

3. 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 2.

V mnoha situacích se stává, že při práci s objekty nějakého typu nerozlišujeme mezi individuálními zástupci, ale rozdělíme si je do typů a nic víc nás nezajímá. Například mince máme rozděleny podle jejich hodnoty. Určitě existuje mnoho individuálních a rozeznatelných pětikorun lišících se datem vydání a způsobem ošoupaní, ale nám je to jedno, pro nás je pětikoruna jako pětikoruna.

V této kapitole prozkoumáme jednu takovou situaci, samozřejmě matematickou.

3a. Kongruence, počítání modulo

Existují situace, kdy ztotožňujeme různá čísla. Pro příklad nemusíme chodit daleko, při počítání hodin je pro nás obvykle 13 totéž co 1. Nemáme problém s takovými ztotožněnými čísly počítat, například pokud v jedenáct požádáme počítač o zkompilevání tří domácích videí a každé zabere dvě hodiny, tak hravě spočítáme, že skončí v pět. Dokonce i při používání cyklu 24 hodin musíme občas takto ztotožňovat, takže když například v 15 hodin spustíme kultivaci vzorku, která má jet 56 hodin, tak víme, že skončíme o pár dní později v jedenáct v noci, protože čísla 71 a 23 udávají tutéž denní dobu.

Tento příklad je krásnou inspirací pro následující pojem.

Definice.

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

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 $n \mid (b - a)$.

Někteří autoři používají definici $n \mid (a - b)$, jak brzy uvidíme, vyjde to nastejno.

Příklad 3a.a: Z hodin víme, že $21 \equiv 9 \pmod{12}$. Zkouška podle definice: $9 - 21 = -12$, což je dělitelné dvanácti. Jiný příklad: $(-2) \equiv 13 \pmod{5}$, protože $13 - (-2) = 15$, což je dělitelné pěti.

△

Někdy se hodí poznávat kongruenci jinak než podle definice.

Věta 3a.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 $b = a + kn$,
- (iii) $a \bmod n = b \bmod n$, tj. jsou si rovny zbytky po dělení číslem n .

S Rozbor: Přesný význam uvozovací věty je, že libovolná dvě tvrzení z oněch tří jsou spolu ekvivalentní, jde tedy o tři ekvivalence. Ty tradičně dokazujeme pomocí implikace v obou směrech, takže bychom formálně vzato měli dokazovat šest implikací. To se ale nedělá, místo toho se volí metoda kolečka, kdy tvrzení propojíme jednou cestou dokola. V tomto případě není důvod preferovat nějaký speciální průchod, tak to uděláme, jak to přišlo, tedy dokážeme implikace (i) \implies (ii), (ii) \implies (iii) a nakonec (iii) \implies (i), která uzavře cyklus. Díky možnosti navazování implikací pak už automaticky platí i všechny další implikace, například spojením druhých dvou dostáváme pravdivost implikace (ii) \implies (i). Tato obíhačka nám ušetřila polovinu práce.

Rozmyslete si, že kdybychom dokazovali vzájemnou ekvivalenci pěti podmínek, tak bychom formálně museli probrat $4 \cdot 5 = 20$ implikací, ale trik s obíhačkou by tuto práci zredukoval na pět. To už je docela úspora.

Důkazy samotné jsou (většinou) přímočaré a snadné, stačí si u každé implikace napsat, co víme a co potřebujeme, a cesta by se měla nabídnout.

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

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

(iii) \implies (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. \square

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 3a.b: Ověříme, že $21 \equiv 9 \pmod{6}$. Podle definice máme zkusit, zda 6 dělí $9 - 21 = -12$, což tedy platí.

Podle podmínky (ii) to vidíme také, dvojnásobkem odečtením 6 od 21 dostaneme 9. I zbytky po dělení hravě spočítáme, $21 \bmod 6 = 3$ a $9 \bmod 6 = 3$ se rovnají a podmínka (iii) dává $21 \equiv 9 \pmod{6}$.

Podmínka (ii) bývá pro mnohé pohodlná, když dojde na záporná čísla, nemusí si tolik dávat pozor na znaménka. Například dvojnásobkem odečtením trojky od -68 dostaneme -74 , proto určitě $-68 \equiv -74 \pmod{3}$, mnoha lidem to přijde pohodlnější než odečítat $(-74) - (-68)$.

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 $37 \equiv 12 \pmod{5}$.

\triangle

Když se přeneseme do světa nějakého konkrétního modula n , stane se několik věcí. Ta hlavní je, že se množina celých čísel rozpadne na přirozené skupiny. V případě $n = 5$ například vidíme, že $3 \equiv 8 \equiv 13 \equiv 18 \equiv 23 \equiv \dots$ a také $3 \equiv -2 \equiv -7 \equiv -12 \equiv -17 \equiv \dots$. Vznikla nám skupina čísel $\{\dots, -17, -12, -7, -2, 3, 8, 13, 18, 23, \dots\}$, kterou jsme vygenerovali z trojky a dá se zapsat jako $\{3 + 5k : k \in \mathbb{Z}\}$. Důležité na takové skupině je, že všichni její členové jsou navzájem kongruentní modulo 5. Je také snadné si rozmyslet, že bychom úplně stejnou skupinu vygenerovali třeba z třináctky. Jedenáctka by pak vygenerovala skupinu $\{\dots, -14, -9, -4, 1, 6, 11, 16, 21, \dots\}$, kterou lze zapsat například takto: $\{6 + 5k : k \in \mathbb{Z}\}$.

Dokážeme teď tvrzení, které vystihne klíčové vlastnosti stojící za tímto sdružováním čísel.

Fakt 3a.2.

Nechť $n \in \mathbb{N}$. Pak platí:

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

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

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

S Rozbor: Tvrzení (i) nemá předpoklady, máme prostě něco dokázat. Pokud si napíšete podle definice, co se po nás chce, určitě důkaz uvidíte. Necháme jej jako cvičení 3a.5.

Druhé tvrzení je ekvivalence, takže bychom měli provést dva důkazy implikace. Protože jsou však role a a b zcela zaměnitelné, bude stačit implikace jedna, třeba zleva doprava. Situace je pak dle definice následující:

- Známο: n dělí $b - a$
- Chceme: n dělí $a - b$.

Teď již jistě naleznete můstek zleva doprava, odvoláme se na stejné cvičení. Abychom všechno nenechali na čtenáři, ukážeme jako inspiraci alespoň důkaz trojky, kde zároveň ukážeme využití alternativního testu pro kongruenci.

Důkaz (rutinní): (iii): Jestliže $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, pak podle věty 3a.1 máme $b = a + kn$ pro nějaké $k \in \mathbb{Z}$ a $c = b + ln$ pro nějaké $l \in \mathbb{Z}$. Odtud $c = a + (k+l)n$ a $(k+l) \in \mathbb{Z}$, tedy podle stejné věty $a \equiv c \pmod{n}$. \square

Tyto tři vlastnosti mají svá jména a věnujeme jim dokonce dvě kapitoly o relacích. Pomocí nich teď snadno dokážeme základní poznatky o skupinách, na které se nám rozpadla množina \mathbb{Z} po zavedení modula n .

- Všechna čísla z jedné skupiny jsou navzájem kongruentní.

Abychom to dokázali, vezmeme nějaké celé číslo a a libovolná dvě čísla x, y , která jsou v jeho skupině, tedy $a \equiv x \pmod{n}$ a $a \equiv y \pmod{n}$. Potřebujeme tato dvě čísla propojit kongruencí, dá se čekat, že to nějakým způsobem půjde odvodit z těch dvou předpokladů. Přidáme-li nápovědu, že se má použít fakt 3a.2, mohl by to čtenář vymyslet.

Důkaz: Podle (ii) lze jeden předpoklad přepsat jako $x \equiv a \pmod{n}$, dostáváme řetízek $x \equiv a \equiv y$. Podle (iii) pak $x \equiv y \pmod{n}$.

- Pokud čísla a a b nejsou kongruentní, tak nejenže jsou jejich skupiny disjunktní, ale dokonce se ani nemůže stát, že by se našlo číslo x ve skupině a a číslo y ze skupiny b takové, že x, y jsou kongruentní.

Dokazovat, že se něco nestane, bývá obvykle obtížnější, typicky proto přecházíme k důkazu sporem či obměnou. Zkusíme spor.

Důkaz: Budeme předpokládat, že existují x, y takové, že $a \equiv x \pmod{n}$ a $b \equiv y \pmod{n}$, a také platí $x \equiv y \pmod{n}$. Pomocí (ii) dostáváme řetízek $a \equiv x \equiv y \equiv b \pmod{n}$, ze kterého dvojným použitím (iii) odvodíme nejprve $a \equiv y \equiv b \pmod{n}$ a pak $a \equiv b \pmod{n}$, což odporuje předpokladu, že a, b nejsou kongruentní.

Tím jsme si potvrdili naši intuitivní představu, že se množina celých čísel přechodem k modulu rozpadne na skupiny, které jsou od sebe izolovány ve smyslu kongruence a zároveň v rámci každé skupiny máme vzájemnou kongruenci mezi všemi členy. Pěkně je to vidět na příkladu modulu $n = 2$. Čísla jsou spolu kongruentní přesně tehdy, pokud mají stejnou paritu, tedy sudá se sudými a lichá s lichými. Vzniknou proto skupiny $\{0, 2, -2, 4, -4, \dots\}$ a $\{1, -1, 3, -3, 5, -5, \dots\}$.

Zdá se také jasné, že obecně by u modulu n těch skupin mělo být vždy n a brzy to dokážeme. Odborně se těmto skupinám říká **zbytkové třídy**, ale s oficiálním zavedením si počkáme až na kapitolu 6b.

Teď bychom rádi vystihli to, že čísla z jedné skupiny lze často při práci vzájemně zaměňovat, nebo řečeno jinak, můžeme si z každé skupiny vybírat zástupce dle libosti. Nebude to možné úplně vždycky, záleží na tom, co děláme, ale rozhodně to platí při algebraických výpočtech.

Věta 3a.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) $ab \equiv uv \pmod{n}$.

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

- Jestliže $a \equiv u \pmod{n}$ a $b \equiv v \pmod{n}$, pak $a + b \equiv u + v \pmod{n}$.

