MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

DIPLOMOVÁ PRÁCE

Jan Hamáček

Kombinatorické úlohy o mincích

Katedra didaktiky matematiky

Vedoucí diplomové práce:	doc. RNDr. Antonín Slavík, Ph.D.
Studijní program:	Matematika
Studijní obor:	MIUSSS

Praha 2016

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V Praze dne 26. 7. 2016 Podpis autora

Název práce: Kombinatorické úlohy o mincích

Autor: Jan Hamáček

Katedra: Katedra didaktiky matematiky

Vedoucí diplomové práce: doc. RNDr. Antonín Slavík, Ph.D., Katedra didaktiky matematiky

Abstrakt: Práce se zabývá otázkami reprezentace zvolené částky pomocí libovolného množství mincí předepsaného typu. V první kapitole odvozujeme vzorce pro počet nereprezentovatelných částek a hodnotu největší nereprezentovatelné částky pro dvoumincové systémy. Dále ukazujeme grafový algoritmus pro výpočet Frobeniova čísla a důkaz NP-úplnosti rozhodovacího problému reprezentovatelnosti zvolené částky v systému s více mincemi. V druhé kapitole se zabýváme výpočtem počtu reprezentací částky zvlášť v systémech o dvou nebo více mincích. Ve třetí kapitole se věnujeme otázce, zda lze ve zvoleném systému mincí použít hladový algoritmus pro nalezení reprezentace částky pomocí nejmenšího možného množství mincí. Poslední kapitola obsahuje sbírku řešených logických úloh o mincích.

Klíčová slova: reprezentovatelnost, počet reprezentací, systémy mincí, Frobeniovo číslo, hladový algoritmus, minimální reprezentace, úlohy o mincích

Title: Combinatorial problems with coins

Author: Jan Hamáček

Department: Department of Mathematics Education

Supervisor: doc. RNDr. Antonín Slavík, Ph.D., Department of Mathematics Education

Abstract: The thesis deals with various problems involving representations of a certain amount of money using coins of prescribed type. In the first chapter, we derive formulas for the number of nonrepresentable amounts, as well as the greatest nonrepresentable amount for systems of coins with two denominations. Next, we present a graph algorithm for calculating the Frobenius number, and prove NP-completeness of the question whether a certain amount is representable in systems with multiple denominations. In the second chapter, we compute the number of representations of a given amount in systems with two or more denominations. The third chapter is devoted to the question whether the greedy algorithm can be used for a given coin system to obtain the minimal representation of any value. The last chapter contains a collection of solved combinatorial problems with coins.

Keywords: representability, representation count, coin system, Frobenius number, greedy algorithm, minimal representation, problems with coins

Rád bych poděkoval doc. RNDr. Antonínu Slavíkovi, Ph.D. za cenné připomínky a rady při vypracování této práce.

Obsah

Úvod

První tři kapitoly práce se zabývají otázkami souvisejícími s hledáním způsobů, jak rozměnit (reprezentovat) částku pomocí libovolného množství mincí s předepsanými hodnotami. Poslední kapitola představuje sbírku dalších (většinou logických) řešených úloh týkajících se mincí. Jednotlivé kapitoly na sobě nezávisí a je možné je číst odděleně. Práce je především matematická, ale obsahuje i části zajímavé z pohledu informatiky.

Práce je určena zejména pro středoškolské a vysokoškolské studenty a pedagogy, organizátory různých seminářů či přednášek pro středoškoláky a všechny, kteří si chtějí rozšířit matematické znalosti. Některé části práce používají výhradně středoškolskou matematiku. V ostatních částech předpokládáme některé znalosti zhruba na úrovni bakalářského studia matematiky nebo informatiky na MFF UK, snažíme se však, aby byl text přístupný co nejširšímu okruhu čtenářů.

První kapitola se zabývá zjišťováním počtu částek, které nelze reprezentovat pomocí mincí o zadaných hodnotách a hledáním největší takové částky. Dále v první kapitole popisujeme hru pro dva hráče, která souvisí s hledáním nereprezentovatelných částek. Dokazujeme, že problém reprezentovatelnosti libovolné částky je NP-úplný, a tedy není znám efektivní algoritmus pro jeho řešení. Většina první kapitoly využívá pouze středoškolskou látku. V částech o počtu nereprezentovatelných částek a největší nereprezentovatelné částce pro dvoumincové systémy si vystačíme se základními matematickými poznatky, trochou geometrie a s dělitelností. V části o největší nereprezentovatelné částce pro vícemincové systémy přibude použití grafů. Popis hry v poslední části kapitoly i důkaz existence vyhrávající strategie opět vystačí se středoškolskými znalostmi. K důkazu složitosti rozhodnutí o reprezentovatelnosti částky využíváme znalosti o třídě NP-úplných problémů a o polynomiální převoditelnosti problémů.

Druhá kapitola je věnována hledání počtu reprezentací částky. V první části odvozujeme pomocí vytvořujících funkcí vzorec pro dvoumincové systémy. Systémům s více mincemi je věnována druhá část kapitoly, ve které pomocí principu inkluze a exkluze dokazujeme rekurentní vzorec pro počet reprezentací libovolné částky.

Třetí kapitola je věnována otázce, jak složit zadanou částku a spotřebovat přitom co nejmenší počet mincí. Popisujeme v ní hladový algoritmus, který je součástí výuky informatiky na některých technicky zaměřených středních školách a gymnáziích. Dále ukazujeme postup, pomocí kterého zjistíme, jestli v daném systému mincí můžeme využít hladový algoritmus k rozměnění částky pomocí co nejméně mincí. K pochopení důkazů i vět v této části by měl mít středoškolák dostatek matematických vědomostí, ale důkazy samotné jsou logicky poměrně komplikované.

Čtvrtá kapitola využívá výhradně středoškolské znalosti. Obsahuje různé řešené logické úlohy o mincích. Její přečtení doporučujeme zejména středoškolským učitelům, organizátorům korespondenčních seminářů a dalších akcí pro talentované středoškoláky se zájmem o matematiku. Jednotlivé úlohy na sobě z větší části nezávisí a můžeme je proto využít například jako zpestření výuky.

1. Reprezentovatelnost

V první kapitole se budeme zabývat otázkami podobnými následující.

Otázka. *Máme neomezené množství mincí o hodnotách 10, 16 a 34. Které částky můžeme z těchto mincí poskládat?*

Budeme se samozřejmě snažit najít řešení otázky v obecnějším tvaru. Hledáme odpověď i při obecných hodnotách mincí $x_1, x_2, \ldots, x_n$.

Definice 1.1. *Reprezentace částky a v systému mincí o hodnotách* $x_1, x_2, \ldots, x_n$ *je n-tice* $(b_1, b_2, \ldots b_n)$ *taková, že* $b_1, b_2, \ldots, b_n$ *jsou nezáporná celá čísla a*

$$b_1x_1 + b_2x_2 + \cdots + b_nx_n = a.$$

Reprezentací částky a jsou tedy počty vybraných mincí, jejichž celková hodnota je a.

Definice 1.2. *Řekneme, že částka a je reprezentovatelná v systému mincí o hodnotách* $x_1, x_2, \ldots, x_n$*, pokud v daném systému existuje alespoň jedna její reprezentace.*

Hledáme tedy všechny částky, které jsou reprezentovatelné pomocí mincí o hodnotách $x_1, x_2, \ldots, x_n$.

Poznámka. *Symbolem* $\mathbb{N}_0$ *v dalším textu označujeme množinu všech nezáporných celých čísel.*

1.1 Systémy soudělných mincí

Podívejme se nejprve na mince o hodnotách 10, 16 a 34. Selským rozumem dojdeme k závěru, že existuje nekonečně mnoho částek, které pomocí těchto mincí nemůžeme složit. Například žádnou lichou částku jistě nesložíme pomocí mincí o sudých hodnotách.

Obecněji můžeme říct, že v systému mincí o hodnotách $x_1, x_2, \ldots, x_n$ jejichž největší společný dělitel d je větší než 1 platí, že existuje nekonečně mnoho nereprezentovatelných částek. Tuto myšlenku můžeme shrnout následující větou.

Věta 1.3. *Každá částka reprezentovatelná pomocí systému mincí* $x_1, x_2, \ldots, x_n$ *je násobkem* $d = NSD(x_1, x_2, \ldots, x_n)$.

Důkaz. Pro libovolnou částku a, reprezentovatelnou pomocí $x_1, x_2, \ldots, x_n$, platí:

$$a = b_1x_1 + b_2x_2 + \cdots + b_nx_n$$

Největším společným dělitelem systému mincí je d. Proto můžeme z každého $x_1, \ldots, x_n$ vytknout d:

$$a = d \cdot (b_1y_1 + b_2y_2 + \cdots + b_ny_n)$$

Proto je a násobkem d. □

V našem systému mincí o hodnotách 10, 16 a 34 je největším společným dělitelem 2. Každá reprezentovatelná částka je proto násobkem dvou. Opačná implikace neplatí, neboť například číslo 12 je násobkem dvou, ale v našem systému mincí není reprezentovatelné.

Náš systém mincí bychom mohli vydělit jejich největším společným dělitelem. Dostali bychom tím systém mincí 5, 8 a 17. Čísla nedosažitelná kvůli větě 1.3 už v novém systému mincí nejsou.

Každé nedosažitelné číslo v novém systému mincí má svůj ekvivalent v původním systému mincí. Je jím jeho d-násobek.

Věta 1.4. *Mějme systém mincí o hodnotách $x_1, x_2, \ldots, x_n$ takový, že*

$$NSD(x_1, x_2, \ldots, x_n) = d > 1$$

a systém mincí o hodnotách $y_1, y_2, \ldots, y_n$ tak, že

$$y_i = \frac{x_i}{d}, \quad i \in \{1, 2, \ldots, n\}.$$

Potom a je reprezentovatelné v druhém systému mincí právě tehdy, když $d \cdot a$ je reprezentovatelné v prvním systému mincí.

