

Univerzita Karlova
Pedagogická fakulta
Katedra matematiky a didaktiky matematiky

BAKALÁŘSKÁ PRÁCE

Lineární diofantické rovnice a kongruence
Linear Diophantine equations and congruences

Natálie Kaňáková

Vedoucí práce: JUDr. Mgr. Filip Beran
Studijní program: Specializace v pedagogice
Studijní obor: Informační technologie se zaměřením na vzdělávání – Matematika se zaměřením na vzdělávání

Odevzdáním této bakalářské práce na téma Lineární diofantické rovnice a kongruence potvrzuji, že jsem ji vypracovala pod vedením vedoucího práce samostatně za použití v práci uvedených pramenů a literatury. Dále potvrzuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Praha, 11. 7. 2022

Velice děkuji vedoucímu této práce JUDr. Mgr. Filipovi Beranovi za rady a konzultace při psaní bakalářské práce a za inspirativní vedení seminářů, které vedly k napsání této práce. Také bych chtěla poděkovat rodině, kamarádům a kolegům za podporu při celém studiu.

ABSTRAKT

Bakalářská práce shrnuje a systematizuje poznatky o kongruencích a lineárních diofantických rovnicích. Práce je rozdělena do dvou částí. První část se věnuje kongruencím. Nejdříve ukazuje kongruence na příkladech z běžného života, popisuje kongruenci jako relaci, její vlastnosti a aplikaci v podobě výpočtu posledních cifer velkých čísel, odvození kritérií dělitelnosti nebo výpočtu data Velikonoc. Poté se zabývá kongruencemi obsahujícími neznámou, tedy kongruenčními rovnicemi; uvádí způsoby řešení lineárních kongruenčních rovnic a ilustruje je na příkladech. Posledním tématem první části jsou soustavy kongruencí a Čínská věta o zbytcích, její znění pro po dvou nesoudělná i soudělná čísla, algebraické znění, využití v různých typech úloh a při reprezentaci čísel pomocí zbytků. Druhá část je věnována lineárním diofantickým rovnicím, tedy rovnicím s neznámými z oboru celých čísel. Ukazuje metody řešení lineárních diofantických o dvou, třech i více neznámých – řešení s využitím Eukleidova algoritmu, redukční metodu, substituční metodu a další. V této části je také vysvětlen vztah mezi lineárními kongruencemi a lineárními diofantickými rovnicemi a využití tohoto vztahu při řešení kongruencí i diofantických rovnic. Nakonec se práce věnuje soustavám lineárních diofantických rovnic a způsobům jejich řešení. Ukazuje také geometrickou interpretaci diofantických rovnic a jejich soustav. Součástí každého tématu jsou nejen řešené příklady, ale i úlohy k procvičení, jejichž řešení je uvedeno na konci práce.

KLÍČOVÁ SLOVA

teorie čísel, kongruence, diofantické rovnice, Čínská věta o zbytcích

ABSTRACT

This bachelor's thesis summarizes and systematizes knowledge about congruences and linear Diophantine equations. This work is divided into two parts. The first part is dedicated to congruences. At first, it shows where we can find congruences in real life, congruence as a relation, its properties, and applications in calculating the last ciphers of large numbers, proofs of divisibility rules, or calculating the date of Easter. Afterward, we look into congruences containing unknowns – linear congruence equations. It looks into methods of solving linear congruences and illustrates them in exercises. The last topic of the first part is oriented on systems of linear congruences and the Chinese remainder theorem, both for non-coprime and coprime moduli, the algebraic version, applications in various types of problems, and modular representation of numbers. The second part of this thesis is dedicated to linear Diophantine equations – equations with integer solutions. It shows various methods of solving linear Diophantine equations with two, three, or more unknowns – the extended Euclidean algorithm, reduction method, substitution method, and others. This part also describes the relationship between linear congruences and linear Diophantine equations and the use of this relationship in solving both linear congruences and Diophantine equations. The last section deals with systems of linear Diophantine equations and methods of solving. This work also includes the geometric interpretation of Diophantine equations and systems of Diophantine equations. Each section includes solved examples and tasks for practicing with solutions at the end of this work.

KEYWORDS

number theory, congruences, Diophantine equations, Chinese remainder theorem

Obsah

Úvod	8
1 Lineární kongruence	10
1.1 Úvod: kongruence jako relace	11
1.1.1 Využití: odvození kritérií dělitelnosti.....	15
1.1.2 Využití: Gaussův výpočet data Velikonoc	19
1.2 Řešení lineárních kongruenčních rovnic.....	21
1.3 Čínská věta o zbytcích	26
1.3.1 Rozdělení velké kongruence na několik malých	34
1.3.2 Sloučení malých kongruencí do velké.....	40
1.3.3 Reprezentace čísel pomocí zbytků a algebraická verze.....	43
2 Lineární diofantické rovnice.....	45
2.1 Lineární diofantické rovnice o dvou neznámých.....	46
2.1.1 Řešení pomocí rozšířeného Eukleidova algoritmu.....	48
2.1.2 Řešení pomocí kongruencí	50
2.1.3 Redukční metoda	52
2.1.4 Další metody.....	52
2.2 Lineární diofantické rovnice o třech neznámých.....	56
2.2.1 Řešení pomocí rozšířeného Eukleidova algoritmu.....	57
2.2.2 Řešení pomocí kongruencí	59
2.2.3 Redukční metoda	60
2.2.4 Další metody.....	61
2.3 Lineární diofantické rovnice o čtyřech a více neznámých	64
2.4 Soustavy lineárních diofantických rovnic.....	66
Závěr.....	70

Seznam příkladů	71
Seznam úloh	74
Seznam použitých informačních zdrojů	78

Úvod

Teorie čísel je odvětví matematiky zabývající se především studiem celých čísel a jejich vlastností. Problémům s celočíselným řešením se věnovali lidé už od nepaměti. Je to logické, neboť v běžném životě se setkáváme s celými čísly daleko častěji než s čísly racionálními. Ať už počítáme lidi, živá zvířata, nebo cokoli jiného, co nemůžeme libovolně dělit, výsledky dávají smysl, jen pokud jsou celočíselné a ve většině případů zároveň kladné. Právě takovým problémům se v práci budeme věnovat. Také si představíme *modulární aritmetiku* neboli počítání se zbytky po dělení. Přestože to není na první pohled zřejmé, tato témata spolu úzce souvisí. Nejdříve se podíváme na abstraktnější z nich, tedy modulární aritmetiku, kterou poté využijeme při hledání celočíselných řešení rovnic.

První část začíná tříděním čísel do určitých skupin. V každé ze skupin budou čísla, která dávají po dělení nějakým daným číslem stejný zbytek. Tomuto vztahu říkáme *kongruence*. Kongruentní čísla můžeme ve výpočtech vzájemně nahrazovat a tím si zjednodušovat výpočty. S kongruencemi se setkáváme i v běžném životě, nejčastěji v souvislosti s časem. Když jdeme spát ve 22:40 a spíme 8 a půl hodiny, nikoho nepřekvapí, že se vzbudíme v 7:10, nikoli ve 30:70 nebo 31:10. Díky souvislosti s časem se tomuto počítání někdy říká hodinová nebo ciferníková aritmetika.

V první části si také ukážeme, jak můžeme kongruence použít při počítání posledních číslic velkých čísel, odvození kritérií dělitelnosti a pro výpočet data Velikonoc. Dále se podíváme na *lineární kongruenční rovnice* a hledání jejich řešení. Stejně jako u „obyčejných“ rovnic budeme hledat čísla, která můžeme do rovnice dosadit, aby daná rovnice platila. Poté se podíváme na *Čínskou větu o zbytcích*, která se týká soustav kongruenčních rovnic, s jejímž speciálním případem jsme se setkali už na základní škole.

Druhá část této práce se týká *lineárních diofantických rovnic*. Pod tímto poetickým názvem se nenachází nic jiného, než už zmiňované hledání celočíselných řešení rovnic. Protože existuje mnoho typů diofantických rovnic, zde se omezíme právě jen na ty nejjednodušší z nich – lineární. Podíváme se na rovnice o dvou i více neznámých a jejich soustavy. Ukážeme si několik metod řešení a praktické úlohy vedoucí na tyto rovnice. Rovněž se dozvíte, jak spolu obě části práce souvisejí a k čemu je dobré umět řešit rovnice kongruenční i diofantické.

Motivací pro výběr tohoto tématu byl předmět Teorie čísel, kde jsme se lineárním kongruencím a diofantickým rovnicím věnovali, ovšem při studiu chyběl nějaký shrnující text, který by se danými tématy zabýval. Tato práce tak může v příštích letech sloužit jako studijní opora pro tato témata.

Mezi hlavní zdroje patří kniha *Kouzlo čísel* (Křížek, 2018), věnující se tématům teorie čísel na hranici populárně-naučné a odborné úrovně, dále skripta *Diskrétní matematika* (Habala, 2019a; 2019b; 2019c) a skripta *Algebra* (Stanovský, 2022), jejichž dřívější verze byla vydána jako učebnice *Základy algebry* (Stanovský, 2010). Některé úlohy byly převzaty ze sbírek úloh pro základní školy (Česenek, 1994; Trejbal, 1995). Dalšími zdroji jsou různé české i zahraniční knihy, texty a internetové zdroje, na které budu v práci odkazovat.

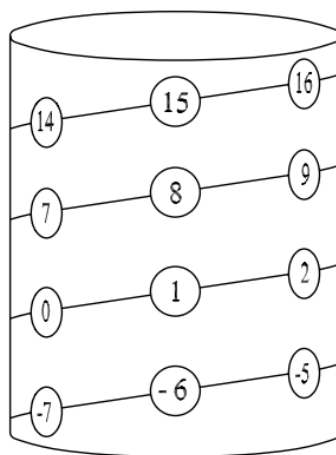
Věřím, že tato práce splní svůj účel a nabídne stručné shrnutí základních poznatků a metod týkajících se lineárních diofantických rovnic a kongruencí.

1 Lineární kongruence

Pojem *kongruence* včetně dodnes používaného značení ($\equiv$) zavedl německý matematik Carl Friedrich Gauss (1777–1855) v roce 1801 ve svém díle *Disquisitiones Arithmeticae*. Témata, kterými se budu v této práci zabývat, se v Gaussově díle nacházejí v prvních dvou sekcích. První sekce jeho díla se zabývá kongruencemi čísel obecně, druhá sekce je věnována kongruencím prvního řádu, tj. lineárním kongruencím (Gauss, 1986). Kongruencím se ale implicitně věnovali už matematici v Řecku, Číně i Indii v prvním tisíciletí našeho letopočtu, pouze je takto neznačili a nenazývali (Katz, 2009).

Vraťme se k situaci z úvodu. Proč platí, že když jdeme spát ve 22:40 a spíme 8 a půl hodiny, vstaneme v 7:10 a nikoli v 30:70 nebo 31:10? Jelikož každá hodina má 60 minut, vždy počítáme po tomto časovém úseku minuty od nuly. Matematicky bychom řekli, že počítáme *modulo 60*, čísla 10 a 70 jsou *kongruentní modulo 60* a píšeme $10 \equiv 70 \pmod{60}$. Oproti tomu hodiny počítáme *modulo 24*, protože každý den má 24 hodin.

Kongruence rozděluje čísla do skupin obsahujících navzájem kongruentní. Takových skupin, které obsahují čísla navzájem kongruentní, bude například při počítání modulo 24 přesně 24. Graficky si můžeme kongruenci představit tak, že na válec navineme provázek, na kterém leží postupně všechna celá čísla. Čísla, která leží nad sebou, jsou navzájem kongruentní a všechna patří do jedné skupiny.



Obr. 1: Grafická interpretace kongruence modulo 7 (Křížek, 2018, s. 40)

Každé z čísel bude jednoznačně náležet jedné z těchto skupin. Těmto skupinám říkáme třídy ekvivalence a kongruenci můžeme chápat jako relaci ekvivalence. Kongruenci jako relaci se budeme věnovat v první podkapitole.

Ve chvíli, kdy na nějakou stranu kongruence přidáme neznámou, dostaneme kongruenční rovnici. V této práci se budu zabývat pouze lineárními kongruenčními rovnicemi, tedy rovnicemi obsahujícími neznámou pouze v první mocnině. Tyto rovnice se označují také jako *lineární kongruence* nebo jednoduše jen jako *kongruence* a bude jim věnována druhá podkapitola.

1.1 Úvod: kongruence jako relace

Než zadefinujeme samotnou kongruenci, připomeneme si, co je to dělitelnost a další příbuzné pojmy, a uvedeme si větu, která nás bude provázet celou kapitolou o kongruencích.

Pozn.: Na základní škole se dělitelnost typicky definuje v přirozených číslech (většinou se téma dělitelnosti dokonce probírá dříve, než se žáci formálně seznámí s celými čísly), v této práci budeme používat rozšíření dělitelnosti na celá čísla. Naopak největší společný násobek a nejmenší společný dělitel budou v této práci vždy z přirozených čísel v zájmu zachování jednoznačnosti.

Definice 1 (Dělitelnost v $\mathbb{Z}$)

Nechť $a, b \in \mathbb{Z}$. Řekneme, že číslo a *dělí* číslo b , jestliže existuje číslo $c \in \mathbb{Z}$ takové, že $ac = b$. Tuto relaci nazýváme *dělitelnost* a píšeme $a \mid b$.

Definice 2 (Největší společný dělitel)

Největší společný dělitel celých čísel $a_1, a_2, \dots, a_k$ je největší přirozené číslo c splňující $c \mid a_i$ pro všechna $i \in \{1, 2, \dots, k\}$. Značíme $c = D(a_1, a_2, \dots, a_k)$.

Definice 3 (Nejmenší společný násobek)

Nejmenší společný násobek celých čísel $a_1, a_2, \dots, a_k$ je nejmenší přirozené číslo c splňující $a_i \mid c$ pro všechna $i \in \{1, 2, \dots, k\}$. Značíme $c = n(a_1, a_2, \dots, a_k)$.

Věta 1 (Dělení celých čísel se zbytkem, též Eukleidovské dělení)

Nechť $a, b \in \mathbb{Z}$, $b \neq 0$. Pak existuje právě jedna dvojice celých čísel q, r splňující $a = q \cdot b + r$ a $0 \leq r < |b|$.

Důkaz: Pro jednoduchost předpokládejme $a, b > 0$, ostatní případy by se řešily analogicky. Nechť q je největší číslo, pro které platí $q \cdot b \leq a$. Položme $r = a - q \cdot b$. Z toho vyplývá, že $0 \leq r < b$ a $a = q \cdot b + r$.

Kdyby existovalo více dvojic q, r , tedy $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$, pak by platilo $b(q_1 - q_2) = r_2 - r_1$, tedy $b \mid r_2 - r_1$. Ovšem $0 \leq |r_2 - r_1| < |b|$, proto musí $r_2 - r_1 = 0$. Z toho plyne $r_1 = r_2$ a také $q_1 = q_2$. (Stanovský, 2022, s. 22)

Definice 4 (Kongruence)

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

Příklad 1.1 Najděte nejmenší přirozené číslo, se kterým je kongruentní číslo 14 modulo 6.

Řešení: $14 \equiv 2 \pmod{6}$, protože $14 - 2 = 12$ a 6 dělí 12.

Často bude užitečné nahlížet na kongruenci i jinak:

Věta 2 (Ekvivalentní vyjádření kongruence)

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

- (i) $a \equiv b \pmod{n}$,
- (ii) existuje $k \in \mathbb{Z}$ takové, že $a = b + kn$,
- (iii) $a \bmod n = b \bmod n$, tj. jsou si rovny zbytky po dělení číslem n .

Důkaz: Jedná se o tři tvrzení, z nichž každé dvě jsou si ekvivalentní. Místo toho, abychom dokazovali ekvivalenci každých dvou tvrzení dokazováním jednotlivých implikací, dokážeme implikace (i) $\Rightarrow$ (ii), (ii) $\Rightarrow$ (iii) a (iii) $\Rightarrow$ (i), z čehož plyne také například implikace (ii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): Z definice kongruence platí $n \mid a - b$, neboli existuje $k \in \mathbb{Z}$: $kn = a - b$. Tedy $a = b + kn$.

(ii) $\Rightarrow$ (iii): Předpokládáme $a = b + kn$ pro nějaké $k \in \mathbb{Z}$. Necht' r je zbytek po dělení čísla b číslem n , tedy $r = b \bmod n$. Potom můžeme psát $b = qn + r$, $q \in \mathbb{Z}$, $0 \leq r < n$. Pak $a = b + kn = qn + r + kn = (q + k)n + r$, kde $(q + k) \in \mathbb{Z}$ a $0 \leq r < n$. Jde tedy o rozklad z věty o dělení celých čísel a $r = a \bmod n = b \bmod n$, tedy zbytky se rovnají.

(iii) $\Rightarrow$ (i): Necht' $a \bmod n = b \bmod n = r$. Pak existují $p, q \in \mathbb{Z}$ takové, že $a = pn + r$ a $b = qn + r$. Odtud $a - b = (p - q)n$, $(p - q) \in \mathbb{Z}$, tedy $n \mid a - b$, což z definice znamená, že $a \equiv b \pmod{n}$. (Habala, 2019a, s. 1-2)

Ekvivalenci podmínek si můžeme vyzkoušet na výše uvedeném příkladu $14 \equiv 2 \pmod{6}$. Podle věty má být tato kongruence ekvivalentní s tvrzením $14 = 2 + 6k$, což je zjevně pravda pro $k = 2$, a také mají mít čísla 14 a 2 stejný zbytek po dělení 6, což platí, protože obě čísla dávají zbytek 2.

Když budeme počítat s jedním konkrétním modulem n , dostaneme n skupin čísel daných zbytky po dělení číslem n . Pokud počítáme modulo 6, dostaneme 6 skupin čísel. První skupinou budou čísla, která jsou dělitelná šesti (tedy dávají po dělení šesti zbytek 0), například čísla $-12, 0, 6$ nebo 300 . Další skupinou jsou čísla, která dávají po dělení šesti zbytek 1, tedy například čísla $1, 7, 19$ nebo -5 (když snížíme -5 o 1, dostaneme -6 , tedy číslo dělitelné šesti). Prvky této skupiny budou všechna čísla ve tvaru $1 + 6k$; $k \in \mathbb{Z}$. Další skupiny bychom dostali pro zbytky 2, 3, 4 a 5.

Když se blíže podíváme na relaci „být kongruentní modulo n “, zjistíme, že má tyto vlastnosti:

- (i) $a \equiv a \pmod{n}$,
- (ii) jestliže $a \equiv b \pmod{n}$, pak $b \equiv a \pmod{n}$,
- (iii) jestliže $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, potom $a \equiv c \pmod{n}$

pro všechna $a, b, c \in \mathbb{Z}$ a všechna $n \in \mathbb{N}$.

Všechny vlastnosti jsou zřejmé ve chvíli, když se na kongruence budeme dívat jako na zbytky po dělení, můžeme je dokázat ale také z definice. Vlastnost (i) znamená, že $n \mid a - a = 0$, což platí, protože $n \mid 0$. Bod (ii) říká, že jestliže $n \mid a - b$, pak $n \mid b - a$, což je zřejmě pravda, protože pokud n dělí nějaké číslo, pak dělí i číslo k němu opačné.

Pohledem na kongruence jako na zbytky po dělení číslem n vidíme, že jestliže a má stejný zbytek po dělení jako b , pak b má stejný zbytek po dělení jako a . Vlastnost (iii) říká, že má-li číslo a stejný zbytek po dělení jako číslo b a číslo b jako číslo c , pak také číslo a má stejný zbytek po dělení jako číslo c , což je triviální, neboť zbytky jsou definovány modulo n jednoznačně.

Relace $\equiv$ je tedy reflexivní (i), symetrická (ii) a tranzitivní (iii), neboli je to relace ekvivalence. Třídami ekvivalence jsou množiny čísel se stejným zbytkem po dělení číslem n . (Habala, 2019a, s. 2; Stanovský, 2022, s. 5)

Věta 3 (Vlastnosti kongruence)

Nechť $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$. Pak platí

- $a + c \equiv b + d \pmod{n}$,
- $a - c \equiv b - d \pmod{n}$,
- $a \cdot c \equiv b \cdot d \pmod{n}$
- $a^k \equiv b^k \pmod{n}$ pro každé přirozené číslo k .

