

### 3. Rovnice a celá čísla

Jedním z častých úkolů matematiky je řešení rovnic a jejich soustav. To obvykle děláme ve světě reálných čísel, popřípadě komplexních, a s určitými typy rovnic si umíme docela dobře poradit. Někdy nás ale aplikace donutí pracovat v některém ze světů pocházejících z celých čísel (máme teď také celá čísla s kongruencí a prostory  $\mathbb{Z}_n$ ). V takovém případě je třeba se připravit na to, že věci fungují jinak, mimo jiné začnou selhávat obvyklé metody.

Stačí se podívat na nejjednodušší rovnici ze všech, tedy lineární rovnici jedné proměnné. Například rovnici  $6x = 3$  ve světě reálných čísel hravě vyřešíme a najdeme  $x = \frac{1}{2}$ . Ve světě celých čísel už ale řešení neexistuje, ani ve světě  $\mathbb{Z}_8$ . Naopak v  $\mathbb{Z}_{27}$  řešení máme, jmenovitě  $x = 5$  (udělejte zkoušku dosazením). Aby to bylo zajímavější, máme tam i řešení  $x = 14$ . Je ještě nějaké jiné? Dokážeme řešení najít jinak než metodou pokus-omyl?

### 3a. Diofantické rovnice

Rovnice, ve kterých se vyskytují pouze celá čísla a také očekáváme celočíselná řešení, se nazývají **diofantické rovnice** (Diophantine equations). Diofanus z Alexandrie je zkoumal ve 3. století, ale najdeme je také třeba ve starých textech indických (už od 800 př.n.l s důležitými aplikacemi v astronomii). Čtenář se nejspíše s diofantickými rovnicemi setkal, konkrétně v geometrii, když se dozvěděl Pythagorovu větu  $x^2 + y^2 = z^2$  a ocenil příklady, ve kterých měly pravouhlé trojúhelníky celočíselné délky stran, třeba 3, 4 a 5. Zrovna tímto problémem se zabývali již antičtí Řekové, ale ještě se tomu neříkalo diofantické rovnice. Zajímavých rovnic řešených v oboru celých čísel bylo více (viz ukázky aplikací v příkladech níže a příklad 3a.i), ale nebyly vnímány jako jeden okruh problémů, řešily se individuálně a pokrok byl pomalý, protože jsou těžké.

Teprve ve 20. století se lidé podívali na celou problematiku souhrnně a mimo jiné se nakonec ukázalo, že nějaký univerzální přístup neexistuje. Diofantické rovnice tedy řešíme podle typů a je to obtížný obor. Proto se zde zaměříme na nejjednodušší případ, což jsou lineární rovnice.

!

#### Definice.

Pojmem **lineární diofantická rovnice** o dvou neznámých označujeme libovolnou rovnici typu  $ax + by = c$  s neznámými  $x, y$ , kde  $a, b, c \in \mathbb{Z}$  a vyžadujeme také řešení  $x_0, y_0 \in \mathbb{Z}$ .

By a **linear diophantine equation** of two variables we mean any equation of the form  $ax + by = c$  with unknowns  $x, y$ , where  $a, b, c \in \mathbb{Z}$  and only integer solutions are allowed.

Diofantickým rovnicím s  $a = b = 0$  budeme říkat „triviální“ a v praxi je nepotkáváme. Jsou jednoduché, pro  $c \neq 0$  řešení nemají, naopak pro  $c = 0$  jsou řešením všechny  $x, y \in \mathbb{Z}$ . Tím vybočují ze standardních postupů a proto se obvykle budeme zabývat jen rovnicemi netriviálními.

**Příklad 3a.a:** Víme, že netriviální rovnice  $ax + by = c$  (tak, jak ji tradičně chápeme) popisuje přímku v rovině. Přesněji řečeno, pokud budeme její řešení  $x, y$  interpretovat jako souřadnice  $(x, y)$  bodů v rovině, pak množina řešení tvoří přímku.

Napravo vidíme množinu všech řešení rovnice  $3x + 5y = 2$ . Tato řešení se často vyjadřují pomocí parametru, například takto:

$$\begin{aligned} x &= t, \\ y &= \frac{2 - 3t}{5}, \quad t \in \mathbb{R}. \end{aligned}$$

Pokud bychom ji považovali za diofantickou rovnici, tak by nás zajímalo, zda na dotyčné přímce leží nějaké body s celočíselnými souřadnicemi. Lze se také ptát, zda pro nějaké celočíselné hodnoty parametru  $t$  vyjde rovněž  $y$  celé.

Zkusmo můžeme najít třeba řešení  $x = -1, y = 1$  nebo  $x = 4, y = -2$ . Tento přístup ale není příliš perspektivní, tyto rovnice budeme řešit jinak.

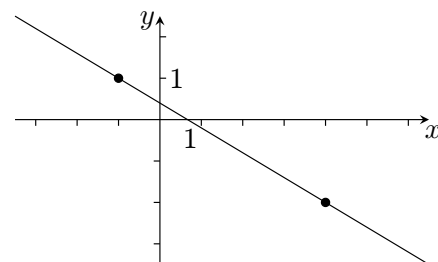
△

Jednu rovnici tohoto typu jsme už potkali a vyřešili, jmenovitě při hledání inverzního čísla  $k$   $a$  modulo  $n$  jsme měli rovnici  $ax + kn = 1$ . Ukáže se, že metoda, kterou jsme tam použili, se snadno upraví také na případ, kdy místo 1 máme  $c$ .

!

#### Věta 3a.1. (o existenci řešení)

Nechť  $a, b, c \in \mathbb{Z}$ . Lineární diofantická rovnice  $ax + by = c$  má alespoň jedno řešení právě tehdy, když  $c$  je násobkem  $\gcd(a, b)$ .



**S Rozbor:** Budeme dokazovat dvě implikace. Ta zleva doprava nás staví do následující situace:

- Máme:  $x_0, y_0 \in \mathbb{Z}$  • Chceme:  $\gcd(a, b)$  dělí  $c$   
 $ax_0 + by_0 = c$

Čtenář by již mohl vidět cestu, argument je stejný jako v důkazu věty 2a.12.

Obdobný je také důkaz opačného směru, který je hlubší a využije možnost vyjádřit  $\gcd(a, b)$  pomocí Bezoutovy identity, tentokrát s jednou úpravou navíc.

**Důkaz (poučný):**  $1) \implies$ : Předpokládejme, že existují  $x_0, y_0 \in \mathbb{Z}$  takové, že  $ax_0 + by_0 = c$ . Protože  $\gcd(a, b)$  dělí  $a$  i  $b$ , musí podle důsledku 1a.20 dělit i jejich lineární kombinaci, tedy také  $c$ .

$2) \impliedby$ : Předpokládejme, že  $c = \gcd(a, b) \cdot k$  pro nějaké  $k \in \mathbb{Z}$ . Podle Bezoutovy identity 1b.15 existují  $A, B \in \mathbb{Z}$  takové, že  $Aa + Bb = \gcd(a, b)$ . Pak  $Aak + Bbk = \gcd(a, b)k$  neboli  $a(kA) + b(kB) = c$ , tedy celá čísla  $x_0 = kA$ ,  $y_0 = kB$  řeší  $ax + by = c$ . □

Mimochodem, tato věta platí i pro triviální rovnici.  $\gcd(0, 0) = 0$  a jediným násobkem nuly je  $c = 0$ .

Důkaz nám poskytl návod, jak rovnice řešit.

**Příklad 3a.b:** Lze vyplatit 1250 korun pomocí mincí o hodnotách 6 a 15?

Ptáme se, zda lze vzít  $x$  šestikorun a  $y$  patnáctikorun a poskládat 1250. Matematicky jde o rovnici  $6x + 15y = 1250$ , přičemž  $x, y$  chceme celočíselné. Víme, že  $\gcd(6, 15) = 3$ , a číslo 1250 není dělitelné třemi, proto podle věty 3a.1 vyplacení nejde.

△

**! Příklad 3a.c:** Lze odměřit 1251 litrů pomocí nádob s objemem 6 a 15 litrů?

Doplňující otázka: Ve kterém filmu se řešila podobná úloha?

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

	(15)	(6)
15	1	0
6	0	1
3●	1●	-2●
0		

Máme  $3 = 1 \cdot 15 + (-2) \cdot 6$  neboli  $15 \cdot 1 + 6 \cdot (-2) = 3$ . Těmi koeficienty 15 a 6 se to velmi podobá rovnici, kterou řešíme, ale neshoduje se pravá strana. To snadno napravíme násobením, jmenovitě rovnici pronásobíme číslem 417. Na levé straně si musíme dát pozor, kam toto číslo přinášíme, rozhodně chceme zachovat koeficienty 15 a 6. Dostáváme proto  $15 \cdot 417 + 6 \cdot (-834) = 1251$ . Porovnáním se zadanou rovnicí vidíme, že  $x = 417$  a  $y = -834$  je řešení.

Interpretace v jazyce zadání: Nejprve do nádrže přidáme 417 krát obsah patnáctilitrové nádoby, pak odebereme 834 krát obsah šestilitrové a zůstane nám 1251 litrů. Z praktického pohledu asi bude lepší nalévání a vybírání střídat, abychom nepotřebovali nádrž o objemu  $417 \cdot 15 = 6225$ .

Poznámka: Obvykle se  $\gcd(a, b)$  nevidí rovnou, ale také se musí spočítat, než zjistíme, zda řešení existuje. Ale nedělají se dva běhy Euklidova algoritmu, rovnou se nasadí rozšířená verze. V případě, že řešení neexistuje, jsme ty pomocné sloupce počítali zbytečně, ale u školních příkladů se to děje zřídka.

Někdy rovnou vidíme nějakého společného dělitele čísel  $a, b, c$ , což láká ke krácení v rovnici. Například v tomto příkladě bychom rádi danou rovnici zkrátili třemi a řešili  $5x + 2y = 417$ . Je to možné, krácení rovnic funguje i u těch diofantických.

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

△

Z pohledu praktického nás nalezené řešení příliš neuspokojuje, protože nás nutí vylévat vodu, kterou jsme předtím nanosili. To nás přivádí k otázce, zda není ještě nějaké jiné řešení oné rovnice. Naději máme, protože postup vychází z Bezoutovy identity a již jsme viděli, že Bezoutových vyjádření může být více.

Když v matematice řešíme rovnice, tak se snažíme o nalezení všech řešení a preferujeme nějaké praktické vyjádření celé množiny řešení. Jakýmsi grálem teorie rovnic je takzvané **obecné řešení**, což je vzorec s jedním či více parametry, jejichž změnou obsáhneme celou množinu řešení. Viz onen vzorec s parametrem  $t$  v úvodním příkladě. Rádi bychom něco podobného udělali pro diofantické rovnice.

Začneme homogenními rovnicemi, u kterých je vždy situace výrazně snazší. Homogenní verzi snadno vyrobíme také z nehomogenní rovnice.

**Definice.**

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

**Příklad 3a.d:** Vypustili jsme děti na kolech na okruh v parku. Jednomu trvá objetí okruhu 7 minut, druhému 5 minut. Za jak dlouho se opět u nás setkají?

Aby se u nás setkali, musí každé dítě ujet plný počet kol, označme jejich počet  $x$  a  $y$  pro jednotlivé děti. Doba, která do tohoto setkání uplyne, je  $7x$ , popřípadě  $5y$ , a musí být stejná, tedy  $7x = 5y$ . Po přepisu  $7x - 5y = 0$  dostáváme homogenní lineární diofantickou rovnici.

Původní tvar  $7x = 5y$  je nicméně praktičtější. Protože  $x \in \mathbb{Z}$ , je na levé straně číslo dělitelné sedmičkou. Proto musí být dělitelné sedmi i číslo  $5y$  napravo, ale 5 nám v tom nepomůže, proto musí být  $y$  násobek sedmi (Euklidovo lemma 1b.23). Označme  $y = 7k$ ,  $k \in \mathbb{Z}$ . Po dosazení do rovnice vyjde  $x = 5k$  a máme řešení homogenní rovnice:  $x_h = 5k$ ,  $y_h = 7k$  pro  $k \in \mathbb{Z}$ .

Nejmenší řešení je tedy  $x = 5$ ,  $y = 7$  a děti se u nás sejdou za 35 minut. Možná by bylo lepší tomu pomalejšímu říct, ať to víc fláká a udělá kolo za 10 minut.

V postupu jsme významně použili fakt, že koeficienty rovnice jsou nesoudělné. Co kdyby nebyly? Pak stačí rovnici zkrátit číslem  $\gcd(a, b)$  a problém je vyřešen.

△

Tento postup teď uděláme obecně, přičemž se vyhneme triviálnímu případu. Homogenní triviální rovnice je  $0 = 0$  a výrazně vybočuje, protože ji řeší všechna  $x, y \in \mathbb{Z}$ .

**Věta 3a.2.** (o struktuře množiny řešení homogenní rovnice)

Uvažujme netriviální rovnici  $ax + by = 0$  pro  $a, b \in \mathbb{Z}$ . Její obecné řešení je dáno vzorcem

$$x = \frac{b}{\gcd(a, b)}k, \quad y = -\frac{a}{\gcd(a, b)}k, \quad k \in \mathbb{Z}.$$

Tato věta mimo jiné ukazuje, že homogenní lineární diofantická rovnice má nekonečně mnoho řešení. Zároveň pro všechna z nich poskytuje vzorec, je to tedy obecné řešení.

**S Rozbor:** Potřebujeme ukázat dvě věci: Že vzorec z věty produkuje řešení dané rovnice, a že umí poskytnout všechna z nich. Použijeme k tomu přístup z příkladu 3a.d.

**Důkaz** (poučný): Protože je rovnice netriviální, alespoň jedno z čísel  $a, b$  je nenulové. Pak je také  $\gcd(a, b)$  nenulové.

1) Nechť je  $x_0, y_0 \in \mathbb{Z}$  nějaké řešení rovnice  $ax + by = 0$ . Dosazením tohoto řešení do rovnice získáme platnou rovnost  $ax_0 + by_0 = 0$ . Upravíme ji na tvar  $\frac{a}{\gcd(a, b)}x_0 = -\frac{b}{\gcd(a, b)}y_0$ , kde podle faktu 1b.21 jsou koeficienty celá a navzájem nesoudělná čísla. Číslo  $\frac{a}{\gcd(a, b)}$  musí dělit  $-\frac{b}{\gcd(a, b)}y_0$ , ovšem kvůli nesoudělnosti s číslem  $\frac{b}{\gcd(a, b)}$  musí podle lemma 1b.23 dělit  $-y_0$ . Existuje tedy  $k \in \mathbb{Z}$  takové, že  $y_0 = -\frac{a}{\gcd(a, b)}k$ . Z rovnice  $ax = -by$  pak snadno dostaneme vzorec  $x_0 = \frac{b}{\gcd(a, b)}k$ .

Ukázali jsme, že každé řešení lze vygenerovat pomocí vzorce z věty.

2) Nyní ověříme, že naopak každá dvojice  $x_h = \frac{b}{\gcd(a, b)}k$ ,  $y_h = -\frac{a}{\gcd(a, b)}k$  je opravdu řešení rovnice ze  $\mathbb{Z}$ .

Celočíselnost plyne z toho, že  $\frac{b}{\gcd(a, b)}$  a  $\frac{a}{\gcd(a, b)}$  jsou celá čísla (viz fakt 1b.21). Po dosazení  $x_h, y_h$  do rovnice pak okamžitě dostáváme  $ax_h + by_h = a\frac{b}{\gcd(a, b)}k - b\frac{a}{\gcd(a, b)}k = 0$ , takže  $x_h, y_h$  je řešení. □

**Poznámka:** Opatrného čtenáře napadne, zda nemůže v důkazu nastat problém v případě, že některý z koeficientů je nulový. My ale víme, že alespoň jeden z nich nula není, proto také  $\gcd(a, b) \neq 0$  a postup v důkazu je platný. Smysl má i závěr. Například pokud  $a = 0$ , pak  $b \neq 0$  a řešíme rovnici  $by = 0$ . Jejím řešením je  $x \in \mathbb{Z}$  a  $y = 0$ , což vyhovuje vzorcům:

$$y = \frac{0}{\gcd(0, b)}k = 0, \quad x = \frac{b}{\gcd(0, b)}k = \frac{b}{|b|}k = \text{sign}(b)k, \quad k \in \mathbb{Z}.$$

△

! **Poznámka:** Čtenáře možná napadlo, že jsme při převodu rovnice mohli dát mínus na druhou stranu a dojít ke vzorcům

$$x = -\frac{b}{\gcd(a, b)}k, \quad y = \frac{a}{\gcd(a, b)}k, \quad k \in \mathbb{Z}.$$

Obojí je správné, jsou to dva různé způsoby, jak vygenerovat stejnou množinu řešení.

Například v příkladě 3a.d jsme dostali řešení  $x = 5k, y = 7k$ . Různými volbami  $k$  dostaneme dvojice  $(0, 0), (5, 7), (10, 14), (15, 21)$  atd. a také  $(-5, -7), (-10, -14)$  atd. Ke každé dvojici se dostaneme určitou volbou hodnoty pro parametr  $k$ , a když takto projdeme všechny hodnoty, dostaneme nekonečnou množinu dvojic coby konečný cíl našeho snažení. V této množině žádné  $k$  nenajdeme, je to jen technický nástroj k jejímu získání a je lokální, vně tohoto zápisu neexistuje.

Alternativní popis  $x = -5k, y = -7k$  má své vlastní lokální  $k$ , které je odlišné od toho z předchozího popisu. Možná by bylo lepší říkat jednomu  $k$  a druhému  $l$  a někdy to tak budeme dělat, ale mnohdy lidé preferují jedno jméno pro parametr, tak je dobré si na to zvyknout.

Podstatné je, že tento jiný vzorec vygeneruje stejnou množinu dvojic řešících rovnici:  $(0, 0), (5, 7), (10, 14), (-5, -7)$  atd. Jediný rozdíl je v tom, že abychom dostali řekněme řešení  $(20, 28)$ , tak u prvního popisu použijeme  $k = 4$  a u druhého  $k = -4$ . Je to možné, protože každý popis řešení má své vlastní  $k$ .

Vidíme, že množina řešení rovnice je jen jedna, ale může být více vzorců, které ji generují, tedy více obecných řešení. V případě homogenní lineární rovnice jsou dvě možnosti.

Bude užitečné se na toto podívat blíže.

Uvažujme nějakou dvojici čísel  $A_h, B_h \in \mathbb{Z}$ , která řeší rovnici  $ax + by = 0$ . Pak už ji musí řešit i každá dvojice  $x_h = A_h k, y_h = B_h k$  pro  $k \in \mathbb{Z}$ . Důkaz:

$$ax_h + by_h = aA_h k + bB_h k = (aA_h + bB_h)k = 0 \cdot k = 0.$$

Můžeme říct, že dvojice  $A_h, B_h$  generuje řešení. Pak ovšem řešení generuje i dvojice  $-A_h, -B_h$ . Je tedy na nás, jakou variantu znamének použijeme.

△

**Poznámka:** Krácení v rovnici bylo klíčové. Uvažujme rovnici  $2x + 6y = 0$ . Z tvaru  $2x = -6y$  bychom mohli tipnout, že řešení jsou dána vzorcem  $x_h = -6k, y_h = 2k, k \in \mathbb{Z}$ . Popřípadě by někdo mohl preferovat možnost  $x_h = 6k, y_h = -2k, k \in \mathbb{Z}$ . Obojí vzorce opravdu generují řešení, ale nejsou to **všechna** řešení, například tak nedostaneme řešení  $x = 3, y = -2$ .