Důkaz. Ze vztahu reprezentace $d \cdot a$ v prvním systému mincí vytkneme d. Tím dostaneme vztah reprezentace a v druhém systému mincí. □

Díky větě 1.4 nyní můžeme použít systém mincí o hodnotách 5, 8 a 17 ke zkoumání původního systému mincí 10, 16 a 34.

Zkoušením všech možností zjistíme, že pomocí mincí o hodnotách 5, 8 a 17 nejdou reprezentovat částky

$$1, 2, 3, 4, 6, 7, 9, 11, 12, 13, 14, 19$$

Všechny ostatní částky reprezentovat jdou. Platí totiž

$$\begin{aligned} 20 &= 4 \cdot 5 \\ 21 &= 5 + 2 \cdot 8 \\ 22 &= 5 + 17 \\ 23 &= 3 \cdot 5 + 8 \\ 24 &= 3 \cdot 8 \end{aligned}$$

a všechny další částky můžeme reprezentovat například přidáním vhodného množství mincí o hodnotě 5.

Podle věty 1.4 tedy víme, že v původním systému mincí nejsou reprezentovatelné částky

$$2, 4, 6, 8, 12, 14, 18, 22, 24, 26, 28, 38.$$

Podle věty 1.3 navíc nejsou reprezentovatelné žádné liché částky. Všechny ostatní částky reprezentovatelné jsou.

Při zkoumání reprezentovatelnosti částek v systému mincí se díky větám 1.3 a 1.4 můžeme omezit na systémy mincí s největším společným dělitelem rovným 1.

1.2 Počet nereprezentovatelných částek

Otázka, kterou jsme si položili v úvodu, je poměrně obtížná. Zkusme si pro začátek položit raději jinou otázku. Kolik je hodnot, které neumíme reprezentovat pomocí mincí o hodnotách $x_1, x_2, \ldots, x_n$?

1.2.1 Sylvesterův problém pro dvě mince

Problémy reprezentovatelnosti částek pomocí mincí dvou hodnot popisované v této kapitole zkoumal britský matematik James Joseph Sylvester. K popisu problému použil známky dvou hodnot namísto mincí dvou hodnot. V literatuře proto můžeme problémy popsané v této kapitole nalézt pod názvem „The Stamp Problem“[20]. V následujícím textu vycházíme z [18, kapitola 6].

Už víme, že pro systém mincí s hodnotami $x_1, x_2, \ldots, x_n$ s největším společným dělitelem $d > 1$ existuje nekonečně mnoho nereprezentovatelných částek. Říká to věta 1.3. Kolik jich je, pokud největší společný dělitel je roven 1?

Vyřešíme tuto otázku nejprve pro systémy mincí o dvou hodnotách.

Otázka. *Máme neomezené množství mincí o hodnotách a a b, přičemž čísla a, b jsou nesoudělná. Kolik různých částek menších než ab nedokážeme pomocí těchto mincí reprezentovat?*

Obecnější verze této otázky by neobsahovala omezení na částky menší než ab. Později si ukážeme, že všechny částky větší nebo rovny ab jsou v systému mincí a, b reprezentovatelné. Nejprve ale vyřešíme původní otázku.

Pro konkrétní hodnoty $a = 5$ a $b = 9$ si vytvoříme tabulku všech reprezentovatelných částek menších než ab. Hodnotou v u-tém řádku a v-tém sloupci bude $u \cdot b + v \cdot a$.

u \ v	0	1	2	3	4	5	6	7	8	9
0	0	5	10	15	20	25	30	35	40	45
1	9	14	19	24	29	34	39	44	49	54
2	18	23	28	33	38	43	48	53	58	63
3	27	32	37	42	47	52	57	62	67	72
4	36	41	46	51	56	61	66	71	76	81
5	45	50	55	60	65	70	75	80	85	90

Tabulka 1.1: Reprezentovatelné částky pro hodnoty $a = 5$, $b = 9$

V tabulce 1.1 jsou všechny reprezentovatelné částky do $5 \cdot 9 = 45$. Kromě nich jsou v tabulce ještě další. Každá částka menší než 45, která v tabulce chybí, není reprezentovatelná pomocí mincí o hodnotách 5 a 9.

Podobnou tabulku můžeme vytvořit pro libovolnou dvojici čísel a a b. To popisuje následující definice.

Definice 1.5. *Mějme nesoudělná $a, b \in \mathbb{N}$. Uvažujme matici o $a + 1$ řádcích a $b + 1$ sloupcích, kde pro $u, v \in \mathbb{N}_0$, $u \leq a$, $v \leq b$ je hodnota prvku matice na u-tém řádku a v-tém sloupci rovna*

$$u \cdot b + v \cdot a.$$

Tuto matici budeme označovat $A_{a,b}$.
Hodnotu $A_{a,b}$ v u-tém řádku a v-tém sloupci budeme značit $A_{a,b}(u,v)$.

Tabulka 1.1 podle této definice odpovídá matici $A_{5,9}$.

Počet všech nereprezentovatelných částek menších než ab můžeme spočítat pomocí počtu všech reprezentovatelných. Platí totiž rovnost

$$\begin{pmatrix} \text{počet} \\ \text{reprezentovatelných} \end{pmatrix} + \begin{pmatrix} \text{počet} \\ \text{nereprezentovatelných} \end{pmatrix} = \begin{pmatrix} \text{počet} \\ \text{všech} \end{pmatrix}. \qquad (1.1)$$

Zbývá zjistit, kolik je v tabulce (matici $A_{a,b}$) různých reprezentovatelných částek menších než ab.

Tabulka 1.1 obsahuje tři části. V levé horní části jsou hodnoty menší než $ab = 45$. V pravé dolní části jsou hodnoty větší než 45. Ve zbylých dvou rozích jsou potom právě dvě hodnoty 45. Navíc platí, že hodnot menších než 45 je v tabulce stejný počet jako hodnot větších než 45.

Ověříme, že uvedená tvrzení platí nejen pro hodnoty $a = 5$ a $b = 9$, ale i v obecném případě.

Z následující věty plyne, že v matici $A_{a,b}$ je částek menších než ab stejně jako částek větších než ab.

Věta 1.6. *Nechť $a, b \in \mathbb{N}$ jsou větší než 1.*
Potom pro $u, v \in \mathbb{N}_0$, $u \leq a$, $v \leq b$ platí

$$A_{a,b}(u,v) + A_{a,b}(a-u, b-v) = 2ab.$$

Důkaz. Dosadíme hodnoty matice:

$$A_{a,b}(u,v) + A_{a,b}(a-u, b-v) = ub + va + (a-u)b + (b-v)a = 2ab$$

□

Dále potřebujeme dokázat, že v matici jsou právě dvě hodnoty ab.

Věta 1.7. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná, pak jsou v matici $A_{a,b}$ právě dvě hodnoty ab.*

Důkaz. Na pozici (u, v), kde $u, v \in \mathbb{N}_0$, $u \leq a$, $v \leq b$ je hodnota ab, právě tehdy když platí:

$$ab = ua + vb$$

Úpravami tohoto výrazu získáme

$$au = b(a-v).$$

Proto b dělí au. Navíc víme, že a je nesoudělné s b. Proto platí, že b dělí u. Z předpokladů ale plyne, že $u \leq b$.

Pro u proto připadají v úvahu pouze možnosti možnosti $u = 0$ a $u = b$. Těmto možnostem odpovídají hodnoty $v = a$ a $v = 0$. □

Abychom mohli pomocí vzorce (1.1) zjistit počet nereprezentovatelných částek, musíme ještě ověřit, že v matici $A_{a,b}$ se žádná hodnota kromě ab nevyskytuje více než jednou.

Věta 1.8. *Jsou-li čísla $a, b \in \mathbb{N}$ nesoudělná, pak se v matici $A_{a,b}$ žádná hodnota kromě ab nevyskytuje více než jednou.*

Důkaz. Aby se hodnota x vyskytovala v matici $A_{a,b}$ více než jednou, musí se vyskytovat v řádku u_1 a sloupci v_1 a zároveň v řádku u_2 a sloupci v_2. Musí tedy existovat $u_1, u_2, v_1, v_2 \in \mathbb{N}_0$ tak, že platí $u_1, u_2 \leq a$, $v_1, v_2 \leq b$ a x můžeme vyjádřit dvěma způsoby

$$x = u_1 b + v_1 a,$$

$$x = u_2 b + v_2 a.$$

Bez újmy na obecnosti předpokládejme, že $u_2 < u_1$. Musí proto platit $v_2 > v_1$.

Úpravami dostaneme

$$b \cdot (u_1 - u_2) = a \cdot (v_2 - v_1). \tag{1.2}$$

Odtud plyne, že a dělí $b \cdot (u_1 - u_2)$. Hodnoty a a b jsou nesoudělné. Platí proto, že a dělí $u_1 - u_2$. To můžeme interpretovat tak, že čísla řádků u_1, u_2 dvou stejných hodnot se musí lišit o násobek a.

Stejným způsobem z rovnice (1.2) plyne, že b dělí $a \cdot (v_2 - v_1)$, tedy b dělí $v_2 - v_1$. Čísla sloupců v_1, v_2 dvou stejných hodnot se proto musí lišit o násobek b.

V matici $A_{a,b}$ jsou takové hodnoty pouze čtyři v rozích matice. Rozborem případů zjistíme, že jediné stejné hodnoty v matici jsou

1. hodnota ab v a-tém řádku a nultém sloupci,

2. hodnota ab v nultém řádku a b-tém sloupci.

□

Nyní můžeme využít vzorec (1.1) k výpočtu počtu všech nereprezentovatelných částek menších než ab.

Věta 1.9. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná, pak počet všech nereprezentovatelných částek menších než ab je*

$$\frac{(a-1)(b-1)}{2}.$$

Důkaz. V tabulce $A_{a,b}$ je celkem $(a+1)(b+1)$ hodnot. Dvě z nich jsou podle předchozí věty rovny ab. Polovina ze zbylých hodnot je podle věty 1.6 menší než ab. Tyto hodnoty jsou navíc podle věty 1.8 různé.