Důkaz: Z předpokladu $n \mid a - b$ a $n \mid c - d$ plyne

- $n \mid (a - b) + (c - d) = (a + c) - (b + d)$, tedy $a + c \equiv b + d \pmod{n}$,
- $n \mid (a - b) - (c - d) = (a - c) - (b - d)$, tedy $a - c \equiv b - d \pmod{n}$,
- $n \mid (a - b) \cdot c$ a $n \mid (c - d) \cdot d$, tedy $n \mid (a - b) \cdot c + (c - d) \cdot b = ac - bd$, neboli $a \cdot c \equiv b \cdot d \pmod{n}$.

Poslední tvrzení dokážeme indukcí: $a^{i+1} = a^i \cdot a \equiv b^i \cdot b = b^{i+1} \pmod{n}$. (Stanovský, 2022, s. 5)

Příklad 1.2 Vypočítejte $48^{111} + 2^{34} \pmod{7}$.

Řešení: Víme, že $48 \equiv -1 \pmod{7}$ a $2^3 = 8 \equiv 1$. Proto $48^{111} + 2^{34} = 48^{111} + 2 \cdot 2^{33} = 48^{111} + 2 \cdot (2^3)^{11} \equiv (-1)^{111} + 2 \cdot 1^{11} = -1 + 2 = 1$

Zamysleme se, jak je to s dělením. Platí $12 \equiv 3 \pmod{9}$, pokud bychom obě strany kongruence vydělili 3, dostali bychom $4 \equiv 1 \pmod{9}$, což zjevně není pravda. Musíme proto vydělit i modulo, dostaneme tedy $4 \equiv 1 \pmod{3}$, což platí. Podrobněji v následující větě:

Věta 4 (Vlastnosti kongruence II)

Nechť $a, b, c, n \in \mathbb{Z}; c, n \neq 0$. Pak

- $a \equiv b \pmod{n} \Leftrightarrow ca \equiv cb \pmod{cn}$;
- jsou-li c, n nesoudělná, pak $a \equiv b \pmod{n} \Leftrightarrow ca \equiv cb \pmod{n}$.

Důkaz: (1) Obě strany si přepíšeme podle definice. Nalevo dostaneme $a - b = nq$, $q \in \mathbb{Z}$, napravo dostaneme $ca - cb = c(a - b) = cnq$. Po vykrácení dostaneme stejný výraz jako z levé strany.

(2) Implikace $(\Rightarrow)$ plyne z Věty 3. Implikace $(\Leftarrow)$: Nechť $n \mid ca - cb = c(a - b)$. Uvažujeme libovolnou mocninu p^k z prvočíselného rozkladu čísla n . Protože jsou čísla c, n nesoudělná, musí p^k dělit $a - b$. Úvahou přes všechny mocniny dostaneme $n \mid a - b$. (Stanovský, 2022, s. 5)

Úlohy

1.1 Určete, jaký zbytek dává číslo 5^{81} po dělení 26.

1.2 Určete poslední číslici čísla 77^{333} .

1.3 Určete paritu, poslední cifru a zbytek po dělení sedmi čísla $N = 22 \cdot 31 + 11 \cdot 17 + 13 \cdot 19$. (Čermák, 2020, s. 9)

1.1.1 Využití: odvození kritérií dělitelnosti

S dělitelností se setkáváme už na základní škole, většinou ve formě tvrzení bez většího porozumění. Ukážeme si, jak lze některá pravidla odvodit jednoduše pomocí kongruencí a jak vypadá obecné kritérium dělitelnosti. Podrobněji o méně známých kritériích dělitelnosti píše Slavík (2018). Dělitelnost čísla 2, 4, 5, 8, 10 apod. si zde ukazovat nebudeme, neboť jejich odvození je triviální.

Dělitelnost třemi

Pravidlo pro dělitelnost třemi říká, že číslo je dělitelné třemi právě tehdy, když je jeho ciferný součet dělitelný třemi. Každé číslo a můžeme jednoznačně zapsat jako $n = n_k \cdot 10^k + \dots + n_2 \cdot 10^2 + n_1 \cdot 10 + n_0$, kde $n_0, \dots, n_k, k \in \mathbb{N}$ jsou čísla z množiny $\{0, \dots, 9\}$, tedy jednotlivé cifry čísla n . Zároveň pro všechna $i \in \mathbb{N}$ platí $10^i \equiv 1 \pmod{3}$, protože například $10\,000 = 9\,999 + 1 = 3 \cdot 3\,333 + 1 \equiv 1 \pmod{3}$, obecně platí

$10^i = 3 \cdot 3 \sum_{k=0}^{i-1} 10^k + 1$, kde je první člen vždy dělitelný třemi, takže zůstane pouze 1. Po dělení třemi můžeme v každém členu rozvinutého zápisu čísla n nahradit mocninu deseti jedničkou. Dostaneme tedy pouze $n_k + \dots + n_2 + n_1 + n_0$, což je ciferný součet čísla n . Z toho vyplývá, že ciferný součet čísla n dává po dělení třemi stejný zbytek, jako dostaneme po dělení původního čísla třemi. Pokud tedy tento součet dává zbytek po dělení třemi zbytek nula, číslo je dělitelné třemi.

Příklad 1.3 Jaký je zbytek po dělení třemi čísla 5 342 019?

Řešení: Spočítáme ciferný součet: $5 + 3 + 4 + 2 + 0 + 1 + 9 = 24$. Toto číslo je násobek 3, takže zbytek po dělení třemi je 0, neboli číslo je dělitelné třemi. Pokud nevíme, jaký je zbytek po dělení třemi, pravidlo můžeme použít opakovaně. Protože $2 + 4 = 6$ dává po dělení třemi zbytek 0, původní číslo dává po dělení třemi také zbytek nula, tedy je dělitelné třemi.

Dělitelnost devíti

Obdobně jako u dělitelnosti třemi, protože $10^i \equiv 1 \pmod{9}$ pro všechna $i \in \mathbb{N}$.

Příklad 1.4 Jaký je zbytek po dělení devíti čísla 5 342 019?

Řešení: Jak jsme spočítali v příkladu 1.3, ciferný součet tohoto čísla je 24. Po dělení tohoto čísla devíti dostaneme zbytek 6, proto zbytek po dělení devíti je 6 (nebo opět můžeme použít pravidlo opakovaně, čímž dostaneme ciferný součet $2 + 4 = 6$, takže zbytek po dělení je 6.)

Dělitelnost jedenácti

Pro odvození pravidla dělitelnosti budeme sledovat, jak se chovají mocniny 10 modulo 11:

$$10^0 \equiv 1 \pmod{11},$$

$$10^1 \equiv 10 \equiv -1 \pmod{11},$$

$$10^2 \equiv 1 \pmod{11},$$

$$10^3 \equiv 10 \equiv -1 \pmod{11},$$

$$\text{atd., obecně } 10^i \equiv (-1)^i \pmod{11}.$$

Můžeme tedy při počítání modulo 11 nahradit v rozvinutém zápisu čísla všechny sudé mocniny deseti číslem 1 a všechny liché mocniny deseti číslem -1 :
 $n \equiv n_k \cdot (-1)^k + n_{k-1} \cdot (-1)^{k-1} + \dots + n_0 \cdot 1 \pmod{11}$.

Výraz napravo je rozdíl součtu číslic na lichých pozicích a součtu číslic na sudých pozicích (počítáno zprava). Pokud je tento výraz kongruentní s 0 modulo 11, je i původní číslo kongruentní s 0 modulo 11, neboli je dělitelné jedenácti. Pokud je výraz kongruentní s jiným číslem, tedy dává nějaký zbytek r , původní číslo dává po dělení 11 také zbytek r .

Dělitelnost jedenácti se využívá v České republice u přidělování rodných čísel. Poslední čtyřčíslí je voleno tak, aby bylo celé číslo dělitelné 11. Mírně složitější algoritmus, který ale také využívá dělitelnosti jedenácti, se využívá u čísel bankovních účtů, čísel ISBN a dalších.

Příklad 1.5 Jaký je zbytek po dělení jedenácti čísla 5 342 019?

Řešení: Spočítáme rozdíl součtu čísel na sudých a lichých pozicích: $(5 + 4 + 0 + 9) - (3 + 2 + 1) = 12$. Vidíme, že zbytek po dělení jedenácti je 1.

Dělitelnost sedmi

Postupujeme stejně jako u dělitelnosti jedenácti. Budeme pozorovat, jak se chovají mocniny 10 při počítání modulo 7:

$$\begin{aligned} 10^0 &\equiv 1 \pmod{7}, \\ 10^1 &\equiv 3 \pmod{7}, \\ 10^2 &\equiv 2 \pmod{7}, \\ 10^3 &\equiv 6 \equiv -1 \pmod{7}, \\ 10^4 &\equiv 4 \pmod{7}, \\ 10^5 &\equiv 5 \pmod{7}, \\ 10^6 &\equiv 1 \pmod{7}, \\ &\vdots \end{aligned}$$

Všimněme si, že na každém třetím místě dostáváme střídavě 1 a -1 . Tentokrát tedy nebudeme brát jednotlivé cifry, ale trojčíslí, která budeme střídavě přičítat a odčítat. Pokud tímto postupem vyjde číslo dělitelné 7, je i původní číslo dělitelné 7. Pokud vyjde dělením tohoto čísla nějaký zbytek, stejný zbytek dává i původní číslo po dělení 7.

Zde si ukážeme ještě druhý způsob. Vidíme, že po dělení 7 dostáváme pro jednotlivé mocniny 10 zbytky 1, 3, 2, 6, 4, 5, které se poté periodicky opakují. Tyto mocniny tak můžeme nahradit příslušnými zbytky a pro libovolné n dostaneme

$$n \equiv n_0 \cdot 1 + n_1 \cdot 3 + n_2 \cdot 2 + n_3 \cdot 6 + n_4 \cdot 4 + n_5 \cdot 5 + \dots \pmod{7}.$$

Tedy zbytek libovolného čísla po dělení sedmi je stejný jako zbytek čísla získaného tak, že první, druhou, ... číslici odzadu násobíme postupně čísla z periodické posloupnosti 1, 3, 2, 6, 4, 5 a tyto součiny sečteme.

Příklad 1.6 Jaký je zbytek po dělení sedmi čísla 5 342 019?

Řešení: Prvním způsobem získáme $5 - 342 + 19 = -318$. Po dělení sedmi dostaneme číslo -3 , které je kongruentní s číslem 4. Zbytek po dělení je tedy číslo 4.

Druhým způsobem budeme počítat $9 \cdot 1 + 1 \cdot 3 + 0 \cdot 2 + 2 \cdot 6 + 4 \cdot 4 + 3 \cdot 5 + 5 \cdot 1 = 60$. Po dělení sedmi dostaneme zbytek 4.

Dělitelnost třinácti

Stejně jako v předchozích případech si napíšeme zbytky po dělení 13 pro jednotlivé mocniny 10:

$$\begin{aligned} 10^0 &\equiv 1 \pmod{13}, \\ 10^1 &\equiv 10 \pmod{13}, \\ 10^2 &\equiv 9 \pmod{13}, \\ 10^3 &\equiv 12 \equiv -1 \pmod{13}, \\ 10^4 &\equiv 3 \pmod{13}, \\ 10^5 &\equiv 4 \pmod{13}, \\ 10^6 &\equiv 1 \pmod{13}, \\ &\text{atd.} \end{aligned}$$

Stejně jako u dělitelnosti sedmi můžeme přičítat a odčítat jednotlivá trojčíslí, protože na každém třetím místě dostáváme střídavě 1 a -1 . Při použití druhého kritéria bychom jednotlivé mocniny 10 nahrazovali posloupností 1, 10, 9, 12, 3, 4 ...

Výsledek je dělitelný 13 právě tehdy, když původní číslo je dělitelné 13. Pokud výsledek 13 dělitelný není a zůstane nějaký zbytek, stejný zbytek dává po dělení 13 i původní číslo.

Příklad 1.7 Jaký je zbytek po dělení třinácti čísla 5 342 019?

Řešení: Sčítáme a odčítáme jednotlivá trojčíslí, tedy: $5 - 342 + 19 = -318$. Když toto číslo vydělíme 13, dostaneme zbytek -6 ; protože zbytky rozumíme nezáporná čísla (bude definováno v další kapitole), přičtením 13 dostaneme zbytek 7.

Druhým způsobem získáme $9 \cdot 1 + 1 \cdot 10 + 0 \cdot 9 + 2 \cdot 12 + 4 \cdot 3 + 3 \cdot 4 + 5 \cdot 1 = 72$. Nejbližší menší číslo dělitelné 13 je 65, proto zbytek je 7.

Obecné kritérium dělitelnosti

Zmiňovaný postup můžeme použít obecně pro dělitelnost libovolným přirozeným číslem m . Tedy:

- 1) Pro všechna $i \in \mathbb{N}_0$ najdeme $a_i \in \mathbb{Z}$ takové, že $10^i \equiv a_i \pmod{m}$.
- 2) Pro libovolné přirozené číslo $n = n_k \cdot 10^k + \dots + n_2 \cdot 10^2 + n_1 \cdot 10 + n_0$ platí
$$n \equiv n_k \cdot a_k + \dots + n_2 \cdot a_2 + n_1 \cdot a_1 + n_0. \text{ (Slavík, 2018)}$$

Úlohy

1.4 Ověřte si, že vaše rodné číslo je dělitelné jedenácti.

1.5 Určete, jaký zbytek dostaneme, když číslo 4 294 967 297 vydělíme

- a) třemi,
- b) devíti,
- c) jedenácti,
- d) sedmi,
- e) třinácti.

1.6 Odvoďte dělitelnost číslem 73.

1.1.2 Využití: Gaussův výpočet data Velikonoc

Velikonoce jsou pohyblivým svátkem, tj. každý rok připadají na jiné datum. Velikonoční neděle byla stanovena první neděle po prvním jarním úplňku. Přesné datum Velikonoc se až do počátku 19. století počítalo velice složitým způsobem, kdy bylo nutné využívat několika proměnných. V roce 1800 publikoval německý matematik Carl Friedrich Gauss algoritmus výpočtu data Velikonoc, jehož jediným vstupním údajem byl rok a tím výpočet

značně zjednodušil. K výpočtu Gauss používal kongruence. Pro roky 1900 až 2099 vypadá výpočet takto:

$$a := r \bmod 19,$$

$$d := 24 + 19a \bmod 30,$$

$$b := r \bmod 4,$$

$$e := 5 + 2b + 4c + 6d \bmod 7.$$

$$c := r \bmod 7,$$

Velikonoční neděle nastává $d + e$ dní po 22. březnu kromě případu, kdy $d + e = 35$, kdy je o týden dříve, a let 1954 a 2049, kdy také nastává o týden dříve. (Křížek, 2018, s. 41; Novotný, 2016; Gauss, 1800)

Příklad 1.8 Vypočítejte, kdy nastane Velikonoční neděle v roce 2042.

Řešení:

$$a = 2042 \bmod 19 = 9$$

$$b = 2042 \bmod 4 = 2$$

$$c = 2042 \bmod 7 = 5$$

$$d = 24 + 19a \bmod 30 = 24 + 19 \cdot 9 \bmod 30 = 195 \bmod 30 = 15$$

$$e = 5 + 2b + 4c + 6d \bmod 7 = 5 + 2 \cdot 2 + 4 \cdot 5 + 6 \cdot 15 \bmod 7 = 119 \bmod 7 = 0$$

$$d + e = 15 + 0 = 15$$

Velikonoční neděle tedy nastává 15 dní po 22. březnu neboli 6. dubna.

Úlohy

1.7 Vypočítejte datum Velikonoční neděle v následujícím roce.

1.2 Řešení lineárních kongruenčních rovnic

Zatím jsme chápali kongruenci jako relaci, která nám říkála, jaká čísla jsou ekvivalentní modulo n , neboli jaká čísla mají stejný zbytek po dělení číslem n . V této kapitole se podíváme na kongruence jako rovnice, tedy na aspoň jedné straně se bude vyskytovat neznámá. Budeme hledat hodnoty, které můžeme za neznámou dosadit, aby byly obě strany rovnice kongruentní.

Definice 5 (Lineární kongruence)

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 . (Habala, 2019b, s. 10)

Podívejme se na několik lineárních kongruencí.

Příklad 1.9 Vyřešte následující lineární kongruence:

- a) $5x \equiv 3 \pmod{2}$
- b) $2x \equiv 3 \pmod{7}$
- c) $2x \equiv 3 \pmod{4}$
- d) $2x \equiv 2 \pmod{5}$
- e) $2x \equiv 2 \pmod{4}$

Řešení:

- a) $5x \equiv 3 \pmod{2}$

Co tento zápis znamená? Podle definice platí $2 \mid 5x - 3$. Pravou stranu můžeme upravit na $5x - 3 = 4x + x - 2 - 1 = (4x - 2) + (x - 1)$. Platí tedy $2 \mid (4x - 2) + (x - 1)$. Protože $2 \mid 4$ a $2 \mid 2$, výraz v první závorce je určitě dělitelný dvěma. Zůstalo nám $2 \mid x - 1$. Když toto nyní přepíšeme zpět jako kongruenci, dostaneme $x \equiv 1 \pmod{2}$. Která čísla tuto kongruenci splňují? Určitě číslo 1, ale jistě také čísla 3, 5, 7, ..., tedy všechna lichá čísla. To stále není vše, protože například pro $x = -1$ je kongruence také platná, protože $-1 - 1 = -2$ a $2 \mid -2$. Za neznámou x můžeme tedy dosadit jakékoli liché číslo (kladné i záporné). Algebraický tvar řešení vypadá takto: $x = 1 + 2k$, $k \in \mathbb{Z}$.

b) $2x \equiv 3 \pmod{7}$

Hledáme číslo, které bude po vynásobení dvěma o tři větší než nějaký násobek 7. Číslo o 3 větší, než je jednonásobek 7, je číslo 10. My potřebujeme jen jeho polovinu, čímž dostaneme řešení $x = 5$. Není to ale jediné řešení; kongruenci vyhovuje například také $x = 12$, protože číslo 24 dává po dělení sedmi opět zbytek 3. Řešením budou tedy všechna čísla ve tvaru $5 + 7k$, $k \in \mathbb{Z}$, protože přičtením k -násobku modulu se zbytek po dělení nezmění.

c) $2x \equiv 3 \pmod{4}$

Jakékoli číslo vynásobené dvěma je sudé číslo, proto nalevo dostaneme vždy sudé číslo. Po dělení sudého čísla čtyřmi nikdy nemůžeme dostat lichý zbytek, proto tato rovnice nemá řešení.

d) $2x \equiv 2 \pmod{5}$

Stejně jako u „obyčejné“ rovnice můžeme obě strany kongruence vydělit dvěma. Dostaneme kongruenční rovnici $x \equiv 1 \pmod{5}$. Řešením jsou všechna čísla o jedna větší než 5, tedy čísla ve tvaru $x = 1 + 5k$, $k \in \mathbb{Z}$.

e) $2x \equiv 2 \pmod{4}$

Pokud budeme postupovat stejně jako u předchozí kongruence, dostaneme kongruenci $x \equiv 1 \pmod{4}$, která má řešení $x = 1 + 4k$, $k \in \mathbb{Z}$ (obdobně jako v přechozích příkladech). Jenže to nejsou všechna řešení – rovnici vyhovuje také například $x = 3$ a tedy i další čísla ve tvaru $3 + 4k$, $k \in \mathbb{Z}$.

Z prvního řešení dostaneme množinu čísel $\{\dots, -7, -3, 1, 5, 9, \dots\}$, ze druhého $\{\dots, -5, -1, 3, 7, 11, \dots\}$.

Sjednocením těchto množin dostaneme množinu všech lichých čísel, tedy čísla ve tvaru $1 + 2k$, $k \in \mathbb{Z}$.

