 + 7 = 6$; (iii): 3 hotovo; (iv): $-14 + 13 + 13 = 12$; (v): 0 neboť $8 \mid 48$; (vi): $\left\lfloor \frac{-37}{5} \right\rfloor = \lfloor -7.4 \rfloor = -8$, proto $-37 \bmod 5 = -37 - (-8) \cdot 5 = 3$; (vii): 0 neboť $4 \mid (-8)$; (viii): třeba $-15 + 6 + 6 + 6 = 3$.
7a.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.
7a.3: (i): $(3 \cdot 13 + 11)^4 \cdot (37 + 14 \cdot 5) \equiv (3 \cdot 1 + 5)^4 \cdot (1 + 2 \cdot 5) = 8^4 \cdot 11 \equiv 2^4 \cdot 5 = 16 \cdot 5 \equiv 4 \cdot 5 = 20 \equiv 2 \pmod{6}$.
(ii): $(13 - 39) \cdot 37 \cdot (-14)^2 \equiv (3 - 4) \cdot 2 \cdot 1^2 = (-1) \cdot 2 = -2 \equiv 3 \pmod{5}$.
(iii): $(24 \cdot 135 + 9)^7 \cdot 15 \cdot 18 \equiv (0 \cdot 135 + 1)^7 \cdot 7 \cdot 2 = 1^7 \cdot 14 \equiv 1 \cdot 6 = 6 \pmod{8}$.
Mimochodem, kdyby v tom prvním součinu nevyšla nula, museli bychom nahradit i 135. To odečítáním trvá dlouho, zde je asi lepší přístup přes zbytek po dělení. $q = \left\lfloor \frac{135}{8} \right\rfloor = \lfloor 16.87... \rfloor = 16$, $135 - 16 \cdot 8 = 135 - 128 = 7$. Proto $135 \equiv 7 \pmod{8}$.
7a.4: (i): $10 \equiv 1 \pmod{3}$, proto $a = \sum a_i 10^i \equiv \sum a_i \cdot 1^i = \sum a_i \pmod{3}$.
(iii): $10 \equiv (-1) \pmod{11}$, proto $a = \sum a_i 10^i \equiv \sum a_i \cdot (-1)^i = \sum a_{2i} - \sum a_{2i+1} \pmod{11}$.
7a.5:
(i): $(-a) = n - a = 35 - 12 = 23$,
hledáme $x \in \mathbb{Z}$ aby $12x + 35k = 1$ pro nějaké $k \in \mathbb{Z}$,
toto děláme Euklidem.
Dostali jsme $3 \cdot 12 + (-1) \cdot 35 = 1$,
modulo 35 to dává $3 \cdot 12 \equiv 1$.
Takže $12^{-1} = 3$.

35		1	0
12	2	0	1
11	1	1	−2
1•	11	−1•	3•
0			

(ii): $(-a) = 36 - 15 = 21$,
hledáme $x \in \mathbb{Z}$ aby $15x + 36k = 1$ pro nějaké $k \in \mathbb{Z}$,
toto děláme Euklidem.
Dostali jsme $\gcd(15, 36) > 1$,
proto 15^{-1} v $\mathbb{Z}_{36}$ neexistuje.

36		1	0
15	2	0	1
6	2	1	−2
3•	2	−2•	5•
0			

(iii): $(-a) = 42 - 25 = 17$,
hledáme $x \in \mathbb{Z}$ aby $25x + 42k = 1$ pro nějaké $k \in \mathbb{Z}$,
toto děláme Euklidem.
Dostali jsme $(-5) \cdot 25 + 3 \cdot 42 = 1$,
modulo 42 to dává $(-5) \cdot 25 \equiv 1$.
Přičteme $-5 + 42 = 37$, takže $25^{-1} = 37$.

42		1	0
25	1	0	1
17	1	1	−1
8	2	−1	2
1•	8	3•	−5•
0			

(iv): $(-a) = 146 - 75 = 71$,
hledáme $x \in \mathbb{Z}$ aby $75x + 146k = 1$ pro nějaké $k \in \mathbb{Z}$,
toto děláme Euklidem.
Dostali jsme $(-19) \cdot 146 + 37 \cdot 75 = 1$,
modulo 146 to dává $37 \cdot 75 \equiv 1$.
Takže $75^{-1} = 37$.

146		1	0
75	1	0	1
71	1	1	−1
4	17	−1	2
3	1	18	−35
1•	3	−19•	37•
0			

7a.6: (i): $= 3^{3\cdot 10+3} = (3^{10})^3 \cdot 3^3 \equiv 1^3 \cdot 3^3 = 27 \equiv 5 \pmod{11}$. Výpočet je platný, protože $\gcd(3, 11) = 1$ a 11 je prvočíslo.
(ii): $= 4^{3\cdot 12+8} = (4^{12})^3 \cdot 4^8 \equiv 1^3 \cdot (4^2)^4 = 16^4 \equiv 3^4 = 81 \equiv 3 \pmod{13}$. Výpočet je platný, protože $\gcd(4, 13) = 1$ a 13 je prvočíslo.
(iii): $= 5^{2\cdot 22+11} = (5^{22})^2 \cdot 5^{11} \equiv 1^2 \cdot 5 \cdot (5^2)^5 = 5 \cdot 25^5 \equiv 5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 9 = 45 \equiv 22 \pmod{23}$. Výpočet je platný, protože $\gcd(5, 23) = 1$ a 23 je prvočíslo.
7a.7: (i): $\equiv (7+8)^{146} + 5 = 15^{146} + 5 \equiv 2^{146} + 5 = 2^{12\cdot 12+2} + 5 = (2^{12})^{12} \cdot 2^2 + 5 = 1^{12} \cdot 4 + 5 = 9 \pmod{13}$. Výpočet je platný, protože $\gcd(2, 13) = 1$ a 13 je prvočíslo.
(ii): $= (31 \cdot 4 + 19)^{192} \equiv (11 \cdot 4 + 19)^{192} = (44 + 19)^{192} \equiv (4 + 19)^{192} = 23^{192} \equiv 3^{192} \pmod{20}$. Nelze použít malého fermata (20 není prvočíso).
Redukce mocniny: $3^{192} = 3^{3\cdot 64} = (3^3)^{64} = 27^{64} \equiv 7^6 4 = (7^2)^3 2 \equiv 9^{32} = (9^2)^{16} \equiv 1^{16} = 1 \pmod{20}$.
Euler: $\varphi(20) = \varphi(2^2 \cdot 5) = 20\big(1 - \frac{1}{2}\big)\big(1 - \frac{1}{5}\big) = 8$, dále $\gcd(3, 20) = 1$, proto $3^{192} = 3^{8\cdot 24} = (3^8)^{24} \equiv 1^{24} = 1 \pmod{20}$.
7a.8: $n = 2k + 1 \implies n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$ a 2 dělí $k(k+1)$.
7a.9: 3, 6, 4, 3, 6, 4, 3, 6, 4, 3...
7a.10: $a = u + kn$, $b = v + ln$ pak $a + b = (u + v) + (k + l)n$.
7a.11: Indukcí. $m = 1$ dává $a_1 \equiv u_1 \pmod{n}$, což platí dle předpokladu.
(1) Nechť $m \in \mathbb{N}$. Předpoklad $\prod_{i=1}^{m} a_i \equiv \prod_{i=1}^{m} u_i \pmod{n}$.

Mějme $a_1, \ldots, a_{m+1}$ a $u_1, \ldots, u_{m+1}$ po dvou kongruentní viz předpoklad tvrzení. Předpoklad indukce 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 7a.3 (iii) platí $\Big(\prod_{i=1}^{m} a_i\Big) \cdot a_{m+1} \equiv \Big(\prod_{i=1}^{m} u_i\Big) \cdot u_{m+1} \pmod{n}$ neboli $\prod_{i=1}^{m+1} a_i \equiv \prod_{i=1}^{m+1} u_i \pmod{n}$.
7a.12: Indukcí, $k = 1$ jasné.
(1) Nechť $k \in \mathbb{N}$. Indukční předpoklad: $a^k \equiv u^k \pmod{n}$. Také $a \equiv u$, proto dle Věty 7a.3 (iii) platí $a^k \cdot a \equiv u^k \cdot u \pmod{n}$ neboli $a^{k+1} \equiv u^{k+1} \pmod{n}$.
7a.13: (i): $a - a = 0$, proto $n \,|\, (a - a)$.
(ii): $a \equiv 0 \pmod{n} \iff n \,|\, (a - 0) \iff n \,|\, a$.
7a.14: Evidentně $0 \le n - a \le n - 1$, proto $n - a \in \mathbb{Z}_n$. Platí $a \oplus (-a) = a \oplus (n - a) = (a + (n - a)) \bmod n = n \bmod n = 0$.
7a.15: $a \equiv b \pmod{n} \implies n \,|\, (a - b) \implies n \,|\, (b - a) \implies b \equiv a \pmod{n}$.
7a.16: Předpoklad dává $m \,|\, (x - y)$ a $n \,|\, (x - y)$, takže číslo $x - y$ je společný násobek m, n, tudíž podle Lemma 6a.10 také $\operatorname{lcm}(m, n) \,|\, (x - y)$.

7b. Řešení rovnic modulo

Jednou ze základních aritmetických úloh je řešení rovnic. Když řešíme rovnice v $\mathbb{R}$ či $\mathbb{Q}$, tak na to máme tradiční nástroje, jmenovitě ekvivalentní (a neekvivalentní) úpravy rovnic, kterými si je přetváříme na příjemnější verze,

a vzorečky, které nám pomáhají s určitými typy rovnic. V této kapitole se zaměříme na rovnice ve světě modula, začneme zamyšlením, jak jsou vlastně takové rovnice formulovány a jaká řešení budeme očekávat.

Jako příklad uvažujme rovnici $x^2 = 6$. Podle toho, jakou verzi počítání modulo zrovna používáme, dostáváme různé úlohy.

• Pracujeme v $\mathbb{Z}$ modulo n.

Pak bychom řešili úlohu „Najdi $x \in \mathbb{Z}$ takové, že $x^2 \equiv 6 \pmod{n}$“.

Tato formulace je nejjednodušší (nepoužívá složitější konstrukce) a záhy uvidíme, že z praktického pohledu je také základem, i úlohy z dalších formulací převádíme při výpočtech na tuto.

• Pracujeme v $\mathbb{Z}_n$ dle novější definice s třídami.

Pak bychom řešili úlohu „Najdi $[x]_n \in \mathbb{Z}_n$ takové, že ${[x]_n}^2 = [6]_n$“. Zde samozřejmě ${[x]_n}^2 = [x]_n \odot [x]_n$.

• Pracujeme v $\mathbb{Z}_n$ dle první definice.

Pak bychom řešili úlohu „Najdi $x \in \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ takové, že $x^2 = 6$“. Tentokráte je x^2 zkratka pro $x \odot x$.

Jaká řešení očekáváme?

• V první formulaci chceme najít množinu všech čísel $x \in \mathbb{Z}$, které splňují danou rovnici. Protože víme, že při počítání modulo je možné čísla ve výrazech nahrazovat kongruenčními bratříčky, je hned jasné, že jakmile najdeme jedno řešení, bude jich už nekonečně mnoho.

Například při volbě $n = 10$ můžeme zkusmo zjistit, že $x = 4$ splňuje rovnici $x^2 \equiv 6 \pmod{10}$, máme tedy jedno řešení, a proto budou řešeními i všechna čísla typu $x = 4 + 10k$ pro $k \in \mathbb{Z}$.

Zajímavější otázka je, jestli už tak dostáváme všechna možná řešení, nebo existují ještě i jiná. V našem případě je možné najít i číslo $y = 6$, které rozhodně není kongruentní s $x = 4$ a také řeší danou rovnici. Je tedy druhá „rodina“ řešení ve tvaru $6 + 10k$. Je ještě nějaká další? To je jedna z otázek, kterými se zde budeme zabývat.

• Formulace v jazyce $[\ ]_n$: Pokud v rovnosti $[x]_n \odot [x]_n = [6]_n$ přepíšeme násobení podle definice, dostáváme $[x^2]_n = [6]_n$ neboli $x^2 \equiv 6 \pmod{n}$. To znamená, že každé řešení první formulace úlohy rovnou dá i řešení druhé formulace (po přikreslení ohrádky), naopak pokud nějaké $[x]_n$ splňuje druhou formulaci, pak x musí splňovat rovnici v jazyce modula. Zjistili jsme, že první dvě verze rovnice jsou v praxi totéž, stačí umět řešit rovnici dle první formulace (což je příjemnější) a po připsání ohrádek dostáváme řešení úlohy dle druhé formulace. Například rovnice ${[x]_{10}}^2 = [6]_{10}$ má určitě řešení $[4]_{10}$ a $[6]_{10}$.

Kolik bude řešení? Je snadné si rozmyslet, že všechna řešení typu $4 + 10k$ dají po přechodu k třídám kongruence totéž, třídu $[4]_{10}$, podobně to platí pro $[6 + 10k]_{10} = [6]_{10}$. Obecně, každá konguenční rodinka řešení pro první formulaci úlohy daná jedním konkrétním řešením x dá ve světě $\mathbb{Z}_n$ jedno řešení $[x]_n$. Počet řešení úlohy dle druhé formulace je tedy stejný jako počet různých kongruenčních skupin nalezených při řešení úlohy dle první formulace.

• Formulace v jazyce $\mathbb{Z}_n$: I zde existuje blízký vztah s řešeními první formulace. Pokud nějaké $x \in \mathbb{Z}_n$ řeší $x^2 = 6$, pak to znamená, že $x \in \{0, 1, \dots, n-1\}$ a $x^2 \equiv 6 \pmod{n}$. Máme-li naopak nějaké řešení $z \in \mathbb{Z}$, pak k němu najdeme zbytek modulo n neboli x, které je se z kongruentní (tudíž také řeší danou rovnici) a je z množiny $\{0, 1, \dots, n-1\}$, dostaneme tak řešení dle třetí formulace.

Jinak řešeno, pokud vezmeme všechna řešení $[x]_n$ dle druhé formulace a z každého vezmeme ideálního zástupce, dostaneme množinu všech řešení dle třetí formulace. Vidíme, že zase stačí umět řešit rovnice v modulární formulaci, rozdělit je do skupin podle kongruence a z každé pak vhodnou volbou dostáváme řešení pro svět $\mathbb{Z}_n$.

Například jsme již zjistili, že rovnice $x^2 = 6$ má v $\mathbb{Z}_{10}$ řešení 4 a 6 (ale nevíme, zda nejsou nějaká další).

Jaký je závěr? Základem je rovnice vzhledem k počítání modulo n řešená v prostoru $\mathbb{Z}$, řešení v jiných variantách pak dostáváme tak, že si nalezená řešení vhodně uspořádáme a vybereme vhodné zástupce.

Teď bychom rádi odvodili na řešení postupy, jmenovitě chceme algoritmy, které pro danou rovnici umí rozhodnout, zda je řešitelná, a v případě, že ano, tak nalézt množinu všech řešení včetně konguenční struktury. To je ovšem úloha vysoce náročná a obecně neřešitelná. Již tradičně se proto omezíme na speciální typy rovnic, jmenovitě na typ nejpříjemnější.

! 7b.1 Lineární kongruence

Rozumíme tím rovnice typu $ax \equiv b \pmod{n}$ pro daná $a, b \in \mathbb{Z}$, popřípadě tutéž rovnici v řeči $\mathbb{Z}_n$.

Shrňme poznatky z úvodu:

1) Rovnice formulované v $\mathbb{Z}_n$ převedeme do jazyka modula, například namísto úlohy „najděte (všechna) řešení $5x = 7$ v $\mathbb{Z}_8$“ bychom řešili úlohu „najděte (všechna) řešení $x \in \mathbb{Z}$ rovnice $5x = 7 \pmod{8}$“.

Nalezená řešení pak rozdělíme do skupin dle kongruence, z každé vybereme zástupce a máme řešení v $\mathbb{Z}_n$.

2) Základem je proto umět řešit rovnici $ax = b \pmod{n}$. Množina řešení je buď prázdná, nebo nekonečná, pro každé nalezené řešení x již bude řešením i celá množina $x + kn$ pro $k \in \mathbb{Z}$.

Dokažme si to: Jestliže x splňuje $ax = b \pmod{n}$, pak platí $a(x + kn) = ax + (ka)n \equiv b + 0 = b \pmod{n}$.

Než se dáme do práce, trochu si zjednodušíme značení.