Počet všech různých reprezentovatelných částek menších než ab je

$$\frac{(a+1)(b+1)-2}{2} = \frac{ab+a+b-1}{2}.$$

Počet všech nereprezentovatelných částek menších než ab je proto podle rovnice (1.1)

$$ab - \frac{ab+a+b-1}{2} = \frac{(a-1)(b-1)}{2}.$$

□

S počtem nereprezentovatelných částek menších než ab se prozatím spokojíme. K závěru s tímto omezením dospěl i Sylvester [18, str. 172]. V částech 1.2.2 a 1.3.1 ukážeme dvěma různými způsoby, že všechny částky větší než ab jsou reprezentovatelné.

1.2.2 Geometrické odvození

Tato část obsahuje jiný způsob odvození vzorce pro získání počtu nereprezentovatelných částek v systémech mincí o dvou nesoudělných hodnotách $a, b \in \mathbb{N}$. Naším cílem je znovu dokázat větu 1.9, tentokrát bez omezení na částky menší než ab. Čerpáme přitom z [11, kap. 13].

Počet reprezentací částky n v systému mincí o hodnotách a, b je podle definice 1.1 roven počtu dvojic $x, y \in \mathbb{N}_0$ takových, že

$$n = xa + yb.$$

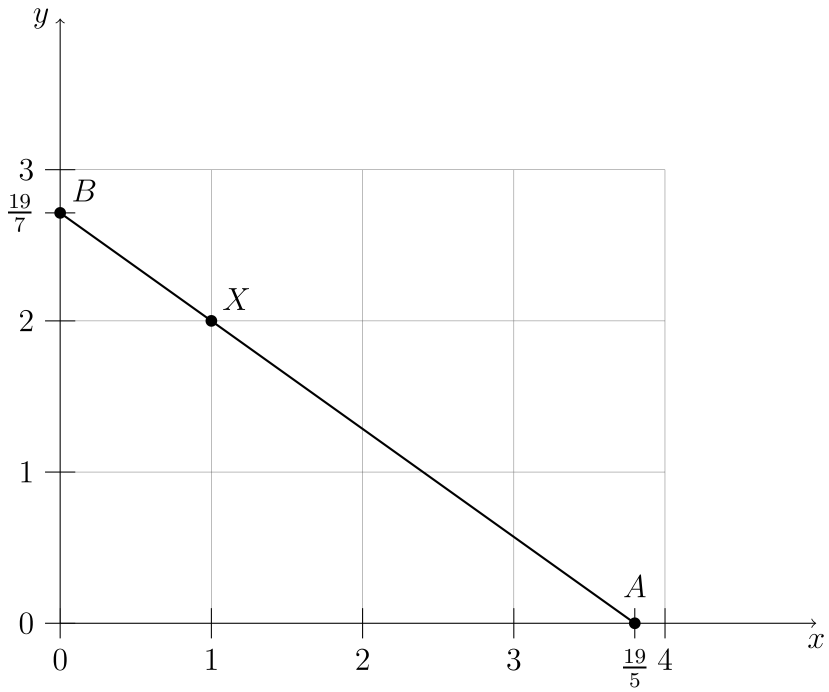
Jednoduchými úpravami získáme ekvivalentní vyjádření

$$y = \frac{-a}{b}x + \frac{n}{b},$$

což je rovnice přímky protínající osy v bodech $A = [n/a, 0]$ a $B = [0, n/b]$.

Částka n je proto v systému mincí reprezentovatelná právě tehdy, když na úsečce AB leží alespoň jeden bod s celočíselnými souřadnicemi $[x, y]$.

Na obrázku 1.1 je příklad reprezentovatelné čásky 19 v systému mincí s $a = 5$ a $b = 7$. Na úsečce AB leží jediný bod X s celočíselnými souřadnicemi $[1, 2]$, neboť částku 19 lze reprezentovat jedině pomocí jedné mince o hodnotě 5 a dvou mincí o hodnotě 7.



Obrázek 1.1: Příklad reprezentovatelné částky 19 v systému mincí $a = 5$, $b = 7$

Lemma 1.10. *Leží-li bod $X = [x, y]$ s celočíselnými souřadnicemi na přímce*

$$p : n = xa + yb,$$

pak na stejné přímce leží i body $Y_1 = [x+b, y-a]$ a $Y_2 = [x-b, y+a]$. Mezi body X a Y_1 ani mezi body X a Y_2 na přímce navíc neleží žádný další bod s celočíselnými souřadnicemi.

Důkaz. Bod Y_1 leží na přímce p, protože

$$a(x+b)+b(y-a)=ax+ab+by-ba=ax+by=n.$$

Podobně bod Y_2 leží na přímce p, protože

$$a(x-b)+b(y+a)=ax+by=n.$$

Volme pro spor bod $Q=[x+u,y-v]$ s celočíselnými souřadnicemi, ležící na přímce mezi body X a Y_1. Konstanty u,v proto musí splňovat $u,v\in\mathbb{N}$, $1\leq u<b$ a $1\leq v<a$. Platí

$$a(x+u)+b(y-v)=ax+by+au-bv=n.$$

Dalšími úpravami získané rovnice získáme

$$\begin{aligned} n+au-bv&=n\\ au&=bv\\ \frac{a}{b}&=\frac{v}{u}. \end{aligned}$$

Zlomek $\frac{a}{b}$ je v základním tvaru, protože a a b jsou nesoudělná. Všechny zlomky, vyjadřující stejné racionální číslo jsou proto ve tvaru $\frac{ma}{mb}$, kde $m\in\mathbb{Z},m\neq 0$. Zlomek $\frac{v}{u}$ v tomto tvaru není, neboť $1\leq v<a$ a $1\leq u<b$.

Stejným způsobem bychom mohli dokázat, že mezi body X a Y_2 na přímce neleží bod $Q'=[x-u,y+v]$, kde opět $u,v\in\mathbb{N}$, $1\leq u<b$ a $1\leq v<a$. □

Víme-li, že na přímce p z lemmatu 1.10 leží alespoň jeden bod s celočíselnými souřadnicemi, pak opakovaným použitím lemmatu získáváme nekonečně mnoho bodů s celočíselnými souřadnicemi.

Věta 1.11. *Volme nesoudělná $a,b\in\mathbb{N}$ a $n\in\mathbb{N}_0$. Na přímce*

$$p:n=xa+yb$$

leží nekonečně mnoho bodů s celočíselnými souřadnicemi. Vzdálenost každých dvou sousedních bodů s celočíselnými souřadnicemi na přímce p je rovna

$$s=\sqrt{a^2+b^2}.$$

Důkaz. Nejprve dokážeme, že na přímce p leží nějaký bod s celočíselnými souřadnicemi. Z Bézoutovy rovnosti [23, věta 3.3] a nesoudělnosti a,b plyne existence $x',y'\in\mathbb{Z}$ takových, že

$$ax'+by'=1.$$

Úpravou vzniklé rovnice získáme $anx'+bny'=n$. Bod $[nx',ny']$ proto leží na přímce p.

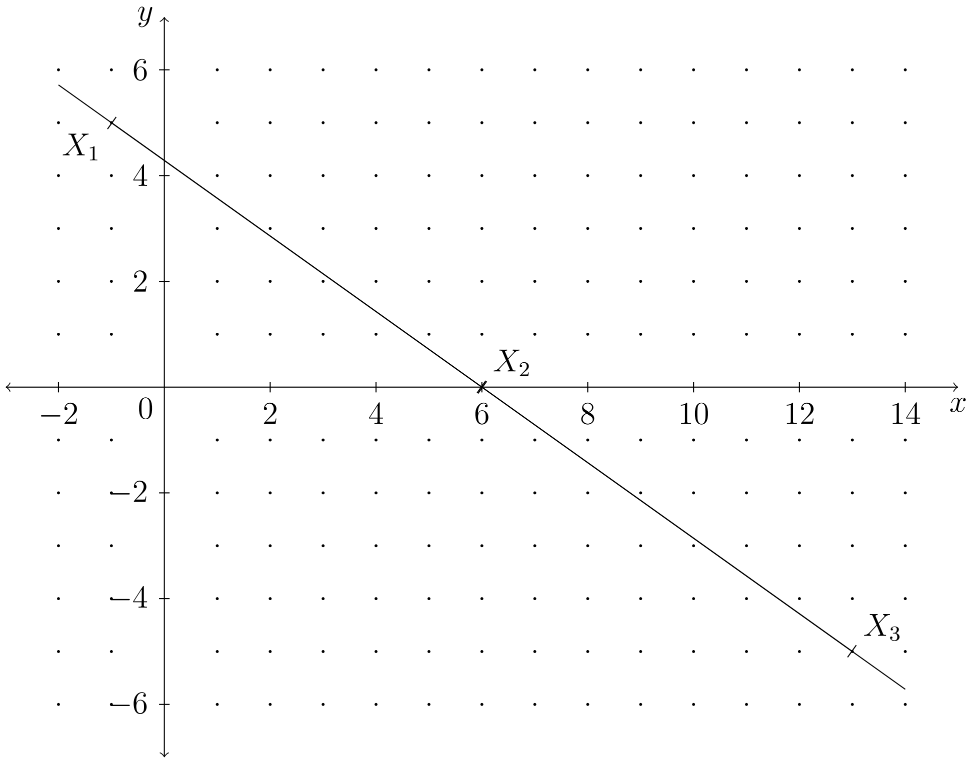
Podle lemmatu 1.10 leží na přímce p nekonečně mnoho bodů s celočíselnými souřadnicemi v pravidelných intervalech. Vzdálenost dvou sousedních bodů $X=[x,y]$ a $Y=[x+b,y-a]$ je

$$s=\sqrt{(x-x-b)^2+(y-y+b)^2}=\sqrt{a^2+b^2}.$$

□

Na obrázku 1.2 je znázorněna přímka p odpovídající volbě $n = 30$, $a = 5$ a $b = 7$. Vyznačené body X_1, X_2 a X_3 na přímce p jsou tři po sobě jdoucí body s celočíselnými souřadnicemi. Jejich vzdálenosti jsou podle věty 1.11

$$|X_1X_2| = |X_2X_3| = \sqrt{5^2 + 7^2} = \sqrt{74}.$$



Obrázek 1.2: Přímka s vyznačenými body s celočíselnými souřadnicemi pro $a = 5$, $b = 7$ a $n = 30$

Věta 1.12. *Mějme systém mincí s nesoudělnými hodnotami a, b. Částka $n = ab$ je v tomto systému reprezentovatelná dvěma způsoby. Všechny částky $n > ab$ jsou reprezentovatelné. Částky $n < ab$ jsou reprezentovatelné maximálně jedním způsobem.*

Důkaz. Pokud je úsečka AB s krajními body $A = [n/a, 0]$ a $B = [0, n/b]$ delší než $\sqrt{a^2 + b^2}$, pak na ní podle věty 1.11 leží alespoň jeden bod s celočíselnými souřadnicemi.