Čím se kongruence e) liší od kongruence d)? Čísla a, b, n jsou v kongruenci e) soudělná, protože všechna tři čísla můžeme dělit dvěma. Pokud bychom původní kongruenci $2x \equiv 2 \pmod{4}$ celou zkrátili dvěma, dostali bychom kongruenci $x \equiv 1 \pmod{2}$, jejíž

řešení odpovídá námi nalezenému řešení $x = 1 + 2k$, $k \in \mathbb{Z}$ (viz a)). Z toho vyplývá, že pokud při dělení rovnice můžeme zkrátit i modulo, musíme to udělat, abychom nepřišli o některá řešení (Věta 4).

Tvar řešení lineárních kongruencí zobecníme v následující větě.

Věta 5 (Řešitelnost a tvar řešení lineární kongruence)

Necht' $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$.

- (i) Jestliže b není násobkem $D(a, n)$, řešení rovnice $ax \equiv b \pmod{n}$ neexistuje.
- (ii) Jestliže $D(a, n)$ dělí b , rovnice $ax \equiv b \pmod{n}$ má nějaké řešení $x_p \in \mathbb{Z}$.

Označme $n' = \frac{n}{D(a, n)}$. Množina všech řešení lineární kongruence $ax \equiv b \pmod{n}$ je $\{x_p + kn'; k \in \mathbb{Z}\}$. (Habala, 2019b)

Každou lineární kongruenci o jedné neznámé můžeme převést na lineární diofantickou rovnici o dvou neznámých a tu některou z metod vyřešit (viz podkapitolu 2.1). Z toho vyplývá i důkaz Věty 5. Často to ale není nejvýhodnější postup, protože vhodnými úpravami kongruence můžeme získat řešení v některých případech daleko rychleji. Několik typických úprav si ukážeme na následujících kongruencích.

Příklad 1.10

- a) Zmenšení koeficientů pomocí modulu

První krok, který bychom měli udělat, protože je téměř vždy výhodné počítat s co nejmenšími čísly.

$$46x \equiv 127 \pmod{15}$$

$$x \equiv 7 \pmod{15}$$

$$x = 7 + 15k$$

- b) Vydělení celé kongruence nenulovým celým číslem

$$3x \equiv 6 \pmod{10}$$

$$x \equiv 2 \pmod{10}$$

$$x = 2 + 10k$$

Pozor, jak už jsme uvedli výše, pokud můžeme daným číslem vydělit i modulo, musíme tak učinit (Věta 4):

$$3x \equiv 6 \pmod{9}$$

$$x \equiv 2 \pmod{3}$$

$$x = 2 + 3k$$

c) Přičtení násobku modulu k jedné či oběma stranám

$$4x \equiv 1 \pmod{15}$$

$$4x \equiv 16 \pmod{15}$$

$$x \equiv 4 \pmod{15}$$

$$x = 4 + 15k$$

d) Odečtení násobku modulu od jedné nebo od obou ze stran

$$11x \equiv 8 \pmod{13}$$

$$-2x \equiv 8 \pmod{13}$$

$$x \equiv -4 \equiv 9 \pmod{13}$$

$$x = 9 + 13k$$

e) Vynásobení obou stran kongruence stejným nenulovým celým číslem, které je nesoudělné s modulem

$$5x \equiv 3 \pmod{14}$$

$$15x \equiv 9 \pmod{14}$$

$$x \equiv 9 \pmod{14}$$

$$x = 9 + 14k$$

Pokud bychom násobili kongruenci číslem, které je soudělné s modulem, museli bychom vynásobit také modul (Věta 4). Taková úprava nám ale v hledání řešení nepomůže.

Ve všech případech $k \in \mathbb{Z}$.

Zjištění, kterým číslem máme kongruenci vynásobit, není vždy tak jednoduché jako u výše uvedeného příkladu. Pokud chceme nalevo dostat pouze x , musíme výraz ax vynásobit číslem inverzním k číslu a (počítáno modulo n), tedy číslem a^{-1} . Tím nalevo dostaneme

$a^{-1}ax = x$. Inverzní číslo k číslu a najdeme buď zkoušením různých čísel, nebo systematicky pomocí řešení diofantické rovnice $ax + mn = 1$ (viz další kapitola). Blíže hledání inverzních čísel rozebírá Habala (2019a).

Úlohy

1.8 Najděte všechna řešení kongruenčních rovnic

- a) $4x \equiv 1 \pmod{7}$
- b) $7x \equiv 5 \pmod{4}$
- c) $8x \equiv 0 \pmod{12}$
- d) $51x \equiv 4 \pmod{34}$
- e) $200x \equiv 240 \pmod{101}$
- f) $200x \equiv 240 \pmod{360}$

1.3 Čínská věta o zbytcích

Čínská věta o zbytcích (také *Čínská zbytková věta*) vychází z problému, který formuloval ve své knize o aritmetice okolo 3.–5. století staročínský matematik Sun Zi (Křížek, 2018, s. 42; Stanovský, 2022, s. 8–9).

Příklad 1.11 Necht' x označuje určitý počet předmětů. Počítáme-li je po trojicích, zbydou dva, počítáme-li je po peticích, zbydou tři, a konečně počítáme-li je po sedmicích, zbydou dva. Kolik je x ?

Úlohu můžeme přepsat na soustavu tří kongruencí (o jedné neznámé x):

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}.$$

Řešení podle autora úlohy je podrobně uvedeno v (Katz, 2009, s. 222–223). Zde si postup uvedeme ve zkratce. Sun Zi si všiml, že

$$70 \equiv 1 \pmod{3} \equiv 0 \pmod{5} \equiv 0 \pmod{7},$$

$$21 \equiv 1 \pmod{5} \equiv 0 \pmod{3} \equiv 0 \pmod{7},$$

$$15 \equiv 1 \pmod{7} \equiv 0 \pmod{3} \equiv 0 \pmod{5}.$$

Proto $2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233$ vyhovuje zadaným kongruencím. Protože číslo 105 je dělitelné 3, 5 i 7, můžeme toto číslo od řešení odečíst a výsledek bude pořád zadaným kongruencím vyhovovat. Abychom dostali nejmenší možné řešení, odečteme číslo 105 dvakrát a dostaneme $233 - 210 = 23$, což je nejmenší možné řešení v kladných číslech. Tuto metodu využijeme i v důkazu Čínské věty o zbytcích.

Jiný způsob řešení vypadá takto:

Řešením kongruence $x \equiv 2 \pmod{3}$ je $x = 2 + 3k$, $k \in \mathbb{Z}$.

Toto řešení dosadíme do druhé kongruence a dostaneme $2 + 3k \equiv 3 \pmod{5}$.

$$3k \equiv 1 \pmod{5}$$

$$3k \equiv 6 \pmod{5}$$

$$k \equiv 2 \pmod{5}$$

Před formulací samotné Čínské věty o zbytcích uvedeme ještě jinou větu, které využijeme v důkazu Čínské věty o zbytcích a bude nás provázet celou kapitolou o diofantických rovnicích.

Věta 6 (Bézoutova rovnost)

Pro každou dvojici celých čísel a, b existují celá čísla u, v (tzv. *Bézoutovy koeficienty*) splňující $D(a, b) = u \cdot a + v \cdot b$.

Důkaz: Pokud $a = 0$, pak $D(0, b) = b = 0 \cdot a + 1 \cdot b$, obdobně pro $b = 0$. Budeme tedy předpokládat $a, b \neq 0$.

Uvažujeme množinu M všech celých čísel ve tvaru $ua + vb$, kde $u, v \in \mathbb{Z}$. Tato množina jistě obsahuje kladná celá čísla, protože kdyby číslo $t = ua + vb$ bylo záporné, číslo $-t = (-u)a + (-v)b$, které také náleží do množiny M , bude jistě kladné celé číslo.

Jistě existuje nějaké nejmenší kladné celé číslo $c = u_c a + v_c b$. Tvrdíme, že $c = D(a, b)$.

Protože $D(a, b)$ dělí a i b , musí dělit i $ua + vb$, a tedy i c . Protože $c > 0$, tak $D(a, b) \leq c$.

Nyní ukážeme, že c je společný dělitel a a b . Necht' $a = qc + r$, $0 \leq r < c$. Potom $r = a - qc = a - q(u_c a + v_c b) = (1 - qu_c)a - qv_c b$, číslo r je tedy také celočíselná kombinace čísel a a b . Nemůže to ale být kladné celé číslo, protože c je nejmenší kladné celé číslo ve tvaru $ua + vb$ a podle počáteční podmínky $r < c$. Proto $r = 0$ a tedy $c \mid a$. Obdobně bychom ukázali, že $c \mid b$. Protože c je společný dělitel čísel a, b , musí platit $c \leq D(a, b)$.

Protože $D(a, b) \leq c$ a zároveň $c \leq D(a, b)$, musí $c = D(a, b)$, tedy $D(a, b) = u_c a + v_c b$.

(Habala, 2019c, s. 19; Křížek, 2018, s. 38; Stanovský, 2022, s. 3)

Bézoutova rovnost je velice užitečné tvrzení, protože nám říká, že největší společný dělitel dvou čísel (a tedy i každý jeho násobek) můžeme vyjádřit lineární kombinací těchto čísel s celočíselnými koeficienty.

Konečně se dostáváme ke znění Čínské věty o zbytcích:

Věta 7 (Čínská věta o zbytcích)

Nechť $m_1, m_2, \dots, m_k$ jsou po dvojicích nesoudělná přirozená čísla. Pak pro soustavu kongruencí

$$\begin{aligned}x &\equiv r_1 \pmod{m_1}, \\x &\equiv r_2 \pmod{m_2}, \\&\vdots \\x &\equiv r_k \pmod{m_k},\end{aligned}$$

kde r_i jsou celá čísla, existuje právě jedno řešení x modulo m , kde $m = m_1 m_2 \dots m_k$.

Důkaz: Nejprve ukážeme existenci řešení x . Definujeme n_i pomocí rovnic

$$m = m_1 n_1 = m_2 n_2 = \dots = m_k n_k.$$

Protože m_i a n_i jsou nesoudělná, existují podle Bézoutovy věty (Věta 6) celá čísla y_i , $i = 1, 2, \dots, k$, taková, že $n_i y_i + k m_i = 1$, tedy $n_i y_i \equiv 1 \pmod{m_i}$.

Tvrdíme, že obecné řešení soustavy kongruencí má tvar

$$x \equiv r_1 n_1 y_1 + r_2 n_2 y_2 + \dots + r_k n_k y_k \pmod{m}.$$

Pro každé $i \in \{1, 2, \dots, k\}$ dostaneme

$$x \equiv r_1 n_1 y_1 + r_2 n_2 y_2 + \dots + r_k n_k y_k \pmod{m_i},$$

$$x \equiv r_i n_i y_i \pmod{m_i} \text{ (protože každý člen kromě tohoto je násobkem } m_i),$$

$$x \equiv r_i \pmod{m_i} \text{ (protože } n_i y_i \equiv 1).$$

Proto $x \equiv r_i \pmod{m_i}$ pro všechna $i \in \{1, 2, \dots, k\}$ a tedy existuje řešení $x \equiv r_1 n_1 y_1 + r_2 n_2 y_2 + \dots + r_k n_k y_k \pmod{m}$. (Křížek, 2018, s. 44-45; Radcliffe, 2019)

Zbývá nám ukázat jednoznačnost řešení. Předpokládejme, že soustava má dvě řešení $x, y \in \{0, 1, \dots, m-1\}$. Pak pro každé $i \in \{1, 2, \dots, k\}$ platí $x \equiv y \equiv r_i \pmod{m_i}$.

Z toho vyplývá, že $m_i \mid x - y$ pro všechna i . Protože jsou čísla m_i navzájem nesoudělná, dostáváme $m = m_1 m_2 \dots m_k \mid x - y$. Jelikož čísla x i y jsou menší než m , je určitě i jejich

rozdíl menší než m . Ale protože zároveň $m \mid x - y$, musí platit $x - y = 0$ a tedy $x = y$.
(Stanovský, 2022, s. 9)

Postup uvedený v tomto důkazu můžeme využít pro řešení soustav lineárních kongruencí, jak si ukážeme v následujícím příkladu.

Příklad 1.12 Najděte všechna x splňující následující kongruence:

$$x \equiv 4 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$x \equiv 10 \pmod{11}.$$

Řešení 1: Spočítáme $m = 5 \cdot 7 \cdot 11 = 385$ a $n_1 = 385 : 5 = 77$, $n_2 = 385 : 7 = 55$, $n_3 = 385 : 11 = 35$.

Nyní musíme najít y_i tak, aby $y_i n_i \equiv 1 \pmod{m_i}$.

$$77y_1 \equiv 1 \pmod{5}$$

$$55y_2 \equiv 1 \pmod{7}$$

$$35y_3 \equiv 1 \pmod{11}$$

$$2y_1 \equiv 1 \pmod{5}$$

$$-y_2 \equiv 1 \pmod{7}$$

$$2y_3 \equiv 1 \pmod{11}$$

$$y_1 \equiv 3 \pmod{5}$$

$$y_2 \equiv -1 \equiv 6 \pmod{7}$$

$$2y_3 \equiv 12 \pmod{11}$$

$$y_3 \equiv 6 \pmod{11}$$

Důkaz nám říká, že řešení bude tvaru $x = r_1 n_1 y_1 + r_2 n_2 y_2 + r_3 n_3 y_3 = 4 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 10 \cdot 35 \cdot 6 = 3684$. Tento výsledek zmenšíme pomocí modulu 385 na $x = 219$, což je podle Čínské zbytkové věty jediné řešení modulo 385. Všechna řešení budou ve tvaru $219 + 385k$, $k \in \mathbb{Z}$. (Radcliffe, 2019; Habala, 2019b)

Zkouška:

$$219 - 4 = 215, 5 \mid 215,$$

$$219 - 2 = 217, 7 \mid 217,$$

$$219 - 10 = 209, 11 \mid 209.$$

Řešení 2: Druhou metodou je řešení jednotlivých kongruencí a dosazování výsledků.

$$x \equiv 4 \pmod{5}$$

$$x = 4 + 5k, k \in \mathbb{Z}$$

Dosadíme do druhé kongruence, tu vyřešíme a řešení dosadíme zpět. Tím získáme řešení prvních dvou kongruencí.

$$\begin{aligned}x &\equiv 2 \pmod{7} \\4 + 5k &\equiv 2 \pmod{7} \\5k &\equiv -2 \equiv 5 \pmod{7} \\k &\equiv 1 \pmod{7} \\k &= 1 + 7l, l \in \mathbb{Z} \\x = 4 + 5k &= 4 + 5(1 + 7l) = 9 + 35l\end{aligned}$$

Dosadíme do třetí kongruence, tu vyřešíme a opět dosadíme zpět.

$$\begin{aligned}x &\equiv 10 \pmod{11} \\9 + 35l &\equiv 10 \pmod{11} \\2l &\equiv 1 \pmod{11} \\2l &\equiv 12 \pmod{11} \\l &\equiv 6 \pmod{11} \\l &= 6 + 11m, m \in \mathbb{Z} \\x = 9 + 35l &= 9 + 35(6 + 11m) = 219 + 385m\end{aligned}$$

Všechna x , která splňují kongruence, jsou tedy ve tvaru $219 + 385m$, $m \in \mathbb{Z}$, což je ekvivalentní s řešením získaným druhou metodou.

Zatím jsme řešili soustavy kongruencí, kde moduly byly po dvou nesoudělné (což je podmínka pro platnost Čínské věty o zbytcích). Na následujícím příkladu si ukážeme, že se díky této větě můžeme popasovat i se soustavami, kde jsou moduly navzájem soudělná čísla.

Příklad 1.13 (Habala, 2019b, s. 21) Řešte soustavu kongruencí

$$\begin{aligned}x &\equiv 2 \pmod{24} \\x &\equiv 6 \pmod{20} \\x &\equiv 8 \pmod{30}.\end{aligned}$$

Řešení: Protože $24 = 3 \cdot 2^3$, první kongruenci můžeme rozdělit na kongruence $x \equiv 2 \pmod{3}$ a $x \equiv 2 \pmod{2^3}$. Podobně $20 = 5 \cdot 2^2$, druhou kongruenci můžeme rozdělit na $x \equiv 6 \pmod{5}$ a $x \equiv 6 \pmod{2^2}$. A protože $30 = 2 \cdot 3 \cdot 5$, třetí kongruenci rozdělíme na tři

kongruence: $x \equiv 8 \pmod{2}$, $x \equiv 8 \pmod{3}$ a $x \equiv 8 \pmod{5}$. Dostali jsme tedy soustavu sedmi kongruencí:

$$x \equiv 2 \pmod{2^3}$$

$$x \equiv 6 \pmod{2^2}$$

$$x \equiv 8 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 8 \pmod{3}$$

$$x \equiv 6 \pmod{5}$$

$$x \equiv 8 \pmod{5}$$

První tři kongruence mají modul nějakou mocninu čísla 2. Úpravou druhé rovnice dostaneme $x \equiv 2 \pmod{4}$. Protože $4 \mid 8$, druhá rovnice nám oproti první nepřidává žádnou novou podmínku pro x . Podobně úpravou třetí rovnice dostaneme $x \equiv 0 \pmod{2}$, tedy x bude sudé číslo, to je ale opět obsaženo v první rovnici. Druhou a třetí rovnici tedy nemusíme brát v potaz.

Úpravou páté rovnice dostaneme čtvrtou rovnici, pátou proto také můžeme přeskočit.

U posledních dvou rovnic ale nastává problém, protože jsme zjistili, že po dělení pěti má číslo x dávat dva různé zbytky. To nemůže nastat, proto tato soustava kongruencí nemá řešení.

Příklad 1.14 Tento příklad je stejný jako předchozí, jen změníme zbytek v poslední kongruenci na 26. Máme tedy soustavu kongruencí

$$x \equiv 2 \pmod{24}$$

$$x \equiv 6 \pmod{20}$$

$$x \equiv 26 \pmod{30}.$$

Řešení: U prvních dvou rovnic se nic nezmění, proto můžeme místo nich pracovat pouze s rovnicemi $x \equiv 2 \pmod{8}$, $x \equiv 2 \pmod{3}$ a $x \equiv 6 \equiv 1 \pmod{5}$.

Ze třetí rovnice dostaneme kongruence

$x \equiv 26 \pmod{2}$, tj. sudá čísla, což už je obsaženo v první kongruenci,

$x \equiv 26 \pmod{3}$, tj. kongruence ekvivalentní s kongruencí $x \equiv 2 \pmod{3}$,

$x \equiv 26 \pmod{5}$, tj. kongruence ekvivalentní s kongruencí $x \equiv 1 \pmod{5}$.

Dostali jsme tedy soustavu tří kongruencí, kterou vyřešíme jedním ze způsobů uvedených výše.

$$x \equiv 2 \pmod{8}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 1 \pmod{5}$$

Z první rovnice máme $x = 2 + 8k$, $k \in \mathbb{Z}$. Dosazením do druhé rovnice získáme

$$2 + 8k \equiv 2 \pmod{3}$$

$$8k \equiv 0 \pmod{3}$$

$$k = 3l, l \in \mathbb{Z}$$

$$x = 2 + 8k = 2 + 24l$$

$$2 + 24l \equiv 1 \pmod{5}$$

$$-l \equiv -1 \pmod{5}$$

$$l \equiv 1 \pmod{5}$$

$$l = 1 + 5m, m \in \mathbb{Z}$$

$$x = 2 + 24l = 2 + 24(1 + 5m) = 26 + 120m$$

Řešením je tedy číslo 26 a všechna čísla vzniklá přičtením nějakého násobku 120. Všimněme si, že 120 je nejmenší společný násobek původních modulů, tedy čísel 24, 20 a 30.