Úmluva. V této sekci přestaneme pro kongruenci používat značení $\equiv$ a coby zkušení modulární veteráni budeme prostě psát třeba $3x = 5 \pmod{13}$. Rovněž budeme psát obvyklé značky pro operace namísto $\oplus$ a $\odot$. Je to (zejména u rovnic) tradiční a příjemnější. Pozorný čtenář by měl být schopen při čtení odvodit, kdy se hovoří o běžné rovnosti (a operacích) nebo o práci vzhledem k modulo n.

Jak budeme modulární rovnice řešit? Základem je následující pozorování, které vychází přímo z definice.

• $x \in \mathbb{Z}$ splňuje $ax \equiv b \pmod{n}$ právě tehdy, když existuje $y \in \mathbb{Z}$ takové, že $ax + yn = b$.

To je ovšem diofantická rovnice, u které nás navíc zajímá jen jedna souřadnice řešení x. Diofantické rovnice dokážeme zcela vyřešit, máme na to algoritmy a věty, když si z toho vytáhneme informace o první proměnné, okamžitě dostáváme toto.

Věta 7b.2.
Nechť $n \in \mathbb{N}$, nechť $a, b \in \mathbb{Z}$. Předpokládejme, že $\gcd(a,n) = Aa + Bn$.
(i) Jestliže b není násobkem $\gcd(a,n)$, tak řešení rovnice $ax \equiv b \pmod{n}$ neexistuje.
(ii) Jestliže $\gcd(a,n) \,|\, b$, tak rovnice $ax \equiv b \pmod{n}$ má řešení a množina všech jejích řešení je

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

Tím je v zásadě vše hotovo, dostáváme z toho první možný postup na řešení rovnice $ax \equiv b \pmod{n}$.

Příklad 7b.a: Uvažujme rovnici $14x = 38 \pmod{40}$.

Přeložíme si ji jako $14x + 40y = 38$ pro $x, y \in \mathbb{Z}$. Dle algoritmu pro diofantické rovnice potřebujeme Bezoutovu identitu, použijeme rozšířený Euklidův algoritmus.

40		1	0
14	2	0	1
12	1	1	−2
2•	6	−1•	3•
0			

Máme $\gcd(a,n) = 2$ a pravá strana $b = 38$ je násobkem dvou, takže daná rovnice má řešení. Bezoutova identita říká $14 \cdot 3 + 40 \cdot (-1) = 2$, tedy $A = 3$ a $B = -1$. Podle vzorce dostáváme množinu řešení $x = 3 \cdot \frac{38}{2} + k\frac{40}{2} = 57 + 20k$. Protože pracujeme modulo 40, je možné vybrat pěknějšího zástupce:

Množina všech řešení je $x = 17 + 20k$, $k \in \mathbb{Z}$.

Tím je vyřešena úloha, jak je zadána. Nyní se podíváme na další varianty.

• Vyřešte rovnici $14x = 38$ v $\mathbb{Z}_{40}$.

Nejprve bychom ji převedli na tvar $14x = 38 \pmod{40}$ a vyřešili. Abychom nalezená řešení převedli do $\mathbb{Z}_{40}$, je třeba zjistit, jaké kongruenční třídy se tam vyskytují. Víme, že čísla $14 + 40k$ dávají jedno řešení z prostoru $\mathbb{Z}_{40}$, vyčerpali jsme tím všechna řešení?

První následuící řešení po 17 je $17 + 20 = 37$ a to nevznikne jako $17 + 40k$ pro $k \in \mathbb{Z}$. To znamená, že existuje i další kongruenční skupina $37 + 40k$. Je ještě nějaká další?

Snadno si rozmyslíme, že všechna řešení typu $17 + 20k$ jsou již v obounalezených skupinách obsaženy.

Závěr: Rovnice $14x = 38$ má v $\mathbb{Z}_{40}$ řešení $x = 17, 37$.

• Vyřešte rovnici $[14]_{40}[x]_{40} = [38]_{40}$ v $\mathbb{Z}_{40}$.

Analýza výše ukazuje, že řešením jsou $x = [17]_{40}$ a $x = [37]_{40}$.

△

Protože rovnice řešíme v řeči $\mathbb{Z}_n$ často, bylo by dobré si vnést nějaký řád do hledání skupin. Nejprve to zkusme intuitivně.

Podle věty výše máme řešení ve tvaru $x = x_p + kn'$, kde $n' = \frac{n}{\gcd(a,n)}$. Kolik skupin (tříd ekvivalence) dle modula n dostáváme?

Určitě máme třídu danou $x_p + kn$ neboli $[x_p]_n$. Dostáváme tak všechna řešení? Hned vidíme následující:

• Pokud $\gcd(a,n) = 1$, pak jsou všechna řešení dané rovnice kongruentní modulo n, v jazyce tříd ekvivalence (či v prostoru $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$) bude mít jediné řešení $[x_p]_n$.

Mimochodem, řešení vždy existuje, protože podmínka existence je $\gcd(a,n) \,|\, b$ a to je pro $\gcd(a,n) = 1$ vždy splněno.

Co se stane, když $n' < n$? Pak zbyla nějaká řešení, která nedokážeme najít jako $x_p + kn$. První vynechané řešení po x_p je $x_p + n'$. Protože n nemůže dělit n', nejsou čísla x_p a $x_p + n'$ kongruentní, dostáváme tak proto jinou kongruenční třídu, jmenovitě řešení daná $\{(x_p + n') + kn\} = [x_p + n']_n$.

Zbyla nějaká řešení? Další řešení po $x_p + n'$ je $x_p + 2n'$. To by bylo obsaženo ve třídě $[x_p]_n$ jedině tehdy, pokud $2n' = n$, jinak dostáváme další třídu a tak dále.

Kolik tříd dostaneme? Tolik, kolikrát dokážeme přičíst n' k x_p, než se dostaneme k $x_p + n$. To znamená, že je celkem $\frac{n}{n'} = \gcd(a, n)$ různých tříd řešení.

Toto pozorování si potvrdíme, zvolíme jazyk tříd ekvivalence, který je zde asi nejpříjemnější.

!

!

Věta 7b.3.
Nechť $n \in \mathbb{N}$, nechť $[a]_n, [b]_n \in \mathbb{Z}_n$. Předpokládejme, že $\gcd(a, n)$ dělí b. Nechť $[x_p]_n$ je nějaké řešení rovnice $[a]_n \cdot [x]_n = [b]_n$.
Rovnice $[a]_n \cdot [x]_n = [b]_n$ má v $\mathbb{Z}_n$ celkem $\gcd(a, n)$ různých řešení, jmenovitě

$$\left\{[x_p]_n, \left[x_p + \frac{n}{\gcd(a,n)}\right]_n, \left[x_p + 2\frac{n}{\gcd(a,n)}\right]_n, \dots, \left[x_p + (\gcd(a,n)-1)\frac{n}{\gcd(a,n)}\right]_n\right\}$$
$$= \left\{\left[x_p + k\frac{n}{\gcd(a,n)}\right]_n;\ k = 0, 1, \dots, \gcd(a,n) - 1\right\}.$$

Důkaz (poučný)**:** 1) Nejprve ukážeme, že všechny vypsané třídy jsou opravdu řešením uvažované rovnice.

Jestliže $[x_p]_n$ řeší tuto rovnici, pak musí x_p řešit rovnici $ax = b \pmod n$, proto podle Věty 7b.2 existuje $k' \in \mathbb{Z}$ takové, že $x_p = A\frac{b}{\gcd(a,n)} + k'\frac{n}{\gcd(a,n)}$.

Uvažujme nějakou třídu $\left[x_p + k\frac{n}{\gcd(a,n)}\right]_n$. Pak $x_p + k\frac{n}{\gcd(a,n)} = A\frac{b}{\gcd(a,n)} + (k' + k)\frac{n}{\gcd(a,n)}$, proto podle Věty 7b.2 toto číslo také řeší rovnici $ax = b \pmod n$ a tedy dotyčná třída opravdu řeší $[a]_n \cdot [x]_n = [b]_n$.

2) Dále ukážeme, že každé řešení je obsaženo v některé z tříd. Uvažujme nějaké řešení $[x]_n$, to x pak musí řešit rovnici $ax = b \pmod n$. Podle Věty 7b.2 je určitě tvaru $x = A\frac{b}{\gcd(a,n)} + k\frac{n}{\gcd(a,n)}$ pro nějaké $k \in \mathbb{N}$. Proto $x = x_p + (k - k')\frac{n}{\gcd(a,n)}$.

Číslo $k - k'$ lze vyjádřit jako $k - k' = \gcd(a, n)y + r$, kde $r \in \{0, 1, \dots, \gcd(a, n) - 1\}$. Pak

$$x = x_p + (r + \gcd(a,n)y)\frac{n}{\gcd(a,n)} = x_p + r\frac{n}{\gcd(a,n)} + yn,$$

proto

$$[x]_n = \left[x_p + r\frac{n}{\gcd(a,n)} + yn\right]_n = \left[x_p + r\frac{n}{\gcd(a,n)}\right]_n.$$

Vidíme, že tato třída je mezi těmi vypsanými výše.

3) Již víme, že seznam tříd ve větě opravdu udává všechna řešení. Zbývá dokázat, že jde opravdu o různé třídy.

Uvažujme $[x]_n = \left[x_p + k\frac{n}{\gcd(a,n)}\right]_n$ a $y = \left[x_p + l\frac{n}{\gcd(a,n)}\right]_n$ pro nějaká $k, l \in \{0, 1, \dots, \gcd(a, n) - 1\}$. Pak $|k - l| < \gcd(a, n)$, proto $|x - y| = |k - l|\frac{n}{\gcd(a,n)} < \gcd(a, n)\frac{n}{\gcd(a,n)} = n$. Protože $|x - y| < n$, nemůže n dělit $x - y$ a tudíž tato čísla nejsou kongruentní modulo n. Třídy $[x]_n$ a $[y]_n$ jsou opravdu různé.

□

Souhlasí to s naším příkladem výše? Ano, tam jsme našli řešení x_p a k němu třídy $[x_p]_{40}$ a $[x_p + 20]_{40}$, přesně jak je třeba pro případ $\gcd(14, 40) = 2$.

Shrňme to: Umíme řešit rovnice v řeči modula, umíme také nalézt množinu všech řešení pro formulaci v jazyce tříd kongruence. Pokud by úloha byla zadána v jazyce $\mathbb{Z}_n$ dle první definice, pak stačí z každé kongruenční třídy vybrat vhodné řešení a dostaneme množinu všech řešení. Umíme tedy řešit lineární kongruence.

Mnozí uživatelé volí poněkud jiný postup řešení, takový, který využívá znalosti struktury množiny řešení. Výhodou je, že se pak postup podobá běžné práci s lineárními rovnicemi. I já mu dávám přednost, proto si tu odvodíme příslušný algoritmus. Začneme tradiční větou, viz lineární algebra či kapitola 6c.

Věta 7b.4.
Nechť $n \in \mathbb{N}$. Uvažujme rovnici $ax \equiv b \pmod n$ pro nějaká $a, b \in \mathbb{Z}$, nechť x_p je nějaké její řešení. Pak množina všech jejích řešení je

$$\{x_p + x_h;\ x_h \in \mathbb{Z} \text{ řeší přidruženou homogenní rovnici } ax \equiv 0 \pmod n\}.$$

Důkaz je natolik podobný důkazu Věty 6c.3, že jej s klidným svědomím necháme jako cvičení 7b.9. Co to pro nás znamená prakticky? Je třeba najít jedno partiklární řešení, a to pomocí Bezoutovy identity, tam to jinak nepůjde.

Protože teď ale vyvíjíme algoritmus založený na pochopení procesu, nebudeme si pamatovat vzorec, ale postup, ukážeme to níže.

Dále je třeba znát, jak vypadá množina všech řešení homogenní lineární kongruence. To jsme již vlastně viděli, stačí si ve Větě 7b.2 dosadit $b = 0$. Z cvičných důvodů si výsledek dokážeme pro tento speciální případ, čtenář to zkusí samostatně.

Fakt 7b.5.
Nechť $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Množina všech řešení rovnice $ax \equiv 0 \pmod{n}$ je $\left\{k\frac{n}{\gcd(a,n)};\ k \in \mathbb{Z}\right\}$.

Důkaz (rutinní)**:** 1) Ukážeme, že každé $x = k\frac{n}{\gcd(a,n)}$ je řešením dané rovnice. Dosadíme do levé strany: $ax = k\frac{an}{\gcd(a,n)} = nk\frac{a}{\gcd(a,n)}$, což je násobek n neboť $\frac{a}{\gcd(a,n)} \in \mathbb{Z}$ a tudíž rovno 0 modulo n.

2) Naopak nechť x je nějaké řešení. Pak $ax + yn = 0$ pro nějaké $y \in \mathbb{Z}$, tedy $ax = -yn$. Vydělíme tím gcd, dostaneme $\frac{a}{\gcd(a,n)}x = -y\frac{n}{\gcd(a,n)}$. Celé číslo $\frac{n}{\gcd(a,n)}$ tedy dělí $\frac{a}{\gcd(a,n)}x$, jenže podle Faktu 6a.9 jsou $\frac{n}{\gcd(a,n)}$ a $\frac{a}{\gcd(a,n)}$ nesoudělná čísla, tudíž musí podle Lemma 6a.23 číslo $\frac{n}{\gcd(a,n)}$ dělit x.

□

Protože se snažíme redukovat množství vzorců, které si pamatujeme, podíváme se na to jinak. Práci si ulehčíme, když rovnici hned na začátku co nejvíce zkrátíme. Zde je ovšem třeba pracovat opatrně, protože aby se zachovala množina řešení, je třeba krátit i modulo.

Lemma 7b.6.
Nechť $n \in \mathbb{N}$, uvažujme $a, b \in \mathbb{Z}$. Předpokládejme, že $d \in \mathbb{N}$ dělí čísla a, b, n.
Pak číslo $x \in \mathbb{Z}$ řeší rovnici $ax \equiv b \pmod{n}$ právě tehdy, když řeší rovnici $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

Důkaz (rutinní)**:** $ax \equiv b \pmod{n}$ právě tehdy, když existuje nějaké $k \in \mathbb{Z}$, aby $ax = b + kn$, což je právě tehdy, když existuje nějaké $k \in \mathbb{Z}$, aby $\frac{a}{d}x = \frac{b}{d} + k\frac{n}{d}$, což je právě tehdy, když $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

□

V praxi ale většinou krátíme až odvozenou diofantickou rovnici $ax + yn = b$. Zajímavou shodou okolností je největší číslo, kterým lze krátit na levé straně, právě $\gcd(a, n)$. Vzniká tak docela zajímavý sled kroků, které vypadají docela přirozeně:

Pamatujeme si, že chceme rovnici zkrátit, logicky tedy začneme nalezením čísla $\gcd(a, n)$, uhodnutím nebo rozšířeným Euklidem. Pak rovnici zkusíme zkrátit. Pokud se to na pravé straně nepovede, tak nemá řešení. Pokud se to povede, řešíme jednodušší zkrácenou rovnici.

Pak si musíme zapamatovat, že k nalezení partikulárního řešení vyjdeme z Bezoutovy identity, tu pak upravíme tak, abychom v ní rozpoznali danou rovnici (původní či zkrácenou, vyjde to nastejno).

Zbývá vyřešit přidruženou homogenní rovnici, ale u té je to ve zkráceném stavu jednoduché, máme rovnici ve tvaru $a'x + yn' = 0$ a pro a', n' nesoudělné má množina všech řešení tvar $x = kn'$.

Tím jsme dospěli k algoritmu. Ten má ještě dvě možné varianty, liší se tím, zda krátit danou rovnici hned na začátku, nebo až ve chvíli, kdy řešíme homogenní verzi. Souvisí to s tím, jak jsme našli $\gcd(a, n)$. Pokud jsme to hned viděli, pak má smysl rovnou rovnici vykrátit. Pokud jsme na to museli použít rozšířený Euklidův algoritmus, pak je asi jednodušší rovnou z výsledné Bezoutovy identity najít x_p pomocí původní verze rovnice a ke krácení přistoupit u homogenní rovnice. Tato druhá verze je obecnější, proto ji použijeme v algoritmu a student se jí může bez problémů držet.

Obecně se dá říct, že pokud student postupu dobře rozumí, může si dovolit se od něj občas jemně odchýlit, například tím, že použije první verzi nastíněnou výše či jinou zkratku.

S Algoritmus 7b.7. pro řešení rovnice $ax \equiv b \pmod{n}$ v $\mathbb{Z}$, popřípadě rovnice $[a]_n[x]_n = [b]_n$ v $\mathbb{Z}_n$, popřípadě rovnice $ax = b$ v $\mathbb{Z}_n$ pro $a, b \in \mathbb{Z}_n$.