Délka úsečky AB přitom roste s n lineárně, neboť pro $n \geq 0$ platí

$$|AB| = \sqrt{\left(\frac{n}{a}\right)^2 + \left(\frac{n}{b}\right)^2} = n\sqrt{\left(\frac{1}{a}\right)^2 + \left(\frac{1}{b}\right)^2}.$$

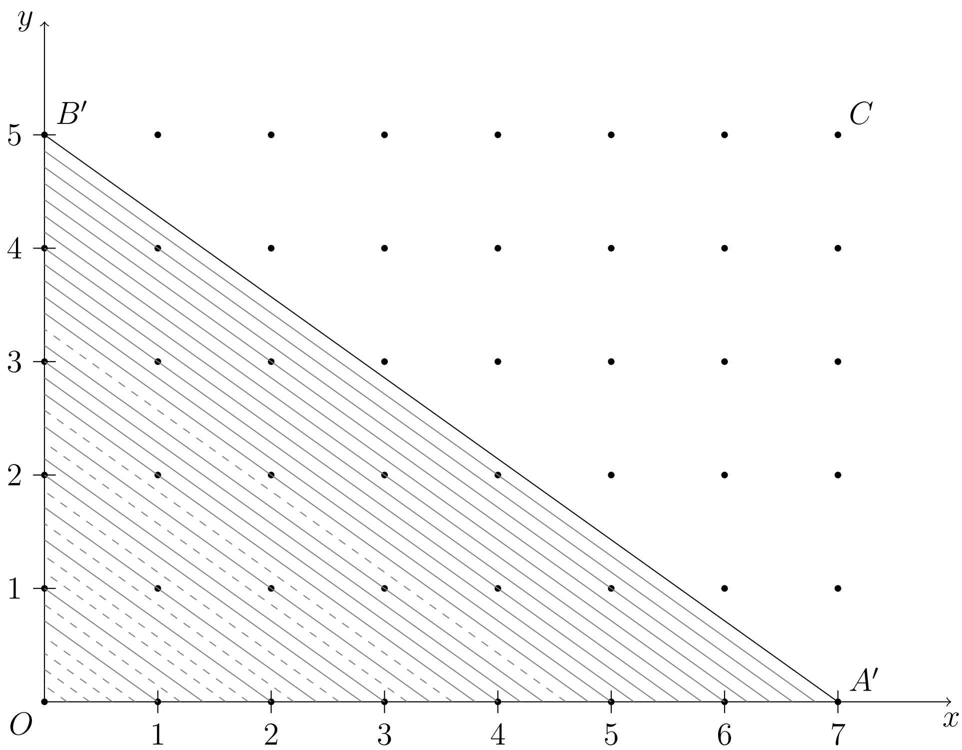
Pro $n = ab$ je $A = [b, 0]$, $B = [0, a]$ a $|AB| = \sqrt{a^2 + b^2}$. Podle věty 1.11 na této úsečce leží maximálně dva body s celočíselnými souřadnicemi. Jsou právě dva a jsou jimi body A, B.

Pro $n > ab$ je odpovídající úsečka delší než vzdálenost sousedních bodů s celočíselnými souřadnicemi, leží na ní proto alespoň jeden z nich. Pro $n < ab$ je odpovídající úsečka kratší než vzdálenost sousedních bodů s celočíselnými souřadnicemi a proto na ní leží maximálně jeden z nich. ☐

Označíme body $A' = [b, 0]$, $B' = [0, a]$ a počátek $O = [0, 0]$. Body A' a B' jsou krajními body úsečky pro $n = ab$. Z věty 1.12 vidíme, že každé reprezentovatelné částce menší než ab odpovídá úsečka, na které leží právě jeden bod s celočíselnými souřadnicemi. Odtud plyne, že reprezentovatelných částek n menších než ab je maximálně tolik, jako bodů s celočíselnými souřadnicemi, které leží uvnitř trojúhelníku $OA'B'$ nebo na jeho obvodu, nepočítáme-li body A' a B'.

Počet reprezentovatelných částek by byl ostře menší než počet popsaných bodů, kdyby existoval bod s celočíselnými souřadnicemi, který neleží na žádné z úseček. Následující větou 1.13 dokážeme, že tomu tak není. Počet bodů s celočíselnými souřadnicemi je proto roven počtu reprezentovatelných částek.

Na obrázku 1.3 jsou na příkladu systému mincí s $a = 5$ a $b = 7$ znázorněny všechny úsečky odpovídající číslům $n \in \{1, 2, \ldots, 5 \cdot 7 = 35\}$. Úsečky, na kterých leží bod s celočíselnými souřadnicemi, a odpovídají tedy reprezentovatelným částkám, jsou znázorněny plnou čarou. Úsečky, na kterých žádný bod s celočíselnými souřadnicemi neleží, a odpovídají tedy nereprezentovatelným částkám, jsou znázorněny přerušovaně.



Obrázek 1.3: Úsečky AB pro $a = 5$, $b = 7$ a $n \in \{0, 1, \ldots, 35\}$

Věta 1.13. *Mějme nesoudělná $a, b \in \mathbb{N}$. Pro každý bod $X = [x, y]$ se souřadnicemi $x, y \in \mathbb{N}_0$ existuje $n \in \mathbb{N}_0$ takové, že X leží na úsečce s krajními body $A = [n/a, 0]$, $B = [0, n/b]$.*

Důkaz. Výraz $ax + by$ je jistě celočíselný. Zvolíme proto

$$n = ax + by. \tag{1.3}$$

Pokud se na vztah (1.3) budeme dívat jako na rovnici přímky, snadno ověříme, že protíná osy v bodech $A = [n/a, 0]$ a $B = [0, n/b]$. Bod X na této přímce leží. Leží i na úsečce AB, neboť se nachází v prvním kvadrantu.

□

Věta 1.14. *Počet všech nereprezentovatelných částek v systému mincí o nesoudělných hodnotách $a, b \in \mathbb{N}$ je*

$$\frac{(a-1)(b-1)}{2}.$$

Důkaz. Počet všech částek menších než ab, včetně nuly, je ab.

Volme $A' = [b, 0], B' = [0, a], O = [0, 0]$ a $C = [b, a]$. Z vět 1.12 a 1.13 plyne, že počet reprezentovatelných částek menších než ab je roven počtu bodů s celočíselnými souřadnicemi, které leží uvnitř trojúhelníku $OA'B'$ nebo na jeho obvodu, bez bodů A' a B'. Těch je polovina z počtu bodů s celočíselnými souřadnicemi, ležících v obdélníku $OA'CB'$, bez bodů A' a B'.

Počet reprezentovatelných částek menších než ab je proto

$$\frac{(a+1)(b+1)-2}{2}.$$

Počet nereprezentovatelných částek menších než ab vypočítáme odečtením počtu reprezentovatelných od počtu všech:

$$ab - \frac{(a+1)(b+1)-2}{2} = ab - \frac{ab}{2} - \frac{a}{2} - \frac{b}{2} + \frac{1}{2} = \frac{(a-1)(b-1)}{2}$$

Z věty 1.12 víme, že každá částka větší nebo rovná ab je reprezentovatelná. □

1.3 Největší nereprezentovatelná částka

V části 1.2 jsme se zajímali o to, kolik částek nelze reprezentovat pomocí systému mincí a, b. Nyní budeme zjišťovat, která z nereprezentovatelných částek je největší. Tuto otázku má smysl zkoumat jen pro nesoudělné systémy mincí. Systémy mincí s největším společným dělitelem $d > 1$ mají totiž nekonečně mnoho nereprezentovatelných částek (viz část 1.1).

1.3.1 Pro dvě mince

Budeme se zabývat následující otázkou:

Otázka. *Máme neomezené množství mincí o hodnotách a a b. Čísla a a b jsou nesoudělná. Jaká je největší částka, kterou pomocí těchto mincí nemůžeme reprezentovat?*

Postup si nejprve ukážeme na konkrétním případě pro systém mincí o nesoudělných hodnotách $a = 5$, $b = 9$.

Opět si vypíšeme tabulku reprezentovatelných částek 1.2. Je to stejná tabulka reprezentovatelných částek jako 1.1. Jen jsou v ní zvýrazněny jiné hodnoty.

Z této tabulky vypustíme poslední řádek a sloupec. Navíc od každého čísla většího než $ab = 45$ odečteme 45. Výsledkem bude tabulka 1.3.