Nám tedy nestačí, že dvojice  $-6, 2$ , popřípadě  $6, -2$  generuje řešení, my potřebujeme najít (či rozpoznat) dvojici, která generuje všechna řešení. Což nás vrací k nesoudělnosti.

△

### Lemma 3a.3.

Nechť  $a, b \in \mathbb{Z}$ . Čísla  $A_h, B_h \in \mathbb{Z}$  generují všechna řešení netriviální rovnice  $ax + by = 0$  právě tehdy, když ji samy řeší a jsou nesoudělná.

V důkazu budeme pracovat s čísly  $\tilde{a} = \frac{a}{\gcd(a, b)}, \tilde{b} = \frac{b}{\gcd(a, b)}$ . Připomeňme, že podle věty 3a.2 dvojice  $\tilde{b}, -\tilde{a}$  generuje všechna řešení rovnice  $ax + by = 0$ .

**Důkaz (poučný):**  $1) \implies$ : Předpokládejme, že čísla  $A_h, B_h$  generují všechna řešení. Pak jsou  $x_h = A_h l, y_h = B_h l$  řešením pro libovolné  $l \in \mathbb{Z}$ , tedy i pro  $l = 1$ . Dvojice  $A_h, B_h$  je tedy sama řešením.

Podle věty 3a.2 pak musí existovat nějaké  $k \in \mathbb{Z}$  takové, že  $A_h = \tilde{b}k$  a  $B_h = -\tilde{a}k$ . Máme tedy  $\tilde{b} | A_h$ . Ovšem dle předpokladu dvojice  $A_h, B_h$  generuje všechna řešení, musí tedy generovat i  $(\tilde{b}, -\tilde{a})$ , takže  $A_h | \tilde{b}$ . Podle věty 1a.25 pak nutně  $|A_h| = |\tilde{b}|$ , tedy  $|k| = 1$ . Můžeme proto s pomocí věty 1b.19 počítat

$$\gcd(A_h, B_h) = \gcd(k\tilde{b}, -k\tilde{a}) = |k| \gcd(\tilde{b}, -\tilde{a}) = 1 \cdot \gcd\left(\frac{b}{\gcd(a, b)}, \frac{a}{\gcd(a, b)}\right) = 1,$$

viz fakt 1b.21.

$2) \implies$ : Jestliže  $(A_h, B_h)$  řeší homogenní lineární rovnici, pak podle věty 3a.2 musí existovat nějaké  $k \in \mathbb{Z}$  takové, že  $A_h = \tilde{b}k$  a  $y = -\tilde{a}k$ . Dostáváme pak

$$\gcd(A_h, B_h) = |k| \gcd(\tilde{b}, -\tilde{a}).$$

Podle předpokladu  $\gcd(A_h, B_h) = 1$ , takže nutně  $k = 1$  nebo  $k = -1$ .

Pokud  $k = 1$ , dostáváme  $A_h = \tilde{b}, B_h = -\tilde{a}$ , je to tedy přímo generující dvojice z věty 3a.2. Pokud  $k = -1$ , tak máme  $A_h = -\tilde{b}, B_h = \tilde{a}$ , což je také generující dvojice.

□

Umíme tedy zcela řešit homogenní rovnice. Jak nám to pomůže v případě, kdy dostaneme rovnici nehomogenní? Odpoví klíčová strukturální věta.

!

**Věta 3a.4.** (o struktuře řešení lineární diofantické rovnice)

Nechť  $a, b, c \in \mathbb{Z}$ . Uvažujme lineární diofantickou rovnici  $ax + by = c$ . Nechť  $x_p, y_p \in \mathbb{Z}$  je nějaké její řešení.

Dvojice  $x_0, y_0 \in \mathbb{Z}$  je řešení této rovnice právě tehdy, když existuje dvojice  $x_h, y_h \in \mathbb{Z}$  taková, že  $x_0 = x_p + x_h, y_0 = y_p + y_h$  a  $x_h, y_h$  řeší přidruženou homogenní rovnici.

! Tvrzení má formu ekvivalence a říká dvě podstatné informace. Na začátku nějakým způsobem seženeme jedno řešení dané rovnice, což už umíme pomocí Bezoutovy identity. Říká se mu **partikulární řešení** (proto index  $p$ ).

Implikace zprava doleva říká, že když k tomuto jednomu partikulárnímu řešení začneme přičítat řešení homogenní přidružené rovnice (budeme jim zde neoficiálně říkat homogenní řešení), tak získáme generátor nových řešení dané rovnice. Implikace zleva doprava pak říká, že každé řešení vzniká tímto generátorem, tedy jde o generátor dostačující. Jinak řečeno, vzorec z věty vede na obecné řešení.

Pokud vezmeme v úvahu také větu 3a.1, dostáváme následující obrázek: Lineární diofantická rovnice buď nemá řešení žádné, nebo jich má nekonečně mnoho.

**S Rozbor:** Důkaz, že přičtením homogenního řešení k partikulárnímu vznikne nové řešení, je přímočarý. Ověřit, že nějaký kandidát řeší danou rovnici, se standardně dělá dosazením. Jako obvykle bude jednodušší dosadit jen do jedné strany (levé) a postupným výpočtem ukázat, že dostaneme stranu pravou.

Druhá implikace je konceptuálně náročnější. Jde o existenční důkaz, že pro dané řešení  $x_0, y_0$  dokážeme najít homogenní řešení, pomocí kterého vzniklo. Jako obvykle to provedeme tím, že dotyčné homogenní řešení předvedeme. Nejprve musíme vymyslet kandidáta. Hledané homogenní řešení musí splnit dvě podmínky a ta algebraická dost výmluvně napovídá, jakého kandidáta má smysl zkoušet.

**Důkaz (poučný):** Mějme nějaké řešení  $x_p, y_p \in \mathbb{Z}$  dané rovnice, tedy platí  $ax_p + by_p = c$ .

1)  $\Leftarrow$ : Předpokládejme, že dvojice  $x_h, y_h \in \mathbb{Z}$  řeší přidruženou homogenní rovnici. Vytvoříme nová čísla  $x_0 = x_p + x_h, y_0 = y_p + y_h$  a dosadíme do levé strany rovnice. Pak použijeme informace o dvojicích  $x_p, y_p$  a  $x_h, y_h$ .

$$L = ax_0 + by_0 = a(x_p + x_h) + b(y_p + y_h) = (ax_p + by_p) + (ax_h + by_h) = c + 0 = c = R.$$

Ano,  $x_0, y_0$  je opravdu řešením dané rovnice.

2)  $\Rightarrow$ : Předpokládejme, že dvojice  $x_0, y_0$  řeší danou rovnici. Uvažujme čísla  $x_h = x_0 - x_p$  a  $y_h = y_0 - y_p$ . Potvrdíme, že splňují požadavky.

a)  $x_p + x_h = x_p + (x_0 - x_p) = x_0$  a  $y_p + y_h = y_p + (y_0 - y_p) = y_0$ , splněno.

b) Dokážeme, že  $x_h, y_h$  řeší přidruženou homogenní rovnici. Dosadíme do levé strany, díky předpokladům dostáváme

$$L = ax_h + by_h = a(x_0 - x_p) + b(y_0 - y_p) = (ax_0 + by_0) - (ax_p + by_p) = c - c = 0 = R.$$

Ano, dvojice  $x_h, y_h$  řeší přidruženou homogenní rovnici. □

Protože víme, jak obecné homogenní řešení vypadá, můžeme napsat vzorec pro obecné řešení netriviální diofantické rovnice  $ax + by = c$  za předpokladu, že známe nějaké její partikulární řešení  $x_p, y_p$ :

$$\begin{aligned} x &= x_p + \frac{b}{\gcd(a, b)}k, \\ y &= y_p - \frac{a}{\gcd(a, b)}k, \quad k \in \mathbb{Z}. \end{aligned}$$

Popřípadě je možné u homogenního řešení dát znaménka naopak.

Kombinace vět 3a.2 a 3a.4 získáme následující tvrzení.

**Důsledek 3a.5.**

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

$$\begin{aligned} x &= A \frac{c}{\gcd(a, b)} + k \frac{b}{\gcd(a, b)}, \\ y &= B \frac{c}{\gcd(a, b)} - k \frac{a}{\gcd(a, b)}, \quad k \in \mathbb{Z}. \end{aligned}$$

Je možné si tento vzorec zapamatovat, ale nebývá to zvykem, protože je snadné si v paměti něco v něm modifikovat a pak je všechno špatně. Jsou dva docela populární přístupy. Jeden vychází ze znalosti teorie a do jisté míry napodobuje důkazy klíčových vět. Protože je založen na principech a postupech, je relativně rezistentní vůči zapomínání.

**! Příklad 3a.e** (pokračování 3a.c): Řešili jsem rovnici  $15x + 6y = 1251$ . Již jsme našli jedno řešení  $x_p = 417$ ,  $y_p = -834$ .

Přidružená homogenní rovnice  $15x + 6y = 0$  neboli (po povinném zkrácení)  $5x = -2y$  má obecné řešení  $x_h = -2k$ ,  $y_h = 5k$  pro  $k \in \mathbb{Z}$ . Pozici znaménka jsem zvolil tak, aby se ve výsledném řešení u nějaké proměnné nesešly dva mínusy, protože mi to přijde neestetické. Klidně si to udělejte naopak.

Sečtením partikulárního a homogenního řešení dostáváme obecné řešení

$$\begin{aligned}x &= x_p + x_h = 417 - 2k, \\y &= y_p + y_h = -834 + 5k = 5k - 834, \quad k \in \mathbb{Z}.\end{aligned}$$

Můžeme udělat zkoušku, jako obvykle dosazením do rovnice:

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

Jestliže nás zajímají řešení z oboru  $\mathbb{N}_0$ , tak potřebujeme, aby  $5k - 834 \geq 0$  a  $417 - 2k \geq 0$  neboli  $k \geq \frac{834}{5}$  a  $k \leq \frac{417}{2}$ . Taková  $k$  existují, jmenovitě jde o všechna  $k \in \mathbb{N}$  splňující  $167 \leq k \leq 208$ . Můžeme si prostě nějaké vybrat, zvolíme třeba  $k = 200$  a vidíme, že 1251 litrů získáme například tak, že do nádrže nalejeme 17 patnáctilitrových nádob a 166 šestilitrových.

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

△

**! Poznámka o obecném řešení:** V příkladě 3a.e jsme našli obecné řešení  $x = 417 - 2k$ ,  $y = 5k - 834$  pro  $k \in \mathbb{Z}$ . Již jsme komentovali, že šlo také použít alternativu  $x = 417 + 2k$ ,  $y = -834 - 5k$  pro  $k \in \mathbb{Z}$ , která má své vlastní  $k$ . Může vzniknout třeba tak, že do první verze obecného řešení namísto  $k$  dosadíme  $-k$ .

V závěru příkladu jsme ovšem našli další, pro nás zajímavější řešení  $x_0 = 83$ ,  $y_0 = 1$ . Je možné jej použít jako partikulární řešení a tak (se stejným homogenním) vygenerovat nové obecné řešení

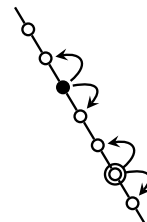
$$\begin{aligned}x &= 83 - 2k, \\y &= 1 + 5k, \quad k \in \mathbb{Z}.\end{aligned}$$

Opět má své vlastní  $k$ . Toto řešení vypadá na první pohled úplně jinak než první verze, ale je stejně legitimní, protože definuje stejnou množinu všech řešení. Například řešení  $x = 13$ ,  $y = 176$  lze z první verze vygenerovat volbou  $k = 202$ , zatímco z této poslední jej dostaneme volbou  $k = 35$ . Čtenář se může přesvědčit, že když do první verze obecného řešení dosadí namísto  $k$  výraz  $k + 167$ , dostane po úpravě třetí verzi obecného řešení.

Toto chování není výjimečné. Víme už, že když má rovnice našeho typu řešení, tak jich má nekonečně mnoho. Každé z nich lze použít jako partikulární řešení ve strukturální větě, tedy nabízí se nekonečně mnoho forem obecného řešení. Všechny jsou mezi sebou převoditelné substitucí za parametr.

Grafické symbolické znázornění: Řešení jsou dvojice čísel, které coby body v  $\mathbb{R}^2$  leží na přímce, v našem případě  $15x + 6y = 1251$ . Dvojici 417, -834 symbolizuje bod, který jsme začernili. Od něj se u první verze obecného řešení pohybujeme pomocí kladných  $k$  doprava a záporných  $k$  doleva k dalším řešením, velikost kroku je určena homogenním řešením. V druhé verzi vycházíme ze stejného místa, ale kladné  $k$  posunuje doleva, záporné doprava. Je zjevné, že nakonec obě verze vytvoří stejné body neboli stejnou množinu řešení. Třetí verze pak vychází z jiného místa, jako příklad jsme jeden bod zdvojili, ale odtud se skáče pomocí stejného homogenního řešení a tudíž se opět vytvoří stejná množina řešení.

△



Postup předvedený v příkladech 3a.c a 3a.e se dá shrnout do „přemýšlivého“ algoritmu založeného na teoretických znalostech chování lineárních diofantických rovnic.

## S Algoritmus 3a.6.

pro nalezení všech celočíselných řešení netriviální rovnice  $ax + by = c$ .

0. Jestliže na první pohled vidíme  $d > 1$ , které dělí  $a$  i  $b$ , ale nedělí  $c$ , tak rovnice nemá řešení.

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

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

Jestliže  $c$  je násobkem  $\gcd(a, b)$ , tak:

a) Získanou rovnost  $aA + bB = \gcd(a, b)$  vynásobíme číslem  $\tilde{c} = \frac{c}{\gcd(a, b)} \in \mathbb{Z}$  tak, aby se zachovaly koeficienty

$a, b$ , a dostaneme  $a(A\tilde{c}) + b(B\tilde{c}) = c$ . To ukazuje partikulární řešení  $x_p = A\tilde{c}$ ,  $y_p = B\tilde{c}$ .

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

c) Sečtením partikulárního a obecného homogenního řešení získáme obecné řešení  $x = x_p + \tilde{b}k$ ,  $y = y_p - \tilde{a}k$ ,  $k \in \mathbb{Z}$ , popřípadě verzi s mínusem u  $x_h$ .

△

Druhý populární přístup využívá možnost vyřešit celou rovnici přímo v rámci Euklidova algoritmu.

! **Příklad 3a.f** (pokračování 3a.c): Řešili jsem rovnici  $15x + 6y = 1251$ . Intuitivně, potřebujeme získat 1251 jako kombinaci vstupních dat.

Euklidův algoritmus nám dal zajímavý řádek s čísly  $|3|1|-2|$ . Ukazuje, jak dostat číslo 3 coby lineární kombinaci vstupních dat 15 a 6. Nás ale nezajímá číslo 3, nýbrž 1251. Již jsme zmínili, že řádky v Euklidovské tabulce je také možno násobit. Když klíčový řádek vynásobíme číslem 417, dostaneme řádek nový, který nám říká, jak ze vstupních dat získat číslo 1251.

Získali jsme tak rovnost  $1251 = 15 \cdot 417 + 6 \cdot (-824)$ , což ukazuje, že  $x_p = 417$ ,  $y_p = -834$  je řešením rovnice.

	(x)	(y)
15	1	0
6	0	1
3●	1●	-2●
0	-2	5
1251	417	-834

Poučení je, že lze zařídit, abychom partikulární řešení  $x_p, y_p$  viděli přímo v příslušném řádku tabulky!

Neméně zajímavý je řádek začínající nulou, který jsme tentokrát dopočetali. Ten říká, že  $0 = 15 \cdot (-2) + 6 \cdot 5$ . To znamená, že čísla  $A_h = -2$  a  $B_h = 5$  řeší homogenní verzi dané rovnice. Jsou to také čísla nesoudělná, proto podle lemma 3a.3 generují všechna homogenní řešení, tedy  $x_h = -2k$ ,  $y = 5k$ .

Spojením homogenního a partikulárního řešení dostáváme obecné řešení  $x = 417 - 2k$ ,  $y = -834 + 5k$ ,  $k \in \mathbb{Z}$ , přesně jako v původním příkladě. Tentokrát jej ale můžeme vykuknout přímo z tabulky.

Aby se nám to lépe vykukovalo, dali jsme si do záhlaví značky, které proměnné odpovídá který pomocný sloupec. Levý pomocný sloupec má iniciační jedničku v prvním řádku začínajícím koeficientem 15, dává tedy informace relevantní pro  $x$ . Pravý pomocný sloupec má iniciační jedničku v „šestkovém“ řádku a vypovídá tedy o  $y$ .

△

Tento postup je vysoce efektivní, ale jeho homogenní krok jsme zatím dostatečně nepodpořili. Potřebujeme vědět, že čísla v „nulovém“ řádku vyjdou nesoudělná. Zatím tomu tak bylo ve všech běžích rozšířeného Euklidova algoritmu, což naznačuje, že to asi bude fungovat. V kapitole 14 dokážeme indukcí, že to platí pro čísla v pomocném sloupci dokonce ve všech krocích algoritmu. Existuje zajímavý alternativní důkaz, který souvisí s trochu jiným pohledem na Euklidův algoritmus, viz bonusová kapitola 18. V ní také čtenář uvidí, jak se náš postup dá upravit na rovnice o více neznámých a dokonce na soustavy lineárních diofantických rovnic.

## S Algoritmus 3a.7.

pro nalezení všech celočíselných řešení netriviální rovnice  $ax + by = c$  Euklidovým algoritmem.

0. Jestliže na první pohled vidíme  $d > 1$ , které dělí  $a$  i  $b$ , ale nedělí  $c$ , tak rovnice nemá řešení.

Jinak sestavíme tabulku pro rozšířený Euklidův algoritmus se vstupními daty  $a, b$  (dosazenými v pořadí větších menších). V pomocných sloupcích vložíme čísla 1 a 0 v jednom, 0 a 1 v druhém. V řádku, který začíná koeficientem  $a$ , najdeme v některém z pomocných sloupců jedničku a napíšeme do jeho záhlaví  $x$ . Obdobně nadepíšeme jako  $y$  pomocný sloupec s jedničkou v řádku koeficientu  $b$ .

1. Aplikujeme Euklidův rozšířený algoritmus.

2. Jestliže řádek ukazující  $\gcd(a, b)$  nelze vynásobit celým číslem tak, aby se místo  $\gcd(a, b)$  objevilo  $c$ , tak daná rovnice nemá řešení.

V opačném případě:

a) Do tabulky přepíšeme takto vynásobený řádek. Čísla v pomocných sloupcích dávají partikulární řešení  $x_p, y_p$  dle nadepsání sloupce.

b) V řádku začínajícím nulou přepíšeme k číslům v pomocných sloupcích parametr  $k$  a získáme tak homogenní řešení  $x_h, y_h$ .

c) Obecné řešení získáme jako  $x = x_p + x_h$ ,  $y = y_p + y_h$ ,  $k \in \mathbb{Z}$ .

△

**Příklad 3a.g:** Vyřešíme rovnici  $208x + 351y = 143$ .

Aplikujeme Euklidův algoritmus na čísla 351 a 208 (začali jsme větším, abychom ušetřili jeden krok). Proměnná  $x$  má koeficient 208, v jeho řádku je jednička v pravém pomocném sloupci, nadepsali jsem jej tedy  $x$ . Obdobně jsme došli k tomu, že levý nám dá  $y$ .

Dostáváme  $\gcd(351, 208) = 13$ , což dělí pravou stranu rovnice, tato rovnice je tedy řešitelná. Tento řádek pak vynásobíme číslem 11, abychom namísto třináctky dostali pravou stranu rovnice 143. Dostáváme  $x_p = -55$ ,  $y_p = 33$ .

Řádek začínající nulou nám dává  $x_h = 27k$ ,  $y_h = -16k$ ,  $k \in \mathbb{Z}$ .

