4. Rovnice a celá čísla

Jedním z častých úkolů matematiky je řešení rovnic a jejich soustav. To obvykle děláme ve světě reálných čísel, někdy dokonce komplexních, a s určitými typy si umíme docela dobře poradit. Někdy nás ale aplikace donutí pracovat v některém ze světů pocházejících z celých čísel. 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. Víme, že třeba rovnici $6x = 3$ ve světě reálných čísel hravě vyřešíme a najdeme $x = \frac{1}{2}$. Ve světě celých čísel už ale řešení neexistuje. Naopak ve světě $\mathbb{Z}_{27}$ řešení máme, jmenovitě $x = 5$ (zkuste se přesvědčit dosazením). Aby to bylo ještě zajímavější, máme tam i řešení $x = 14$. Je ještě nějaké jiné? Dokážeme řešení najít jinak než metodou pokus-omyl?

4a. Diofantické rovnice

Rovnice, kde máme koeficienty i očekávaná řešení celá, se nazývají **diofantické rovnice** (Diophantine equations). Jmenují se podle člověka jménem Diofanus z Alexandrie, který je zkoumal ve 3. století, ale najdeme je třeba i 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 pravoúhlé 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, ale nebyly vnímány jako jeden okruh problémů, řešily se individuálně a pomalu, 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. Protože u rovnice $ax = b$ je situace jasná (číslo $\frac{b}{a}$ je či není celé, matematici by řekli, že je to „triviální“ případ), je tradicí začít druhou nejjednodušší lineární rovnicí.

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

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.

Takovéto rovnice nám mohou odpovědět třeba na tyto otázky:
- Lze vyplatit c korun pomocí mincí o hodnotách a a b?
- Lze vyměřit c litrů pomocí nádob o objemu a a b?
- Vypustíme děti na kolech na okruh v parku. Jednomu trvá objetí a minut, druhému b minut. Kdy se zase u nás potkají?

Jednu rovnici tohoto typu jsme již 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 našli, se snadno upraví i na případ, kdy místo 1 máme c.

Věta 4a.1.
Nechť $a, b, c \in \mathbb{Z}$. Lineární diofantická rovnice $ax + by = c$ má alespoň jedno řešení právě tehdy, když c je násobkem $\gcd(a, b)$.

Připomeňme, že ekvivalence v sobě skrývá dvě implikace, ke kterým se váže užitečná terminologie. Implikace, že z existence řešení plyne $\gcd(a, b) \mid c$, se dá vyjádřit slovy, že ona dělitelnost je nutnou podmínkou pro existenci řešení. Bez ní tedy rovnice řešit nejde, na druhou stranu ještě její pravdivost nic nezaručuje. Chceme tedy také vědět, že ta dělitelnost je podmínkou postačující, což právě říká ona implikace v opačném směru, že z dělitelnosti plyne existence řešení.

V důkazu věty musíme potvrdit oba tyto směry. Připomeňme nejjednodušší metodu, jak poznat, že nějaký objekt řeší danou rovnici: prostě jej do rovnice dosadíme.

Důkaz (poučný)**:** 1) $\Longrightarrow$: 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 2a.3 dělit i c.

2) $\Longleftarrow$: Předpokládejme, že $c = k \gcd(a, b)$ pro nějaké $k \in \mathbb{Z}$. Podle Bezoutovy identity 2b.16 existují $A, B \in \mathbb{Z}$ takové, že $Aa + Bb = \gcd(a, b)$. Pak $kAa + kBb = k \gcd(a, b)$ neboli $a(kA) + b(kB) = c$, tedy celá čísla $x_0 = kA$, $y_0 = kB$ řeší $ax + by = c$.

□

Důkaz nám poskytl návod, jak rovnice řešit.

Příklad 4a.a: 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 to podle věty nejde.

△

Tak tohle nevyšlo, zkusíme to znovu.

Příklad 4a.b: 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 $\frac{1251}{3} = 417 \in \mathbb{Z}$, je tato úloha řešitelná. Potřebujeme koeficienty Bezoutovy identity.

a, b	A	B
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 přinásobíme, 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: Podle věty a jejího důkazu bychom měli zjistit, jaké je $\gcd(a, b)$, a v případě existence řešení pak najít nějakou Bezoutovu identitu. To je lepší udělat obojí najednou, jedním během Euklidova algoritmu. Tento přístup funguje vždy, mohli bychom jej brát jako algoritmus.

Někdy se ovšem nabídne možnost, jak si ušetřit práci. Například u naší rovnice si lze všimnout, že všechna čísla jsou dělitelná třemi, lze tedy rovnici zkrátit (což je i ve světě celých čísel ekvivalentní operace) a řešit $5x+2y = 417$. Pokud na tuto rovnici aplikujeme onen postup výše, budou všechny výpočty příjemnější, takže se to vyplatí.

Ovšem pokud máme opravdu hodně štěstí, tak ani nic počítat nemusíme. Hned vidíme, že $\gcd(5, 2) = 1$ (což dělí novou pravou stranu 417), a Bezoutovu identitu lze uhodnout, třeba $1 = 1 \cdot 5 + (-2) \cdot 2$. Vynásobíme ji číslem 417 a dostaneme $417 = 5 \cdot 417 + 2 \cdot (-834)$, odtud pak máme hledaná řešení $x = 417$ a $y = -834$.

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

△

Příklad ukázal dvě věci. Jedna je, že od algoritmu je možné se odchýlit, pokud víme, co děláme. Druhá věc je, že bychom se měli povrtat v otázce, kolik existuje řešení, protože to nalezené nás jistě neuspokojuje, určitě bychom preferovali jiné, které po nás nebude vyžadovat vylívání vody, kterou jsme předtím pracně nanosili. Naději máme, protože postup vychází z Bezoutovy identity a již jsme viděli, že Bezoutových vyjádření existuje více.

Řečeno matematickým jazykem, rádi bychom získali nějaký použitelný popis množiny všech řešení dané rovnice. Čtenáře obeznámeného s lineární algebrou následující pasáže jistě nepřekvapí, protože už něco podobného viděl u soustav lineárních rovnic, dokonce i důkazy budou mít stejnou myšlenkou, liší se jen zápisem rovnice. Linearita je mocná vlastnost, a jakmile ji máme, spousta věcí už vyplyne.

Při zkoumání nám velmi pomůže, když si situace zabalíme do jazyka, který uvidí každé řešení jako jeden objekt a navíc nám umožní používat nástroje z lineární algebry. Budeme proto pracovat s vektory $(x, y) \in \mathbb{Z}^2$, například v případě s vodou bychom mohli napsat, že $(417, -834)$ je řešením dané rovnice. Množina všech řešení je pak určitou podmnožinou „vektorového postoru“ $\mathbb{Z}^2$ a nás zajímá, jaké má vlastnosti.

→ Proč jsme ten „vektorový prostor“ dali do uvozovek? Protože definice vektorového prostoru vyžaduje, aby skaláry, kterými vektory násobíme, tvořily těleso (typicky $\mathbb{R}$ nebo $\mathbb{C}$). To si ale v $\mathbb{Z}^2$ nemůžeme dovolit, protože požadavek, aby pro $(x, y) \in \mathbb{Z}^2$ a skalár c platilo $c(x, y) \in \mathbb{Z}^2$, nás nutí vzít jako množinu skalárů pouze celá čísla. Formálně tedy $\mathbb{Z}^2$ vektorový prostor není, ale velká část vlastností je u něj splněna (například všechny algebraické podmínky z definice vektorového prostoru). Pro čtenáře, který je s vektorovými prostory již obeznámen (báze, podprostory atd.), je tedy paralela mezi vektorovými prostory a tím, co zde objevíme, velmi zajímavá. ←

Zápis budeme volit podle okolností, v teoretických úvahách je lepší pracovat s vektory, u praktických úloh bývá často příjemnější používat zápis $x = ..., y = ...$

U lineárních rovnic bývají homogenní rovnice výrazně příjemnější. To platí i tady, takže si uděláme definici, která nám umožní k takovým rovnicím přejít.

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

Teď ukážeme, že stačí umět opravdu dobře řešit jen homogenní rovnice.

Věta 4a.2.
Nechť $a, b, c \in \mathbb{Z}$. Uvažujme lineární diofantickou rovnici $ax + by = c$. Nechť $(x_p, y_p) \in \mathbb{Z}^2$ je nějaké její řešení.
Dvojice $(x_0, y_0) \in \mathbb{Z}^2$ je řešení této rovnice právě tehdy, když existuje $(x_h, y_h) \in \mathbb{Z}^2$ takové, že $(x_0, y_0) = (x_p, y_p) + (x_h, y_h)$ 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. Implikace zleva doprava pak říká, že libovolné další její řešení dokážeme získat jedině tak, že k tomu jednomu přidáváme řešení přidržené homogenní rovnice (budeme jim říkat „homogenní řešení“ a měli bychom je získávat snadněji, ale o tom později). Implikace zprava doleva pak říká, že tím přidáváním homogenních řešení nelze nic zkazit, vždycky tím dostaneme řešení dané rovnice. Dohromady z toho vychází, že přičítáním homogenních řešeními dostáváme přesně množinu všech řešení dané rovnice.

Jako obvykle budeme každou implikaci dokazovat zvlášť a začneme tou zprava doleva (že když přidáváme homogenní řešení, tak vznikne řešení dané rovnice), protože je to snažší.

Důkaz (poučný)**:** Mějme nějaké řešení (x_p, y_p) dané rovnice, tedy platí $ax_p + by_p = c$.

1) $\Longleftarrow$: Předpokládejme, že $(x_h, y_h) \in \mathbb{Z}^2$ řeší přidruženou homogenní rovnici. Dosaďme tedy $x_0 = x_p + x_h$ a $y_0 = y_p + y_h$ do dané rovnice, začneme levou stranou a uvidíme, co se z ní vyvrbí:
$ax_0 + by_0 = a(x_p + x_h) + b(y_p + y_h) = (ax_p + by_p) + (ax_h + by_h) = c + 0 = c.$
Ano, (x_0, y_0) je opravdu řešením dané rovnice.

2) $\Longrightarrow$: Předpokládejme, že (x_0, y_0) řeší danou rovnici. Potřebujeme najít vektor (x_h, y_h) splňující dvě podmínky. Ta algebraická nedává na výběr, aby to vyšlo, musíme zvolit $x_h = x_p - x_0$ a $y_h = y_p - y_0$. Tvrdíme, že toto je hledaný vektor.

Evidentně $(x_h, y_h) \in \mathbb{Z}^2$ a $(x_0, y_0) = (x_p, y_p) + (x_h, y_h)$. Zbývá ukázat, že (x_h, y_h) řeší přidruženou homogenní rovnici. Zkusíme dosadit do její levé strany, využijeme pak toho, že (x_p, y_p) i (x_0, y_0) jsou řešení původní rovnice: $ax_h + by_h = a(x_p - x_0) + b(y_p - y_0) = (ax_p + by_p) - (ax_0 + by_0) = c - c = 0$. Ano, (x_h, y_h) řeší přidruženou homogenní rovnici.

□

Takže jakmile už jedno konkrétní řešení (x_p, y_p) dané diofantické rovnice máme (tomu pak říkáme **partikulární řešení** a umíme ho najít tím postupem přes Bezoutovu identitu), tak lze množinu všech (celočíselných) řešení získat takto:

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

Zbývá vymyslet, jak zcela řešit homogenní rovnice, tedy jak najít všechna celočíselná řešení takových rovnic. To nám prozradí následující věta, ale nejprve si to zkusme rozmyslet. Rovnici $ax + by = 0$ lze přepsat jako $ax = -by$. Snadno pak uhádneme jedno řešení, stačí dát třeba $x = -b$ a $y = a$. Všimněme si také, že jakmile máme jedno řešení (x_0, y_0), tak další získáme vynásobením čísel x_0, y_0 libovolným celým číslem k, protože z $ax_0 = -by_0$ plyne $akx_0 = -bky_0$. Řešení tedy bude nekonečně mnoho, například všechna ve tvaru $x = -bk$, $y = ak$ pro $k \in \mathbb{Z}$. Kritická otázka ovšem je, jestli jsou i jiná.

Představme si na chvíli, že a, b v rovnici $ax = -by$ jsou nesoudělná. Koeficient b dělí levou stranu ax, ale je nesoudělný s a, takže (viz lemma 2b.19) musí dělit x. Jinými slovy, řešení x hledáme jen mezi násobky b. Obdobně budeme hledat y jen mezi násobky čísla a. Ona řešení z předchozího odstavce tedy budou (pro a, b nesoudělná) jediná možná.

Co když a, b nesoudělná nejsou? Pak jsou i řešení jiná než $(-kb, ka)$. Například u rovnice $4x + 6y = 0$ nám předchozí postup dává řešení ve tvaru $x = -6k$, $y = 4k$ neboli $(-6k, 4k)$ pro $k \in \mathbb{Z}$, ale vidíme také řešení $x = 3$, $y = -2$, které nelze volbou $k \in \mathbb{Z}$ získat z toho obecného vzorce. Situace je tedy obecně složitější, ale naštěstí se k té nesoudělné dokážeme dostat jednoduše tak, že koeficienty v rovnici vykrátíme.

Věta 4a.3.
Uvažujme rovnici $ax + by = 0$ pro $a, b \in \mathbb{Z}$. Množina všech jejích celočíselných řešení je

$$\left\{\left(k\frac{b}{\gcd(a,b)}, -k\frac{a}{\gcd(a,b)}\right) : k \in \mathbb{Z}\right\}.$$

Důkaz (poučný)**:** 1) Nejprve ověříme, že dvojice $x_h = k\frac{b}{\gcd(a,b)}$, $y_h = -k\frac{a}{\gcd(a,b)}$ jsou opravdu řešení ze $\mathbb{Z}$. Celočíselnost plyne z toho, že $\frac{b}{\gcd(a,b)}$ a $\frac{a}{\gcd(a,b)}$ jsou celá čísla, po dosazení x_h, y_h do rovnice pak okamžitě dostáváme $ax_h + by_h = ak\frac{b}{\gcd(a,b)} - bk\frac{a}{\gcd(a,b)} = 0$. Takže to souhlasí.

2) Zbývá ukázat, že řešení daná tímto předpisem jsou všechna, tj. že žádné jiné neexistuje. Nechť je tedy (x_0, y_0) nějaké řešení rovnice $ax+by = 0$. Vydělíme ji číslem $\gcd(a,b)$ a převedeme jeden člen na druhou stranu: $\frac{b}{\gcd(a,b)}y_0 = -\frac{a}{\gcd(a,b)}x_0$. Vidíme, že celé číslo $\frac{b}{\gcd(a,b)}$ musí dělit $\frac{a}{\gcd(a,b)}x_0$, jenže podle faktu 2b.8 jsou $\frac{b}{\gcd(a,b)}$ a $\frac{a}{\gcd(a,b)}$ nesoudělná čísla, tudíž musí podle lemma 2b.19 číslo $\frac{b}{\gcd(a,b)}$ dělit x_0. Existuje tedy $k \in \mathbb{Z}$ takové, že $x_0 = k\frac{b}{\gcd(a,b)}$, z rovnice $by = -ax$ pak snadno dostaneme příslušný vzorec pro y_0.

□

Na otázku „najděte řešení rovnice“ lze odpovědět více způsoby. Je například možné poskytnout přímo popis množiny všech řešení, jak jsme to udělali ve znění věty. Další (a možná populárnější) podoba je poskytnout vzorec, který takovou množinu generuje pomocí nějaké pomocné proměnné, ve větě bychom mohli místo množiny napsat „$x = k\frac{b}{\gcd(a,b)}$, $y = -k\frac{a}{\gcd(a,b)}$ pro $k \in \mathbb{Z}$“. Takovému vzorci se říká **obecné řešení**.

Pozorný čtenář si teď jistě všimnul, že ve znění věty je znaménko mínus u y, zatímco v úvahách před větou bylo u x. Vysvětlení je snadné, nás zajímá množina všech řešení a tam na umístění znaménka nesejde. Pokud bychom například při řešení rovnice $3x + 4y = 0$ použili intuitivní přístup předvedený před větou, dostaneme množinu danou vzorcem $x = -4k$, $y = 3k$ pro $k \in \mathbb{Z}$. Volbou $k = 3$ pak dostaneme konkrétní řešení $x = -12$, $y = 9$ neboli $(-12, 9)$. Pokud bychom použili vzorec $(4k, -3k)$ z věty, pak totéž řešení dostaneme volbou $k = -3$. Oba vzorce tedy dokážou poskytnout stejné řešení, jen k tomu používají jinou hodnotu k. Je snadné dokázat toto obecně, pro všechna řešení z množiny.

Zde narážíme na lokálnost proměnných, každý vzorec pro řešení má jakoby svoje vlastní k, nejde o totéž písmeno. Asi by bylo lepší použít v druhém vzorci jiný parametr místo k, třeba l, pak by to bylo jasnější, ale není to nutné.

My se zde totiž bavíme o množině všech řešení, vzorec „$x = -4k$, $y = 3k$ pro $k \in \mathbb{Z}$“ reprezentuje množinu dvojic, které lze získat proběhnutím k skrz celou množinu $\mathbb{Z}$. Tento objekt (množina dvojic) při pohledu zvenčí žádné k nemá, to je jen pracovní proměnná, jejíž význam je tedy lokální a lze ji nahradit jiným písmenem. Ten alternativní vzorec pomocí své pomocné proměnné také vytvoří nekonečnou množinu dvojic a ty dvě množiny souhlasí.

Máme tedy u mínusu na výběr a v praxi většinou volíme tu variantu, která nám přijde příjemnější, například u rovnice $10x - 15y = 0$ dostáváme buď řešení ve tvaru $(3k, 2k)$, $k \in \mathbb{Z}$ nebo ve tvaru $(-3k, -2k)$, $k \in \mathbb{Z}$, první se mi líbí víc.