Předchozí dva příklady zobecníme do následující věty:

Věta 8 (Čínská věta o zbytcích pro soudělná čísla)

Nechť $m_1, m_2, \dots, m_k \in \mathbb{Z}$. Soustava rovnic

$$x \equiv r_1 \pmod{m_1},$$

$$x \equiv r_2 \pmod{m_2},$$

$$\vdots$$

$$x \equiv r_k \pmod{m_k},$$

má řešení právě tehdy, když $r_i \equiv r_j \pmod{D(m_i, m_j)}$ pro všechna $i, j; i \neq j$. Řešení soustavy je jednoznačné modulo $n(m_1, m_2, \dots, m_k)$. (Habala, 2019b)

Tato formulace není příliš častá, důkaz lze najít v (Bogomolny, c1996-2018).

Kde byl v Příkladu 1.13 problém? Měli jsme kongruence $x \equiv 6 \pmod{20}$ a $x \equiv 8 \pmod{30}$. Protože $D(20, 30) = 10$, soustava nemá řešení, protože $6 \not\equiv 8 \pmod{10}$. Oproti tomu v Příkladu 1.14 jsme měli poslední rovnici $x \equiv 26 \pmod{30}$ a protože $6 \equiv 26 \pmod{10}$, soustava měla řešení.

Úlohy

1.9 Najděte všechna řešení soustav rovnic

a) $x \equiv 2 \pmod{3}$

$$x \equiv 1 \pmod{7}$$

$$x \equiv 5 \pmod{8}$$

b) $3x \equiv 1 \pmod{5}$

$$7x \equiv 5 \pmod{6}$$

$$8x \equiv 2 \pmod{11}$$

c) $x \equiv 3 \pmod{20}$

$$x \equiv 19 \pmod{28}$$

$$x \equiv 33 \pmod{35}.$$

V následujících podkapitolách si ukážeme využití Čínské věty o zbytcích v různých typech úloh.

1.3.1 Rozdělení velké kongruence na několik malých

Podívejme se ještě jednou na poslední Příklad 1.10e) z minulé kapitoly: $5x \equiv 3 \pmod{14}$. Pokud je číslo dělitelné 14, musí být určité dělitelné zároveň 2 a 7. Což platí také naopak: pokud je číslo dělitelné zároveň 2 a 7, musí být určité dělitelné 14. Zkusme toho využít u výše uvedené kongruence.

Zadanou kongruenci „rozbijeme“ na dvě kongruence: $5x \equiv 3 \pmod{2}$ a $5x \equiv 3 \pmod{7}$, které musí platit zároveň.

Nejdříve vyřešíme první kongruenci.

$$5x \equiv 3 \pmod{2}$$

$$x \equiv 1 \pmod{2}$$

$$x = 1 + 2k, k \in \mathbb{Z}.$$

Toto řešení dosadíme do druhé kongruence a vyřešíme.

$$5 \cdot (1 + 2k) \equiv 3 \pmod{7}$$

$$5 + 10k \equiv 3 \pmod{7}$$

$$5 + 3k \equiv 3 \pmod{7}$$

$$3k \equiv -2 \pmod{7}$$

$$3k \equiv -9 \pmod{7}$$

$$k \equiv -3 \equiv 4 \pmod{7}$$

$$k = 4 + 7l, l \in \mathbb{Z}$$

Dosadíme zpět do vyjádření x z první kongruence.

$$x = 1 + 2k = 1 + 2 \cdot (4 + 7l) = 1 + 8 + 14l = 9 + 14l$$

Dostali jsme tedy řešení $x = 9 + 14l, l \in \mathbb{Z}$, které je shodné s řešením v předchozí kapitole.

Ukážeme si i opačný postup, kdy nejdříve budeme počítat kongruenci $5x \equiv 3 \pmod{7}$.

$$5x \equiv 3 \pmod{7}$$

$$5x \equiv 10 \pmod{7}$$

$$x \equiv 2 \pmod{7}$$

$$x = 2 + 7k, k \in \mathbb{Z}$$

Dosadíme do druhé kongruence, kterou si ale nejdříve upravíme.

$$5x \equiv 3 \pmod{2}$$

$$x \equiv 1 \pmod{2}$$

$$2 + 7k \equiv 1 \pmod{2}$$

$$k \equiv 1 \pmod{2}$$

$$k = 1 + 2l, l \in \mathbb{Z}$$

Dosadíme zpět a dostaneme řešení $x = 2 + 7k = 2 + 7 \cdot (1 + 2l) = 9 + 14l, l \in \mathbb{Z}$, které je shodné s řešením získaným předchozími způsoby.

Často je výhodnější začít nejdříve počítat kongruenci s menším modulem, ale není to pravidlem.

V tomto případě bylo řešení pomocí rozbití na menší moduly poměrně zdlouhavé a neefektivní, protože původní kongruence se dala poměrně jednoduše vyřešit i bez rozbití na menší moduly. Ukážeme si ale kongruenční rovnice, u nichž nám rozbití na menší moduly velice pomůže.

Příklad 1.15 Najděte všechna řešení kongruence $7x \equiv 11 \pmod{12}$.

Špatné řešení: Číslo 12 můžeme rozložit na $3 \cdot 4 = 3 \cdot 2 \cdot 2$. Vypadá to tedy, že původní kongruenci můžeme rozložit na $7x \equiv 11 \pmod{3}$, $7x \equiv 11 \pmod{2}$ a ještě jednou $7x \equiv 11 \pmod{2}$.

Z první kongruence dostaneme $x \equiv 2 \pmod{3}$, tedy $x = 2 + 3k, k \in \mathbb{Z}$.

Dosazením do druhé kongruence dostaneme

$$7 \cdot (2 + 3k) \equiv 11 \pmod{2}$$

$$14 + 21k \equiv 11 \pmod{2}$$

$$k \equiv 1 \pmod{2}$$

$$k = 1 + 2l, l \in \mathbb{Z}.$$

Dosazením do řešení první kongruence získáme $x = 2 + 3k = 2 + 3 \cdot (1 + 2l) = 5 + 6l$, $l \in \mathbb{Z}$.

Zkouška: Pro $x = 5$ máme $35 \equiv 11 \pmod{12}$, což platí. Dalším řešením by mělo být $x = 11$. Zde ale narazíme, protože $77 \not\equiv 11 \pmod{12}$.

Kde je problém? Číslo 12 jsme rozdělili na příliš malá čísla, dostali jsme tak dvakrát stejnou kongruenci. To se nám stát nesmí, protože získáme navíc neplatná řešení. Proto abychom dostali pouze správné řešení, čísla, na které původní číslo rozkládáme, musí být po dvou nesoudělná.

Správné řešení: Kongruenci rozložíme na kongruence $7x \equiv 11 \pmod{3}$ a $7x \equiv 11 \pmod{4}$. Vyřešíme první kongruenci:

$$7x \equiv 11 \pmod{3}$$

$$x \equiv 2 \pmod{3}$$

$$x = 2 + 3k, k \in \mathbb{Z}$$

Upravíme druhou kongruenci a dosadíme.

$$7x \equiv 11 \pmod{4}$$

$$-x \equiv 3 \pmod{4}$$

$$x \equiv -3 \equiv 1 \pmod{4}$$

$$2 + 3k \equiv 1 \pmod{4}$$

$$3k \equiv -1 \pmod{4}$$

$$3k \equiv 3 \pmod{4}$$

$$k \equiv 1 \pmod{4}$$

$$k = 1 + 4l, l \in \mathbb{Z}$$

Dosadíme zpět do řešení první kongruence $x = 2 + 3k = 2 + 3 \cdot (1 + 4l) = 5 + 12l$, $l \in \mathbb{Z}$.

Už víme, že pro $x = 5$ kongruence platí. Další čísla ve tvaru $5 + 12l$ budou také zjevně kongruenci vyhovovat, protože k číslu 5 přičítáme pouze násobky modulu.

Příklad 1.16 Najděte všechna řešení kongruence $31x \equiv 53 \pmod{60}$.

Řešení: Vzhledem k tomu, že koeficienty jsou poměrně velká prvočísla a na první pohled žádné řešení není vidět, použijeme rozklad na menší moduly. Číslo 60 můžeme rozložit na $3 \cdot 4 \cdot 5$. Nemůžeme použít rozklad $3 \cdot 2 \cdot 2 \cdot 5$, neboť čísla musí být po dvou nesoudělná, jak jsme si ukázali v předchozím příkladu.

Budeme tedy řešit soustavu kongruencí

$$31x \equiv 53 \pmod{3},$$

$$31x \equiv 53 \pmod{4},$$

$$31x \equiv 53 \pmod{5}.$$

Nejdříve najdeme řešení první kongruence:

$$31x \equiv 53 \pmod{3}$$

$$x \equiv 2 \pmod{3}$$

$$x = 2 + 3k, k \in \mathbb{Z}.$$

Upravíme druhou kongruenci a dosadíme za x řešení první kongruence:

$$31x \equiv 53 \pmod{4}$$

$$-x \equiv 1 \pmod{4}$$

$$x \equiv -1 \equiv 3 \pmod{4}$$

$$2 + 3k \equiv 3 \pmod{4}$$

$$3k \equiv 1 \pmod{4}$$

$$-k \equiv 1 \pmod{4}$$

$$k \equiv -1 \equiv 3 \pmod{4}$$

$$k = 3 + 4l, l \in \mathbb{Z}.$$

Řešením prvních dvou kongruencí je $x = 2 + 3k = 2 + 3 \cdot (3 + 4l) = 11 + 12l$.

Dosadíme do třetí kongruence.

$$31x \equiv 53 \pmod{5}$$

$$x \equiv 3 \pmod{5}$$

$$11 + 12l \equiv 3 \pmod{5}$$

$$2l \equiv -8 \pmod{5}$$

$$2l \equiv 2 \pmod{5}$$

$$l \equiv 1 \pmod{5}$$

$$l = 1 + 5m, m \in \mathbb{Z}$$

Opět dosadíme a získáme řešení:

$$x = 11 + 12l = 11 + 12 \cdot (1 + 5m) = 23 + 60m; m \in \mathbb{Z}.$$

$$\text{Zkouška: } 31 \cdot (23 + 60m) \equiv 31 \cdot 23 = 713 \equiv 53 \pmod{60}$$

Zde jsme řešili kongruence v pořadí podle nejmenšího modulu. Můžeme je ale řešit v libovolném pořadí. Pro 3 rovnice máme $3! = 6$ možností pořadí, všechny ale pochopitelně vedou ke stejnému výsledku.

Příklad 1.17 Najděte všechna řešení kongruenční rovnice $19x \equiv 23 \pmod{32}$.

Řešení: Protože $32 = 2^5$, jakýmkoli rozkladem bychom získali soudělná čísla, proto zde rozklad na menší kongruence nemůžeme použít. Musíme tedy řešit rovnici v zadaném tvaru.

Ani zkoušením úprav uvedených v Příkladu 1.10 zde bohužel nenajdeme řešení přímočaře.

Zbývají nám tedy 2 způsoby řešení – buď kongruenci převedeme na diofantickou rovnici tvaru $19x + 32y = 23$, kterou vyřešíme některou z metod z další kapitoly, nebo najdeme inverzní číslo k číslu 19 (počítáno modulo 32). Tento postup je naznačen na konci Příkladu 1.10 a vede také na diofantickou rovnici. Proto na tomto místě postup řešení uvádět nebudeme a uvedeme pouze výsledek $x = 13 + 32k, k \in \mathbb{Z}$.

Příklad 1.18 Zjistěte poslední dvojčíslí čísla 49^{35} .

Řešení: Abychom zjistili poslední dvojčíslí, potřebujeme zjistit zbytek po dělení tohoto čísla stem, tedy hledáme řešení kongruence $x \equiv 49^{35} \pmod{100}$. Díky Čínské větě o zbytecích můžeme tuto kongruenci rozdělit na $x \equiv 49^{35} \pmod{4}$ a $x \equiv 49^{35} \pmod{25}$.

Protože $49 \equiv 1 \pmod{4}$ a $49 \equiv -1 \pmod{25}$, dostaneme

$$x \equiv 1^{35} \equiv 1 \pmod{4}$$

$$x \equiv (-1)^{35} \equiv -1 \pmod{25}$$

Z první kongruence máme řešení $x = 1 + 4k, k \in \mathbb{Z}$. Dosadíme jej do druhé kongruence a vypočítáme k , které dosadíme do řešení první kongruence.

$$x \equiv -1 \pmod{25}$$

$$1 + 4k \equiv -1 \pmod{25}$$

$$4k \equiv -2 \pmod{25}$$

$$2k \equiv -1 \equiv 24 \pmod{25}$$

$$k \equiv 12 \pmod{25}$$

$$k = 12 + 25l, l \in \mathbb{Z}$$

$$x = 1 + 4k = 1 + 4 \cdot (12 + 25l) = 49 + 100l$$

Zjistili jsme, že poslední dvojčíslí čísla 49^{35} je 49.

Úlohy

1.10 Najděte všechna řešení kongruenčních rovnic

a) $24x \equiv 7322 \pmod{38}$

b) $61x \equiv 6213 \pmod{77}$

c) $59x \equiv 157 \pmod{140}$.

1.11 Zjistěte poslední dvojčíslí čísla 76^{24} .

1.3.2 Sloučení malých kongruencí do velké

Čínská věta o zbytcích může být užitečná také pro opačný proces, než jaký jsme viděli v minulé podkapitole. Tuto podkapitolu začneme úlohou ze základní školy:

Příklad 1.19 Taneční kroužek měl tolik členů, že mohli nastupovat po třech nebo po čtyřech nebo po osmi. Kolik členů měl kroužek, víte-li, že to byl nejnižší možný počet? (Běloun, 2010, s. 23)

Řešení: Úloha se typicky řeší nalezením nejmenšího společného násobku čísel 3, 4 a 8. Protože $n(3, 4, 8) = 24$, kroužek měl 24 členů. V případě, že bychom neměli zadanou podmínku na nejnižší možný počet, mohl by mi kroužek také například 48, 72, 96, obecně $24n$ členů.

Pomocí kongruencí bychom úlohu mohli zapsat takto:

$$x \equiv 0 \pmod{3},$$

$$x \equiv 0 \pmod{4},$$

$$x \equiv 0 \pmod{8},$$

přičemž všechny kongruence musí platit zároveň. Řešením soustavy kongruencí jsou zřejmě čísla, která jsou společnými násobky čísel 3, 4 a 8; řešením úlohy bude nejmenší takové číslo.

Následující úloha je také řešitelná žáky základní školy:

Příklad 1.20 Pokaždé, když se na táboře děti rozdělily do trojic, čtveřic nebo petic, vždy jedno dítě zůstalo navíc. Kolik nejméně dětí mohlo být na táboře?

Řešení lze opět najít pomocí nalezení nejmenšího společného násobku s tím rozdílem, že nakonec musíme přičíst 1, protože jedno dítě vždy přebývalo.

Pomocí kongruencí bychom úlohu zapsali takto:

$$x \equiv 1 \pmod{3},$$

$$x \equiv 1 \pmod{4},$$

$$x \equiv 1 \pmod{5},$$

přičemž všechny kongruence musí platit zároveň.

Řešení: Nejmenší společný násobek čísel 3, 4 a 5 je 60, protože ale vždy jedno dítě přebývalo, dětí bylo na táboře 61.

Následující úloha je o něco složitější:

Příklad 1.21 Všichni žáci školy se během představení na konci školního roku několikrát rozdělovali do skupin. Když vytvořili skupiny po třech, zbyl jeden žák, to stejné se stalo, když byli ve skupinách po čtyřech. Když se ale rozdělili do skupin po jedenácti, nikdo nezůstal navíc. Kolik žáků mohla mít škola, jestliže víme, že to bylo méně než 500?

Řešení: Pomocí kongruencí bychom úlohu zapsali takto:

$$x \equiv 1 \pmod{3},$$

$$x \equiv 1 \pmod{4},$$

$$x \equiv 0 \pmod{11},$$

$$\text{a zároveň } x < 500.$$

Úloha se dá ale vyřešit i bez použití kongruencí.

Zkusíme nejdříve najít alespoň jedno řešení. Protože číslo má dát po dělení čtyřmi zbytek 1, poslední dvojčíslí by mohlo být 13. První číslo musíme doplnit tak, abychom po dělení třemi dostali zbytek jedna, tj. ciferný součet musí být o jedna větší než nějaký násobek tří. V úvahu tedy připadají čísla 3, 6 a 9. Podmínku dělitelnosti jedenácti splňuje číslo pouze po doplnění devítky, takže jsme dostali číslo 913. Z tohoto řešení můžeme získat další řešení tak, že budeme přičítat k -násobek nějakého vhodného čísla. Tím bude nejmenší společný násobek čísel 3, 4 a 11, tedy 132, protože po přičtení násobku tohoto čísla budou pořád splněny všechny tři kongruence. Protože žáků bylo určitě méně než 500, budeme násobky pouze odčítat. Dostaneme tak dostaneme čísla 781, 649, 517, 385, 253, 121, z nichž poslední podmínku splňující poslední tři čísla. Škola měla tedy buď 121, 253 nebo 385 žáků.

Na začátku jsme mohli zvolit poslední dvojčíslí také například 17, 21 nebo jiné a obdobnými úvahami dojít ke stejnému výsledku.

Úlohy

- 1.12 Pořadatelé průvodu, kterého se zúčastnilo méně než 1000 lidí, chtěli mít všechny řady plné. Ať seřadili účastníky do dvojstupů, trojstupů, čtyřstupů, pětistupů, šestistupů, sedmistupů, či osmistupů, nikdy nebyla poslední řada plná. Přihlízející matematik navrhl jednomu z pořadatelů, aby se postavil i on do průvodu. Potom byly všechny řady plné, ať se vytvořily dvojstupy, trojstupy, čtyřstupy, pětistupy, šestistupy, sedmistupy, či osmistupy. Kolik lidí bylo původně v průvodu? (Česenek, 1994, s. 36)
- 1.13 Pastýř pásł ovce. Kolemjdoucí pocestný se ho zeptal, kolik jich má. Pastýř odpověděl: „Je jich méně než 500. Kdybych je postavil do dvojřadu, trojřadu, čtyřřadu, pětiřadu nebo šestiřadu, pokaždé by zůstala jedna ovce. Mohu je však seřadit přesně do sedmiřadu. Kolik měl pastýř ovcí? (Česenek, 1994, s. 36)
- 1.14 Myslím si trojčíferné číslo. Když od něho odečtu 7, bude výsledek dělitelný sedmi. Když od něho odečtu 8, bude výsledek dělitelný osmi. A když od něho odečtu 9, bude výsledek dělitelný devíti. Jaké číslo jsem si myslel? (Česenek, 1994, s. 36)
- 1.15 Na hřišti cvičili žáci ze dvou tříd. Když se seřadili do trojstupů, zbyl jeden žák, když vytvořili čtyřstupy, zbyli dva, při pětistupech zbyli tři a šestistupech čtyři žáci. Kolik žáků bylo na hřišti? (Trejbal, 1995, s. 11)
- 1.16 Generál zjišťuje po bitvě počet přeživších vojáků tím, že je nechává srovnat se do řad o určitých délkách a počítá, kolik vojáků přebývá. Do bitvy šlo 1200 vojáků, když je po bitvě seřadil, tak při řazení po pětících i po šestících zbyli vždy 3 vojáci, po sedmicích přebýval 1 voják a při seřazení do řad po jedenácti nezůstal nikdo. Kolik vojáků bitvu přežilo? (Chinese Remainder Theorem, 2022)

1.3.3 Reprezentace čísel pomocí zbytků a algebraická verze

Pro zajímavost se podíváme ještě na dvě využití Čínské věty o zbytcích – reprezentaci čísla pomocí zbytků a zobecnění Čínské věty o zbytcích pro okruhy.

Díky Čínské větě o zbytcích můžeme každé nezáporné celé číslo x menší než $m = m_1 m_2 \dots m_k$ jednoznačně reprezentovat uspořádanou k -ticí čísel $(r_1, r_2, \dots, r_k)$, což jsou zbytky po dělení čísla x čísly $m_1, m_2, \dots, m_k$, kde $0 \leq r_i < m_i, i = 1, 2, \dots, k$.