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

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

Je potřeba najít můstek vedoucí od poznatků nalevo k tomu napravo. Někomu může přijít jednodušší pracovat s násobky než s pojmem dělitelnosti. Pomocí věty 3a.1 lze naši situaci přepsat takto:

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

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

Důkaz (poučný): (iii): Podle předpokladu a věty 3a.1 platí $u = a + kn$ a $v = b + ln$ pro nějaká $k, l \in \mathbb{Z}$. Pak máme také $uv = ab + aln + bkn + kln^2 = (ab) + (al + bk + kln)n$ a $(al + bk + kln) \in \mathbb{Z}$, závěr zase plyne z dotyčné věty.

Důkazy (i) a (ii) necháme jako cvičení 3a.7, jsou obdobné. □

Přeloženo do lidštiny, třeba (i) říká, že když při sčítání nahradíme čísla nějakými jejich kongruentními zástupci, tak dostaneme stejný výsledek, ovšem ve světě dotyčného modulu. Proto můžeme například ve světě modulu 5 místo výpočtu $195376 \cdot 16239 + 32532675$ počítat třeba $1 \cdot 4 + 0 = 4$ či ještě lépe $1 \cdot (-1) + 0 = -1$ a výsledky se budou (modulo 5) rovnat. Věta nás nenutí k výběru nějakých speciálních zástupců, obvykle preferujeme co nejmenší. Jeden speciální tu vždycky je k dispozici.

Fakt 3a.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 $r - a = -qn$, tedy n dělí $r - a$. □

Protože je možných zbytků právě n , potvrdili jsme náš pocit, že po zavedení modulu vznikne právě n skupin čísel, jmenovitě skupiny kongruentní s čísly $0, 1, \dots, n - 1$.

Poznamenejme nicméně, že ne vždy je zrovna zbytek po dělení tím nejlepším zástupcem. Pokud potřebujeme spočítat $398 \cdot 1283$ modulo 100, pak přechod ke zbytkům dá $98 \cdot 83$, což je v pohodě pro počítač, při ručním výpočtu ale určitě dáme přednost verzi $(-2) \cdot (-17) = 34$.

Než se podíváme na další operace, zobecníme si právě dokázané vztahy na případy s více členy. Protože odčítání lze převést na sčítání záporných čísel, nebudeme ho zbytečně vypisovat. Zobecňování pravidel ze dvou na více se standardně dělá matematickou indukcí. Zatím jsme ji oficiálně neprobrali, ale mnozí čtenáři ji znají a v tomto důkazu je použita dosti transparentním způsobem, takže by to nemělo vadit. Je to taková upoutávka na důležité téma, které na nás čeká v další kapitole.

Důsledek 3a.5.

Nechť $n \in \mathbb{Z}$.

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

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

(ii) Uvažujme $a_1, b_1, u_1, v_1, \dots, a_m, b_m, u_m, v_m \in \mathbb{Z}$ takové, že $a_i \equiv u_i \pmod{n}$ a $b_i \equiv v_i \pmod{n}$ pro všechna $i = 1, \dots, m$. Pak $\sum_{i=1}^m a_i b_i \equiv \sum_{i=1}^m u_i v_i \pmod{n}$.

Důkaz (rutinní): (i): Dokážeme to indukcí na m pro sčítání, násobení necháme jako cvičení 3a.8.

(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 $a_1 \equiv u_1, \dots, a_m \equiv u_m$. Mějme čísla $a_1, u_1, \dots, a_{m+1}, u_{m+1}$ splňující $a_i \equiv u_i \pmod{n}$ pro všechna i . Podle indukčního předpokladu pak máme $\sum_{i=1}^m a_i \equiv \sum_{i=1}^m u_i \pmod{n}$, proto podle věty 3a.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 3a.3 (iii) platí $a_i b_i \equiv u_i v_i \pmod{n}$ pro všechna i , na tato čísla pak aplikujeme část (i) a sečteme je. □

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 3a.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 $a^k \equiv u^k \pmod{n}$.

S Rozbor: Vlastně to plyne už z právě dokázaného výsledku pro násobení, protože $a^k = a \cdot a \cdots a$. Pro zajímavost ukážeme ještě jeden důkaz. Jsme v situaci, kdy z předpokladu máme informaci $u - a = mn$ pro nějaké $m \in \mathbb{Z}$. Potřebujeme se pomocí tohoto faktu dozvědět něco o čísle $u^k - a^k$. Zde by se čtenáři mohl vybavit vzorec $u^2 - a^2 = (u - a)(u + a)$ či $u^3 - a^3 = (u - a)(u^2 + ua + a^2)$, který přivádí do hry právě výraz $u - a$. Obdobné vzorce platí i pro vyšší mocniny, čímž je plán důkazu hotov.

Důkaz (poučný): Podle předpokladu existuje $m \in \mathbb{Z}$ takové, že $u - a = mn$.

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

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

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

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

Další alternativní důkaz (indukcí) najdete jako cvičení. □

Příklad 3a.c: Vypočítáme, čemu je kongruentní výraz $(3 \cdot 5 \cdot 17 + 6 \cdot 3 + 10)^8 \cdot (2 + 35 - 4 \cdot 5)$ 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 3a.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:

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

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 zkušeni nejsme a navíc se tu snažíme pochopit i teorii, takže budeme pečlivě psát kongruence, ať v tom není zmatek.

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

Je to dáno tím, že mocnění ve skutečnosti není algebraická operace, ale speciální zápis (zkratka) pro opakované násobení. Třeba $a^4 = a \cdot a \cdot a \cdot a$, přičemž čísla a mohou být z různých světů (reálná čísla, celá, celá modulo n) a dokonce to ani nemusí být čísla, mocnit umíme třeba i matice či funkce. Exponent mocniny je ale vždy ze světa \mathbb{N} a není důvod, proč by pro něj měla platit pravidla ze světa, odkud bereme a , exponenty mají svá vlastní pravidla. Blíže se o tom dočteme v kapitole 10.

Nám by se samozřejmě zmenšování exponentů hodilo, určitě nechceme počítat třeba 13^{4179} přímo, ale na vhodné triky si musíme chvíli počkat.

Místo toho se podíváme ještě na jednu operaci, o které zatím nebyla řeč, jmenovitě na dělení. V praxi dělíme běžně v oboru reálných čísel (s výjimkou dělení nulou) a občas dokonce i v oboru celých čísel, třeba $6 \div 3 = 2$. Můžeme si to představit tak, že si to dělení vypůjčíme od reálných čísel (6 i 3 jsou také reálná čísla) a ke svému příjemnému překvapení zjistíme, že i výsledek najdeme v našem světě celých čísel. Někdy to nejde, třeba $7 \div 4$, to je život.

V matematické teorii operací se ale s dělením neworkuje, nejen kvůli nespolehlivosti třeba pro celá čísla, ale hlavně proto, že mu chybí určité vlastnosti, které jsou v teorii považovány za klíčové, zejména asociativita (viz kapitola 10). Místo toho se zavede převrácená hodnota $\frac{1}{a}$ a používá se lépe vychovaná operace násobení. Matematická teorie operací tedy před dělením $6 \div 3 = 2$ preferuje $6 \cdot \frac{1}{3} = 2$. Vyjde to samozřejmě nastejno, ale z hlediska teorie v tom brzy uvidíme rozdíl.

My bychom totiž rádi zavedli dělení do světa modulo a tam ten „půjčovací“ přístup zklame. Představme si, že chceme ve světě modula 5 vydělit $6 \div 3$. Mohli bychom zkusit odskočit do světa reálných čísel a přinést si odpověď 2, jenže my chceme být schopni nahrazovat čísla jejich kongruentními bratříčky. Pokud to uděláme v našem výpočtu, třeba takto $11 \div 8$, tak si z reálných čísel přineseme jinou odpověď, což je velmi nemilé.

Teď se podíváme na nápad s převrácenou hodnotou. Nejprve se musíme zamyslet, co tím vlastně myslíme, když ve světě reálných (nebo třeba racionálních) čísel napíšeme $\frac{1}{a}$. Je to jakési číslo, kvantita x , která má vlastnost, že $a \cdot x = 1$. Lze se na to podívat geometricky. Chceme-li najít $\frac{1}{3}$, tak na číselné ose najdeme tak velký úsek, že když jej dáme třikrát za sebe, tak dostaneme úsek délky 1. Má to smysl a je to něco, co se dá přenést i do jiných světů. Nejprve uděláme malý experiment.

Chtěli jsme dělit třema ve světě modula 5. Nejprve najdeme převrácenou hodnotu trojky, kdy hledáme x splňující $3x = 1$ ve světě modula 5, tedy $3x \equiv 1 \pmod{5}$. Zkusmo najdeme třeba číslo 2, můžeme si představit, že jakoby $\frac{1}{3} = 2$ ve světě modula 5. Jako dopadne násobení?

$$6 \div 3 = 6 \cdot \frac{1}{3} = 6 \cdot 2 = 12 \equiv 2 \pmod{5}.$$

Vyšlo to. Je tento přístup rezistentní na záměny v rámci kongruentní skupiny? Číslo je 2 kongruentní modulo 5 třeba s číslem 12, a $6 \cdot 12 = 72 \equiv 2 \pmod{5}$, stejný výsledek. To vypadá nadějně. Co když nahradíme čísla v příkladu a namísto $6 \div 3$ počítáme třeba $11 \div 8$? Hravě ověříme, že ona dvojka funguje i coby $\frac{1}{8}$ ($8 \cdot 2 \equiv 1 \pmod{5}$), takže máme

$$11 \div 8 = 11 \cdot \frac{1}{8} = 11 \cdot 2 = 22 \equiv 2 \pmod{5}.$$

Vypadá to velmi nadějně, zavedeme si to oficiálně.

Definice.

Uvažujme $n \in \mathbb{N}$.

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

Z našeho experimentu už víme, že 2 i 12 jsou inverzní čísla k trojce modulo 5. V definici jsme pro inverzní číslo nezavedli značení. Není to zvykem, jedním důvodem může být právě to, že toto číslo není jediné, matematici takové situace nemají moc rádi.

Jak to vypadá s existencí inverzních čísel? Pokud zkusíme najít inverzní číslo k trojce modulo 7, nebude už dvojka fungovat, zato zkusmo dojdeme třeba k číslu $x = 5$, opravdu $3 \cdot 5 = 15 \equiv 1 \pmod{7}$. Hodnota inverzního čísla tedy záleží na modulu, se kterým pracujeme. Ve světě modula 6 pak inverzní číslo k trojce nenajdeme vůbec. Hledáme totiž celé číslo x splňující rovnost $3 \cdot x \equiv 1 \pmod{6}$ neboli $3x = 1 + 6k$ pro nějaké $k \in \mathbb{Z}$, ale takové není, jak zjistíme dosazením čísel $0, 1, \dots, 5$ (ostatní nemusíme zkoušet, jsou s těmito kongruentní).