0. Přepište si rovnici do tvaru $ax + ny = b$. Rozšířeným Euklidovým algoritmem najděte $\gcd(a, n) = Aa + Bn$ (či to uhodněte).
1. Jestliže $\gcd(a, n)$ nedělí b, pak řešení neexistuje.
2. Jestliže $\gcd(a, n)$ dělí b, rovnice má řešení.

a) Vynásobte identitu $\gcd(a,n) = Aa + Bn$ číslem $\frac{b}{\gcd(a,n)}$, čímž se změní na tvar $a\frac{Ab}{\gcd(a,n)} + n\frac{Bb}{\gcd(a,n)} = b$, přesně jako rovnice v kroku **0**. Vidíme partikulární řešení $x_p = \frac{Ab}{\gcd(a,n)}$.

b) Přidruženou homogenní rovnici $ax + ny = 0$ zkraťte číslem $\gcd(a,n)$ na tvar $a'x + n'y = 0$, ta má obecné řešení $x_h = kn'$, $k \in \mathbb{Z}$.

c) Obecné řešení dané rovnice je pak $x_p + x_h$.

V závislosti na formě zadání tak dostáváte následující:

• Množina všech celočíselných řešení kongruence $ax \equiv b \pmod n$ je $\{x_p + kn';\ k \in \mathbb{Z}\}$ neboli $x = x_p + kn'$, $k \in \mathbb{Z}$.

• Množina všech řešení v $\mathbb{Z}_n$ rovnice $[a]_n[x]_n = [b]_n$ je $\{[x_p + kn']_n;\ k = 0, 1, 2, \dots, \gcd(a,n) - 1\}$.

• Množinu řešení v $\mathbb{Z}_n$ rovnice $ax = b$ dostaneme tak, že pro každé $k = 0, 1, \dots, \gcd(a,n) - 1$ vybereme vhodného zástupce třídy $[x_p + kn']_n$.

Formálně, nechť k_0 je nejmenší celé číslo takové, že $x_p + kn' \geq 0$. Pak množina všech řešení v $\mathbb{Z}_n$ rovnice $ax = b$ je $\{x_p + kn';\ k = k_0, k_0 + 1, \dots, k_0 + \gcd(a,n) - 1\}$.

△

! Příklad 7b.b: Vyřešíme rovnici $66x = 18$ ve světě modulo $n = 150$ v různých podobách.

Ať už je zadání jakékoliv, vždy si nejprve rovnici přepíšeme jako $66x + 150y = 18$. Podle algoritmu máme nejprve najít $\gcd(66, 150)$, takže na koeficienty poštveme rozšířený Euklidův algoritmus.

150		1	0
66	2	0	1
18	3	1	−2
12	1	−3	7
6•	2	4•	−9•
0			

Dostáváme $\gcd(150, 66) = 6 = 4 \cdot 150 + (-9) \cdot 66$. Protože $\gcd(66, 150) = 6$ dělí pravou stranu, rovnice má řešení. Abychom našli partikulární řešení, je třeba upravit rovnost $66 \cdot (-9) + 150 \cdot 4 = 6$ do tvaru odpovídajícího zadané rovnici. Koeficienty 66 a 150 levé strany již souhlasí, zbývá upravit pravou stranu. Číslo 18 dostaneme, když celou rovnici vynásobíme trojkou, na levé straně tu trojku rozhodně nedáme ke koeficientům. Dostáváme $66 \cdot (-27) + 150 \cdot 12 = 18$, což mimochodem modulo 150 dává $66 \cdot (-27) \equiv 18$, prostě vidíme partikulární řešení $x_p = -27$.

Teď vyřešíme homogenní rovnici $66x + 150y = 0$. Zkrátíme nalezeným $\gcd(66, 150) = 6$, dostáváme rovnici $11x + 25y = 0$ a z ní $x_h = 25k$, $k \in \mathbb{Z}$.

Sečteme: Obecné řešení je $x = x_p + x_h = 25k - 27$.

Odpovědi dle formy zadání:

• Pokud máme řešit rovnici $66x = 18 \pmod{150}$, odpověď zní:

Množina řešení je $x = 25k - 27$, $k \in \mathbb{Z}$, popřípadě $\{25k - 27,\ k \in \mathbb{Z}\}$.

Je také možné použít lepšího zástupce, třeba $x = 25k - 2$ nebo $x = 23 + 25k$.

• Pokud máme řešit rovnici $[66]_{150}[x]_{150} = [18]_{150}$, pak víme, že existuje $\gcd(66, 150) = 6$ různých řešení, jmenovitě $[-27]_{150}$, $[-27 + 25]_{150}$, $[-27 + 50]_{150}$, $[-27 + 75]_{150}$, $[-27 + 100]_{150}$, $[-27 + 125]_{150}$. Množina všech řešení je $\{[-27]_{150}, [-2]_{150}, [23]_{150}, [48]_{150}, [73]_{150}, [98]_{150}\}$.

• Pokud máme řešit rovnici $66x = 18$ v $\mathbb{Z}_{150}$, pak množinu všech řešení, kterých je $\gcd(66, 150) = 6$, dostaneme výběrem vhodných kongruentních zástupců z šesti tříd výše. V praxi se to ale často dělá hned z prvního výsledku takto: nejprve najdeme nejmenší nezáporné číslo typu $x = -27 + 25k$, jmenovitě 23, z něj pak vyrobíme 6 řešení obvyklým způsobem. Množina všech řešení je $\{23, 48, 73, 98, 123, 148\}$.

Zkouška: Namátkou třeba $66 \cdot 48 = 3168 \bmod 150 = 18$, použili jsme $3168 - 21 \cdot 150 = 18$. Ověření ostatních řešení necháme pilnému čtenáři.

△

Poznámka: Řešení, které jsme právě viděli, je vzorové, ale nabízí se pár odboček.

1) Jedna možnost je zkrátit přímo danou rovnici číslem 6, což je rozumné dělat jen v situaci, kdy $\gcd(66, 150)$ umíme odhadnout. Dostaneme rovnici $11x + 25y = 3$, kterou pak dále řešíme obvyklým způsobem. Je třeba najít Bezoutovo vyjádření pro novou zkrácenou rovnici, pomocí rozšířeného Euklidova algoritmu odhalíme $\gcd(11, 25) = 1 = (-9) \cdot 11 + 4 \cdot 25$, tuto rovnost pak vynásobením trojkou upravíme na tvar $11 \cdot (-27) + 25 \cdot 12 = 3$, což odpovídá řešené (zkrácené rovnici) a máme $x_p = -27$.

Dál už pokračujeme běžným způsobem (x_h, následně $x_p + x_h$).

Proč takovéto brzké krácení rovnice doporučujeme jen pro případ, že $\gcd(66, 150)$ uhodneme? Pokud jej uhodnout neumíme a použijeme Euklidův algoritmus, tak po jeho běhu dostaneme $\gcd(66, 150) = 6 = 66 \cdot (-9) + 150 \cdot 4$. Z této rovnosti se většinou snáze dostaneme úpravou k rovnici původní než k té zkrácené, je tedy lepší odložit krácení až na homogenní případ.

2) Občas se naskytne jiný trik na zkrácení výpočtu. Pokud čtenář chápe, že smyslem prvního kroku je najít něco, co vypadá jako daná rovnice, pak je pro něj zajímavý třetí (nenulový) řádek zdola v tabulce Euklidova algoritmu

výše. Ten totiž říká, že $18 = 1 \cdot 150 + (-2) \cdot 66$ neboli $66 \cdot (-2) + 150 \cdot 1 = 18$. Rovnou vidíme řešení $x_p = 18$, protože dostáváme verzi dané rovnice, souhlasí koeficienty i pravá strana.

Je jasné, že člověk musí mít štěstí, aby se mu v tabulce objevila pravá strana rovnice, také musí dobře rozumět algoritmu i smyslu Euklidovy tabulky, ale když už se to zadaří, tak to potěší.

△

! 7b.8 Soustavy lineárních kongruencí

Zde budeme uvažovat následující typ soustav. Jsou dány moduly $n_1, \dots, n_m \in \mathbb{N}$ a pravé strany $b_1, \dots, b_m \in \mathbb{Z}$. Hledáme celá čísla x taková, že

$$\begin{aligned} x &\equiv b_1 \pmod{n_1},\\ x &\equiv b_2 \pmod{n_2},\\ &\vdots\\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

Jde o speciální případ soustav lineárních konguencí $a_i x \equiv b_i \pmod{n_i}$, ale ty by byly nad naše síly. Dokonce i naše speciální volba $a_i = 1$ pořád vede na zajímavé věci. Začneme klasikou.

Věta 7b.9.
Uvažujme moduly $n_1, n_2, \dots, n_m \in \mathbb{N}$ a čísla $b_1, b_2, \dots, b_m \in \mathbb{Z}$.
Nechť x_p je nějaké řešení soustavy kongruencí

$$\begin{aligned} x &\equiv b_1 \pmod{n_1},\\ x &\equiv b_2 \pmod{n_2},\\ &\vdots\\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

Číslo x je také řešením této soustavy právě tehdy, pokud existuje číslo x_h takové, že $x = x_p + x_h$ a x_h je řešením přidružené homogenní soustavy kongruencí

$$\begin{aligned} x &\equiv 0 \pmod{n_1},\\ x &\equiv 0 \pmod{n_2},\\ &\vdots\\ x &\equiv 0 \pmod{n_m}. \end{aligned}$$

Důkaz se od dvou obdobných vět dokázaných již dříve liší jen v detailech a necháme jej čtenáři.

Jako obvykle tedy stačí umět najít jedno partikulární řešení a pak pořádně prozkoumat homogenní rovnice. Těmi začneme, jsou snadné.

Uvažujme tedy soustavu rovnic

$$\begin{aligned} x &\equiv 0 \pmod{n_1},\\ x &\equiv 0 \pmod{n_2},\\ &\vdots\\ x &\equiv 0 \pmod{n_m}. \end{aligned}$$

Každá z těchto rovnic vyžaduje, aby x bylo násobkem příslušného modulu, takže vlastně hledáme taková x, která jsou společnými násobky všech modulů n_i.

Fakt 7b.10.
Uvažujme moduly $n_1, n_2, \dots, n_m \in \mathbb{N}$. Číslo $x \in \mathbb{Z}$ splňuje kongruence $x \equiv 0 \pmod{n_i}$ pro všechna $i = 1, \dots, m$ právě tehdy, když je x násobkem čísla $\operatorname{lcm}(n_1, n_2, \dots, n_m)$.

Důkaz: Každé číslo ve tvaru $k \operatorname{lcm}(n_1, \dots, n_m)$ pro $k \in \mathbb{Z}$ je dělitelné všemi n_i, tudíž vždy dává modulo n_i nulu a řeší uvažované kongruence.

Naopak každé řešení x oněch kongruencí musí být násobkem jednotlivých n_i, je to tedy společný násobek $n_1, \dots, n_m$. Protože je $\operatorname{lcm}(n_1, \dots, n_m)$ nejmenším společným násobkem, a to i ve smyslu dělitelnosti, musí platit $\operatorname{lcm}(n_1, \dots, n_m) \mid x$.

□

Pokud máme moduly $n_1, \dots, n_m$ takové, že pro $i \neq j$ jsou n_i, n_j nesoudělná čísla, pak je množina všech řešení příslušných kongruenci $x \equiv 0 \pmod{n_i}$ rovna $\{k n_1 n_2 \cdots n_m;\ k \in \mathbb{Z}\}$. Právě tento případ budeme dále uvažovat.

Zbývá vymyslet, jak nějak najít jedno partikulární řešení, což bude znatelně komplikovanější než v případě diofantických rovnic a lineárních kongruencí probraných výše. Existenci takového řešení nám za určitých podmínek potvrdí věta, dokonce dodá návod, jak takové řešení najít. Abychom ale důkazu lépe porozuměli, bude dobré si nejprve rozmyslet, odkud se výsledný vzorec bere.

Začneme první rovnicí. Pokud ji x řeší, tak jistě musí mít tvar $x = b_1 + kn_1$. Podobně snadno najdeme obecná řešení i pro další rovnice, problém je v tom, že potřebujeme jedno řešení společné.

Vezměme tedy všechna možná řešení první rovnice $x = b_1 + kn_1$, měli bychom zařídit, aby mezi nimi bylo i partikulární řešení druhé rovnice, jinými slovy, měli bychom zařídit, aby se při pohledu modulo n_2 objevilo b_2. Klíčová myšlenka je následující: Protože budeme mít více rovnic, tak nechceme, aby se nám v x vlivy míchaly. Přesněji řečeno, máme x jako součet dvou částí a zatím to funguje tak, že se při pohledu modulo n_1 druhá vynuluje a první dá žádané b_1. Rádi bychom, aby to obdobně (jen obráceně) fungovalo modulo n_2.

Nápad: Použijeme $x = b_1 + b_2kn_1$. Zatím jsme měli k jako libovolný parametr, čehož teď využijeme. Zvolíme takové k, aby se z výrazu b_2kn_1 při pohledu modulo n_2 stalo b_2. To vyžaduje, aby $kn_1 = 1 \pmod{n_2}$, tedy stačí za k zvolit ${n_1}^{-1}$ vzhledem k modulo n_2. Pokud to uděláme, tak $(b_2{n_1}^{-1}n_1) \bmod n_2 = b_2 \cdot 1 = b_2$, zatímco $(b_2{n_1}^{-1}n_1) \bmod n_1 = b_2{n_1}^{-1} \cdot 0 = 0$. Vidíme, že druhý člen teď funguje tak, jak chceme, vůči jednomu modulu se vynuluje a vůči druhému dá potřebnou pravou stranu.

První člen to zatím ale neumí, modulo n_1 dává žádané b_1, ale modulo n_2 se nevynuluje. Máme už ale nápad, jak to zařídit. Dostáváme lepší verzi $x = b_1{n_2}^{-1}n_2 + b_2{n_1}^{-1}n_1$, kde se inverze ${n_2}^{-1}$ bere vzhledem k modulo n_1.

Funguje to pěkně, rozmyslíme si případ tří rovnic. Pak x sestavíme ze tří členů, u každého potřebujeme, aby se vynuloval vzhledem ke dvěma modulům, což se snadno udělá zahrnutím těchto modulů. Napíšeme si kandidáty a přehledně si napíšeme, co od nich očekáváme vzhledem k různým modulům.

	$b_1x_1n_2n_3$	$b_2x_2n_1n_3$	$b_3x_3n_1n_2$
n_1	b_1	0	0
n_2	0	b_2	0
n_3	0	0	b_3

Ty nuly již opravdu fungují, bez ohledu na to, co zvolíme za x_i, takže máme svobodu si zvolit x_i tak, aby dobře dopadly i zbývající políčka v tabulce. Jestliže například má být $(b_1x_1n_2n_3) \bmod n_1 = b_1$, tak potřebujeme $(x_1n_2n_3) \bmod n_1 = 1$. To znamená, že by x_1 měl být inverzní prvek k n_2n_3 vzhledem k modulu n_1, podobně by x_2 měl být inverzní prvek k n_1n_3 vzhledem k modulu n_2 a x_3 by měl být inverzní prvek k n_1n_2 vzhledem k modulu n_3.

Aby šly tyto prvky najít, musí být vždy n_i nesoudělné se součinem ostatních modulů. Máme nápad, který zdá se funguje. Abychom vše řádně dokázali, uděláme si nejprve lématko.

Lemma 7b.11.
Nechť $n_1, n_2, \dots, n_m \in \mathbb{N}$ jsou po dvou nesoudělná. Označme $n = n_1 \cdot n_2 \cdots n_m$.
Jestliže $a, b \in \mathbb{Z}$ splňují $a \equiv b \pmod{n_i}$ pro všechna $i = 1, \dots, m$, pak $a \equiv b \pmod{n}$.

Důkaz (poučný)**:** Předpoklad říká, že $n_i \mid (a - b)$ pro všechna i. Podle Faktu výše je pak nutně $a - b$ násobkem čísla $\operatorname{lcm}(n_1, n_2, \dots, n_m)$. Protože jsou n_i navzájem nesoudělná, podle cvičení 6b.4 je $\operatorname{lcm}(n_1, n_2, \dots, n_m) = n$, tedy n dělí $a - b$.

□

Jako cvičení 7b.8 nabízíme alternativní důkaz indukcí, který může čtenáři přijít stravitelnější (nebo také ne). Jsme připraveni.

! **Věta 7b.12.** (Čínská věta o zbytcích)
Nechť $n_1, n_2, \dots, n_m \in \mathbb{N}$, $b_1, b_2, \dots, b_m \in \mathbb{Z}$. Uvažujme soustavu rovnic

$$\begin{aligned} x &\equiv b_1 \pmod{n_1},\\ x &\equiv b_2 \pmod{n_2},\\ &\vdots\\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

Jestliže jsou všechna čísla n_i po dvou nesoudělná, pak má tato soustava řešení.
Toto řešení je jediné modulo $n = n_1n_2 \cdots n_m$, množina všech řešení je $\{x + kn;\ k \in \mathbb{Z}\}$.