Například pro $m_1 = 3$ a $m_2 = 5$ můžeme vytvořit tuto tabulku:

r_2	0	1	2	3	4
$r_1 = 0$	0	6	12	3	9
$r_2 = 1$	10	1	7	13	4
$r_3 = 2$	5	11	2	8	14

Obr. 3: Tabulka pro $k = 2, m_1 = 3$ a $m_2 = 5$. (Křížek, 2018, s. 46)

Podíváme-li se na číslo 7, po dělení třemi dává zbytek 1, proto leží ve druhém řádku, a po dělení pěti zbytek 2, proto je ve třetím sloupci. Všimněme si, že se čísla zvětšují o jedno vždy diagonálně.

Reprezentaci čísel pomocí zbytků se říká také *sinoreprezentace*.

Proč jsou čísla jednoznačně určena pomocí zbytků? Po dělení třemi dostáváme zbytky 0, 1 a 2, které se periodicky opakují, podobně se opakují zbytky 0, 1, 2, 3 a 4 po dělení pěti. Protože zbytky se opakují s periodami 3 a 5, stejné zbytky dostaneme poprvé po $3 \cdot 5 = 15$ krocích. Každé číslo menší než 15 je tak určeno jednoznačně uspořádanou dvojicí zbytků.

Číslo 7 je pro $m_1 = 3$ a $m_2 = 5$ reprezentováno dvojicí $(1, 2)$.

Čísla reprezentována k -ticemi můžeme sčítat, odčítat nebo násobit. Operace si ukážeme na číslech $7 = (1, 2)$ a $14 = (2, 4)$.

Sčítat budeme po složkách, tedy $(1, 2) + (2, 4) = (3, 6)$. Protože ale zbytky v první složce musí být menší než 3 a ve druhé složce menší než 5, musíme výsledná čísla počítat modulo příslušné číslo. Protože $3 \equiv 0 \pmod{3}$ a $5 \equiv 1 \pmod{6}$, dostaneme výslednou dvojici $(0, 1)$. Mělo nám vyjít $7 + 14 = 21 \equiv 6 \pmod{15}$. Číslo 6 opravdu dává zbytek 0 po dělení třemi a zbytek 1 po dělení pěti.

Zjevně funguje odčítání po složkách: $14 - 7 = (2, 4) - (1, 2) = (1, 2) = 7$. V případě $7 - 14 = (1, 2) - (2, 4) = (-1, -2)$ dostaneme záporná čísla. Opět musíme najít nejmenší nezáporná čísla s nimi kongruentní. Protože $-1 \equiv 2 \pmod{3}$ a $-2 \equiv 3 \pmod{5}$, rozdíl $7 - 14$ je reprezentován dvojicí $(2, 3)$. Z tabulky vidíme, že tato dvojice zjevně odpovídá číslu 8, které jsme očekávali.

Násobit budeme také po složkách, tedy $7 \cdot 14 = (1, 2) \cdot (2, 4) = (2, 8)$. Opět musíme najít číslo kongruentní ve druhé složce, to bude $8 \equiv 3 \pmod{5}$. Dostali jsme tedy $7 \cdot 14 = (2, 3)$. Dvojice $(2, 3)$ odpovídá číslu 8, což je v pořádku, protože $7 \cdot 14 = 98 \equiv 8 \pmod{15}$. (Stillwell, 2003, s. 171-175)

Na sinoreprezentaci je založen také tradiční čínský kalendář (Křížek, 2018, s. 46-47).

Věta 9 (Algebraická verze Čínské věty o zbytcích)

Nechť $m_1, \dots, m_n$ jsou po dvou nesoudělná přirozená čísla a označme $m = m_1 \cdot \dots \cdot m_n$. Zobrazení $\varphi: \mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$, $a \mapsto (a \bmod m_1, \dots, a \bmod m_n)$ je izomorfismem těchto okruhů. Restrikce $\varphi|_{\mathbb{Z}_m^*}$ je grupovým izomorfismem $\mathbb{Z}_m^* \simeq \mathbb{Z}_{m_1}^* \times \dots \times \mathbb{Z}_{m_n}^*$.

Důkaz je uveden v textu (Stanovský, 2022, s. 72)

Věta nám říká, že například $\mathbb{Z}_{105} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$. Znamená to, že například číslo 23 by bylo v okruhu $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ reprezentováno trojicí $(2, 3, 2)$, protože tato čísla odpovídají číslu 23 v jednotlivých okruzích, neboli zbytek po dělení třemi je 2, zbytek po dělení pěti je 3 a zbytek po dělení sedmi je 2.

Okruh $\mathbb{Z}_{105}$ je izomorfní nejen okruhu $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$, ale také například okruhu $\mathbb{Z}_{15} \times \mathbb{Z}_7$. Další izomorfní okruhy jsou například $\mathbb{Z}_6 \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$ nebo $\mathbb{Z}_{63} \simeq \mathbb{Z}_9 \times \mathbb{Z}_7$.

Okruhy $\mathbb{Z}_8$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ale izomorfní nejsou, protože číslo 2 je samo se sebou soudělné. (Stanovský, 2022, s. 72-75)

Úlohy

1.17 Pro $m_1 = 7, m_2 = 9$ a $m_3 = 13$

- najděte sinoreprezentaci čísla 80,
- určete číslo, které odpovídá trojici $(1, 6, 2)$,
- pomocí sinoreprezentace těchto čísel najděte jejich součet, rozdíl a součin.

2 Lineární diofantické rovnice

Diofantické (též *diofantské*, *diofantovské* nebo *neurčité*) rovnice získaly své jméno podle řeckého matematika Diofanta, který působil ve 3. století v Alexandrii. Zabýval se především problémy z oblasti teorie čísel a algebry, někdy je také nazýván „otcem algebry“. Jeho nejvýznamnější dílo *Aritmetika* obsahuje mnoho problémů, které většinou vedou na rovnice a soustavy rovnic s větším počtem neznámých než rovnic. Diofantos ale hledal řešení pouze v kladných racionálních číslech, protože záporná řešení při řešení jeho problémů nedávala smysl.

Dnes jako diofantické rovnice označujeme rovnice, jejichž řešení hledáme v oboru celých čísel. S diofantickou rovnicí jsme se setkali již na základní škole při hledání „hezkých“ (neboli celočíselných) čísel vyhovujících rovnici $a^2 + b^2 = c^2$, tedy Pythagorově větě. Takovým řešením se říká *pythagorejské trojice*; nejmenší a nejznámější z nich je trojice čísel 3, 4, 5.

Diofantova *Aritmetika* měla velký vliv na práci matematiků v 17. až 19. století, kdy se jí podrobněji věnovali Euler, Gauss nebo Fermat. Právě poslední zmiňovaný dokonce na okraj svého vydání *Aritmetiky* napsal tvrzení dnes známé jako Velká Fermatova věta. (Křížek, 2018, s. 37; Habala, 2019b, s. 1; Dlab, 2016, s. 108)

Existuje velké množství typů diofantických rovnic. Otázka jejich řešitelnosti byla dokonce jedním ze slavných *Hilbertových problémů*, publikovaných v roce 1900. Hilbert požadoval udání metody, pomocí které bychom mohli po konečném počtu kroků rozhodnout, zdali daná diofantická rovnice má řešení, nebo ne. Až v roce 1970 Jurij Matijasevič dokázal, že taková metoda neexistuje. (Havel, 1973)

V této práci se ovšem budu zabývat pouze nejjednoduššími diofantickými rovnicemi, což jsou rovnice lineární, a jejich soustavami.

2.1 Lineární diofantické rovnice o dvou neznámých

Definice 6 (Lineární diofantické rovnice o dvou neznámých)

Lineární diofantické rovnice o dvou neznámých je libovolná rovnice ve tvaru $ax + by = c$, s neznámými x, y , kde $a, b, c \in \mathbb{Z}$ a vyžadujeme řešení $x, y \in \mathbb{Z}$.

Věta 10 (Řešitelnost lineární diofantické rovnice)

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

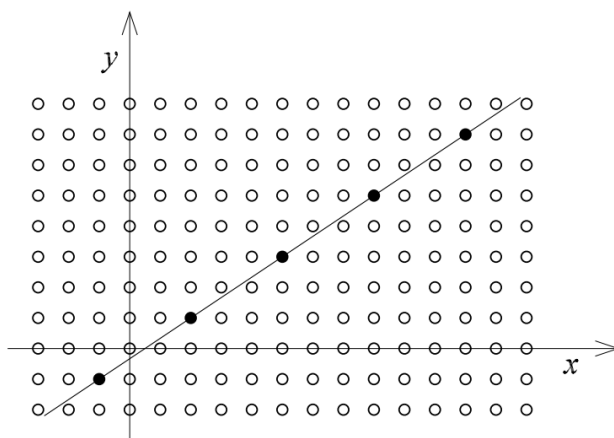
Důkaz: ($\Rightarrow$) Předpokládejme řešení $x_0, y_0 \in \mathbb{Z}$ takové, že $ax_0 + by_0 = c$. Protože $D(a, b)$ dělí a i b , dělí i jejich součet, tedy číslo c .

($\Leftarrow$) Předpokládejme $c = k \cdot D(a, b)$ pro nějaké $k \in \mathbb{Z}$. Podle Bézoutovy věty (Věta 6) existují $u, v \in \mathbb{Z}$ takové, že $au + bv = D(a, b)$. Potom $k \cdot (au) + k \cdot (bv) = k \cdot D(a, b)$, tedy $a \cdot (ku) + b \cdot (kv) = c$. Našli jsme celočíselná řešení $x_0 = ku$ a $y_0 = kv$ rovnice $ax + by = c$, což bylo naším cílem. (Habala, 2019b, s. 1)

Například rovnice $2x + 4y = 5$ zjevně řešení mít nebude, protože nalevo budeme mít vždy součet dvou sudých čísel, zatímco napravo je liché číslo.

Grafické znázornění

Přímku odpovídající diofantické rovnici můžeme zakreslit do soustavy souřadnic. Pokud má rovnice řešení, přímka prochází body s celočíselnými souřadnicemi. Pokud řešení nemá, žádnými takovými body neprochází.



Obr. 4: Přímka odpovídající diofantické rovnici $2x - 3y = 1$ (Křížek, 2018, s. 39)

Definice 7 (Homogenní rovnice)

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

Věta 11 (Tvar řešení lineární diofantické rovnice)

Nechť $a, b, c \in \mathbb{Z}$. Uvažujeme lineární diofantickou rovnici $ax + by = c$. Necht' $(x_p, y_p) \in \mathbb{Z}^2$ je nějaké její řešení (*partikulární řešení*). Potom $(x_0, y_0) \in \mathbb{Z}^2$ 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.

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

($\Leftarrow$) Předpokládejme, že (x_h, y_h) řeší přidruženou homogenní rovnici. Můžeme dosadit $x_0 = x_p + x_h$ a $y_0 = y_p + y_h$ do rovnice $ax + by = c$. Dostaneme $a(x_p + x_h) + b(y_p + y_h) = (ax_p + by_p) + (ax_h + by_h) = c + 0 = c$. Dvojice (x_0, y_0) je tedy opravdu řešením rovnice $ax + by = c$.

($\Rightarrow$) Předpokládejme, že (x_0, y_0) řeší rovnici $ax + by = c$. Potřebujeme najít dvojici (x_h, y_h) , pro kterou bude platit $(x_0, y_0) = (x_p, y_p) + (x_h, y_h)$, proto $x_h = x_0 - x_p$ a $y_h = y_0 - y_p$. Musíme ověřit, že (x_h, y_h) řeší přidruženou homogenní rovnici, tedy $ax_h + by_h = 0$. To uděláme dosazením: $a(x_0 - x_p) + b(y_0 - y_p) = (ax_0 + by_0) - (ax_p + by_p)$. Protože (x_0, y_0) i (x_p, y_p) jsou řešení původní rovnice, dostaneme $c - c = 0$. Dvojice (x_h, y_h) je tedy opravdu řešením rovnice $ax + by = 0$.

Ukažme si to na konkrétním příkladu. Budeme hledat řešení rovnice $4x + 3y = 26$. Protože $D(4, 3) = 1$ a $1 \mid 26$, rovnice má řešení. Jedno řešení této rovnice můžeme uhádnout, rovnici splňují například $x_p = 5$ a $y_p = 2$. Jak budou vypadat další řešení? Musíme najít řešení homogenní rovnice $4x + 3y = 0$. Tato rovnice má řešení $x_h = -3k$ a $y_h = 4k$, $k \in \mathbb{Z}$. Toto řešení dostaneme jednoduše tak, že čísla „prohodíme“ a k jednomu z nich přidáme mínus. Všechna řešení rovnice tedy mají tvar $x = 5 - 3k$ a $y = 2 + 4k$, $k \in \mathbb{Z}$, neboli $(5, 2) + k \cdot (-3, 4)$, $k \in \mathbb{Z}$. (Habala, 2019b, s. 3)

Většinou se nám nepodaří uhádnout řešení a potřebujeme tak nějaký postup, kterým řešení najdeme vždy. Takových postupů (metod) existuje mnoho, v této práci si ukážeme některé z nich.

Příklad 2.1 Najděte všechna řešení diofantické rovnice $43x + 15y = 110$.

2.1.1 Řešení pomocí rozšířeného Eukleidova algoritmu

Věta 12 (Eukleidův algoritmus)

Nechť $a > b$ jsou přirozená čísla. Potom následující posloupnost celočíselných dělení s příslušnými vztahy mezi děliteli

$$\begin{aligned} a &= bq_0 + r_0, & 0 \leq r_0 < b, \\ b &= r_0q_1 + r_1, & 0 \leq r_1 < r_0 \quad (\text{jestliže } r_0 \neq 0), \\ r_0 &= r_1q_2 + r_2, & 0 \leq r_2 < r_1 \quad (\text{jestliže } r_1 \neq 0), \\ &\vdots \\ r_{t-1} &= r_tq_{t+1} + r_{t+1}, & 0 \leq r_{t+1} < r_t \quad (\text{jestliže } r_t \neq 0), \\ &\vdots \end{aligned}$$

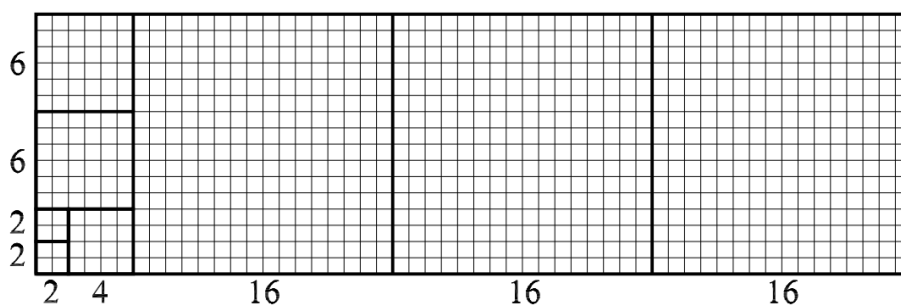
je konečná: končí v okamžiku, kdy je některý zbytek roven nule, tj. takto:

$$\begin{aligned} r_{k-2} &= r_{k-1}q_k + r_k, & 0 \leq r_k < r_{k-1}, \\ r_{k-1} &= r_kq_{k+1}. \end{aligned}$$

Poslední nenulový zbytek r_k je největším společným dělitelem čísel a a b . Jestliže je již $r_0 = 0$, potom $D(a, b) = b$.

Důkaz: Protože posloupnost přirozených čísel $b > r_0 > r_1 > \dots > r_t > \dots \geq 0$ je klesající a zdola omezená, algoritmus musí skončit po konečném počtu kroků.

Označme jako $S(a_1, a_2, \dots, a_n)$ množinu všech kladných společných dělitelů čísel $a_1, a_2, \dots, a_n$. Vzhledem k uvedeným vztahům platí $S(a, b) = S(b, r_0) = S(r_1, r_2) = \dots = S(r_{k-2}, r_{k-1}) = S(r_{k-1}, r_k) = S(r_k)$. Určitě je r_k dělitelem čísel a, b , ale také každý dělitel čísel a, b dělí r_k . Proto je $r_k = D(a, b)$. (Dlab, 2016, s. 101)



Obr. 5: Grafické znázornění Eukleidova algoritmu pro výpočet $D(54, 16)$.

(Křížek, 2018)

Rozšířený Eukleidův algoritmus spočívá v tom, že kromě největšího společného dělitele najdeme i jeho vyjádření pomocí Bézoutovy rovnosti (Věta 6), tedy najdeme koeficienty $u, v \in \mathbb{Z}$ takové, že $D(a, b) = au + bv$.

Na rovnici $43x + 15y = 110$ si ukážeme, jak rozšířený Eukleidův algoritmus můžeme přehledně zapsat pomocí tabulky.

	a, b	u	v
	43	1	0
2	15	0	1
1	13	1	-2
6	2	-1	3
2	1	7	-20
	0	-15	43

Ve sloupci a, b vidíme Eukleidův algoritmus, poslední nenulový zbytek je 1, $D(43, 15)$ je tedy 1. Nalevo je koeficient, který nám říká, kolikrát se číslo v daném řádku vejde do čísla o řádek výše. Koeficienty u, v počítáme takto: na začátku napíšeme jedničky a nuly tak, jak je v tabulce uvedeno. Další řádek dostaneme odečtením druhého řádku vynásobeného koeficientem od prvního řádku.

Rozšířeným Eukleidovým algoritmem jsme dostali vyjádření $7 \cdot 43 + (-20) \cdot 15 = 1$. V původní rovnici ale máme napravo číslo 110, proto musíme celou rovnost tímto číslem vynásobit. Dostaneme tak $(7 \cdot 110) \cdot 43 + (-20 \cdot 110) \cdot 15 = 770 \cdot 43 - 2200 \cdot 15 = 110$. Našli jsme tedy řešení $x = 770, y = -2200$. Další řešení dostaneme přičtením

řešení přidružené homogenní rovnice $43x + 15y = 0$. Protože $x_h = -15k$ a $y_h = 43k$, $k \in \mathbb{Z}$, všechna řešení této rovnice jsou tvaru $x = 770 - 15k$, $y = -2\,200 + 43k$, $k \in \mathbb{Z}$.

Zkoušku můžeme provést dosazením: $43 \cdot (770 - 15k) + 15 \cdot (-2\,200 + 43k) = 33\,110 - 43 \cdot 15k - 33\,000 + 15 \cdot 43k = 110$.

Takto vysoká čísla ale nemusí být při řešení úloh příliš praktická. Proto je často dobré upravit řešení pomocí zvolení vhodného k , v tomto případě můžeme například zvolit $k = 51$ a dostaneme řešení $x_1 = 5$, $y_1 = -7$, všechna řešení potom budou mít tvar $x = 5 - 15k'$, $y = -7 + 43k'$, $k' \in \mathbb{Z}$.

Všimněme si, že použitím rozšířeného Eukleidova algoritmu jsme v tabulce dostali v posledních dvou řádcích matici $\begin{pmatrix} D(a,b) & A & B \\ 0 & A_h & B_h \end{pmatrix}$, tedy Bézoutovu rovnost a řešení homogenní rovnice. (Habala, 2019b, s. 6-9)

Řešení pomocí Eukleidova algoritmu je spolehlivý způsob řešení diofantických rovnic. Nevýhodou může být tvar získaných řešení, protože čím větší je číslo napravo, tím větší partikulární řešení získáme.

2.1.2 Řešení pomocí kongruencí

Další metodou je řešení pomocí převodu na lineární kongruenci. Budeme řešit stejnou rovnici jako u předchozí metody, tedy $43x + 15y = 110$.

Úpravou dostaneme rovnici $43x = 110 - 15y$. Substitucí $y = -t$ dostaneme rovnici $43x = 110 + 15t$, což ale není nic jiného než lineární kongruence $43x \equiv 110 \pmod{15}$, kterou nyní vhodnými úpravami vyřešíme. (S kongruencí byla ekvivalentní již rovnice $43x = 110 - 15y$, protože u kongruencí nezáleží, jestli modulo přičítáme nebo odčítáme.)

$$43x \equiv 110 \pmod{15}$$

$$13x \equiv 5 \pmod{15}$$

$$-2x \equiv -10 \pmod{15}$$

$$x \equiv 5 \pmod{15}$$

Dostáváme tedy řešení $x = 5 + 15k, k \in \mathbb{Z}$. Pro řešení této kongruence jsme mohli rovněž aplikovat Čínskou větu o zbytcích a řešit soustavu kongruencí $43x \equiv 110 \pmod{3}$ a $43x \equiv 110 \pmod{5}$.