Vidíme, že inverzní čísla existovat mohou a nemusí, a příklad naznačuje, že když už nějaké existuje, tak díky kongruentnímu nahrazování jich je hodně. Následující tvrzení ukážou, jak přesně se věci mají.

Věta 3a.7.

Nechť $n \in \mathbb{N}$.

Pro $a \in \mathbb{Z}$ existuje $x \in \mathbb{Z}$ takové, že $ax \equiv 1 \pmod{n}$, právě tehdy, když $\gcd(a, n) = 1$.

Důkaz (poučný): Protože jde o ekvivalenci, bude třeba dokázat dvě implikace.

1) \implies : Předpokládejme, že existuje $x \in \mathbb{Z}$ takové, že $ax \equiv 1 \pmod{n}$. Pak také existuje $k \in \mathbb{Z}$ takové, že $1 = ax + kn$. Uvažujme nějaký společný dělitel $d \in \mathbb{N}$ čísel a a n . Pak podle důsledku 2a.3 d dělí také celý výraz $ax + kn$, tedy dělí jedničku. Proto nutně $d = 1$. Jediný společný dělitel čísel a, n je jednička, tedy $\gcd(a, n) = 1$.

2) \impliedby : Předpokládejme, že $\gcd(a, n) = 1$. Pak podle Bezoutovy identity 2b.16 existují čísla $A, B \in \mathbb{Z}$ taková, že $Aa + Bn = 1$, tedy $Aa \equiv 1 \pmod{n}$. Zvolíme $x = A$ a důkaz je hotov. □

Důkaz je důležitý, protože zároveň dává návod, jak inverzní prvky v případě existence najít.

Příklad 3a.d: Před chvílí jsme se zmínili, že ve světě celých čísel nemá smysl zkoušet dělení $7 \div 4$. Co když jsme ale ve světě modulu $n = 13$? Protože je čtyřka nesoudělná s třináctkou, má inverzní číslo modulo 13.

Podle důkazu věty hledáme Bezoutovo vyjádření $1 = 4A + 13B$, jedno je vidět hned, $1 = 4 \cdot (-3) + 13 \cdot 1$. To ukazuje, že $4 \cdot (-3) \equiv 1 \pmod{13}$ a tedy máme inverzní číslo $x = -3$ ke čtyřce modulo 13. Můžeme pak zkusit počítat

$$7 \div 4 = 7 \cdot \frac{1}{4} = 7 \cdot (-3) = -21 \equiv 5 \pmod{13}.$$

Není jasné, jaký význam má tvrdit, že jakoby $7 \div 4 = 5$, ale jistý smysl to má. My jsme se totiž na základní škole učili ověřovat výsledek dělení zkouškou a ta zde funguje: $5 \cdot 4 = 20 \equiv 7 \pmod{13}$.

△

Teď se podíváme na to, jak to vypadá s množinou inverzních čísel k danému a vzhledem k určitému modulu.

Věta 3a.8.

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

Důkaz (poučný): 1) \impliedby : Nejprve předpokládejme, že $y \equiv x \pmod{n}$. Pak podle věty 3a.3 máme $ay \equiv ax \equiv 1 \pmod{n}$, tedy y je inverzní prvek k a modulo n .

2) \implies : Nechť jsou $x, y \in \mathbb{Z}$ oba inverzní prvky k a modulo n . Pak existují $k, l \in \mathbb{Z}$ takové, že $ax = 1 + kn$ a $ay = 1 + ln$. Odečtením získáme $ax - ay = kn - ln$, tedy $a(x - y) = (k - l)n$, tedy n dělí $a(x - y)$. Protože a má inverzní prvek modulo n , musí být podle věty 3a.7 tato čísla nesoudělná, tudíž podle Eulerova lemmatu 2b.19 musí n dělit $x - y$, tedy $x \equiv y \pmod{n}$. □

Věty tohoto typu mají matematici rádi, dostali jsme totiž vyčerpávající popis množiny všech inverzních prvků k a : Je to přesně skupina pocházející z jednoho inverzního prvku x , žádné jiné nejsou.

Věta nám zároveň odpověděla na otázku, kolik je inverzních prvků k danému a vzhledem k určitému modulu. Odpověď zní, že buď nekonečně mnoho, nebo žádný.

Příklad 3a.e: Najdeme inverzní prvek k $a = 23$ modulo $n = 169$.

Protože 23 je prvočíslo, snadno nahlédneme, že nedělí $169 = 13^2$ a tudíž jsou čísla 23, 169 nesoudělná. Hledaný inverzní prvek proto existuje.

Pomocí Euklidova algoritmu najdeme nějakou Bezoutovu identitu pro $1 = \gcd(169, 23)$. Vychází $1 = 3 \cdot 169 - 22 \cdot 23$, tedy $-22 \cdot 23 \equiv 1 \pmod{169}$. Nalezli jsme inverzní prvek -22 .

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

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

△

Ve cvičení 3a.12 si pak čtenář dokáže, že ve vztahu „ x je inverzní číslo k a modulo n “ lze zaměňovat v rámci kongruentní skupiny i číslo a .

Podmínka pro existenci inverzních prvků nás přivádí k zajímavému případu: Pokud by modulo bylo nějaké prvočíslo p , tak jediná čísla, která s p nejsou nesoudělná, jsou jeho násobky, viz fakt 2b.7. Tato čísla jsou ovšem kongruentní s nulou modulo p . To znamená, že ve světě modulo prvočíslo najdeme inverzní prvky ke všem číslům, která nejsou ztotožněná s nulou, což je úplný luxus, vlastně v takovém světě můžeme dělit vším kromě nuly. K tomuto pozorování se dostaneme ještě jednou, v trochu jiném převleku, a je to jeden z důvodů, proč lidé pracující ve světě modula preferují mít jako modulus prvočíslo.

Ted' si ukážeme jednu zajímavou aplikaci.

Příklad 3a.f: 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 číslu $1, \dots, 26$ a pak používáme jako šifru funkci $T(a) = (a + 3) \pmod{26}$, tedy výsledek operace nahradíme zbytkem po dělení.

Obecně lze posouvat i o jiné číslo než o tu Césarovu trojku. Zvolíme si nějaké k mezi 1 a 25 a dostáváme „šifrování posunem“: $T(a) = (a + k) \pmod{26}$. Toto se snadno dešifruje, inverzní funkce je $T^{-1}(b) = (b - k) \pmod{26}$.

Například pokud zvolíme číslo $k = 8$, tak písmeno 20 zašifrujeme jako $T(20) = (20 + 8) \pmod{26} = 28 \pmod{26} = 2$. Zpět se dostaneme funkcí $T^{-1}(2) = (2 - 8) \pmod{26} = -6 \pmod{26} = 20$. Pokud se vám nelíbí odčítání, je možno ve výrazu $2 + (-8)$ nahradit druhé číslo vhodným kongruentním zástupcem, nabízí se osmnáctka. A opravdu, $T^{-1}(2) = (2 + 18) \pmod{26} = 20 \pmod{26} = 20$. Výhoda tohoto pohledu je, že vlastně používáme stejný obecný vzorec jako pro kódování, jen s jinou posunovou konstantou. Není třeba vymýšlet speciální dekódovací přístroj, jen jinak nastavíme ten kódovací.

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, který znak se v zašifrované zprávě vyskytuje nejčastěji, a je vysoce pravděpodobné, že odpovídá nejčastějšímu písmenu daného jazyka. Velice pěkně toto popsal E.A. Poe v povídce *Zlatý skarabeus*.

Lépe vypadá šifrování dané předpisem $T(a) = (ea + k) \pmod{26}$, kde e je zvoleno tak, aby T bylo prosté (tedy aby se dvě písmena nekódovala stejně, na to je třeba zvolit něco nesoudělného s 26). Jak se takový vzkaz dekóduje? Zvolili jsme e nesoudělné s 26, pak už víme (věta 3a.7), že k němu existuje inverzní prvek d modulo 26, tedy prvek splňující $ed \pmod{26} = 1$. Ukážeme, že $T^{-1}(b) = d(b - k)$ dekóduje zprávu:

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

Zvolme třeba $e = 7$ a $k = 3$. Pak potřebujeme vyřešit rovnici $7x + 26m = 1$, buď algoritmem nebo to zkusíme uhádnout. Vyjde například $x = -11$ a $m = 3$, nás zajímá x , tradičně se bere kladné, zvolíme tedy $d = 15$.

Ted' zakódujeme třeba písmeno B odpovídající hodnotě $a = 2$, takže vyšleme zprávu $T(2) = (7 \cdot 2 + 3) \pmod{26} = 17$ neboli písmeno Q . Příjemce na zprávu aplikuje T^{-1} :

$$T^{-1}(17) = 15(17 - 3) \pmod{26} = 15 \cdot 14 \pmod{26} = 210 \pmod{26} = 2.$$

Vyšlo to.

Ale lépe tato šifra jen vypadá, pořád na ni funguje frekvenční analýza. 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.

△

Nyní se vrátíme k dříve nakousnutému problému mocnění.

Příklad 3a.g: Pokusíme se spočítat 136^{182} modulo 13. Nejprve nahradíme v základu: $136^{182} \equiv 6^{182} \pmod{13}$. Víc nám zatím známá pravidla neumožňují, situace vypadá zralá na kalkulačku. Bohužel, problém je v tom, že číslo 6^{182} má 142 cifer, přičemž na zjištění zbytku po dělení je potřebujeme znát všechny, zatímco kalkulačky si typicky pamatují pouze prvních cca 13 cifer. Můžeme si samozřejmě napsat program, který dokáže násobit s libovolnou přesností, či si nějaký již hotový najdeme, ale takovýto výpočet by nebyl nejrychlejší.

Mnohem lépe funguje redukce mocniny pomocí odebrání malých exponentů, zde použijme běžná pravidla pro práci s exponenty.

$$6^{182} = 6^{2 \cdot 91} = (6^2)^{91} = 36^{91} \equiv (-3)^{91} \pmod{13}.$$

Teď už dvojku oddělit neumíme. Mohli bychom použít rozklad $91 = 7 \cdot 13$, což by znamenalo nutnost počítat 3^7 . To už by asi ta kalkulačka zvládla, ale co kdyby nám v rozkladu vyšla velká čísla? Vždycky lze použít další snadný trik, vyrobíme si v exponentu oblíbené sudé číslo a provedeme další redukci.

$$6^{182} \equiv (-3)^{91} = (-3)^{1+2 \cdot 45} = -3 \cdot ((-3)^2)^{45} = -3 \cdot 9^{45} \equiv -3 \cdot (-4)^{45} \pmod{13}.$$

Tady by zase pomohlo odebrání jedničky, ale urychlíme to, na třetí mocninu si troufneme.