Důkaz (poučný)**:** 1) Nejprve ukážeme, že řešení existuje. Pro $i = 1, \dots, m$ definujeme $N_i = \frac{n}{n_i}$, tedy je to součin všech n_j s výjimkou n_i. Tvrdíme, že $\gcd(N_i, n_i) = 1$.

Kdyby tomu tak nebylo, pak by existovalo číslo, tudíž podle Faktu 6b.1 i prvočíslo p, které by dělilo n_i a $N_i = \prod_{j\neq i} n_j$. Podle Lemmatu 6b.2 by tedy p dělilo některé n_j a máme spor s $\gcd(n_i, n_j) = 1$.

Čísla N_i, n_i jsou tedy nesoudělná, proto existuje inverzní prvek k N_i vzhledem k násobení modulo n_i, tedy x_i takové, že $x_i N_i \equiv 1 \pmod{n_i}$. Nechť $x = \sum_{i=1}^{m} b_i N_i x_i$. Tvrdíme, že je to řešení dané soustavy.

Zvolme i. Pro $j \neq i$ pak $n_i \mid N_j$, proto $N_j \equiv 0 \pmod{n_i}$, tedy i $(b_j N_j x_j) \equiv 0 \pmod{n_i}$. Následně modulo n_i dostaneme $x \equiv b_i N_i x_i \equiv b_i \cdot 1 = b_i \pmod{n_i}$.

2) Jednoznačnost: Nechť je y nějaké řešení. Pak $(x - y) \equiv (b_i - b_i) = 0 \pmod{n_i}$, tedy $x \equiv y \pmod{n_i}$ pro všechna n_i. Podle Lemmatu 7b.11 pak $x \equiv y \pmod{n}$.

3) Tvar množiny všech řešení vyplývá okamžitě z našich předchozích úvah.

□

Při důkazu jsme opakovaně používali vzájemnou nesoudělnost jednotlivých dvojic. Poznamenejme, že by nestačilo jen chtít, aby největší společný dělitel všech n_i byl 1, protože to je jiná, mnohem slabší podmínka. Například největší společný dělitel čísel $3, 4, 8$ je 1, ale 4 a 8 rozhodně nejsou nesoudělné, tudíž by naše triky nefungovaly. Požadavek „po dvou nesoudělná“ tuto trojici správně vyřadí.

Důkaz věty a předchozí pozorování o homogenní rovnici dávají algoritmus.

S **Algoritmus 7b.13.** pro řešení soustavy kongruencí $x \equiv b_1 \pmod{n_1}, x \equiv b_2 \pmod{n_2}, \ldots, x \equiv b_m \pmod{n_m}$ pro případ, že jsou všechna čísla n_i po dvou nesoudělná.

1. Označte $n = n_1 n_2 \cdots n_m$ a $N_i = \dfrac{n}{n_i}$ pro všechna i.

2. Pro každé i najděte inverzní prvek k N_i vzhledem k násobení modulo n_i, viz algoritmus 7a.11.

3. Nechť $x = \sum_{i=1}^{m} b_i N_i x_i$. Množina všech řešení soustavy je $\{x + kn;\ k \in \mathbb{Z}\}$.

△

! **Příklad 7b.c:** Větě se říká čínská, protože soustavy kongruencí jdou zpět ke starým Číňanům někam do 3. století. Asi nejznámější je následující úloha z klasické knihy *Matematický manuál* mistra Sun-Tzu (to byl matematik, neplést se stejnojmenným autorem klasické knihy o vojenské strategii známe jako *The Art of War*).

Mějme určitý neznámý počet věcí. Když je uspořádáme po třech, zbydou dvě. Když je uspořádáme po pěti, zbydou tři. Když je uspořádáme po sedmi, zbydou dvě. Kolik je věcí?

Přeloženo do moderního jazyka, hledáme řešení soustavy rovnic $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ a $x \equiv 2 \pmod 7$. Použijeme příslušný algoritmus.

Máme $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, proto $n = 3 \cdot 5 \cdot 7 = 105$. Uděláme si doplňkové součiny $N_1 = \frac{n}{n_1} = n_2 \cdot n_3 = 35$, $N_2 = \frac{n}{n_1} = n_1 \cdot n_3 = 21$, $N_3 = \frac{n}{n_3} = n_1 \cdot n_2 = 15$.

Teď pro každé i potřebujeme inverzní prvek k N_i vzhledem k násobení modulo n_i. Budeme tedy řešit diofantické rovnice $35x + 3k = 1$, $21x + 5k = 1$ a $15x + 7k = 1$.

35		1	0
3	11	0	1
2	1	1	−11
1•	2	−1•	12•
0			

21		1	0
5	4	0	1
1•	5	1•	−4•
0			

15		1	0
7	2	0	1
1•	7	1•	−2•
0			

Dostáváme následující:

$\gcd(35, 3) = 1 = (-1) \cdot 35 + 12 \cdot 3$, tedy $2 \cdot 35 \equiv 1 \pmod 3$ a proto $x_1 = 35^{-1} = -1$;

$\gcd(21, 5) = 1 = 1 \cdot 21 + (-4) \cdot 5$, tedy $1 \cdot 21 \equiv 1 \pmod 5$ a proto $x_2 = 21^{-1} = 1$;

$\gcd(15, 7) = 1 = 1 \cdot 15 + (-2) \cdot 7$, tedy $1 \cdot 15 \equiv 1 \pmod 7$ a proto $x_3 = 15^{-1} = 1$.

Ty poslední dva se daly odhadnout i bez výpočtu.

Dosadíme do vzorce a dostáváme $x = 2 \cdot (-1) \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 23$.

Řešení je $23 + 105k$ pro $k \in \mathbb{N}_0$ (vzhledem k tomu, že jde o počty věcí, jsme nezahrnuli záporná k).

△

Poznámka: Pokud nesoudělnost těch n_i, n_j nemáme, nastává vážný problém, a to nejen s nalezením řešení (Čínskou větu nelze použít), ale dokonce s jeho existencí: Například soustava $x \equiv 2 \pmod 6$ a $x \equiv 3 \pmod 9$ vůbec nemá řešení. Existuje přesná podmínka: Máme-li dánu soustavu a n_i jsou obecná (ne nutně nesoudělná) přirozená čísla, pak tato soustava má řešení právě tehdy, když pro každé $i \neq j$ platí $a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$. Pak je řešení jednoznačné modulo $\operatorname{lcm}(n_1, \ldots, n_m)$. To už ale zase zabíháme mimo rozsah tohoto skripta.

△

! Příklad 7b.d: Vyřešíme soustavu $x \equiv 8 \pmod 5$, $x \equiv -1 \pmod 6$ a $x \equiv 14 \pmod 7$.

Tento příklad má připomenout, že se ve větě ani algoritmu nikde nepožadovalo, aby n_i byla prvočísla, jen nesoudělnost po dvojicích, a na pravé strany b_i nebyly už vůbec žádné požadavky. Ukážeme si také pár zjednodušujících triků.

První věc je, že u každé rovnice si můžeme pravé strany modifikovat dle příslušného modula. Budeme tedy namísto té zadané řešit soustavu $x \equiv 3 \pmod 5$, $x \equiv -1 \pmod 6$ a $x \equiv 0 \pmod 7$.

Teď také vidíme další zjednodušení, třetí člen v řešení se násobí nulou, tedy vůbec jej nemusíme vytvářet. Ale z cvičných důvodů si to také uděláme. Pro vytváření jednotlivých členů řešení použijeme systematický zápis, který některým (třeba mi) vyhovuje.

$x \equiv 3 \pmod 5$	$x \equiv -1 \pmod 6$	$x \equiv 0 \pmod 7$	
$3 \cdot 6 \cdot 7 \cdot ?$	$-1 \cdot 5 \cdot 7 \cdot ?$	$0 \cdot 5 \cdot 6 \cdot ?$	
$x_1 = 42^{-1} \pmod 5$	$x_2 = 35^{-1} \pmod 6$	$x_3 = 30^{-1} \pmod 7$	
$42x_1 + 5y = 1$	$35x_2 + 6y = 1$	$30x_3 + 7y = 1$	
$x_1 = -2$	$x_2 = -1$	$x_3 = -3$	
$x = 3 \cdot 42 \cdot (-2)$	$+(-1) \cdot 35 \cdot (-1)$	$+0$	$= -252 + 35 = -217$

Inverze x_i jsme uhádli, to je často možné, v případě nouze si bokem uděláme tabulky pro rozšířený Euklidův algoritmus. Máme také $n = 5 \cdot 6 \cdot 7 = 210$.

Dostáváme množinu řešení $x = 210k - 217$ pro $k \in \mathbb{Z}$. Kdyby chtěl někdo lepšího reprezentanta, nabízí se $-217 + 2 \cdot 210 = 203$, tedy množina všech řešení je $x = 203 + 210k$, $k \in \mathbb{Z}$.

△

Poznámka: Hledání inverzních čísel lze podstatně zjednodušit, když si uvědomíme, že pracujeme ve světě modula. Například u prvního členu jsme měli řešit rovnici $42x \equiv 1 \pmod 5$, což je ale ekvivalentní rovnici $2x_1 \equiv 1$, takže stačí hledat 2^{-1} pro modulo 5. Řešení příslušné rovnice $2x + 5y = 1$ lze snadno uhodnout. Podobně v dalších dvou případech stačí hledat $x_2 = 5^{-1} \pmod 6$ a $x_3 = 2^{-1} \pmod 7$.

Další prostor pro zjednodušení nám nabízí fáze formování členů. My jsme si do prvního přidávali $6 \cdot 7$, abychom zajistili vynulování vůči modulům 6 a 7. Jenže pravá strana první rovnice už dodala trojku, lze tedy pracovat se členem $3 \cdot 2 \cdot 7x_1$, kde $x_1 = 14^{-1} \pmod 5$. Z tohoto pohledu se může vyplatit přepis druhé rovnice do tvaru $x \equiv 5 \pmod 6$, protože pak druhý člen nemusí být $5 \cdot 5 \cdot 7x_2$, ale stačí $5 \cdot 7x_2$ a hledat $x_2 = 7^{-1} \pmod 6$.

Pokud vidíme, že nám x bobtná, máme jej někdy možnost redukovat vhodnou volbou čísel x_i. Každé z nich je totiž určeno jen modulo n_i, takže například u druhého členu jsme coby řešení rovnice $35x_2 \equiv 1 \pmod 6$ namísto $x_2 = -1$ mohli vzít $x_2 = -1 + 6 = 5$. Pak bychom měli $x = -252 - 175 = -427$. Dalo by se také použít $x_2 = -1 - 2 \cdot 6 = -13$ a máme $x = -252 + 455 = 203$, našeho nejlepšího zástupce.

Algoritmus je tedy (při ručním provádění) docela flexibilní, zejména pokud víme, oč v něm jde.

△

Čínská věta o zbytcích má mnoho praktických aplikací. Naštěstí se řešení dá najít algoritmicky, takže to nedělá počítačům problém a nemusíme se bát postupů, které Čínskou větu používají. Tímto optimistickým prohlášením končí hlavní část této sekce o soustavách, pokročilejší či odvážnější čtenáři si ale jistě její zbytek užijí. V něm si ukážeme jednu aplikaci Čínské věty, která dokáže významným způsobem urychlit násobení velkých čísel. Nejprve se trochu připravíme.

Souřadnice podruhé. Připomeneme si pojem kartézského součinu, nás bude konkrétně zajímat součin typu $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m}$, je to tedy množina vektorů o m souřadnicích, přičemž každá souřadnice používá čísel z příslušného $\mathbb{Z}_{n_i}$.

Na takovéto množině si zavedeme operace. Sčítání bude obdobné jako běžné sčítání vektorů, prostě sčítáme po souřadnicích, jen si teď musíme dát pozor, abychom v každé souřadnici používali správné sčítání z prostoru $\mathbb{Z}_{n_i}$. Podobně zavedeme i násobení vektorů, dva vektory násobíme tak, že vždy spolu vynásobíme odpovídající souřadnice dle odpovídající operace ze $\mathbb{Z}_{n_i}$ a z výsledků vytvoříme nový vektor.

Příklad: Množina $\mathbb{Z}_4 \times \mathbb{Z}_7$ je množina všech vektorů (x, y), přičemž x může nabývat hodnot $0, 1, 2, 3$ a y může nabývat hodnot $0, 1, \ldots, 6$. Když chceme sčítat dva takové vektory, tak v první souřadnici sčítáme modulo 4 a ve druhé modulo 7, podobně násobíme. Takže třeba $(3, 2) \oplus (1, 4) = (3 + 1 \bmod 4, 2 + 4 \bmod 7) = (0, 6)$ nebo $(3, 2) \odot (1, 4) = (3 \cdot 1 \bmod 4, 2 \cdot 4 \bmod 7) = (3, 1)$.

V části 7a.27 jsme ukázali, nač taková věc může být, pomocí souřadnic ze $\mathbb{Z}_4 \times \mathbb{Z}_7$ si dokážeme kódovat čísla z množiny $\mathbb{Z}_{4 \cdot 7} = \mathbb{Z}_{28}$ předpisem, že souřadnice čísla $a \in \mathbb{Z}_{28}$ jsou dána jako $(a \bmod 4, a \bmod 7)$. Lemma 7a.28 nám zaručilo, že opravdu každé číslo ze $\mathbb{Z}_{28}$ má jedinečně přiřazené souřadnice a naopak ke každé dvojici souřadnic $(x, y) \in \mathbb{Z}_4 \times \mathbb{Z}_7$ dokážeme najít odpovídající číslo a. Mělo to malý zádrhel, v té chvíli jsme ještě nevěděli, jak to a najít.

Tento problém je nyní vyřešen. Hledané a totiž musí splňovat $a \equiv x \pmod 4$ a $a \equiv y \pmod 7$, což je soustava lineárních kongruencí, kterou už umíme řešit. Vidíme tedy, že Čínská věta nám doplnila chybějící cihličku při výstavbě souřadnicového nápadu. Čínská věta to také umí pro více souřadnic než jen dvě, což ukazuje, že to budeme chtít takto zobecnit.

Než se k tomu dostaneme, připomeneme si, proč jsou pro nás souřadnice zajímavé. Každý čtenář zná souřadnice vektoru. Vektory v rovině jsou šipky, se kterými sice manipulovat umíme, ale dělat to graficky dá práci. Mnohem jednodušší je vyjádřit si vektory pomocí souřadnic, operace pak provádíme mnohem snáze. Podobně zde jsme v situaci, kdy si umíme čísla z rozmezí $0, 1, \dots, n_1 \cdot n_2$ kódovat pomocí souřadnic, které nepřevýší větší čísel z n_1, n_2, třeba v našem příkladě nemusíme pracovat s ohromnými čísly do 27, ale stačí umět pracovat s čísly do 6, na což stačí prsty na rukou. Máme tu tedy analogii s těmi vektory, ale aby byla analogie úplná (a užitečná), musíme také ukázat, že operace, které bychom chtěli provádět s těmi velkými čísly, můžeme namísto toho provádět s jejich souřadnicemi a vyjde to nastejno.

Tím se konečně dostáváme k jádru problému. Máme čísla $n_1, n_2, \dots, n_m$ a v prostorech $\mathbb{Z}_{n_i}$ odpovídající operace. Pomocí nich teď už také umíme sčítat a násobit vektory z prostoru $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$. Na druhé straně máme čísla z množiny $\mathbb{Z}_{n_1 \cdot n_2 \cdots n_m}$, která bychom také rádi sčítali a násobili. Klíčová otázka zní: Když dvě čísla ze $\mathbb{Z}_{n_1 \cdots n_m}$ sečteme, popř. vynásobíme, dokážeme tento výsledek získat tak, že si dotyčná čísla nahradíme jejich souřadnicemi z $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$, provedeme tam žádanou operaci a k výslednému vektoru souřadnic zase najdeme (Čínskou větou) odpovídající číslo ze $\mathbb{Z}_{n_1 \cdots n_m}$?

Dokážeme, že to funguje, nejprve si ale ujasníme, jak se kongruence chová při změně modula.

Lemma 7b.14.
Nechť $m, n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$. Jestliže $a \equiv b \pmod n$ a m dělí n, pak $a \equiv b \pmod m$.