Podobná úvaha platí pro větu o struktuře řešení, která nevyžadovala nějaké speciální partikulární řešení (x_p, y_p). Pokud své obecné řešení vybudujete pomocí jistého (x_p, y_p) a kamarád se rozhodně vyjít z jiného, tak nejspíše získá jiné konkrétní vzorce pro obecné řešení (x, y), ale jako množiny se vaše odpovědi musejí rovnat. Jinak řečeno, abyste se dostali ke stejnému konkrétnímu řešení od různých partikulárních, budeme se také muset posunout o jiná řešení přidružené homogenní rovnice, ale určitě to půjde.

Příklad 4a.c (pokračování 4a.b)**:** Již jsme našli jedno řešení $x_p = 417$, $y_p = -834$.

Přidružená homogenní rovnice $15x + 6y = 0$ neboli $5x = -2y$ 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 dostáváme obecné řešení $x = 417 - 2k$, $y = 5k - 834$ pro $k \in \mathbb{Z}$.

Můžeme udělat zkoušku, jako obvykle dosazením do rovnice:

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

Vyšla.

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 nejaké 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 $x + y = (417 - 2k) +$

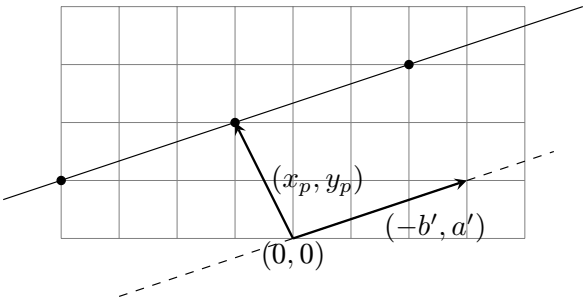
$(5k - 834) = 3k - 417$, ale zajímají nás jen hodnoty k mezi 167 a 208. Řešením je evidentně volba co nejmenšího možného k, tedy $k = 167$. Nejméně se naběháme, pokud použijeme $x = 83$ patnáctilitrovek a jednu šestilitrovku.
△

4a.4 Poznámka: Vzorec z věty o homogenní rovnici si můžeme přepsat do podoby $\{k(b', -a') : k \in \mathbb{Z}\}$, kde písmeny a', b' označíme koeficienty vykrácené rovnice. Máme tedy vektor $(b', -a')$, který generuje všechna řešení. Kdybychom pracovali v rovině $\mathbb{R}^2$ a nechali k probíhat všemi reálnými čísly, dostali bychom parametrický popis jednorozměrného útvaru, přímky procházející skrz počátek. To není překvapení, hledat celočíselná řešení rovnice $ax + by = 0$ můžeme tak, že nejprve rovnici $ax + by = 0$ vyřešíme v reálném oboru, dostaneme onu přímku, a pak se podíváme, zda tato přímka neprotíná nějaké body s celočíselnými souřadnicemi. Odtud pak plyne obdobné chování rovnic v $\mathbb{R}^2$ a v $\mathbb{Z}^2$, ačkoliv ten druhý není vektorový prostor (jak jsme již zmínili). Pojďme tedy následovat onu paralelu dále.

U parametrické přímky v $\mathbb{R}^2$ můžeme zvolit i jiný směrový vektor, například vektor opačný neboli $(-b', a')$. Dostáváme tím alternativní popis množiny řešení, přesně jak jsme se o tom bavili před chvílí. Teď ovšem přichází první rozdíl. Zatímco v $\mathbb{R}^2$ si můžeme volit i další směrové vektory, třeba $(2b', -2a')$, a dají nám stejnou přímku, v $\mathbb{Z}^2$ už to nejde, protože díky omezení $k \in \mathbb{Z}$ bychom se nedokázali od vektoru $(2b', -2a')$ dostat zpět k $(b', -a')$. Při volbě generujícího vektoru tedy budeme muset být opatrnější a ještě se k tomu vrátíme.

V lineární algebře bychom si také všimli, že množina ve tvaru $\{t(b', -a') : t \in \mathbb{R}\}$ je uzavřená na součet a násobení skalárem, je to tedy vektorový podprostor $\mathbb{R}^2$, přičemž vektor $(b', -a')$ je jeho báze. V $\mathbb{Z}^2$ o podprostoru a bázi mluvit nelze, nicméně množina všech řešení homogenní rovnice je uzavřená na součet a také na násobení celočíselným skalárem. Nelze oficiálně říct, že tato množina je jednorozměrná, ale pocit je to správný, v reálném i celočíselném případě máme jeden stupeň volnosti reprezentovaný parametrem $t \in \mathbb{R}$, popř. $k \in \mathbb{Z}$.

Podívejme se nyní na případ nehomogenní rovnice $ax+by = c$, u které jsme (například pomocí Bezoutovy identity) získali jedno řešení (x_p, y_p). Množinu všech řešení dostaneme tak, že tento vektor přičítáme k oné množině homogenních řešení. Geometricky vzato, my tu přímku (přesněji řečeno body s celočíselnými souřadnicemi z oné přímky) jako celek posuneme pomocí vektoru (x_p, y_p).



Obrázek ukazuje případ rovnice, kde $a > 0$ a $b < 0$, pak opravdu $(-b', a')$ vede doprava nahoru. Podobnost s rovnicemi nad reálnými čísly bude fungovat i v bonusové sekci 4d, kde se podíváme na soustavy rovnic více proměnných.
△

Teoretické poznatky o množině řešení si převedeme do formy algoritmu.

S Algoritmus 4a.5.
pro nalezení všech celočíselných řešení rovnice $ax + by = c$.

0. Například pomocí rozšířeného Euklidova algoritmu najděte $\gcd(a, b) = Aa + Bb$.

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

2. Případ $\gcd(a, b)$ dělí c:

a) Získanou rovnost $aA + bB = \gcd(a, b)$ vynásobte číslem $c' = \frac{c}{\gcd(a,b)} \in \mathbb{Z}$ tak, aby se zachovaly koeficienty a, b, a dostanete $a(Ac') + b(Bc') = c$, tudíž i jedno partikulární řešení $x_p = Ac'$, $y_p = Bc'$ neboli vektor (Ac', Bc').

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

c) Sečtením partikulárního a obecného homogenního řešení získáte množinu všech celočíselných řešení

$$\{(x_p + kb', y_p - ka') : k \in \mathbb{Z}\} \text{ neboli } x = x_p + kb',\ y = x_p - ka' \text{ pro } k \in \mathbb{Z},$$

popřípadě verzi s mínusem u y_h.
△

Příklad 4a.d: Vyřešíme rovnici $351x + 208y = 143$.

Aplikujeme Euklidův aloritmus na čísla 351 a 208:

a,b	A	B
351	1	0
208	0	1
143	1	-1
65	-1	2
13•	3•	-5•
0	-16	27

Dostáváme $\gcd(351,208)=13$, což dělí pravou stranu, rovnice je řešitelná.

Dostali jsme také vyjádření $351\cdot 3+208\cdot(-5)=13$. Abychom měli na pravé straně 143, vynásobíme tuto identitu jedenácti, na levé straně si chceme zachovat čísla 351 a 208: $351\cdot 33+208\cdot(-55)=143$. Porovnáním s danou rovnicí vidíme řešení $x_p=33$, $y_p=-55$.

Homogenní řešení: Rovnici $351x+208y=143$ vykrátíme číslem 13 a máme $27x+16y=0$. Odtud $x_h=-16k$, $y_h=27k$ pro $k\in\mathbb{Z}$.

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

Kdyby to někdo chtěl množinově, tak množina všech řešení dané rovnice je

$$\{(33-16k,27k-55):k\in\mathbb{Z}\}.$$

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

Pokud bychom chtěli řešení, kde $x,y\in\mathbb{N}_0$, tak máme smůlu, žádná nejsou.

△

Máme tedy funkční postup. Dá se vyjádřit vzorcem, kombinací vět 4a.2 a 4a.3 získáme následující tvrzení.

Důsledek 4a.6.
Uvažujme 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 množina všech řešení dané rovnice je

$$\left\{\left(A\frac{c}{\gcd(a,b)}+k\frac{b}{\gcd(a,b)},B\frac{c}{\gcd(a,b)}-k\frac{a}{\gcd(a,b)}\right):k\in\mathbb{Z}\right\}.$$

Někteří studenti toto vnímají jako alternativní postup řešení, prostě si tyto vzorce zapamatují a pak do nich dosazují. Funguje to, ale zkušenost ze zkoušek naznačuje, že to není velmi spolehlivé, protože je snadné si něco ve vzorci splést. Spíše tedy doporučujeme následovat některý z algoritmů výše či níže. Pro počítač je ovšem použití vzorce snadné a spolehlivé. Z pohledu programátora je proto nyní situace jasná. Pro nalezení Bezoutovy identity máme efektivní algoritmus (který můžeme o něco urychlit prací se zápornými zbytky), pak stačí dosadit do vzorce a hotovo.

Přesto neodoláme a ještě přidáme dvě zamyšlení. V sekci 2c.6 jsme vyzkoušeli alternativní pohled na Euklidův algoritmus prostřednictvím matic, tak to zkusíme znovu a dostaneme některé zajímavé výsledky. Mimo jiné se nabídne efektivní ruční výpočet, k možným zkratkám se dostaneme v druhém zamyšlení.

4a.7 Řádková eliminace a Euklidův algoritmus

Vraťme se na chvíli k příkladu 4a.d. Výjimečně jsme spočítali celý ukončovací řádek (s nulou vlevo) a objevila se tam čísla -16 a 27 neboli vektor $(-16,27)$, což je úžasnou shodou okolností přesně vektor, který nám tam generoval homogenní řešení. Ono to asi shoda okolností nebude, evidentně zde máme zajímavý jev, který stojí za bližší prozkoumání. Podíváme se tedy na náš postup jako na úpravy matice.

Algoritmus začíná s řádky $\left|\,a\,\middle|\,1\,\middle|\,0\,\right|$ a $\left|\,b\,\middle|\,0\,\middle|\,1\,\right|$, což odpovídá matici $\begin{pmatrix}a&1&0\\b&0&1\end{pmatrix}$ a reprezentuje to soustavu

$$1\cdot u+0\cdot v=a$$
$$0\cdot u+1\cdot v=b,$$

která má jediné řešení $u=a$, $v=b$. Již víme, že Euklidův algoritmus je totéž, jako redukování této matice na tvar $\begin{pmatrix}\gcd(a,b)&A&B\\0&A_h&B_h\end{pmatrix}$. Tato matice reprezentuje soustavu

$$A\cdot u+B\cdot v=\gcd(a,b)$$
$$A_h\cdot u+B_h\cdot v=0.$$

Protože šlo o ekvivalentní úpravy, má tato soustava stejné řešení jako ta původní, tedy platí

$$a\cdot A_p+b\cdot B_p=\gcd(a,b)$$
$$a\cdot A_h+b\cdot B_h=0.$$

První řádek už jsme probírali v sekci 2c.6, potvrzuje, že algoritmus poskytuje Bezoutovu identitu. Zajímavá je druhá rovnost, ukazuje, že čísla A_h,B_h řeší přidruženou homogenní rovnici. Dostáváme tak vektor, který generuje homogenní řešení vzorcem $x_h=A_hk$, $y_h=B_hk$. V této chvíli ovšem nevíme, zda je generuje všechna, to už z této úvahy nevyplývá.

My samozřejmě díky větě 4a.3 víme, jak správné generující vektory vypadají. Dá se dokázat, že čísla A_h, B_h opravdu jsou ona čísla z věty, ale dá to práci, viz kapitola 16. Zkusíme tady jiný přístup, který vychází z naší situace.

Představme si tedy, že nám někdo dal čísla A_h, B_h s tím, že možná generují množinu homogenních řešení. Umíme poznat, zda je to pravda?

Lemma 4a.8.
Nechť $a, b \in \mathbb{Z}$. Vektor $(A_h, B_h) \in \mathbb{Z}^2$ generuje všechna řešení rovnice $ax + by = 0$ právě tehdy, když ji sám řeší a čísla A_h, B_h jsou nesoudělná.

Důkaz (poučný)**:** 1) $\Longrightarrow$: Pokud vektor (A_h, B_h) generuje řešení, pak musí rovnici řešit i čísla $x = A_h \cdot 1$, $y = B_h \cdot 1$ neboli A_h, B_h. Je tedy sám řešením.

Podle věty 4a.3 pak musí existovat nějaké $k \in \mathbb{Z}$ takové, že $A_h = k\frac{b}{\gcd(a,b)} = kb'$ a $y = -k\frac{a}{\gcd(a,b)} = -ka'$. Máme tedy $b' \mid A_h$. Ovšem dle předpokladu (A_h, B_h) generuje všechna řešení, musí tedy generovat i $(b', -a')$, takže $A_h \mid b'$. Podle věty 2a.5 (ii) pak nutně $|A_h| = |b'|$, tedy $|k| = 1$. Můžeme proto počítat

$$\gcd(A_h, B_h) = \gcd(kb', -ka') = |k| \gcd(b', -a') = 1 \cdot \gcd\Big(\frac{b}{\gcd(a,b)}, \frac{a}{\gcd(a,b)}\Big) = 1,$$

viz fakt 2b.8.

2) $\Longleftarrow$: Jestliže (A_h, B_h) řeší homogenní lineární rovnici, pak podle věty 4a.3 musí existovat nějaké $k \in \mathbb{Z}$ takové, že $A_h = k\frac{b}{\gcd(a,b)} = kb'$ a $y = -k\frac{a}{\gcd(a,b)} = -ka'$. Dostáváme pak

$$\gcd(A_h, B_h) = |k| \gcd(b', -a').$$

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

Pokud $k = 1$, dostáváme $(A_h, B_h) = (b', -a')$, je to tedy přímo generující vektor z věty 4a.3. Pokud $k = -1$, tak máme $(A_h, B_h) = (-b', a')$, což je ten druhý možný generující vektor.

□

Tím se naše pozornost přesouvá k jiné otázce: Jsou čísla v nulovém řádku nesoudělná? Podíváme-li se na všechny příklady s rozšířeným Euklidovým algoritmem, které jsme zatím v knize měli, zjistíme, že čísla ve sloupcích A, B jsou nesoudělná nejen v řádku nulovém, ale dokonce ve všech řádcích. V kapitole 16 toto dokážeme indukcí, teď se jen podíváme na řádek, který nás zajímá, a použijeme k potvrzení nesoudělnosti zajímavý trik.

V našich úvahách jsme pomocí přičítání násobku řádku k řádku jinému došli od matice $\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$ k matici $\begin{pmatrix} \gcd(a,b) & A & B \\ 0 & A_h & B_h \end{pmatrix}$. Pokud ignorujeme levý sloupec, vidíme přechod od jedné čtvercové matice k druhé, přičemž použitá operace zachovává determinant. Proto platí, že

$$\det \begin{pmatrix} A & B \\ A_h & B_h \end{pmatrix} = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$

Máme tedy $AB_h - BA_h = 1$. Pokud je číslo $d \in \mathbb{N}$ společným dělitelem A_h a B_h, tak podle tohoto vzorce musí také dělit jedničku, tedy nutně $d = 1$. Vidíme, že větší společní dělitelé než 1 nejsou, proto $\gcd(A_h, B_h) = 1$ a podle lemma 4a.8 tedy vektor (A_h, B_h) generuje všechna homogenní řešení.

Máme tedy potvrzeno, že vektor generující homogenní řešení lze nalézt přímo v tabulce. Nabízí se další zjednodušení, že bychom si v prvním řádku matice pomocí $\gcd(a, b)$ vyrobili přímo c. To znamená, že bychom z matice $\begin{pmatrix} \gcd(a,b) & A & B \\ 0 & A_h & B_h \end{pmatrix}$ přešli na matici $\begin{pmatrix} c & A_p & B_p \\ 0 & A_h & B_h \end{pmatrix}$. Tato matice reprezentuje soustavu

$$A_p \cdot u + B_p \cdot v = \gcd(a, b)$$
$$A_h \cdot u + B_h \cdot v = 0.$$

Dosadíme-li řešení $u = a$, $v = b$, dostáváme

$$a \cdot A_p + b \cdot B_p = c$$
$$a \cdot A_h + b \cdot B_h = 0.$$

První řádek ukazuje, že (A_p, B_p) je partikulární řešení.

Získáváme tak zajímavý alternativní postup. Je-li dána rovnice $ax + by = c$, sestavíme příslušnou matici a upravíme ji tak, aby v první sloupci vznikla čísla c a 0. V pravé části řádků pak najdeme přímo hledaná čísla pro sestavení řešení.

Protože má v našem případě matice pouze dva řádky, je možné tento postup zachytit v tabulce, která se velmi podobá Euklidovu algoritmu. Zde je ovšem dobré podotknout, že se k řádkům začínajícím nulou a c dostaneme nejspolehlivěji právě tím, že nejprve vytvoříme $\gcd(a,b)$. To znamená, že vlastně jde jen o mírnou úpravu známého postupu. Nejprve použijeme rozšířený Euklidův algoritmus (ať už klasický nebo se zápornými zbytky), přičemž dopočítáme i nulový řádek, následně pomocí řádku před ním vytvoříme ještě řádek dodatečný, který bude mít vlevo c (pokud je to možné).

S Algoritmus 4a.9.
pro snadné nalezení všech celočíselných řešení rovnice $ax + by = c$.
0. Aplikujte rozšířený Euklidův algoritmus na čísla a, b, přičemž lze využívat i záporné zbytky. Poslední řádek tabulky bude $\mid 0 \mid A_h \mid B_h \mid$.
1. Vytvořte ještě jeden řádek navíc tak, že předposlední řádek (ten s gcd) vynásobíte vhodným číslem, aby se vlevo objevilo c.
Pokud to nejde, rovnice není řešitelná a algoritmus skončil.
2. Pokud to jde, v tabulce přibude řádek $\mid c \mid A_p \mid B_p \mid$.
Obecné řešení rovnice je $x = A_p + A_h k$, $y = B_p + B_h k$ pro $k \in \mathbb{Z}$,
popřípadě $x = A_p - A_h k$, $y = B_p - B_h k$ pro $k \in \mathbb{Z}$.
△

Příklad 4a.e: Vrátíme se k příkladu 4a.d a vyřešíme $351x + 208y = 143$ podle nového algoritmu.