Závěr: Daná rovnice má obecné řešení  $x = -55 + 27k$ ,  $y = 33 - 16k$ ,  $k \in \mathbb{Z}$ .

Zkouška: Dosadíme do dané rovnice:  $208 \cdot (27k - 55) + 351 \cdot (33 - 16k) = 5616k - 11440 + 11583 - 5616k = 143$ .

Pro srovnání přístup inspirovaný teorií: Z tabulky máme Bezoutovu identitu  $208 \cdot (-5) + 351 \cdot 3 = 13$ . Vynásobíme ji číslem 11 na tvar  $208 \cdot (-55) + 351 \cdot 33 = 143$ . Porovnáním s danou rovnicí vidíme řešení  $x_p = -55$ ,  $y_p = 33$ .

Homogenní řešení: Rovnici  $208x + 351y = 0$  vykrátíme číslem 13 a přepíšeme na  $16x = -27y$ . Odtud  $x_h = -27k$ ,  $y_h = 16k$  pro  $k \in \mathbb{Z}$ .

Sečtením partikulárního a obecného homogenního řešení dostáváme obecné řešení dané rovnice  $x = -55 - 27k$ ,  $y = 33 + 16k$ ,  $k \in \mathbb{Z}$ .

Bonus: Pokud bychom chtěli řešení, kde  $x, y \in \mathbb{N}_0$ , tak máme smůlu, žádná nejsou. Vede to totiž na podmínky  $k \leq -\frac{55}{27}$ ,  $k \geq -\frac{33}{16}$ , které se v oboru celých čísel navzájem vylučují.

△

Tento postup je zajímavý v tom, že pokud jej uživatel neaplikuje mechanicky, ale se znalostí toho, proč a jak funguje, tak se při ručním výpočtu občas nabízejí zajímavé zkratky. Ostatně i počítač ocení možnost použít záporné zbytky k potenciálnímu urychlení výpočtů.

**Příklad 3a.h:** Vyřešíme rovnici  $119x - 273y = -70$ .

Zahrajeme si na počítač a koeficienty dáme do tabulky v pořadí, v jakém přišly, a včetně znamének, takže v pomocných sloupcích najdeme řešení ve správném pořadí  $x, y$ .

V prvním kroku počítáme zbytek po dělení menšího čísla větším, což je to menší číslo. Jinak řečeno, druhý řádek odečteme od prvního nulakrát, praktickým důsledkem je změna pořadí čísel.

Z tabulky dostáváme obecné řešení  $x = 160 + 39k$ ,  $y = 70 + 17k$ ,  $k \in \mathbb{Z}$ .

Z pohledu počítače je hotovo. Lidský uživatel by možná preferoval příjemnější partikulární složku. Můžeme k tomu využít obecné řešení a získat jedno takové dosazením  $k = -4$ . Dostaneme  $x_p = 4$ ,  $y_p = 2$  a novou verzi obecného řešení. Tentokrát zkusíme jiný parametr, takže máme  $x = 4 + 39l$ ,  $y = 2 + 17l$  pro  $l \in \mathbb{Z}$ .

Pomocí substituce  $l = k + 4$  snadno ukážeme, že tato nová verze generuje stejnou množinu řešení jako původní:

$$x = 4 + 39l = 4 + 39(k + 4) = 4 + 156 + 39k = 160 + 39k,$$

$$y = 2 + 17l = 2 + 17(k + 4) = 2 + 68 + 17k = 70 + 17k.$$

Je zajímavé, že toto příjemnější partikulární řešení lze získat přímo v průběhu Euklidova algoritmu. My samozřejmě potřebujeme dojet až do  $\gcd(a, b)$  a nuly, ale pak je naším cílem získat číslo  $-70$  a vlastně nás nic nenutí používat zrovna to  $\gcd(a, b) = -7$ . O několik řádků výše si všimneme řádku začínajícího číslem  $-35$ . Když jej vynásobíme dvěma, dostaneme alternativní řádek  $-70 \mid 4 \mid 2$  a z něj  $x_p = 4$ ,  $y_p = 2$ .

V zásadě čím „vyšší“ řádek použijeme, tím menší čísla dostáváme pro partikulární řešení. Lze také řádky skládat, například pokud by pravá strana byla 21, tak to lze získat odečtením řádku s  $\gcd(a, b)$  od předchozího.

Bonus: Pokud bychom pro nějakou aplikaci potřebovali čistě řešení z  $\mathbb{N}$ , tak ze vzorečku vidíme, že jich je nekonečně mnoho.

△

**! Poznámka o linearitě:** Věty o struktuře množiny řešení se mohly čtenáři zdát povědomé. V lineární algebře se studují soustavy lineárních algebraických rovnic a dojde se ke dvěma klíčovými poznatkům.

Tím prvním je, že množina všech řešení homogenní lineární soustavy je vektorový prostor (či také lineární prostor). Typicky si představujeme přímku či rovinu v 3D prostoru, která prochází počátkem. Obecný přístup je, že se identifikuje vektorový prostor  $V$  objektů, se kterými uvažovaný typ rovnice pracuje, a v něm se uvažuje množina  $M$  všech řešení homogenní rovnice. Pak se dokáže se, že  $M$  je podprostor  $V$ . Z praktického pohledu je důležité, že takovýto podprostor lze generovat pomocí báze, což umožní snadné nalezení obecného řešení.

Když pracujeme s netriviální diofantickou rovnicí  $ax + by = c$ , je možné ji interpretovat jako rovnici testující vektory  $(x, y) \in \mathbb{Z}^2$ . Hned narazíme na problém, protože  $\mathbb{Z}^2$  není vektorový prostor. To bychom totiž museli

	(y)	(x)
351	1	0
208	0	1
143	1	-1
65	-1	2
13●	3●	-5●
0	-16	27
143	33	-55

	(x)	(y)
119	1	0
-273	0	1
119	1	0
-35	2	1
14	7	3
-7●	16●	7●
0	39	17
-70	160	70

dovolit násobení vektorů  $(x, y) \in \mathbb{Z}^2$  reálnými skaláry  $\alpha$ , zatímco zde jsme omezeni na  $\alpha \in \mathbb{Z}$ . Proto zde nebudeme oficiálně používat pojmy z lineární teorie, nicméně nacházíme zajímavé paralely.

Zjistili jsme, že pro homogenní rovnice lze řešení zapsat jako  $x_h = \tilde{b}k$ ,  $y_h = -\tilde{a}k$  pro  $k \in \mathbb{Z}$ . Ve vektorovém pohledu to znamená

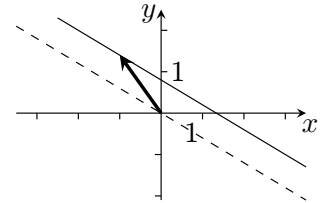
$$(x_h, y_h) = (\tilde{b}k, -\tilde{a}k) = (\tilde{b}, -\tilde{a})k, \quad k \in \mathbb{Z}.$$

Je to, jako by vektor  $(\tilde{b}, -\tilde{a})$  byl bází jednorozměrného prostoru řešení. Odpovídá to i graficky, vzorec pro  $(x_h, y_h)$  vybírá celočíselné body z přímky neboli vektorového prostoru řešení algebraické rovnice  $ax + by = 0$ .

V lineární algebře se to, že  $M$  je podprostor, dokazuje přes jeho uzavřenost na vektorové operace. Jmenovitě se ukáže, že když si vezmeme dva vektory  $\vec{u}, \vec{v} \in M$ , pak také  $\vec{u} + \vec{v} \in M$  a  $\alpha\vec{u} \in M$  pro všechny skaláry.

Pro množinu řešení všech řešení homogenní lineární diofantické rovnice to platí také, je uzavřená na operace sčítání a násobení číslem  $\alpha \in \mathbb{Z}$ , viz cvičení 3a.7. Stojí za poznámku, že optimální důkaz nepoužívá znalost vzorce pro  $x_h, y_h$  a vystačí si jen s tím, že čísla řeší homogenní rovnici, je tedy konceptuálně identický obdobnému důkazu z lineární algebry.

Druhý klíčový poznatek lineární algebry je, že množinu všech řešení nehomogenní soustavy získáme následovně: Najdeme podprostor  $M$  všech řešení přidružené homogenní rovnice a pak jej posuneme přičtením jednoho partikulárního řešení. Na obrázku vidíme množinu všech řešení rovnice  $3x + 5y = 0$  jako přímku procházející počátkem. Když ji posuneme o vektor  $(-1, 1.4)$  řešící rovnici  $3x + 5y = 4$ , tak získáme množinu všech řešení této rovnice.



Matematicky se to vyjádří jako vzorec  $\vec{y}_0 = \vec{y}_p + \vec{y}_h$ .

Přesně totéž ale říká věta 3a.4. Pokud budeme naše řešení zapisovat jako vektory, tak se množina všech řešení rovnice dá zapsat jako

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

Vrátíme-li se k vizuální představě, tak množina řešení přidružené homogenní diofantické rovnice  $ax + by = 0$  jsou korálky pravidelně rozmístěné na přímce procházející počátkem. Když tuto šňůru korálků posuneme o nějaké partikulární řešení, získáme další šňůrku korálků představující množinu všech řešení dané nehomogenní rovnice  $ax + by = c$ .

Ačkoliv nám tedy svět celých čísel nedovoluje pracovat přímo s pojmy lineární algebry, což by nám umožnilo řadu poznatků o množinách řešení prostě zdědit, tak se podstatné chování zachovává. Podobnost jde dokonce ještě dál: Důkaz věty o struktuře řešení v lineární algebře je veden stejně jako důkaz náš, liší se jen zápis rovnice.

Může za to slovo „lineární“. Jakmile si nějaká rovnice či soustava rovnic libovolného druhu (algebraická) zaslouží označení lineární, tak můžeme čekat stejné strukturální věty se stejnými důkazy. Ostatně to čtenář uvidí i v této knize, kde ještě potkáme další typy lineárních rovnic.

Poznamenejme, že ačkoliv nemůžeme používat vektorové pojmy, tak vektorový zápis nabízí pohodlnější zápis některých vzorců, protože umožňuje zahrnout paralelní práci s  $x$  a  $y$  pomocí jedné vektorové operace, viz například zápis množiny všech řešení. Proto jej někteří autoři preferují.

△

K diofantickým rovnicím je ještě vrátíme v bonusových kapitolách. Pro zájemce zde přidáme něco z historie.

**Příklad 3a.i** (slavné diofantické rovnice): Asi nejznámější diofantická rovnice druhého řádu je již zmíněný Pythagorejský vztah  $x^2 + y^2 = z^2$ . Již staří Řekové si kladli otázku, jak to vypadá s celočíselnými (a kladnými) řešeními této rovnice, říká se jim „pythagorejské trojice“ (ačkoliv je již dříve, skoro 2000 let př.n.l., zkoumali Babyloňané). Jistě znáte trojici čísel 3, 4, 5, která tvoří pythagorejskou trojici a jsou to shodou okolností nejmenší možná taková přirozená čísla. Jak je to s dalšími?

Staří Řekové věděli, že pokud nějakou takovou trojici  $(x, y, z)$  máme, tak pro libovolné  $k \in \mathbb{N}$  je rovněž  $(kx, ky, kz)$  pythagorejskou trojicí. Tedy jakmile máme jednu, je jich nekonečně mnoho.

Všimli si také, že pokud jsou čísla  $x, y$  soudělná, pak lze celou rovnost vykrátit číslem  $\gcd(x, y)$  a dostaneme další pythagorejskou trojici, která už má  $x, y$  nesoudělné. Takovým trojicím se říká „primitivní“ a jsou jakýmsi semínky všech pythagorejských trojic.

Jedním z cílů teorie rovnic je schopnost generovat všechna řešení, podobně jako jsme se to učili u lineárních rovnic. Antičtí Řekové to zvládli, vymysleli tohle: Pro libovolné  $u, v \in \mathbb{N}$  tvoří čísla  $x = u^2 - v^2$ ,  $y = 2uv$ ,  $z = u^2 + v^2$  pythagorejské trojice. To se snadno ověří, náročnější je ukázat, že pokud se omezíme na množinu takových dvojic  $(u, v)$ , které jsou nesoudělné a opačné parity, tak již dostáváme přesně množinu všech primitivních pythagorejských trojic.

Rovnici  $x^2 + y^2 = z^2$  tedy rozumíme docela dobře. Naskytá se otázka, jak to dopadne pro vyšší mocninu. V polovině 17. století si známý matematik Fermat četl o pythagorejských trojicích v knize *Arithmetica* napsané

právě Diofantem. Povedlo se mu dokázat, že rovnice  $x^4 + y^4 = z^4$  nemá celočíselná řešení. Na okraj knihy pak poznamenal, že objevil úžasný důkaz, že pro všechny vyšší mocniny než 2 už rovnice  $x^n + y^n = z^n$  nemá celočíselné řešení, ale na okraj se mu nevěle, tak ho tam nenapíše. Tato hypotéza (zvaná „Velká Fermatova věta“ či „Fermatova poslední věta“) byla velkou výzvou. Na konci 18. století dokázal Euler správnost tvrzení pro  $n = 3$ , na počátku 19. století dokázali Legendre a Dirichlet (nezávisle) případ  $n = 5$ , v pololetí onoho století padla sedmička díky Lamému (viz věta 14a.3). Čísel pomalu přibývalo, ale obecný důkaz nikde. Protože jde o snadno pochopitelný problém, pustili se do něj i laici a blouznivci.

Když jsem v 80. letech 20. století studoval na katedře matematiky Karlovy univerzity, objevil se tam každých pár let člověk s hromadou papírů a tvrdil, že dokázal Velkou Fermatovu větu. Profesoři samozřejmě vždy našli chybu, ale obvykle to nebylo lehké, protože v typickém případě šlo o naprostého laika, který příliš neovládal ani jednodušší matematiku, tudíž se na těch stránkách odehrávaly dosti divné věci a vyznat se v nich býval oříšek. Ještě těžší pak bylo takovému laikovi vysvětlit, proč je jeho chyba chybou.

Ale i mezi věhlasnými vědci se čas od času objevil někdo, kdo doufal, že něco dokázal, ale většinou se na to po nějaké době s odstupem podíval, plácl se do čela a sám to stáhl. Nakonec to udolal až Andrew Wiles s pomocníky v roce 1995 a jeho důkaz byl tak komplikovaný, že trvalo několik let, než jej matematici dokázali celý pořádně projít a ověřit. Dnes převažuje názor, že Fermat korektní důkaz neměl.

Další velice populární rovnice je „Pellova rovnice“  $x^2 - ny^2 = 1$ . Speciální verzi  $x^2 - 2y^2 = 1$  studovali již staří Indové, například slavný Brahmagupta (7. století). Inspirací byla snaha najít racionální aproximaci čísla  $\sqrt{2}$ , protože řešení rovnice  $x^2 - 2y^2 = 1$  dává jako zlomek  $\frac{x}{y}$  přibližnou hodnotu  $\sqrt{2}$ . Obecně nám řešení rovnice  $x^2 - ny^2 = 1$  dá  $\frac{x}{y} \sim \sqrt{n}$ , chyba této aproximace není větší než  $\frac{1}{2y^2}$ , což je slušné. Přes tisíc let byli matematici rádi, když dokázali nalézt řešení pro speciální hodnoty  $n$ , například právě Fermat se marně snažil vyřešit speciální případ  $x^2 - 61y^2 = 1$ , uspěl až Euler. Teprve na konci 18. století se objevil obecný postup na řešení těchto rovnic.

S Eulerovým jménem je svázána „Eulerova cihla“. Je to hranol, který má všechny strany celočíselné a také všechny jeho stěny mají celočíselné diagonály. Otázka jejich existence byla jedním z populárních témat matematiky 18. století a bylo nalezeno několik způsobů, jak takové cihly generovat, ale nenašel se generátor všech Eulerových cihel.

Perfektní Eulerova cihla je taková, která má i hlavní diagonálu (vedoucí napříč hranolem) celočíselnou. Dodnes není známo, zda taková cihla existuje. Jinak řečeno, hledá se sedm celých čísel splňujících rovnice

$$a^2 + b^2 = d^2, \quad a^2 + c^2 = e^2, \quad b^2 + c^2 = f^2, \quad a^2 + b^2 + c^2 = g^2.$$

Můžete si hrát.

Jako poslední zajímavost představíme problém dělových koulí (cannonball problem). Na lodích se koule skládaly do pyramid se základnou čtvercovou či tvaru rovnostranného trojúhelníka. Na konci 16. století se známý vědec Raleigh zeptal, zda lze snadno zjistit počet koulí, když víme, kolik jich je ve spodním patře na jedné straně. Matematici mu rádi odpověděli, pro čtvercovou pyramidu to je

$$\sum_{i=1}^k i^2 = \frac{1}{6}k(k+1)(2k+1).$$

Pak někoho napadlo se zeptat: Existuje taková pyramida, že lze z dotyčných koulí sestavit plný čtverec? Dostáváme diofantickou rovnici  $k(k+1)(2k+1) = 6n^2$ . Řešení  $k = n = 1$  je zjevné, našli také řešení  $k = 24$ ,  $n = 70$  (celkem 4900 koulí). Pak se ale na dlouho pokrok zastavil, až v roce 1918 přišel důkaz, že další možnosti už nejsou.

△

## Cvičení

**Cvičení 3a.1** (rutinní, zkouškové): Najděte všechna řešení  $x, y \in \mathbb{Z}$  a  $x, y \in \mathbb{N}_0$  pro následující diofantické rovnice:

- |                        |                         |                          |
|------------------------|-------------------------|--------------------------|
| a) $91x + 65y = 39$ ;  | c) $105x - 63y = 126$ ; | e) $315x + 819y = 126$ ; |
| b) $15x - 65y = 131$ ; | d) $105x - 75y = 0$ ;   | f) $65x + 273y = 157$ .  |

**Cvičení 3a.2:** Dostali jste stokorunu s tím, že za ni máte nakoupit lízátko a bonbóny na dětský den. Lízátko stojí pět korun a bonbón tři koruny. Jaké se nabízejí možnosti, jestliže si nechcete nechat nic od cesty ani nákup dotovat ze svého?

**Cvičení 3a.3:** Podle váhy byste za balík měli platit 74 korun. Na poště zbyly jenom známky v hodnotách 4 a 10. Budou vám schopni vyznačit cenu?

Poznámka: V dávných dobách se balíky platily prostřednictvím lepených známek, podobně jako dopisy, a byly na to speciální známky s vyšší cenou. Když jsem si na jaře 1995 posílal třicetikilový balík knih domů z Kanady, potřebovali se zbavit dopisních známek s Vánočním obrázkem a pokryli s nimi celé dvě stěny balíku.

**Cvičení 3a.4:** Máte k dispozici klasické váhy s dvěma miskami a libovolný počet závaží o váze 15 nebo 55 gramů. Jakou nejmenší hmotnost jste schopni odvážit?

**Cvičení 3a.5:** Máte dvě tyče, jedna má délku 60 dm a druhá má délku 25 dm. Jaká je nejmenší délka látky, kterou pomocí nich dokážete odměřit, pokud odměřujete podél okraje a děláte čárky?

**Cvičení 3a.6** (dobré, první tři zkouškové): Pro každou diofantickou rovnici rozhodněte, pro které hodnoty parametru  $t \in \mathbb{Z}$  je řešitelná.

a)  $8x + 12y = 7t$ ;

c)  $4tx + 5ty = 6$ ;

b)  $12x + 30y = 18 - 4t$ ;

d)  $12x + ty = 13$ .