Důkaz necháváme jako cvičení 7b.7. Mělo by to být jasné, například když $9 \equiv 21 \pmod{12}$, tedy od 9 se dá k 21 doskákat pomocí 12, tak už se dá určitě doskákat i pomocí 3 neboli $9 \equiv 21 \pmod 3$. Je také zjevné, že toto tvrzení nebude platit naopak, pokud se dá od a k b doskákat pomocí menšího čísla, pak to ještě nemusí znamenat, že to půjde i pomocí většího.

Teď jsme připraveni dokázat, že operace lze provádět pomocí souřadnic, což ovšem musíme vyjádřit ve správném matematickém jazyce. Přechod od čísla k jeho souřadnicím vlastně vytváří jisté zobrazení, jeho inverze pak reprezentuje přechod od souřadnic zpět. Fungování operací, jak jsme jej výše naznačili, se pak musí převést na vlastnosti tohoto zobrazení.

Protože teď budeme muset opatrně pracovat s různými operacemi, v následujícím lemmatu a jeho důkazu raději zase budeme používat $\oplus$ a $\odot$ pro operace v $\mathbb{Z}_n$ a zavedeme ještě (dočasně) speciální značení pro operace s vektory.

Lemma 7b.15.
Nechť $n_1, n_2, \dots, n_m \in \mathbb{N}$ jsou po dvou nesoudělná, $n_i \geq 2$. Označme $n = n_1 n_2 \cdots n_m$.
Tvrdíme, že zobrazení $T\colon \mathbb{Z}_n \mapsto \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ definované jako $T(a) = (a \bmod n_1, a \bmod n_2, \dots a \bmod n_m)$ je bijekce.
Pro $(x_1, x_2, \dots, x_m), (y_1, y_2, \dots, y_m) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ definujme operace

$$(x_1, x_2, \dots, x_m) \boxplus (y_1, y_2, \dots, y_m) = (x_1 \oplus y_1, x_2 \oplus y_2, \dots, x_m \oplus y_m),$$
$$(x_1, x_2, \dots, x_m) \boxdot (y_1, y_2, \dots, y_m) = (x_1 \odot y_1, x_2 \odot y_2, \dots, x_m \odot y_m),$$

kde $x_i \oplus y_i$ a $x_i \odot y_i$ jsou operace v příslušném $\mathbb{Z}_{n_i}$, tedy operace modulo n_i, a $x \oplus y$ a $x \odot y$ jsou operace v $\mathbb{Z}_n$.
Pak pro všechna $a, b \in \mathbb{Z}_n$ platí $T(a \oplus b) = T(a) \boxplus T(b)$ a $T(a \odot b) = T(a) \boxdot T(b)$.

Důkaz (náznak)**:** T je evidentně dobře definováno, neboť $a \bmod n_i \in \mathbb{Z}_{n_i}$ a tedy obrazy $T(a)$ neboli vektory $(a \bmod n_1, a \bmod n_2, \dots a \bmod n_m)$ opravdu leží ve specifikované cílové množině.

Prostota: Jestliže $T(x) = T(y) = (b_1, b_2, \dots, b_m)$, pak obě čísla řeší soustavu rovnic $x \equiv b_i \pmod{n_i}$, tudíž podle Čínské větě o zbytcích $x \equiv y \pmod n$, pro prvky ze $\mathbb{Z}_n$ pak nutně $x = y$.

T je na díky Čínské větě o zbytcích, pro dané $b_i \in \mathbb{Z}_{n_i}$ hledáme x takové, že $x \equiv b_i \pmod{n_i}$. Máme tedy bijekci.

Zbývají ověřit pravidla pro operace. Nejprve ověříme, že pro $a, b \in \mathbb{Z}_n$ platí $(a \oplus b) \bmod n_i = (a + b) \bmod n_i$: Podle definice $a \oplus b \equiv a + b \pmod n$, a protože $n_i \mid n$, pak podle Lemma 7b.14 také $a \oplus b \equiv a + b \pmod{n_i}$. Proto podle Věty 7a.1 dávají obě čísla stejný zbytek po dělení n_i.

Dále si všimneme, že $(a + b) \bmod n_i = ([a \bmod n_i] + [b \bmod n_i]) \bmod n_i$. To plyne z Faktu 7a.3, při počítání modulo n_i lze vstupní čísla nahradit kongruentními alternativami.

Teď už můžeme počítat

$$\begin{aligned} T(a \oplus b) &= \big((a \oplus b) \bmod n_1, \dots, (a \oplus b) \bmod n_m\big) \\ &= \big((a + b) \bmod n_1, \dots, (a + b) \bmod n_m\big) \\ &= \big(([a \bmod n_1] + [b \bmod n_1]) \bmod n_1, \dots, ([a \bmod n_m] + [b \bmod n_m]) \bmod n_m\big) \\ &= \big(a \bmod n_1, \dots, a \bmod n_m\big) \boxplus \big(b \bmod n_1, \dots, b \bmod n_m\big) = T(a) \boxplus T(b). \end{aligned}$$

Obdobný důkaz potvrdí pravidlo pro součin.

□

Toto Lemma vlastně říká, že prostory $\mathbb{Z}_n$ a $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ jsou z hlediska algebraického totožné. Když chci něco vypočítat, tak se pomocí T a T^{-1} mohu volně pohybovat mezi těmito dvěma prostory a je jedno, kde výpočet provedu, nakonec to vyjde nastejno. Ukažme si to pro sčítání. Pokud na vzoreček z Lemmatu aplikujeme inverzní zobrazení T^{-1}, dostaneme $T^{-1}(T(a \oplus b)) = T^{-1}(T(a) \oplus T(b))$ neboli $a \oplus b = T^{-1}(T(a) \oplus T(b))$. Přeloženo do lidštiny: Pokud chci spočítat $a \oplus b$, tak namísto přímého výpočtu mohu nejprve obě čísla nahradit souřadnicemi pomocí T, tyto vektory sečíst a od výsledného vektoru pak pomocí T^{-1} přejít zpět do původní množiny. Vidíme, že náš výsledek o zobrazení T opravdu říká to, o čem jsme neformálně rozmýšleli dříve.

Jaký je praktický dopad? Pokud umíme dobře násobit „malá“ čísla velikosti zhruba n_i, pak pomocí souřadnic už vlastně umíme i násobit čísla velikosti $n_1 \cdots n_m$. To je velice důležité, protože každý procesor má určitou mezní velikost, po kterou umí násobit opravdu hbitě, větší čísla pak násobí podstatně líněji. Náš trik nám umožní využít počítání s malými čísly k výpočtům s velkými čísly, časově se to i přes tu Čínskou větu vyplatí.

Například pokud procesor umí rychle počítat do 100, tak lze za n_i zvolit 95, 97, 98 a 99 a pak můžeme počítat rychle až do 89403930, navíc ty souřadnicové výpočty lze dělat paralelně. Populární volba jsou čísla tvaru $2^a - 1$, protože $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$ (viz cvičení 7b.10).

Příklad 7b.e: Nechť $n_1 = 3$, $n_2 = 4$. Pak $n = 12$ a množina $\mathbb{Z}_{12}$ je reprezentována množinou $\mathbb{Z}_3 \times \mathbb{Z}_4$ takto:
$T(0) = (0,0)$, $T(1) = (1,1)$, $T(2) = (2,2)$, $T(3) = (0,3)$, $T(4) = (1,0)$, $T(5) = (2,1)$, $T(6) = (0,2)$, $T(7) = (1,3)$, $T(8) = (2,0)$, $T(9) = (0,1)$, $T(10) = (1,2)$, $T(11) = (2,3)$.

Fungují opravdu operace? Pro zjednodušení už zase budeme psát normální značky.

Začneme sčítáním, v $\mathbb{Z}_{12}$ máme například $7 + 10 = 5$. Teď to zkusíme přes souřadnice. Nejprve čísla nahradíme souřadnicemi, tedy použijeme T, pak provedeme operaci na vektorech.

$$7 + 10 \mapsto T(7) + T(10) = (1,3) + (1,2) = ([1 + 1] \bmod 3, [3 + 2] \bmod 4) = (2,1).$$

Teď se vrátíme do $\mathbb{Z}_{12}$, $T^{-1}(2,1) = 5$, opravdu to souhlasí.

Zkusíme násobení, kolik je $2 \cdot 3$? Přeneseme pomocí T: $(2,2) \cdot (0,3) = ([2 \cdot 0] \bmod 3, [2 \cdot 3] \bmod 4) = (0,2)$ a $T^{-1}(0,2) = 6$. Vyšlo to.

△

Kromě násobení dokáže Čínská věta pomoci i s umocňováním.

Příklad 7b.f: V příkladě 7a.o jsme počítali 6^{1040} modulo 91 a dalo to docela práci. Zde si zkusíme jiný postup.

Máme $91 = 7 \cdot 13$, tak se podíváme na výpočet modulo tato dvě čísla. Jsou to prvočísla, takže lze použít malou Fermatovu větu 7a.12, navíc budeme mít ve výpočtu znatelně menší čísla než v 7a.o.

$$\begin{aligned} \text{modulo } 7: \;& 6^{1040} = 6^{173 \cdot 6 + 2} = (6^6)^{173} \cdot 6^2 \equiv 1^{173} \cdot 6^2 = 1 \cdot 36 \equiv 1 \pmod 7, \\ \text{modulo } 13: \;& 6^{1040} = 6^{86 \cdot 12 + 8} = (6^{12})^{86} \cdot 6^8 \equiv 1^{86} \cdot 36^4 \equiv 1 \cdot 10^4 = 100^2 \equiv 9^2 = 81 \equiv 3 \pmod{13}. \end{aligned}$$

Číslo $x = 6^{1040}$ tedy splňuje kongruence $x \equiv 1 \pmod 7$ a $x \equiv 3 \pmod{13}$, my už víme, jak takovou soustavu řešit (algoritmus 7b.13).

$x \equiv 1 \pmod 7$	$x \equiv 3 \pmod{13}$
$1 \cdot 13 \cdot ?$	$3 \cdot 7 \cdot ?$
$x_1 = 13^{-1} \pmod 7$	$x_2 = 7^{-1} \pmod{13}$
$13x_1 + 7y = 1$	$7x_2 + 13y = 1$
$x_1 = -1$	$x_2 = 2$

$$x = 1 \cdot 13 \cdot (-1) + 3 \cdot 7 \cdot 2 = -13 + 42 = 29$$

Dostali jsme 29, což je stejný výsledek jako v příkladě 7a.o a zdá se, že pohodlněji, ještě lepší by bylo, kdybychom měli na řešení soustav kongruencí hotový prográmek.

△

Pro lidi zabývající se rychlými výpočty modulo jsou podobné metody velice důležité.

7b.16 Bonus: Úpravy rovnic

Samozřejmě ne všechny rovnice jsou lineární, pak to začne být zajímavé. My se zde doplňkově zaměříme na otázku, které z našich obvyklých triků pro práci s rovnicemi fungují i ve světě modulo n, kde řešíme kongruence typu $x \equiv y \pmod n$. Mnohé z výsledků již vlastně máme dokázány, jen se na ně podíváme z jiného úhlu.

Ze symetrie relace kongruence (Fakt 7a.16) třeba vyplývá, že můžeme u rovnic modulo prohazovat strany, to je dobrý začátek. Měli jsme tam i tranzitivitu, což nám zase říká, že pokud k rovnici $x \equiv y \pmod n$ dostaneme $y \equiv z \pmod n$, tak už platí $x \equiv z \pmod n$. Jinými slovy, jednu stranu rovnice můžeme nahradit něčím jiným, co je jí rovno ve smyslu modula.

Zkusme něco méně triviálního. Jak se změní množina řešení, pokud k rovnicím něco přičteme či je vynásobíme číslem?

! **Fakt 7b.17.**
Nechť $n \in \mathbb{N}$. Uvažujme rovnici $x \equiv y \pmod n$ pro $x, y \in \mathbb{Z}$. Pak pro každé $c \in \mathbb{Z}$ platí:
(i) Rovnice $x + c \equiv y + c \pmod n$ a $x - c \equiv y - c \pmod n$ mají stejnou množinu řešení jako rovnice původní.
(ii) Jestliže x, y řeší rovnici původní, tak řeší i rovnice $cx \equiv cy \pmod n$ a $x^c \equiv y^c \pmod n$.

Důkaz (rutinní, poučný)**:** (i) 1) Nejprve ukážeme, že každé řešení původní rovnice je i řešením upravené rovnice $x + c \equiv y + c \pmod n$. Mějme tedy čísla $x, y \in \mathbb{Z}$ splňující $x \equiv y \pmod n$. Máme určitě i $c \equiv c \pmod n$ a podle Věty 7a.3 po sečtení zase dostaneme platnou kongruenci.

2) Teď potřebujeme ukázat, že naopak pokud máme nějaká řešení x, y rovnice $x + c \equiv y + c \pmod n$, pak už nutně musí splňovat $x \equiv y \pmod n$. Ale to je snadné, aplikujeme 1) s opačným prvkem $-c$ a dostaneme $(x + c) + (-c) \equiv (y + c) + (-c) \pmod n$, asociativní zákon nám umožňuje to přepsat jako $x + [c + (-c)] \equiv y + [c + (-c)] \pmod n$, tedy $x + 0 \equiv y + 0 \pmod n$ a je to.

Tvrzení o odčítání se snadno dostane tak, že se ekvivalence přičítání aplikuje na opačný prvek $-c$.

(ii) Nechť čísla x, y řeší rovnost $x \equiv y \pmod n$. Pak máme kongruenci $x \equiv y \pmod n$, tudíž podle Faktu 7a.6 platí $x^c \equiv y^c \pmod n$, a navíc $c \equiv c \pmod n$, proto podle Věty 7a.3 (iii) platí $cx \equiv cy \pmod n$.

□

Vidíme, že přičítat k rovnicím je bez problémů, ale u násobení a umocňování se dají čekat problémy, protože jsme v našem tvrzení napsali implikaci, ne ekvivalenci.

U umocňování to není překvapovák, dokonce i v oboru reálných čísel se snadno stane, že rovnice $x = y$ má méně řešení než rovnice $x^2 = y^2$, tedy umocněním rovnice mohou přibýt další řešení. Je to známý problém a nebudeme se v tom dále vrtat.

Mnohem zajímavější je násobení rovnic. Ani tam nejsme v $\mathbb{R}$ zcela v bezpečí, my totiž víme, že násobení rovnice je ekvivalentní operací jen v případě, že použijeme nenulové číslo, jinými slovy číslo, ke kterému existuje inverze. Tím máme možnost ono dodané číslo zase zkrátit a vrátit se k původní rovnici, množiny řešení tedy souhlasí. A přesně tady je problém při počítání modulo. Máme tedy následující výstrahu:

• Z platnosti rovnice $cx \equiv cy \pmod n$ obecně nedostáváme $x \equiv y \pmod n$. Jinými slovy, **nelze krátit**. Příklad: Platí $3 \cdot 4 \equiv 3 \cdot 2 \pmod 6$, neboť $12 - 6 = 6$ je dělitelné šesti. Když ale zkusíme zkrátit trojku, dostaneme nepravdivou rovnost $4 \equiv 2 \pmod 6$.

Zajímavý případ je, když na pravé straně použijeme $y = 0$.

• Z platnosti rovnice $cx \equiv 0 \pmod n$ obecně nemůžeme odvodit, že alespoň jedno z čísel nalevo je nulové modulo n. Například $3 \cdot 2 \equiv 0 \pmod 6$. I s tímto jsme se již setkali, když jsme disktovali dělitele nuly.

Protože jádrem problému je možnost najít inverzní prvek, poznatky z kapitoly 7a nám okamžitě řeknou, jak se věci mají.

! **Fakt 7b.18.**
Nechť $n \in \mathbb{N}$, uvažujme $y, x, c \in \mathbb{Z}$.
(i) Jestliže $cx \equiv cy \pmod n$ a $\gcd(c, n) = 1$, pak $x \equiv y \pmod n$.
(ii) Jestliže $cx \equiv 0 \pmod n$ a $\gcd(c, n) = 1$, pak $x \equiv 0 \pmod n$.

Důkaz (rutinní)**:** (i): Podle Věty 7a.10 má c inverzní prvek c^{-1} modulo n, díky kterému lze počítat

$$x = 1x \equiv (c^{-1}c)x \equiv c^{-1}(cx) \equiv c^{-1}(cy) \equiv 1y = y \pmod n.$$

Alternativa: Inverzním prvkem c^{-1} vynásobíme podle Faktu 7b.17 obě strany dané rovnice, použijeme asociativitu k přezávorkování a máme $(c^{-1}c)x \equiv (c^{-1}c)y \pmod n$ neboli $1x \equiv 1y \pmod n$, a je to.

(ii): Vynásobíme obě strany rovnice prvkem c^{-1}.