Použili jsme záporné zbytky, čímž se postup o něco zrychlil. Pomocí posledních dvou řádků napíšeme obecné řešení $x = 33 + 16k$, $y = -55 - 27k$ pro $k \in \mathbb{Z}$.

Samozřejmě výpočty, které se prováděly, jsou stejné jako u předchozího řešení, liší se jen prezentace. Z pohledu počítače či programátora tedy mezi oněmi algoritmy není rozdíl. Přesto stojí za to si toto ukázat. Jednak proto, že to je zajímavá možnost pro ruční výpočet (viz další sekce). Další důvod je, že Euklidův algoritmus funguje pouze pro dvě proměnné, zatímco maticový pohled lze přímočaře rozšířit na případ více proměnných a soustav, viz 4e. To už pak je zajímavé i pro programátora.

a, b	A	B
351	1	0
208	0	1
−65	1	−2
13	3	−5
0	16	−27
143	33	−55

4a.10 Ruční výpočet

Předchozí sekce nám nabídla zajímavou možnost, která může významně zpříjemnit ruční výpočet. Nevýhoda je, že je to mechanický postup, který zakrývá, co se vlastně děje. To neznamená, že by jej člověk neměl používat, ale je zároveň dobré pochopit, z čeho vychází a co se za ním skrývá, třeba proto, aby se člověk mohl od postupu odchýlit, případně jej úplně opustit, když je to výhodné. Čtenář má na výběr docela široké rozmezí možností. Může použít strukturovaný postup podle prvního algoritmu, urychlit si jej uvažováním záporných zbytků, ještě více urychlit pomocí druhého algoritmu, jsou možné i další modifikace postupu. Probereme si to na příkladě.

Příklad 4a.f: Vyřešíme rovnici $119x - 273y = -70$.

Nejprve pro srovnání ukážeme, jak by vypadal postup podle algoritmu 4a.5, kdy využíváme věty o struktuře řešení.

Potřebujeme najít Bezoutovu identitu pro čísla 119 a −273, standardně se ovšem Euklidův algoritmus zavádí pro $a > b > 0$. Proto v tabulce použijeme čísla 273 a 119 a přecházíme ke zbytkům po dělení.

Dostáváme identitu $7 = 7 \cdot 273 + (-16) \cdot 119$. Upravíme ji tak, aby se i znaménkově shodovala s danou rovnicí, nejprve jen přeorganizujeme, $119 \cdot (-16) - 273 \cdot (-7) = 7$, pak ji vynásobíme mínus deseti: $119 \cdot 160 - 273 \cdot 70 = -70$. Šlo to, tedy řešení existuje. Vidíme partikulární řešení $x_p = 160$, $y_p = 70$.

a, b	A	B
273	1	0
119	0	1
35	1	−2
14	−3	7
7•	7•	−16•
0		

Teď homogenní rovnice. Vykrátíme ji společným dělitelem 7 na tvar $17x - 39y = 0$ a vidíme řešení $x_h = 39k$, $y_h = 17k$ pro $k \in \mathbb{Z}$.

Závěr: Obecné řešení je $x = 160 + 39k$, $y = 70 + 17k$ pro $k \in \mathbb{Z}$.

Ž úsporných důvodů by někdo ještě mohl chtít vybrat lepší partikulární řešení, třeba tak, že od $(160, 70)$ odečte čtyřikrát homogenní řešení $(39, 17)$, pro obecné řešení pak vyjde vzorec $x = 4 + 39l$, $y = 2 + 17l$ pro $l \in \mathbb{Z}$. Tentokráte jsme použili pro „jiné k“ samostatné písmeno, ať je to formálně správně. Víme, že oba vzorce pro obecné řešení generují stejnou množinu, pro zajímavost se zkusíme přesvědčit:

$$x = 4 + 39l = 4 + 39(l + 4 - 4) = 4 + 156 + 39(l - 4) = 160 + 39(l - 4),$$
$$y = 2 + 17l = 2 + 17(l + 4 - 4) = 2 + 68 + 17(l - 4) = 70 + 17(l - 4).$$

Vidíme, že mezi vzorci lze přecházet posunem parametru o čtyři.

Lze tento standardní postup nějak zkrátit? Jedna možnost je povolit si záporné zbytky v Euklidově algoritmu. Zde to ovšem nikterak nepomůže, vedlo by to na přesně stejný výpočet. Podíváme-li se do tabulky, uvidíme, že vždy platí $r_{k+1} \leq \frac{1}{2} r_k$, takže již náš postup používal optimální záporné zbytky, shodou okolností byly vždy kladné.

Zajímavější možnost nabízí, když si uvědomíme, že naším konečným cílem není získat $\gcd(a,b)$, ale vyjádřit pravou stranu 70. Víme, že číslo v levém sloupci tabulky lze získat pomocí koeficientů v dalších dvou sloupcích nejen v posledním řádku, ale ve všech. Nabízí se tedy třetí řádek neboli $35 = 273 \cdot 1 + 119 \cdot (-2)$. Když jej vynásobíme mínus dvojkou a přeorganizujeme, dostáváme $119 \cdot 4 - 273 \cdot 2 = -70$, odtud $x_p = 4$, $y_p = 2$. Dostali jsme ona příjemnější čísla z alternativního vzorce. Asi nemá smysl obtěžovat počítač testováním, ze kterého řádku by se tak mohl dostat k c, ale při ručním výpočtu toto může být zajímavé, protože čím „vyšší“ řádek použijeme, tím menší čísla dostáváme pro partikulární řešení.

Je tu ještě otázka znaménka. V sekci 2b.15 jsme ukázali, že Euklidův algoritmus funguje obecně, pro libovolné dva vstupy. Můžeme jej tedy aplikovat přímo na koeficienty z rovnice, ve správném pořadí a včetně znaménka. A když už máme záporné číslo, má smysl dovolit si záporné zbytky. Jdeme na to.

a,b	A	B
119	1	0
−273	0	1
119	1	0
−35	2	1
14	7	3
−7•	16•	7•
0		

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.

Dostali jsme $-7 = -273 \cdot 7 + 119 \cdot 16$, vynásobením deseti pak obdržíme partikulární řešení. Z pohledu počítače je toto ideální, v nejhorším případě děláme jeden cyklus navíc na úpravu pošadí a nemusíme vůbec řešit znaménka.

V rámci strukturovaného postupu už asi nic lepšího nevymyslíme. Teď se podíváme na postup pomocí algoritmu 4a.9. Zde je zase možné pracovat jen s kladnými čísly a znaménko doplnit později, nebo rovnou brát záporná čísla. Protože chceme efektivní postup (jinak bychom tento algoritmus asi nepoužívali), vezmeme to cestou se znaménky. Určitě budeme chtít ušetřit jeden krok tím, že do tabulky nejprve zapíšeme to číslo, které je větší (v absolutní hodnotě).

To má jeden důležitý aspekt, my chceme z řádků rovnou vyčítat vektory řešení, ale pořadí proměnných je navázáno na pořadí koeficientů v tabulce. Je tedy nutné si toto hlídat. O návaznosti koeficientů a sloupců nejlépe vypovídají jedničky v úvodních dvou řádcích. Osvědčilo se mi nepsat do hlavičky A a B, ale rovnou jména proměnných, kterých se jednotlivé sloupce týkají. Jdeme na to, použijeme také trik s vytvářením sedmdesátky pomocí řádku začínajícího 35.

a,b	y	x
−273	1	0
119	0	1
−35	1	2
14	3	7
−7	7	16
0	17	39
−70	2	4

Rovnice je řešitelná, protože se podařilo vyrobit sedmdesátku. Z posledních dvou řádků si (díky označeným sloupcům) hravě přečteme, že $(x_p, y_p) = (4,2)$ a $(x_h, y_h) = (39,17)k$. To bylo lehké.

Kdyby chtěl někdo pracovat jen s kladnými čísly, protože mu to jde lépe, tak je to možné, patřičné znaménko lze například indikovat v hlavičce pomocných sloupců. Jak jsme již viděli, v tomto příkladě to vyžaduje stejně kroků jako obecně úspornější metoda záporných zbytků.

V tabulce si pak přečteme správné vektory $(x_p, y_p) = (4,2)$ a $(x_h, y_h) = (39,17)k$.

a,b	$-y$	x
273	1	0
119	0	1
35	1	−2
14	−3	7
7	7	−16
0	−17	39
−70	−2	4

Jako poslední nahlédnutí do fungování algoritmu si ukážeme, že není nutné začínat zrovna připojením jednotkové matice. Podstatné je mít v každém řádku pomocné části jednu jedničku. Správné označení sloupců pak zajistí správnou interpretaci výsledků.

Je vidět, že je dost možností si výpočet přizpůsobit a vytvarovat dle osobní preference. Obecně platí, že čím vice se člověk hodlá odchýlit od standardního postupu, tím lépe by měl rozumět tomu, co vlastně má ten standardní postup za lubem, aby docenil dopady změn, které udělá.

a,b	x	$-y$
273	0	1
119	1	0
35	−2	1
14	7	−3
7	−16	7
0	39	−17
−70	4	−2

Na závěr ještě poznámku. Několikrát jsme pak mezi řešeními hledali nějaká zajímavější. Pokud bychom pro nějakou aplikaci potřebovali čistě řešení z $\mathbb{N}$, tak ze vzorečku vidíme, že jich je nekonečně mnoho.

△

Cvičení

Cvičení 4a.1 (rutinní)**:** Najděte všechna řešení $(x, y) \in \mathbb{Z}^2$ a $(x, y) \in \mathbb{N}_0^2$ pro následující diofantické rovnice:
(i) $6x + 9y = 204$; (iii) $10x - 4y = 26$; (v) $819x + 315y = 126$;
(ii) $10x - 15y = 131$; (iv) $105x - 75y = 0$; (vi) $65x + 273y = 157$.

Cvičení 4a.2: Dostali jste stokorunu s tím, že za ni máte nakoupit lízátka 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 4a.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. 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 4a.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 4a.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 si odměřujete podél okraje a děláte čárky?

Řešení:
4a.1: (i): $\gcd(6, 9) = 3$ uhodneme, řešíme $2x + 3y = 68$: $\gcd(3, 2) = 1 = 1 \cdot 3 + (-1) \cdot 2$, proto $\gcd(2, 3) = 1 = (-1) \cdot 2 + 1 \cdot 3$, po vynásobení $2 \cdot (-68) + 3 \cdot 68 = 68$. Řešení $(x, y) = (-68 + 3k, 68 - 2k)$ neboli $x = 3k - 68$, $y = 68 - 2k$ pro $k \in \mathbb{Z}$. Řešení v $\mathbb{N}_0$: $23 \leq k \leq 34$.
(ii): $\gcd(10, -15) = 5$ nedělí 131. Nemá řešení.
(iii): $\gcd(10, -4) = 2$ uhodneme, řešíme $5x - 2y = 13$: $\gcd(5, 2) = 1 = 1 \cdot 5 + (-2) \cdot 2$, proto $\gcd(5, -2) = 1 = 1 \cdot 5 + 2 \cdot (-2)$, po vynásobení $5 \cdot 13 - 2 \cdot 26 = 13$. Řešení $(x, y) = (13 - (-2)k, 26 + 5k)$ neboli $x = 2k + 13$, $y = 5k + 26$ pro $k \in \mathbb{Z}$. Řešení v $\mathbb{N}_0$: $k \geq -5$.
(iv): $\gcd(105, 75) = 15$, $7x - 5y = 0$ homogenní rovnice. Řešení $(x, y) = (5k, 7k)$ neboli $x = 5k$, $y = 7k$ pro $k \in \mathbb{Z}$. Řešení v $\mathbb{N}_0$: $k \geq 0$.
(v): $\gcd(819, 315) = 63$, $13x + 5y = 2$. $\gcd(819, 315) = 63 = 2 \cdot 819 + (-5) \cdot 315$, proto $819 \cdot 4 + 315 \cdot (-10) = 126$. Řešení $(x, y) = (4 - 5k, -10 + 13k)$ neboli $x = 4 - 5k$, $y = 13k - 10$ pro $k \in \mathbb{Z}$. Řešení v $\mathbb{N}_0$: nelze.
(vi): $\gcd(65, 273) = 13$ nedělí 157. Nemá řešení.
4a.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 $3 \geq 34$, celkem 7 možností $(2, 30)$, $(5, 25)$, $(8, 20)$, $(11, 15)$, $(14, 10)$, $(17, 5)$, $(20, 0)$, $(0, 50)$.
4a.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.
4a.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.
4a.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.

4b. 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. Jako obvykle jsou nejjednodušší rovnice ty lineární, tentokráte najdeme něco zajímavého i na rovnici o jedné proměnné neboli $ax \equiv b \pmod{n}$.

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.

Jaká řešení se dají čekat? Jednu věc vidíme hned. Jestliže je x_0 nějaké řešení, tak máme platnou kongruenci $ax_0 \equiv 1 \pmod{n}$, ve které lze podle věty 3a.3 nahradit x_0 libovolným kongruentním číslem. Dostáváme tak nekonečnou množinu řešení $\{x_0 + kn : k \in \mathbb{Z}\}$. Je už to všechno? Příklady napoví, že ne nutně.

Například u kongruence $2x \equiv 6 \pmod{10}$ vidíme na první pohled řešení $x = 3$, máme tedy množinu řešení $\{3 + 10k : k \in \mathbb{Z}\}$, ale zkusmo se lze dobrat k tomu, že i $x = 8$ je řešením. Dostáváme tím novou nekonečnou

množinu řešení $\{8 + 10k : k \in \mathbb{Z}\}$, která je s tou předchozí disjunktní. Jsou ještě nějaká další řešení? Umíme je systematicky hledat? To jsou dobré otázky, na které si hned odpovíme.

Klíčem k úspěchu je zde jednoduché tvrzení.

Fakt 4b.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 $y_0 \in \mathbb{Z}$ řeší vektor (x_0, y_0) diofantickou rovnici $ax + ny = b$.

Důkaz: Dokážeme oba směry v ekvivalenci najednou.

$x_0 \in \mathbb{Z}$ je řešením právě tehdy, platí-li $ax_0 \equiv b \pmod{n}$. To je podle věty 3a.1 ekvivalentní existenci $y_0 \in \mathbb{Z}$ takového, že $b = ax_0 + y_0 n$. To ovšem znamená, že (x_0, y_0) řeší diofantickou rovnici $ax + ny = b$.

□

Stačí tedy najít všechna řešení rovnice $ax + ny = b$, načež ignorujeme složku y a ta x nám dají hledaná řešení lineární kongruence. Znamená to, že poznatky z předchozí části lze přímo přenést do naší situace. Výsledky 4a.1, 4a.2 a 4a.3 lze zkombinovat v následující tvrzení.

Věta 4b.2.
Nechť $n \in \mathbb{N}$, uvažujme $a, b \in \mathbb{Z}$.
(i) Jestliže b není násobkem $\gcd(a, n)$, tak řešení rovnice $ax \equiv b \pmod{n}$ neexistuje.
(ii) Jestliže $\gcd(a, n)$ dělí b, tak rovnice $ax \equiv b \pmod{n}$ má nějaké řešení $x_p \in \mathbb{Z}$.
Označme $n' = \frac{n}{\gcd(a,n)}$. Množina všech řešení lineární kongruence $ax \equiv b \pmod{n}$ je

$$\{x_p + kn' : k \in \mathbb{Z}\}.$$

Tento vzorec umožňuje přímý výpočet řešení, což je vhodné pro počítač a pro studenty, kteří si rádi pamatují vzorečky nazpaměť. Spíš bych doporučil převádět kongruenci na diofantickou rovnici a tu vyřešit oblíbeným způsobem, přičemž se ignoruje složka y.

Příklad 4b.a: Vyřešíme kongruenci $45x \equiv 9 \pmod{231}$.

Rovnici převedeme na diofantickou rovnici $45x + 231y = 9$. Tuto vyřešíme pomocí algoritmu 4a.9. 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.

a, b	y	x
231	1	0
45	0	1
6		-5
3		36
0		-77
9		108

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

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

Normálně bychom ve světě modula 231 mohli nahrazovat číslo 108 posunem o tuto hodnotu, což se nevyplatí. Vzorec pro obecné řešení ovšem naznačuje, že v tomto případě jsou možné posuny o 77, takže to vypadá, že je možné nabídnout příjemnější partikulární řešení než 108. Využijeme také možnosti změnit znaménko u k (ne že by to bylo nutné, ale sčítání je v mnoha směrech příjemnější operace než odčítání). Dospěli jsme tak k alternativnímu vzorci $x = 31 + 77k$, pro který si uděláme zkoušku:

$$45 \cdot (31 + 77k) = 1395 + 3465k = (231 \cdot 6 + 9) + 15 \cdot 231k \equiv 9 + 0k = 9 \pmod{231}.$$

Mimochodem, 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“.

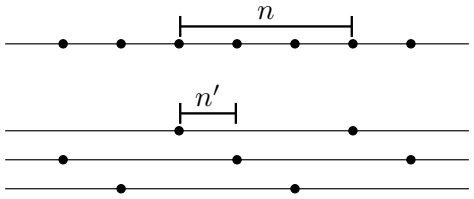
Poznamenejme ještě, že mnozí studenti dávají přednost mírně jinému postupu. Používají strukturovaný algoritmus, přičemž tabulku vytvoří celou, jak jsou zvyklí, a ignorování y nastoupí teprve ve fázi, kdy se z Bezoutovy rovnosti přechází k řešení. Zkušenost se zkouškami se zdá naznačovat, že tento postup je odolnější vůči chybám ze stresu. Proto jej nabízíme jako pracnější, ale možná bezpečnější variantu, ukázka je v příkladě 4c.a.

△

Podívejme se blíže na řešení, která jsme získali, vyjdeme ze vzorce $x = 31 + 77k$. Máme partikulární řešení 31 a jak jsme již diskutovali, z pravidel pro nahrazování ve světě modula okamžitě vyplývá, že čísla ve tvaru $31 + 231k$, $k \in \mathbb{Z}$ jsou všechna řešením dané rovnice. Máme tedy jednu kongruentní skupinu (zbytkovou třídu čísla 31), která poskytuje řešení, ale zjevně ne všechna, protože podle vzorce existuje i řešení $31 + 77 = 108$, které v dotyčné třídě neleží.