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

Teď už to hravě dorazíme.

$$6^{182} \equiv \dots \equiv -3 \cdot 1^{15} = -3 \cdot 1 = -3 \equiv 10 \pmod{13}.$$

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

△

Máme tedy postup na počítání vysokých mocnin, který funguje obecně a snadno se algoritmizuje, to je dobrý a spolehlivý základ. Navíc je relativně rychlá, k nejrychlejší a často používané metodě se dostaneme už jen drobnou úpravou. Vyplývá z pozorování, že nejlépe by se nám (nebo spíše počítači) počítaly mocniny s exponentem ve tvaru 2^k , protože u nich stačí stále odebrat dvojku.

Příklad 3a.h: Ještě jednou $6^{182} \pmod{13}$. Nejprve si exponent vyjádříme pomocí mocnin dvojky, tedy vlastně jde o převod do binárního tvaru, na který máme algoritmus v příkladě 2a.g. Dostáváme $182 = 128 + 32 + 16 + 4 + 2$, proto $6^{182} = 6^{128} \cdot 6^{32} \cdot 6^{16} \cdot 6^4 \cdot 6^2$. Mocniny dvojky lze spočítat odebráním dvojky jako výše, ale pokud začneme od největší, dostaneme se k nižším, například $6^{32} = (6^{16})^2$, je zbytečné je počítat vícekrát. Neefektivnější je tedy začít od nejmenších, počítáme modulo 13:

$$\begin{aligned} 6^2 &= 36 \equiv 10 \pmod{13}, & 6^4 &= (6^2)^2 = 10^2 = 100 \equiv 9 \pmod{13}, & 6^8 &= (6^4)^2 = 9^2 = 81 \equiv 3 \pmod{13}, \\ 6^{16} &= (6^8)^2 = 3^2 = 9 \pmod{13}, & 6^{32} &= (6^{16})^2 = 9^2 = 81 \equiv 3 \pmod{13}, \\ 6^{64} &= (6^{32})^2 = 3^2 = 9 \pmod{13}, & 6^{128} &= (6^{64})^2 = 9^2 = 81 \equiv 9 \pmod{13}. \end{aligned}$$

To bylo snadné, zejména zacyklení ušetřilo práci, to byl takový bonus. Pak už to jen dáme dohromady:

$$6^{182} = 6^{128} \cdot 6^{32} \cdot 6^{16} \cdot 6^4 \cdot 6^2 = 9 \cdot 3 \cdot 9 \cdot 9 \cdot 10 = 27 \cdot 81 \cdot 10 \equiv 1 \cdot 3 \cdot 10 = 30 \equiv 6 \pmod{13}.$$

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

△

Pokud máme štěstí a naše modulo je prvočíslo, pak existuje další velmi zajímavá metoda.

Věta 3a.9. (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 $a, 2a, \dots, (n-1)a$ nejsou navzájem kongruentní modulo n . Když totiž $ia \equiv ja \pmod{n}$, pak n dělí $a(i-j)$, ale n je nesoudělné s a , proto (lemma 2b.19) n dělí $i-j$. Nicméně $|i-j| < n$, proto $i-j = 0$, tedy $ia = ja$. Stejný argument ukáže, že žádné z čísel ia pro $i = 1, \dots, n-1$ nemůže být kongruentní s nulou.

Když tedy vezmeme $a, 2a, \dots, (n-1)a$ a přejdeme ke zbytkům modulo n , dostaneme v nějakém pořadí všechna čísla $1, 2, \dots, n-1$. Když je všechny spolu vynásobíme, což lze psát jako $\prod_{i=1}^{n-1} (ia) \pmod{n}$, dostaneme $(n-1)!$.

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

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

Protože n jako prvočíslo nemůže dělit $1 \cdot 2 \cdot \dots \cdot (n-2)(n-1)$, viz důsledek 2b.20 a jeho zobecnění, musí platit $\gcd((n-1)!, n) = 1$. Podle lemma 2b.19 proto n dělí $a^{n-1} - 1$ neboli $1 \equiv a^{n-1} \pmod{n}$.

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

Jestliže $\gcd(a, n) > 1$, pak (viz fakt 2b.7) n dělí a . Proto $a \equiv 0 \pmod{n}$, tedy podle faktu 3a.6 $a^n \equiv 0^n = 0 = a \pmod{n}$. □

Alternativní důkaz se najde jako Poznámka 3a.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, protože do dalšího výpočtu posílá jedničku, zatímco verze (ii) nechává a . Proto všichni za „malou Fermatovu větu“ považují tvrzení (i), budeme to tak dělat i my.

Příklad 3a.i: Spočítáme zase 136^{182} modulo 13. Zase nahradíme $136^{182} \equiv 6^{182} \pmod{13}$ a protože je 13 prvočíslo nesoudělné s šestkou, můžeme použít malého Fermata. Na to si tam ale musíme vyrobit mocninu čísla $13 - 1 = 12$, což je snadné, $6^{182} = 6^{12 \cdot 15 + 2}$. Podle malé Fermatovy věty pak máme $6^{12} \equiv 1 \pmod{13}$, proto

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

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

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

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

a čekala by nás další práce.

△

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

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

Fakt 3a.10.

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 $n-1$.

Jinými slovy, stačí umět počítat mocniny až po exponent $n-1$, což mimochodem může být pořád dost velké číslo. Čímž se dostáváme zpět k redukci exponentu či rychlému mocnění z příkladu 3a.h.

Jako ukázkou použití malé Fermatovy věty se vrátíme ke kódování.

Příklad 3a.j (pokračování 3a.f): Vrátime 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 dvoučíslicím 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 předchozí pokusy, protože se maskují frekvence a má obecně méně vnitřních pravidelností, čímž se protivníkovi ztěžuje protiútok.

Její nevýhodou je, že výpočet odmocniny je velice náročná operace. Proto si teď nápad vylepšíme.

Zvolíme nějaké prvočíslo n strašlivě velké, aby byly zprávy vždy o hodně menší (dlouhé zprávy můžeme sekát). Zvolme libovolné číslo $e \in \mathbb{N}$ nesoudělné s $n-1$, pak podle věty 3a.7 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 $T(M) = M^e \bmod n$ (proto jsme volili zkratku e jako „encode“). Jak se dělá dešifrování? Tvrdíme, že to dělá zobrazení $T^{-1}(C) = C^d \bmod n$ (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. Nejprve ale budeme muset vyvinout vhodný nástroj, který se mimochodem bude hodit i jinde v této knize.

△

Zatím jsme v příkladech měli malá modula. V praxi se ale objevují i opravdu velká čísla n a pak může být problémem třeba i ověření, že opravdu $a \equiv b \pmod{n}$, protože dělení patří mezi náročnější operace. Existuje zajímavý trik, který se nám bude záhy hodit. Začneme otázkou, co se stane, když při porovnávání čísel používáme dva různé moduly. Obecně mezi kongruencí modulo m a kongruencí modulo n žádný vztah není, ale pokud je mezi čísly m a n vhodná souvislost, něco se nabídne.

Lemma 3a.11.

Nechť $m, n \in \mathbb{N}$ splňují $m \mid n$. Pokud pro čísla $a, b \in \mathbb{Z}$ platí $a \equiv b \pmod{n}$, pak nutně $a \equiv b \pmod{m}$.

Důkaz je přímočarý, viz cvičení 3a.10. Mělo by to být jasné, například když $9 \equiv 21 \pmod{12}$, tedy od 9 se dá k 21 dosáknout pomocí 12, tak už se dá určitě dosáknout 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 dosáknout pomocí menšího čísla, pak to ještě nemusí znamenat, že to půjde i pomocí většího.

Jenže nás právě tento opačný směr, od menšího modula k většímu, zajímá. Abychom něco dostali, musíme se omezit na speciální případ.

Lemma 3a.12.

Nechť $m, n \in \mathbb{N}$ jsou nesoudělná. Pokud pro čísla $a, b \in \mathbb{Z}$ platí, že $a \equiv b \pmod{mn}$, právě tehdy když $a \equiv b \pmod{m}$ a $a \equiv b \pmod{n}$.

S Rozbor: Jde o ekvivalenci, tedy potřebujeme dokázat dva směry. Jeden je už vlastně hotov, protože přecházíme od modulu mn k modulu n či m , ty oba dělí mn a předchozí tvrzení to řeší. Tím opravdu novým je tedy opačný směr, ze znalosti kongruence vůči m a n potřebujeme získat informaci o kongruenci vzhledem k mn . Jak to uděláme?

Pro kongruenci máme tři ekvivalentní vyjádření, ale asi nebudeme chtít hledat zbytky po dělení, takže reálně zbývají dvě. Měli jsme docela dobrou zkušenost s alternativním vyjádřením (ii). V tom případě bychom byli v následující situaci:

- Známο: $b = a + kn$ pro jisté $k \in \mathbb{Z}$
- Chceme: $b = a + xmn$ pro jisté $x \in \mathbb{Z}$.
- $b = a + lm$ pro jisté $l \in \mathbb{Z}$
- $\gcd(m, n) = 1$

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

- Známο: m dělí $b - a$
- Chceme: mn dělí $b - a$.
- n dělí $b - a$
- $\gcd(m, n) = 1$

Tady zase máme v předpokladu dvě dělitelnosti, my jsme ovšem měli pravidla jen ohledně čísel napravo, žádné se netýkalo míchání dělitelů.

Klíčem k důkazu je ty dva přístupy spojit, tedy pracovat zároveň s algebraickým vzorcem a pojmem dělitelnosti. To jde proti obvyklému postupu, kdy se naopak snažíme najít pro předpoklad a závěr společný jazyk, dokonce se začátečníkům vyloženě nedoporučuje míchat dva jazyky v jednom důkazu. Jenže to je jen doporučení vhodné pro jednoduché situace, jakmile se začnou dokazovat složitější věci, žádná pravidla nejsou, někdy se úspěch dostává právě spojením rozdílných přístupů.