□

Tím máme jasno. Pro doplnění se podíváme na situaci, kdy máme $cx \equiv cy \pmod{n}$, ale c a n nesoudělné nejsou. Pak lze pořád něco odvodit, ale za cenu změny referenčního základu modula.

Věta 7b.19.
Nechť $n \in \mathbb{N}$, uvažujme $x, y, c \in \mathbb{Z}$. Jestliže $cx \equiv cy \pmod{n}$, pak $x \equiv y \pmod{\frac{n}{\gcd(c,n)}}$.

Důkaz (poučný)**:** Podle předpokladu máme $k \in \mathbb{Z}$ takové, že $c(x-y) = kn$. To znamená, že $\frac{c}{\gcd(c,n)}(x-y) = k\frac{n}{\gcd(c,n)}$, takže $\frac{n}{\gcd(c,n)}$ dělí $\frac{c}{\gcd(c,n)}(x-y)$. Podle Lemma 6a.9 jsou ovšem $\frac{n}{\gcd(c,n)}$ a $\frac{c}{\gcd(c,n)}$ čísla nesoudělná, tudíž podle Lemma 6a.23 musí $\frac{n}{\gcd(c,n)}$ dělit $x-y$.

□

Vyzkoušíme si to. Před chvílí jsme v poznámce o nemožnosti krátit uvažovali rovnici $3 \cdot 4 \equiv 3 \cdot 2 \pmod{6}$. Podle právě dokázané věty by mělo platit $4 \equiv 2 \pmod{\frac{6}{\gcd(3,6)}}$ neboli $4 \equiv 2 \pmod{2}$, což opravdu funguje.

To je sice pěkné, ale my přece žijeme ve světě modula n! Informace používající nějaké jiné modulo se občas dá částečně použít i ve světě n, ale je to komplikovanější a záleží na typu rovnice, který řešíme, takže se tomu nebudeme dále věnovat. Dá se říct, že se změně modula uprostřed výpočtu snažíme vyhýbat a dochází k tomu málokdy.

Cvičení

Cvičení 7b.1 (rutinní, zkouškové)**:** Vyřešte následující kongruence:
(i) $3x \equiv 7 \pmod{10}$;
(ii) $12x \equiv 0 \pmod{20}$;
(iii) $84x \equiv -56 \pmod{308}$;
(iv) $3x \equiv 7 \pmod{9}$;
(v) $6x \equiv 10 \pmod{8}$;
(vi) $11x \equiv 0 \pmod{40}$.

Cvičení 7b.2 (rutinní, zkouškové)**:** Vyřešte následující rovnice v daném $\mathbb{Z}_n$:
(i) $12x = 18$ v $\mathbb{Z}_{42}$;
(ii) $9x = 7$ v $\mathbb{Z}_{20}$;
(iii) $10x = 0$ v $\mathbb{Z}_{35}$;
(iv) $8x = 10$ v $\mathbb{Z}_{12}$;
(v) $84x = 126$ v $\mathbb{Z}_{210}$;
(vi) $8x = 0$ v $\mathbb{Z}_{12}$;

Cvičení 7b.3 (rutinní, zkouškové)**:** Vyřešte následující soustavy kongruencí:
(i) $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$;
(ii) $x \equiv 4 \pmod{2}$, $x \equiv -4 \pmod{3}$, $x \equiv 4 \pmod{5}$;
(iii) $x \equiv 1 \pmod{7}$, $x \equiv 0 \pmod{9}$, $x \equiv -1 \pmod{11}$;
(iv) $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{4}$, $x \equiv 5 \pmod{3}$.

Cvičení 7b.4 (rutinní, zkouškové)**:** Které z následujících rovnic jsou řešitelné v $\mathbb{Z}_{168}$?
a) $25x = 13$;
b) $30x = 12$;
c) $30x = 15$;
d) $16x = 24$.

Cvičení 7b.5 (dobré, zkouškové)**:** Uvažujme rovnici $(6-t)x = 24$ v Z_{40}. Pro které hodnoty t z rozmezí $0, \ldots, 5$ má tato rovnice
a) přesně čtyři řešení?
b) přesně tři řešení?
c) přesně pět řešení?
d) žádné řešení?

Cvičení 7b.6 (rutinní, poučné)**:** Nechť $n \in \mathbb{N}$ a $c \in \mathbb{Z}$, předpokládejme, že $\gcd(c,n) = 1$. Dokažte, že jestliže $x, y \in \mathbb{Z}$ splňují $cx \equiv 1 \pmod{n}$ a $cy \equiv 1 \pmod{n}$, pak $x \equiv y \pmod{n}$.

Cvičení 7b.7 (rutinní, poučné)**:** Nechť $m, n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$. Dokažte, že jestliže $a \equiv b \pmod{n}$ a m dělí n, pak $a \equiv b \pmod{m}$.

Cvičení 7b.8 (poučné)**:** (i) Nechť m, n jsou nesoudělná. Předpokládejte, že $a \equiv b \pmod{m}$ a $a \equiv b \pmod{n}$. Pak existuje $k \in \mathbb{Z}$ takové, že $a - b = km$. Z druhého předpokladu zase víme, že $n \,|\, (a-b)$, tedy $n \,|\, (km)$. Použijte Lemma 6a.23 k důkazu, že $a \equiv b \pmod{mn}$
(ii) Nechť $n_1, n_2, \ldots, n_m \in \mathbb{N}$ jsou po dvou nesoudělná. Označme $n = n_1 \cdot n_2 \cdots n_m$. Dokažte matematickou indukcí na m, že jestliže $a, b \in \mathbb{Z}$ splňují $a \equiv b \pmod{n_i}$ pro všechna $i = 1, \ldots, m$, pak $a \equiv b \pmod{n}$.
Bude se hodit (i).

Cvičení 7b.9 (rutinní, poučné)**:** Nechť $n \in \mathbb{N}$, nechť $a, b \in \mathbb{Z}$. Uvažujme nějaké řešení x_p kongruence $ax \equiv b$.
(i) Dokažte, že když je i $x \in \mathbb{Z}$ řešením této kongruence, tak číslo $x_h = x - x_p$ řeší kongruenci $ax \equiv 0 \pmod{n}$.
(ii) Dokažte, že když $x_h \in \mathbb{Z}$ je řešením kongruence $ax \equiv 0 \pmod{n}$, tak $x = x_p + x_h$ řeší kongruenci $ax \equiv b \pmod{n}$.

Cvičení 7b.10 (poučné)**:** Nechť $c \in \mathbb{N}$. Zde dokážeme, že pro $a, b \in \mathbb{N}$ platí $\gcd(c^a - 1, c^b - 1) = c^{\gcd(a,b)} - 1$. Vyplyne to z následujících kroků:
(i) Pomocí cvičení 9c.4 dokažte, že když $d \,|\, a$, pak také $(c^d - 1) \,|\, (c^a - 1)$.
(ii) Odvoďte, že $(c^{\gcd(a,b)} - 1) \,|\, (c^a - 1)$ a $(c^{\gcd(a,b)} - 1) \,|\, (c^b - 1)$.

(iii) Ukažte, že když číslo d dělí c^a-1 a c^b-1, pak $d\,|\,(c^{\gcd(a,b)-1})$.
Návod pro (iii): Přepište dělitelnost jako kongruenci, použijte Bezouta.
(ii) a (iii) říkají, že $c^{\gcd(a,b)}-1$ je společný dělitel a je největší takový.

Řešení:
7b.1: (i): $7=3x+10k$, evidentně $\gcd(3,10)=1=(-3)\cdot 3+1\cdot 10$ (lze uhádnout), vynásobíme Bezouta sedmi, $7=3\cdot(-21)+7\cdot 10$, tedy $x=-21$ je řešení.
Rovnice $3x\equiv 0 \pmod{10}$ má řešení $x_h=10k$, proto řešení dané rovnice je $x=-21+10k$, $k\in\mathbb{Z}$. Kdo chce, použije $x=9+10k$, $k\in\mathbb{Z}$.
(ii): Evidentně $\gcd(12,20)=4$, zkrátíme, $3x\equiv 0 \pmod 5$ má řešení $x=5k$, $k\in\mathbb{Z}$.
(iii): $-56=84x+308k$, Euklidem $\gcd(308,84)=28=(-1)\cdot 308+4\cdot 84$, protože $\frac{-56}{28}=-2\in\mathbb{Z}$ má rovnice řešení, vynásobíme Bezouta tou mínus dvojkou, $-56=84\cdot(-8)+2\cdot 308$, tedy $x=-8$ je řešení.
Rovnice $84x\equiv 0 \pmod{308}$ se vydělí 28 na $3x\equiv 0 \pmod{11}$, má řešení $x_h=11k$, proto řešení dané rovnice je $x=-8+11k$, $k\in\mathbb{Z}$. Kdo chce, použije $x=3+11k$, $k\in\mathbb{Z}$.
(iv): protože $\gcd(3,9)=3$ a 7 není násobkem 3, rovnice nemá řešení.
(v): $10=6x+8k$, evidentně $\gcd(6,8)=2=(-1)\cdot 6+1\cdot 8$ (lze uhádnout), rovnice má řešení, neboť $\frac{10}{2}=5\in\mathbb{Z}$, vynásobíme Bezouta tou pětkou, $10=6\cdot(-5)+5\cdot 8$, tedy $x=-5$ je řešení.
Rovnice $6x\equiv 0 \pmod 8$ se vydělí 2 na $3x\equiv 0 \pmod 4$, má řešení $x_h=4k$, proto řešení dané rovnice je $x=-5+4k$, $k\in\mathbb{Z}$. Kdo chce, použije $x=3+4k$, $k\in\mathbb{Z}$.
(vi): Protože $\gcd(11,40)=1$, je množina řešení $x=40k$, $k\in\mathbb{Z}$.
7b.2: (i): $18=12x+42k$, Euklidem nebo odhadem $\gcd(42,12)=6=1\cdot 42+(-3)\cdot 12$, protože $\frac{18}{6}=3\in\mathbb{Z}$ má rovnice řešení, vynásobíme Bezouta tou trojkou, $18=(-9)\cdot 12+3\cdot 42$, tedy $x=-9$ je řešení.
Rovnice $12x\equiv 0 \pmod{42}$ se vydělí 6 na $2x\equiv 0 \pmod 7$, má řešení $x_h=7k$, proto řešení kongruenční rovnice je $x=-9+7k$, přepíšeme na kongruentní $x=-9+7\cdot 2+7k=5+7k$. Je $\gcd(42,12)=6$ řešení v $\mathbb{Z}_{42}$, proto řešení dané úlohy je $x=5+7k$ pro $k=0,1,2,3,4,5$ neboli $\{5,12,19,26,33,40\}$.
(ii): $9x=7$ v $\mathbb{Z}_{20}$; $7=9x+20k$, Euklidem nebo odhadem $\gcd(20,9)=1=(-4)\cdot 20+9\cdot 9$, protože $\frac{7}{1}=7\in\mathbb{Z}$ má rovnice řešení, vynásobíme Bezouta tou sedmičkou, $7=9\cdot 63+(-28)\cdot 20$, tedy $x=63$ je řešení.
Rovnice $9x\equiv 0 \pmod{20}$ má řešení $x_h=20k$, proto řešení kongruenční rovnice je $x=63+20k$, přepíšeme na kongruentní $x=3+20k$. Je $\gcd(20,9)=1$ řešení v $\mathbb{Z}_{20}$, proto řešení dané úlohy je $x=3$.
(iii): Řešíme $10x\equiv 0 \pmod{35}$, uhodneme $\gcd(35,10)=5$, vydělíme rovnici na $2x\equiv 0 \pmod 7$, takže řešení kongruenční rovnice jsou $x=7k$. Je $\gcd(35,10)=5$ řešení v $\mathbb{Z}_{35}$, proto řešení dané úlohy je $x=7k$ pro $k=0,1,2,3,4$ neboli $\{0,7,14,21,28\}$.
(iv): $10=8x+12k$, Euklidem nebo odhadem $\gcd(12,8)=4=1\cdot 12+(-1)\cdot 8$, protože 4 nedělí 10, rovnice nemá řešení.
(v): $126=84x+210k$, Euklidem $\gcd(210,84)=42=1\cdot 210+(-2)\cdot 84$, protože $\frac{126}{42}=3\in\mathbb{Z}$ má rovnice řešení, vynásobíme Bezouta tou trojkou, $126=(-6)\cdot 84+3\cdot 210$, tedy $x=-6$ je řešení.
Rovnice $84x\equiv 0 \pmod{210}$ se vydělí 42 na $3x\equiv 0 \pmod 5$, má řešení $x_h=5k$, proto řešení kongruenční rovnice je $x=-6+5k$, přepíšeme na kongruentní $x=4+5k$. Je $\gcd(210,84)=42$ řešení v $\mathbb{Z}_{210}$, proto řešení dané úlohy je $x=4+5k$ pro $k=0,1,\ldots,41$ neboli $\{4,9,14,19,\ldots,204,209\}$.
(vi): Řešíme $8x\equiv 0 \pmod{12}$, uhodneme $\gcd(12,8)=4$, vydělíme rovnici na $2x\equiv 0 \pmod 3$, takže řešení kongruenční rovnice jsou $x=3k$. Je $\gcd(12,8)=4$ řešení v $\mathbb{Z}_{12}$, proto řešení dané úlohy je $x=3k$ pro $k=0,1,2,3$ neboli $\{0,3,6,9\}$.
7b.3: (i): $n=60$, $N_1=20$, inverze v $\mathbb{Z}_3$ je $x_1=-1$; $N_2=15$, inverze v $\mathbb{Z}_4$ je $x_2=-1$; $N_3=12$, inverze v $\mathbb{Z}_5$ je $x_3=-2$. $x=0\cdot 20\cdot(-1)+1\cdot 15\cdot(-1)+2\cdot 12\cdot(-2)=-63\equiv 57 \pmod{60}$. Řešení jsou $x=60k-63$ nebo třeba $57+60k$ pro $k\in\mathbb{Z}$.
(ii): $n=30$, $N_1=15$, inverze v $\mathbb{Z}_2$ je $x_1=1$; $N_2=10$, inverze v $\mathbb{Z}_3$ je $x_2=1$; $N_3=6$, inverze v $\mathbb{Z}_5$ je $x_3=1$. $x=4\cdot 15\cdot 1+(-4)\cdot 10\cdot 1+4\cdot 6\cdot 1=44\equiv 14 \pmod{30}$. Řešení jsou $x=44+30k$ nebo třeba $14+30k$ pro $k\in\mathbb{Z}$.
(iii): $n=693$, $N_1=99$, inverze v $\mathbb{Z}_7$ je $x_1=1$; $N_2=77$, inverze v $\mathbb{Z}_9$ je $x_2=2$; $N_3=63$, inverze v $\mathbb{Z}_{11}$ je $x_3=-4$. $x=1\cdot 99\cdot 1+0\cdot 77\cdot 2+(-1)\cdot 63\cdot(-4)=351$. Řešení jsou $x=351+693k$ pro $k\in\mathbb{Z}$.
(iv): Přepis na $x\equiv 3 \pmod 5$, $x\equiv 0 \pmod 4$, $x\equiv 2 \pmod 3$. $n=60$, $N_1=12$, inverze v $\mathbb{Z}_5$ je $x_1=3$; N_2 netřeba řešit; $N_3=20$, inverze v $\mathbb{Z}_3$ je $x_3=2$. $x=3\cdot 12\cdot 3+0+2\cdot 20\cdot 2=188$. Řešení jsou $x=188+60k$ nebo třeba $x=8+60k$ pro $k\in\mathbb{Z}$.
7b.4: Podmínka je $\gcd(a,n)\,|\,b$. a): $\gcd(25,168)=1$, $1\,|\,13$, ano. b): $\gcd(30,168)=6$, $6\,|\,12$, ano. c): $\gcd(30,168)=6$, neplatí $6\,|\,15$, ne. d): $\gcd(16,168)=8$, $8\,|\,24$, ano.
7b.5: Počet řešení je roven $\gcd(a,n)$, ale musí platit $\gcd(a,n)\,|\,b$. a): Potřebujeme $\gcd(6-t,40)=4$, pak také $4\,|\,24$, to platí pro $t=2$.
b): Potřebujeme $\gcd(6-t,40)=3$, to není možné.