Neznámou y vypočítáme dosazením do původní rovnice:

$$43 \cdot (5 + 15k) + 15y = 110$$

$$215 + 43 \cdot 15k + 15y = 110$$

$$15y = -105 - 43 \cdot 15k$$

$$y = -7 - 43k$$

(Můžeme také dosadit pouze partikulární řešení $x = 5$, čímž dostaneme $y = -7$ a dále k těmto řešením přičteme řešení homogenní rovnice.)

$$\text{Zkouška: } 43 \cdot (5 + 15k) + 15 \cdot (-7 - 43k) = 215 + 43 \cdot 15k - 105 - 15 \cdot 43k = 110.$$

Na začátku jsme mohli rovněž rovnici převést na kongruenci $15y \equiv 110 \pmod{43}$ a získat tak nejdříve řešení pro y .

$$15y \equiv 110 \pmod{43}$$

$$15y \equiv 24 \pmod{43}$$

$$5y \equiv 8 \pmod{43}$$

$$5y \equiv -35 \pmod{43}$$

$$y \equiv -7 \pmod{43}$$

Dostaneme tedy řešení $y = -7 + 43k, k \in \mathbb{Z}$. Hodnotu neznámé x získáme opět dosazením.

Řešení pomocí kongruencí je často rychlé a elegantní díky tomu, že pomocí modulu dostaneme malá čísla, je ovšem nutné umět s kongruencemi pracovat. Většinou je vhodné zvolit jako modulo menší z koeficientů, ale v některých případech může být vhodnější vybrat větší koeficient. Může se stát, že kongruence nepůjde vyřešit jednoduše (jako v Příkladu 1.17), v tom případě je lepší zvolit jinou metodu řešení, než strávit hodně času nad kongruenční rovnicí.

2.1.3 Redukční metoda

Tato metoda spočívá ve vyjádření neznámé s menším koeficientem a hledání neznámých tak, abychom získali ze zlomku celé číslo. Opět si metodu ukážeme na rovnici $43x + 15y = 110$.

$$43x + 15y = 110$$
$$y = \frac{110 - 43x}{15} = -2x + \frac{110 - 13x}{15}$$

Abychom dostali celočíselné řešení, musíme dostat ze zlomku $\frac{110-13x}{15}$ celé číslo, tedy $110 - 13x$ musí být násobkem 15, neboli $110 - 13x = 15u$. Nyní vyjádříme neznámou x .

$$-13x = 15u - 110$$
$$x = \frac{110 - 15u}{13} = -u + \frac{110 - 2u}{13}$$

Opakujeme postup pro tento nový zlomek. Protože $\frac{110-2u}{13}$ musí být celé číslo, musíme hledat takové hodnoty u , pro které je výraz $110 - 2u$ dělitelný třinácti. Násobek 13 nejbližší číslu 110 je 104, zvolíme tedy $u = 3$. Nebo můžeme i ze zlomku $\frac{110-2u}{13}$ odebrat celou část a dostat tak $8 + \frac{6-2u}{13}$. Odtud vidíme, že výraz dával celé číslo, musíme najít u takové, aby $6 - 2u$ bylo násobkem třinácti. Nejjednodušší řešení je $u = 3$.

Zpětným dosazením získáme $x = 5$, což opět dosadíme a získáme řešení $y = -7$. Tím jsme získali partikulární řešení $(5, -7)$, všechna řešení dostaneme přičtením řešení homogenní rovnice.

Tato metoda řešení je výhodná v tom, že potřebujeme jen matematiku základní školy. Může být ale trochu nepřehledná.

2.1.4 Další metody

Řešení pomocí substituce

Metodu využívající substituci si ukážeme opět na rovnici $43x + 15y = 110$.

$$43x + 15y = 110$$
$$13x + 15 \cdot (2x + y) = 110$$

$$\begin{aligned}
x^i &= x; y^i = 2x + y \\
13x^i + 15y^i &= 110 \\
13 \cdot (x^i + y^i) + 2y^i &= 110 \\
x^{ii} &= x^i + y^i; y^{ii} = y^i \\
13x^{ii} + 2y^{ii} &= 110 \\
x^{ii} + 2 \cdot (6x^{ii} + y^{ii}) &= 110 \\
x^{(3)} &= x^{ii}; y^{(3)} = 6x^{ii} + y^{ii} \\
x^{(3)} + 2y^{(3)} &= 110 \\
x^{(4)} &= x^{(3)} + 2y^{(3)}; y^{(4)} = y^{(3)} \\
x^{(4)} &= 110
\end{aligned}$$

Původní rovnice je ekvivalentní s $x^{(4)}$. Hodnota $x^{(4)}$ je pevně daná, hodnota $y^{(4)}$ může být libovolná. Proto si zvolíme $y^{(4)} = t$; $t \in \mathbb{Z}$. Zpětnou substitucí zjistíme řešení x a y :

$$\begin{aligned}
x^{(3)} &= 110 - 2t = x^{ii} \\
y^{ii} &= t - 6 \cdot (110 - 2t) = 13t - 660 = y^i \\
x^i &= x^{ii} - y^i = 110 - 2t - (13t - 660) = 770 - 15t = x \\
y &= y^i - 2x = 13t - 660 - 2 \cdot (770 - 15t) = -2200 + 43t = y
\end{aligned}$$

Získali jsme tedy řešení $x = 770 - 15t$, $y = -2200 + 43t$, $t \in \mathbb{Z}$, které je totožné s řešením získaným rozšířeným Eukleidovým algoritmem a dává pochopitelně stejné hodnoty jako řešení pomocí ostatních metod. (Niven, 1991, s. 214-217)

Stejně jako redukční metoda, ani tento způsob řešení nevyžaduje žádné znalosti nad rámec učiva ZŠ. Je ale velice nepřehledná a proto bych ji až na výjimky k řešení nedoporučovala. Můžeme si všimnout, že také využívá věty o dělení čísel se zbytkem a dostáváme zde stejné koeficienty jako u řešení rozšířeným Eukleidovým algoritmem.

Řešení pomocí matice

Poslední zmiňovanou metodu lze zapsat také v maticích, čímž dostaneme přehlednější zápis postupu. Zde si pouze ukážeme postup na nám známé rovnici $43x + 15y = 110$, podrobněji je metoda vysvětlena v knize (Niven, 1991). Sloupcovými úpravami převedeme tuto matici na tvar, kdy bude v prvním řádku na jednom místě 0.

$$\begin{pmatrix} 43 & 15 & 110 \\ 1 & 0 & x \\ 0 & 1 & y \end{pmatrix} \sim \begin{pmatrix} 13 & 15 & 110 \\ 1 & 0 & x \\ -2 & 1 & y \end{pmatrix} \sim \begin{pmatrix} 13 & 2 & 110 \\ 1 & -1 & x \\ -2 & 3 & y \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 2 & 110 \\ 7 & -1 & x \\ -20 & 3 & y \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 110 \\ 7 & -15 & x \\ -20 & 43 & y \end{pmatrix}$$

Dostali jsme vyjádření

$$\begin{aligned} x' &= 110 \\ 7x' - 15y' &= x \\ -20x' + 43y' &= y. \end{aligned}$$

Po dosazení a substituci $y' = t$ dostaneme řešení $x = 770 - 15t$, $y = -2200 + 43t$, $t \in \mathbb{Z}$. (Niven, 1991, s. 218)

Tato metoda je dle mého vylepšením předchozí metody a opět v podstatě jen jiným zápisem rozšířeného Eukleidova algoritmu, který je ale přehlednější.

Řešení pomocí řetězového zlomku

Tuto metodu můžeme využít ve chvíli, kdy už je daná rovnice v základním tvaru, tj. už ji nemůžeme krátit, neboli $D(a, b, c) = 1$. Metoda je více rozebrána v (Steinsdörfer, 2015, s. 24-35). Zde si ukážeme na rovnici $43x + 15y = 110$ pouze postup.

Koeficienty z rovnice si napíšeme do zlomku a následně tento zlomek vyjádříme jako řetězový zlomek.

$$\frac{43}{15} = 2 + \frac{13}{15} = 2 + \frac{1}{\frac{15}{13}} = 2 + \frac{1}{1 + \frac{2}{13}} = 2 + \frac{1}{1 + \frac{1}{\frac{13}{2}}} = 2 + \frac{1}{1 + \frac{1}{6 + \frac{1}{2}}}$$

Nyní poslední zlomek $(\frac{1}{2})$ odebereme a řetězový zlomek opět vyjádříme jako zlomek v základním tvaru.

$$2 + \frac{1}{1 + \frac{1}{6}} = 2 + \frac{1}{\frac{7}{6}} = 2 + \frac{6}{7} = \frac{20}{7}$$

Nyní od sebe odečteme původní zlomek a nově získaný zlomek.

$$\frac{43}{15} - \frac{20}{7} = \frac{301 - 300}{105} = \frac{1}{105}$$

Z rovnosti vidíme, že platí $43 \cdot 7 - 15 \cdot 20 = 1$, což připomíná zadanou rovnici. Aby se rovnaly pravé strany, vynásobíme celou rovnici 110 a dostaneme $43 \cdot 770 - 15 \cdot 2200 = 110$. Našli jsme tedy partikulární řešení $x = 770, y = 2200$, pro získání všech řešení přičteme k získané dvojici čísel řešení homogenní rovnice stejně jako u předchozích metod.

Tato metoda opět využívá věty o dělení celých čísel se zbytkem. Na příkladu vidíme, že metoda funguje, není ale příliš zřejmé, proč tomu tak je.

Úlohy

2.1 Najděte všechna řešení lineárních diofantických rovnic

- a) $17x + 29y = 101$
- b) $76x - 19y = 51$
- c) $28x - 63y = 3227$
- d) $37x + 57y = 8276$

2.2 Určete rozměry všech rovnoramenných trojúhelníků s obvodem 15 cm, které mají celočíselné délky stran.

2.3 Máme nádoby o objemech 5 litrů a 7 litrů. Ve třetí nádobě potřebujeme získat 1 l litrů. Jak budeme postupovat?

2.4 Správce tělocvičny dostal 12 000 Kč na nákup míčů. Menší míč stojí 320 Kč, větší míč stojí 360 Kč. Nemá určeno, kolik míčů má koupit, ale musí za ně utratit celou částku. Kolik kterých míčů může koupit? (Rubeš, 2022)

2.5 V prodejně suvenýrů prodávají dva druhy trpaslíků. První druh stojí 330 Kč, druhý druh stojí 450 Kč. Přijel autobus turistů, kteří nakoupili trpaslíky za 5 670 Kč. Kolik kterých trpaslíků koupili? (Rubeš, 2022)

2.6 V zahradnictví prodávají sazenice rybízu a angreštu. Jedna sazenice rybízu stojí 99 Kč, jedna sazenice angreštu stojí 126 Kč.

- a) Koupili jsme nějaký počet sazenic rybízu a angreštu. Mohl nákup stát přesně 2000 Kč?
- b) Kolik jsme koupili kterých sazenic, když nám prodavač vrátil po platbě dvoutisícovou bankovkou méně než 10 Kč?

2.2 Lineární diofantické rovnice o třech neznámých

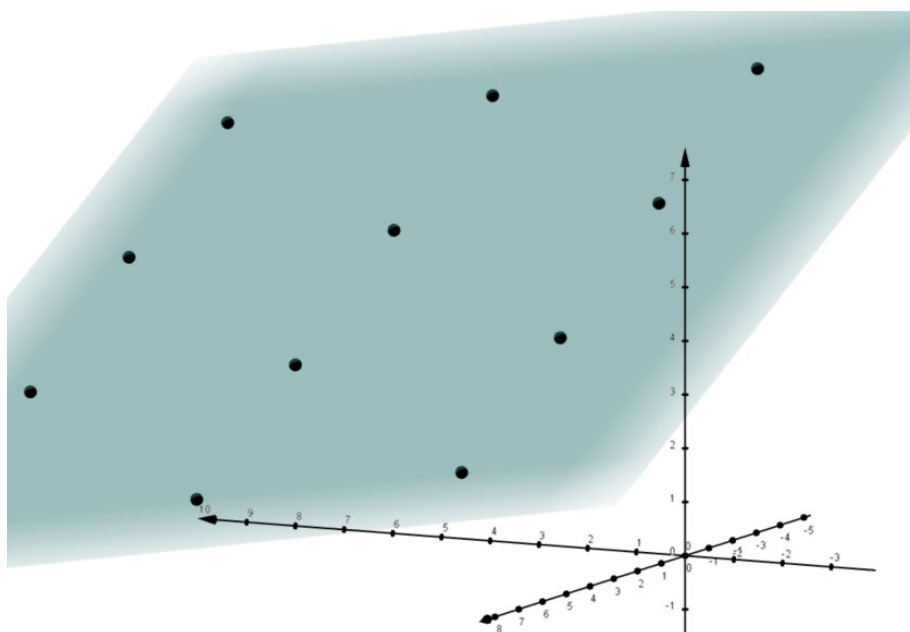
Definice 8 (Lineární diofantická rovnice o třech neznámých)

Lineární diofantickou rovnicí o třech neznámých rozumíme rovnici ve tvaru $ax + by + cz = d$ s koeficienty $a, b, c \in \mathbb{Z}$ s řešením $x, y, z \in \mathbb{Z}$.

Pro řešitelnost rovnice o třech neznámých platí stejné pravidlo jako pro řešitelnost rovnice o dvou neznámých, tedy že rovnice má celočíselná řešení právě tehdy, když největší společný dělitel koeficientů dělí číslo na pravé straně, neboli $\exists k \in \mathbb{Z}: D(a, b, c) \cdot k = d$.

Jak bude vypadat řešení? V případě, že nám podaří najít nějaké jedno partikulární řešení rovnice, získáme všechna řešení opět přičtením řešení přidružené homogenní rovnice. Jelikož řešíme jednu rovnici o třech neznámých, budeme potřebovat k vyjádření všech řešení dva parametry.

Geometricky se jedná o rovinu, přičemž hledáme body náležící rovině, které mají všechny tři souřadnice celočíselné. Partikulární řešení odpovídá jednomu konkrétnímu bodu splňujícímu tyto podmínky; řešením homogenní rovnice je rovina. Dva parametry odpovídají dvěma vektorům, které generují tento prostor – rovinu. Jejich celočíselné násobky dávají další řešení diofantické rovnice.



Obr. 6: Geometrické znázornění řešení diofantické rovnice $5x - 3y + 7z = 61$.

(Vytvořeno pomocí programu GeoGebra.)

2.2.1 Řešení pomocí rozšířeného Eukleidova algoritmu

Při použití Eukleidova algoritmu pro rovnici se dvěma neznámými $ax + by = c$ jsme vlastně převáděli matici tvaru $\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$ na tvar $\begin{pmatrix} D(a,b) & A & B \\ 0 & A_h & B_h \end{pmatrix}$. Nyní se o něco

podobného pokusíme s rovnicí $ax + by + cz = d$ reprezentovanou maticí $\begin{pmatrix} a & 1 & 0 & 0 \\ b & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{pmatrix}$.

Tuto matici můžeme řádkovými úpravami převést na tvar $\begin{pmatrix} D(a,b,c) & A_1 & A_2 & A_3 \\ 0 & B_1 & B_2 & B_3 \\ 0 & C_1 & C_2 & C_3 \end{pmatrix}$.

Pokud je rovnice řešitelná, tuto matici můžeme převést na tvar $\begin{pmatrix} d & A_{p1} & A_{p2} & A_{p3} \\ 0 & B_{h1} & B_{h2} & B_{h3} \\ 0 & 0 & C_{h2} & C_{h3} \end{pmatrix}$.

V prvním řádku získáme partikulární řešení rovnice, ve zbývajících dvou řádcích řešení homogenní rovnice. (Habala, 2019b, s. 22-24)

Postup si ukážeme na následující rovnici.

Příklad 2.2 Najděte všechna řešení diofantické rovnice $5x - 3y + 7z = 61$.

Řešení: Do prvního sloupce si napíšeme koeficienty z levé části rovnice, vedle nich jednotkovou matici. Řádkovými úpravami budeme matici upravovat tak, abychom na místě a_{11} (vlevo nahoře) dostali číslo z pravé strany rovnice a matice byla ve stupňovitém (schodovitém) tvaru.

$$\begin{pmatrix} 5 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0 \\ 7 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 70 & 14 & 0 & 0 \\ -3 & 0 & 1 & 0 \\ 7 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 70 & 14 & 0 & 0 \\ -3 & 0 & 1 & 0 \\ 0 & 14 & 0 & -10 \end{pmatrix} \sim \\ \sim \begin{pmatrix} 61 & 14 & 3 & 0 \\ -3 & 0 & 1 & 0 \\ 0 & 14 & 0 & -10 \end{pmatrix} \sim \begin{pmatrix} 61 & 14 & 3 & 0 \\ 0 & 42 & 70 & 0 \\ 0 & 14 & 0 & -10 \end{pmatrix} \sim \begin{pmatrix} 61 & 14 & 3 & 0 \\ 0 & 42 & 70 & 0 \\ 0 & 0 & 70 & 30 \end{pmatrix} \sim \\ \sim \begin{pmatrix} 61 & 14 & 3 & 0 \\ 0 & 3 & 5 & 0 \\ 0 & 0 & 7 & 3 \end{pmatrix}$$

V prvním řádku jsme získali partikulární řešení, ve zbývajících dvou řádcích řešení homogenní rovnice. Dostali jsme tedy řešení $[14, 3, 0] + k \cdot (3, 5, 0) + l \cdot (0, 7, 3)$ neboli

$$\begin{aligned}x &= 14 + 3k, \\y &= 3 + 5k + 7l, \\z &= 3l,\end{aligned}$$

kde $k, l \in \mathbb{Z}$.

Zkouška: $5 \cdot (14 + 3k) - 3 \cdot (3 + 5k + 7l) + 7 \cdot 3l = 70 + 15k - 9 - 15k - 21l + 21l = 61$

Řešení 2: Místo práce s jednou maticí bychom také mohli opakovaně použít rozšířený Eukleidův algoritmus pro dvě neznámé. Využijeme faktu, že $D(a, b, c) = D(D(a, b), c)$.

Opět budeme řešit rovnici $5x - 3y + 7z = 61$. Hledáme koeficienty u, v, w , pro které bude platit $5u - 3v + 7w = D(a, b, c)$. Nejdříve provedeme Eukleidův algoritmus pro čísla 5 a -3 (to můžeme udělat tak, že provedeme algoritmus pro čísla 5 a 3 a ve výsledném vyjádření Bézoutovy rovnosti upravíme znaménka, aby rovnost platila).

	a, b	u	v
	5	1	0
1	3	0	1
1	2	1	-1
2	1	-1	2
	0	3	-5

Dostali jsme vyjádření $1 = -1 \cdot 5 + 2 \cdot 3$. Protože původní koeficient byl -3 , Bézoutovu rovnost upravíme na $1 = -1 \cdot 5 - 2 \cdot (-3)$. Získali jsme tedy koeficienty $u = -1$ a $v = -2$. Řešením homogenní rovnice $5u - 3v = 0$ jsou čísla $u = 3$ a $v = 5$.

Nyní napíšeme obdobnou tabulku pro koeficienty u, v, w . Koeficienty u, v jsme již získali, potřebujeme dopočítat koeficient w . Protože v tomto případě $D(a, b) = D(a, b, c)$, dopočítáme pouze poslední řádek pro získání řešení homogenní rovnice.

	a, b	w	u	v
	7	1	0	0
7	1	0	-1	2
	0	1	7	-14

Dostali jsme vyjádření $5 \cdot (-1) - 3 \cdot (-2) + 7 \cdot 0 = 1$. Protože v původní rovnici je na pravé straně číslo 61, tímto číslem celou rovnost vynásobíme a máme $5 \cdot (-61) - 3 \cdot (-122) + 7 \cdot 0 = 61$. Dostali jsme partikulární řešení $[-61, -122, 0]$.