Stejnou úvahou dojdeme k tomu, že všechna čísla ze zbytkové třídy $\{108 + 231k : k \in \mathbb{Z}\}$ jsou řešeními, ale zase nám ještě zbývají některá další, protože i $108 + 77 = 185$ musí být řešení, ale zjevně nepatří do oněch dvou již vytvořených skupin.

Tak získáme třetí kongruentní skupinu řešení $\{185 + 77k : k \in \mathbb{Z}\}$. Čtvrtá již nebude. Když se totiž pokusíme posunout z čísla 185, dostaneme číslo $185 + 77 = 31 + 3 \cdot 77 = 31 + 231$, které je již obsaženo v první uvažované skupině. Další přičítání čísla 77 (či jeho odečítání) nás pak přesunuje mezi oněmi třemi skupinami řešení. Zkusíme to znázornit obrázkem.



Proč tohle děláme? Představme si, že žijeme ve světě modula 231. Kolik řešení rovnice vidíme? Protože v tomto světě považujeme navzájem kongruentní čísla za stejnou věc, tak vlastně při pohledu na množinu $\{31 + 231k\}$ nevidíme nekonečně mnoho čísel, ale jedno, třeba to 31, všechna ostatní jsou jen jiní zástupci téhož. Podobně to platí i o dalších zbytkových třídách, takže vlastně vidíme jen tři rozdílná řešení. Jejich zástupce lze vybrat tak, že z obecného řešení $x = 31 + 77k$ vygenerujeme libovolná tři čísla, která nejsou navzájem kongruentní, třeba 31, -46 a 670, a už budeme mít všechna řešení z pohledu světa modulo 231. Bývá ovšem zvykem brát tři po sobě následující čísla ze vzorce $31 + 77k$, pak automaticky nejsou navzájem kongruentní.

Bude něco takového fungovat obecně? Věta 4b.2 říká, že řešení přicházejí ve tvaru $x_p + \frac{n}{\gcd(a,n)}k$, $k \in \mathbb{Z}$. První skupina řešení je jasná, je to zbytková třída $\{x_p + nk : k \in \mathbb{Z}\}$. Pokud $\gcd(a, n) > 1$, tak číslo $x_p + \frac{n}{\gcd(a,n)}$ nemůže být kongruentní s x_p modulo n, tudíž získáme druhou skupinu řešení. Takto pokračujeme, dokud se od x_p neposuneme celkem o n. Je zjevné, že toto nastane, když číslo $\frac{n}{\gcd(a,n)}$ přičteme $\gcd(a, b)$ krát.

Protože se nám toto pozorování ještě bude hodit, shrneme to v oficiálním tvrzení.

Věta 4b.3.
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 $i = 0, 1, \ldots, \gcd(a, b) - 1$. Množina všech řešení dané kongruence je sjednocením množin $\{x_i + kn : k \in \mathbb{Z}\}$ pro $i = 0, 1, \ldots, \gcd(a, b) - 1$, tyto množiny jsou navzájem disjunktní.

O několik kapitol později se dozvíme, že situaci, kdy množinu rozdělíme na navzájem disjunktní části, se říká rozklad. My jsme zde získali rozklad množiny všech řešení na zbytkové třídy a brzy pro nás bude velmi užitečný. Z našich úvah také plyne, že rozsah indexů uvedený ve větě není jediný možný. Můžeme jako i vzít libovolných $\gcd(a, n)$ po sobě jdoucích celých čísel, spočítat si odpovídající x_i (ty pak nebudou navzájem kongruentní) a opět dostaneme rozklad množiny všech řešení na skupiny čísel kongruentní s těmito x_i.

Tímto končí praktická část o řešení kongruencí. Bylo to snadné, přetáhli jsme si to hlavní od diofantických rovnic. Teď si ovšem představme, že jsme žádné diofantické rovnice neprobrali a začali rovnou zkoumat lineární kongruence. Co by se dalo čekat? Slovo „lineární“ by nás navedlo k obdobným strukturálním větám jako v předchozí části, jen v jiném jazyce. Jmenovitě bychom čekali toto tvrzení.

Věta 4b.4.
Nechť $n \in \mathbb{N}$. Uvažujme rovnici $ax \equiv b \pmod{n}$ pro nějaká $a, b \in \mathbb{Z}$, nechť x_p je nějaké její řešení.
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 rovnice $ax \equiv 0 \pmod{n}$.

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

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

Platí rovněž to, že množina všech řešení homogenní rovnice je jakoby jednorozměrná, daná jedním „vektorem“, v tomto případě číslem x_h. Část odvození jsme nechali jako cvičení 4b.3. Máme zde tedy zase analogii s lineární algebrou a soustavami lineárních rovnic.

Ukažme si ještě jeden příklad.

Příklad 4b.b: Vyřešíme rovnici $30x \equiv 0 \pmod{33}$.

Přepis na diofantickou rovnici: $30x + 33y = 0$. Je to rovnice homogenní, proto stačí zkrátit a rovnou napíšeme řešení: Z rovnice $10x + 11y = 0$ dostáváme $x_h = 11k$, $y_h = -10k$. Ale vlastně jsme řešili kongruenci, tudíž y ignorujeme. Závěr: Obecné řešení dané kongruence je $x = 11k$, $k \in \mathbb{Z}$.

Jen tak mimochodem, jsou to celkem tři – viz $\gcd(30, 33)$ – disjunktní zbytkové třídy, dané například zástupci $0, 11, 22$.

To bylo až směšně snadné, proč to ukazujeme? Protože na řešení rovnic máme obecný algoritmus, který by si měl poradit i s tímto příkladem. Jak to pak bude fungovat? Máme začít Euklidovým algoritmem.

a, b	y	x
33	1	0
30	0	1
3	1	-1
0	-10	11

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 $\vert\, 0 \,\vert\, 0 \,\vert\, 0 \,\vert$.

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

△

Na závěr se zamyslíme nad jednou možností, jak si ulehčit život. U diofantických rovnic jsme v situaci, kdy jsme si všimli nějakého společného dělitelé všech čísel a, b, c, mohli rovnici zkrátit ještě předtím, než jsme spustili řešící proces. Co když si všimneme, že by šlo krátit v kongruenci $ax \equiv b$? Bohužel to ještě nestačí.

Lemma 4b.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 rovnici $ax \equiv b \pmod{n}$ právě tehdy, když řeší rovnici $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

Důkaz: $ax_0 \equiv b \pmod{n}$ právě tehdy, když existuje nějaké $y_0 \in \mathbb{Z}$, aby $ax_0 = b + y_0 n$, 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 modulus, je bezpečnější tohle prostě vypustit a případné krácení dělat až po převodu na diofantickou rovnici.

Cvičení

Cvičení 4b.1 (rutinní)**:** Vyřešte následující kongruence:
(i) $3x \equiv 7 \pmod{10}$; (iii) $84x \equiv -56 \pmod{308}$; (v) $6x \equiv 10 \pmod{8}$;
(ii) $12x \equiv 0 \pmod{20}$; (iv) $3x \equiv 7 \pmod{9}$; (vi) $11x \equiv 0 \pmod{40}$.

Cvičení 4b.2 (rutinní, poučné)**:** Nechť $n \in \mathbb{N}$, nechť $a, b \in \mathbb{Z}$. Uvažujme nějaké řešení x_p kongruence $ax \equiv b$.
(i) Dokažte, že když je i $x_0 \in \mathbb{Z}$ řešením této kongruence, tak číslo $x_h = x_0 - x_p$ řeší kongruenci $ax \equiv 0 \pmod{n}$.
(ii) Dokažte, že když $x_h \in \mathbb{Z}$ je řešením kongruence $ax \equiv 0 \pmod{n}$, tak $x_0 = x_p + x_h$ řeší kongruenci $ax \equiv b \pmod{n}$.

Cvičení 4b.3 (rutinní, poučné)**:** Nechť $n \in \mathbb{N}$, nechť $a \in \mathbb{Z}$. Dokažte, že jestliže x_h řeší kongruenci $ax \equiv 0$, tak také kx_h řeší kongruenci $ax \equiv 0$ pro libovolné $k \in \mathbb{Z}$.

Cvičení 4b.4 (rutinní, poučné)**:** Nechť $n \in \mathbb{N}$ a $c \in \mathbb{Z}$, předpokládejme, že $\gcd(c, n) = 1$. Dokažte, že jestliže $x, y \in \mathbb{Z}$ splňují $cx \equiv cy \pmod{n}$, pak $x \equiv y \pmod{n}$.
Vlastně tady dokazujeme, že ve světě modula lze v rovnicích krátit, ale jen invertibilními čísly. To odpovídá zkušenostem s rovnicemi v reálném světě, kde také lze krátit jen invertibilními (tedy nenulovými) čísly.

Cvičení 4b.5 (dobré, poučné)**:** Nechť $n \in \mathbb{N}$ a $c \in \mathbb{Z}$, předpokládejme, že $\gcd(c, n) > 1$. Dokažte, že pak existují $x, y \in \mathbb{Z}$ takové, že $cx \equiv cy \pmod{n}$, ale neplatí $x \equiv y \pmod{n}$.

Řešení:
4b.1: (i): $7 = 3x + 10y$, evidentně $\gcd(3, 10) = 1 = (-3) \cdot 3 + 1 \cdot 10$ (lze uhádnout), vynásobíme Bezouta sedmi, $7 = 3 \cdot (-21) + 7 \cdot 10$, tedy $x = -21$ je řešení.
Rovnice $3x + 10y = 0$ má řešení $x_h = 10k$, proto řešení dané rovnice je $x = -21 + 10k$, $k \in \mathbb{Z}$. Kdo chce, použije $x = 9 + 10k$, $k \in \mathbb{Z}$.

(ii): $12x + 20y = 0$, je už homogenní. Evidentně $\gcd(12, 20) = 4$, zkrátíme, $3x \equiv 0 \pmod 5$ má řešení $x = 5k$, $k \in \mathbb{Z}$.
(iii): $-56 = 84x + 308y$, Euklidem $\gcd(308, 84) = 28 = (-1) \cdot 308 + 4 \cdot 84$, protože $\frac{-56}{28} = -2 \in \mathbb{Z}$, má rovnice řešení, vynásobíme Bezouta tou mínus dvojkou, $-56 = 84 \cdot (-8) + 2 \cdot 308$, tedy $x = -8$ je řešení.
Rovnice $84x+308y = 0$ se vydělí 28 na $3x+11y = 0$, má řešení $x_h = 11k$, proto řešení dané rovnice je $x = -8+11k$, $k \in \mathbb{Z}$. Kdo chce, použije $x = 3 + 11k$, $k \in \mathbb{Z}$.
(iv): protože $\gcd(3, 9) = 3$ a 7 není násobkem 3, rovnice nemá řešení.
(v): $10 = 6x + 8y$, evidentně $\gcd(6, 8) = 2 = (-1) \cdot 6 + 1 \cdot 8$ (lze uhádnout), rovnice má řešení, neboť $\frac{10}{2} = 5 \in \mathbb{Z}$, vynásobíme Bezouta tou pětkou, $10 = 6 \cdot (-5) + 5 \cdot 8$, tedy $x = -5$ je řešení.
Rovnice $6x + 8y = 0$ se vydělí 2 na $3x + 4y = 0$, má řešení $x_h = 4k$, proto řešení dané rovnice je $x = -5 + 4k$, $k \in \mathbb{Z}$. Kdo chce, použije $x = 3 + 4k$, $k \in \mathbb{Z}$.
(vi): Protože $\gcd(11, 40) = 1$, je množina řešení $x = 40k$, $k \in \mathbb{Z}$.
4b.2: (i): $a(x_0 - x_p) = ax_0 - ax_p \equiv b - b = 0 \pmod n$.
(ii) je podobné.
4b.3: $a(kx_h) = k \cdot (ax_h) \equiv k \cdot 0 = 0 \pmod n$.
4b.4: Podle věty 3a.7 má c inverzní prvek c^{-1} modulo n, díky kterému lze počítat
$x = 1x \equiv (c^{-1}c)x \equiv c^{-1}(cx) \equiv c^{-1}(cy) \equiv 1y = y \pmod n$.
Důkaz pomocí přepisu kongruence je možný, ale obsahuje problém: Pro nějaké $k \in \mathbb{Z}$ platí $cy = cx + kn$, tedy $kn = c(y - x)$. Protože $x - y \in \mathbb{Z}$, číslo c dělí kn. Máme $\gcd(c, n) = 1$, lemma 2b.19) dává $c \mid k$. Tedy $k = cl$ pro $l \in \mathbb{Z}$, tedy $c(y - x) = cln$. Chceme zkrátit celé číslo c, není náhodou nula?
Pozor! Kdyby $n = 1$, tak jsou všechna čísla navzájem kongruentní, proto $x \equiv y \pmod n$.
Případ $n \geq 2$: Jelikož $\gcd(0, n) = n \geq 2$, nevyhovuje nula podmínce $\gcd(c, n)$ a tedy opravdu $c \neq 0$. Vykrátíme rovnici, $y - x = ln$, kde $l \in \mathbb{Z}$, proto $x \equiv y \pmod n$.
4b.5: Označme $d = \gcd(c, n)$, pak $c = dk$ a $n = dm$ pro $k, m \in \mathbb{Z}$. Protože $d > 1$, je $m < n$. Hledáme $x, y \in \mathbb{Z}$ tak, aby $c(y - x)$ bylo násobkem n, ale $y - x$ ne. Ovšem c už má „kousek n“ v sobě, stačí tedy zařídit, aby se v rozdílu $y - k$ objevilo m, ale ne celé n.
Zvolme například $x = 0$ a $y = m$. Pak $0 < y - x = n < m$, jsou to tedy nekongruentní čísla. Ale $c(y - x) = dkm = k(dm) = kn$.

4c. Rovnice v prostorech $\mathbb{Z}_n$

Zvolíme modulus $n \in \mathbb{N}$ a přesuneme se do konečného světa $\mathbb{Z}_n$. I v něm se omezíme na nejjednodušší typ, lineární rovnici jedné proměnné.

Uvažujme tedy rovnici $a \odot x = b$, kde $a, b \in \mathbb{Z}_n$. Hledáme řešení $x_0 \in \mathbb{Z}_n$. Vyjdeme-li z definice násobení, hledáme x_0 splňující $(a \cdot x_0) \bmod n = b$. Protože $b \in \mathbb{Z}_n$, je $b = b \bmod n$, máme tedy $(a \cdot x_0) \bmod n = b \bmod n$, čísla ax_0 a b mají stejný zbytek po dělení modulem n. Podle věty 3a.1 vychází, že $ax_0 \equiv b \pmod n$. Právě jsme odvodili následující:

• Jestliže $x_0 \in \mathbb{Z}_n$ řeší rovnici $a \odot x = b$ v $\mathbb{Z}_n$, pak x_0 musí řešit kongruenci $ax \equiv b \pmod n$.

Z praktického pohledu to znamená, že nemá smysl hledat řešení dané rovnice jinde než mezi řešeními oné kongruence. Jak to tedy s nimi vypadá?

Vezměme nějaké řešení x_0 kongruence $ax \equiv b \pmod n$. Podle věty 3a.1 pak $(a \cdot x_0) \bmod n = b \bmod n$, díky $b \in \mathbb{Z}_n$ tedy $(a \cdot x_0) \bmod n = b$. Teď bychom strašně rádi na levé straně napsali $a \odot x_0$, ale tato operace je definována pouze pro čísla ze $\mathbb{Z}_n$. O čísle x_0 to nevíme a s vysokou pravděpodobností tam ani neleží.

Naštěstí je nám u kongruence povoleno ve výpočtech nahradit čísla zástupci. Kongruenci $ax \equiv b \pmod n$ tedy řeší i číslo $r = x_0 \bmod n \in \mathbb{Z}_n$, s ním se stejným způsobem dostaneme k rovnosti $(a \cdot r) \bmod n = b$. Tu jsme již oprávněni přepsat jako $a \odot r = b$ v $\mathbb{Z}_n$ a máme řešení. Dostáváme následující.

• Je-li $x_0 \in \mathbb{Z}$ řešením kongruence $ax \equiv b \pmod n$, pak zbytek po dělení $r = x_0 \bmod n$ řeší rovnici $a \odot x = b$ v $\mathbb{Z}_n$.

Tyto dva poznatky lze shrnout do následujícího pozorování:

• Množinu všech řešení rovnice $a \odot x = b$ v $\mathbb{Z}_n$ získáme tak, že nahradíme v množině všech řešení kongruence $ax \equiv b \pmod n$ všechna čísla jejich zbytky po dělení n neboli jejich kongruentními zástupci z množiny $\mathbb{Z}_n$.

Východiskem je věta 4b.3. Uvažujme jednu konkrétní zbytkovou třídu $\{x_i + kn : k \in \mathbb{Z}\}$. Protože jsou všechna tato čísla navzájem kongruentní modulo n, budou mít i stejné zbytky po dělení. To znamená, že se při onom přechodu ke zbytkům celá skupina změní v jedno číslo, třeba to, které získáme z x_i. V předchozí sekci jsme komentovali, že ve světě modulo vidíme tuto nekonečnou množinu řešení jako jedno číslo (s mnoha možnými zástupci). Přechodem do $\mathbb{Z}_n$ se tento dojem stává realitou, z množiny už je jen jedno číslo.

Toto samozřejmě platí pro všechny skupiny, takže vidíme, že množinu všech řešení rovnice $\mathbb{Z}_n$ lze získat tak, že si najdeme zbytky oněch čísel x_i. Protože byla zvolena tak, aby nebyla navzájem kongruentní modulo n, získáme tak $\gcd(a,n)$ různých řešení ze $\mathbb{Z}_n$. Protože jsme měli při volbě zástupců x_i určitou svobodu, nabízí se nápad, že je rovnou vybereme tak, aby byly ze $\mathbb{Z}_n$. Vyzkoušíme si to, nejprve ještě jedna věc.

Úmluva. V dalším textu budeme pro operace v prostoru $\mathbb{Z}_n$ používat běžné značky $\cdot$ a $+$.