**Cvičení 3a.7:** Uvažujte diofantickou rovnici  $ax + by = 0$ . Ukažte následující:

a) Jestliže jsou  $(x_1, y_1), (x_2, y_2)$  řešení této rovnice, tak ji řeší i jejich součet  $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_2 + y_2)$ .

b) Jestliže je  $(x_0, y_0)$  řešení této rovnice a  $\alpha \in \mathbb{Z}$ , tak ji řeší i  $\alpha(x_0, y_0) = (\alpha x_0, \alpha y_0)$ .

**Řešení:**

**3a.1:**

	(x)	(y)
91	1	0
65	0	1
26	1	-1
13●	-2●	3●
0	5	-7
39	-6	9

$$\gcd(91, 65) = 13 = 91 \cdot (-2) + 65 \cdot 3$$

$$\rightarrow 39 = 91 \cdot (-6) + 65 \cdot 9 \rightarrow x_p = -6, y_p = 9$$

$$91x + 65y = 0 \rightarrow 7x + 5y = 0 \rightarrow 7x = -5y$$

$$\rightarrow x_h = 5k, y_h = -7k$$

Odtud  $x = -6 + 5k, y = 9 - 7k, k \in \mathbb{Z}$   
 Nebo to vykougáme z tabulky.  
 $x, y \in \mathbb{N}_0$  nelze.

	(y)	(x)
-65	1	0
15	0	1
-5	1	4
5●	-1●	-4●
0		

$$\gcd(15, -65) = 5 \text{ nedělí } 131. \text{ Nemá řešení.}$$

	(x)	(y)
105	1	0
-63	0	1
42	1	1
21●	2●	3●
0	-3	-5
126	12	18

$$\gcd(105, -63) = 21 = 105 \cdot 2 - 63 \cdot 3$$

$$\rightarrow 126 = 105 \cdot 12 - 63 \cdot 18 \rightarrow x_p = 12, y_p = 18$$

$$105x - 63y = 0 \rightarrow 5x - 3y = 0 \rightarrow 5x = 3y$$

$$\rightarrow x_h = 3k, y_h = 5k$$

Odtud  $x = 12 + 3k, y = 18 + 5k, k \in \mathbb{Z}$   
 Nebo to vykougáme z tabulky.  
 $x, y \in \mathbb{N}_0$  pro  $k \geq -3$ .

d)  $\gcd(105, 75) = 15, 7x - 5y = 0$  homogenní rovnice. Řešení  $x = 5k, y = 7k$  pro  $k \in \mathbb{Z}$ . Řešení v  $\mathbb{N}_0$  pro  $k \geq 0$ .

	(y)	(x)
819	1	0
315	0	1
-126	1	-3
63●	2●	-5●
0	5	-13
126	4	-10

$$\gcd(315, 819) = 63 = 315 \cdot (-5) + 819 \cdot 2$$

$$\rightarrow 126 = 315 \cdot (-10) + 819 \cdot 4 \rightarrow x_p = -10, y_p = 4$$

$$315x + 819y = 0 \rightarrow 5x + 13y = 0 \rightarrow 5x = -13y$$

$$\rightarrow x_h = 13k, y_h = -5k$$

Odtud  $x = -10 + 13k, y = 4 - 5k, k \in \mathbb{Z}$   
 Nebo to vykougáme z tabulky.  
 $x, y \in \mathbb{N}$  nelze.

f)  $\gcd(65, 273) = 13$  nedělí 157. Nemá řešení.

**3a.2:** Rovnice  $5l + 3b = 100$ .  $\gcd(5, 3) = 1 = 5 \cdot (-1) + 3 \cdot 2$  tedy  $5 \cdot (-100) + 3 \cdot 200 = 100, l_p = -100, b_p = 200$ .  
 $5l + 3b = 0$  dá  $l_h = 3k, b_h = -5k$ , obecné řešení  $l = 3k - 100, b = 200 - 5k$  pro  $k \in \mathbb{Z}$ . Chceme  $l, b \geq 0, k \leq 40$  a  $k \geq 34$ , celkem 7 možností  $(2, 30), (5, 25), (8, 20), (11, 15), (14, 10), (17, 5), (20, 0), (0, 50)$ .

**3a.3:** Rovnice  $10x + 4y = 74$ .  $\gcd(10, 4) = 2 = 10 \cdot 1 + 4 \cdot (-2)$  tedy  $10 \cdot 37 + 4 \cdot (-74) = 74, x_p = 37, y_p = -74$ .  
 $10x + 4y = 0$  neboli  $5x + 2y = 0$  dá  $x_h = -2k, y_h = 5k$ , obecné řešení  $x = 37 - 2k, y = 5k - 74$  pro  $k \in \mathbb{Z}$ . Chceme  $x, y \geq 0$ , třeba  $k = 15$  dá  $x = 7$  desetikorunových a  $y = 1$  čtyřkorunovou známku jako řešení.

**3a.4:** Váhu  $c$  odměříme, pokud lze napsat  $c = 15x + 55y$ , kde  $x, y \in \mathbb{Z}$  a záporné hodnoty znamenají, že takováto závaží dáváme na stejnou misku jako dotyčný předmět. Rovnice má řešení, pokud  $\gcd(15, 55)$  dělí  $c$ , tedy nejmenší váha je 5 gramů.

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

**Cvičení 3a.6** (dobré, zkouškové): a) Řešitelná pokud  $\gcd(8, 12)$  dělí  $t$  neboli pokud 4 dělí  $7t$  neboli (díky  $\gcd(4, 7) = 1$ ) pokud  $4 \mid t$ . Závěr: Řešitelná pro  $t = 4k, k \in \mathbb{Z}$ .

b) Řešitelná pokud  $\gcd(12, 30)$  dělí  $18 - 4t$  neboli pokud 6 dělí  $18 - 4t$  neboli (díky  $6 \mid 18$ ) pokud  $6 \mid 4t$  neboli pokud  $3 \mid t$ . Závěr: Řešitelná pro  $t = 3k, k \in \mathbb{Z}$ .

c) Řešitelná pokud  $\gcd(4t, 5t)$  dělí 6 neboli pokud  $t \gcd(4, 5)$  dělí 6 neboli pokud  $t \mid 6$ . Závěr: Řešitelná pro  $t = 1, 2, 3, 6$ .

d) Řešitelná pokud  $\gcd(12, t)$  dělí 13 neboli pokud  $\gcd(4 \cdot 3, t)$  dělí 13 neboli pokud  $\gcd(4 \cdot 3, t) = 1$ . Závěr: Řešitelná pokud  $\gcd(12, t) = 1$ . (Šlo by také chtít  $\gcd(6, t) = 1$ , pak totiž  $\gcd(12, t) = 1$ ).

**3a.7:** a) Dosadíme  $x = x_1 + x_2, y = y_2 + y_2$  do rovnice:  $L = a(x_1 + x_2) + b(y_1 + y_2) = (ax_1 + by_1) + (ax_2 + by + 2) = 0 + 0 = 0$ .

b) Dosadíme  $x = \alpha x_0, y = \alpha y_0$  do rovnice:  $L = a(\alpha x_0) + b(\alpha y_0) = \alpha(ax_0 + by_0) = \alpha \cdot 0 = 0$ .

### 3b. Lineární kongruence

Nyní se přeneseme do světa celých čísel modulo  $n$ . I tam někdy potřebujeme řešit rovnice, přičemž rovnost se bere jako rovnost modulo neboli kongruence. Opět se omezíme na nejjednodušší lineární rovnice.



#### Definice.

Termínem **lineární kongruence** označujeme rovnice typu  $ax \equiv b \pmod{n}$ , kde  $n \in \mathbb{N}, a, b \in \mathbb{Z}$  a hledáme celočíselná řešení  $x_0$ .

Tyto „rovnice“ už vlastně umíme řešit. Kongruenci  $ax \equiv b \pmod{n}$  umíme přepsat jako  $ax = b + kn, k \in \mathbb{Z}$ , což je povědomý tvar. Pro Euklidův algoritmus bude výhodnější úprava  $ax - kn = b$  neboli  $ax + n(-k) = b$ .



#### Fakt 3b.1.

Nechť  $n \in \mathbb{N}$ . Uvažujme  $a, b \in \mathbb{Z}$ . Číslo  $x_0 \in \mathbb{Z}$  řeší lineární kongruenci  $ax \equiv b \pmod{n}$  právě tehdy, když pro nějaké  $y_0 \in \mathbb{Z}$  dvojice  $x_0, y_0$  řeší diofantickou rovnici  $ax + ny = b$ .

**Důkaz:** Pokud je  $x_0$  řešení kongruence  $ax_0 \equiv b \pmod{n}$ , tak podle věty 2a.1  $ax_0 = b + kn$  pro nějaké  $k \in \mathbb{Z}$ . Označme  $y_0 = -k$ . Pak  $ax_0 + ny_0 = b$  a  $x_0, y_0 \in \mathbb{Z}$ , tedy  $x_0, y_0$  řeší rovnici  $ax + ny = b$ .

Pokud dvojice  $x_0, y_0 \in \mathbb{Z}$  řeší rovnici  $ax + ny = b$ , tak platí rovnost  $ax_0 + ny_0 = b$ . Podle faktu 2a.6 a díky  $n \equiv 0 \pmod{n}$  pak platí  $ax_0 + 0 \equiv b \pmod{n}$  a proto  $x_0$  řeší  $ax \equiv b \pmod{n}$ . □

! Důkaz je zároveň návodem. Stačí najít všechna řešení rovnice  $ax + ny = b$ , načež ignorujeme složku  $y$  a ta  $x$  nám dají hledaná řešení lineární kongruence. Tvar  $ax + nk = b$  znamená, že pokud pro  $a$  vhodně zvolíme zástupce, tak máme na vstupu Euklidova algoritmu nezáporná čísla, což je příjemné.

Díky  $n \in \mathbb{N}$  je výsledná rovnice  $ax + ny = b$  vždy netriviální, tedy se na ni vztahují všechna tvrzení z předchozí sekce. Výsledky 3a.1, 3a.4 a 3a.2 lze také přenést do světa kongruencí a zkombinovat v následující tvrzení.



#### Věta 3b.2.

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

(i) Jestliže  $b$  není násobkem  $\gcd(a, n)$ , tak řešení kongruence  $ax \equiv b \pmod{n}$  neexistuje.

(ii) Jestliže  $\gcd(a, n)$  dělí  $b$ , tak kongruence  $ax \equiv b \pmod{n}$  má nějaké řešení  $x_p \in \mathbb{Z}$ .

Označme  $\tilde{n} = \frac{n}{\gcd(a, n)}$ . Pak obecné řešení lineární kongruence  $ax \equiv b \pmod{n}$  je

$$x = x_p + k\tilde{n}, k \in \mathbb{Z}.$$

! **Příklad 3b.a:** Vyřešíme kongruenci  $45x \equiv 9 \pmod{231}$ .

Kongruenci převedeme na diofantickou rovnici  $45x + 231y = 9$ . Tu vyřešíme pomocí algoritmu 3a.7. Protože nás  $y$  nezajímá, nemusíme odpovídající hodnoty počítat. Vlastně bychom ani nemuseli ten sloupec uvádět, chtěli jsme jen čtenáři ukázat, jaká je spojitost s algoritmem z minulé části. Zde je třeba být trochu opatrný, ať neignorujeme zrovna ten sloupec, který potřebujeme, raději si je nadepíšeme jmény proměnných.

Řešení existuje, dostali jsme obecné řešení  $x = 108 - 77k$  pro  $k \in \mathbb{Z}$ .

Poznamenejme, že to odpovídá vzorci z věty, opravdu  $77 = \frac{231}{\gcd(45, 231)}$ .

Zkouška:

$$45 \cdot (108 - 77k) = 4860 - 3465k = (231 \cdot 21 + 9) + 15 \cdot 231k \equiv 9 + 0k = 9 \pmod{231}.$$

	(y)	(x)
231	1	0
45	0	1
6		-5
3		36
0		-77
9		108

Ve světě modulo bychom mohli posouvat  $x_p = 108$  o 231, což moc nepomůže. Ve vzorci pro obecné řešení ale vidíme, že nová řešení dostaneme i při posunu o 77, takže bychom mohli nabídnout také obecné řešení  $x = 31 - 77k$ ,  $k \in \mathbb{Z}$ . Protože u homogenního řešení  $x_h = -77k$  je možné znaménko změnit (formálně například substitucí  $k = -l$ ), je také možné použít vzorec  $x = 31 + 77k$ ,  $k \in \mathbb{Z}$ . Jako obvykle, každý z těchto vzorců má své vlastní  $k$ .

Mimořádně, příjemnější partikulární řešení  $x = 31$  lze získat rovnou pomocí tabulky. Jak víme, cílem je získat v posledním řádku vlevo číslo 9. To lze získat nejen jako trojnásobek řádku „trojkového“, ale také sečtením řádku „trojkového“ a „šestkového“.

△

**Příklad 3b.b:** Uvažujme modifikovaný příklad  $45x \equiv 8 \pmod{231}$ .

Kongruenci převedeme na diofantickou rovnici  $45x + 231y = 8$ . Protože má stejnou levou stranu jako příklad 3b.a, dostaneme stejný běh Euklidova algoritmu. Rozdíl je v tom, že teď v levém sloupci neumíme získat pravou stranu 8. To ukazuje, že  $3 = \gcd(45, 231)$  nedělí pravou stranu, a proto podle věty 3b.2 řešení úlohy neexistuje.

Opravdu? Když trojkový řádek vynásobíme číslem  $\frac{8}{3}$ , dostaneme řádek  $| 8 | 96 |$ , což ukazuje na  $x_p = 96$ . Kde je problém?

V tom, že sloupec pro  $y$  sice nepotřebujeme pro řešení kongruence, ale je nezbytný pro přechod mezi kongruencí a diofantickou rovnicí dle faktu. Celý řádek je  $| 3 | -7 | 36 |$ , po vynásobení  $| 8 | -\frac{56}{3} | 96 |$  a hned vidíme problém.

△

	(x)
231	0
45	1
6	-5
3	36
0	-77
?	

### S Algoritmus 3b.3.

pro nalezení všech řešení kongruence  $ax \equiv b \pmod{n}$  Euklidovým algoritmem.

**0.** Pokud je to třeba, nahradíme  $a$  zástupcem  $a \pmod{n}$ .

Sestavíme tabulku pro rozšířený Euklidův algoritmus se vstupními daty  $n, a$  a pomocným sloupcem s iniciačními hodnotami 0, 1.

**1.** Aplikujeme Euklidův rozšířený algoritmus.

**2.** Jestliže řádek ukazující  $\gcd(a, n)$  nelze vynásobit celým číslem tak, aby se místo  $\gcd(a, n)$  objevilo  $b$ , tak daná kongruence nemá řešení.

V opačném případě:

a) Do tabulky přepíšeme takto vynásobený řádek. Číslo v pomocném sloupci dává  $x_p$ .

b) V řádku začínajícím nulou přepíšeme k číslu v pomocném sloupci parametr  $k$  a získáme tak homogenní řešení  $x_h$ .

c) Obecné řešení získáme jako  $x = x_p + x_h, k \in \mathbb{Z}$ .

△

**! Poznámka:** Podívejme se blíže na řešení, která jsme získali v příkladě 3b.a. Našli jsme partikulární řešení  $x_p = 108$  a poté obecné řešení  $108 + 77l$ , které generuje množinu řešení

$$\dots, -123, -46, 31, 108, 185, 262, 339, 416, \dots$$

Ovšem ve světě modula považujeme určitá čísla za stejná. Kolik máme skutečně různých řešení?

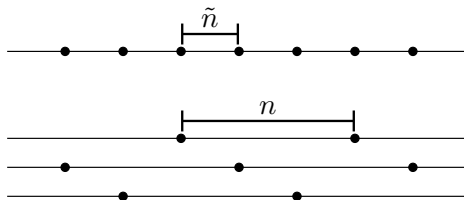
Naše partikulární řešení splňuje rovnost  $45x \equiv 9 \pmod{231}$ , ovšem podle věty 2a.7 ji bude splňovat také každý jeho kongruentní zástupce. Čísla  $108 + 231k, k \in \mathbb{Z}$  neboli

$$\dots, -123, 108, 339, \dots$$

tedy budou všechna řešením dané kongruence, a skutečně je najdeme v tom seznamu výše. Musí to tak být a je to založeno na faktu, že 77 dělí 231. V množině všech řešení se od 108 pohybujeme kroky velikosti 77 a každé tři takové kroky nás posunou o 231, tedy dostaneme se k dalšímu členu zbytkové třídy  $[108]_{231}$ . Množina všech řešení proto obsahuje tuto třídu.

Když se posuneme o 77 jednou, dostaneme se k číslu 185, které do  $[108]_{231}$  nepatří, jde tedy o jiné řešení (z pohledu kongruence). Stejný argument jako výše ukazuje, že jeho třída kongruence  $[185]_{231}$  bude součástí řešení. Když se posuneme z 108 o 77 dvakrát, dostaneme se k číslu  $185 + 77 = 262$ , což je další nová hodnota mezi řešeními, jde o třídu  $[262]_{231} = [31]_{231}$ . Ale tři posuny o 77 od čísla 108 nás zavedou zpět do třídy  $[108]_{231}$ , takže nic dalšího nedostaneme.

Vidíme, že se množina všech řešení skládá ze tří různých proplétajících se tříd, například  $[31]_{231}$ ,  $[108]_{231}$  a  $[185]_{231}$ . Z pohledu kongruence má tedy rovnice tři různá řešení.



Toto chování je univerzální. Jestliže je  $x_p$  nějaké řešení, tak je obecné řešení zapsatelné jako  $x_p + \tilde{n}k$ , kde  $\tilde{n} = \frac{n}{\gcd(a, n)}$ . Pak  $n = \tilde{n} \cdot \gcd(a, n)$ , kde  $\gcd(a, n) \in \mathbb{Z}$ , tedy  $n$  je násobkem  $\tilde{n}$  a proto budou řešení vytvořená vzorcem  $x = x_p + nl$  neboli třída  $[x_p]_n$  vždy součástí množiny dané vzorcem  $x_p + \tilde{n}k$ . Vidíme také, že je potřeba udělat  $\gcd(a, n)$  kroků velikosti  $\tilde{n}$ , než z toho bude jeden krok velikosti  $n$ , což určuje počet různých zbytkových tříd v našem řešení. Potvrdíme to oficiálně.

△

**! Věta 3b.4.**

Nechť  $n \in \mathbb{N}$ , uvažujme kongruenci  $ax \equiv b \pmod{n}$  pro nějaká  $a, b \in \mathbb{Z}$ . Nechť  $x_p$  je nějaké její partikulární řešení.

Definujme čísla  $x_i = x_p + \frac{n}{\gcd(a, n)}i$  pro  $i = 0, 1, \dots, \gcd(a, n) - 1$ . Množina všech řešení dané kongruence je sjednocením zbytkových tříd  $[x_i]_n$  pro  $i = 0, 1, \dots, \gcd(a, n) - 1$ , tyto třídy jsou navzájem disjunktní.

**Důkaz:** Uvažujme partikulární řešení  $x_p$  a čísla  $x_i$  dle tvrzení. Všimneme si, že  $x_0 = x_p$ .

Zvolme libovolné  $i, j \in \{0, 1, \dots, \gcd(a, n) - 1\}$ . Pak  $|i - j| < \gcd(a, n)$ , a proto

$$|x_i - x_j| = \left| x_p + \frac{n}{\gcd(a, n)}i - \left( x_p + \frac{n}{\gcd(a, n)}j \right) \right| = \frac{n}{\gcd(a, n)}|i - j| < n.$$

Pokud by platilo  $x_i \equiv x_j \pmod{n}$ , pak by podle faktu 2a.4 muselo platit i  $x_i = x_j$  a tedy  $i = j$ . To znamená, že pro  $i \neq j$  nejsou  $x_i, x_j$  kongruentní a proto jsou třídy  $[x_i]_n, [x_j]_n$  disjunktní.