Řešení přidružené homogenní rovnice získáme z posledních řádků Eukleidových algoritmů, z prvního máme $(3, 5, 0)$, z druhého jsme dostali $(7, 14, 1)$ (opět změníme znaménko u koeficientu v , aby platilo $5u - 3v + 7w = 0$). Všechna řešení rovnice mají tedy tvar $[-61, -122, 0] + k \cdot (3, 5, 0) + l \cdot (7, 14, 1)$, neboli

$$\begin{aligned}x &= -61 + 3k + 7l, \\y &= -122 + 5k + 14l, \\z &= l,\end{aligned}$$

kde $k, l \in \mathbb{Z}$.

Zkouška: $5 \cdot (-61 + 3k + 7l) - 3 \cdot (-122 + 5k - 14l) + 7l = -305 + 15k + 35l + 366 - 15k - 42l + 7l = 61$

2.2.2 Řešení pomocí kongruencí

Podobně jako u rovnice se dvěma neznámými můžeme převést rovnici se třemi neznámými na lineární kongruenci a tu vyřešit.

$$\begin{aligned}5x - 3y + 7z &= 61 \\5x + 7z &\equiv 61 \pmod{3} \\2x + z &\equiv 1 \pmod{3} \\2x + z &= 1 + 3k \\z &= 1 + 3k - 2x \\5x - 3y + 7 \cdot (1 + 3k - 2x) &= 61 \\-9x - 3y + 21k &= 54 \\y &= -18 + 7k - 3x\end{aligned}$$

Za x můžeme zvolit libovolné číslo. Dostáváme řešení

$$\begin{aligned}x &= l, \\y &= -18 + 7k - 3l, \\z &= 1 + 3k - 2l,\end{aligned}$$

kde $k, l \in \mathbb{Z}$, neboli $[0, -18, 1] + k \cdot (0, 7, 3) + l \cdot (1, -3, -2)$.

Zkouška: $5x - 3y + 7z = 5l - 3 \cdot (-18 + 7k - 3l) + 7 \cdot (1 + 3k - 2l) = 5l + 54 - 21k + 9l + 7 + 21k - 14l = 61$.

2.2.3 Redukční metoda

Pro řešení lineární diofantické rovnice o třech neznámých můžeme použít také redukční metodu.

$$\begin{aligned}5x - 3y + 7z &= 61 \\y &= \frac{5x + 7z - 61}{3} = x + 2z - 20 + \frac{2x + z - 1}{3}\end{aligned}$$

Zlomek musí být celé číslo, proto $2x + z - 1 = 3k$. Nyní si vyjádříme další proměnnou.

$$z = 3k - 2x + 1$$

Za neznámou x si můžeme zvolit libovolnou proměnnou, použijeme tedy substituci $x = l, l \in \mathbb{Z}$.

Dosadíme $z = 3k - 2l + 1$ a vyjádříme $y = (5l + 21k - 14l + 7 - 61) : 3 = -18 + 7k - 3l$.

Dostaneme tedy řešení

$$\begin{aligned}x &= l, \\y &= -18 + 7k - 3l, \\z &= 1 + 3k - 2l,\end{aligned}$$

kde $k, l \in \mathbb{Z}$.

Toto řešení můžeme také zapsat jako $[0, -18, 1] + k \cdot (0, 7, 3) + l \cdot (1, -3, -2)$. Zkouška by byla totožná jako u předchozí metody.

2.2.4 Další metody

Řešení pomocí matice

Rovnici o třech neznámých můžeme řešit také pomocí metody Nivena (1991), zapsanou pomocí matice. V matici upravujeme sloupce tak, abychom v prvním řádku dostali na jednom z míst v prvních třech sloupcích jedničku a na ostatních místech nulu.

$$\begin{pmatrix} 5 & -3 & 7 & 61 \\ 1 & 0 & 0 & x \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & z \end{pmatrix} \sim \begin{pmatrix} 5 & -3 & 1 & 61 \\ 1 & 0 & 0 & x \\ 0 & 1 & 2 & y \\ 0 & 0 & 1 & z \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 & 61 \\ 1 & 0 & 0 & x \\ -10 & 7 & 2 & y \\ -5 & 3 & 1 & z \end{pmatrix}$$

Odtud

$$\begin{aligned} x &= k, \\ y &= -10k + 7l + 122, \\ z &= -5k + 3l + 61, \end{aligned}$$

kde $k, l \in \mathbb{Z}$, neboli $[0, 122, 61] + k \cdot (0, 7, 3) + l \cdot (1, -10, -5)$.

Zkouška: $5k - 3 \cdot (-10k + 7l + 122) + 7 \cdot (-5k + 3l + 61) = 5k + 30k - 21l - 366 - 35k + 21l + 427 = 61$.

Metoda redukce na menší počet neznámých

Tato metoda spočívá ve vhodné substituci a redukci na lineární diofantickou rovnici o dvou neznámých. (Steinsdörfer, 2015)

$$\begin{aligned} 5x - 3y + 7z &= 61 \\ u &= 5x - 3y \\ u + 7z &= 61 \end{aligned}$$

Tuto rovnici můžeme vyřešit jakýmkoli způsobem uvedeným v části 4.1.1. Zde můžeme řešení také uhodnout. Jedním řešením určitě bude $u = 5$ a $z = 8$. Všechna řešení této rovnice budou tvaru $u = 5 + 7k, z = 8 - k, k \in \mathbb{Z}$. Nyní musíme dosadit za u a řešit rovnici $5x - 3y = 5 + 7k$.

Podle Bézoutovy věty má rovnice $5x - 3y = 1$ řešení, toto řešení najdeme rozšířeným Eukleidovým algoritmem (nebo jiným způsobem). Dostaneme Bézoutovu rovnost

$$5 \cdot 2 - 3 \cdot 3 = 1,$$

vynásobením výrazem napravo získáme

$$5 \cdot (10 + 14k) - 3 \cdot (15 + 21k) = 5 + 7k.$$

Řešením jsou tedy čísla tvaru $x = 10 + 14k + 3l, y = 15 + 21k + 5l; k, l \in \mathbb{Z}$, původní rovnici řeší čísla tvaru

$$x = 10 + 14k + 3l,$$

$$y = 15 + 21k + 5l,$$

$$z = 8 - k,$$

kde $k, l \in \mathbb{Z}$, řešení můžeme zapsat také jako $[10, 15, 8] + k \cdot (14, 21, -1) + l \cdot (3, 5, 0)$.

$$\text{Zkouška: } 5 \cdot (10 + 14p + 3q) - 3 \cdot (15 + 21p + 5q) + 7 \cdot (8 - p) = 50 + 70p + 15q - 45 - 63p - 15q + 56 - 7p = 61.$$

Obecně provedeme substituci takto:

Označme $e = D(a, b)$, potom $a = ea', b = eb'$, kde $a', b' \in \mathbb{Z}^+$ a platí $D(a', b') = 1, D(e, b') = 1$.

$$ax + by + cz = d$$

$$ea'x + eb'y + cz = d$$

$$e(a'x + b'y) + cz = d$$

$$eu + cz = d$$

Neboli v případě, že mají některé z koeficientů společného dělitele většího než 1, tohoto společného dělitele vytkneme a substituci provádíme pouze za výraz v závorce.

Poslední zmiňovaná metoda je pravděpodobně nejnázornější, protože nepoužíváme matice ani kongruence, ale pouze způsob řešení úloh známý již ze SŠ. Řešení pomocí kongruencí je ale i v tomto případě poměrně efektivní. Viděli jsme, že jsme dostávali řešení v různých tvarech. Všechny tvary ale generují stejné řešení, o čemž bychom se mohli přesvědčit vhodnou volbou parametrů k a l .

Úlohy

2.7 Najděte všechna řešení následujících lineárních diofantických rovnic

a) $17x + 28y + 3z = 421$

b) $36x + 52y + 32z = 1072$.

2.8 V obchodě prodávají trička po 230 Kč, pár ponožek za 40 Kč a košile po 350 Kč.

Za nákup jsme zaplatili 1250 Kč. Od každého druhu výrobku jsme koupili minimálně jeden kus. Kolik kterého oblečení jsme mohli koupit?

2.3 Lineární diofantické rovnice o čtyřech a více neznámých

Pro řešení lineárních diofantických rovnic o čtyřech a více neznámých můžeme používat stejné metody jako u řešení rovnic o třech neznámých. Se zvyšujícím se počtem neznámých se některé metody ale stávají méně efektivními. V metodách využívajících matice se zvětšují matice, které musíme upravovat, metodu redukce počtu neznámých bychom museli použít několikrát. Nejsnadněji se jeví převod na kongruence, kde s každou další neznámou všude přibude jen jeden člen, což obtížnost a čas řešení prodlouží jen nepatrně.

Řešení rovnice o čtyřech neznámých pomocí kongruencí si ukážeme na následující rovnici.

Příklad 2.3 Najděte všechna celočíselná řešení rovnice $14x - 15y - 9z + 26u = 53$.

Jako modul si zvolíme nejmenší z koeficientů – číslo 9.

$$14x - 15y + 26u \equiv 53 \pmod{9}$$

$$5x - 6y + 8u \equiv 8 \pmod{9}$$

$$5x + 3y - u \equiv -1 \pmod{9}$$

$$u = 5x + 3y + 1 + 9r$$

Nechť $x = s$ a $y = t$, kde $s, t \in \mathbb{Z}$, potom $u = 5s + 3t + 1 + 9r$, kde $r \in \mathbb{Z}$.

Dopočítáme neznámou z .

$$14s - 15t - 9z + 26(5s + 3t + 1 + 9r) = 53$$

$$14s - 15t - 9z + 130s + 78t + 26 + 234r = 53$$

$$144s + 63t + 234r - 9z = 27$$

$$9z = 144s + 63t + 234r - 27$$

$$z = 16s + 7t + 26r - 3$$

Řešením rovnice je tedy

$$x = s,$$

$$y = t,$$

$$z = 16s + 7t + 26r - 3,$$

$$u = 5s + 3t + 1 + 9r,$$

kde $s, t, r \in \mathbb{Z}$.

Zkouška: $14x - 15y - 9z + 26u =$

$$= 14s - 15t - 9 \cdot (16s + 7t + 26r - 3) + 26 \cdot (5s + 3t + 1 + 9r) =$$

$$= 14s - 15t - 144s - 63t - 234r + 27 + 130s + 78t + 26 + 234r = 53.$$

Grafické znázornění by bylo nepřehledné, neboť jsme se dostali již do čtvrtého rozměru, který se v našem trojrozměrném světě zobrazuje poměrně obtížně.

Úlohy

2.9 Najděte všechna řešení lineární diofantické rovnice $26x + 31y + 11z + 53w = 256$.

2.4 Soustavy lineárních diofantických rovnic

Definice 9 (Soustava lineárních diofantických rovnic)

Soustavou lineárních diofantických rovnic rozumíme soustavu m lineárních diofantických rovnic o n neznámých:

$$\begin{aligned}a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= c_1, \\a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= c_2, \\&\vdots \\a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= c_m.\end{aligned}$$

Typicky $m \leq n$.

Soustavu rovnic můžeme zapsat také v maticovém tvaru jako $A\vec{x} = \vec{c}$, kde $A = (a_{ij})$ typu $m \times n$. (Habala, 2019b, s. 25)

Jak je to s řešitelností? Jistě musí být každá z rovnic řešitelná sama o sobě, tedy největší společný dělitel všech koeficientů rovnice na levé straně musí dělit číslo napravo. To nám bohužel nezajistí, že bude řešitelná celá soustava, jak si ukážeme později na příkladu.

V případě soustavy dvou diofantických rovnic o dvou neznámých můžeme soustavu řešit stejně jako v reálných číslech. Pokud dostaneme nějaké řešení, pak toto řešení bude řešením soustavy diofantických rovnic, jestliže to jsou celá čísla. Pokud dostaneme nekonečně mnoho řešení, znamená to, že můžeme soustavu zredukovat na jednu rovnici, kterou vyřešíme podle části 2.1.

Proto budeme typicky řešit soustavy rovnic, které mají větší počet neznámých než rovnic. Způsoby řešení těchto soustav si ukážeme na následujících příkladech.

Příklad 2.4 Najděte všechna celočíselná řešení soustavy rovnic

$$\begin{aligned}x + y + 2z &= 7 \\4x + 5y &= 11.\end{aligned}$$

Můžeme použít sčítací metodu. První rovnici vynásobíme číslem -4 a rovnice sečteme.

$$y - 8z = -17$$

Dostali jsme diofantickou rovnici o 2 neznámých, kterou již umíme vyřešit. Řešením této rovnice je

$$\begin{aligned}y &= -1 + 8t \\z &= 2 + t, t \in \mathbb{Z}.\end{aligned}$$

Dosazením do druhé rovnice dostaneme

$$\begin{aligned}4x + 5(-1 + 8t) &= 11, \\4x - 5 + 40t &= 11, \\4x &= 16 + 40t, \\x &= 4 + 10t.\end{aligned}$$

Příklad 2.5 Najděte všechna celočíselná řešení soustavy rovnic

$$\begin{aligned}4x + 9y &= -3, \\7x + 3y + z &= 1.\end{aligned}$$

Druhou rovnici vynásobíme číslem -3 a rovnice sečteme.

$$-17x - 3z = -6$$

Tato rovnice má řešení $x = 0 + 3t, z = 2 - 17t, t \in \mathbb{Z}$. Dosazením do první rovnice dostaneme rovnici $12t + 9y = -3$. V tuto chvíli nemůžeme hned vyjádřit neznámou y , protože bychom nedostali celočíselné řešení. Musíme na ni tedy nahlížet jako na diofantickou rovnici.

Tu můžeme nejdříve zkrátit na $4t + 3y = -1$.

Řešením bude $t = -1 + 3s, y = 1 - 4s, s \in \mathbb{Z}$.

Dosadíme $t = -1 + 3s$ do předchozích vyjádření a dostaneme řešení soustavy ve tvaru

$$\begin{aligned}x &= 0 + 3t = -3 + 9s, \\y &= 1 - 4s, \\z &= 2 + 17t = 2 + 17 - 51s = 19 - 51s.\end{aligned}$$

Příklad 2.6 Najděte všechna celočíselná řešení soustavy rovnic

$$x + 3y + 4z = 4$$

$$2x - y - 3z = -5.$$

Na této soustavě si ukážeme další způsob řešení soustav diofantických rovnic. Z první rovnice vyjádříme $x = 4 - 3y - 4z$ a dosadíme do druhé rovnice.

$$2 \cdot (4 - 3y - 4z) - y - 3z = -5$$

$$8 - 6y - 8z - y - 3z = -5$$

$$7y + 11z = 13$$

Dostali jsme jednu rovnici o dvou neznámých, kterou už umíme řešit. Některou z metod zjistíme, že řešení této rovnice je $y = -6 + 11k$, $z = 5 - 7k$, $k \in \mathbb{Z}$. Toto řešení dosadíme do vyjádření x z první rovnice.

$$x = 4 - 3y - 4z = 4 - 3(-6 + 11k) - 4(5 - 7k) = 2 - 5k$$

Získali jsme řešení

$$x = 2 - 5k,$$

$$y = -6 + 11k,$$

$$z = 5 - 7k,$$

kde $k \in \mathbb{Z}$.

Geometrickou interpretací této soustavy jsou dvě roviny, jejichž průsečíkem je přímka, jejíž parametrické vyjádření jsme získali jako řešení této soustavy. Přesněji řečeno by se o přímku jednalo v případě, že $k \in \mathbb{R}$. Protože hledáme pouze celočíselná řešení, jedná se o body ležící na této přímce.

Existují i další metody řešení soustav lineárních rovnic, na které pouze odkážeme. Dvě různé metody využívající matice uvádí Habala (2019b, s. 25-28) a Dlab (2016, s. 116).

Podobně bychom řešili soustavy rovnic o více neznámých. V některých případech by se lišil počet parametrů. Pokud máme o jednu neznámou více, než je počet rovnic, budeme potřebovat jeden parametr, s každou další neznámou (při stejném počtu rovnic) přibude také parametr.

Úlohy

2.10 Najděte všechna řešení soustavy diofantických rovnic

$$5x + 6y + 8z = 1$$

$$6x - 11y + 7z = 9$$

2.11 Na farmě je několik slepic, několik psů a několik bezhlavých trojnohých mimozemšťanů (tj. aspoň jeden od každého druhu). Dohromady mají 10 hlav a 43 nohou. Kolik mimozemšťanů je na farmě, když psů je nejvíce? (Rubeš, 2022)

2.12 Eratosthenes šel do Alexandrie a cestou na trhu koupil kohouty, slepice a malá kuřátka. Celkem nakoupil 100 kusů drůbeže za 100 denárů. Kolik koupil slepic, kohoutů a kuřat, jestliže kohout stál 5 denárů, slepice 3 denáry a 3 kuřátka stále 1 denár? (Rubeš, 2022)

Závěr

Cílem bakalářské práce bylo shrnout základní poznatky o lineárních diofantických rovnicích a kongruencích a vytvořit tak souvislý text věnující se těmto dvěma příbuzným tématům. Práce byla rozdělena do dvou částí, přičemž první z nich byla věnována kongruencím. Po krátkém historickém úvodu jsme si ukázali, co tento pojem znamená, a se seznámili z různými pohledy na relaci kongruence. Ukázali jsme si, kdy je užitečné s moduly počítat a jak toho můžeme využít například pro odvození kritérií dělitelnosti. Dále jsme se v první části věnovali lineárním kongruenčním rovnicím, a to především postupy při jejich řešení. Vyvrcholením první části práce byla Čínská věta o zbytcích a její využití v rozmanitých typech úloh.

Druhá část byla věnována lineárním diofantickým rovnicím. Po historickém okénku jsme se seznámili se základní teorií týkající se diofantických rovnic o dvou neznámých. Ukázali jsme si několik metod jejich řešení, přičemž se ukázalo, že velká část metod si je vzájemně podobných, jelikož se v nich v nějaké podobě vyskytuje Eukleidův algoritmus. Podívali jsme se na vztah lineárních diofantických rovnic a lineárních kongruencí a možnosti oboustranného využití tohoto vztahu. Poznatky získané z této části jsme rozšířili na rovnice o třech i více neznámých a soustavy diofantických rovnic, u kterých jsme si také uvedli metody jejich výpočtu. V této části se nachází také mnoho úloh, na kterých ilustrujeme možné využití diofantických rovnic v reálných situacích.

V závěru práce se nachází seznamy příkladů a úloh vyskytujících se v práci, které by mohly sloužit studentům a učitelům jako jakási malá sbírka úloh.

Na práci by se dalo navázat například zkoumáním kongruencí a diofantických rovnic vyšších řádů nebo exponenciálních diofantických rovnic. Zajímavé by bylo též zabývat se rozšířením Čínské věty o zbytcích na polynomy nebo grupy.