Důkaz (poučný): Z předpokladu $a \equiv b \pmod{m}$ vyplývá existence $k \in \mathbb{Z}$ takového, že $a - b = km$. Z druhého předpokladu zase víme, že $n \mid (b - a)$, tedy $n \mid (km)$. Ovšem m a n jsou nesoudělná čísla, proto podle lemma 2b.19 musí platit $n \mid k$ neboli $k = ln$ pro nějaké $l \in \mathbb{Z}$. Pak $b - a = lnm$, tedy $(mn) \mid (b - a)$, přesně jak jsme potřebovali. □

V cvičení 3a.11 se podíváme na případ, kdy m, n nejsou nesoudělná. Lemma 3a.12 se dá snadno zobecnit i na vyšší počet činitelů modula.

Lemma 3a.13.

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 $n_i \mid (b - a)$ pro všechna i . Číslo $b - a$ je proto společným násobkem čísel n_1, \dots, n_m . Protože je $\text{lcm}(n_1, n_2, \dots, n_m)$ mezi společnými násobky nejmenší, a to i ve smyslu dělitelnosti, musí dělit to $b - a$.

Protože jsou n_i navzájem nesoudělná, podle cvičení 2b.4 je $\text{lcm}(n_1, n_2, \dots, n_m) = n$, tedy n dělí $b - a$. \square

Jako cvičení x.y nabízíme alternativní důkaz indukci, který může čtenáři přijít stravitelnější (nebo také ne).

Příklad 3a.k: Dokážeme, že $7362894567 \equiv 327 \pmod{360}$.

Zajímá nás tedy dělitelnost čísla $7362894567 - 327 = 7362894240$. Použijeme rozklad $360 = 5 \cdot 8 \cdot 9$ a kritéria dělitelnosti, viz také sekce 3a.14. Dělitelnost pěti čísla 7362894240 poznáme podle poslední číslice (vychází to), dělitelnost osmi podle posledního trojčíslí (dá se dělit osmičkou, tedy i celé číslo), dělitelnost devítkou rozhodne ciferný součet 45, který dělitelný devíti opravdu je. Podle lemma tedy dostáváme $7362894567 \equiv 327 \pmod{360}$.

Tohle byl samozřejmě lehký ilustrační příklad, 360 je běžné trojčiferné číslo, čtenář by si teď měl zkusit představit modulus s řádově stovkou cifer.

Zvídavého čtenáře teď možná napadlo, že je sice pěkné umět ověřit kongruenci, ale kde jsme vlastně toho ideálního zástupce 327 pro číslo 7362894567 vzali, když se nám nechce dělit? To je pro některé aplikace naprosto zásadní otázka a dostaneme se k ní, až si vyrobíme pokročilejší nástroje.

\triangle

Příklad 3a.l (pokračování 3a.k): 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 „sukromý 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 $(M^e)^d \equiv M \pmod{q}$. Protože jsou p, q coby různá prvočísla nesoudělná, použijeme lemma 3a.12 a dostáváme $(M^e)^d \equiv M \pmod{n}$. 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 11b). Odhaduje se, že nejvýkonnější dekódovací centra světových tajných služeb dokážou dnes požívané RSA metody zlomit po několika desetiletích práce, což už nikoho nepálí.

Mimoходом, pokud bychom prozradili zároveň n a $m = (p - 1)(q - 1)$, tak už nejen může kdokoliv zjistit d řešením $ed \equiv 1 \pmod{m}$, ale dokonce snadno zjistí naši faktorizaci: Máme $m = pq - p - q + 1 = n - p - q + 1$, čísla p, q tedy řeší rovnice $pq = n$, $p + q = n - m + 1$, což je snadná algebraická úloha. Například z druhé rovnice vyjádříme q , dáme do první a dostáváme $p^2 - (n - m + 1)p + n = 0$.

\triangle

Máme tedy kvalitní kódování, ale také nový problém: Kde vezmeme prvočísla o 200 cifrách? To je hodně dobrá otázka, na kterou určitě nezapomeneme v kapitole 15 o prvočíslech.

3a.14 Poznámka (kritéria dělitelnosti): V kapitole 2 jsme se zmínili o existenci kritérií dělitelnosti, ale pořádně se na ně podíváme až zde, protože počítání modulo občas nabídne pohodlný zápis. Mějme tedy číslo d a chceme najít nějaký pohodlný způsob, jak rozpoznat čísla dělitelná tímto d . Lidé obvykle znají kritéria pro několik

menších čísel, relativně populární byvají testy pro dělitelnost čísla 2, 3, 4, 5, 6 (použijí se testy pro 2 a 3), 8, 9, 10 a 11. Dosti nápadně v tomto seznamu chybí sedmička.

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

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

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

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

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

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

a vidíme, že poslední dvojčíslí rozhoduje o dělitelnosti čísla čtyřkou, viz také 2a.10. Podobně se dokazuje kritérium pro $d = 25$. Můžete zkusit oddělit poslední trojčíslí a zamyslet se, jakými zajímavými čísly je dělitelné číslo 1000.

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

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

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

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

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

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

2) Další populární rodinka kritérií vychází z dekadického rozvoje čísla. Jako inspiraci 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.

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

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

Toto se dá vyjádřit rozumně slovy.

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

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

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

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

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

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

Dostáváme tak další možné kritérium.

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

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

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

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

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

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

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

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

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

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

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

Poněkud jednodušší a známá kritéria připomínáme ve cvičení 3a.13.

△

Cvičení

Cvičení 3a.1 (rutinní): Spočítejte následující výrazy (zbytky po dělení), tedy ideální zástupce v kongruenci modulu dané číslo:

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

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

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

- (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 3a.4 (rutinní): Použijte malou Fermatovu větu k výpočtu následujících výrazů modulu zadané n . Očekávají se výsledky z $\{0, 1, \dots, n - 1\}$.

- (i) 3^{33} modulu $n = 11$; (ii) 4^{44} modulu $n = 13$; (iii) 5^{55} modulu $n = 23$.

Cvičení 3a.5 (rutinní): Nechť $n \in \mathbb{N}$. Dokažte, že

- (i) pro každé $a \in \mathbb{Z}$ platí $a \equiv a \pmod{n}$;
(ii) pro každé $a, b \in \mathbb{Z}$ platí: Jestliže $a \equiv b \pmod{n}$, pak $b \equiv a \pmod{n}$.

Viz fakt 3a.2.

Cvičení 3a.6 (rutinní): Nechť $n \in \mathbb{N}$. Dokažte, že pro každé $a \in \mathbb{Z}$ platí: $a \equiv 0 \pmod{n}$ právě tehdy, když $n|a$.

Cvičení 3a.7 (rutinní, poučné): Nechť $n \in \mathbb{N}$, uvažujme $a, b, u, v \in \mathbb{Z}$ takové, že $a \equiv u \pmod{n}$ a $b \equiv v \pmod{n}$. Dokažte, že pak $a + b \equiv u + v \pmod{n}$ a $a - b \equiv u - v \pmod{n}$ (viz věta 3a.3).

Cvičení 3a.8 (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 3a.5.

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

Cvičení 3a.10 (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 $a \equiv b \pmod{m}$.

Viz lemma 3a.11.

Cvičení 3a.11 (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 $a \equiv b \pmod{\text{lcm}(m, n)}$.

Cvičení 3a.12 (poučné): Nechť $n \in \mathbb{N}$. Dokažte, že pro každé $a, u, x \in \mathbb{Z}$ platí: Jestliže je x inverzní číslo k a modulo n a $a \equiv u \pmod{n}$, pak je x inverzní číslo k u modulo n .

Cvičení 3a.13 (rutinní, poučné): Nechť $a = \sum_{i=0}^m a_i 10^i$. Dokažte následující:

(i) a je dělitelné osmi právě tehdy, když je dělitelné třemi posledními trojčíslí.

(ii) a je dělitelné třemi právě tehdy, když je ciferný součet a (daný $\sum a_i$) dělitelný třemi.

(iii) a je dělitelné devíti právě tehdy, když je ciferný součet a dělitelný devíti.

(iv) a je dělitelné jedenácti právě tehdy, když je jedenácti dělitelné číslo, které získáme sečtením sudých cifer a a odečtením lichých cifer a .

Nápověda: Viz poznámka 3a.14.

Cvičení 3a.14 (dobré): Dokažte, že jestliže je $n \in \mathbb{N}$ liché, pak $n^2 \equiv 1 \pmod{8}$.

Řešení:

Připomínáme, že zde v řešeních symbol \implies neznamená logickou implikaci, ale je to zkratka pro „z toho nalevo vyplývá to napravo“.

3a.1: (i): $\lfloor \frac{81}{11} \rfloor = \lfloor 7.4... \rfloor = 7$, proto $81 \pmod{11} = 81 - 7 \cdot 11 = 4$; (ii): $-1 + 7 = 6$, proto $-1 \pmod{7} = -1 - (-1) \cdot 7 = 6$; (iii): 3 hotovo; (iv): $-14 + 13 + 13 = 12$; (v): 0 neboť $8 \nmid 48$; (vi): $\lfloor \frac{-37}{5} \rfloor = \lfloor -7.4 \rfloor = -8$, proto $-37 \pmod{5} = -37 - (-8) \cdot 5 = 3$; (vii): 0 neboť $4 \nmid (-8)$; (viii): třeba $-15 + 6 + 6 + 6 = 3$.

3a.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.

3a.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. $q = \lfloor \frac{135}{8} \rfloor = \lfloor 16.87... \rfloor = 16$, $135 - 16 \cdot 8 = 135 - 128 = 7$. Proto $135 \equiv 7 \pmod{8}$.

3a.4: (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 $\text{gcd}(3, 11) = 1$ 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 $\text{gcd}(4, 13) = 1$ 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 $\text{gcd}(5, 23) = 1$ a 23 je prvočíslo.

3a.5: (i): $a - a = 0$, proto $n|(a - a)$.

(ii): $a \equiv b \pmod{n} \implies n|(b - a) \implies n|-(b - a) \implies n|(a - b) \implies b \equiv a \pmod{n}$.

3a.6: $a \equiv 0 \pmod{n} \iff n|(a - 0) \iff n|a$.

3a.7: $u = a + kn$, $v = b + ln$ pak $u + v = (a + b) + (k + l)n$ a $u - v = (a - b) + (k - l)n$, kde $k + l, k - l \in \mathbb{Z}$.

3a.8: Indukcí. $m = 1$ dává $a_1 \equiv u_1 \pmod{n}$, což platí dle předpokladu.