Označme jako  $M = \{x_p + \frac{n}{\gcd(a, n)}l; l \in \mathbb{Z}\}$  množinu všech řešení dané kongruence.

Uvažujme  $x \in [x_i]_n$ . Pak pro nějaké  $k \in \mathbb{Z}$  máme

$$x = x_i + kn = x_p + \frac{n}{\gcd(a, n)}i + k \gcd(a, n) \frac{n}{\gcd(a, n)} = x_p + \frac{n}{\gcd(a, n)}(i + k \gcd(a, n)),$$

kde  $i + k \gcd(a, n) \in \mathbb{Z}$ . Proto je dle věty 3b.2  $x$  řešením dané kongruence. Ukázali jsme, že  $\bigcup [x_i]_n \subseteq M$ .

Nechť je naopak  $x$  nějaké řešení dané kongruence. Pak pro nějaké  $l \in \mathbb{Z}$  máme  $x = x_p + \frac{n}{\gcd(a, n)}l$ . Nechť  $i = l \bmod \gcd(a, n)$ , tedy  $l = q \gcd(a, n) + i$  pro  $q \in \mathbb{Z}$ . Pak

$$x = x_p + \frac{n}{\gcd(a, n)}(q \gcd(a, n) + i) = x_p + \frac{n}{\gcd(a, n)}i + x_p + nq = x_i + nq,$$

tedy  $x \in [x_i]_n$  a  $i \in \{0, 1, \dots, \gcd(a, n) - 1\}$ . Dokázali jsme, že  $M \subseteq \bigcup [x_i]_n$ .

Proto  $M = \bigcup_{i=0}^{\gcd(a, n)-1} [x_i]_n$ .

□

Při ručním počítání nemusíme jako základ brát přímo to  $x_p$ , které vyšlo z algoritmu, ale můžeme jej nejprve vhodně posunout o  $\tilde{n}$ . Je tedy možné mít reprezentanty řešení z množiny  $\{0, 1, \dots, n - 1\}$ . Dosáhneme toho tak, větu 3b.4 aplikujeme s výchozí hodnotou  $x_p \bmod \tilde{n}$ , v příkladě 3b.a by to bylo 31.

Nemusíme nutně brát jednotlivé zástupce podle věty neboli tak, jak jdou za sebou. Můžeme je vybírat z různých period, třeba 108, 262 a 878. Je to ale nepraktické a pro uživatele matoucí.

Vlastně jsme ukázali rozklad množiny řešení, viz poznámka 1b.2 a kapitola 5.

**Příklad 3b.c:** Vyřešíme kongruenci  $30x \equiv 0 \pmod{33}$ .

Máme homogenní kongruenci, která by měla být jednodušší, proto to zkusíme jinak. Podle cvičení 1a.11 je  $x \in \mathbb{Z}$  řešením právě tehdy, když  $33 \mid (30x)$ . Protože  $\gcd(30, 33) = 3$ , tak dělitelnost platí právě tehdy, když  $11 \mid (10x)$  (viz cvičení 1a.7). Protože  $\gcd(10, 11) = 1$ , díky lemma 1b.23 dostáváme ekvivalentní podmínku  $11 \mid x$ . Máme tedy obecné řešení  $x = 11k, k \in \mathbb{Z}$ .

Mimočodem, protože  $\gcd(30, 33) = 3$ , tak toto řešení sestává ze tří různých zbytkových tříd zastoupených například čísly 0, 11, 22.

Co se stane, když na tuto kongruenci aplikujeme standardní postup?

Vidíme řádek se správným generátorem homogenního řešení, my bychom ovšem měli ještě vygenerovat partikulární řešení. Jako počítač bychom dostali instrukci, že máme předposlední řádek vynásobit číslem  $\frac{c}{\gcd(a, n)}$ , čímž dostaneme potřebné informace. V tomto případě násobíme nulou a dole v tabulce přibude řádek  $|0 \ 0|$ .

	(x)
33	0
30	1
3	-1
0	11

Dostáváme pak obecné řešení  $x = 0 + 11k$ ,  $k \in \mathbb{Z}$ , tedy algoritmus opravdu dospěl ke správnému řešení, i když poněkud srandovněm způsobem.

△

Při ručním počítání jsme rádi, když si můžeme výpočty zjednodušit, při řešení rovnic například s oblibou krátíme (pokud je to možné). Bude to také možné dělat s kongruencemi?

**Příklad 3b.d:** V příkladě 3b.a jsme řešili kongruenci  $45x \equiv 9 \pmod{231}$ . Protože jsou 45 i 9 dělitelné devíti, nabízí se krácení.

Kongruenci  $5 \equiv 1 \pmod{231}$  hravě vyřešíme, díky krácení byl algoritmus kratší. Dostali jsme obecné řešení  $x = -46 + 231k$ ,  $k \in \mathbb{Z}$  a máme problém, protože krok je  $n = 231$ , řešením je tedy jedna zbytková třída  $[-46]_{231} = [185]_{231}$ . My ale víme, že mají být tři, takže jsme přišli o dvě třetiny řešení.

	(x)
231	0
5	1
1	-46
0	231

Vidíme, že krácení v kongruenci není možné.

△

Abychom lépe viděli, co se děje, přepíšeme kongruenci  $ax \equiv b \pmod{n}$  na algebraickou rovnost  $ax + ny = b$ . Vidíme, že jsem při našem pokusu vlastně krátili jen dva koeficienty ze tří, takže není divu, že to nedopadlo dobře. Zároveň to napovídá, co by fungovat mohlo.

#### Lemma 3b.5.

Nechť  $n \in \mathbb{N}$ , uvažujme  $a, b \in \mathbb{Z}$ . Předpokládejme, že  $d \in \mathbb{N}$  dělí čísla  $a, b, n$ .

Pak číslo  $x_0 \in \mathbb{Z}$  řeší kongruenci  $ax \equiv b \pmod{n}$  právě tehdy,

když řeší kongruenci  $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ .

**Důkaz:**  $ax_0 \equiv b \pmod{n}$  právě tehdy, když existuje nějaké  $y_0 \in \mathbb{Z}$ , aby  $ax_0 = b + y_0n$ , což je právě tehdy, když existuje nějaké  $y_0 \in \mathbb{Z}$ , aby  $\frac{a}{d}x_0 = \frac{b}{d} + y_0\frac{n}{d}$ , což je právě tehdy, když  $\frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ . □

Protože je snadné ve stresu zapomenout krátit i modul, je bezpečnější tohle prostě vypustit a případné krácení dělat až po převodu na diofantickou rovnici.

Protože se kongruence  $ax \equiv b \pmod{n}$  nazývá lineární, dá se čekat, že pro její řešení budeme mít příslušné strukturální chování. Je tomu tak.

Homogenní kongruence má obecné řešení  $x_h = \frac{n}{\gcd(a, n)}k$ , množina všech řešení je tedy generována číslem  $\tilde{n} = \frac{n}{\gcd(a, n)}$  a opět si ji můžeme představit jako jednorozměrnou. Ve cvičení 3b.4 si dokážete, že množina řešení homogenní lineární kongruence je uzavřená na operace, opět stačí vyjít z vlastností, nikoliv z přesného popisu.

Množinu řešení pro nehomogenní verzi pak získáme posunem této množiny.

#### ! Věta 3b.6.

Nechť  $n \in \mathbb{N}$ . Uvažujme kongruenci  $ax \equiv b \pmod{n}$  pro nějaká  $a, b \in \mathbb{Z}$ , nechť  $x_p$  je nějaké její řešení.

Číslo  $x_0 \in \mathbb{Z}$  je řešením kongruence  $ax \equiv b \pmod{n}$  právě tehdy, když existuje  $x_h \in \mathbb{Z}$ , které splňuje  $x_0 = x_p + x_h$  a je řešením přidružené homogenní kongruence  $ax \equiv 0 \pmod{n}$ .

Důkaz je natolik podobný důkazu věty 3a.4, že jej s klidným svědomím necháme jako cvičení 3b.3. Je dokonce ještě snadnější, protože se pracuje jen s jednou proměnnou, dají se také použít věty z kapitoly 2 o aritmetice ve světě modula. A stejně jako v předchozí sekci, i teď lze větu shrnout prohlášením, že množina všech řešení dané kongruence je

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

## Cvičení

**Cvičení 3b.1** (rutinní, zkouškové): Vyřešte následující kongruence:

- a)  $84x \equiv -56 \pmod{308}$ ;      c)  $12x \equiv 0 \pmod{20}$ ;      e)  $40x \equiv 16 \pmod{132}$ ;  
 b)  $34x \equiv 5 \pmod{79}$ ;      d)  $33x \equiv 17 \pmod{99}$ ;      f)  $11x \equiv 0 \pmod{40}$ .

**Cvičení 3b.2** (dobré, zkouškové): Pro každou z následujících kongruencí rozhodněte, pro které hodnoty parametru  $t \in \mathbb{Z}$  bude řešitelná.

- a)  $4x \equiv 2t \pmod{6}$ ,      b)  $30x \equiv 20 - 8t \pmod{40}$ .

**Cvičení 3b.3** (rutinní, poučné): Necht'  $n \in \mathbb{N}$ , necht'  $a, b \in \mathbb{Z}$ . Uvažujme nějaké řešení  $x_p$  kongruence  $ax \equiv b$ .

- a) Dokažte, že když je i  $x_0 \in \mathbb{Z}$  řešením této kongruence, tak číslo  $x_h = x_0 - x_p$  řeší kongruenci  $ax \equiv 0 \pmod{n}$ .  
 b) Dokažte, že když  $x_h \in \mathbb{Z}$  je řešením kongruence  $ax \equiv 0 \pmod{n}$ , tak  $x_0 = x_p + x_h$  řeší kongruenci  $ax \equiv b \pmod{n}$ .

**Cvičení 3b.4** (rutinní, poučné): Necht'  $n \in \mathbb{N}$ , necht'  $a \in \mathbb{Z}$ .

- a) Dokažte, že jestliže  $x_1, x_2$  řeší kongruenci  $ax \equiv 0$ , tak také  $x_1 + x_2$  ji řeší.  
 b) Dokažte, že jestliže  $x_0$  řeší kongruenci  $ax \equiv 0$ , tak také  $\alpha x_0$  ji řeší pro libovolné  $\alpha \in \mathbb{Z}$ .

## Řešení:

- 3b.1:** a) 

308	0
84	1
-28	-4
28●	4●
0	-11
-56	-8

      Rovnice  $84x + 308y = -56$   
 $\gcd(84, 308) = 28 = 84 \cdot 4 + 308 \cdot (-1)$   
 $\rightarrow -56 = 84 \cdot (-8) + 308 \cdot 2 \rightarrow x_p = -8$   
 $84x + 308y = 0 \rightarrow 3x + 11y = 0 \rightarrow 7x = -11y \rightarrow x_h = 11k$   
 Odtud  $x = -8 + 11k$  nebo  $x = 3 + 11k, k \in \mathbb{Z}$   
 Nebo to vykoukáme z tabulky.
- b) 

79	0
34	1
11	-2
1●	7●
0	-79
5	35

      Rovnice  $34x + 79y = 5$   
 $\gcd(34, 79) = 1 = 34 \cdot 7 + 79 \cdot (-3)$   
 $\rightarrow 5 = 34 \cdot 35 + 79 \cdot (-15) \rightarrow x_p = 35$   
 $35x + 79y = 0 \rightarrow 34x = -79y \rightarrow x_h = 79k$   
 Odtud  $x = 35 + 79k, k \in \mathbb{Z}$   
 Nebo to vykoukáme z tabulky.
- c)  $12x + 20y = 0$ , je už homogenní. Evidentně  $\gcd(12, 20) = 4$ , zkrátíme,  $3x + 5y = 0 \rightarrow 3x = -5y. x = 5k, k \in \mathbb{Z}$ .
- d) protože  $\gcd(33, 99) = 33$  a 17 není násobkem 33, kongruence nemá řešení.
- e) 

132	0
40	1
12	-3
4●	10●
0	-33
16	40

      Rovnice  $40x + 132y = 16$   
 $\gcd(40, 132) = 4 = 40 \cdot 10 + 132 \cdot (-3)$   
 $\rightarrow 16 = 40 \cdot 40 + 132 \cdot (-12) \rightarrow x_p = 40$   
 $40x + 132y = 0 \rightarrow 10x + 33y = 0 \rightarrow 10x = -33y \rightarrow x_h = 33k$   
 Odtud  $x = 40 + 33k$  nebo  $x = 7 + 33k, k \in \mathbb{Z}$   
 Nebo to vykoukáme z tabulky.
- f) Protože  $\gcd(11, 40) = 1$ , je množina řešení  $x = 40k, k \in \mathbb{Z}$ .
- 3b.2:** a) Řešení existuje, pokud  $\gcd(4, 6)$  dělí  $2t$  neboli pokud 2 dělí  $2t$ , což je pro všechna  $t \in \mathbb{Z}$ . b) Řešení existuje, pokud  $\gcd(30, 40)$  dělí  $20 - 8t$  neboli pokud 10 dělí  $20 - 8t$  neboli (díky  $10 \mid 20$ ) pokud 10 dělí  $8t$  neboli pokud 5 dělí  $t$ . Závěr: Kongruence je řešitelná pro  $t = 5k, k \in \mathbb{Z}$ .
- 3b.3:** a)  $a(x_0 - x_p) = ax_0 - ax_p \equiv b - b = 0 \pmod{n}$ .  
 b) je podobné.
- 3b.4:** a)  $a(x + 1 + x_2) = ax_1 + ax_2 \equiv 0 + 0 = 0$ . b)  $a(\alpha x_0) = \alpha \cdot (ax_0) \equiv \alpha \cdot 0 = 0 \pmod{n}$ .

3c. Rovnice v prostorech  $\mathbb{Z}_n$ 

V prostorech  $\mathbb{Z}_n$  máme čísla a standardní rovnost, můžeme tedy formovat rovnice. Opět se zaměříme na tu nejjednodušší, nicméně velmi užitečnou: lineární rovnici  $a \odot x = b$ . A opět konstatujeme, že jsme již řešili její speciální případ  $a \odot x = 1$  při hledání inverzního čísla. Obecnější případ se řeší obdobně a je založen na následující větě.

! **Věta 3c.1.**

Necht'  $n \in \mathbb{Z}$ ,  $a, b \in \mathbb{Z}_n$ . Číslo  $x_0 \in \mathbb{Z}$  řeší rovnici  $a \odot x = b$  v  $\mathbb{Z}_n$  právě tehdy, když  $x_0 \in \mathbb{Z}_n$  a  $ax_0 \equiv b \pmod{n}$ .

Platnost vyplývá z poznámky 2b.3, což ovšem není důkaz, tak ho uděláme.

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

1)  $\implies$ : Pokud  $x_0$  řeší  $a \odot x_0 = b$  v  $\mathbb{Z}_n$ , tak samozřejmě  $x_0 \in \mathbb{Z}_n$  a také  $ax_0 \bmod n = b$ . Protože  $b \in \mathbb{Z}_n$ , platí  $b = b \bmod n$ . Máme tedy  $ax_0 \bmod n = b \bmod n$ , proto podle věty 2a.1 platí  $ax_0 \equiv b \pmod{n}$ .

2)  $\impliedby$ : Předpoklady:  $x_0 \in \mathbb{Z}_n$  a  $ax_0 \equiv b \pmod{n}$ . Podle věty 2a.1 pak  $ax_0 \bmod n = b \bmod n = b$  díky  $b \in \mathbb{Z}_n$ . Máme tedy  $ax_0 \bmod n = b$ . Protože  $a, x_0 \in \mathbb{Z}_n$ , výraz nalevo lze interpretovat jako  $a \odot x_0$ . Proto  $a \odot x_0 = b$  a  $x_0$  je řešení dané rovnice. □

Z praktického pohledu to znamená následující:

- Množinu všech řešení rovnice  $a \odot x = b$  v  $\mathbb{Z}_n$  získáme tak, že z řešení kongruence  $ax \equiv b \pmod{n}$  vybereme ta, která jsou ze  $\mathbb{Z}_n$ .

Při práci s rovnicemi v  $\mathbb{Z}_n$  bývá zvykem ignorovat speciální značení pro operace a používat běžné značky pro násobení a sčítání. Budeme to zde dělat také, jen v důkazech budeme rozlišovat.

**! Příklad 3c.a:** Vyřešíme rovnici  $42x = 18$  v  $\mathbb{Z}_{180}$ .

Přepíšeme ji jako kongruenci  $42x \equiv 18 \pmod{180}$ , ze které pak přecházíme k diofantické rovnici  $42x + 180y = 18$ . Řešíme ji tradičně Euklidovým algoritmem, v tabulce nás zajímá jen pomocný sloupec pro  $x$ .

Dostáváme  $x_p = 39$ ,  $x_h = -30k$ , tedy kongruence  $42x \equiv 18 \pmod{180}$  má obecné řešení  $x = 39 - 30k$ ,  $k \in \mathbb{Z}$ .

Než začneme další postup, najdeme si lepšího zástupce. Nejmenší nezáporné číslo získatelné ze vzorce je 9, také změním znaménko u  $k$ . Budeme tedy pracovat s obecným řešením  $x = 9 + 30k$ ,  $k \in \mathbb{Z}$ .

Nyní potřebujeme najít všechna z těchto čísel, která leží v rozmezí 0 až 179. Jednoduchým přičítáním zjistíme, že jde o čísla 9, 39, 69, 99, 129, 159.

Závěr: Řešením rovnice  $42x = 18$  v  $\mathbb{Z}_{180}$  jsou  $x = 9, 39, 69, 99, 129, 159$ . Příznivci množin mohou napsat, že řešením jsou  $x \in \{9, 39, 69, 99, 129, 159\}$ .

Poznamenejme, že toto řešení šlo také napsat jako  $x = 9 + 30k$ ,  $k \in \{0, 1, \dots, 5\}$ , popřípadě jako  $x = 9 + 30k$ ,  $k = 0, 1, \dots, 5$ , popřípadě jako  $\{9 + 30k; 0 \leq k \leq 5\}$ . Tento zápis je výhodný pro případ, že je těch řešení hodně.

Pokud by chtěl někdo použít původní vzorec, musel by trochu přemýšlet a dospěl by k závěru, že řešením dané rovnice jsou  $x = 39 - 30k$ ,  $k \in \{-4, -3, \dots, 1\}$ .

△

**Poznámka:** Vraťme se znovu k obecnému řešení  $x = 39 + 30k$  pro kongruenci  $42x \equiv 18 \pmod{180}$ . Podle věty 3b.4 se tato množina řešení skládá z  $\gcd(42, 18) = 6$  různých zbytkových tříd modulo 180. Každá zbytková třída obsahuje jen jedno číslo z množiny  $\mathbb{Z}_{180} = \{0, 1, \dots, 179\}$ , takže bude jen 6 řešení původní rovnice v  $\mathbb{Z}_{180}$ . To souhlasí.

Věta nám také říká, že se k zástupcům zbytkových tříd dostaneme tak, že se od jednoho vybraného budeme posunovat o 30. Dostáváme tak  $\{9 + 180k; k \in \mathbb{Z}\}$ ,  $\{39 + 180k; k \in \mathbb{Z}\}$ ,  $\{69 + 180k; k \in \mathbb{Z}\}$ ,  $\{99 + 180k; k \in \mathbb{Z}\}$ ,  $\{129 + 180k; k \in \mathbb{Z}\}$  a  $\{159 + 180k; k \in \mathbb{Z}\}$ . Mimochodem, také vidíme, že další posun by nás dostal k číslu 189, které už patří do první zbytkové třídy.