$u \backslash v$	0	1	2	3	4	5	6	7	8	9
0	0	5	10	15	20	25	30	35	40	45
1	9	14	19	24	29	34	39	44	49	54
2	18	23	28	33	38	43	48	53	58	63
3	27	32	37	42	47	52	57	62	67	72
4	36	41	46	51	56	61	66	71	76	81
5	45	50	55	60	65	70	75	80	85	90

Tabulka 1.2: Reprezentovatelné částky pro hodnoty $a = 5$, $b = 9$

$u \backslash v$	0	1	2	3	4	5	6	7	8
0	0	5	10	15	20	25	30	35	40
1	9	14	19	24	29	34	39	44	4
2	18	23	28	33	38	43	3	8	13
3	27	32	37	42	2	7	12	17	22
4	36	41	1	6	11	16	21	26	31

Tabulka 1.3: Reprezentovatelné a nereprezentovatelné částky pro hodnoty $a = 5$, $b = 9$

Tabulka 1.3 obsahuje všechna čísla mezi 0 a $ab - 1$ včetně. Jsou v ní proto všechny reprezentovatelné i nereprezentovatelné částky menší než ab. Žádné číslo se v ní navíc neopakuje. V levé horní vyznačené části tabulky jsou všechny reprezentovatelné částky.

V pravé dolní části tabulky tedy musí být všechny nereprezentovatelné částky. Největší nereprezentovatelná částka menší než ab se nachází v pravém dolním rohu. Je jí hodnota 31. Mezi 31 a $ab = 45$ je 14 reprezentovatelných částek. Přičtením vhodného násobku pěti k nějaké z nich tak můžeme reprezentovat libovolnou částku vyšší než 45.

Nyní zopakujeme stejný postup pro libovolný systém mincí o nesoudělných hodnotách a, b.

Definice 1.15. *Nechť $a, b \in \mathbb{N}$ jsou nesoudělná čísla. Uvažujme matici o a řádcích a b sloupcích, kde pro čísla $u, v \in \mathbb{N}_0$ taková, že $u < a$ a $v < b$, je hodnota prvku matice na u-tém řádku a v-tém sloupci rovna*

$$\begin{cases} u \cdot b + v \cdot a & \text{pro } u \cdot b + v \cdot a < ab, \\ u \cdot b + v \cdot a - ab & \text{pro } u \cdot b + v \cdot a \geq ab. \end{cases}$$

Tuto matici budeme označovat $A^*_{a,b}$. Hodnotu v u-tém řádku a v-tém sloupci budeme značit $A^*_{a,b}(u, v)$.

Matice $A^*_{a,b}$ odpovídá obsahu tabulky 1.3.

Věta 1.16. *Máme-li $a, b \in \mathbb{N}$ nesoudělná, pak jsou v matici $A^*_{a,b}$ všechna čísla různá.*

Důkaz. Podle věty 1.8 jsou v matici $A_{a,b}$ bez posledního řádku a sloupce všechna čísla různá.

Na souřadnicích (u, v), kde $ub + va < ab$, se matice $A^*_{a,b}$ od $A_{a,b}$ neliší. Žádná dvojice čísel z této části proto není stejná.

Na souřadnicích (u, v), kde $ub + va \geq ab$ je v matici $A^*_{a,b}$ hodnota

$$ub + va - ab = A_{a,b}(u, v) - ab.$$

Žádná dvojice čísel z této části proto také není stejná.

Zbývá zjistit, jestli nemůže existovat číslo z první části stejné jako číslo z druhé části. Takové číslo by muselo být v první části na pozici (u_1, v_1) s reprezentací

$$x = u_1 b + v_1 a.$$

Zároveň by muselo být na pozici (u_2, v_2) v druhé části s reprezentací

$$x = u_2 b + v_2 a - ab$$

Úpravami těchto rovnic dostaneme:

$$(v_1 - v_2 + b)a = (u_2 - u_1)b \tag{1.4}$$

Vidíme, že a dělí $(u_2 - u_1)b$. Protože a, b jsou nesoudělná, a dělí $u_2 - u_1$. První souřadnice čísel se tedy liší o násobek a. Protože matice $A^*_{a,b}$ má $a - 1$ řádků, musí být tento násobek roven 0. První souřadnice čísel jsou proto stejné.

Z rovnice (1.4) také vidíme, že b dělí $(v_1 - v_2 + b)a$. Protože a, b jsou nesoudělná, tak b dělí $v_1 - v_2 + b$. Odtud b dělí $v_1 - v_2$. Druhá souřadnice čísel se tedy liší o násobek b. Protože matice $A^*_{a,b}$ má $b - 1$ sloupců, musí být tento násobek roven 0. Druhé souřadnice čísel jsou proto stejné.

Obě čísla mají stejné souřadnice, což je ve sporu s předpokladem, že leží v různých částech matice. V matici $A^*_{a,b}$ proto nejsou dvě stejná čísla. □

Matice $A^*_{a,b}$ obsahuje ab čísel. Všechna jsou menší než ab. Podle věty 1.16 jsou navíc všechna čísla v matici různá. Matice $A^*_{a,b}$ proto obsahuje všechny reprezentovatelné i nereprezentovatelné kladné částky menší než ab.

Věta 1.17. *Mějme $a, b \in \mathbb{N}$ nesoudělná. Částka na souřadnicích (u, v) v matici $A^*_{a,b}$ je reprezentovatelná právě tehdy, když platí*

$$ub + va < ab.$$

Důkaz. Na souřadnicích $ub + va < ab$ je částka $ub + va$, je proto reprezentovatelná.

Ukážeme naopak, že každá částka, která nemá souřadnice (u, v) splňující $ub + va < ab$, není reprezentovatelná. Matice $A_{a,b}$ obsahovala všechny reprezentovatelné částky menší než ab. Odstraněním posledního řádku a sloupce žádná z nich nezmizela. Odečtením ab od hodnot $ub + va \geq ab$ jsme s částkami menšími než ab nic neudělali. Matice $A^*_{a,b}$ proto stále obsahuje všechny reprezentovatelné částky menší než ab.

Podle věty 1.16 jsou navíc v matici $A^*_{a,b}$ všechny hodnoty různé. Na souřadnicích s $ub + va \geq ab$ proto nemůže být reprezentovatelná částka. □

Podle věty 1.17 dokážeme určit, na kterých souřadnicích v $A^*_{a,b}$ se nachází reprezentovatelné částky. Na ostatních souřadnicích se proto nacházejí částky nereprezentovatelné.

Věta 1.18. *V systému mincí o nesoudělných hodnotách $a, b \in \mathbb{N}$ je největší nereprezentovatelná částka menší než ab rovna*

$$ab - a - b.$$

Důkaz. Z věty 1.17 plyne, že v matici $A^*_{a,b}$ jsou všechny nereprezentovatelné částky menší než ab na pozicích (u, v), kde

$$ub + va \geq ab.$$

Největší z nich je v pravém dolním rohu matice $A^*_{a,b}$, tedy na souřadnicích $(a-1, b-1)$. Její hodnota je:

$$A_{a,b}(a-1, b-1) - ab = (a-1)b + (b-1)a - ab = ab - a - b$$

□

Nyní jsme se dostali do stejné situace jako v části 1.2.1. Našli jsme řešení s omezením pro částky menší než ab. Větou 1.12 už jsme dokázali, že všechny větší částky jsou reprezentovatelné. Raději to ale dokážeme ještě jednou použitím poznatků z této části.

Věta 1.19. *V systému mincí o nesoudělných hodnotách $a, b \in \mathbb{N}$ jsou všechny částky větší nebo rovné ab reprezentovatelné.*

Důkaz. Mezi největší nereprezentovatelnou částkou $ab - a - b$ a ab je $a + b$ reprezentovatelných částek. Přičtením vhodného násobku čísla b k některé z nich získáme reprezentaci libovolné částky větší nebo rovné ab. □

V kapitolách 1.2 a 1.3 jsme pro systémy mincí o nesoudělných hodnotách $a, b \in \mathbb{N}$ dospěli k následujícím závěrům:

- Počet všech nereprezentovatelných částek je roven $\frac{(a-1)(b-1)}{2}$.
- Největší nereprezentovatelná částka je rovna $ab - a - b$.

Příklad 1.20. *Ve dvoumincovém systému mincí o hodnotách a, b, kde $a < b$, je 35 nereprezentovatelných částek, z nichž jedna je 58. Jaké jsou hodnoty a, b? [11, kap. 13]*

Řešení. Hodnoty a, b jsou nesoudělné. Kdyby to tak nebylo, pak by podle věty 1.3 existovalo nekonečně mnoho nereprezentovatelných částek. Dále víme, že

$$\frac{(a-1)(b-1)}{2} = 35, \tag{1.5}$$

tedy $(a-1)(b-1) = 70$.

Hledáme tedy čísla $k, l \in \mathbb{N}$ tak, aby platilo $kl = 70$ a $k < l$. Řešením úlohy je dvojice (a, b) taková, že $a = k + 1$ a $b = l + 1$, a, b jsou nesoudělná a částka 58 není reprezentovatelná v systému mincí o hodnotách a, b.

Číslo 70 můžeme rozložit na součin dvou přirozených čísel například pomocí rozkladu na součin prvočísel:

$$70 = 2 \cdot 5 \cdot 7$$

Všechny dvojice přirozených čísel (a, b), pro které platí rovnice (1.5) a $a < b$, jsou tedy: $(2, 71), (3, 36)$, $(6, 15)$ a $(8, 11)$.

Dvojice $(3, 36)$ a $(6, 15)$ vyřadíme, neboť jde o dvojice soudělných čísel. Dvojici $(2, 71)$ vyřadíme, neboť $58 = 2 \cdot 29$.

Zbylá dvojice $(8, 11)$ splňuje všechny požadavky. Jediným řešením je tedy $a = 8$ a $b = 11$.

1.3.2 Pro více mincí

Dosud jsme našli největší nereprezentovatelnou částku pro systémy tvořené dvěma mincemi. Pro více mincí je stejný problém výrazně obtížnější.

Otázka. *Máme systém mincí o nesoudělných hodnotách* $x_1, x_2, \ldots, x_n \in \mathbb{N}$. *Jaká je v tomto systému největší nereprezentovatelná částka?*

V systémech, obsahujících minci o hodnotě 1, jsou všechny částky reprezentovatelné. V této části proto budeme zkoumat pouze systémy, které neobsahují minci o hodnotě 1, a existuje v nich proto alespoň jedna nereprezentovatelná částka. V systémech s nesoudělnými hodnotami mincí je konečně mnoho nereprezentovatelných částek. Ukážeme to následující větou.