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

Mějme a_1, \dots, a_{m+1} a u_1, \dots, u_{m+1} po dvou kongruentní viz předpoklad tvrzení. Předpoklad dává $\prod_{i=1}^m a_i \equiv \prod_{i=1}^m u_i \pmod{n}$, také $a_{m+1} \equiv u_{m+1} \pmod{n}$, proto dle věty 3a.3 (iii) platí $\left(\prod_{i=1}^m a_i\right) \cdot a_{m+1} \equiv \left(\prod_{i=1}^m u_i\right) \cdot u_{m+1} \pmod{n}$

neboli $\prod_{i=1}^{m+1} a_i \equiv \prod_{i=1}^{m+1} u_i \pmod{n}$.

3a.9: 3, 6, 4, 3, 6, 4, 3, 6, 4, 3...

3a.10: Předpoklad $m|n$ dává $n = km$ pro nějaké $k \in \mathbb{Z}$. Předpoklad $a \equiv b \pmod{n}$ dává $b = a + ln$ pro nějaké $l \in \mathbb{Z}$. Pak $b = a + (kl)m$ a $kl \in \mathbb{Z}$.

3a.11: Předpoklad dává $m|(x-y)$ a $n|(x-y)$, takže číslo $x-y$ je společný násobek m, n , tudíž podle faktu 2b.9 také $\text{lcm}(m, n)|(x-y)$.

3a.12: x je inverzní číslo k a modulo n , tedy $ax \equiv 1 \pmod{n}$, podle $a \equiv u \pmod{n}$ a věty 3a.3 pak také $ux \equiv 1 \pmod{n}$ a x inverzní číslo k u modulo n .

3a.13: (i): $a = 1000A + r$ a $8|1000$, proto $a \equiv r \pmod{8}$.

(ii): $10 \equiv 1 \pmod{3}$, proto $a = \sum a_i 10^i \equiv \sum a_i \cdot 1^i = \sum a_i \pmod{3}$.

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

3a.14: $n = 2k + 1 \implies n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$ a 2 dělí $k(k+1)$.

3b. Prostor \mathbb{Z}_n

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. To 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 $n-1$. Dohodneme se tedy, že všechna čísla, zejména výsledky operací, okamžitě nahradíme zbytkem modulo n . Tento mechanismus počítání, tedy nejprve výpočet s celými čísly a poté přechod ke zbytku, lze před uživatelem schovat zavedením nových operací.

Definice.

Nechť $n \in \mathbb{N}$. Symbolem \mathbb{Z}_n značíme množinu $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$.

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

$$a \oplus b = (a + b) \pmod{n},$$

$$a \odot b = (a \cdot b) \pmod{n}.$$

Z pohledu teorie teď už vůbec nejsou jiná čísla než $\{0, 1, 2, \dots, n-1\}$ třeba. Zdálo by se, že je to jen trik, protože je potřebujeme na výpočet, ale to platí jen pro ruční počítání, protože si neumíme pomoci a při výpočtu řekněme $4 \odot 5$ tu dvacítku vidíme. Jenže počítač má výsledky naučený, takže mu prostě namluvíme, že $4 \odot 5 = 7$ (v prostoru \mathbb{Z}_{13}) a on tak normálně funguje, nepotřebuje vědět, kde se to vzalo. Podobně i teorie prostě bere na vědomí, že $a \oplus b$ má určitý výsledek, a s ním pak dále pracuje (ovšem v důkazech se budeme muset dívat na to, kde se ty výsledky berou).

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

△

Příklad 3b.b: 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 $2 \odot 4 = 2$.

△

Čtenář se zatím setkával s operacemi sčítání a násobení, které používal v rozličných světech, například pro reálná čísla, pro celá čísla, komplexní čísla a podobně, dokonce i ve světě modula jsme pořád používali stejné operace,

jen jsme měli povoleno přecházet ke kongruentním zástupcům. Zde jsme ale zasáhli přímo do mechanismu jejich fungování, takže máme nový svět, ve kterém mohou být věci jinak, než jsme zvyklí. Potřebujeme tedy zjistit, jak dalece se lze v tomto novém světě cítit doma.

Zajímají nás zejména algebraické výpočty, přesněji počítání výrazů vzniklých kombinováním čísel a operací násobení a sčítání. Jako obvykle se poradí v případě nejasností určuje závorkami a jako obvykle i pro nové operace zavedeme, že násobení má prioritu před sčítáním, abychom si nějaké závorky ušetřili. Začneme jedním užitečným pozorováním.

3b.1 Poznámka: Uvažujme čísla $a, b \in \mathbb{Z}$. Abychom našli $a \oplus b$, potřebujeme najít zbytek čísla $a + b$. My ovšem víme, že se zbytek nemění přechodu ke kongruentnímu číslu. Další úvahy v tomto směru vedou k následujícímu závěru: Pokud máme vypočítat nějaký algebraický výraz ve světě \mathbb{Z}_n , pak jej můžeme počítat s běžnými operacemi ve světě celých čísel modulo n a pro výsledek nakonec najít zbytek modulo n .

Toto je užitečné zejména pro ruční výpočty, nemusíme hledat zbytky po každém kroku (počítači je to ovšem jedno). Je také dobré si uvědomit souvislosti, než začneme s důkazy.

△

Příklad 3b.c: Hledáme výsledek výrazu $(9 \odot 5 \oplus 21)^2$ v prostoru \mathbb{Z}_{23} .

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

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

V každém kroku jsme vypočetli operaci a okamžitě výsledek nahradili zbytkem.

Nyní se podíváme na alternativu: Nejprve budeme počítat v celých číslech modulo n , na konci najdeme správného zástupce.

$$(9 \cdot 5 + 21)^2 = (22 + 21)^2 \equiv ((-1) + (-2))^2 = (-3)^2 = 9 \pmod{23}.$$

Možnost využívat záporná čísla nám výpočet ulehčila.

Zkušeni 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 (o kterých zatím mnoho nevíme), rozličné značení nám pomůže, ať v tom není zmatek.

△

Příklad jako by naznačoval, že prací v \mathbb{Z}_n o něco přicházíme, například o možnost pracovat s malými zápornými čísly, ale ono to není zas tak hrozné. Pokud se omezíme na zbytky po dělení, pak se nám objevují čísla až po $n-1$. Pokud si dovolíme „záporné zbytky“, tak je největší možné číslo $\frac{n}{2}$. Rozdíl mezi $n-1$ a $\frac{n}{2}$ není nijak zásadní, zejména pokud jsme počítač, takže přechodem do \mathbb{Z}_n netrpíme. Počítači naopak velmi vyhovuje, že si vystačí s konečnou množinou čísel. I z pohledu teorie je prostor \mathbb{Z}_n užitečný, brzy uvidíme, že je tam spousta věcí vypadá velmi pěkně, je to takový pěkný kabátek pro svět modula n .

Jednou z věcí, které s výrazy děláme, jsou úpravy, kdy se spoléháme na platnost rozličných pravidel. Ukážeme, že v našem novém světě pořád fungují.

Věta 3b.2.

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

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

Většina částí se dokazuje stejně jako (i), kterou ukážeme, ostatní přenecháme čtenáři s výjimkou částí, které zahrnují více proměnných a vyžadují zvláštní péči.

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

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

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

(v): Důkaz je obdobný jako pro (ii).

(viii): Obdobně ukážeme, že levá strana se dá získat jako zbytek čísla $a(b + c)$. Na pravé straně nejprve spočítáme $a \odot b = r$ a $a \odot c = s$, kde $ab = r + kn$ a $ac = s + ln$. Celkov výsledek pak najdeme jako zbytek čísla

$$r + s = (ab - kn) + (ac - ln) = ab + ac - (k + l)n = a(b + c) - (k + l)n \equiv a(b + c) \pmod{n},$$

vyjde to tedy stejně. □

Závěr je, že při úpravách výrazů se v \mathbb{Z}_n nemusíme bát, je to jako v \mathbb{Z} .

Teď si do řeči světa \mathbb{Z}_n převedeme několik dřívějších pojmů a poznatků.

3b.3 Dělení v \mathbb{Z}_n .

Definice.

Uvažujme $n \in \mathbb{N}$.

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)** v \mathbb{Z}_n .

Aby bylo číslo b inverzním prvkem k a v \mathbb{Z}_n , musí platit $a \cdot b \pmod{n} = 1$ neboli $a \cdot b \equiv 1 \pmod{n}$, tedy b je inverzní číslo k a modulo n .

Naopak, je-li b je inverzní číslo k a modulo n , pak splňuje $a \cdot b \equiv 1 \pmod{n}$. Totéž pak musí splňovat i jeho vzorový kongruentní zástupce neboli zbytek $r = b \pmod{n}$, takže $a \odot r = a \cdot r \pmod{n} = 1$ a samozřejmě $r \in \{0, 1, \dots, n-1\}$. Proto $r = a^{-1}$ v \mathbb{Z}_n .

Našli jsme obousměrné spojení mezi inverzními čísly modulo n a inverzními prvky v \mathbb{Z}_n . Díky tomu snadno přeložíme naše poznatky o inverzních číslech do nového jazyka.

Věta 3b.4.

Nechť $n \in \mathbb{N}$.

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

Důkaz: 1) \implies : Pokud $b = a^{-1}$ existuje, tak je to inverzní číslo k a vzhledem k modulu n . Podle věty 3a.7 proto musí platit $\gcd(a, n) = 1$.

2) \impliedby : Nechť $\gcd(a, n) = 1$. Pak podle věty 3a.7 existuje $b \in \mathbb{Z}$ splňující $a \cdot b \equiv 1 \pmod{n}$. Zvolme $r = b \pmod{n}$, pak $r = a^{-1}$.

3) Jednoznačnost: Nechť $x, y \in \mathbb{Z}_n$ splňují $x = a^{-1}$ a $y = a^{-1}$. Pak jsou to inverzní čísla k a modulo n , tudíž podle věty 3a.8 platí $x \equiv y \pmod{n}$ neboli $y - x = kn$ pro nějaké $k \in \mathbb{Z}$. Ale $x, y \in \mathbb{Z}_n$ znamená, že $|x - y| < n$, tedy jediná možnost je $k = 0$ neboli $x = y$. □

V kapitole 10a uvidíme, že inverzní prvek, jak jsme jej definovali pro \mathbb{Z}_n , musí být nutně jediný, plyne to z obecnějších zákonitostí (viz fakt 8a.5). Pokročilejší matematické knihy jsou psány tak, že se nejprve udělá co nejobecnější teorie, pak se přechází na speciálnější oblasti a spoustu důkazů si může odpustit, protože se zdědí z obecně platných principů. V takto napsané knize o diskretní matematice by přišla kapitola 10 dříve než tato, takže bychom si mohli část práce ušetřit. My se ale v této knize chceme dostat k obtížnějším partiím postupně a dozrát k nim, takže občas děláme práci navíc. Určitě to není na škodu.