c): Potřebujeme $\gcd(6-t,40)=5$, nastane pro $t=1$, ale neplatí $5\,|\,24$, takže žádné řešení.
d): Žádné řešení nastane, když $\gcd(6-t,40)$ nedělí 24. Protože $40=8\cdot 5$ a $6-t\leq 6$, možná gcd jsou $2,4,5$. Z nich jen 5 nedělí 24, u ostatních budou řešení. Závěr: Žádné řešení nebude pro $t=1$.
7b.6: Použijte tranzitivitu, $cx\equiv cy \pmod n$, pak krácení.
Nebo: Z rovnic plyne, že pro nějaká $k,l\in\mathbb{Z}$ platí $cx=1+kn$ a $cy=1+ln$. Pak $cy-cy=(k-l)n$, tedy $c(x-y)=(k-l)n$, a protože $\gcd(c,n)=1$, musí n dělit $x-y$ (Lemma 6a.23).
7b.7: $n\,|\,(a-b)$, $m\,|\,n$ a tranzitivita, nebo $a-b=kn$, $n=lm$ a dosadit.
7b.8: (i) Víme, že $n\,|\,(km)$. Ale $\gcd(m,n)=1$, proto podle Lemma 6a.23 platí $n\,|\,k$ neboli $k=ln$ pro nějaké $l\in\mathbb{Z}$. Pak $a-b=lnm$, tedy $(mn)\,|\,(a-b)$, což dává závěr.
(ii) (0) $m=1$ evidentně platí.
(1) Předpokládejme platnost pro m. Mějme $n_1,\dots,n_m,n_{m+1}$ po dvou nesoudělná a a,b dle předpokladu. Protože $a\equiv b \pmod{n_1},\dots,a\equiv b \pmod{n_m}$, musí podle indukčního předpokladu platit $a\equiv b \pmod{n'}$, kde $n'=n_1\cdot n_2\cdots n_m$. Také $a\equiv b \pmod{n_{m+1}}$, proto podle (i) platí $a\equiv b \pmod{n'n_{m+1}}$, ale $n'n_{m+1}=n1\cdot n_2\cdots n_m\cdot n_{m+1}$, přesně jak jsme potřebovali.
7b.9: (i): $a(x-x_p)=ax-ax_p\equiv b-b=0 \pmod n$.
(ii) je podobné.
7b.10: (i): $d\,|\,a \implies a=dm$, podle cvičení 9c.4 s dosazením c za x je $c^a-1=(c^d-1)(c^{(m-1)d}+\cdots+c^d+1)$.
(ii): Protože $\gcd(a,b)\,|\,a$ a $\gcd(a,b)\,|\,b$, plyne to hned z (i).
(iii): $d\mid(c^a-1)$, proto $c^a\equiv 1 \pmod d$, podobně $c^b\equiv 1 \pmod d$. Podle Bezouta $\gcd(a,b)=ax+by$, tedy $c^{\gcd(a,b)}=(c^a)^x\cdot(a^b)^y\equiv 1^x\cdot 1^y=1 \pmod d$, tedy $d\,|\,(c^{\gcd(a,b)}-1)$.

7c. Matice a polynomy modulo

S maticemi a polynomy se pracuje také v jiných světech než ve světě reálných čísel. Věci pak mohou fungovat trochu jinak, než jsme zvyklí. Pro příklad není třeba chodit daleko, například polynom $p=2x-1$ má kořen v oboru reálných čísel (jmenovitě $x=\frac{1}{2}$ splňuje $p(x)=0$), ale nemá kořen v oboru celých čísel. Nebo třeba matice $A=\begin{pmatrix}2&0\\0&1\end{pmatrix}$ má inverzní matici $A^{-1}=\begin{pmatrix}\frac{1}{2}&0\\0&1\end{pmatrix}$ v oboru reálných čísel, ale v oboru celých čísel už invertibilní není (stává se singulární). Ještě zajímavější to je, když začneme pracovat v $\mathbb{Z}_n$. Podíváme se, na které věci se stále můžeme spolehnout (to bude krátký seznam) a kde naopak může číhat překvapení.

7c.1 Matice nad $\mathbb{Z}_n$

Začneme dobrou zprávou: Sčítání a násobení matic i přechod k transponované matici fungují v $\mathbb{Z}$ i v $\mathbb{Z}_n$ přesně tak, jak jsme zvyklí. Rovněž determinanty mají stále dobrý smysl a můžeme je počítat podle definice (přes všechny permutace, což známe dobře pro matice 2×2 a 3×3) a také rozvojem podle sloupce či řádku. Platí také, že podle determinantu poznáme, zda je matice regulární neboli invertibilní, tedy zda k ní existuje inverzní matice. Zde si ale musíme kritérium trochu upravit.

Věta 7c.2.
Ke čtvercové matici A nad $\mathbb{Z}_n$ existuje matice inverzní právě tehdy, když je její determinant $|A|$ invertibilní v $\mathbb{Z}_n$.
Tato inverzní matice je pak dána vzorcem $A^{-1}=|A|^{-1}D^T$, kde D je matice kofaktorů.

Připomeňme, že prvek d_{ij} matice D získáme tak, že z matice A vyškrtneme řádek i a sloupec j, spočítáme determinant výsledné matice a vynásobíme jej číslem $(-1)^{i+j}$.

Tato věta je zobecněním situace z reálného oboru, kde jsou regulární ty matice, které mají nenulový determinant, což souhlasí, právě nenulová čísla jsou v $\mathbb{R}$ invertibilní. Podobně matice nad $\mathbb{Z}$ jsou regulární právě tehdy, když mají determinant roven ± 1.

Příklad 7c.a: Najdeme A^{-1} pro $A=\begin{pmatrix}2&3\\4&13\end{pmatrix}$ v prostoru $\mathbb{Z}_{45}$.

Nejprve spočítáme $|A|=2\cdot 13-4\cdot 3=14$. Protože $\gcd(14,45)=1$, je 14 invertibilní v $\mathbb{Z}_{45}$ a tudíž je i A regulární.

Rovnou najdeme $|A|^{-1}=14^{-1}$ v $\mathbb{Z}_{45}$. Pomocí rozšířeného Euklidova algoritmu získáme $1=5\cdot 45+(-16)\cdot 14$, proto $(-16)\cdot 14\equiv 1 \pmod{45}$, tedy $14^{-1}=29$ v $\mathbb{Z}_{45}$.

Teď sestavíme matici D: d_{11} dostaneme vyškrtnutím prvního řádku a sloupce z A a nalezením determinantu výsledné matice (13), výsledek je $d_{11} = (-1)^{1+1} \cdot 13 = 13$, podobně je $d_{12} = (-1)^{1+2} \cdot 4 = -4 \equiv 41 \pmod{45}$, $d_{21} = (-1)^{2+1} \cdot 3 = -3 \equiv 42 \pmod{45}$, $d_{22} = (-1)^{2+2} \cdot 2 = 2$. Proto $D = \begin{pmatrix} 13 & 41 \\ 42 & 2 \end{pmatrix}$ a tedy

$$A^{-1} = 29 \begin{pmatrix} 13 & 42 \\ 41 & 2 \end{pmatrix} = \begin{pmatrix} 17 & 3 \\ 19 & 13 \end{pmatrix}.$$

Ověřte, že opravdu $\begin{pmatrix} 2 & 3 \\ 4 & 13 \end{pmatrix} \begin{pmatrix} 17 & 3 \\ 19 & 13 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ při počítání v $\mathbb{Z}_{45}$.

△

Čtenáře možná napadne, proč jsme u metod výpočtu determinantu, popřípadě u metody výpočtu inverzní matice neuvedli Gaussovu eliminaci. Důvod je jednoduchý, tato metoda totiž při práci v $\mathbb{Z}_n$ naráží na nečekané potíže.

Příklad 7c.b: Uvažujme matici $A = \begin{pmatrix} 2 & 3 \\ 2 & 2 \end{pmatrix}$ nad $\mathbb{Z}_6$. Výpočtem modulo 6 hravě zjistíme, že tato matice má determinant $|A| = 2 \cdot 2 - 3 \cdot 2 = 2 \cdot 2 + 3 \cdot 2 = 4$.

Jak bychom na to útočili Gaussovkou? Nejprve bychom si vyrobili vlevo nahoře jedničku dělením prvního řádku dvěma, což ovšem v Z_6 nejde, tam umíme jen násobit. Protože $\gcd(2, 6) > 1$, nemáme inverzní prvek k 2 a tudíž pomocí násobení z dvojky jedničku neuděláme. Z podobného důvodu si násobením nevyrobíme jedničku ani na začátku druhého řádku.

To ale zase takový problém není, pro nás je teď hlavním cílem trojúhelníkový tvar, což zde uděláme relativně snadno, stačí přičíst první řádek vynásobený dvěma k řádku druhému a dostaneme $\begin{pmatrix} 2 & 3 \\ 0 & 2 \end{pmatrix}$, což vypadá nadějně. Otázka ovšem zní, zda je tato operace korektní i nad $\mathbb{Z}_n$. Odpověď zní, že ano, přičítání násobku jednoho řádku k řádku jinému je i nad $\mathbb{Z}$ či $\mathbb{Z}_n$ zcela korektní úprava. Nová matice proto musí mít a evidentně má determinant 4. Co bychom ale dělali, kdyby v druhém řádku nebylo číslo, které lze takto vynulovat (tedy pokud by tam nebyl násobek dvou)? Začalo by to být zajímavé.

Máme ovšem ještě další oblíbenou operaci, tedy násobení řádku číslem. Co dostaneme, když v nové matici vynásobíme druhý řádek trojkou? Matici $\begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix}$, která má determinant nulový, což jasně ukazuje, že to není korektní úprava.

Přemýšlivějšího čtenáře možná napadne, že problém trojky je v tom, že je dělitelem nuly, viz kapitola 8c. Pokud násobíme řádky výhradně čísly, která jsou v daném $\mathbb{Z}_n$ invertibilní, pak se problémům tohoto typu vyhneme, na druhou stranu si takovým pravidlem silně omezujeme možnosti výpočtu. Praktickým důsledkem je, že Gaussova eliminační metoda přestává být spolehlivým nástrojem pro výpočet determinantu, výpočet inverzní matice či řešení soustav rovnic.

△

Protože na Gaussově eliminaci závisí důkaz toho, že transponováním reálné matice se nezmění její hodnost, naskýtá se otázka, zda i nad $\mathbb{Z}_n$ platí důležitá rovnost $\hod(A^T) = \hod(A)$. Ukáže se, že ne, což je docela problém.

Příklad 7c.c: Uvažujme matici $A = \begin{pmatrix} 1 & 1 & 29 \\ 0 & 2 & 3 \end{pmatrix}$ nad $\mathbb{Z}_{30}$.

Vzhledem k jejímu tvaru by se zdálo, že řádky jsou lineárně nezávislé, tudíž má hodnost 2. Pro jistotu to zkusíme pořádně podle definice: Jaká řešení má rovnost $\alpha(1, 1, 29) + \beta(0, 2, 3) = (0, 0, 0)$?

Vzniká tak soustava $\alpha = 0$, $\alpha + 2\beta = 0$ a $29\alpha + 3\beta = 0$ řešená v $\mathbb{Z}_{30}$. Z první rovnice dosadíme do druhých dvou a máme systém $2\beta = 0$ a $3\beta = 0$ v $\mathbb{Z}_{30}$. Rovnice $2\beta = 0$ má v $\mathbb{Z}_{30}$ množinu řešení $\{0, 15\}$, rovnice $3\beta = 0$ má v $\mathbb{Z}_{30}$ množinu řešení $\{0, 10, 20\}$ a celý systém má tedy jediné řešené $\beta = 0$. Řešená vektorová rovnice má tedy jen triviální řešení a vektory jsou proto lineárně nezávislé.

Teď se podíváme na transponovanou matici $A^T = \begin{pmatrix} 1 & 0 \\ 1 & 2 \\ 29 & 3 \end{pmatrix}$. Podle definice je její hodnost rovna maximálnímu počtu lineárně nezávislých řádků. Ukážeme, že žádné dva nejsou lineárně nezávislé, protože z každé dvojice umíme vyrobit pomocí netriviální lineární kombinace nulový řádek:

$$15 \cdot (1, 0) + 15 \cdot (1, 2) = (0, 0), \quad 10 \cdot (1, 0) + 10 \cdot (29, 3) = (0, 0), \quad 6 \cdot (1, 2) + 6 \cdot (29, 3) = (0, 0).$$

To dokazuje, že maximální počet lineárně nezávislých řádků této transponované matice je 1, tedy $\hod(A^T) = 1$.

△

Těmto nepříjemnostem se vyhneme, pokud se nám podaří pracovat v $\mathbb{Z}_n$, kde n je prvočíslo. Pak je totiž $\mathbb{Z}_n$ těleso (viz kapitola 8c), hlavně je každý nenulový prvek v $\mathbb{Z}_n$ invertibilní a tudíž se zase můžeme odvolávat na své zkušenosti z práce nad $\mathbb{R}$, například nám bude fungovat Gaussovka. Inverzní matici tedy bude možné hledat převodem $(A|E_n)$ pomocí řádkových úprav na $(E_n|A^{-1})$, což je samozřejmě ta nejpraktičtější metoda.

Příklad 7c.d: Najdeme matici inverzní k $A = \begin{pmatrix} 2 & 3 \\ 4 & 0 \end{pmatrix}$ nad $\mathbb{Z}_5$.

Je vůbec regulární? V $\mathbb{Z}_5$ počítáme $|A| = 2 \cdot 0 - 4 \cdot 3 = -12 = 3$, což je v $\mathbb{Z}_5$ invertibilní. Proto s důvěrou upravujeme, pamatujeme si ovšem, že můžeme jen násobit a přičítat kladné násobky řádků. Nejprve přičteme první řádek k druhému, pak řádky prohodíme a přičteme trojnásobek nového prvního řádku k řádku druhému.

$$\left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 1 & 3 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 3 & 1 & 1 \\ 2 & 3 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 3 & 1 & 1 \\ 0 & 2 & 4 & 3 \end{array}\right).$$

Nakonec přičteme druhý řádek k prvnímu a poté jej vynásobíme číslem $3 = 2^{-1}$.

$$\left(\begin{array}{cc|cc} 1 & 3 & 1 & 1 \\ 0 & 2 & 4 & 3 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 0 & 4 \\ 0 & 2 & 4 & 3 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 0 & 4 \\ 0 & 1 & 2 & 4 \end{array}\right).$$

Zkouška:

$$\begin{pmatrix} 2 & 3 \\ 4 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 4 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Takže opravdu $A^{-1} = \begin{pmatrix} 0 & 4 \\ 2 & 4 \end{pmatrix}$.

△

Jednou ze zajímavých aplikací lineární algebry nad $\mathbb{Z}_n$ jsou samoopravné kódy, o kterých se lze dočíst například ve skriptu kolegy Velebila zmíněném v úvodu.

7c.3 Polynomy nad $\mathbb{R}$ a $\mathbb{Z}$

Toto je opakovací kapitola, která jen připomene, co všechno nám bude chybět, když se pak přesuneme k $\mathbb{Z}_n$.

Polynomy nad $\mathbb{R}$ jsou výrazy typu $a_n x^n + \cdots + a_1 x + a_0$, jejichž koeficienty a_i jsou z $\mathbb{R}$, třeba $p = \sqrt{2}\, x^5 - \pi x + e$. Množina všech takovýchto polynomů se značí $\mathbb{R}[x]$. Pro polynomy máme pravidla pro sčítání a násobení číslem (třeba umíme spočítat $3p$ pro ten polynom výše) i pro násobení polynomů mezi sebou, například pro $p = x + 1$ a $q = x - 1$ dostáváme $p \cdot q = x^2 - 1$.

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

U polynomů $a_n x^n + \cdots + a_0$ umíme obecně zadefinovat stupeň polynomu jako největší koeficient i takový, aby $a_i \neq 0$, a pro polynomy reálné se stupeň chová velice rozumně. Reálné polynomy dokonce umíme i navzájem dělit se zbytkem a zbytek po dělení i částečný podíl jsou jednoznačné (viz Věta o dělení pro čísla 6a.6). Shrneme si to základní ve větě.

Věta 7c.4.
Uvažujme polynomy p, q nad $\mathbb{R}$. Pak platí následující:
(i) $\mathrm{st}(pq) = \mathrm{st}(p) + \mathrm{st}(q)$.
(ii) Existují jediné polynomy d a r takové, že $p = d \cdot q + r$ a $\mathrm{st}(r) < \mathrm{st}(q)$.
(iii) Polynom p má nejvýše $\mathrm{st}(p)$ kořenů v $\mathbb{R}$.
(iv) $a \in \mathbb{R}$ je kořenem p právě tehdy, když polynom $x - a$ dělí p.

Pro polynomy můžeme definovat i dělitelnost naprosto stejným způsobem jako pro celá čísla, tedy $q \,|\, p$ pokud existuje polynom r tak, aby $p = qr$. Například polynom $q = x - 1$ dělí polynom $p = x^2 - x$, protože $p = q \cdot r$ pro volbu $r = x$.