Věta 1.21. *Pro každý systém mincí o nesoudělných hodnotách* $x_1, x_2, \ldots, x_n \in \mathbb{N}$ *existuje částka* $g(x_1, x_2, \ldots, x_n)$ *taková, že každá částka* $a > g(x_1, x_2, \ldots, x_n)$ *je reprezentovatelná.* [25, věta 8]

Důkaz. Větu dokážeme matematickou indukcí podle počtu mincí. Pro dvoumincové systémy jsme existenci největší nereprezentovatelné částky ukázali v části 1.3.1.

Předpokládejme nyní, že pro systémy o $n-1$ nesoudělných mincích věta platí. Chceme dokázat, že platí i pro systém o nesoudělných hodnotách $x_1, x_2, \ldots, x_n$.

Nechť d je největší společný dělitel $x_1, x_2, \ldots, x_{n-1}$. Pokud je $d = 1$, pak je podle indukčního předpokladu každá částka větší než $g(x_1, x_2, \ldots, x_{n-1})$ v systému o hodnotách $x_1, x_2, \ldots, x_{n-1}$ reprezentovatelná. Přidáním poslední mince x_n na tom nic nezměníme.

Pokud je $d > 1$, pak označíme $x'_1 = x_1/d$, $x'_2 = x_2/d, \ldots, x'_{n-1} = x_{n-1}/d$. Podle indukčního předpokladu existuje $g(x'_1, x'_2, \ldots, x'_{n-1})$.

Dokážeme, že libovolná částka a splňující

$$a > x_n(d-1) + dg(x'_1, x'_2, \ldots, x'_{n-1}) \tag{1.6}$$

je v systému mincí o hodnotách $x_1, x_2, \ldots, x_n$ reprezentovatelná.

Z předpokladu věty víme, že d a x_n jsou nesoudělná. Z Bézoutovy rovnosti [23, věta 3.3] proto plyne existence $k, l \in \mathbb{Z}$ takových, že platí

$$\begin{aligned} ld + kx_n &= 1 \\ kx_n &\equiv 1 \pmod{d} \\ kx_n a &\equiv a \pmod{d}. \end{aligned}$$

a proto existuje $0 \leq c \leq d-1$, pro které platí

$$x_n c \equiv a \pmod{d}. \tag{1.7}$$

Odtud a z (1.6) získáváme

$$\frac{a - x_n c}{d} \geq \frac{a - x_n(d-1)}{d} > g(x'_1, x'_2, \ldots, x'_{n-1}). \tag{1.8}$$

Částka $(a - x_n c)/d$ je podle (1.7) celočíselná. Podle (1.8) je navíc v systému mincí o hodnotách $x'_1, x'_2, \ldots, x'_{n-1}$ reprezentovatelná, a existují tedy nezáporná celá čísla $b_1, b_2, \ldots, b_{n-1}$ taková, že platí

$$\frac{a - x_n c}{d} = b_1 x'_1 + b_2 x'_2 + \cdots + b_{n-1} x'_{n-1}.$$

Částku a tedy můžeme reprezentovat následujícím způsobem:

$$a = b_1 dx'_1 + b_2 dx'_2 + \cdots + b_{n-1} dx'_{n-1} + cx_n = b_1 x_1 + b_2 x_2 + \cdots + b_{n-1} x_{n-1} + cx_n$$

□

Z předchozí věty plyne existence největší nereprezentovatelné částky; budeme ji značit $f(x_1, \ldots, x_n)$ a nazývat Frobeniovým číslem.

Už pro systémy o třech mincích není znám vzorec pro výpočet Frobeniova čísla. Existuje však několik algoritmů, pomocí kterých ho zjistíme efektivněji než zkoušením všech možností. Jeden takový algoritmus si ukážeme. Popis algoritmu vychází z publikace [24, str. 536–542].

Obecný postup budeme ilustrovat na hledání čísla $f(6, 9, 20)$, které lze interpretovat např. jako řešení následující úlohy:

Otázka. *Ve stravovacím řetězci prodávají kuřecí kousky v balení po šesti, devíti a dvaceti kusech. Jaké největší množství kousků si nemůžeme koupit?*

Ve zbytku kapitoly budeme předpokládat, že hodnoty mincí jsou seřazené od nejmenšího k největšímu, tj. $x_1 < x_2 < \cdots < x_n$.

Vytvoříme si ohodnocený orientovaný graf $G = (V, E, h)$ s množinou vrcholů V, množinou hran E a funkcí přiřazující ohodnocení jednotlivých hran $h : E \to \mathbb{N}$. Množina vrcholů tohoto grafu má x_1 prvků:

$$V = \{0, 1, \ldots, x_1 - 1\}$$

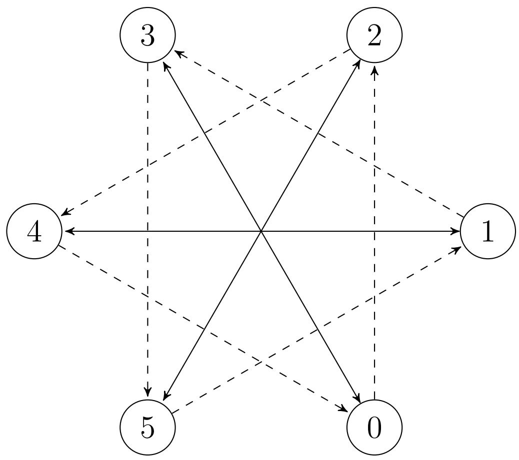
Z vrcholu u vede do vrcholu v hrana právě tehdy když existuje i tak, že

$$u + x_i \equiv v \pmod{x_1}. \tag{1.9}$$

Tato hrana má ohodnocení x_i.

Pro systém mincí o hodnotách 6, 9 a 20 je $x_1 = 6$. Sestavený graf je na obrázku 1.4. Hrany, které jsou v grafu vyznačeny plnou čarou, vznikly dosazením $x_i = 9$ do vztahu (1.9). Jejich ohodnocení je proto rovno 9.

Hrany, které jsou v grafu vyznačeny přerušovanou čarou, vznikly dosazením $x_i = 20$ do stejného vztahu. Jejich ohodnocení je proto 20.



Obrázek 1.4: Orientovaný graf pro systém mincí o hodnotách $6, 9$ a 20.

Nyní najdeme nejkratší cestu od vrcholu 0 ke každému z ostatních vrcholů. Největší z délek nalezených cest označíme $D(G)$. Frobeniovo číslo spočítáme následovně:

$$f(x_1, x_2, \ldots, x_n) = D(G) - x_1 \tag{1.10}$$

Vrchol	1	2	3	4	5
Vzdálenost	49	20	9	40	29

Tabulka 1.4: Tabulka nejkratších vzdáleností od vrcholu 0 pro graf systému mincí o hodnotách $6, 9$ a 20

Hledání nejkratších cest v grafu je známý problém. K jeho vyřešení můžeme použít například Dijkstrův algoritmus [22, str. 206–210]. Nalezené délky nejkratších cest jsou uvedeny v tabulce 1.4. Nejvzdálenější od vrcholu 0 je vrchol 1 se vzdáleností 49. Frobeniovo číslo je podle (1.10) rovno:

$$f(6, 9, 20) = 49 - 6 = 43$$

Ve stravovacím řetězci si nemůžeme koupit 43 kuřecích kousků. Libovolný vyšší počet už si koupit můžeme.

Z popisu algoritmu není na první pohled zřejmé, že výsledkem výrazu (1.10) je skutečně Frobeniovo číslo. V následující části textu ukážeme, že tomu tak je. Budeme přitom vycházet z důkazu popsaného v [5].

Poznámka. *V našem popisu algoritmu předpokládáme, že graf není multigrafem, tedy neobsahuje vícenásobné hrany. Dosazením do rovnice* (1.9) *zjistíme, že násobná hrana mezi vrcholy* u, v *vznikne v grafu právě tehdy, když platí*

$$\begin{aligned} u + x_i &\equiv v \pmod{x_1} \\ u + x_j &\equiv v \pmod{x_1} \end{aligned}$$

pro $i > j$.

Úpravami zjistíme, že tento případ nastane právě tehdy, když platí

$$\exists k \in \mathbb{N} \quad x_i = x_j + kx_1.$$

V takovém případě má systém mincí bez mince x_i *stejná reprezentovatelná a nereprezentovatelná čísla jako původní systém mincí. Minci* x_i *proto můžeme pro hledání Frobeniova čísla vynechat a omezit se tak na grafy bez násobných hran.*

Například v systému mincí o hodnotách $6, 7$ *a* 13 *není mince s hodnotou* 13 *z hlediska reprezentovatelnosti potřeba, protože* $6 + 7 = 13$.

Poznámka. *V celém odvození správnosti algoritmu budeme pracovat se systémem mincí se seřazenými nesoudělnými hodnotami* $x_1, x_2, \ldots, x_n$. *Kdykoliv budeme uvažovat graf* G, *myslíme tím graf, který vznikl pomocí algoritmu popsaného výše.*

Předtím, než dokážeme správnost algoritmu, podíváme se na vlastnosti sestrojeného grafu.

Definice 1.22. *Sled v grafu $G = (V, E, h)$ je posloupnost vrcholů $(v_1, v_2, \ldots, v_n)$, kde každé dva po sobě jdoucí vrcholy jsou spojeny hranou, tedy*

$$v_i \in V, (v_j, v_{j+1}) \in E.$$

Z (1.9) přímo plyne, že z každého vrcholu grafu G vychází hrana s ohodnocením x_i pro $i \in \{2, 3, \ldots, n\}$. Žádné dvě hrany vycházející z jednoho vrcholu navíc nemají stejné ohodnocení.