Při praktickém počítání to bývá zvykem, je to mnohem příjemnější na čtení i psaní. Problém nastává jen v teoretických úvahách, kde je třeba pečlivě rozlišovat, o kterých operacích se mluví. Zkušený matematik si to odvodí z kontextu.

Příklad 4c.a: Vyřešíme rovnici $42x = 18$ v $\mathbb{Z}_{180}$.

Přepíšeme si ji jako kongruenci $42x \equiv 18 \pmod{180}$, ze které pak přecházíme k diofantické rovnici $42x + 180y = 18$. Řešíme ji tradičně tabulkou.

a, b	y	x
180	1	0
42	0	1
12	1	-4
6	-3	13
0	7	-30
18	-9	39

Vidíme v ní informace k napsání obecného řešení, ale nás zajímá jen proměnná u 42 neboli x, tabulka dává $x_p = 39$, $x_h = -30$. Dostáváme obecné řešení $x = 39 - 30k$, $k \in \mathbb{Z}$ kongruence $42x \equiv 18 \pmod{180}$.

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

Tato množina řešení se rozpadne na celkem $\gcd(42, 180) = 6$ skupin (zbytkových tříd), jmenovitě jde o skupiny $\{9 + 180k : k \in \mathbb{Z}\}$, $\{39 + 180k : k \in \mathbb{Z}\}$, $\{69 + 180l : k \in \mathbb{Z}\}$, $\{99 + 180k : k \in \mathbb{Z}\}$, $\{129 + 180l : k \in \mathbb{Z}\}$ a $\{159 + 180k : k \in \mathbb{Z}\}$. Mimochodem, vidíme, že další posun by nás dostal k číslu 189, které už opravdu patří do první skupiny, vše souhlasí.

Když u každé ze skupin přejdeme ke zbytkům modulo 180, dostáváme čísla $9, 39, 69, 99, 129, 159$. Tato čísla jsou řešeními rovnice $42x = 18$ v $\mathbb{Z}_{180}$.

Závěr: Množina všech řešení rovnice $42x = 18 \pmod{180}$ je $\{9, 39, 69, 99, 129, 159\}$. Lze ji také zapsat jako $\{9 + 30k : k = 0, 1, \dots, 5\}$, což se bude hodit, až někdy vyjde $\gcd(a, n)$ jako velké číslo.

Poznámka: Záměrně jsme volili podrobnější řešení, které sledovalo naše předchozí úvahy. Zkušený řešič by patrně některé fáze zkrátil.

△

Postup si shrneme v oficiálním tvrzení.

Věta 4c.1.
Nechť $n \in \mathbb{N}$, uvažujme rovnici $ax = b$ v $\mathbb{Z}_n$ pro nějaká $a, b \in \mathbb{Z}_n$.
(i) Jestliže $\gcd(a, n)$ nedělí b, pak řešení neexistuje.
(ii) Předpokládejme, že $\gcd(a, n)$ dělí b. Nechť $x_p \in \mathbb{Z}$ řeší kongruenci $ax \equiv \pmod{n}$, označme $n' = \frac{n}{\gcd(a,n)}$.
Nechť $x_0 = \min\{x_p + kn' : k \in \mathbb{Z} \text{ a } x_p + kn' \geq 0\}$. Pak množina všech řešení rovnice $ax = b$ v $\mathbb{Z}_n$ je

$$\{x_0 + in' : i = 0, 1, \dots, \gcd(a, n) - 1\}.$$

Jde o $\gcd(a, n)$ různých čísel.

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

Pokud by rovnice $ax = b$ měla řešení v $\mathbb{Z}_n$, tak by (viz výše) bylo i řešením pro kongruenci $ax \equiv b \pmod{n}$. Podle věty 4b.2 pak $\gcd(a, n)$ musí dělit b.

(ii): 1) Nejprve ukážeme, že všechna uvedená čísla jsou řešením. Označme jako k_0 číslo, které vytvořilo $x_0 + k_0 n'$.

Víme z předchozí sekce, že čísla ve tvaru $x_p + kn'$ pro $k \in \mathbb{Z}$ řeší kongruenci $ax \equiv b \pmod{n}$. Platí to tedy i pro čísla $x_0 + in' = x_p + (k_0 + i)n'$. Podle našich předchozích pozorování proto jejich zbytky $(x_0 + in') \bmod n$ řeší rovnici $ax = b$ v $\mathbb{Z}_n$. Zbývá ukázat, že čísla samotná leží v množině $\mathbb{Z}_n$.

Podle volby je $x_0 \geq 0$, díky $n' > 0$ pak $x_0 + in' \geq 0$. Ještě potřebujeme omezení shora. Začneme pozorováním, že $x_0 < n'$. V opačném případě by totiž platilo $x_0 - n' \geq 0$, což odporuje definici x_0 jako nejmenšího nezáporného čísla daného typu. Můžeme pak odhadovat

$$x_0 + in' \leq x_0 + (\gcd(a, n) - 1)n' < n' + (\gcd(a, n) - 1)n' = \gcd(a, b)n' = n,$$

tedy čísla jsou opravdu ze $\mathbb{Z}_n$.

2) Že jde o $\gcd(a,b)$ různých čísel vyplývá z toho, že $n' \neq 0$, tedy pro $i \neq j$ je i $x_0 + in' \neq x_0 + jn'$. Zde hraje rovněž roli výsledek části 1), že jde o čísla přímo ze $\mathbb{Z}_n$, tudíž se nemusíme obávat, že bychom pro různá i, j nakonec skončili se stejným číslem po nuceném přechodu ke zbytkům.

3) Nakonec ukážeme, že každé řešení dané rovnice lze v tomto seznamu najít.

Uvažujme tedy řešení $\tilde{x} \in \mathbb{Z}_n$ rovnice $ax = b$ v $\mathbb{Z}_n$. Ukázali jsme, že pak musí řešit kongruenci $ax \equiv b \pmod{n}$. Z věty 4b.2 plyne, že pak $x = x_p + lx_h$ pro nějaké $l \in \mathbb{Z}$. Pak ovšem

$$\tilde{x} = x_p + ln' = x_0 - k_0 n' + ln' = x_0 + (l - k_0)n' = x_0 + mn',$$

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

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

Víme také, že $0 \leq x_0$ a $\tilde{x} \in \mathbb{Z}_n$, tedy $\tilde{x} < n = \gcd(a,n) \cdot n'$. Proto můžeme odhadovat

$$mn' = \tilde{x} - x_0 < \gcd(a,n)n'.$$

Vydělením kladným číslem n' vychází $m < gcd(a,n)$. Shrnuto, řešení $\tilde{x}$ lze zapsat jako $x_0 + mn'$, kde $m \in \{0, 1, \ldots, \gcd(a,n)\}$, tedy toto x je v našem seznamu.

□

Jako obvykle není nutné sledovat přesně algoritmus zachycený v této větě. Je například možné nezavádět speciální řešení x_0, ale pracovat s odpovídajícím startovacím indexem $k_0 = \min\{k : x_p + kn' \geq 0\}$ a poskytnout množinu řešení ve tvaru

$$\{x_p + kn' : k = k_0, k_0 + 1, \ldots, k_0 + \gcd(a,h) - 1\}.$$

Komu se nelíbí odečítání jedničky, může to zkusit ještě jinak. Rozmyslete si, že následující postup dá stejný výsledek: Nejprve určíme konstantu $K = \max\{k \in \mathbb{Z} : x_p + Kn' < 0\}$ a pak sestavíme množinu

$$\{x_p + kn' : k = K + 1, K + 2, \ldots, K + \gcd(a,h)\}.$$

Přístupu z věty by odpovídalo, že si najdeme $x_0 = \max\{x_p + kn' : k \in \mathbb{Z} \text{ a } x_p + kn' < 0\}$ a pak použijeme množinu

$$\{x_0 + kn' : k = 1, 2, \ldots, \gcd(a,h)\}.$$

Podstatné je, abychom nakonec měli $\gcd(a,n)$ čísel z rozmezí $0, 1, \ldots, n-1$. V praxi člověk prostě dělá, co potřebuje, jen si tu trénujeme matematický zápis.

Na závěr ještě jeden příklad, řešení bude stručnější.

Příklad 4c.b: Vyřešte rovnici $14x = 38$ v $\mathbb{Z}_{40}$.

Přeložíme si ji jako $14x + 40y = 38$ pro $x, y \in \mathbb{Z}$. Použijeme pohodlný algoritmus pro diofantické rovnice.

Ignorujeme y, dostáváme množinu řešení $x = 57 + 20k$. Pomocí $n' = 20$ najdeme lepšího zástupce 17 a jsme připraveni.

Daná rovice má řešení $x = 17, 37$.

a/b	y	x
40	1	0
14	0	1
−2	1	−3
0	7	−20
38	−19	57

△

Cvičení

Cvičení 4c.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 4c.2 (rutinní)**:** Vyřešte následující rovnice v daném $\mathbb{Z}_n$:
(i) $12x = 18$ v $\mathbb{Z}_{42}$; (iii) $10x = 0$ v $\mathbb{Z}_{35}$; (v) $84x = 126$ v $\mathbb{Z}_{210}$;
(ii) $9x = 7$ v $\mathbb{Z}_{20}$; (iv) $8x = 10$ v $\mathbb{Z}_{12}$; (vi) $8x = 0$ v $\mathbb{Z}_{12}$;

Cvičení 4c.3 (dobré)**:** Uvažujme rovnici $(6 - t)x = 24$ v Z_{40}. Pro které hodnoty t z rozmezí $0, \ldots, 5$ má tato rovnice
a) přesně čtyři řešení? b) přesně tři řešení? c) přesně pět řešení? d) žádné řešení?

Řešení:
4c.1: Podmínka je $\gcd(a,n) \,|\, b$. a): $\gcd(25, 168) = 1$, $1 \,|\, 13$, ano. b): $\gcd(30, 168) = 6$, $6 \,|\, 12$, ano. c): $\gcd(30, 168) = 6$, neplatí $6 \,|\, 15$, ne. d): $\gcd(16, 168) = 8$, $8 \,|\, 24$, ano.
4c.2: (i): $18 = 12x + 42y$, $\gcd(42, 12) = 6 = 1 \cdot 42 + (-3) \cdot 12$, vynásobíme trojkou, $18 = (-9) \cdot 12 + 3 \cdot 42$, tedy $x_p = -9$.

Rovnice $12x+42y=0$ se vykrátí na $2x+7y=0$, má řešení $x_h=7k$, proto řešení kongruenční rovnice $x=-9+7k$. Je $\gcd(42,12)=6$ řešení v $\mathbb{Z}_{42}$, $x=5+7k$ pro $k=0,1,\dots,5$ neboli $\{5,12,19,26,33,40\}$.
(ii): $9x+20y=7$, $\gcd(20,9)=1=(-4)\cdot 20+9\cdot 9$, vynásobíme na $7=9\cdot 63+(-28)\cdot 20$, tedy $x_p=63$.
Rovnice $9x+20y=0$ má řešení $x_h=20k$, proto $x=63+20k$. Je $\gcd(20,9)=1$ řešení v $\mathbb{Z}_{20}$, $x=3$.
(iii): $10x+35y=0$, uhodneme $\gcd(35,10)=5$, 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 $\{0,7,14,21,28\}$.
(iv): $8x+12y=10$, $\gcd(12,8)=4=1\cdot 12+(-1)\cdot 8$, protože 4 nedělí 10, rovnice nemá řešení.
(v): $84x+210y=126$, $\gcd(210,84)=42=1\cdot 210+(-2)\cdot 84$, vynásobíme na $126=(-6)\cdot 84+3\cdot 210$, tedy $x_p=-6$.
Rovnice $84x+210y=0$ na $3x+5y=0$, má řešení $x_h=5k$, proto řešení kongruenční rovnice je $x=-6+5k$. Je $\gcd(210,84)=42$ řešení v $\mathbb{Z}_{210}$, $x=4+5k$ pro $k=0,1,\dots,41$, neoficiálně $\{4,9,14,19,\dots,204,209\}$.
(vi): $8x+12y=0$, 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 $\{0,3,6,9\}$.
4c.3: Počet řešení je roven $\gcd(a,n)$, ale musí platit $\gcd(a,n)\mid b$. a): Potřebujeme $\gcd(6-t,40)=4$, pak také $4\mid 24$, to platí pro $t=2$.
b): Potřebujeme $\gcd(6-t,40)=3$, to není možné.
c): Potřebujeme $\gcd(6-t,40)=5$, nastane pro $t=1$, ale neplatí $5\mid 24$, takže žádné řešení.
d): Žádné řešení nastane, když $\gcd(6-t,40)$ nedělí 24. Protože $40=8\cdot 5$ a $6-t\le 6$, možná gcd jsou $2,4,5$. Z nich jen 5 nedělí 24, u ostatních budou řešení. Závěr: Žádné řešení nebude pro $t=1$.

4d. 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 klasikou.

Věta 4d.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 rovnice. Těmi začneme, jsou snadné.

Uvažujme tedy soustavu rovnic

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

Každá z těchto rovnic vyžaduje, aby x bylo násobkem příslušného modulu, takže vlastně hledáme taková x, která jsou společnými násobky všech modulů n_i. To jsou přesně čísla ve tvaru $x=k\,\mathrm{lcm}(n_1,n_2,\dots,n_m)$ pro $k\in\mathbb{Z}$. Homogenní soustavy tedy umíme snadno vyřešit.

Od této chvíle se omezíme na speciální případ, kdy jsou n_i po dvou nesoudělné, tedy pro $i \neq j$ platí $\gcd(n_i, n_j) = 1$. Pro homogenní rovnici hned získáme pěkné řešení.

Fakt 4d.2.
Uvažujme moduly $n_1, n_2, \dots, n_m \in \mathbb{N}$. Předpokládejme, že tato čísla jsou po dvou nesoudělná. Pak číslo $x_0 \in \mathbb{Z}$ splňuje kongruence $x \equiv 0 \pmod{n_i}$ pro všechna $i = 1, \dots, m$ právě tehdy, když je x_0 násobkem čísla $n_1 \cdot n_2 \cdots n_m$.

Využili jsme vztah $\operatorname{lcm}(n_1, \dots, n_m) = n_1 \cdot n_2 \cdots n_m$, viz cvičení 2b.5.

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

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

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

Nápad: Použijeme $x = b_1 + b_2 kn_1$. Z pohledu modula n_1 je pořád vše při starém, ale pokoušíme se v druhém členu mít pohledem modula n_2 číslo b_2. Aby to vyšlo, muselo by být $kn_1 = 1 \pmod{n_2}$. My jsme si ale mohli zatím volit k libovolně, takže si teď to správné vybereme, pokud ovšem existuje. Vlastně chceme, aby k bylo inverzní číslo k n_1 modulo n_2. To díky předpokladu o nesoudělnosti n_1, n_2 máme, nazvěme jej x_2.

Výraz $b_2 x_2 n_1$ teď dělá přesně, co chceme, modulo n_1 dává $(b_2 x_2) \cdot n_1 \equiv 0$ a modulo n_2 dává $b_2 \cdot (x_2 n_1) \equiv b_2 \cdot 1 = b_2$.Teď ještě potřebujeme zařídit, aby se obdobně choval první výraz, ale to zařídíme podobně. Dostáváme lepší verzi $x = b_1 x_1 n_2 + b_2 x_2 n_1$, kde se x_1 je inverzní číslo k n_2 modulo n_1.

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

	$b_1 x_1 n_2 n_3$	$b_2 x_2 n_1 n_3$	$b_3 x_3 n_1 n_2$
n_1	b_1	0	0
n_2	0	b_2	0
n_3	0	0	b_3

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

Aby šly tyto prvky najít, musí být vždy n_i nesoudělné se součinem ostatních modulů, teď vidíme, proč jsme se omezili na tento speciální případ. Máme nápad, který zdá se funguje.

Věta 4d.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 rovnic

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

Jestliže jsou všechna čísla n_i po dvou nesoudělná, pak má tato soustava řešení $x_0 \in \mathbb{Z}$. Množina všech řešení je $\{x_0 + kn : k \in \mathbb{Z}\}$, 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 2b.26 pak $\gcd(N_i, n_i) = 1$. Proto existuje inverzní číslo x_i k N_i vzhledem k násobení modulo n_i. Nechť $x_0 = \sum_{i=1}^{m} b_i N_i x_i$. Tvrdíme, že je to řešení dané soustavy.

Zvolme i. Pro $j \neq i$ pak $n_i \mid N_j$, proto $N_j \equiv 0 \pmod{n_i}$, tedy i $(b_j N_j x_j) \equiv 0 \pmod{n_i}$. Následně modulo n_i dostaneme $x_0 \equiv b_i N_i x_i \equiv b_i \cdot 1 = b_i \pmod{n_i}$.

2) Tvar množiny všech řešení vyplývá z věty a faktu výše.

□

Mnozí autoři namísto tvrzení o množině všech řešení preferují zakončit Čínskou větu 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 $y - x_0$ řeší přidruženou homogenní soustavu, proto podle faktu máme $y - x_0 = kn$ pro nějaké $k \in \mathbb{Z}$. Pak $y \equiv x_0 \pmod{n}$.

Důkaz věty dává algoritmus.

S Algoritmus 4d.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. Označte $n = n_1 n_2 \cdots n_m$ a $N_i = \dfrac{n}{n_i}$ pro všechna i.

2. Pro každé i najděte inverzní číslo k N_i vzhledem k násobení modulo n_i, viz algoritmus 3b.6.

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

△

Příklad 4d.a: Větě se říká čínská, protože soustavy kongruencí jdou zpět ke starým Číňanům někam do 3. století. Asi nejznámější je následující úloha z klasické knihy *Matematický manuál* mistra Sun-Tzu (to byl matematik, neplést se stejnojmenným autorem klasické knihy o vojenské strategii známe jako *The Art of War*).

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

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

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

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

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

21		1	0
5	4	0	1
1•	5	1•	−4•
0			

15		1	0
7	2	0	1
1•	7	1•	−2•
0			

Dostáváme následující:

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

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

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

Ty poslední dva se daly odhadnout i bez výpočtu.