Máme tedy jasno o tom, jak to vypadá s inverzními prvky v \mathbb{Z}_n , buď není, nebo je jediný. Obzvláště pěkně to vychází pro prvočíselné modulo. Protože pro prvočíselné n a nenulové $a \in \mathbb{Z}$ platí, že buď $\gcd(a, n) = 1$ nebo n dělí a , nemají čísla ze \mathbb{Z}_n , která jsou menší než n , moc na výběr.

Důsledek 3b.5.

Je-li n prvočíselné, pak jsou všechna $a \in \mathbb{Z}_n - \{0\}$ invertibilní.

To už je skoro jako ve světě reálných čísel. V mnoha aplikacích skutečně úspěšně nahrazujeme svět \mathbb{R} světem \mathbb{Z}_p pro p prvočíselné.

Jak se inverzní čísla určují? Bohužel na to není vzorec (s výjimkou evidentního $1^{-1} = 1$, pak je tu ještě jedna známá věc, viz cvičení 3b.4). Je tedy nutno využít souvislosti s inverzními čísly modulo n , které již hledat umíme.

S Algoritmus 3b.6.

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 $a \cdot A \equiv 1 \pmod{n}$ a $x = A$ je inverzní číslo k a modulo n . Pak $a^{-1} = A \pmod{n}$.

(Ideálního kongruentního zástupce čísla A z rozmezí $1, 2, \dots, n-1$ získáme buď přičtením/odečtením vhodného násobku n , nebo dělením se zbytkem.)

△

Příklad 3b.d: 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	0	1
31	1	-4
5	-1	5
1●	7●	-34●
0		

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

Nalezením zástupce pro -34 z množiny \mathbb{Z}_{175} (například přičtením čísla 175) dostáváme odpověď.

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

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

△

Invertibilní a inverzní prvky jsou velice užitečné. Jako ukázkou si připomeneme řešení rovnic. Kdybychom potkali rovnici $3x = 4$ ve světě reálných čísel, tak prostě rovnicí vydělíme trojkou, my už víme, že ji ve skutečnosti násobíme číslem $3^{-1} = \frac{1}{3}$. Dostaneme $x = \frac{4}{3}$.

Pokud bychom tuto rovnici potkali ve světě třeba \mathbb{Z}_{10} , tak také najdeme 3^{-1} (trojka je s modulem 10 nesoudělná), jmenovitě $3^{-1} = 7$ v \mathbb{Z}_{10} . Můžeme pak odvozovat takto:

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

To bylo podrobné odvození, kde jsme mimo jiné viděli, že je třeba využít některé z vlastností našich nových operací vypsanych výše. V praxi bychom prostě vynásobili obě strany rovnice číslem $3^{-1} = 7$ a rovnou na levé straně „zkrátíme“ s trojkou.

Pokud je modulo n prvočíslo, pak máme inverze ke všem nenulovým číslům a řešení (jednoduchých) rovnic se dělá jako obvykle. Jinak záleží na štěstí. V tom příkladě rovnice v \mathbb{Z}_{10} jsme ho měli, ale nedá se na to spoléhat.

Uvažujme rovnici $9x = 6$ v \mathbb{Z}_{12} . V oboru reálných čísel má řešení, $x = \frac{2}{3}$. Má také řešení v \mathbb{Z}_{12} , jmenovitě $x = 2$ (ověřte). My ale toto řešení neumíme najít „běžným“ způsobem, protože $\gcd(9, 12) = 3 > 1$ a tudíž neexistuje 9^{-1} v \mathbb{Z}_{12} . Rovnice ve světě modula jsou mnohem zajímavější než v oboru reálných čísel a věnujeme jim zde speciální kapitolu 4.

Toto téma uzavřeme návštěvou několika konkrétních \mathbb{Z}_n .

Příklad 3b.e: Jako první se podíváme na \mathbb{Z}_6 .

⊙	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 věc zvanou „dělitel 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 prvočíselného modula, 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

Máme potvrzeno, 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 $4 \odot 4 = 1$.

Typický prostor \mathbb{Z}_n je nicméně někde mezi právě předvedenými extrémami, 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 $13^{-1} = 13$.

Vidíme rovněž řádky s nulou, tedy v \mathbb{Z}_{14} najdeme ony nezvyklé dělitele nuly. Jmenovitě jde o čísla 2, 4, 6, 7, 8, 10, 12. Můžete si rozmyslet, že nenulové číslo v \mathbb{Z}_n je vždy buď invertibilní nebo dělitel nuly, uděláme z toho cvičení 3b.5.

△

3b.7 Odčítání v \mathbb{Z}_n .

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. Podobně jako dělení, ani odčítání se nebere jako jedna ze základních algebraických operací, pro reálná (racionální, celá, komplexní, ...) čísla je to příjemná zkratka pro přičítání opačného prvku. Například $3 - 5$ je symbol pro $3 + (-5)$, kde -5 je číslo opačné k pětce, při pokusu přenést tuto myšlenku do světa \mathbb{Z}_n ovšem narážíme na drobný problém, že tam záporná čísla nemáme.

Abychom jej vyřešili, zamysleme se, co je to vlastně opačný prvek. Co mají společná čísla 5 a -5 ? To, že se navzájem vynulují, tedy $5 + (-5) = 0$. Šlo by to napodobit 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 3b.b, zjistíme, že $5 \oplus 1 = 0$. Zkusmo tedy prohlášíme, že opačné číslo k 5 v \mathbb{Z}_6 je 1, označíme jej (-5) .

Letný 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 \mathbb{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}_9 , tak musíme použít opačný prvek k 5 vzhledem k modulu 9, 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 3b.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 3b.3. Vidíme, že na rozdíl od inverzních čísel se ta opačná hledají snadno.

Jako příklad využití nových pojmů si teď vyřešíme rovnici. Je to příklad velmi užitečný, lidé jsou totiž zvyklí při řešení rovnic používat triky typu „zkrátíme na obou stranách rovnice“, ty jsou ale zase jen pohodlnou zkratkou. Naštěstí fungují i ve světě \mathbb{Z}_n , v důkazu ukážeme podrobnými kroky, že tyto triky závisejí na platnosti vlastností z věty 3b.2.

Příklad 3b.f: Uvažujme rovnici $5 \odot x \oplus 3 = 2$ v \mathbb{Z}_{14} . Napodobíme postup, kterým bychom řešili rovnici $5x + 3 = 2$ v oboru reálných čísel.

Nejprve bychom od obo stran odečetli trojku, což zde nahradíme přičtením (zprava) opačného čísla $(-3) = 11$.

$$(5 \odot x \oplus 3) \oplus 11 = 2 \oplus 11 \iff (5 \odot x) \oplus (3 \oplus 11) = 13 \iff (5 \odot x) \oplus 0 = 13 \iff 5 \odot x = 13.$$

Vidíme, že jsme na levé straně potřebovali přeorganizovat závorky, tedy použili jsme asociativitu sčítání.

Teď bychom rádi rovnici dělili třináctkou, což napodobíme tak, že rovnici vynásobíme (zleva) číslem $5^{-1} = 3$ (vzhledem k $n = 14$).

$$3 \odot (5 \odot x) = 3 \odot 13 \iff (3 \odot 5) \odot x = 11 \iff 1 \odot x = 11 \iff x = 11.$$

Udělejte si zkoušku (já jsem si ji udělal).

△

Ve světě \mathbb{Z}_n se tedy pracuje docela dobře, i když hůře než s reálnými čísly, ne každé číslo je invertibilní. V tomto směru je příjemné \mathbb{Z}_p pro p prvočíslo, tam už v zásadě není rozdíl oproti reálným číslům.

Cvičení

Cvičení 3b.1 (rutinní): Pro daná n a a najděte opačný prvek $(-a)$ a inverzní prvek a^{-1} v prostoru \mathbb{Z}_n .

(i) $n = 35$, $a = 12$;(iii) $n = 42$, $a = 25$;(ii) $n = 36$, $a = 15$;(iv) $n = 146$, $a = 75$.

Cvičení 3b.2 (rutinní): Spočítejte následující výrazy v daném \mathbb{Z}_n . Nejprve převedte odčítání na sčítání s opačnými prvky.

(i) $(7 + 8)^{146} - 21$ modulo $n = 13$;(ii) $(31 \cdot 4 - 1)^{192}$ modulo $n = 20$.

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

(Viz fakt 3b.8.)

Cvičení 3b.4: Dokažte, že pro každé $n \in \mathbb{N}$, $n > 1$ platí $(n - 1)^{-1} = (n - 1)$ v \mathbb{Z}_n .

Cvičení 3b.5 (poučné): Nechť $n \in \mathbb{N}$. Dokažte, že pro každé $a \in \mathbb{Z}_n - \{0\}$ platí, že buď je a invertibilní, nebo je to dělitel nuly, tedy existuje $b \in \mathbb{Z}_n - \{0\}$ takové, že $a \odot b = 0$.

Řešení:

3b.1:

(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 $12^{-1} = 3$.(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.

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

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			

3b.2: (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): $\equiv (31 \cdot 4 + 19)^{192} \equiv (11 \cdot 4 + 19)^{192} = (44 + 19)^{192} \equiv (4 + 19)^{192} = 23^{192} \equiv 3^{192} \pmod{20}$. Nelze použít malého fermata (20 není prvočíslo).

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

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

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

3b.4: $(n - 1)^2 = n^2 - 2n + 1 = 1 + n(n - 2)$ a $k = n - 2 \in \mathbb{Z}$, tedy $(n - 1)^2 \equiv 1 \pmod{n}$.

3b.5: Pokud je a invertibilní, máme hotovo. Jinak $\gcd(a, n) = d > 1$, tedy $a = dk$ pro nějaké $k \in \mathbb{N}$ a $n = dl$ pro $l \in \mathbb{N}$. Tvrdíme, že $b = l$ funguje. Z rovnosti $n = dl$ a $d > 1$ máme $b < n$, také $b \neq 0$, tedy $b \in \mathbb{Z}_n$. Dále $ab = dkl = k(dl) = kn$ a $k \in \mathbb{Z}$, proto $ab \equiv 0 \pmod{n}$, tedy $ab \bmod n \odot b = 0$.