Sled proto můžeme popsat jako posloupnost ohodnocení hran spolu s výchozím vrcholem. Každé ohodnocení v posloupnosti určuje, po které hraně sled pokračuje.

Definice 1.23. *Ohodnocením sledu $s = (v_1, v_2, \ldots, v_n)$ rozumíme součet ohodnocení všech jeho hran tj.*

$$h(s) = \sum_{i=1}^{n-1} h((v_i, v_{i+1})).$$

Věta 1.24. *Nechť p je sled v grafu G s ohodnocením w, jehož začátek je ve vrcholu 0. Ohodnocení hran sledu p označíme po řadě $(h_1, h_2, \ldots, h_m)$.*

Potom koncový vrchol sledu p je vrchol v, pro který platí

$$w = \sum_{i=1}^{m} h_i \equiv v \pmod{x_1}.$$

Důkaz. První rovnost plyne z definice ohodnocení sledu. Opakovaným použitím vztahu (1.9) dokážeme kongruenci. □

Každé ohodnocení hrany v grafu má jednu z hodnot $x_2, x_3, \ldots, x_n$. Vztah ve větě 1.24 proto můžeme přepsat do tvaru

$$w = \sum_{i=2}^{n} a_i x_i \equiv v \pmod{x_1}, \tag{1.11}$$

kde a_i jsou počty hran s ohodnocením x_i ve sledu p.

Poznámka. *Výraz a mod b v následující části textu znamená zbytek po celočíselném dělení čísla a číslem b.*

Pro výraz

$$(v_1 \ mod\ b, v_2 \ mod\ b, \ldots, v_n \ mod\ b)$$

dále zavádíme zkrácený zápis

$$(v_1, v_2, \ldots, v_n) \mod b.$$

Věta 1.25. *Sled se začátkem ve vrcholu u a koncem ve vrcholu v existuje právě tehdy, když existuje sled se začátkem ve vrcholu 0 a koncem ve vrcholu*

$$v - u \mod x_1.$$

Důkaz. Mějme sled $(v_1 = u, v_2, \ldots, v_m = v)$, který má začátek ve vrcholu u a konec ve vrcholu v. Posloupnost vrcholů

$$(v_1 - u, v_2 - u, v_3 - u, \ldots, v - u) \mod x_1$$

začíná v 0 a končí v $v-u \mod x_1$. Ze vztahu (1.9) navíc plyne, že každá dvojice $(v_i - u \mod x_1, v_{i+1} - u \mod x_1)$ odpovídá hraně. Výše uvedená posloupnost vrcholů je tedy sled v grafu G.

Opačnou implikaci dokážeme analogicky přičtením u ke všem vrcholům sledu.

□

Věta 1.26. *Jsou-li hodnoty $x_1, x_2, \ldots, x_n$ nesoudělné, pak je graf $G = (V, E, h)$ silně souvislý, tj. pro každé $u, v \in V$ existuje sled s počátečním vrcholem u a koncovým vrcholem v.*

Důkaz. Podle věty 1.25 stačí dokázat, že existuje sled z vrcholu 0 do $v-u \mod x_1$.

K tomu stačí najít nějaké koeficienty $a_2, a_3, \ldots, a_n$ takové, že platí

$$\sum_{i=2}^{n} a_i x_i \equiv v - u \pmod{x_1}.$$

Součet na levé straně potom odpovídá ohodnocení hran hledaného sledu.

Pokud zvolíme $k \in \mathbb{N}$ tak, že $v - u + kx_1 > f(x_1, x_2, \ldots, x_n)$, pak je číslo na levé straně nerovnosti reprezentovatelné a existují koeficienty $a_1, a_2, \ldots, a_n$ tak, že platí

$$\sum_{i=1}^{n} a_i x_i = v - u + kx_1.$$

□

Věta 1.27. *Číslo x je reprezentovatelné v systému o hodnotách $x_1, x_2, \ldots, x_n$ právě tehdy, když $x \geq h$, kde h je ohodnocení nejkratšího sledu z vrcholu 0 do vrcholu $v \in V$ splňujícího $v \equiv x \pmod{x_1}$.*

Důkaz. Nejprve dokážeme implikaci $\Rightarrow$. Máme-li reprezentovatelné $x = \sum_{i=1}^{n} a_i x_i$, pak podle předpokladu věty platí

$$\sum_{i=2}^{n} a_i x_i \equiv v \pmod{x_1}.$$

Levá strana kongruence udává ohodnocení hran nějakého sledu z vrcholu 0 do vrcholu v. Ten je jistě alespoň tak dlouhý jako nejkratší sled. Platí proto

$$x = \sum_{i=1}^{n} a_i x_i \geq \sum_{i=2}^{n} a_i x_i \geq h.$$

Pro důkaz implikace $\Leftarrow$ budeme předpokládat, že $x \geq h$. Číslo h je ohodnocení sledu končícího ve vrcholu v. Pro koeficienty a_i určující počet hran s ohodnocením x_i proto platí

$$h = \sum_{i=2}^{n} a_i x_i \equiv v \pmod{x_1}.$$

Odtud a z předpokladu věty vidíme, že

$$\sum_{i=2}^{n} a_i x_i \equiv x \pmod{x_1}.$$

Odstraněním kongruence dostaneme pro $k \in \mathbb{Z}$

$$kx_1 + \sum_{i=2}^{n} a_i x_i = kx_1 + h = x.$$

Koeficient k je nezáporný, protože $x \geq h$. Hodnoty $k, a_2, a_3, \ldots, a_n$ udávají reprezentaci x v systému mincí o hodnotách $x_1, x_2, \ldots, x_n$. □

Nyní už dokážeme najít největší nereprezentovatelné číslo x.

Věta 1.28. *Mějme nesoudělný systém mincí o hodnotách $x_1, x_2, \ldots, x_n \in \mathbb{N}$ a graf G tohoto systému. Označíme $d_0, d_1, \ldots, d_{x_1-1}$ délky nejkratších cest k vrcholům $0, 1, \ldots, x_1 - 1$. Pak platí*

$$f(x_1, x_2, \ldots, x_n) = D(G) - x_1,$$

kde $D(G)$ je největší z $d_0, d_1, \ldots, d_{x_1-1}$.

Důkaz. Volme libovolné $i \in \{0, 1, \ldots, x_1 - 1\}$. Podle věty 1.24 platí

$$d_i \equiv i \pmod{x_1},$$

a tedy také

$$d_i - x_1 \equiv i \pmod{x_1}.$$

Ve větě 1.27 zvolíme $x = d_i - x_1$ a $v = i$. Číslo $d_i - x_1$ je kongruentní s i a zároveň je menší než délka d_i nejkratšího sledu do vrcholu i. Všechna větší čísla kongruentní s i jsou navíc větší nebo rovna d_i.

Podle věty 1.27 je proto $d_i - x_1$ největší nereprezentovatelné číslo kongruentní s i.

Největší nereprezentovatelné číslo je proto $D(G) - x_1$, kde $D(G)$ je největší z $d_0, d_1, \ldots, d_{x_1-1}$. □

1.4 Reprezentovatelnost zvolené částky

1.4.1 Hra hledání nereprezentovatelných hodnot

S využitím znalostí z předchozího textu si můžeme zahrát hru. Při jejím popisu vycházíme z [18, str. 194–197]. Hru hrají dva hráči, kteří se střídají po tazích. Říkejme jim Alice a Bob. Každý z nich ve svém tahu vybere jedno přirozené číslo, které není reprezentovatelné pomocí mincí o již vybraných hodnotách. Ten, kdo vybere číslo 1, prohrává. Alice začíná.

Zajímá nás, kdo z nich vyhraje, pokud budou oba hrát optimálním způsobem. Zkusíme se pro začátek podívat na jednoduché případy.

Alice na začátku vybere 2. Bob tedy ve svém tahu nesmí vybrat žádné sudé číslo. Nejlepší volbou je pro něj číslo 3, protože tím Alici zbude jediná nereprezentovatelná hodnota 1, která je prohrávající.

Alice na začátku vybere 3. Potom je situace stejná. Bob vybere 2 a na Alici zbude 1. Alice opět prohrává.

Alice na začátku vybere 4. Pro Boba je situace složitější. Řekněme, že vybere 5. Alice může jistě vyhrát, pokud ve svém tahu vybere 11. V systému mincí o hodnotách 4, 5 a 11 jsou totiž nereprezentovatelné pouze hodnoty $1, 2, 3, 6, 7$. Pokud Bob vybere 7, Alice odpoví 6. Bob potom musí vybrat 2 nebo 3, čímž se dostane do prohrávající situace, ve které byla Alice v prvních dvou případech. Kdyby Bob vybral 6, Alice odpoví 7 a dalšími tahy vyhraje Alice stejným způsobem. Výběr 2 nebo 3 Boba dostane do stejné prohrávající situace.

Kdybychom chtěli zkoušet všechny možnosti, následoval by nejspíš rozbor případu, kdy Alice začíná 4 a Bob odpoví 6. Zkoušení všech možností by ale byla velmi dlouhá cesta.

Ukážeme, že pro Alici existuje strategie, která jí zaručí výhru za všech okolností. Alice začne tím, že vybere 5. Bob jí může odpovědět libovolným dosud nereprezentovatelným číslem b. Systém mincí o hodnotách 5 a b je nesoudělný, protože 5 je prvočíslo.

Největší nereprezentovatelné číslo systému mincí o hodnotách 5 a b je $4b - 5$ (viz část 1.3.1). Pokud je toto číslo pro Alici vítězné, pak si ho jistě vybere. Pokud toto číslo pro Alici vítězné není, zamyslí se, jakým číslem by odpověděl Bob, kdyby si Alice vybrala prohrávající tah $4b - 5$. Řekněme, že Bob by v takovém případě vyhrál výběrem čísla n. Alice proto namísto prohrávajícího tahu $4b - 5$ vezme Bobovi jeho strategii a vybere rovnou číslo n. Bob si ve svém tahu nemůže vybrat číslo n. Následující větou dokážeme, že si nemůže vybrat ani číslo $4b-5$ a dostává se tak do stejné prohrávající pozice, ve které by byla Alice, kdyby chybně vybrala $4b - 5$.