△

Věta 3c.1 nám nejen dala návod na praktické počítání, ale také umožní převést teoretické poznatky, pomocí kterých potvrdíme pozorování z příkladu.

**! Věta 3c.2.**

Nechť  $n \in \mathbb{N}$ , uvažujme rovnici  $a \odot x = b$  v  $\mathbb{Z}_n$  pro nějaká  $a, b \in \mathbb{Z}_n$ .

(i) Jestliže  $\gcd(a, n)$  nedělí  $b$ , pak řešení rovnice neexistuje.

(ii) Jestliže  $\gcd(a, n)$  dělí  $b$ , pak má rovnice  $\gcd(a, n)$  řešení.

Nechť  $x_p \in \mathbb{Z}$  řeší kongruenci  $ax \equiv b \pmod{n}$ , označme  $\tilde{n} = \frac{n}{\gcd(a, n)}$ .

Nechť  $x_0 = x_p \bmod \tilde{n}$ . Pak množina všech řešení rovnice  $a \odot x = b$  v  $\mathbb{Z}_n$  je

$$\{x_0 + i\tilde{n}; i = 0, 1, \dots, \gcd(a, n) - 1\}.$$

**Důkaz (poučný):** (i): Použijeme nepřímý důkaz, tedy dokážeme obměnu této implikace.

Pokud by rovnice  $a \odot x = b$  měla řešení v  $\mathbb{Z}_n$ , tak by dle věty 3c.1 bylo i řešením pro kongruenci  $ax \equiv b \pmod{n}$ . Podle věty 3b.2 pak  $\gcd(a, n)$  musí dělit  $b$ .

(ii): Máme partikulární řešení  $x_p$  kongruence  $ax \equiv b \pmod{n}$  a  $x_0 = x_p \pmod{\tilde{n}}$ . Nechť  $k_0 \in \mathbb{Z}$  je takové, že  $x_0 = x_p - k_0\tilde{n}$ . Označme  $x_i = x_0 + i\tilde{n}$ .

1) Zvolme  $i \in \{0, \dots, \gcd(a, n) - 1\}$ . Ukážeme, že  $x_i \in \mathbb{Z}_n$ . Zjevně  $x_i \in \mathbb{Z}$ . Podle definice je  $x_0 \geq 0$ , proto díky  $\tilde{n}, i \geq 0$  také  $x_i \geq 0$ .

Coby zbytek  $x_0$  splňuje  $x_0 < \tilde{n}$  a  $i \leq \gcd(a, n) - 1$ , proto

$$x_0 + i\tilde{n} < \tilde{n} + (\gcd(a, n) - 1)\tilde{n} = \gcd(a, n)\tilde{n} = n.$$

Takže  $x_i \in \{0, \dots, n - 1\} = \mathbb{Z}_n$ .

2) Protože  $x_i = x_0 + i\tilde{n} = x_p + (i - k_0)\tilde{n}$  a  $i - k_0 \in \mathbb{Z}$ , podle věty 3b.2  $x_i$  řeší  $ax \equiv b \pmod{n}$ . Podle 1) je  $x_i \in \mathbb{Z}_n$  a proto podle věty 3c.1 řeší  $x_i$  rovnici  $a \odot x = b$  v  $\mathbb{Z}_n$ .

3) Ukážeme, že jiná řešení než  $x_i$  již neexistují.

Uvažujme řešení  $\tilde{x} \in \mathbb{Z}_n$  rovnice  $a \odot x = b$  v  $\mathbb{Z}_n$ . Pak musí řešit kongruenci  $ax \equiv b \pmod{n}$ . Z věty 3b.2 plyne, že tedy  $\tilde{x} = x_p + l\tilde{n}$  pro nějaké  $l \in \mathbb{Z}$ . Proto

$$\tilde{x} = x_p + l\tilde{n} = x_0 + k_0\tilde{n} + l\tilde{n} = x_0 + (l + k_0)\tilde{n} = x_0 + m\tilde{n},$$

kde  $m = l + k_0 \in \mathbb{Z}$ . Číslo  $\tilde{x}$  je tedy ve správném tvaru, zbývá dokázat, že  $m$  leží v rozsahu  $0, 1, \dots, \gcd(a, n) - 1$ .

Již jsme odvodili, že z volby  $x_0$  dostáváme  $x_0 < \tilde{n}$ . Pokud by  $m$  bylo záporné, tak bychom měli  $\tilde{x} \leq x_0 - \tilde{n} < 0$ , což je ve sporu s  $\tilde{x} \in \mathbb{Z}_n$ . Proto  $m \in \mathbb{N}_0$ .

Pokud by naopak platilo  $m \geq \gcd(a, n)$ , pak bychom měli

$$\tilde{x} = x_0 + m\tilde{n} \geq 0 + \gcd(a, n)\tilde{n} = n,$$

což je ve sporu s  $\tilde{x} \in \mathbb{Z}_n$ . Takže  $m \leq \gcd(a, n) - 1$ .

Shrnuto, řešení  $\tilde{x}$  lze zapsat jako  $x_0 + m\tilde{n}$ , kde  $m \in \{0, 1, \dots, \gcd(a, n) - 1\}$ , tedy  $\tilde{x}$  je mezi čísly  $x_i$ .

Ukázali jsme, že čísla  $x_i$  dávají všechna řešení dané rovnice a jde zjevně o  $\gcd(a, n)$  různých čísel. □

Postup opět shrneme.

### S Algoritmus 3c.3.

pro nalezení všech řešení rovnice  $ax = b$  v  $\mathbb{Z}_n$  Euklidovým algoritmem.

**0.** Sestavíme tabulku pro rozšířený Euklidův algoritmus se vstupními daty  $n, a$  a pomocným sloupcem s iniciačními hodnotami 0, 1.

**1.** Aplikujeme Euklidův rozšířený algoritmus.

**2.** Jestliže řádek ukazující  $\gcd(a, n)$  nelze vynásobit celým číslem tak, aby se místo  $\gcd(a, n)$  objevilo  $b$ , tak daná rovnice nemá řešení.

V opačném případě:

a) Do tabulky připišeme takto vynásobený řádek. Číslo v pomocném sloupci dává  $x_p$ .

b) V řádku začínajícím nulou najdeme v pomocném sloupci číslo, které v absolutní hodnotě dává  $\tilde{n}$ . Označíme  $x_0 = x_p \pmod{\tilde{n}}$ .

c) Řešení rovnice jsou  $x = x_0 + i\tilde{n}$ ,  $i \in \{0, 1, \dots, \gcd(a, n) - 1\}$ .

△

Jako obvykle není nutné sledovat přesně algoritmus. Je možné si nechat  $x_p$  a použít vzorec  $x = x_p + i\tilde{n}$ , ovšem s příslušně upraveným rozsahem pro  $i$ . Obvykle je to pak méně přehledné, takže se to spíš nedělá.

Pokud někdo potřebuje řešit takovéto rovnice ručně, pak by rád věděl, zda je možné krátit v rovnicích v  $\mathbb{Z}_n$ . Vzhledem k souvislosti s kongruencemi je jasné, že to nebude fungovat. Je možné krátit, pokud si rovnici  $ax = b$  v  $\mathbb{Z}_n$  přepíšeme na diofantickou rovnici  $ax + ny = b$ , ale pak je třeba mít na paměti, že ve zkrácené rovnici  $\tilde{a}x + \tilde{n}y = \tilde{b}$  už  $\gcd(\tilde{a}, \tilde{b})$  nedá počet řešení pro  $\mathbb{Z}_n$ . Kdo tomu rozumí, se s tím vyrovná.

**Příklad 3c.b:** Vyřešíme rovnici  $14x = 38$  v  $\mathbb{Z}_{40}$ .

Přeložíme ji jako  $14x + 40y = 38$  pro  $x, y \in \mathbb{Z}$ . Použijeme obvyklý algoritmus pro diofantické rovnice s tím, že ignorujeme  $y$ , a zkusíme záporné zbytky. Namísto  $\gcd(14, 40) = 2$  jsme dostali řádek s číslem  $-2$ , což nám nevadí, správnou pravou stranu 38 z něj vyrobit umíme. Máme  $x_p = 57$  a  $\tilde{n} = 20$ , najdeme  $x_0 = 57 \pmod{20} = 17$ .

Daná rovnice má dvě řešení, a to 17, 37.

	(x)
40	0
14	1
-2	-3
0	-20
38	57

Pokud nechceme použít přímo vzorce z věty či algoritmu, ale spíš souvislost s kongruencemi, můžeme postupovat takto: Z tabulky najdeme řešení  $x = 57 - 20k$ . Rozmyslíme si, že mezi těmito řešeními jsou ze  $\mathbb{Z}_{40}$  tato: 17, 37. Díky  $\gcd(14, 40) = 2$  víme, že jich máme správný počet. Osobně tento přístup preferuji.

Pokud bychom zkrátili jen v rovnici a řešili  $7x = 19$  v  $\mathbb{Z}_{40}$ , dostali bychom z Euklidovy tabulky  $\gcd(7, 40) = 1$ ,  $x_p = -323$ ,  $\tilde{n} = 40$  a  $x_0 = 37$ . Měli bychom jen jedno řešení  $x = 37$ . Nepomůže ani návrat ke kongruenci  $7x \equiv 19 \pmod{40}$ , ta má řešení  $x = -323 + 40k$ .

Když už chceme krátit, tak nejlépe v rovnici  $14x + 20y = 38$ . Vznikne  $7x + 10y = 19$ , což vede na  $x = 47 + 20k$ ,  $k \in \mathbb{Z}$ . Vidíme, že z této množiny leží v  $\mathbb{Z}_{40}$  čísla 17, 37, najdeme tedy dvě řešení a nenecháme se zmást tím, že  $\gcd(7, 10) = 1$ .

△

I v prostoru  $\mathbb{Z}_n$  platí analogie s lineárními prostory. Určitě pořád platí, že všechna řešení dané rovnice lze získat mechanismem  $x_0 + x_h$ . Poněkud komplikovanější je to s uzavřeností množiny řešení homogenní rovnice. Násobení skalárem totiž nefunguje kvůli omezení na čísla z  $\mathbb{Z}_n$ , takže počítat  $\alpha \cdot a$  pro  $a \in \mathbb{Z}_n$  a  $\alpha \in \mathbb{Z}$  nelze.

## Cvičení

**Cvičení 3c.1** (rutinní): Které z následujících rovnic jsou řešitelné v  $\mathbb{Z}_{168}$ ?

a)  $25x = 13$ ; b)  $30x = 12$ ; c)  $30x = 15$ ; d)  $16x = 24$ .

**Cvičení 3c.2** (rutinní, zkouškové): Vyřešte následující rovnice v daném  $\mathbb{Z}_n$ :

a)  $95x = 50$  v  $\mathbb{Z}_{220}$ ; c)  $10x = 0$  v  $\mathbb{Z}_{35}$ ; e)  $84x = 126$  v  $\mathbb{Z}_{210}$ ;  
b)  $9x = 13$  v  $\mathbb{Z}_{80}$ ; d)  $48x = 10$  v  $\mathbb{Z}_{120}$ ; f)  $8x = 0$  v  $\mathbb{Z}_{12}$ .

**Cvičení 3c.3** (dobré): Uvažujme rovnici  $(6 - t)x = 24$  v  $\mathbb{Z}_{40}$ . Pro které hodnoty  $t$  z rozmezí  $0, \dots, 5$  má tato rovnice

a) přesně čtyři řešení? b) přesně tři řešení? c) přesně pět řešení? d) žádné řešení?

## Řešení:

**3c.1:** Podmínka je  $\gcd(a, n) \mid b$ . a)  $\gcd(25, 168) = 1$ ,  $1 \mid 13$ , ano. b)  $\gcd(30, 168) = 6$ ,  $6 \mid 12$ , ano. c)  $\gcd(30, 168) = 6$ , neplatí  $6 \mid 15$ , ne. d)  $\gcd(16, 168) = 8$ ,  $8 \mid 24$ , ano.

**3c.2:** a) 

220	0
95	1
30	-2
5●	7●
0	-44
50	70

 Rovnice  $95x + 220y = 50$   
 $\gcd(95, 220) = 5 = 95 \cdot 7 + 220 \cdot (-3)$   
 $\rightarrow 50 = 95 \cdot 70 + 220 \cdot (-30) \rightarrow x_p = 70$   
 $95x + 220y = 0 \rightarrow 19x + 44y = 0 \rightarrow 19x = -44y \rightarrow x_h = 44k$   
Odtud  $x = 70 + 44k$ ,  $k \in \mathbb{Z}$ . Nebo to vykougáme z tabulky.  
Řešení ze  $\mathbb{Z}_{220}$ :  $x = 26 + 44k$ ,  $k = 0, \dots, 4$  neboli  $x = 26, 70, 114, 158, 202$ .

b) 

80	0
9	1
8	-8
1●	9●
0	-80
13	117

 Rovnice  $9x + 80y = 13$   
 $\gcd(9, 80) = 1 = 9 \cdot 9 + 80 \cdot (-1)$   
 $\rightarrow 13 = 9 \cdot 117 + 80 \cdot (-13) \rightarrow x_p = 117$   
 $9x + 80y = 0 \rightarrow 9x = -80y \rightarrow x_h = 80k$   
Odtud  $x = 117 + 80k$ ,  $k \in \mathbb{Z}$ . Nebo to vykougáme z tabulky.  
Řešení ze  $\mathbb{Z}_{80}$ :  $x = 37 + 80k$ ,  $k = 0$  neboli  $x = 37$ .

c)  $10x + 35y = 0$ , uhadneme  $\gcd(35, 10) = 5$ , vykrátíme na  $2x + 7y = 0$ , takže řešení  $x_h = 7k$ . Je  $\gcd(35, 10) = 5$  řešení v  $\mathbb{Z}_{35}$ ,  $x = 7k$  pro  $k = 0, 1, 2, 3, 4$  neboli  $x = 0, 7, 14, 21, 28$ .

d)  $\gcd(120, 48) = 24$ , protože 24 nedělí 10, rovnice nemá řešení.

e) 

210	0
84	1
42●	-2●
0	5
126	-6

 Rovnice  $84x + 210y = 126$   
 $\gcd(84, 210) = 42 = 84 \cdot (-2) + 210 \cdot 1$   
 $\rightarrow 126 = 84 \cdot (-6) + 210 \cdot 3 \rightarrow x_p = -6$   
 $84x + 210y = 0 \rightarrow 2x + 5y = 0 \rightarrow 2x = -5y \rightarrow x_h = 5k$   
Odtud  $x = -6 + 5k$ ,  $k \in \mathbb{Z}$ . Nebo to vykougáme z tabulky.

Řešení ze  $\mathbb{Z}_{210}$ :  $x = 4 + 5k$ ,  $k = 0, \dots, 41$  neboli  $x = 4, 9, 14, 19, \dots, 204, 209$ .

f)  $8x + 12y = 0$ , na  $2x + 3y = 0$ , takže  $x_h = 3k$ . Je  $\gcd(12, 8) = 4$  řešení v  $\mathbb{Z}_{12}$ ,  $x = 3k$  pro  $k = 0, 1, 2, 3$  neboli  $x = 0, 3, 6, 9$ .

**3c.3:** Počet řešení je roven  $\gcd(a, n)$ , ale musí platit  $\gcd(a, n) \mid b$ . a) Potřebujeme  $\gcd(6 - t, 40) = 4$ , splněno  $4 \mid 24$  pro existenci řešení. Potřebujeme  $4 \mid (6 - t)$ , to platí pro  $t = 2$ .

b) Potřebujeme  $\gcd(6 - t, 40) = 3$ , to není možné.

c) Potřebujeme  $\gcd(6 - t, 40) = 5$ , nastane pro  $t = 1$ , ale neplatí  $5 \mid 24$ , takže žádné řešení.

d) Žádné řešení nastane, když  $\gcd(6-t, 40)$  nedělí 24. Protože  $40 = 8 \cdot 5$  a  $6-t \leq 6$ , možná gcd jsou 2, 4, 5. Z nich jen 5 nedělí 24, u ostatních budou řešení. Závěr: Žádné řešení nebude pro  $t = 1$ .

### 3d. Soustavy lineárních kongruencí

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

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

Začneme lineární klasikou.



#### Věta 3d.1.

Uvažujme moduly  $n_1, n_2, \dots, n_m \in \mathbb{N}$  a čísla  $b_1, b_2, \dots, b_m \in \mathbb{Z}$ .

Nechť  $x_p$  je nějaké řešení soustavy kongruencí

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

Číslo  $x_0$  je také řešením této soustavy právě tehdy, pokud existuje číslo  $x_h$  takové, že  $x_0 = x_p + x_h$  a  $x_h$  je řešením přidružené homogenní soustavy kongruencí

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

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

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

! Ve cvičení 2a.6 jsme dokázali, že  $a \equiv 0 \pmod{n}$  právě tehdy, když  $n \mid a$ . To znamená, že číslo  $x \in \mathbb{Z}$  řeší homogenní soustavu

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

právě tehdy, když je  $x$  dělitelné všemi moduly  $n_1, \dots, n_m$ . To znamená, že  $x$  je jejich společným násobkem. Jak jsme si rozmysleli v kapitole 1b (viz například věta 1b.11), tato  $x$  lze vyjádřit jako  $x = k \operatorname{lcm}(n_1, n_2, \dots, n_m)$  pro  $k \in \mathbb{Z}$ .

Teď se omezíme na speciální případ, kdy jsou  $n_i$  po dvou nesoudělné, tedy pro  $i \neq j$  platí  $\gcd(n_i, n_j) = 1$ . Pak  $\operatorname{lcm}(n_1, \dots, n_m) = n_1 \cdot n_2 \cdots n_m$ , viz cvičení 1b.15, a pro homogenní soustavu získáme pěkné řešení.



#### Fakt 3d.2.

Uvažujme moduly  $n_1, n_2, \dots, n_m \in \mathbb{N}$ . Předpokládejme, že tato čísla jsou po dvou nesoudělná. Pak číslo  $x_h \in \mathbb{Z}$  splňuje kongruence  $x \equiv 0 \pmod{n_i}$  pro všechna  $i = 1, \dots, m$  právě tehdy, když je  $x_h$  násobkem čísla  $n_1 \cdot n_2 \cdots n_m$ .

Umíme tedy napsat obecné řešení  $x_h = n_1 \cdots n_m k$ ,  $k \in \mathbb{Z}$ .

Zbývá vymyslet, jak najít jedno partikulární řešení, což bude komplikovanější než v případě diofantických rovnic a lineárních kongruencí.

Začneme první kongruencí. Pokud ji  $x$  řeší, tak jistě musí mít tvar  $x = b_1 + kn_1$ . Teď potřebujeme zařídit, aby také splňovalo druhou kongruenci, tedy aby  $(b_1 + kn_1) \pmod{n_2} = b_2$ . K dosažení tohoto cíle máme k dispozici zatím neurčené  $k \in \mathbb{Z}$ , ale je to komplikováno tím, že se nám do toho plete to  $b_1$ .

Zajímavý nápad: Nepoužijeme  $b_1$ , ale  $b_1 \cdot \Phi$ , přičemž  $\Phi$  bude vypadat jako jednička z pohledu modula  $n_1$ , díky čemuž pořád máme  $x \equiv b_1 \pmod{n_1}$ , ale zároveň chceme, aby  $\Phi$  byla nula z pohledu modula  $n_2$ , čímž ten první

člen přestane zasahovat do našeho pokusu o řešení druhé kongruence. Pak ale musí být  $\Phi = x_1 n_2$ , přičemž chceme, aby  $x_1 n_2 \equiv 1 \pmod{n_1}$ . To je ale známý požadavek na inverzní číslo a umíme jej splnit.