Seznam příkladů

Lineární kongruence

- 1.1 Najděte nejmenší přirozené číslo, se kterým je kongruentní číslo 14 modulo 6.
- 1.2 Vypočítejte $48^{111} + 2^{34} \pmod{7}$.
- 1.3 Jaký je zbytek po dělení třemi čísla 5 342 019?
- 1.4 Jaký je zbytek po dělení devíti čísla 5 342 019?
- 1.5 Jaký je zbytek po dělení jedenácti čísla 5 342 019?
- 1.6 Jaký je zbytek po dělení sedmi čísla 5 342 019?
- 1.7 Jaký je zbytek po dělení třinácti čísla 5 342 019?
- 1.8 Vypočítejte, kdy nastane Velikonoční neděle v roce 2042.
- 1.9 Vyřešte následující lineární kongruence:
- | | |
|---------------------------|---------------------------|
| a) $5x \equiv 3 \pmod{2}$ | d) $2x \equiv 2 \pmod{5}$ |
| b) $2x \equiv 3 \pmod{7}$ | e) $2x \equiv 2 \pmod{4}$ |
| c) $2x \equiv 3 \pmod{4}$ | |
- 1.10 Vyřešte následující lineární kongruence:
- | | |
|--|-----------------------------|
| a) $46x \equiv 127 \pmod{15}$ | d) $11x \equiv 8 \pmod{13}$ |
| b) $3x \equiv 6 \pmod{10}, 3x \equiv 6 \pmod{9}$ | e) $5x \equiv 3 \pmod{14}$ |
| c) $4x \equiv 1 \pmod{15}$ | |
- 1.11 Necht' x označuje určitý počet předmětů. Počítáme-li je po trojicích, zbydou dva, počítáme-li je po peticích, zbydou tři, a konečně počítáme-li je po sedmicích, zbydou dva. Kolik je x ?
- 1.12 Najděte všechna x splňující následující kongruence:
- $$x \equiv 4 \pmod{5}$$
- $$x \equiv 2 \pmod{7}$$
- $$x \equiv 10 \pmod{11}.$$
- 1.13 Řešte soustavu kongruencí
- $$x \equiv 2 \pmod{24}$$
- $$x \equiv 6 \pmod{20}$$
- $$x \equiv 8 \pmod{30}.$$

1.14 Řešte soustavu kongruencí

$$x \equiv 2 \pmod{24}$$

$$x \equiv 6 \pmod{20}$$

$$x \equiv 26 \pmod{30}.$$

1.15 Najděte všechna řešení kongruence $7x \equiv 11 \pmod{12}$.

1.16 Najděte všechna řešení kongruence $31x \equiv 53 \pmod{60}$.

1.17 Najděte všechna řešení kongruence $19x \equiv 23 \pmod{32}$.

1.18 Zjistěte poslední dvojčíslí čísla 49^{35}

1.19 Taneční kroužek měl tolik členů, že mohli nastupovat po třech nebo po čtyřech nebo po osmi. Kolik členů měl kroužek, víte-li, že to byl nejmenší možný počet?

1.20 Pokaždé, když se na táboře děti rozdělily do trojic, čtveřic nebo pětic, vždy jedno dítě zůstalo navíc. Kolik nejméně dětí mohlo být na táboře?

1.21 Všichni žáci školy se během představení na konci školního roku několikrát rozdělovali do skupin. Když vytvořili skupiny po třech, zbyl jeden žák, to stejné se stalo, když byli ve skupinách po čtyřech. Když se ale rozdělili do skupin po jedenácti, nikdo nezůstal navíc. Kolik žáků mohla mít škola, jestliže víme, že to bylo méně než 500?

Lineární diofantické rovnice

2.1 Najděte všechna řešení diofantické rovnice $43x + 15y = 110$.

2.2 Najděte všechna řešení diofantické rovnice $5x - 3y + 7z = 61$.

2.3 Najděte všechna celočíselná řešení rovnice $14x - 15y - 9z + 26u = 53$.

2.4 Najděte všechna celočíselná řešení soustavy rovnic

$$x + y + 2z = 7$$

$$4x + 5y = 11.$$

2.5 Najděte všechna celočíselná řešení soustavy rovnic

$$4x + 9y = -3,$$

$$7x + 3y + z = 1.$$

2.6 Najděte všechna celočíselná řešení soustavy rovnic

$$x + 3y + 4z = 4$$

$$2x - y - 3z = -5.$$

Řešení příkladů

U všech řešení $k \in \mathbb{Z}$.

1.1 2

1.2 1

1.3 0

1.4 6

1.5 1

1.6 4

1.7 7

1.8 6 . dubna.

1.9 a) $1 + 2k$, b) $5 + 7k$, c) nemá řešení,

d) $1 + 5k$, e) $1 + 2k$

1.10 a) $7 + 15k$, b) $2 + 10k$, $2 + 3k$,

c) $4 + 15k$, d) $9 + 13k$, e) $9 + 14k$

1.11 $23 + 105k$

1.12 $219 + 385k$

1.13 nemá řešení

1.14 $26 + 120k$

1.15 $5 + 12k$

1.16 $23 + 60k$

1.17 $13 + 32k$

1.18 49

1.19 24

1.20 61

1.21 $121, 253, 385$

2.1 $x = 5 - 15k, y = -7 + 43k$

2.2 $x = l, y = -18 + 7k - 3l, z = 1 + 3k - 2l$

2.3 $x = s, y = t, z = 16s + 7t + 26r - 3, u = 5s + 3t + 9r + 1$

2.4 $x = 4 + 10k, y = -1 + 8k, z = 2 + k$

2.5 $x = -3 + 9k, y = 1 - 4k, z = 19 - 51k$

2.6 $x = 2 - 5k, y = -6 + 11k, z = 5 - 7k$

Seznam úloh

Lineární kongruence

1.1 Určete, jaký zbytek dává číslo 5^{81} po dělení 26.

1.2 Určete poslední číslici čísla 77^{333} .

1.3 Určete paritu, poslední cifru a zbytek po dělení sedmi čísla

$$N = 22 \cdot 31 + 11 \cdot 17 + + 13 \cdot 19$$

1.4 Ověřte si, že vaše rodné číslo je dělitelné jedenácti.

1.5 Určete, jaký zbytek dostaneme, když číslo 4 294 967 297 vydělíme

a) třemi,

d) sedmi,

b) devíti,

e) třinácti.

c) jedenácti,

1.6 Odvoďte dělitelnost číslem 73.

1.7 Vypočítejte datum Velikonoční neděle v následujícím roce.

1.8 Najděte všechna řešení kongruencí

a) $4x \equiv 1 \pmod{7}$

d) $51x \equiv 4 \pmod{34}$

b) $7x \equiv 5 \pmod{4}$

e) $200x \equiv 240 \pmod{101}$

c) $8x \equiv 0 \pmod{12}$

f) $200x \equiv 240 \pmod{360}$

1.9 Najděte všechna řešení soustav kongruencí o jedné neznámé

a) $x \equiv 2 \pmod{3}$

c) $x \equiv 3 \pmod{20}$

$x \equiv 1 \pmod{7}$

$x \equiv 19 \pmod{28}$

$x \equiv 5 \pmod{8}$

$x \equiv 33 \pmod{35}$.

b) $3x \equiv 1 \pmod{5}$

$7x \equiv 5 \pmod{6}$

$8x \equiv 2 \pmod{11}$

1.10 Najděte všechna řešení kongruencí

a) $24x \equiv 7322 \pmod{38}$

b) $61x \equiv 6213 \pmod{77}$

c) $59x \equiv 157 \pmod{140}$.

1.11 Zjistěte poslední dvojčíslí čísla 49^{35} .

- 1.12 Pořadatelé průvodu, kterého se zúčastnilo méně než 1000 lidí, chtěli mít všechny řady plné. Ať seřadili účastníky do dvojstupů, trojstupů, čtyřstupů, pětistupů, šestistupů, sedmistupů, či osmistupů, nikdy nebyla poslední řada plná. Přihlížející matematik navrhl jednomu z pořadatelů, aby se postavil i on do průvodu. Potom byly všechny řady plné, ať se vytvořily dvojstupy, trojstupy, čtyřstupy, pětistupy, šestistupy, sedmistupy, či osmistupy. Kolik lidí bylo původně v průvodu?
- 1.13 Pastýř pásł ovce. Kolemjdoucí pocestný se ho zeptal, kolik jich má. Pastýř odpověděl: „Je jich méně než 500. Kdybych je postavil do dvojřadu, trojřadu, čtyřřadu, pětiřadu nebo šestiřadu, pokaždé by zůstala jedna ovce. Mohu je však seřadit přesně do sedmiřadu. Kolik měl pastýř ovcí?
- 1.14 Myslím si trojciferné číslo. Když od něho odečtu 7, bude výsledek dělitelný sedmi. Když od něho odečtu 8, bude výsledek dělitelný osmi. A když od něho odečtu 9, bude výsledek dělitelný devíti. Jaké číslo jsem si myslel?
- 1.15 Na hřišti cvičili žáci ze dvou tříd. Když se seřadili do trojstupů, zbyl jeden žák, když vytvořili čtyřstupy, zbyli dva, při pětistupech zbyli tři a šestistupech čtyři žáci. Kolik žáků bylo na hřišti?
- 1.16 Generál zjišťuje po bitvě počet přeživších vojáků tím, že je nechává srovnat se do řad o určitých délkách a počítá, kolik vojáků přebývá. Do bitvy šlo 1200 vojáků, když je po bitvě seřadil, tak při řazení po pěticích i po šesticích zbyli vždy 3 vojáci, po sedmicích přebýval 1 voják a při seřazení do řad po jedenácti nezůstal nikdo. Kolik vojáků bitvu přežilo?
- 1.17 Pro $m_1 = 7, m_2 = 9$ a $m_3 = 13$
- najděte sinoreprezentaci čísla 80,
 - určete číslo, které odpovídá trojici (1, 6, 2),
 - pomocí sinoreprezentace těchto čísel najděte jejich součet, rozdíl a součin.

Lineární diofantické rovnice

2.1 Najděte všechna řešení lineárních diofantických rovnic

a) $17x + 29y = 101$

c) $28x - 63y = 3227$

b) $76x - 19y = 51$

d) $37x + 57y = 8276$.

- 2.2 Určete rozměry všech rovnoramenných trojúhelníků s obvodem 15 cm, které mají celočíselné délky stran.
- 2.3 Máme nádoby o objemech 5 litrů a 7 litrů. Ve třetí nádobě potřebujeme získat 11 litrů. Jak budeme postupovat?
- 2.4 Správce tělocvičny dostal 12 000 Kč na nákup míčů. Menší míč stojí 320 Kč, větší míč stojí 360 Kč. Nemá určeno, kolik míčů má koupit, ale musí za ně utratit celou částku. Kolik kterých míčů může koupit?
- 2.5 V prodejně suvenýrů prodávají dva druhy trpaslíků. První druh stojí 330 Kč, druhý druh stojí 450 Kč. Přijel autobus turistů, kteří nakoupili trpaslíky za 5 670 Kč. Kolik kterých trpaslíků koupili?
- 2.6 V zahradnictví prodávají sazenice rybízu a angreštu. Jedna sazenice rybízu stojí 99 Kč, jedna sazenice angreštu stojí 126 Kč.
- Koupili jsme nějaký počet sazenic rybízu a angreštu. Mohl nákup stát přesně 2000 Kč?
 - Kolik jsme koupili kterých sazenic, když nám prodavač vrátil po platbě dvoutisícovou bankovkou méně než 10 Kč?
- 2.7 Najděte všechna řešení následujících lineárních diofantických rovnic
- $17x + 28y + 3z = 421$
 - $36x + 52y + 32z = 1072$.
- 2.8 V obchodě prodávají trička po 230 Kč, pár ponožek za 40 Kč a košile po 350 Kč. Za nákup jsme zaplatili 1250 Kč. Od každého druhu výrobku jsme koupili minimálně jeden kus. Kolik kterého oblečení jsme mohli koupit?
- 2.9 Najděte všechna řešení lineární diofantické rovnice $26x + 31y + 11z + 53w = 256$.
- 2.10 Najděte všechna řešení soustavy diofantických rovnic
- $$\begin{aligned} 5x + 6y + 8z &= 1 \\ 6x - 11y + 7z &= 9 \end{aligned}$$
- 2.11 Na farmě je několik slepic, několik psů a několik bezhlavých trojnohých mimozemšťanů (tj. aspoň jeden od každého druhu). Dohromady mají 10 hlav a 43 nohou. Kolik mimozemšťanů je na farmě, když psů je nejvíce?

2.12 Eratosthenes šel do Alexandrie a cestou na trhu koupil kohouty, slepice a malá kuřátka. Celkem nakoupil 100 kusů drůbeže za 100 denárů. Kolik koupil slepic, kohoutů a kuřat, jestliže kohout stál 5 denárů, slepice 3 denáry a 3 kuřátka stále 1 denár?

Řešení úloh

U všech řešení $k, l, m \in \mathbb{Z}$.

1.1 5

1.2 7

1.3 Parita: číslo je sudé, poslední cifra: 6, zbytek po dělení sedmi: 3.

1.4 -

1.5 a) 2, b) 5, c) 5, d) 5, e) 10

1.6 Střídavě přičítáme a odčítáme čtyřčíslí.

1.7 2023: 9. dubna, 2024: 31. března, 2025: 20. dubna, 2026: 5. dubna, 2027: 28. března, ...

1.8 a) $2 + 7k$, b) $3 + 4k$, c) $3k$, d) nemá řešení, e) $82 + 101k$, f) $3 + 9k$

1.9 a) $29 + 168k$, b) $47 + 330k$, c) $103 + 140k$

1.10 a) $9 + 19k$, b) $40 + 77k$, c) $43 + 140k$

1.11 76

1.12 839

1.13 427

1.14 504

1.15 58

1.16 1023

1.17 a) (3, 8, 2), b) 15, c) (4, 5, 4); (2, 2, 0); (3, 3, 4)

2.1 a) $x = -6 - 29k, y = 7 + 17k$,

b) nemá řešení, c) $x = 5 + 9k$,

$y = -49 + 4k$, d) $x = 8 + 57k$,

$y = -37 + 140k$

2.2 [4, 4, 7], [5, 5, 5], [6, 6, 3], [7, 7, 1]

2.3 $5x + 7y = 11, x = -2 + 7k$,

$y = 3 - 5k$, například třikrát

nalejeme 7litrovou nádobu a poté

odebereme dvakrát 5litrovou nádobu

2.4 $24 + 12, 15 + 20$ nebo $6 + 28$

(malých + velkých)

2.5 9 ks po 330 Kč a 6 ks po 450 Kč

2.6 a) ne, b) 10 sazenic rybízu, 8 angreštu

2.7 a) $x = k, y = 1 + k + 3l, z = 131 -$

$-15k = 28l$, b) $x = 4 + 8k -$

$-5l, y = l, z = 29 - 9k + 4l$

2.8 2 trička, 11 párů ponožek a 1 košili

nebo 1 tričko, 8 párů ponožek a 2

košile

2.9 $x = k, y = 4 + 2k + 10l + 11m$,

$z = 12 - 8k - 33l - 31m, w = l$

2.10 $x = 5 + 10k, y = k, z = -3 - 7k$

2.11 3

2.12 4 kohouty, 18 slepic a 78 kuřat

nebo 12 kohoutů, 4 slepice a 84

kuřat

Seznam použitých informačních zdrojů

BĚLOUN, František, 2010. *Sbírka úloh z matematiky pro základní školy*. 8. vydání. Praha: Prometheus. ISBN 80-7196-104-3.

BOGOMOLNY, Alexander, c1996-2018. Chinese Remainder Theorem. In: *Cut The Knot* [online]. [cit. 2022-07-06]. Dostupné z: <https://www.cut-the-knot.org/blue/chinese.shtml>

ČERMÁK, Filip a Matěj DOLEŽÁLEK, 2020. Teorie nejen čísel 1 – Součiny. In: *Matematický korespondenční seminář* [online]. Praha [cit. 2022-07-06]. Dostupné z: <https://prase.cz/archive/40/uvod1s.pdf>

ČESENĚK, Jaroslav, 1994. *Sbírka úloh z matematiky pro 6. ročník základní školy*. 3. vydání. Praha: Prometheus. ISBN 80-85849-11-9.

DLAB, Vlastimil a Jindřich BEČVÁŘ, 2016. *Od aritmetiky k abstraktní algebře*. Praha. ISBN 976-80-260-9838-6.

GAUSS, Carl Friedrich, 1800. Berechnung des Osterfestes. In: *Monatliche Correspondenz zur Beförderung der Erd- und Himmels-Kunde, herausgeben vom Freiherrn von Zach*. s. 121–130.

GAUSS, Carl, 1986. *Disquisitiones Arithmeticae*. 1. New York: Springer. ISBN 978-0-387-96254-2. Dostupné z: doi:<https://doi.org/10.1007/978-1-4939-7560-0>

HABALA, Petr, 2019a. Diskrétní matematika: 3. Počítání modulo. In: *ČVUT - Fakulta elektrotechnická, Katedra matematiky* [online]. Praha [cit. 2022-07-22]. Dostupné z: <https://math.fel.cvut.cz/cz/lide/habala/teaching/dma/dmkni03.pdf>

HABALA, Petr, 2019b. Diskrétní matematika: 4. Rovnice a celá čísla. In: *ČVUT - Fakulta elektrotechnická, Katedra matematiky* [online]. Praha [cit. 2022-06-13]. Dostupné z: <https://math.fel.cvut.cz/cz/lide/habala/teaching/dma/dmkni04.pdf>

HABALA, Petr, 2019c. Diskrétní matematika: 2. Dělitelnost. In: *ČVUT - Fakulta elektrotechnická, Katedra matematiky* [online]. Praha [cit. 2022-07-06]. Dostupné z: <https://math.fel.cvut.cz/cz/lide/habala/teaching/dma/dmkni02.pdf>

HAVEL, Ivan, 1973. O desátém Hilbertově problému. *Pokroky matematiky, fyziky a astronomie*. Praha: Jednota českých matematiků a fyziků, **18**(4), 185-192.

- Chinese Remainder Theorem, 2022. In: *Brilliant* [online]. [cit. 2022-07-10]. Dostupné z: <https://brilliant.org/wiki/chinese-remainder-theorem/>
- KATZ, Victor, 2009. *A History of Mathematics: An Introduction*. 3rd ed. Boston: Addison-Wesley. ISBN 0-321-38700-7.
- KŘÍŽEK, Michal, Lawrence SOMER a Alena ŠOLCOVÁ, 2018. *Kouzlo čísel: od velkých objevů k aplikacím*. Vydání 3. Praha: Academia. Galileo. ISBN 978-80-200-2840-2.
- NIVEN, Ivan, Herbert ZUCKERMAN a Hugh MONTGOMERY, 1991. *An Introduction to the Theory of Numbers*. 5th edition. Hoboken: Wiley. ISBN 0-471-62546-9.
- NOVOTNÝ, Vladimír, 2016. Velikonoce a Carl Friedrich Gauss. *Pokroky matematiky, fyziky a astronomie*. Praha: Jednota českých matematiků a fyziků, **61**(1), 39-51. Dostupné také z: <http://dml.cz/dmlcz/144900>
- RADCLIFFE, Mary, 2019. *Chinese Remainder Theorem* [online]. In: . [cit. 2022-07-06]. Dostupné z: <https://www.math.cmu.edu/~mradclif/teaching/127S19/Notes/ChineseRemainderTheorem.pdf>
- RUBEŠ, Zdeněk, 2022. Diofantické úlohy. In: *Slovní úlohy* [online]. [cit. 2022-07-10]. Dostupné z: <http://su.rubesz.cz/smes/diofanticke-ulohy/>
- SLAVÍK, Antonín, 2018. Méně známá kritéria dělitelnosti. In: *Rozvíjení matematické gramotnosti na středních školách II*. Praha: MatfyzPress, s. 93-102. ISBN 978-80-7378-407-2.
- STANOVSKÝ, David, 2010. *Základy algebry*. 1. vydání. Praha: MatfyzPress. ISBN 978-80-7378-105-7.
- STANOVSKÝ, David, 2022. *Algebra* [online]. [cit. 2022-07-06]. Dostupné z: <https://www2.karlin.mff.cuni.cz/~stanovsk/vyuka/algebra22.pdf>
- STEINSDÖRFER, Jan, 2015. *Metody řešení diofantických rovnic* [online]. Ústí nad Labem [cit. 2022-07-06]. Dostupné z: http://physics.ujep.cz/~jmaly/mo/Diofanticke_rovnice.pdf. Studijní text. Univerzita Jana Evangelisty Purkyně v Ústí nad Labem, Přírodovědecká fakulta.

STILLWELL, John, 2003. *Elements of Number Theory*. 1. New York: Springer. ISBN 978-1-4419-3066-8.

TREJBAL, Josef, 1995. *Sbírka úloh z matematiky pro 7. ročník základní školy*. 3. vydání. Praha: Prometheus. ISBN 80-7196-036-5.