Dosadíme do vzorce a dostáváme $x_p = 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 140 + 63 + 30 = 233$. Víme, že jsou možné posuny o $3 \cdot 5 \cdot 7 = 105$, tak můžeme vzít lepšího zástupce 23 jako partikulární řešení.

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

△

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

Jako obvykle se při ručním výpočtu nabízejí zkratky. Ta nejužitečnější je, že když pracujeme s konkrétní rovnicí, tak dočasně vnímáme vše pohledem příslušného modula. To znamená, že si můžeme upravit danou rovnici a také nahrazovat ve výpočtech. Například druhou rovnici můžeme nahradit kongruencí $x \equiv -2 \pmod{3}$. To se asi nevyplatí, ale když pak pro odpovídající člen hledáme x_2, můžeme v rovnici $21x_2 \equiv 1 \pmod{5}$ nahradit dvacet jedničku kongruentním zástupcem a řešit $1 \cdot x \equiv 1 \pmod{5}$, což už stojí za to.

Příklad 4d.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 rovnice, 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 si to také uděláme. Pro vytváření jednotlivých členů řešení použijeme systematický zápis, který některým (třeba mi) vyhovuje. U rovnic pro inverzní čísla přejdeme k přijemnějším verzím.

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

Inverze x_i jsme uhádli, to je často možné, v případě nouze si bokem uděláme tabulky pro rozšířený Euklidův algoritmus. Máme také $n = 5\cdot 6\cdot 7 = 210$, nabízí se lepší reprezentant $413 - 210 = 203$.

Dostáváme množinu řešení $x = 203 + 210k$ pro $k \in \mathbb{Z}$.

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 rovnice už dodala trojku, stačí tedy dodat jen 2 a 7, tedy pracovat pracovat se členem $3\cdot 2\cdot 7x_1$. Máme pak požadavek $14x_1 \equiv 1 \pmod 5$. Z tohoto pohledu se může vyplatit přepis druhé rovnice do tvaru $x \equiv 5 \pmod 6$, protože pak druhý člen nemusí být $5\cdot 5\cdot 7x_2$, ale stačí $5\cdot 7x_2$, kde $7x_2 \equiv 1 \pmod 6$.

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

△

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 kapitola 17b. Určitě patří do základního arsenálu computer science.

Tímto jsme probrali to hlavní o soustavách kongruencí. Jako bonus se podíváme na další možnosti, jak řešit soustavy kongruencí. Dopředu přiznáváme, že to není nic extra praktického, ale je to docela zajímavé a taky dobrá rozcvička pro hlavu.

4d.5 Bonus: Více o soustavách 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, pokud chceme rovnice řešit systematicky a najednou. Proto se také tento případ neuvažuje, naštěstí nám v aplikacích nechybí.

Menší komplikací je situace, kdy sice máme rovnice typu $x \equiv b_i \pmod{n_i}$, ale moduly n_i nejsou po dvou nesoudělné. O tom, že jde o výrazně příjemnější případ, svědčí například to, že existuje rozumná podmínka pro existenci řešení.

Věta 4d.6.
Nechť $n_1, n_2, \dots, n_m \in \mathbb{N}$, $b_1, b_2, \dots, b_m \in \mathbb{Z}$. Soustava rovnic

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

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 $\operatorname{lcm}(n_1, \dots, n_m)$. Na rozdíl od nesoudělných modulů už ovšem nemáme pěkný vzorec pro nalezení řešení. Ani tento případ se obvykle neprobírá.

Na závěr zmíníme dvě metody, které se dají použít. Obojí ukážeme na příkladě.

Eliminace.

Vraťme se k příkladu 4d.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 rovnici. Jak vypadají její řešení? Na to máme algoritmus.

Hned vidíme $x_p = 2$, ještě potřebujeme vyřešit $x + 3y = 0$, což dává $x_h = 3k$. Máme tedy $x = 2 + 3k$, $k \in \mathbb{Z}$. Mezi těmito čísly pak budeme hledat řešení dalších dvou rovnic, což matematicky zachytíme známým způsobem,

toto x do nich dosadíme.

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

Dostáváme soustavu, která už nemá u x jedničky, ale to nevadí, stejně nechceme použít čínský algoritmus. Vyřešíme první kongruenci obvyklým způsobem, dostaneme $k_0 = 2$ a posléze $k = 2+5l$ pro $l \in \mathbb{Z}$. Dosadíme do třetí rovnice:

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

Dostáváme $l = 1 + 7m$ pro $m \in \mathbb{Z}$. Teď provedeme zpětnou substituci:

$$k = 2 + 5l = 2 + 5(1+7m) = 7 + 35m \implies x = 2 + 3k = 2 + 3(7+35m) = 23 + 105m,\ m \in \mathbb{Z}.$$

Dospěli jsme ke stejnému výsledku.

Je jasné, jak bychom řešili soustavy s více rovnicemi, prostě bychom snižovali po jedné, po vyčerpání latinské abecedy bychom parametry začali značit písmeny řeckými, hebrejskými atd. Protože v každém kroku řešíme kongruenci, dokážeme takto zvládnout obecné soustavy včetně typu $a_i x \equiv b_i \pmod{n_i}$ (pokud tedy mají řešení). Je ale zjevné, že pro větší soustavy to není perspektivní metoda.

Rozklad modula.

Tato metoda se dokáže vypořádat s případem, kdy u rovnic typu $x \equiv b_i \pmod{n_i}$ nejsou moduly po dvou nesoudělné. Použijeme příklad $x \equiv 2 \pmod{24}$, $x \equiv 6 \pmod{20}$ a $x \equiv 8 \pmod{30}$.

Krok 1: Všechny moduly rozložíme na mocniny prvočísel, pak každou kongruenci přepíšeme pomocí lemma 3a.13.

$$\begin{aligned} x \equiv 2 \pmod{3\cdot 2^3} &\iff \left[\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod{2^3} \end{aligned}\right. \\ x \equiv 6 \pmod{2^2\cdot 5} &\iff \left[\begin{aligned} x &\equiv 6 \pmod{2^2} \\ x &\equiv 6 \pmod 5 \end{aligned}\right. \\ x \equiv 8 \pmod{2\cdot 3\cdot 5} &\iff \left[\begin{aligned} x &\equiv 8 \pmod 2 \\ x &\equiv 8 \pmod 3 \\ x &\equiv 8 \pmod 5 \end{aligned}\right. \end{aligned}$$

Původní soustava tří kongruencí je tedy ekvivalentní soustavě sedmi kongruencí.

Krok 2: Nyní je třeba konsolidovat rovnice 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 splňují i druhou rovnici. Podobně $x = 2 + 2\cdot(4k) \equiv 2 + 0 \equiv 8 \pmod 2$ a splňují i třetí rovnici. Vidíme, že první tři rovnice lze nahradit rovnicí $x \equiv 2 \pmod{2^3}$.

$x \equiv 2 \pmod{2^3}$
$x \equiv 6 \pmod{2^2}$
$x \equiv 8 \pmod 2$
$x \equiv 2 \pmod 3$
$x \equiv 8 \pmod 3$
$x \equiv 6 \pmod 5$
$x \equiv 8 \pmod 5$

Nyní se podíváme na rovnice s modulem 3. Jsou dvě, ale $8 \equiv 2 \pmod 3$, čili vlastně jde o tutéž rovnici. Vezmeme si dále jednu z nich.

Zatím se nám podařilo první dvě skupiny zkonsolidovat do soustavy dvou rovnic $x \equiv 2 \pmod{2^3}$ a $x \equiv 2 \pmod 3$, kde už jsou modula po dvou nesoudělné.

Jako poslední jsou na řadě rovnice s pětkovým modulem. Hledaná x mají splňovat $x \equiv 6 \pmod 5$ a $x \equiv 8 \pmod 5$, což není zároveň možné, protože neplatí $6 \equiv 8 \pmod 5$. Soustava tedy nemá řešení.

Udělejme tedy změnu, v zadání u třetí rovnice uvažujme $x \equiv 26 \pmod{30}$. Jak by se změnilo naše řešení?

U tří rovnic s dvojkovým základem bychom měli $x \equiv 26 \pmod 2$, což lze nahradit kongruencí $x \equiv 0 \pmod 6$, což je splněno v případě $x = 2 + 8k$. Pořád bychom tedy dvojkové rovnice nahradili rovnicí $x \equiv 2 \pmod{2^3}$.

Protože $26 \equiv 2 \pmod 3$, i druhá část kroku 2 funguje stejně.

A protože $26 \equiv 6 \pmod 5$, tak v tomto případě obě rovnice s modulem 5 říkají totéž a stačí si vzít jednu z nich.

Závěr: Daná soustava, kterou jsme převedli na 7 rovnic, 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 řešení.

Tento postup je také pracný a jsme rádi, že si v aplikacích obvykle moduly n_i volíme sami, tudíž dokážeme zajistit vzájemnou nesoudělnost.

Cvičení

Cvičení 4d.1 (rutinní, zkouškové)**:** Vyřešte následující soustavy kongruencí:

(i) $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 5$;

(ii) $x \equiv 4 \pmod 2$, $x \equiv -4 \pmod 3$, $x \equiv 4 \pmod 5$;

(iii) $x \equiv 1 \pmod 7$, $x \equiv 0 \pmod 9$, $x \equiv -1 \pmod{11}$;

(iv) $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 4$, $x \equiv 5 \pmod 3$.

Řešení:

4d.1: (i): $n = 60$, $N_1 = 20$, inverze v $\mathbb{Z}_3$ je $x_1 = -1$; $N_2 = 15$, inverze v $\mathbb{Z}_4$ je $x_2 = -1$; $N_3 = 12$, inverze v $\mathbb{Z}_5$ je $x_3 = -2$. $x = 0 \cdot 20 \cdot (-1) + 1 \cdot 15 \cdot (-1) + 2 \cdot 12 \cdot (-2) = -63 \equiv 57 \pmod{60}$. Řešení jsou $x = 60k - 63$ nebo třeba $57 + 60k$ pro $k \in \mathbb{Z}$.

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

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

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

4e. Bonus: Soustavy lineárních diofantických rovnic

Toto téma je přirozeným pokračováním tématu lineární rovnice o dvou neznámých. Matematici vědí, jak se soustavy lineárních diofantických rovnic řeší, ale používají se při tom pojmy z pokročilejší teorie matic. Snad to je důvod, proč se toto téma v učebnicích diskrétní matematiky neobjevuje. Studenti se proto musejí obracet na knihy o lineárním programování či optimalizaci. Tam zjistí, že jde o důležité a užitečné téma, velké úsilí je věnováno návrhu algoritmů, které by efektivně řešily rozsáhlé systémy.

Jako speciální dárek čtenářům této knihy zde předvedeme postup řešení, který je elementární (ve smyslu, že nepoužívá pojmy z teorie matic) a zobecňuje postup, který jsme používali v části 4a.

Začneme jednou rovnicí o více neznámých $a_1x_1 + \cdots a_nx_n = c$. V sekci 2c.6 jsme odvodili postup, jak najít Bezoutovu identitu pro $\gcd(a_1, \ldots, a_n)$. Inspirací byla maticová interpretace rozšířeného Euklidova algoritmu. Rovněž postup pro řešení rovnic $ax + by = c$ jsme v této kapitole interpretovali jako úpravy matice a vycházel z hledání Bezoutovy identity, takže se zdá, že by toto mělo jít.

Připomeňme to hlavní ze sekce 4a. Abychom našli řešení rovnice $ax + by = c$, upravili jsme pomocí celočíselných řádkových úprav matici $\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$ nejprve na matici $\begin{pmatrix} \gcd(a,b) & A & B \\ 0 & A_h & B_h \end{pmatrix}$ a posléze na matici $\begin{pmatrix} c & A_p & B_p \\ 0 & A_h & B_h \end{pmatrix}$ (pokud toto bylo možné). Když jsme se pak podívali na pravou část matice (tedy bez levého sloupce), tak první řádek dal partikulární vektor a druhý dal generátor homogenního řešení.

Tento postup lze aplikovat i na případ více čísel. Je-li dána rovnice $a_1x_1 + \cdots + a_nx_n = c$, můžeme sestavit matici

$$\begin{pmatrix} a_1 & 1 & 0 & \ldots & 0 \\ a_2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & 0 & \ldots & 1 \end{pmatrix}$$

Jako její pravou část budeme označovat tu část, která má teď jednotkovou matici (tedy to, co zbyde po vynechání prvního sloupce). Ukázali jsme, že matici lze celočíselnými řádkovými úpravami převést na řádkově redukovaný tvar

$$\begin{pmatrix} \gcd(a_1, \ldots, a_n) & A_1 & A_2 & \ldots & A_n \\ 0 & \vdots & \vdots & & \vdots \\ \vdots & & & & \\ 0 & & & & \end{pmatrix}.$$

Pokud by číslo $\gcd(a_1, \ldots, a_n)$ dělilo pravou stranu řešené rovnice c, tak bychom v dalším kroku mohli dostat matici ve tvaru

$$\begin{pmatrix} c & A_{p1} & A_{p2} & \ldots & A_{pn} \\ 0 & B_{h1} & B_{h2} & \ldots & B_{hn} \\ 0 & 0 & C_{h2} & \ldots & C_{hn} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & & & & \end{pmatrix}.$$

Co nám říkají čísla z pravé části matice?

Původní matice reprezentovala soustavu

$$\begin{aligned} 1\cdot x_1 + 0\cdot x_2 + \cdots + 0\cdot x_n &= a_1\\ 0\cdot x_1 + 1\cdot x_2 + \cdots + 0\cdot x_n &= a_2\\ \vdots \qquad\qquad & \vdots\\ 0\cdot x_1 + 0\cdot x_2 + \cdots + 1\cdot x_n &= a_n \end{aligned}$$

s jednoznačným řešením $x_i = a_i$ pro všechna i. Protože řádkové úpravy nemění řešení, stejně jako násobení řádku konstantou v posledním kroku, musí mít stejné řešení i soustava daná poslední maticí, po dosazení dostáváme

$$\begin{aligned} A_{p1}\cdot a_1 + A_{p2}\cdot a_2 + \cdots + A_{pn}\cdot a_n &= c\\ B_{h1}\cdot a_1 + B_{h2}\cdot a_2 + \cdots + B_{hn}\cdot a_n &= 0\\ 0\cdot a_1 + C_{h2}\cdot a_2 + \cdots + C_{hn}\cdot a_n &= 0\\ \vdots \qquad\qquad & \vdots \end{aligned}$$

První řádek říká, že $x_1 = A_{p1}, \dots, x_n = A_{pn}$ je řešení dané rovnice. Zde asi bude lepší přejít na jazyk vektorů, tedy vektor $(A_{p1}, \dots, A_{pn}) \in \mathbb{Z}^n$ řeší danou rovnici.

Druhý řádek říká, že vektor $(B_{h1}, \dots, B_{hn}) \in \mathbb{Z}^n$ řeší přidruženou homogenní rovnici, stejně jako třetí, čtvrtý atd. řádek.

Označme si jednotlivé řádky pravé části matice jako $\vec{r}_1$, $\vec{r}_2$, … , $\vec{r}_n$. Rovnice říkají, že vektor $\vec{r}_1$ je partikulárním řešením dané rovnice, zatímco vektory $\vec{r}_2, \dots, \vec{r}_n$ řeší přidruženou homogenní rovnici. Je snadné dokázat, že pak i jejich libovolná lineární kombinace $\sum u_i\vec{r}_i$ řeší přidruženou homogenní rovnici.

Teď je pro nás zajímavé, že matice je v řádkově redukovaném tvaru, což znamená, že vektory $\vec{r}_2, \dots, \vec{r}_n$ tvoří lineárně nezávislou množinu. Generují proto něco, co bychom v $\mathbb{R}^n$ nazvali $(n-1)$-rozměrným podprostorem (nadrovinou), ale v $\mathbb{Z}^n$ to říct nemůžeme, jen si to představujeme.

Jedna věc nám ještě chybí: Ukázat, že tyto vektory generují všechna homogenní řešení. To už tak snadné není, nicméně je to pravda a bude to vyplývat z poznatků o obecných soustavách. Když to shrneme, pomocí řádkových úprav matice jsme upravili jistou matici do speciálního tvaru. Řádky pravé části pak coby vektory $\vec{r}_i$ dovolují napsat obecné řešení dané rovnice ve tvaru $\vec{r}_1 + \sum_{i=2}^{n} u_i\vec{r}_i$, kde $u_i \in \mathbb{Z}$ jsou parametry.

Postup zároveň ukázal, že toto je možné právě tehdy, když $\gcd(a_1, \dots, a_n)$ dělí c. Máme tedy pěknou paralelu s případem dvou proměnných.

Příklad 4e.a: Vyřešíme rovnici $6x - 12y + 15z = 45$. Přechod k matici:

$$\begin{pmatrix} 6 & 1 & 0 & 0\\ -12 & 0 & 1 & 0\\ 15 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 6 & 1 & 0 & 0\\ 0 & 2 & 1 & 0\\ 3 & -2 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 5 & 0 & -2\\ 0 & 2 & 1 & 0\\ 3 & -2 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 3 & -2 & 0 & 1\\ 0 & 5 & 0 & -2\\ 0 & 2 & 1 & 0 \end{pmatrix}$$
$$\sim \begin{pmatrix} 45 & -30 & 0 & 15\\ 0 & 1 & -2 & -2\\ 0 & 2 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 45 & -30 & 0 & 15\\ 0 & 1 & -2 & -2\\ 0 & 0 & 5 & 4 \end{pmatrix}$$

Protože se nám v prvním řádku a sloupci podařilo vyrobit číslo 45, soustava má řešení. Dostáváme vektory $\vec{r}_1 = (-30, 0, 15)$, $\vec{r}_2 = (1, -2, -2)$ a $\vec{r}_3 = (0, 5, 4)$. Vychází obecné řešení $(-30, 0, 15) + k(1, -2, -2) + l(0, 5, 4)$ neboli

$$\begin{aligned} x &= k - 30\\ y &= 5l - 2k\\ z &= 15 - 2k + 4l \qquad\qquad \text{pro } k, l \in \mathbb{Z}. \end{aligned}$$

Zkouška:

$$6(k-30) - 12(5l-2k) + 15(15 - 2k + 4l) = 6k - 180 - 60l + 24k + 225 - 30k + 60l = 45.$$

Pro zajímavost zkusíme ověřit, že vektory $\vec{r}_2$, $\vec{r}_3$ jsou opravdu lineárně nezávislé ve světě celých čísel. Ptáme se tedy, zda je možné najít celá čísla α, β tak, aby platilo $\alpha(1, -2, -2) + \beta(0, 5, 4) = (0, 0, 0)$ a alespoň jedno nebylo nulové. Ovšem první souřadnice dává rovnici $1\cdot\alpha + 0\cdot\beta = 0$, tedy nutně $\alpha = 0$. Dosazením do rovnice z druhé souřadnice $-2\alpha + 5\beta = 0$ vychází i $\beta = 0$ a vektory jsou proto opravdu lineárně nezávislé.