Dostáváme tedy nového kandidáta na řešení  $x = b_1 x_1 n_2 + k n_1$ . Z pohledu modula  $n_1$  to je  $b_1 x_1 n_2 \equiv b_1 \cdot 1 = b_1$ , tedy první rovnice je stále splněna. Z pohledu modula  $n_2$  to je  $k n_1$ , což se doufejme dá doladit do hodnoty  $b_2$ . Protože je situace symetrická, nabízí se myšlenka, že by obě komponenty  $x$  mohly mít stejný tvar, takže bychom zkusili  $x = b_1 x_1 n_2 + b_2 x_2 n_1$ . Pro splnění tří kongruencí by pak byly tři komponenty a tak dále.

! Vyvineme tedy obecnou strategii, ukážeme ji na případu tří kongruencí. Pak budeme řešení sestavovat ze tří komponent  $C_1, C_2, C_3$ . Na každou komponentu máme tři požadavky, podle toho, z jakého pohledu se na ni díváme, shrnuje to tabulka vpravo. Když jednotlivé komponenty sečteme a podíváme se na výsledný součet očima jednoho modulu, tak vždy bude aktivní jen jeden člen a ostatní do toho nebudou zasahovat, což nám výrazně zjednoduší práci.

	$C_1$	$C_2$	$C_3$
$n_1$ :	$b_1$	0	0
$n_2$ :	0	$b_2$	0
$n_3$ :	0	0	$b_3$

To nezasahování neboli nuly v tabulce se vyrobí snadno. Aby  $C_1$  dalo nulu modulo  $n_2$  a  $n_3$ , musí být ve tvaru  $C_1 = k n_2 n_3$ , obdobně pro ostatní komponenty. Zbývá vyřešit požadavky na diagonále. Z praktického pohledu je jednodušší nechtít rovnou  $b_i$ , ale jen jedničky, protože z nich se správné hodnoty  $b_i$  vyrobí snadno vynásobením. Mám tedy následující požadavky:

	$x_1 n_2 n_3$	$x_2 n_1 n_3$	$x_3 n_1 n_2$
$n_1$ :	1	0	0
$n_2$ :	0	1	0
$n_3$ :	0	0	1

Abychom dostali jedničku vlevo nahoře, musí platit  $x_1(n_2 n_3) \equiv 1 \pmod{n_1}$ , což vlastně znamená, že  $x_1$  má být inverzní číslo k  $n_2 n_3$  modulo  $n_1$ . Díky vzájemné nesoudělnosti modulů existuje a umíme jej najít, obdobně pro  $x_2$  a  $x_3$ .

Komponenty  $b_1 x_1 n_2 n_3, b_2 x_2 n_1 n_3, b_3 x_3 n_1 n_2$  pak budou přesně splňovat požadavky první tabulky a jejich sečtením tak dostaneme řešení. Potvrdíme to v klíčové větě.

!

**Věta 3d.3.** (Čínská věta o zbytcích)

Nechť  $n_1, n_2, \dots, n_m \in \mathbb{N}$ ,  $b_1, b_2, \dots, b_m \in \mathbb{Z}$ . Uvažujme soustavu kongruencí

$$x \equiv b_1 \pmod{n_1}$$

$$x \equiv b_2 \pmod{n_2}$$

$$\vdots$$

$$x \equiv b_m \pmod{n_m}.$$

Jestliže jsou všechna čísla  $n_i$  po dvou nesoudělná, pak má tato soustava řešení  $x_p \in \mathbb{Z}$ . Obecné řešení je  $x = x_p + kn$ ,  $k \in \mathbb{Z}$ , kde  $n = n_1 n_2 \cdots n_m$ .

**Důkaz** (poučný): 1) Nejprve ukážeme, že řešení existuje. Pro  $i = 1, \dots, m$  definujeme  $N_i = \frac{n}{n_i}$ , tedy je to součin všech  $n_j$  s výjimkou  $n_i$ . Podle lemma 1b.27 pak  $\gcd(N_i, n_i) = 1$ . Proto existuje inverzní číslo  $x_i$  k  $N_i$  vzhledem k násobení modulo  $n_i$ . Nechť  $x_p = \sum_{i=1}^m b_i x_i N_i$ . Tvrdíme, že je to řešení dané soustavy.

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

2) Tvar množiny všech řešení vyplývá z věty 3d.1 a faktu 3d.2. □

Mnozí autoři namísto tvrzení o množině všech řešení preferují zakončit Čínskou větou o zbytcích prohlášením, že řešení soustavy je jediné modulo  $n$ . Jak bychom to ukázali?

Vezměme tedy ještě jiné řešení  $y$  soustavy. Snadno nahlédneme, že pak  $y - x_p$  řeší přidruženou homogenní soustavu, proto podle faktu 3d.2 máme  $y - x_p = kn$  pro nějaké  $k \in \mathbb{Z}$ . Pak  $y \equiv x_p \pmod{n}$ .

Důkaz věty dává algoritmus.

### S Algoritmus 3d.4.

pro řešení soustavy kongruencí  $x \equiv b_1 \pmod{n_1}, x \equiv b_2 \pmod{n_2}, \dots, x \equiv b_m \pmod{n_m}$  pro případ, že jsou všechna čísla  $n_i$  po dvou nesoudělná.

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

2. Pro každé  $i$  najdeme inverzní číslo  $x_i$  k  $N_i$  vzhledem k násobení modulo  $n_i$ , viz algoritmus 2a.13.

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

△

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

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

Přeloženo do moderního jazyka, hledáme řešení soustavy kongruencí  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$  a  $x \equiv 2 \pmod{7}$ . Ukážeme dvě podoby řešení.

Nejprve si zahrajeme na počítač a použijeme mechanicky příslušný algoritmus.

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

Teď pro každé  $i$  potřebujeme inverzní číslo k  $N_i$  vzhledem k násobení modulo  $n_i$ , tedy hledáme  $x_1, x_2, x_3$  splňující  $35x_1 \equiv 1 \pmod{3}$ ,  $21x_2 \equiv 1 \pmod{5}$ ,  $15x_3 \equiv 1 \pmod{7}$ .

3	0	5	0	7	0
35	1	21	1	15	1
3	0	5	0	7	0
2	1	1●	1●	1●	1●
1●	-1●	0		0	
0					

Dostáváme  $x_1 = -1$ ,  $x_2 = 1$ ,  $x_3 = 1$ . Pak  $x_p = 2 \cdot (-1) \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 23$ . Obecné řešení je  $x = 23 + 105k$ ,  $k \in \mathbb{Z}$ .

Při ručním výpočtu je možné si práci ulehčit například tím, že čísla nahrazujeme jejich příhodnějšími zástupci modulo, zejména při hledání  $x_i$ . Je potřeba vést v patrnosti, které modulo se při kterém výpočtu používá. Osobně preferuji přístup, který mi v tom pomáhá a který vychází ze znalosti hlavní myšlenky, spíše než následování hotového algoritmu. Pro každou komponentu si vyrobím sloupec, ve kterém se pracuje v tom modulu, který je dotyčnou komponentou obsluhován. Proto jsem si do záhlaví přidal poznámku, kterou kongruenci dotyčná komponenta řeší.

$$\begin{array}{l}
 x_p: \left| \begin{array}{l} \underline{x \equiv 2 \pmod{3}} \\ 2 \cdot x_1 \cdot 5 \cdot 7 \\ 35x_1 \equiv 1 \pmod{3} \\ -1 \cdot x_1 \equiv 1 \pmod{3} \\ x_1 = -1 \end{array} \right| \left| \begin{array}{l} \underline{x \equiv 3 \pmod{5}} \\ 3 \cdot x_2 \cdot 3 \cdot 7 \\ 21x_2 \equiv 1 \pmod{5} \\ 1x_2 \equiv 1 \pmod{5} \\ x_2 = 1 \end{array} \right| \left| \begin{array}{l} \underline{x \equiv 2 \pmod{7}} \\ 2 \cdot x_3 \cdot 3 \cdot 5 \\ 15x_3 \equiv 1 \pmod{7} \\ 1x_3 \equiv 1 \pmod{7} \\ x_3 = 1 \end{array} \right| \text{ protože } 35 \equiv -1 \pmod{3} \text{ atd.} \\
 x_p = 2 \cdot (-1) \cdot 5 \cdot 7 + 3 \cdot 1 \cdot 3 \cdot 7 + 2 \cdot 1 \cdot 3 \cdot 5 = -70 + 63 + 30 = 23.
 \end{array}$$

Dostáváme řešení  $x = 23 + 105k$ ,  $k \in \mathbb{Z}$ .

Vzhledem k tomu, že jde o počty věcí, bychom mohli chtít  $x \geq 0$  a tedy  $k \in \mathbb{N}_0$ .

△

Postup je krásně algoritmizovatelný, podprogram pro hledání inverzních čísel se dá dokonce volat paralelně. Výpočetní čas pak příliš nenarůstá s množstvím kongruencí v soustavě.

Nabízejí se i další zkratky, například můžeme nahrazovat také v kongruencích.

**Příklad 3d.b:** Vyřešíme soustavu  $x \equiv 8 \pmod{5}$ ,  $x \equiv -1 \pmod{6}$  a  $x \equiv 14 \pmod{7}$ .

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

Začneme tím, že zjednodušíme kongruence, každou podle příslušného modula. Budeme tedy namísto té zadané řešit soustavu  $x \equiv 3 \pmod{5}$ ,  $x \equiv -1 \pmod{6}$  a  $x \equiv 0 \pmod{7}$ .

Teď také vidíme další zjednodušení, třetí člen v řešení se násobí nulou, tedy vůbec jej nemusíme vytvářet. Ale z cvičných důvodů to také uděláme.

$$\begin{array}{l}
 x_p: \left| \begin{array}{l} \underline{x \equiv 3 \pmod{5}} \\ 3 \cdot x_1 \cdot 6 \cdot 7 \\ 42x_1 \equiv 1 \pmod{5} \\ 2x_1 \equiv 1 \pmod{5} \\ x_1 = 3 \end{array} \right| \left| \begin{array}{l} \underline{x \equiv -1 \pmod{6}} \\ -1 \cdot x_2 \cdot 5 \cdot 7 \\ 35x_2 \equiv 1 \pmod{6} \\ -x_2 \equiv 1 \pmod{6} \\ x_2 = -1 \end{array} \right| \left| \begin{array}{l} \underline{x \equiv 0 \pmod{7}} \\ 0 \cdot x_3 \cdot 5 \cdot 6 \\ 30x_3 \equiv 1 \pmod{7} \\ 2x_3 \equiv 1 \pmod{7} \\ x_3 = 4 \end{array} \right| \\
 x_p = 3 \cdot 42 \cdot 3 + (-1) \cdot 35 \cdot (-1) + 0 = 378 + 35 = 413
 \end{array}$$

Inverze  $x_i$  jsme uhádli, to je často možné, v případě nouze si bokem uděláme tabulky pro rozšířený Euklidův algoritmus. Máme také  $n = 5 \cdot 6 \cdot 7 = 210$ . Dostáváme obecné řešení  $x = 413 + 210k$  pro  $k \in \mathbb{Z}$ .

Někdo by preferoval lepšího reprezentanta  $413 - 210 = 203$  a dostal obecné řešení  $203 + 210k$ ,  $k \in \mathbb{Z}$ .

V postupu jsou ještě dvě místa, kde se dá ušetřit práce. Často je v zásadě jedno, jestli pro  $x_i$  volíme kladné či záporné číslo, například u  $x_3$  se nabízejí 4 a  $-3$ , přičemž mezi násobením trojkou a čtyřkou zas není takový rozdíl.

Můžeme pak ovlivnit, jestli se jednotlivé členy, ze kterých skládáme  $x_p$ , nasčítají do velkého čísla, nebo se budou vzájemně krátit.

Další prostor pro zjednodušení nám nabízí fáze formování členů. My jsme si do prvního přidávali  $6 \cdot 7$ , abychom zajistili vynulování vůči modulům 6 a 7. Jenže pravá strana první kongruence už dodala trojku, stačí tedy dodat jen 2 a 7, tedy pracovat pracovat se členem  $3 \cdot x_1 \cdot 2 \cdot 7$ . Máme pak požadavek  $14x_1 \equiv 1 \pmod{5}$ . Z tohoto pohledu se může vyplatit přepis druhé kongruence do tvaru  $x \equiv 5 \pmod{6}$ , protože pak druhý člen nemusí být  $5 \cdot x_2 \cdot 5 \cdot 7$ , ale stačí  $5 \cdot x_2 \cdot 7$ , kde  $7x_2 \equiv 1 \pmod{6}$ . Na druhou stranu pak mohou vyjít méně příjemné úlohy na inverzní čísla, takže je otázkou, zda se toto kouzlení vyplatí. Počítač to nemá zapotřebí.

△

Čínská věta o zbytcích má mnoho praktických aplikací. Může například pomoci s urychlením výpočtů v  $\mathbb{Z}_n$ , když je  $n$  velké a složené, viz sekce 3e. Určitě patří do základního arsenálu computer science.

Tuto sekci uzavřeme zamyšlením nad obecnějšími podobami soustav kongruencí.

Když člověk slyší „soustavy lineárních kongruencí“, čekal by spíš rovnice typu  $a_i x \equiv b_i \pmod{n_i}$ . Zavedení násobků  $a_i$  ovšem skokově zvýší náročnost. Dobrá zpráva je, že pořád platí obdoba hlavní strukturální věty 3d.1, ale u věty o homogenních řešeních se to začne komplikovat. Kongruence  $ax \equiv 0 \pmod{n}$  totiž nemá obecné řešení  $x = nk$ , ale  $x = \frac{n}{\gcd(a,n)}k$ . Pro homogenní soustavy s po dvou nesoudělnými moduly  $n_i$  pak dostáváme obecné řešení ve tvaru

$$x = \frac{n_1}{\gcd(a_1, n_1)} \cdot \frac{n_2}{\gcd(a_2, n_2)} \cdots \frac{n_m}{\gcd(a_m, n_m)} k, \quad k \in \mathbb{Z}.$$

V případě obecném, tedy když jsou některá  $n_i$  soudělná, se místo součinu bere největší společný násobek těchto podílů.

To byla ta lepší část. Špatná zpráva je, že pro soustavy kongruencí  $a_i x_i \equiv b_i \pmod{b_i}$  není praktický (pro počítač) způsob, jak najít partikulární řešení  $x_p$ , dokonce ani není praktický test pro rozpoznání řešitelných soustav, a to ani pro po dvou nesoudělné moduly  $n_i$ . Naštěstí se takovéto obecné soustavy v aplikacích tolik nevyskytují.

Abychom to jen tak neodbyli, ukážeme univerzální metodu pozitivní pro menší soustavy a ruční výpočet.

### Příklad 3d.c (Eliminace pro soustavy lineárních kongruencí):

Standardní eliminace funguje následovně: Z první rovnice vyjádříme první proměnnou a dosadíme do ostatních proměnných, první rovnici pak škrtneme ze seznamu. Pokud zbylo více rovnic, pokračujeme dále. Něco podobného funguje pro soustavy kongruencí s jednou neznámou.

Vraťme se k příkladu 3d.a neboli soustavě  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$  a  $x \equiv 2 \pmod{7}$ .

Její řešení  $x$  musí splňovat první kongruenci. Úloha  $x \equiv 2 \pmod{3}$  vede na obecné řešení  $x = 2 + 3k$ ,  $k \in \mathbb{Z}$ . Dosadíme do zbývajících dvou kongruencí:

$$\begin{aligned} 2 + 3k &\equiv 3 \pmod{5} && \iff && 3k &\equiv 1 \pmod{5} \\ 2 + 3k &\equiv 2 \pmod{7} && && 3k &\equiv 0 \pmod{7} \end{aligned}$$

Dostáváme soustavu, která už nemá u neznámé  $k$  jedničky, ale to nevadí, stejně nechceme použít čínský algoritmus. Vyřešíme první kongruenci obvyklým způsobem, dostaneme  $k = 2 + 5l$  pro  $l \in \mathbb{Z}$ . Dosadíme do třetí kongruence:

$$3(2 + 5l) \equiv 0 \pmod{7} \iff 15l \equiv -6 \pmod{7} \iff 1 \cdot l \equiv 1 \pmod{7}.$$

Ta poslední kongruence má řešení  $l = 1 + 7m$  pro  $m \in \mathbb{Z}$ . Teď provedeme zpětnou substituci:

$$x = 2 + 3k = 2 + 3(2 + 5l) = 8 + 15l = 8 + 15(1 + 7m) = 23 + 105m, \quad m \in \mathbb{Z}.$$

Dospěli jsme ke stejnému výsledku.

△

Jakýmsi mezistupněm jsou soustavy, ve kterých  $a_i = 1$ , ale moduly nemusí být po dvou nesoudělné. Pro ty pořád nemáme tak příjemný postup řešení jako v případě nesoudělnosti, ale alespoň umíme rozeznat řešitelné soustavy.

#### Věta 3d.5.

Nechť  $n_1, n_2, \dots, n_m \in \mathbb{N}$ ,  $b_1, b_2, \dots, b_m \in \mathbb{Z}$ . Soustava kongruencí

$$x \equiv b_1 \pmod{n_1},$$

$$x \equiv b_2 \pmod{n_2},$$

⋮

$$x \equiv b_m \pmod{n_m}.$$

má řešení právě tehdy, jestliže pro všechna  $i, j \in \{1, \dots, m\}$ ,  $i \neq j$  platí že  $\gcd(n_i, n_j)$  dělí  $b_i - b_j$ .

Již jsme si rozmysleli, že řešení takové soustavy jsou jednoznačná modulo  $\text{lcm}(n_1, \dots, n_m)$ . I pro tyto soustavy funguje univerzální eliminační metoda, ale existuje i alternativní postup, který opět ukážeme na příkladě.

**Příklad 3d.d** (Rozklad modula pro soustavy lineárních kongruencí):

Uvažujme soustavu  $x \equiv 2 \pmod{24}$ ,  $x \equiv 6 \pmod{20}$  a  $x \equiv 26 \pmod{30}$ .

Test:  $\text{gcd}(24, 20) = 4$  dělí  $2 - 6$ ,  $\text{gcd}(24, 30) = 6$  dělí  $2 - 26$ ,  $\text{gcd}(20, 30) = 10$  dělí  $6 - 26$ . Tato soustava má řešení.

Krok 1: Všechny moduly rozložíme na mocniny prvočísel, pak každou kongruenci přepíšeme pomocí lemma 2a.18.

$$\begin{aligned} x \equiv 2 \pmod{2^3 \cdot 3} &\iff \begin{cases} x \equiv 2 \pmod{2^3} \\ x \equiv 2 \pmod{3} \end{cases} \\ x \equiv 6 \pmod{2^2 \cdot 5} &\iff \begin{cases} x \equiv 6 \pmod{2^2} \\ x \equiv 6 \pmod{5} \end{cases} \\ x \equiv 26 \pmod{2 \cdot 3 \cdot 5} &\iff \begin{cases} x \equiv 26 \pmod{2} \\ x \equiv 26 \pmod{3} \\ x \equiv 26 \pmod{5} \end{cases} \end{aligned}$$

Původní soustava tří kongruencí je tedy ekvivalentní soustavě sedmi kongruencí.

Krok 2: Nyní je třeba konsolidovat kongruence se stejným prvočíslem v základu mocniny, postupujeme od nejvyšší mocniny. Máme tři kongruence s modulem založeným na dvojce. Aby platilo  $x \equiv 2 \pmod{2^3}$ , musí být  $x = 2 + 8k$  pro  $k \in \mathbb{Z}$ . Pak ale  $x = 2 + 4 \cdot (2k) \equiv 2 + 0 \equiv 6 \pmod{2^2}$ , tato  $x$  tedy splňuje i druhou kongruenci. Podobně  $x = 2 + 2 \cdot (4k) \equiv 2 + 0 \equiv 26 \pmod{2}$  a splňuje i třetí kongruenci. Vidíme, že první tři kongruence lze nahradit kongruencí  $x \equiv 2 \pmod{2^3}$ .