3c. Matice a polynomy modulo

V částech 2c a 2d jsme si připomněli základní myšlenky o maticích a polynomech a podívali jsme se na ně ve světě celých čísel. Co se stane, když se přeneseme do světa \mathbb{Z}_n ?

Protože sčítání a násobení čísel v \mathbb{Z}_n splňuje stejná základní pravidla jako obvyklé sčítání a násobení, můžeme definovat sčítání a násobení matic obvyklým způsobem a chová se stejně jako v případě reálných čísel, například sčítání je komutativní, ale násobení obecně není. Rovněž výpočet determinantu podle definice funguje. Platí i věta o existenci inverzní matice, v tomto případě můžeme použít známou charakterizaci invertibilních čísel v \mathbb{Z}_n a napsat následující verzi.

Věta 3c.1.

Ke čtvercové matici A nad \mathbb{Z}_n existuje matice inverzní právě tehdy, když $\gcd(\det(A), n) = 1$. Tato inverzní matice je pak dána vzorcem $A^{-1} = \det(A)^{-1} D^T$, kde D je matice kofaktorů.

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

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

Rovnou najdeme $\det(A)^{-1} = 14^{-1}$ 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} .

Snadno najdeme i D a dostáváme

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

△

Čímž se dostáváme ke klíčové otázce: Jak ve světě \mathbb{Z}_n funguje Gaussova eliminace?

Podobně jako v kapitole 2c, i zde je třeba zamyslet se nad řádkovými úpravami, které jsou invertibilní. Dostáváme následující seznam:

- Přičtení c -násobku jednoho řádku k jinému, kde $c \in \mathbb{Z}_n$;
- vynásobení řádku číslem c , které je invertibilní v \mathbb{Z}_n ;
- prohození dvou řádků.

Je dobré si uvědomit, že tento seznam zahrnuje vše, co jsme dělali v rámci celočíselných řádkových operací. Chybí nám teď násobení řádku číslem -1 , ale to lze nahradit násobením číslem opačným k jedničce v \mathbb{Z}_n , což je číslo $n - 1$. Shodou okolností je toto číslo vždy invertibilní (viz cvičení 3b.4), takže je splněna podmínka druhé operace.

To znamená, že i ve světě \mathbb{Z}_n lze libovolnou matici převést pomocí Gaussovy eliminace na řádkově redukovaný tvar. To je příjemné pro počítání determinantu, dostaneme se tak i k inverzní matici? V oboru celých čísel to bylo jednoduché, tam nám u invertibilních matic vycházely jako pivoty rovnou jedničky. V oboru \mathbb{Z}_n už mohou vznikat i jiná čísla, což je nepříjemná komplikace. Abychom si udělali jasno, podíváme se na výpočet inverzní matice eliminací ve dvou krocích.

Nejprve použijeme pouze první a třetí úpravy, už víme, že tak lze matici převést na řádkově redukovaný tvar. Protože tyto úpravy mohou měnit nejvýše znaménko determinantu (konkrétně prohození řádků jej vynásobí číslem $-1 = n - 1$), vyplývá z toho, že determinant je (až na „znaménko“) roven součinu diagonálních prvků. Pokud je matice invertibilní nad \mathbb{Z}_n (a takovou teď máme), musí být i součin diagonálních prvků invertibilní, tedy nesoudělný s n . To vylučuje nulu na diagonále, budeme tedy mít na diagonále přímo pivoty eliminace. Není těžké ukázat, že i tyto pivoty musí být nesoudělné s n (jinak by to neplatilo o jejich součinu).

Po první etapě jsme tedy skočili s řádkově redukovanou maticí, která má na diagonále invertibilní prvky. Můžeme tedy použít druhou úpravu (násobení řádků inverzními prvky k pivotům), čímž získáme jedničky a lze dalšími řádkovými úpravami získat jednotkovou matici.

Závěr tedy je, že i ve světě \mathbb{Z}_n lze inverzní matice získat Gaussovou eliminací, musíme ovšem používat jen povolené úpravy.

Příklad 3c.b: Opět najdeme A^{-1} pro $A = \begin{pmatrix} 2 & 3 \\ 4 & 13 \end{pmatrix}$ v prostoru \mathbb{Z}_{45} . Začneme s maticí

$$\left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 4 & 13 & 0 & 1 \end{array} \right).$$

Normálně bychom odečetli dvojnásobek prvního řádku od druhého a dostali jedničku, ve světě \mathbb{Z}_{45} místo toho přičteme první řádek vynásobený číslem $c = -2 = 43$, což dává řádek $42 \ 39 \mid 43 \ 0$:

$$\left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 4 & 13 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 0 & 7 & 43 & 1 \end{array} \right).$$

Máme matici v řádkově redukovaném tvaru, podle očekávání jsou na diagonále invertibilní prvky. První řádek vynásobíme číslem $2^{-1} = 26$, druhý číslem $7^{-1} = 13$.

$$\left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 4 & 13 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 0 & 7 & 43 & 1 \end{array} \right) \sim \left(\begin{array}{cc|cc} 1 & 33 & 26 & 0 \\ 0 & 1 & 19 & 13 \end{array} \right).$$

Teď k prvnímu řádku přičteme druhý vynásobený číslem $-33 = 12$.

$$\left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 4 & 13 & 0 & 1 \end{array} \right) \sim \left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 0 & 7 & 43 & 1 \end{array} \right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 29 & 21 \\ 0 & 1 & 19 & 13 \end{array} \right).$$

$$\text{Proto } A^{-1} = \begin{pmatrix} 17 & 3 \\ 19 & 13 \end{pmatrix}.$$

△

Přesto není ve světě \mathbb{Z}_n vše báječné. Hlavním problémem jsou dělitelé nuly, tedy čísla, která nejsou nula, ale dokážou vynásobit jiná nenulová čísla tak, aby vznikla nula. Například v \mathbb{Z}_{45} je dělitelem nuly třeba číslo 30, protože máme $30 \cdot 6 = 0$ v \mathbb{Z}_{45} . U Gaussovy eliminace jsme je vyřadili ze hry podmínkou, že řádky lze násobit pouze invertibilními čísly. V mnoha situacích si ale zakazování nemůžeme dovolit a pak může být problém. Typickým příkladem je lineární nezávislost vektorů. Definice říká, že vektory $\vec{u}_1, \dots, \vec{u}_n$ jsou lineárně závislé, pokud dokážeme vybrat čísla a_1, \dots, a_n taková, že $a_1 \vec{u}_1 + \dots + a_n \vec{u}_n = \vec{0}$. V okamžiku, kdy máme dělitele nuly, tak je mnohem větší šance získat nulu. Proto se může stát, že vektory, které by ve světě reálných či celých čísel byly nezávislé, se náhle stanou závislými.

Velmi nepříznivě se to projeví například u pojmu hodnosti matice. Jednou z důležitých vlastností hodnosti u matic nad reálnými čísly je, že se u čtvercových matic řádková a sloupcová hodnost rovnají, jinak řečeno $\text{hod}(A^T) = \text{hod}(A)$. U matic nad \mathbb{Z}_n už to ale obecně neplatí.

Příklad 3c.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 řešení $\beta = 0$. Řešená vektorová rovnice má 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 hodnota 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 $\text{hod}(A^T) = 1$. \triangle

Nejjednodušším způsobem, jak se vyhnout dělitelům nuly, je zvolit si za modulus n nějaké prvočíslo (pokud máme tu svobodu volby). Pak jsou všechna nenulová čísla inverzibilní a \mathbb{Z}_n se chová stejně jako reálná čísla (odborně řečeno je pro n prvočíselné prostor \mathbb{Z}_n těleso, viz kapitola 10c).

Práce s maticemi nad \mathbb{Z}_n má zajímavé praktické aplikace, například samoopravné kódy.

3c.2 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 části 2d.

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

Příklad 3c.d: 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.

\triangle

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

Příklad 3c.e: 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 $\text{st}(pq) = \text{st}(p) + \text{st}(q)$ 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!

\triangle

Podíváme-li se do věty 2d.1 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 ukážeme i (ii).

Příklad 3c.f: 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 našťestí 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 . \triangle

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 3c.g: Jak vypadá největší společný dělitel polynomů $p = x^2 + x$ a $q = x^2 + 5$ nad \mathbb{Z}_6 ? Podívejme se na rozklady:

$$\begin{aligned}x^2 + x &= x(x + 1) = (x + 3)(x + 4), \\x^2 + 5x &= x(x + 5) = (x + 3)(x + 2).\end{aligned}$$

Podle prvních rozkladů je společným dělitelem polynom x , podle druhých rozkladů je to zase $x + 3$. Který z nich je největší? U polynomů hraje při dělitelnosti roli velikosti jejich stupeň, ale oba kandidáti jsou polynomy prvního stupně, to jsme si moc nepomohli. \triangle

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 3c.3.

Nechť n je prvočíslo, uvažujme polynomy p, q nad \mathbb{Z}_n . Pak platí následující:

- (i) $\text{st}(pq) = \text{st}(p) + \text{st}(q)$.
- (ii) Existují jediné polynomy d a r takové, že $p = d \cdot q + r$ a $\text{st}(r) < \text{st}(q)$.
- (iii) Polynom p má nejvýše $\text{st}(p)$ kořenů.
- (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 3c.h: Najdeme $\text{gcd}(x^3 + 3, x^2 + 1)$ 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 $\text{gcd}(x^3 + 3, x^2 + 1)$, prvním krokem bude vydělení $(x^3 + 3) : (x^2 + 1)$. Algoritmus:

- Vydělíme nejvyšší mocniny, výsledek je x .
- Najdeme zbytek jako $(x^3 + 3) - x \cdot (x^2 + 1) = 3 - x \equiv 3 + 4x \pmod{5}$.
- Pokud má zbytek nižší stupeň než dělitel, algoritmus končí, viz zde $\text{st}(4x + 3) < \text{st}(x^2 + 1)$. 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 $4x + 3$
$4x + 3$	$4x + 2$	1	$-x = 4x$	$(x^2 + 1) : (4x + 3) = 4x + 2$, zb. 0
0				

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

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

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

Zajímavá věc:

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

Takže také $\text{gcd}(x^3 + 3, x^2 + 1) = x + 2$. 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 nejpálčivější 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 nepřenesli návyky z reálných polynomů, například automaticky považujeme polynomy typu $x^2 + 1$ za nerozložitelné a bez kořenů, ale nad \mathbb{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.