Když máme dělitelnost, můžeme zkusit vymyslet pojem největší společný dělitel. Tady je ale problém v nejednoznačnosti rozkladu, kdy můžeme násobící konstanty dle libosti přesouvat mezi faktory, například takto:

$$4x^2 - 16 = (4x - 8)(x + 2) = (2x - 4)(2x + 4) = (x - 2)(4x + 8) = \left(\tfrac{1}{2}x - 1\right)(8x + 16) = \ldots$$

Naštěstí to ale není až tak hrozné, protože v zásadě jsou jen faktory dva, $x-2$ a $x+2$, které chytře vynásobíme konstantami tak, aby to celkově vyšlo. Když tedy mluvíme u reálných polynomů o faktorech, tak tím ani tak nemyslíme konkrétní polynomy, jako spíš množiny, jeden „faktor“ je polynom $x-2$ a všechny jeho nenulové násobky, druhý „faktor“ je $x+2$ a všechny jeho nenulové násobky. Není to až zas tak velký problém, například $x-2$ i všechny jeho nenulové násobky mají stejný stupeň, stejné kořeny a podobně, takže je to z hlediska vlastností množina stejných věcí. Samozřejmě pokud bychom chtěli tuto definici vybudovat pořádně a matematicky korektně, museli bychom se s tímto vypořádat, ale zde si jen tak povídáme.

Když pak u reálných polynomů hledáme největšího společného dělitele, tak přirozeně dostaneme množinu polynomů, které jsou zase jeden vzorový polynom a všechny jeho násobky nenulovými konstantami, což se dá vnímat jako rozumná odpověď. Existuje zajímavý způsob, jak vyjádřit, že jde vlastně o stejný polynom až na násobení konstantou. Platí, že všechny polynomy z této množiny se navzájem dělí.

Příklad: Pro polynomy $p = 8x^2+4x$ a $q = 8x^2-16x$ snadno najdeme společné dělitele stupně 1, jmenovitě x, $2x$, $4x$, ale třeba i $20x$ nebo $\sqrt{13}x$. Opravdu je $20x$ společným dělitelem? Ano, $p = 20x\cdot\left(\frac{2}{5}x+\frac{1}{5}\right)$ a $q = 20x\cdot\left(\frac{2}{5}x-\frac{4}{5}\right)$. Vidíme, že největší společný dělitel je množina polynomů ve tvaru ax pro $a\neq 0$ a opravdu libovolné dva z nich se navzájem dělí ve smyslu polynomů, třeba $4x$ dělí $6x$, protože $6x = \frac{3}{2}(4x)$ a $r=\frac{3}{2}$ je polynom a naopak $4x = \frac{2}{3}(6x)$ a $r=\frac{2}{3}$ je polynom.

Něco podobného už ostatně známe: Při hledání největšího společného dělitele čísel $a,b\in\mathbb{Z}$ jsme dostali jednoznačný výsledek jedině díky tomu, že jsme se omezili jen na kladná čísla. Kdybychom se takto neomezili, pak bychom vlastně měli dva největší společné dělitele, číslo $\gcd(a,b)$ a číslo $-\gcd(a,b)$, přičemž hned vidíme, že se navzájem dělí, takže jde o situaci podobnou jako u těch polynomů.

Není těžké ukázat, že rozšířený Euklidův algoritmus (který využívá jen dělitelnost se zbytkem) funguje i pro polynomy, jeho výsledkem je jeden z polynomů, které lze považovat za největší společný dělitel, a jeho vyjádření pomocí vstupních polynomů. Prostor $\mathbb{R}[x]$ se tedy chová velice civilizovaně.

Obdobně můžeme definovat $\mathbb{Z}[x]$ jako množinu všech polynomů $a_nx^n+\cdots+a_0$, jejichž koeficienty jsou ze $\mathbb{Z}$, kupodivu pak věci fungují úplně stejně. Zase si odpovídají polynomy jako výrazy s funkcemi, přesně řečeno koeficienty takového výrazu jsou jednoznačně určeny hodnotami z něj vzniklé funkce. To se občas velice hodí a my to využijeme v kapitole 10b v tzv. metodě neučitých koeficientů. Také bychom teď mohli opsat Větu výše, jen se změnou $\mathbb{R}$ v $\mathbb{Z}$, a platila by, stejně jako je pro $\mathbb{Z}[x]$ pravdivá i poznámka za ní o dělitelnosti, Euklidovi atd. a můžeme se spolehnout na rozšířený Euklidův algoritmus. Máme i obdobný problém s jednoznačností rozkladu a gcd.

Rozdíly mezi polynomy nad $\mathbb{R}$ a $\mathbb{Z}$ přesto jsou. Čtenáře asi hned napadne, že polynomy nad $\mathbb{Z}$ nemívají tolik kořenů jako polynomy nad $\mathbb{R}$. Třeba polynom $p(x)=2x-1$ má nad $\mathbb{R}$ kořen $x=\frac{1}{2}$, zatímco nad $\mathbb{Z}$ žádný kořen nemá. To je ale spíš podružné.

Podstatnější jsou komplikace, které nastanou okolo dělitelnosti. Například pro polynomy $p=8x^2+4x$ a $q=8x^2-16x$ brány nad $\mathbb{Z}$ dostaneme jako největší společný dělitel jen množinu $\{x,2x,4x\}$. Na rozdíl od reálného případy již neplatí, že by se všechny navzájem dělily, takže toto kritérium, jak poznat, že jde v zásadě o tentýž objekt, nelze použít pro práci nad $\mathbb{Z}$. Nicméně to hlavní funguje podobně, ani u polynomů nad $\mathbb{Z}$ nečíhají nějaké zásadní záludnosti.

7c.5 Polynomy nad $\mathbb{Z}_n$

Obsah této části se dá shrnout velice snadno. Jakmile začneme pracovat s polynomy nad $\mathbb{Z}_n$, tak už se nedá spoléhat na nic, co jsme připomněli v předchozí části.

Začneme tím, že hodnoty polynomu už jej nemusí jednoznačně určovat.

Příklad 7c.e: Polynom $p=x^3$ nad $\mathbb{Z}_6$ definuje tuto funkci: $p(0)=0$, $p(1)=1^3=1$, $p(2)=2^3\equiv 2 \pmod 6$, $p(3)=3^3\equiv 3 \pmod 6$, $p(4)=4^3\equiv 4 \pmod 6$ a $p(5)=5^3\equiv 5 \pmod 6$, což je přesně stejná funkce, jakou definuje polynom $q=x$. To tedy znamená, že dva zcela různé polynomy dávají stejnou funkci.

Praktický dopad je, že přestávají fungovat mnohé oblíbené metody na určování koeficientů. Například když nám někdo dodá informaci, že jistý celostátně hledaný polynom $ax^5+bx^4+cx^3+dx^2+ex+f$ splňuje rovnici $2x^3+2x = ax^5+bx^4+cx^3+dx^2+ex+f$ pro všechna $x\in\mathbb{Z}_6$ (tedy jde o rovnost funkcí), tak už nemusí platit, že je to zrovna ten $2x^3+2x$, klidně to může být i polynom $4x$. Ověřte si, že ani ten není sám, vyhovují třeba i polynomy $4x$, $4x^3$, $4x^5$, $2x^5+x^3+x$ a mnoho dalších.

To je zásadní změna. Mnoho úloh, u kterých oprávněně čekáme jednoznačné řešení při práci nad $\mathbb{R}$, může mít po přechodu do světa $\mathbb{Z}_n[x]$ třeba i nekonečně mnoho řešení.

△

To je ovšem teprve začátek. Rozpadnou se zcela i naše představy o kořenech polynomů a jejich rozkladech.

Příklad 7c.f: Polynom $p = 2x^2 + 1$ nad $\mathbb{Z}_6$ dává funkci $p(0) = p(3) = 1$ a $p(1) = p(2) = p(4) = p(5) = 3$, takže tento polynom nemá kořeny. To zase není nic divného (nemá je ani nad $\mathbb{R}$), ale málokterý čtenář by asi čekal, že tento polynom lze přesto rozložit na lineární faktory! Ověřte si pro sebe roznásobením, že

$$2x^2 + 1 = (2x + 1)(4x + 1).$$

Rozkládat lze evidentně všelicos, čtenář by asi také nečekal třeba toto:

$$x = (3x + 4)(4x + 3) \text{ nad } \mathbb{Z}_6.$$

Zde je zajímavé, že $x = 0$ je evidentně kořenem polynomu nalevo, ale není to kořenem ani jednoho z faktorů napravo. Také to ukazuje, že rovnost $\mathrm{st}(pq) = \mathrm{st}(p) + \mathrm{st}(q)$ evidentně neplatí. Extrémní příklad: $3x(2x + 4) = 0$, součinem dvou polynomů stupně 1 dostaneme polynom stupně $-\infty$.

Poslední podivnosti: Uvažujme polynom $p = x^2 + x$ nad $\mathbb{Z}_6$. Přesvědčte se, že čísla $x = 0, 2, 3, 5$ jsou kořeny tohoto polynomu, je tedy více kořenů, než je stupeň polynomu. Extrémní příklad v tomto směru: polynom $p = 2x^3 + 4x$ nad $\mathbb{Z}_6$ je jako funkce roven identicky nule, tedy všechna čísla ze $\mathbb{Z}_6$ jsou jeho kořeny!

△

Podíváme-li se do Věty 7c.4 o vlastnostech reálných polynomů, tak nám tento příklad ukázal, že při práci nad $\mathbb{Z}_n$ přestávají obecně platit tvrzení (i) a (iii). Teď si pokazíme i (ii).

Příklad 7c.g: Zkusíme vydělit se zbytkem polynom $p = x$ polynomem $q = 3x+4$ nad $\mathbb{Z}_6$. V předchozím příkladě jsme už jeden rozklad viděli:

$$x = (4x + 3)(3x + 4) + 0.$$

Dá se ovšem zkusit třeba toto:

$$x = 2 \cdot (3x + 4) + 4.$$

Nemáme tedy jednoznačnost, není proto definován ani zbytek po dělení p polynomem q. Mimochodem pokus o zbytek jednou vyšel 0 a podruhé nenulový, je tedy p dělitelné polynomem q? Zde naštěstí zmatek nevzniká, v definici se říká, že q dělí p, pokud lze vyjádřit p jako násobek q, což zde lze a víc už definice neřeší. Takže q dělí p.

△

Tento příklad tedy ukazuje, že pojem dělitelnosti se vybudovat dá, ale rozumné dělení se zbytkem nemáme. Pak už se ani nedá čekat rozumné fungování při hledání největšího společného dělitele.

Příklad 7c.h: Jak vypadá největší společný dělitel polynomů $p = x^2 + x$ a $q = x^2 + 5$ nad $\mathbb{Z}_6$? Podívejme se na rozklady:

$$x^2 + x = x(x + 1) = (x + 3)(x + 4),$$
$$x^2 + 5x = x(x + 5) = (x + 3)(x + 2).$$

Podle prvních rozkladů je společným dělitelem polynom x, podle druhých rozkladů je to zase $x + 3$. Oba jsou to ale polynomy prvního stupně, o kterých rozhodně neplatí, že by jeden byl násobkem druhého, což je nepříjemná komplikace.

△

Pracovat s polynomy nad $\mathbb{Z}_n$ je tedy dobrodružné.

Teď dobrá zpráva. Pokud je n prvočíslo, pak nám zase většina věcí bude fungovat, jak jsme zvyklí u $\mathbb{R}[x]$ (viz sekce 8c.4).

Věta 7c.6.
Nechť n je prvočíslo, uvažujme polynomy p, q nad $\mathbb{Z}_n$. Pak platí následující:
(i) $\mathrm{st}(pq) = \mathrm{st}(p) + \mathrm{st}(q)$.
(ii) Existují jediné polynomy d a r takové, že $p = d \cdot q + r$ a $\mathrm{st}(r) < \mathrm{st}(q)$.
(iii) Polynom p má nejvýše $\mathrm{st}(p)$ kořenů.
(iv) $a \in \mathbb{Z}_n$ je kořenem p právě tehdy, když polynom $x + (-a)$ dělí p.

Díky (ii) nám bude fungovat Euklidův algoritmus, zkusíme si to.

Příklad 7c.i: Najdeme $\gcd(x^3 + 3, x^2 + 1)$ pro polynomy nad $\mathbb{Z}_5$ pomocí rozšířeného Euklidova algoritmu.

Jeho nedílnou součástí je dělení se zbytkem, proto si zde připomeneme, jak to funguje pro polynomy. Když budeme počítat $\gcd(x^3 + 3, x^2 + 1)$, prvním krokem bude vydělení $(x^3 + 3) : (x^2 + 1)$. Algoritmus:

1. Vydělíme nejvyšší mocniny, výsledek je x.

2. Najdeme zbytek jako $(x^3+3)-x\cdot(x^2+1)=3-x\equiv 3+4x \pmod 5$.

3. Pokud má zbytek nižší stupeň než dělitel, algoritmus končí, viz zde $\mathrm{st}(4x+3)<\mathrm{st}(x^2+1)$. V opačném případě se vrátíme do kroku 1 s tím, že dělíme zbytek původním dělitelem.

Příklad neukázal, co bychom dělali, kdyby u vedoucích mocnin byly koeficienty. Pak bychom v kroku 1 čelili třeba tomuto: $(2x^5):(3x^2)$. V takovém případě nejprve vydělíme mocniny, vyjde x^3, a pak se postaráme o koeficienty, přičemž dělení převádíme na násobení inverzním prvkem modulo n. V tomto případě namísto $2:3$ počítáme $2\cdot 3^{-1}=2\cdot 2=4$, použili jsme, že $3^{-1}=2 \pmod 5$, což jsme odhadli zkusmo. Výsledek je $(2x^5):(3x^2)=4x^3$.

Teď už by nás nemělo v následujícím běhu Euklidova algoritmu nic překvapit.

a,b	q	A	B	Použito
x^3+3		1	0	
x^2+1	x	0	1	$(x^3+3):(x^2+1)=x$, zbytek $4x+3$
$4x+3\bullet$	$4x+2$	$1\bullet$	$-x=4x\bullet$	$(x^2+1):(4x+3)=4x+2$, zb. 0
0				

Vychází nám $\gcd(x^3+3,x^2+1)=4x+3$, což snadno ověříme:

$$x^3+3=(4x+3)(4x^2+2x+1),\qquad x^2+1=(4x+3)(4x+2).$$

Máme také Bezoutovu identitu $4x+3=1\cdot(x^3+3)+4x\cdot(x^2+1)$, což souhlasí.

Zajímavá věc:

$$x^3+3=(x+2)(x^2+3x+4),\qquad x^2+1=(x+2)(x+3).$$

Takže také $\gcd(x^3+3,x^2+1)=x+2$. Potvrzuje se tedy naše očekávání, u polynomů dostáváme jako největší společný dělitel ne jeden, ale celou množinu polynomů. Ovšem tvrdili jsme, že pro prvočíslo $n=5$ bychom měli mít podobnou situaci jako u $\mathbb{R}$, tedy všechny tyto polynomy by měly být násobky (konstantou) jednoho vzorového polynomu. Je opravdu náš nový kandidát $x+2$ násobkem toho, který vyšel z Euklida? Ano, $x+2=4\cdot(4x+3)$.

Snadno se ověří, že libovolný nenulový násobek polynomu $x+2$ je také společným dělitelem, protože například rozklad u prvního polynomu lze zapsat jako $x^3+3=[a(x+2)]\cdot[a^{-1}(x^2+3x+4)]$. Dá se ukázat, že jiní společní dělitelé nejsou.

△

Psali jsme, že „většina bude fungovat“, takže je dobré ještě přidat varování, kde i pro n prvočíselné může být problém. Asi nejpalčivější je, že různé polynomy mohou pořád dávat stejné funkce, například nad $\mathbb{Z}_2$ oba polynomy 1 a x^2+x+1 dávají konstantní funkci $x\mapsto 1$. Konec konců, nemusíme ani složitě shánět příklady: Pro prvočíslo n platí malá Fermatova věta a tu lze číst i tak, že polynomy x a x^n dávají stejné funkce.

Musíme si také dávat pozor, abychom do práce v $\mathbb{Z}_n$ nepřenášeli návyky z reálných polynomů, například automaticky považujeme polynomy typu x^2+1 za nerozložitelné a bez kořenů, ale nad Z_5 má tento polynom kořeny $x=2,3$ a lze jej napsat jako $x^2+1=(x+2)(x+3)$.

Tímto končíme stručnou exkurzi do podivuhodného světa polynomů nad $\mathbb{Z}_n$, který má mimochodem zásadní aplikace například při kódování.