Nyní se podíváme na kongruence s modulem 3. Jsou dvě, ale  $26 \equiv 2 \pmod{3}$ , čili vlastně jde o tutéž kongruenci. Vezmeme si dále jednu z nich.

Nakonec zpracujeme kongruence s pětkovým modulem. Hledaná  $x$  mají splňovat  $x \equiv 6 \pmod{5}$  a  $x \equiv 26 \pmod{5}$ , což je díky  $6 \equiv 26 \pmod{5}$  totéž a tedy jde zase o jednu kongruenci.

Závěr: Daná soustava, kterou jsme převedli na 7 kongruencí, se dá rovnocenně nahradit soustavou  $x \equiv 2 \pmod{8}$ ,  $x \equiv 2 \pmod{3}$ ,  $x \equiv 6 \pmod{5}$ . Zde jsou již moduly po dvou nesoudělné, tudíž aplikujeme standardní algoritmus a najdeme obecné řešení  $x = 26 + 120k$ ,  $k \in \mathbb{Z}$ .

Uvažujme nyní modifikaci, kdy třetí kongruenci nahradíme kongruencí  $x \equiv 8 \pmod{30}$ . Pak třetí podmínka testu existence selže, protože  $\text{gcd}(20, 30) = 10$  nedělí  $2 - 8$ . Jak by se to odrazilo na postupu?

Čtenář snadno ověří, že konsolidace pro mocniny dvojky a trojku by po náhradě  $26 \mapsto 8$  proběhla stejně. Při pokusu o konsolidaci kongruencí s modulem 5 bychom ale měli kongruence  $x \equiv 6$  a  $x \equiv 8$ , které jsou navzájem ve sporu, protože  $6 \not\equiv 8 \pmod{5}$ . Tím bychom rozpoznali, že soustava nemá řešení.

△

**Poznámka:** Pro úplnost: Jak by si s tímto příkladem poradila eliminace?

$$\begin{array}{lclcl} x \equiv 2 \pmod{24} & \longrightarrow & x = 2 + 24k & & \\ x \equiv 6 \pmod{20} & & & \longrightarrow & 2 + 24k \equiv 6 \pmod{20} & \longrightarrow & 24k \equiv 4 \pmod{20} \\ x \equiv 26 \pmod{30} & & & \longrightarrow & 2 + 24k \equiv 26 \pmod{30} & \longrightarrow & 24k \equiv 24 \pmod{30} \end{array}$$

Z první rovnice nové soustavy  $k = 1 + 5l$ ,  $l \in \mathbb{Z}$ . Po dosazení do druhé rovnice získáme  $24 + 120l \equiv 24 \pmod{30}$  neboli  $120l \equiv 0 \pmod{30}$ . To platí pro všechna  $l \in \mathbb{Z}$ . Zpětnou substitucí pak

$$x = 2 + 24k = 2 + 24(1 + 5l) = 26 + 120l, \quad l \in \mathbb{Z}.$$

Nyní budeme řešit soustavu s nahrazenou třetí rovnicí.

$$\begin{array}{lclcl} x \equiv 2 \pmod{24} & \longrightarrow & x = 2 + 24k & & \\ x \equiv 6 \pmod{20} & & & \longrightarrow & 2 + 24k \equiv 6 \pmod{20} & \longrightarrow & 24k \equiv 4 \pmod{20} \\ x \equiv 8 \pmod{30} & & & \longrightarrow & 2 + 24k \equiv 8 \pmod{30} & \longrightarrow & 24k \equiv 14 \pmod{30} \end{array}$$

Z první rovnice nové soustavy  $k = 1 + 5l$ ,  $l \in \mathbb{Z}$ . Po dosazení do druhé rovnice získáme  $24 + 120l \equiv 14 \pmod{30}$  neboli  $120l \equiv 20 \pmod{30}$ . Protože  $120 \equiv 30$ , jde o rovnici  $0x \equiv 20 \pmod{30}$ , která nemá řešení, protože pro libovolné  $x \in \mathbb{Z}$  je  $0x = 0$ , ale neplatí  $0 \equiv 20 \pmod{30}$ .

△

## Cvičení

**Cvičení 3d.1** (rutinní, zkouškové): Vyřešte následující soustavy kongruencí:

$$\begin{array}{llll} \text{a) } x \equiv 0 \pmod{3} & \text{b) } x \equiv 4 \pmod{2} & \text{c) } x \equiv 1 \pmod{7} & \text{d) } x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{4} & x \equiv -4 \pmod{3} & x \equiv 0 \pmod{9} & x \equiv 4 \pmod{4} \\ x \equiv 2 \pmod{5}; & x \equiv 4 \pmod{5}; & x \equiv -1 \pmod{11}; & x \equiv 5 \pmod{3}. \end{array}$$

**Řešení:**

**3d.1:** a)  $n = 60$ ,  $N_1 = 20$ , inverze v  $\mathbb{Z}_3$  je  $x_1 = -1$ ;  $N_2 = 15$ , inverze v  $\mathbb{Z}_4$  je  $x_2 = -1$ ;  $N_3 = 12$ , inverze v  $\mathbb{Z}_5$  je  $x_3 = -2$ .  $x = 0 \cdot 20 \cdot (-1) + 1 \cdot 15 \cdot (-1) + 2 \cdot 12 \cdot (-2) = -63 \equiv 57 \pmod{60}$ . Řešení jsou  $x = 60k - 63$  nebo třeba  $57 + 60k$  pro  $k \in \mathbb{Z}$ .

b)  $n = 30$ ,  $N_1 = 15$ , inverze v  $\mathbb{Z}_2$  je  $x_1 = 1$ ;  $N_2 = 10$ , inverze v  $\mathbb{Z}_3$  je  $x_2 = 1$ ;  $N_3 = 6$ , inverze v  $\mathbb{Z}_5$  je  $x_3 = 1$ .  $x = 4 \cdot 15 \cdot 1 + (-4) \cdot 10 \cdot 1 + 4 \cdot 6 \cdot 1 = 44 \equiv 14 \pmod{30}$ . Řešení jsou  $x = 44 + 30k$  nebo třeba  $14 + 30k$  pro  $k \in \mathbb{Z}$ .

c)  $n = 693$ ,  $N_1 = 99$ , inverze v  $\mathbb{Z}_7$  je  $x_1 = 1$ ;  $N_2 = 77$ , inverze v  $\mathbb{Z}_9$  je  $x_2 = 2$ ;  $N_3 = 63$ , inverze v  $\mathbb{Z}_{11}$  je  $x_3 = -4$ .  $x = 1 \cdot 99 \cdot 1 + 0 \cdot 77 \cdot 2 + (-1) \cdot 63 \cdot (-4) = 351$ . Řešení jsou  $x = 351 + 693k$  pro  $k \in \mathbb{Z}$ .

d) Přepis na  $x \equiv 3 \pmod{5}$ ,  $x \equiv 0 \pmod{4}$ ,  $x \equiv 2 \pmod{3}$ .  $n = 60$ ,  $N_1 = 12$ , inverze v  $\mathbb{Z}_5$  je  $x_1 = 3$ ;  $N_2$  netřeba řešit;  $N_3 = 20$ , inverze v  $\mathbb{Z}_3$  je  $x_3 = 2$ .  $x = 3 \cdot 12 \cdot 3 + 0 + 2 \cdot 20 \cdot 2 = 188$ . Řešení jsou  $x = 188 + 60k$  nebo třeba  $x = 8 + 60k$  pro  $k \in \mathbb{Z}$ .

### 3e. Bonus: Výpočty modulo po částech

Nechť  $n \in \mathbb{N}$  je zvolený modul, pro který máme rozklad  $n = pq$  na dva nesoudělné faktory. Uvažujme nějaký algebraický výraz  $b$ , o kterém si myslíme, že má modulo  $n$  hodnotu  $x$ . Máme ověřit  $x \equiv b \pmod{n}$ , což ale pro hodně velké  $n$  může být problém. Naštěstí nám lemma 2a.17 umožňuje tuto kongruenci testovat „po částech“ (per partes), tedy stačí ověřit  $x \equiv b \pmod{p}$  a  $x \equiv b \pmod{q}$ . To jistě ušetří práci, ale kde toho kandidáta  $x$  vezmeme? Mohli bychom vypočítat hodnotu  $b$  v kongruenci modulo  $n$ , ale do toho se nám právě nechce.

**Příklad 3e.a:** Spočítáme  $40^{141}$  modulo  $n = 91$ .

Protože  $n = 91$  není prvočíslo, malá Fermatova věta nepomůže. Pokročilí čtenáři si připomněli obecnější Eulerovu větu, která je zde aplikovatelná, protože  $\gcd(40, 91) = 1$ . Pracuje s funkcí  $\varphi(91) = \varphi(7)\varphi(13) = 6 \cdot 12 = 72$  a dovoluje nám redukovat

$$40^{143} = 40^{72+69} = 40^{72}40^{69} \equiv 1 \cdot 40^{69} = 40^{69} \pmod{91}.$$

Víc nám Eulerova věta nepomůže, mocninu  $40^{69}$  bychom museli spočítat například pomocí redukce exponentu, což se nám taky příliš nechce.

Vyzkoušíme proto přístup po částech, což je pro rozklad  $91 = 7 \cdot 13$  na dva nesoudělné faktory možné. Hledáme výsledek  $x$  splňující  $x \equiv 40^{141} \pmod{91}$ , což znamená  $x \equiv 40^{141} \pmod{7}$  a  $x \equiv 40^{141} \pmod{13}$ . Zjistíme, čemu se v příslušných světech modulo rovnají pravé strany, díky prvočíselnosti složek můžeme použít malou Fermatovu větu. Dostáváme:

$$\begin{aligned} p = 7: b_1 &= 40^{141} \equiv 5^{141} = 5^{23 \cdot 6 + 3} = (5^6)^{23}5^3 \equiv 1^{23}5^3 \\ &= 5 \cdot 5^2 = 5 \cdot 25 \equiv 5 \cdot 4 = 20 \equiv -1 \pmod{7}; \end{aligned}$$

$$q = 13: b_2 = 40^{141} \equiv 1^{141} = 1 \pmod{13}.$$

Naše  $x$  tedy musí splňovat  $x \equiv -1 \pmod{7}$  a  $x \equiv 1 \pmod{13}$ . Tuto soustavu vyřešíme postupem dle věty 3d.3.

$$x_p: \left| \begin{array}{l} x \equiv -1 \pmod{7} \\ (-1) \cdot x_1 \cdot 13 \\ 13x_1 \equiv 1 \pmod{7} \\ -1 \cdot x_1 \equiv 1 \pmod{7} \\ x_1 = -1 \end{array} \right| \left| \begin{array}{l} x \equiv 1 \pmod{13} \\ 1 \cdot x_2 \cdot 7 \\ 7x_2 \equiv 1 \pmod{13} \\ x_2 = 2 \end{array} \right| = 13 + 14 = 27$$

Mimočodem inverzní číslo k 7 modulo 13 jsme našli zkusmo. Kdyby nevyšla pěkná malá čísla, použili bychom Euklidův algoritmus.

Každopádně jsme našli  $x = 27 + 91k$ ,  $k \in \mathbb{Z}$ . Platí tedy  $40^{141} \equiv 27 \pmod{91}$ .

△

Tento postup je možné použít pro libovolný výpočet a také pro rozklad  $n$  na více faktorů. Dokáže významným způsobem zrychlit operace, zejména pokud dokážeme všechny výpočty vzhledem k jednotlivým faktorům provádět paralelně.

**S Algoritmus 3e.1.**

pro výpočet modulo po částech.

**0.** Je dán algebraický výraz  $v$  a modul  $n \in \mathbb{N}$ .

**1.** Najdeme rozklad  $n = n_1 \cdots n_m$ , kde  $n_1, \dots, n_m$  jsou po dvou nesoudělná přirozená čísla.

**2.** Pro každé  $i$  spočítáme výraz  $v$  modulo  $n_i$ , tedy najdeme  $b_i \in \mathbb{Z}$  takové, aby  $v \equiv b_i \pmod{n_i}$ .

**3.** Vyřešíme soustavu kongruencí  $x \equiv b_1 \pmod{n_1}, \dots, x \equiv b_m \pmod{n_m}$ .

Řešení  $x \in \mathbb{Z}$  splňuje  $v \equiv x \pmod{n}$ .

△

**Příklad 3e.b:** Vyhodnotíme  $23 \cdot 26^{12} + 782$  modulo  $n = 715 = 5 \cdot 11 \cdot 13$ .

Protože jsou faktory 5, 11, 13 po dvou nesoudělné, můžeme počítat po částech. Nejprve vyhodnotíme výraz:

$$n_1 = 5 : b_1 = 23 \cdot 26^{12} + 782 \equiv 3 \cdot 1^{12} + 2 = 5 \equiv 0 \pmod{5};$$

$$\begin{aligned} n_2 = 11 : b_2 &= 23 \cdot 26^{12} + 782 \equiv 1 \cdot 4^{10+2} + 12 = 4^{11-1} 4^2 + 12 \\ &\equiv 1 \cdot 4^2 + 1 = 16 + 1 = 17 \equiv 6 \pmod{11}; \end{aligned}$$

$$n_3 = 13 : b_3 = 23 \cdot 26^{12} + 782 \equiv 10 \cdot 0^{12} + 2 = 2 \pmod{13}.$$

Nyní vyřešíme soustavy kongruencí:

$$x_p : \left| \begin{array}{l} x \equiv 0 \pmod{5} \\ 0 \cdot x_1 \cdot 11 \cdot 13 \\ 143x_1 \equiv 1 \pmod{5} \\ 3x_1 \equiv 1 \pmod{5} \\ x_1 = 2 \\ 0 \cdot 2 \cdot 11 \cdot 13 \end{array} \right| \left| \begin{array}{l} x \equiv 6 \pmod{11} \\ 6 \cdot x_2 \cdot 5 \cdot 13 \\ 65x_2 \equiv 1 \pmod{11} \\ -x_2 \equiv 1 \pmod{11} \\ x_2 = -1 \\ +6 \cdot (-1) \cdot 5 \cdot 13 \end{array} \right| \left| \begin{array}{l} x \equiv 2 \pmod{13} \\ 2 \cdot x_3 \cdot 5 \cdot 11 \\ 55x_3 \equiv 1 \pmod{13} \\ 3x_3 \equiv 1 \pmod{13} \\ x_3 = 9 \\ +2 \cdot 9 \cdot 5 \cdot 11 \end{array} \right| = 0 - 390 + 990 = 600$$

Dostáváme  $23 \cdot 26^{12} + 782 \equiv 600 \pmod{715}$ .

Dobrovolníci na potvrzení správnosti přímým ručním výpočtem se stále ještě hledají, já jsem zbaběle použil Maple a souhlasí to.

△

Aby tato kapitola nebyla tak krátká, všimneme si zajímavé věci. V obou příkladech jsme měli výrazy, v nichž vystupovala rozličná čísla. My jsme hodnoty těchto výrazů zjistili výpočty, ve kterých se každé číslo účastnilo pouze svými zástupci vůči jednotlivým faktorům modulu a tato informace již stačila. Třeba v prvním příkladu bylo u čísla 40 použito jen  $40 \bmod 7 = 5$  a  $40 \bmod 13 = 1$  a s těmito částečnými informacemi jsme pak paralelně počítali.

Čtenáři to může připomenout situaci s vektory, kdy například síly vyjádříme pomocí složek a pak s nimi počítáme po složkách.

**Příklad 3e.c:** Uvažujme modulo  $n = 40 = 5 \cdot 8$ . Mějme čísla  $a = 13$  a  $b = 23$ . Víme, že ve světě modulo  $n$  tato čísla zastupují zbytkové třídy  $[13]_{40}$  a  $[23]_{40}$ .

Pokud je naše představa správná, tak by tyto dvě třídy měly být jednoznačně určené pomocí „vektorů“, které budeme značit pomocí  $v$ :

$$v(a) = (a \bmod 5, a \bmod 8) = (13 \bmod 5, 13 \bmod 8) = (3, 5);$$

$$v(b) = (b \bmod 5, b \bmod 8) = (23 \bmod 5, 23 \bmod 8) = (3, 7).$$

Pokud vektory sečteme, dostaneme  $v(a) + v(b) = (3+3, 5+7) = (6, 12)$ . Protože v kódujících vektorech očekáváme zbytky, přejdeme k příslušným zástupcům:  $v(a) + v(b) \equiv (1, 4)$ . Vlastně tedy při práci s vektory používáme sčítání z prostorů  $\mathbb{Z}_5$  a  $\mathbb{Z}_8$ ,  $v(a) + v(b) = (3 \oplus 3, 5 \oplus 7)$ .

My ovšem víme, že  $13 + 23 = 36$ . Jakému vektoru to odpovídá?

$$v(36) = (36 \bmod 5, 36 \bmod 8) = (1, 4).$$

Takže sčítání skutečné a sčítání ve formě vektorů vedlo na stejný výsledek.

Zkusíme násobení. Jak ukazují příklady výše, při násobení dvou čísel násobíme v jednotlivých modulech, takže zavedeme speciální násobení vektorů, které funguje podobně jako sčítání, tedy po složkách. Bude to opět násobení  $\odot$ . Vyzkoušíme:

$$v(a) \odot v(b) = (3, 5) \odot (3, 7) = (3 \odot 3, 5 \odot 7) = (4, 3).$$

Správný výsledek je  $13 \cdot 23 = 299$  a je dán vektorem

$$v(299) = (299 \bmod 5, 299 \bmod 8) = (4, 3).$$

Opět to souhlasí. Ovšem finta je v tom, že si chceme to násobení ušetřit, takže bychom se spíš chtěli od vektoru  $(4, 3)$  dostat k výsledku 299 či jeho jinému zástupci modulo 40. Hledáme tedy  $x \in \mathbb{Z}$  splňující  $v(x) = (4, 3)$ . To ale znamená  $x \equiv 4 \pmod{5}$  a  $x \equiv 4 \pmod{8}$ , tedy je to zase úloha pro čínskou větu.

△

Pozorování z příkladu lze potvrdit důkazy. Jmenovitě:

Uvažujme modul  $n = n_1 \cdots n_m$ , kde  $n_i$  jsou po dvou nesoudělné. Pro každé  $a \in \mathbb{Z}$  definujeme

$$v(a) = (a \bmod n_1, \dots, a \bmod n_m).$$

Pak platí následující:

- Pro každé  $a \in \mathbb{Z}$  je  $v(a) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ .
- Pro každý vektor  $\vec{v} \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$  existuje  $a \in \mathbb{Z}$  takové, že  $v(a) = \vec{v}$ , a lze jej nalézt algoritmem podle čínské věty.
- Zbytkové třídy v  $\mathbb{Z}$  modulo  $n$  jsou jednoznačně určeny svými vektory, tedy  $[a]_n = [b]_n$  právě tehdy, když  $v(a) = v(b)$ .
- Sčítání a násobení v  $\mathbb{Z}$  modulo  $n$  lze ekvivalentně provádět jako sčítání a násobení mezi vektory, které probíhá po složkách a v každé složce se používají operace z příslušného  $\mathbb{Z}_{n_i}$ .

Tato tvrzení dokážeme v bonusové sekci .

To znamená, že tímto postupem dokážeme výpočty převést do světa vektorů s menšími souřadnicemi. Takovéto situace jsou nejen užitečné prakticky, ale také zajímavé teoreticky a blíže se na ně podíváme právě v bonusové kapitole 20.