△

Poznamenejme, že v lineární algebře se obvykle vektory uvažují jako sloupcové, ale tady by se to nehodilo, museli bychom pořád transponovat. Budeme tedy pracovat s řádkovými vektory.

Než se vydáme dále, bude užitečné nahlédnout, že se rovnice $a_1x_1+\cdots+a_nx_n=c$ dá zapsat v maticovém tvaru jako

$$(\,a_1\quad\cdots\quad a_n\,)\cdot\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=(c).$$

Označíme-li matici soustavy jako A, vektor neznámých jako $\vec{x}=(x_1,\dots,x_n)$ a vektor pravé strany jako $\vec{c}=(c)$, můžeme rovnici zachytit zápisem $A\vec{x}^T=\vec{c}^T$. Sloupcové vektory jsme získali z řádkových pomocí transpozice. U $\vec{c}$ jsme vlastně nemuseli, ale čtenář asi tuší, že si již připravujeme půdu pro případ více rovnic.

Rovnici jsme řešili tak, že jsme sestavili matici $(A^T|E_n)$, kterou jsme pak řádkovými úpravami redukovali. Jak to asi bude fungovat v případě soustav více rovnic? Než se k nim dostaneme, přidáme ještě jeden bonus v bonusové sekci neboli bonus^2.

4e.1 Eliminace

Když jsme zaváděli největší společný jmenovatel pro více čísel, zvolili jsme definici, která to udělá najednou. Ve cvičení 2b.8 jsme ovšem ještě nastínili druhou možnost, jmenovitě hledat $\gcd(a_1,\dots,a_n)$ induktivně. Nejprve najdeme $b_2=\gcd(a_1,a_2)$, pak $b_3=\gcd(b_2,a_3)$, $b_4=\gcd(b_3,a_4)$ a tak dále až nakonec $\gcd(a_1,\dots,a_n)=\gcd(b_n,a_n)$. Dá se ukázat, že vyjde stejné číslo jako podle definice.

Podobně lze i diofantickou rovnici $a_1x_1+\cdots+a_nx_n=c$ řešit rekurzivně. Platí totiž zajímavé tvrzení:

• Čísla $A_1,\cdots,A_n$ řeší rovnici $a_1x_1+\cdots+a_nx_n=c$ právě tehdy, pokud existuje $U\in\mathbb{Z}$ takové, že čísla $U,A_3,\dots,A_n$ řeší rovnici $\gcd(a_1,a_2)u+a_3x_3+\cdots+a_nx_n=c$ a A_1,A_2 řeší rovnici $a_1x_1+a_2x_2=\gcd(a_1,a_2)U$.

Jak to víme? Předpokládejme, že A_i jsou řešení. Pak po dosazení do dané rovnice a úpravě dostáváme

$$(\star)\qquad a_1A_1+a_2A_2=c-a_3A_3-\cdots-a_nA_n.$$

To se dá interpretovat tak, že A_1,A_2 řeší rovnici

$$a_1x_1+a_2x_2=c-a_3A_3-\cdots-a_nA_n.$$

To znamená, že $\gcd(a_1,a_2)$ musí dělit pravou stranu neboli $c-a_3A_3-\cdots-a_nA_n=U\gcd(a_1,a_2)$ pro nějaké $U\in\mathbb{Z}$. Po úpravě dostáváme $\gcd(a_1,a_2)U+a_3A_3+\cdots+a_nA_n=c$, tedy čísla $U,A_3,\dots,A_n$ opravdu řeší rovnici $\gcd(a_1,a_2)u+a_3x_3+\cdots+a_nx_n=c$.

Když pak dosadíme $c-a_3A_3-\cdots-a_nA_n=U\gcd(a_1,a_2)$ do $(\star)$, dostaneme $a_1A_1+a_2A_2=U\gcd(a_1,a_2)$, tedy A_1,A_2 řeší $a_1x_1+a_2x_2=U\gcd(a_1,a_2)$.

Teď naopak: Mějme čísla $U,A_1,\dots,A_n$ taková, že A_1,A_2 řeší rovnici $a_1x_1+a_2x_2=\gcd(a_1,a_2)U$ a $U,A_3,\dots,A_n$ řeší rovnici $\gcd(a_1,a_2)u+a_3x_3+\cdots+a_nx_n=c$. Po dosazení dostáváme vzorce

$$a_1A_1+a_2A_2=\gcd(a_1,a_2)U,\quad \gcd(a_1,a_2)U+a_3A_3+\cdots+a_nA_n=c,$$

což dává $a_1A_1+\cdots+a_nA_n=c$ a čísla $A_1,\dots,A_n$ tedy řeší danou rovnici.

Tvrzení, které jsme právě dokázali, nám umožňuje namísto rovnice o n neznámých řešit nejprve rovnici o $n-1$ neznámých a pomocí nalezeného řešení pak ještě rovnici o dvou neznámých (to už umíme). Pokud nejsme spokojeni s rovnicí o $n-1$ neznámých, lze na ni aplikovat stejný postup a získat rovnici o $n-2$ neznámých, dříve či později se dobereme k rovnici, kterou už umíme (popřípadě nemá řešení, což je také dobrý konec).

Já bych to tedy osobně nedělal, ale už jsem potkal lidi, kterým redukce vyhovovala. Třeba umí opravdu dobře rovnice o dvou neznámých. Nebo neznají ten postup s maticí.

Vyzkoušíme si to na již jednou řešené rovnici $6x-12y+15z=45$.

Protože $\gcd(6,-12)=6$, měli bychom namísto té zadané řešit rovnice $6u+15z=45$ a $6x-12y=6u$. Začneme přirozeně tou první. Je jednoduchá, to se ani nevyplácí zkoušet algoritmus.

Vidíme, že $\gcd(6,15)=3$, odhadneme $3=1\cdot15+(-2)\cdot6$ a vynásobením a mírnou reorganizací dospějeme k rovnosti $6\cdot(-30)+15\cdot15=45$. Vychází partikulární řešení $u_p=-30$, $z_p=15$. Z homogenní rovnice $6u+15z=0$ vykrácením na $2u+5z=0$ vykoukáme řešení $u_h=5k$, $z_h=-2k$. Než je dáme dohromady, využijeme homogenní řešení k nalezení lepšího partikulárního zástupce, $u_p=-30+5\cdot6=0$, $z_p=15-2\cdot6=3$, budeme tedy dále počítat s řešením $u=5k$, $z=3-2k$ pro $k\in\mathbb{Z}$.

Dostáváme se k druhé rovnici, $6x-12y=6u$ neboli $6x-12y=30k$. Rovnou ji vykrátíme šesti, výslednou rovnici $x-2y=5k$ tentokráte zkusíme pro změnu řešit tabulkou.

a/b	x	y
-2	0	1
1	1	0
0	2	1
$5k$	$5k$	0

To bylo trapně jednoduché, vlastně hned druhý řádek ze zadání dal gcd. Z posledních dvou řádků vyčteme řešení $x=5k+2l$, $y=0+l$ pro $l\in\mathbb{Z}$.

Shrnuto, máme $x=5k+2l$, $y=l$, $z=3-2k$ pro $k,l\in\mathbb{Z}$.

To vypadá podezřele pěkně. Zkouška:

$$6(5k+2l)-12l+15(3-2k)=30k+12l-12l+45-30k=45.$$

Takže opravdu to je řešení. Jsou to ale úplně všechna řešení? Jeden ze způsobů, jak se přesvědčit, je vzít si nějaké obecné řešení obdržené způsobem, kterému důvěřujeme, tedy z předchozího příkladu, a zkusit jej získat pomocí nového vzorce. Aby se nám nepletly parametry, uvažujme tedy řešení $x = K - 30$, $y = 5L - 2K$, $z = 15 - 2K + 4L$ pro nějaká $K, L \in \mathbb{Z}$. Dokážeme jej získat pomocí nových vzorců? Znamená to řešit soustavu rovnic

$$\begin{aligned} K - 30 &= 5k + 2l \\ 5L - 2K &= l \\ 15 - 2K + 4L &= 3 - 2k \end{aligned}$$

s parametry $K, L \in \mathbb{Z}$ a neznámými $k, l \in \mathbb{Z}$. Druhá a třetí rovnice rovnou dají $k = K - 2L - 6$ a $l = 5L - 2K$, což jsou celá čísla, dosazením do první rovnice potvrdíme, že opravdu řeší soustavu, tedy vše je v pořádku.

Zvědavý čtenář by ještě mohl vyzkoušet opačný pohled, tedy zda všechna nová řešení lze získat pomocí těch předchozích. Znamená to tedy, že se při řešní soustavy zamění role parametrů a neznámých. Potvrdí se pak, že obojí vzorce definují stejnou podmnožinu $\mathbb{Z}^3$.

△

4e.2 Soustavy rovnic

Uvažujme obecnou soustavu m rovnic o n neznámých

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= c_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= c_2 \\ &\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= c_m \end{aligned}$$

Typicky máme $m \leq n$.

Vzhledem k postupu pro jednu rovnici by člověk čekal, že to teď bude chtít nasypat koeficienty jednotlivých rovnic do sloupců (to bude „levá část“ pracovní matice), odpovídá to A^T, jak jsme si to rozmysleli u případu jedné rovnice. K tomu se přilepí jednotková matice vhodné velikosti („pravá část“ pracovní matice) a pak redukuje.

Dostaneme matici v řádkově redukovaném tvaru. Abychom pomohli čtenářově představivosti, napravo jsme jednu takovou typickou ukázali, je pro dvě rovnice o čtyřech neznámých. Oddělili jsme také vizuálně levou a pravou část. Co víme o levé části? První sloupec bude mít nahoře číslo, jmenovitě $\pm\gcd(a_{1,1}, \ldots, a_{1,n})$, a pod ním nuly, v dalších sloupcích už není jasné, co nenulová čísla znamenají.

$$\left(\begin{array}{cc|cccc} * & * & * & * & * & * \\ 0 & * & * & * & * & * \\ 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & * & * & * \end{array}\right)$$

Protože máme n řádků a levá část matice (ta, co reprezentuje jednotlivé rovnice) má m sloupců, bude v ní (pokud $m \leq n$) alespoň $n - m$ nulových řádků. Jestli funguje analogie s případem jedné rovnice, tak na těchto řádcích bychom v pravé části měli hledat vektory generující homogenní řešení. Počty se zdají souhlasit s intuicí. Začínáme s prostorem $\mathbb{Z}^n$ a v ideálním případě každá rovnice ubere jednu „dimenzi“ neboli jeden parametr z řešení, takže se dá čekat, že obecné řešení bude mít $n - m$ parametrů (za předpokladu, že rovnice nebudou nějak provázané, to by přibyly nulové řádky).

Partikulární řešení pak budeme hledat v těch řádcích, které v levé části nuly nemají. V prvním sloupci bychom asi měli (viz postup u jedné rovnice) namísto onoho gcd vyrobit c_1 chytrým vynásobením prvního řádku, pokud to tedy jde. Ve druhém sloupci (reprezentujícím druhou rovnici) už to ale tak jednoduché nebude. Patrně bychom si měli vyrobit c_2 násobením řádků. Protože první řádek matice už posloužil k výrobě c_1 v prvním sloupci a třetí (a další) řádky mají v druhém sloupci nulu, je zjevné, že se ono c_2 bude vyrábět pomocí druhého řádku, ale není hned jasné jak.

Dá se to intuitivně vymyslet, ale raději si dáme poradit. Jak je obvyklé, budeme pracovat s maticovým zápisem soustavy.

S **Algoritmus 4e.3.**
pro řešení soustavy lineárních homogenních rovnic $A\vec{x}^T = \vec{c}^T$, kde A je $m \times n$ matice s celočíselnými prvky, $\vec{c} \in \mathbb{Z}^m$ a očekáváme $\vec{x} \in \mathbb{Z}^n$.

1. Vytvořte matici $(A^T|E_n)$ a převeďte ji celočíselnými řádkovými úpravami do řádkově-schodovitého tvaru $(D|S)$. Nechť $N \in \mathbb{N}$ je největší mezi čísly řádků, které nejsou identicky nulové (pokud nějaké takové existují).

2. Pomocí celočíselného násobení prvních N řádků matice $(D|S)$ ji upravte do tvaru $(B|R)$ tak, aby pro každé $j = 1, \ldots, m$ byl součet prvků ve sloupci j matice B roven c_j.

Pokud toto není možné, daná soustava nemá řešení.

3. Předpokládejme, že jste v kroku **2** uspěli.

Nechť $\vec{r}_i$ jsou řádky matice R. Označte $\vec{x}_p = \sum_{i=1}^{N} \vec{r}_i$.

Obecné řešení soustavy $A\vec{x}^T = \vec{c}^T$ je pak dáno vzorcem

$$\vec{x}_p + \sum_{i>N} u_i \vec{r}_i \quad \text{pro} \quad u_i \in \mathbb{Z}.$$

△

Rozmyslete si, že když je jen jedna rovnice, tedy $m = 1$, tak tento algoritmus souhlasí s postupem předvedeným v předchozí sekci. Důkaz správnosti algoritmu je trochu delší, v bonusové kapitole si jej odpustíme.

Trochu nejasný zůstává druhý krok. Jak poznáme, kdy je a kdy není možná ona předepsaná úprava? Tady je klíčové, že matice D je ve schodovitém tvaru. Nejprve si ukážeme příklad. Dohodneme se, že slovem „vedoucí člen řádku“ budeme označovat první nenulový prvek řádku matice, počítáno zleva (pokud takový existuje).

Příklad 4e.b: Vyřešíme soustavu

$$\begin{aligned} 10w + 14x + 16y + 18z &= 4 \\ w - 10x + y + 3z &= -5 \\ 2w - x + 3y + 4z &= -1 \\ 9w + 13x + 16y + 17z &= 0 \end{aligned}$$

Matice soustavy je $A = \begin{pmatrix} 10 & 14 & 16 & 18 \\ 1 & -10 & 1 & 3 \\ 2 & -1 & 3 & 4 \\ 9 & 13 & 16 & 17 \end{pmatrix}$, podle algoritmu bychom tedy měli pracovat s maticí

$$\left(\begin{array}{cccc|cccc} 10 & 1 & 2 & 9 & 1 & 0 & 0 & 0 \\ 14 & -10 & -1 & 13 & 0 & 1 & 0 & 0 \\ 16 & 1 & 3 & 16 & 0 & 0 & 1 & 0 \\ 18 & 3 & 4 & 17 & 0 & 0 & 0 & 1 \end{array}\right).$$

Krok 1: Potřebujeme matici upravit na řádkově-schodovitý tvar pomocí celočíselných řádkových operací.

Začneme redukováním prvního sloupce. Jako pivot zvolíme nejmenší číslo (v absolutní hodnotě), v tomto případě je to 10 v prvním řádku. Odčítáme vhodné násobky od ostatních řádků tak, abychom získali v prvním sloupci co nejmenší čísla, povolíme si i záporná. Dostaneme

$$\left(\begin{array}{cccc|cccc} 10 & 1 & 2 & 9 & 1 & 0 & 0 & 0 \\ 4 & -11 & -3 & 4 & -1 & 1 & 0 & 0 \\ -4 & -1 & -1 & -2 & -2 & 0 & 1 & 0 \\ -2 & 1 & 0 & -1 & -2 & 0 & 0 & 1 \end{array}\right).$$

Teď je nejmenším číslem -2 ve čtvrtém řádku. Vidíme, že dělí všechny ostatní prvky prvního sloupce, takže první etapa tímto skončí. Vyrobíme pomocí čtvrtého řádku nuly v prvním sloupci a pak jej vyměníme s prvním. Není třeba násobit jej mínus jedničkou, záporná čísla nám nevadí. Vychází matice

$$\left(\begin{array}{cccc|cccc} -2 & 1 & 0 & -1 & -2 & 0 & 0 & 1 \\ 0 & -9 & -3 & 2 & -5 & 1 & 0 & 2 \\ 0 & -3 & -1 & 0 & 2 & 0 & 1 & -2 \\ 0 & 6 & 2 & 4 & -9 & 0 & 0 & 5 \end{array}\right).$$

Teď se přesuneme do druhého sloupce. Nejmenší číslo (když neuvažujeme první řádek) je tam -3 ve třetím řádku.Vyrobíme nuly ve druhém a čtvrtém řádku a pak zaměníme třetí s druhým. A abychom měli na diagonále něco kladného, ještě jej jen tak z rozpustilosti vynásobíme mínus jedničkou. Měli byste dostat

$$\left(\begin{array}{cccc|cccc} -2 & 1 & 0 & -1 & -2 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & -2 & 0 & -1 & 2 \\ 0 & 0 & 0 & 2 & -11 & 1 & -3 & 8 \\ 0 & 0 & 0 & 4 & -5 & 0 & 2 & 1 \end{array}\right).$$

Ve třetím sloupci žádný pivot nemáme, takže nám v levé části matice zůstanou nejvýše tři nenulové řádky. Vlastně vidíme, že zůstanou přesně tři. Jinými slovy, vznikne jeden generující vektor pro homogenní řešení. Abychom tento krok dokončili, přesuneme se do čtvrtho sloupce a vyrobíme ve čtvrtém řádku nulu pomocí třetího.

$$\left(\begin{array}{cccc|cccc} -2 & 1 & 0 & -1 & -2 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & -2 & 0 & -1 & 2 \\ 0 & 0 & 0 & 2 & -11 & 1 & -3 & 8 \\ 0 & 0 & 0 & 0 & 17 & -2 & 8 & -15 \end{array}\right).$$

Máme $N = 3$.

Krok 2: Potřebujme vyrobit správné součty v sloupcích.

Aby se první sloupec nasčítal do 4, vynásobíme první řádek číslem -2:

$$\left(\begin{array}{cccc|cccc} 4 & -2 & 0 & 2 & 4 & 0 & 0 & -2 \\ 0 & 3 & 1 & 0 & -2 & 0 & -1 & 2 \\ 0 & 0 & 0 & 2 & -11 & 1 & -3 & 8 \\ 0 & 0 & 0 & 0 & 17 & -2 & 8 & -15 \end{array}\right).$$

Aby dal druhý sloupec součet -5, vynásobíme druhý řádek číslem -1. Protože tam máme vedoucí člen řádku, musí mít v prvním sloupci nulu a tak tímto násobením nepokazíme to, co jsme si před chvílí vytvořili v prvním sloupci.

$$\left(\begin{array}{cccc|cccc} 4 & -2 & 0 & 2 & 4 & 0 & 0 & -2 \\ 0 & -3 & -1 & 0 & 2 & 0 & 1 & -2 \\ 0 & 0 & 0 & 2 & -11 & 1 & -3 & 8 \\ 0 & 0 & 0 & 0 & 17 & -2 & 8 & -15 \end{array}\right).$$

Součet třetího sloupce nelze ovlivnit. První dva řádky jsou již nastaveny, jediná šance něco ovlivnit je mít ve třetím řádku vedoucí člen, ale není tam. Můžeme jen ověřit, zda má třetí sloupec správný součet. Ano, vychází -1, máme štěstí.

Ve čtvrtém sloupci máme vedoucí člen třetího řádku, máme tedy možnost jej nastavit. Aby se čtvrtý sloupec sečetl na nulu, vynásobíme třetí řádek číslem -1:

$$\left(\begin{array}{cccc|cccc} 4 & -2 & 0 & 2 & 4 & 0 & 0 & -2 \\ 0 & -3 & -1 & 0 & 2 & 0 & 1 & -2 \\ 0 & 0 & 0 & -2 & 11 & -1 & 3 & -8 \\ 0 & 0 & 0 & 0 & 17 & -2 & 8 & -15 \end{array}\right).$$

Krok 3: Máme $N = 3$ nenulové řádky, takže $\vec{x}_h = (17, -2, 8, -15)$ a

$$\vec{x}_p = (4, 0, 0, -2) + (2, 0, 1, -2) + (11, -1, 3, -8) = (17, -1, 4, -12).$$

Obecné řešení soustavy je $(17, -1, 4, -12) + u(17, -2, 8, -15)$ neboli

$$\begin{aligned} w &= 17 + 17u, \\ x &= -1 - 2u, \\ y &= 4 + 8u, \\ z &= -12 - 15u, \ u \in \mathbb{Z}. \end{aligned}$$

Zkouška potvrdí, že tato čísla opravdu řeší všechny čtyři rovnice (fakt jsem si ji udělal).

△

Postup z kroku 2, který jsme viděli, je možné formalizovat.

0. Nastavte $j = 1$.

1. Pokud se ve sloupci j nachází vedoucí člen nějakého řádku, vynásobte dotyčný řádek celým číslem tak, aby byl součet sloupce j roven c_j. Pokud to nejde, soustava nemá řešení a postup končí.

Pokud se ve sloupci j žádný vedoucí člen řádku nenachází, ověřte, že součet jeho prvků je c_j. Pokud toto není splněno, soustava nemá řešení a postup končí.

Pokud je $j < m$, zvětšete j o jedničku a zopakujte krok 1.

Není těžké ukázat, že tento postup dokáže správně rozpoznat, kdy je výroba matice $(B|R)$ možná a kdy ne.

Ještě jeden příklad.

Příklad 4e.c: Uvažujme soustavu rovnic

$$\begin{aligned} 15s + 24t - 12u + 30v &= 6 \\ 10s - 4t + 26u + 14v &= 12. \end{aligned}$$

Máme matici soustavy $A = \begin{pmatrix} 15 & 24 & -12 & 30 \\ 10 & -4 & 26 & 14 \end{pmatrix}$.

Sestavíme pracovní matici a redukujeme ji.

$$\left(\begin{array}{cc|cccc} 15 & 10 & 1 & 0 & 0 & 0 \\ 24 & -4 & 0 & 1 & 0 & 0 \\ -12 & 26 & 0 & 0 & 1 & 0 \\ 30 & 14 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & 48 & 0 & 1 & 2 & 0 \\ -12 & 26 & 0 & 0 & 1 & 0 \\ -6 & 92 & 0 & 0 & 3 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & 48 & 0 & 1 & 2 & 0 \\ 0 & 170 & 4 & 0 & 5 & 0 \\ 0 & 164 & 2 & 0 & 5 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & 48 & 0 & 1 & 2 & 0 \\ 0 & -22 & 4 & -4 & -3 & 0 \\ 0 & 20 & 2 & -3 & -1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & 8 & -4 & 7 & 4 & -2 \\ 0 & -2 & 6 & -7 & -4 & 1 \\ 0 & 20 & 2 & -3 & -1 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & 0 & 20 & -21 & -12 & 2 \\ 0 & -2 & 6 & -7 & -4 & 1 \\ 0 & 0 & 62 & -73 & -41 & 11 \end{array}\right) \sim \left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & -2 & 6 & -7 & -4 & 1 \\ 0 & 0 & 20 & -21 & -12 & 2 \\ 0 & 0 & 62 & -73 & -41 & 11 \end{array}\right)$$

$$\sim \left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & -2 & 6 & -7 & -4 & 1 \\ 0 & 0 & 20 & -21 & -12 & 2 \\ 0 & 0 & 2 & -10 & -5 & 5 \end{array}\right) \sim \left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & -2 & 6 & -7 & -4 & 1 \\ 0 & 0 & 0 & 79 & 38 & -48 \\ 0 & 0 & 2 & -10 & -5 & 5 \end{array}\right)$$

Ještě pak prohodíme poslední dva řádky.

Nyní přijde upravovací fáze. Nejprve v prvním sloupci potřebujeme výsledek 6, takže první řádek vynásobíme dvojkou. Přejdeme k druhému sloupci a vynásobíme druhý řádek tak, aby druhý sloupec dal součet 12. I to je možné.

$$\left(\begin{array}{cc|cccc} 3 & 36 & 1 & 0 & 1 & 0 \\ 0 & -2 & 6 & -7 & -4 & 1 \\ 0 & 0 & 2 & -10 & -5 & 5 \\ 0 & 0 & 0 & 79 & 38 & -48 \end{array}\right) \mapsto \left(\begin{array}{cc|cccc} 6 & 72 & 2 & 0 & 2 & 0 \\ 0 & -2 & 6 & -7 & -4 & 1 \\ 0 & 0 & 2 & -10 & -5 & 5 \\ 0 & 0 & 0 & 79 & 38 & -48 \end{array}\right) \mapsto \left(\begin{array}{cc|cccc} 6 & 72 & 2 & 0 & 2 & 0 \\ 0 & -60 & 180 & -210 & -120 & 30 \\ 0 & 0 & 2 & -10 & -5 & 5 \\ 0 & 0 & 0 & 79 & 38 & -48 \end{array}\right)$$

Mimochodem, vidíme, že podmínkou řešitelnosti je, že c_1 je násobkem tří a $c_2 - 72$ je sudé, tedy c_2 musí být sudé.

Dostáváme se k poslední fázi řešení. První dva řádky jsou v levé části nenulové, takže partikulární řešení je

$$\vec{x}_p = (2,0,2,0) + (180,-210,-120,30) = (182,-210,-118,30)$$

a obecné řešení přidružené homogenní rovnice je

$$\vec{x}_h = k(2,-10,-5,5) + l(0,79,38,-48).$$

Máme řešení naší soustavy

$$\begin{aligned} s &= 182 + 2k \\ t &= -210 - 10k + 79l \\ u &= -118 - 5k + 38l \\ v &= 30 + 5k - 48l \end{aligned} \qquad \text{pro } k,l \in \mathbb{Z}.$$

△

4e.4 Poznámka: Zejména v případě velkých matic se vyplatí vědět, že nebylo nutné vytvářet schodovitý tvar v pravé části matice. My jsme podle něj poznali, že vektory generující homogenní řešení budou nezávislé, ale to musí platit vždy. Původně jsme totiž v pravé části matice měli jednotkovou matici s hodností n, což se nezmění ani po řádkových operacích. Proto musí být řádky pravé části matice lineárně nezávislé, ať už se na ně díváme v kterékoliv fázi úprav.

Je tedy možné vyrábět schodovitý tvar jen ve sloupcích levé části matice, což může být výrazná úspora času. My jsme v předchozím příkladě dotáhli celý proces až do konce, protože je docela příjemné mít jednodušší vektory coby generátory, ale občas se mi nebude chtít.

△

Cvičení

Cvičení 4e.1 (rutinní)**:** Najděte obecná řešení pro následující rovnice:

(i) $21x + 28x - 14y = 35$;
(ii) $8x - 12y + 28z = 18$;
(iii) $3a + 5b + 7c = 9$,
(iv) $2r - 3s + 4t - 5u + 6v = 7$.

Cvičení 4e.2 (rutinní)**:** Najděte obecná řešení pro následující soustavy rovnic:

(i) $\begin{cases} 25x - 15y = 10 \\ 4x + 6y = 52; \end{cases}$
(ii) $\begin{cases} 9x + 6y = 5 \\ 6x - 4y = 10; \end{cases}$
(iii) $\begin{cases} 3r + 5s - 7t + 9u = 2 \\ 3r - 5s + 7t - 9u = 3 \\ 2r + 4s + 6t + 8u = 4; \end{cases}$
(iv) $\begin{cases} 6u - 9v + 9w = 12 \\ 2u - 4v + 5w = 13; \end{cases}$
(v) $\begin{cases} 3x + 4y + 5z = 6 \\ 4x + 5y + 6z = 7. \end{cases}$

Řešení:

Poznámka: Protože při redukci matic existuje více možných postupů, může se vaše matice lišit. Podstatné je, že by vaše vektory měly generovat stejný prostor řešení.

4e.1: (i): $\left(\begin{array}{c|ccc} 21 & 1 & 0 & 0 \\ 28 & 0 & 1 & 0 \\ -14 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} 7 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 3 \end{array}\right) \mapsto \left(\begin{array}{c|ccc} 35 & 5 & 0 & 5 \\ 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 3 \end{array}\right)$.

$(5,0,5)+k(0,1,2)+l(2,0,3)$ neboli $x=5+2l$, $y=k$, $z=5+2k+3l$ pro $k,l\in\mathbb{Z}$.

Mimochodem, $\gcd(21,28,-14)=7$.

(ii): $\left(\begin{array}{c|ccc} 8 & 1 & 0 & 0 \\ -12 & 0 & 1 & 0 \\ 28 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} 4 & 2 & 1 & 0 \\ 0 & -3 & -2 & 0 \\ 0 & -5 & -1 & 1 \end{array}\right)$

Nelze $4\mapsto 18$, řešení neexistuje.

(iii): $\left(\begin{array}{c|ccc} 3 & 1 & 0 & 0 \\ 5 & 0 & 1 & 0 \\ 7 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccc} 1 & 2 & -1 & 0 \\ 0 & -5 & 3 & 0 \\ 0 & -3 & 1 & 1 \end{array}\right) \mapsto \left(\begin{array}{c|ccc} 9 & 18 & -9 & 0 \\ 0 & -5 & 3 & 0 \\ 0 & -4 & 1 & 1 \end{array}\right)$.

$(18,-9,0)+k(-5,3,0)+l(-4,1,1)$ neboli $a=18-5k-4l$, $b=-9+3k+l$, $c=l$ pro $k,l\in\mathbb{Z}$.

(iv): $\left(\begin{array}{c|ccccc} 2 & 1 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 0 & 0 & 0 \\ 4 & 0 & 0 & 1 & 0 & 0 \\ -5 & 0 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|ccccc} 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & -3 & -2 & 0 & 0 & 0 \\ 0 & -2 & 0 & 1 & 0 & 0 \\ 0 & 4 & 1 & 0 & 1 & 0 \\ 0 & -3 & 0 & 0 & 0 & 1 \end{array}\right) \mapsto \left(\begin{array}{c|ccccc} 7 & 14 & 7 & 0 & 0 & 0 \\ 0 & -3 & -2 & 0 & 0 & 0 \\ 0 & -2 & 0 & 1 & 0 & 0 \\ 0 & 4 & 1 & 0 & 1 & 0 \\ 0 & -3 & 0 & 0 & 0 & 1 \end{array}\right)$.

$(14,7,0,0,0)+k(-3,-2,0,0,0)+l(-2,0,1,0,0)+m(4,1,0,1,0)+n(-3,0,0,0,1)$ neboli $r=14-3k-2l+4m-3n$, $s=7-2k+m$, $t=l$, $u=m$, $v=n$ pro $k,l,m,n\in\mathbb{Z}$.

4e.2: (i): $\left(\begin{array}{cc|cc} 25 & 4 & 1 & 0 \\ -15 & 6 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 5 & -16 & -1 & -2 \\ 0 & 42 & 3 & 5 \end{array}\right) \mapsto \left(\begin{array}{cc|cc} 10 & -32 & -2 & -4 \\ 0 & 42 & 3 & 5 \end{array}\right) \mapsto \left(\begin{array}{cc|cc} 10 & -32 & -2 & -4 \\ 0 & 84 & 6 & 10 \end{array}\right)$.

$(x,y)=(-2,-4)+(6,10)=(4,6)$ neboli $x=4$, $y=6$.

(ii): $\left(\begin{array}{cc|cc} 9 & 6 & 1 & 0 \\ 6 & -4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 3 & 10 & 1 & -1 \\ 0 & -24 & -2 & 3 \end{array}\right) \mapsto \left(\begin{array}{cc|cc} 8 & 56 & 4 & -4 \\ 0 & -36 & -235 & \end{array}\right)$.

Pomocí $k\in\mathbb{Z}$ nelze vytvořit $3k=5$, proto soustava nemá řešení.

(iii): $\left(\begin{array}{ccc|cccc} 3 & 3 & 2 & 1 & 0 & 0 & 0 \\ 5 & -5 & 4 & 0 & 1 & 0 & 0 \\ -7 & 7 & 6 & 0 & 0 & 1 & 0 \\ 9 & -9 & 8 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 1 & 11 & 0 & 2 & -1 & 0 & 0 \\ 0 & 6 & -2 & 1 & 3 & 0 & -2 \\ 0 & 0 & 2 & 0 & 23 & -1 & -12 \\ 0 & 0 & 0 & 0 & 55 & 2 & -29 \end{array}\right)$

$\mapsto \left(\begin{array}{ccc|cccc} 2 & 22 & 0 & 4 & -2 & 0 & 0 \\ 0 & 6 & -2 & 1 & 3 & 0 & -2 \\ 0 & 0 & 2 & 0 & 23 & -1 & -12 \\ 0 & 0 & 0 & 0 & 55 & 2 & -29 \end{array}\right)$.

Pomocí $k\in\mathbb{Z}$ nelze dosáhnout $22+6k=3$, proto soustava nemá řešení.

(iv): $\left(\begin{array}{cc|ccc} 6 & 2 & 1 & 0 & 0 \\ -9 & -4 & 0 & 1 & 0 \\ 9 & 5 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 3 & 2 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 3 & 4 & 2 \end{array}\right) \mapsto \left(\begin{array}{cc|ccc} 12 & 8 & -4 & -4 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 3 & 4 & 2 \end{array}\right) \mapsto \left(\begin{array}{cc|ccc} 12 & 8 & -4 & -4 & 0 \\ 0 & 5 & 0 & 5 & 5 \\ 0 & 0 & 3 & 4 & 2 \end{array}\right)$.

$(x,y)=(-4,-4,0)+(0,5,5)+k(3,4,2)$ neboli $u=-4+3k$, $v=1+4k$, $w=5+2k$ pro $k\in\mathbb{Z}$.

(v): $\left(\begin{array}{cc|ccc} 3 & 4 & 1 & 0 & 0 \\ 4 & 5 & 0 & 1 & 0 \\ 5 & 6 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 1 & 1 & -1 & 1 & 0 \\ 0 & 1 & 4 & -3 & 0 \\ 0 & 0 & 1 & -2 & 1 \end{array}\right) \mapsto \left(\begin{array}{cc|ccc} 6 & 6 & -6 & 6 & 0 \\ 0 & 1 & 4 & -3 & 0 \\ 0 & 0 & 1 & -2 & 1 \end{array}\right)$.

$(x,y,z)=(-6,6,0)+(4,-3,5)+k(1,-2,1)$ neboli $x=-2+k$, $y=3-2k$, $z=k$ pro $k\in\mathbb{Z}$.

4f. Bonus: Z historie diofantických rovnic

Zde vlastně nic neprobereme, je to jen taková připomínka několika zajímavých rovnic, které se za poslední čtyři tisíce let zkoumaly.

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 pythagorejsou trojici a jsou to shodou okolností nejmenší možná 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 jakýmisi 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. Naskýtá 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 nevleze, 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 (známe ho z věty o počtu kroků Euklidova algoritmu). 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 jednou za pár let nějaký 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 dokázali matematici celý pořádně projít a ověřit. Dnes převažuje názor, že Fermat korektní důkaz neměl.

Další velice populární rovnice je „Pellova rovnice“ $x^2 - ny^2 = 1$. Vlastně se zde ptáme, zda na dotyčné hyperbole najdeme body s celočíselnými souřadnicemi. Tuto rovnici 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 $x^2 - n^2 = 1$ 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 (co vede napříč hranolem) celočíselnou. Dodnes není známo, zda taková cihla existuje. Jinak řečeno, hledá se sedm celých čísel splňujících rovnice

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

Můžete si hrát.

Jako poslední zajímavost si 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 výzkumník 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 i 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.

Tím končí naše povídání o diofantických rovnicích.