Lemma 1.29. *Nechť n je libovolné nereprezentovatelné číslo v systému mincí o hodnotách 5 a b. V systému mincí o hodnotách $5, b$ a n je číslo $4b - 5$ reprezentovatelné.*

Důkaz. Vytvoříme si dvojice čísel $(i, 4b - 5 - i)$ takové, že $i < 4b - 5 - i$:

$$(0, 4b - 5), (1, 4b - 6), (2, 4b - 7), \dots, (2b - 3, 2b - 2)$$

Každá dvojice musí obsahovat aspoň jedno číslo nereprezentovatelné v soustavě o hodnotách 5 a b. Kdyby totiž obě čísla některé dvojice byla reprezentovatelná, pak totéž platí i pro jejich součet; to je ale ve sporu s tím, že číslo $4b - 5$ je nereprezentovatelné (dokonce největší takové).

V systému mincí je ale $(b-1)(5-1)/2 = 2b-2$ nereprezentovatelných hodnot (viz část 1.2.1). V každé z $2b-2$ dvojic proto musí být alespoň jedna z nich, jinak by na všechny nevyzbylo.

Každá dvojice proto obsahuje právě jedno nereprezentovatelné číslo. Číslo n je nereprezentovatelné a nachází se v jedné z dvojic. V systému mincí o hodnotách $5, b$ a n je $4b - 5$ reprezentovatelné, protože je součtem n a reprezentovatelného čísla, které bylo s n ve dvojici. □

Ukázali jsme vlastně, že Alice umí Bobovi ukrást vítěznou strategii. Konkrétní popis kroků ale neznáme. Pokud Bob vybere velké b, bude pro Alici obtížné najít správný další tah.

Hrát popsanou hru je velmi obtížné. Už kontrolovat, jestli hru hrají dva hráči podle pravidel je velmi obtížné. Abychom mohli zkontrolovat, jestli hrál hráč podle pravidel, potřebujeme zjistit jestli ve svém tahu vybral dosud nereprezentovatelné číslo.

1.4.2 Obtížnost reprezentovatelnosti

V této části ukážeme, že rozhodnutí, jestli je daná částka reprezentovatelná, je tzv. NP-úplný problém.

NP-úplné problémy můžeme vnímat jako problémy, pro které neznáme efektivní algoritmické řešení, tj. řešení, které provede maximálně polynomiální množství kroků vzhledem k velikosti zadání problému ve dvojkové soustavě. Budeme hovořit též o tzv. NP-těžkých problémech, což jsou zhruba řečeno úlohy alespoň tak obtížné, jako ostatní NP-úplné problémy. Přesné definice pojmů NP-těžkost a NP-úplnost lze najít v literatuře (viz např. [9]).

NP-těžkost našeho problému ukážeme převedením známého NP-úplného problému LOUPEŽNÍCI (anglicky uváděno jako PARTITION [9]) na problém reprezentovatelnosti částky. Budeme vycházet z důkazu uvedeného v [10].

Problém LOUPEŽNÍCI. Máme předměty o nezáporných celočíselných hodnotách $H = \{v_1, v_2, \dots, v_n\}$. Rozhodněte, jestli existuje množina $S \subseteq H$ taková, že

$$\sum_{v \in S} v = \sum_{u \in S \setminus H} u.$$

Cílem je tedy rozdělit lup H na dvě části tak, aby obě části měly stejnou hodnotu.

Problém reprezentovatelnosti jednou mincí každého druhu REP1 Máme mince o nezáporných celočíselných hodnotách $H = \{x_1, x_2, \dots, x_n\}$ a částku $c \in \mathbb{N}$. Rozhodněte, jestli existuje $S \subseteq H$ tak, že

$$\sum_{x \in S} x = c.$$

V problému REP1 hledáme reprezentaci částky c v systému mincí s omezením, že můžeme použít maximálně jednu minci od každé hodnoty. V anglické literatuře bývá uváděn pod jménem subset sum problem (SSP-DECISION) [14].

Problém reprezentovatelnosti v systému mincí REPN Máme systém mincí o nezáporných celočíselných hodnotách $x_1, x_2, \dots, x_n$ a částku $c \in \mathbb{N}$. Rozhodněte, jestli existuje n-tice nezáporných celých čísel $(b_1, b_2, \dots, b_n)$ taková, že

$$\sum_{i=1}^{n} b_i x_i = c.$$

V problému REPN hledáme libovolnou reprezentaci částky c ve stejném významu jako ve zbytku této práce (definice 1.1). V anglické literatuře bývá uváděn pod jménem unbounded subset sum problem (USSP-DECISION) [14].

Problém LOUPEŽNÍCI patří do třídy NP-úplných problémů [9].

Chceme dokázat, že pokud existuje algoritmus, který řeší problém REPN v polynomiálním čase vzhledem k délce vstupu, pak takový algoritmus existuje i pro problém Loupežníci. To dokážeme tak, že převedeme libovolné zadání problému Loupežníci na zadání problému RepN. Časová složitost algoritmu převodu musí být maximálně polynomiální v délce vstupu.

Tímto důkazem ukážeme, že dokážeme řešit problém Loupežníci pomocí řešení problému RepN. Kdyby pro problém RepN existoval polynomiální algoritmus řešení, existoval by takový i pro problém Loupežníci. Problém RepN proto patří spolu s Loupežníci do třídy NP-těžkých problémů.

Algoritmus převodu navíc nebudeme konstruovat přímo. Nejprve převedením problému Loupežníci na problém Rep1 ukážeme, že Rep1 je NP-těžký. Potom převedením Rep1 na RepN ukážeme, že RepN je NP-těžký.

Věta 1.30. *Existuje algoritmus, který převede zadání problému* Loupežníci *na zadání problému* Rep1 *v polynomiálním čase vzhledem k velikosti vstupu.*

Problém Loupežníci *bude mít s tímto zadáním řešení právě tehdy, když bude mít řešení problém* Rep1 *s převedeným zadáním.*

Důkaz. Popíšeme hledaný algoritmus. Máme hodnoty předmětů z problému Loupežníci $H = \{v_1, v_2, \ldots, v_n\}$. Hodnoty mincí z Rep1 nastavíme stejné jako hodnoty předmětů. Částka, kterou chceme reprezentovat, bude

$$c = \frac{\sum_{i=1}^{n} v_i}{2}.$$

Kdyby bylo $c \notin \mathbb{N}_0$, pak byla celková hodnota původního lupu H lichá a tedy nerozdělitelná na dvě stejné části. Problém Loupežníci nyní má řešení právě tehdy, když má řešení problém Rep1. Algoritmus převodu běží v polynomiálním čase. □

Dokázali jsme tedy, že problém Rep1 je NP-těžký.

Věta 1.31. *Existuje algoritmus, který převede zadání problému* Rep1 *na zadání problému* RepN *v polynomiálním čase vzhledem k velikosti vstupu.*

Problém Rep1 *bude mít s tímto zadáním řešení právě tehdy, když bude mít řešení problém* RepN *s převedeným zadáním.*

Důkaz. Označíme si $x_0, x_1, \ldots, x_{n-1}$ hodnoty mincí, které používáme pro hledání reprezentace částky c v problému Rep1.

Budeme konstruovat systém mincí $y_0, y_1, \ldots, y_m$ a částku c' tak, aby byla c' reprezentovatelná pomocí libovolného počtu mincí hodnot $y_0, y_1, \ldots, y_m$ právě tehdy když je c reprezentovatelná pomocí maximálně jedné mince každé z hodnot $x_0, x_1, \ldots, x_{n-1}$.

Oba problémy jsou téměř stejné. Pro zadání problému RepN bychom mohli použít stejné mince jako pro Rep1. Je pouze potřeba zajistit, aby problém RepN nepoužíval žádnou minci opakovaně.

Myšlenkou důkazu je, že k i-té minci přidáme kromě její hodnoty ještě počítadlo, které bude počítat, kolikrát byla tato mince použita. Každé minci x_i přiřadíme vektor v_i:

$$v_i = (\underbrace{0, 0, 0, \ldots, \overbrace{\quad 1 \quad}^{i\text{-té místo}}, \ldots, 0, 0, 0}_{n \text{ počítadel}}, x_i)$$

Číslo c je v Rep1 reprezentovatelné pomocí $x_0, \ldots, x_{n-1}$, právě když existují $a_i \in \{0, 1\}$ tak, že

$$\sum_{i=0}^{n-1} a_i x_i = c.$$

To nastane právě tehdy, když

$$\sum_{i=0}^{n-1} a_i v_i = (a_0, \ldots, a_{n-1}, c). \tag{1.12}$$

Definujeme-li

$$v'_i = (\underbrace{0, 0, 0, \ldots, \overbrace{1}^{i\text{-té místo}}, \ldots, 0, 0, 0}_{n \text{ počítadel}}, 0),$$

pak je (1.12) ekvivalentní s podmínkou

$$\sum_{i=0}^{n-1} a_i v_i + \sum_{i=0}^{n-1} a'_i v'_i = (1, \ldots, 1, c),$$

kde $a_i, a'_i \in \{0, 1\}$. V poslední rovnici můžeme připustit $a_i, a'_i \in \mathbb{N}_0$, protože to nijak neovlivní její řešitelnost.

Tím jsme původní úlohu Rep1 převedli na cosi jako vektorovou úlohu typu RepN, využívající libovolné množství „mincí“ $v_0, v_1, \ldots, v_{n-1}$ a $v'_0, v'_1, \ldots, v'_{n-1}$ k hledání reprezentace vektoru $(1, \ldots, 1, c)$. Zbývá ukázat, že pomocí kódování ve dvojkové soustavě ji můžeme převést na klasickou RepN.

Budeme uvažovat zápis hodnoty y_i ve dvojkové soustavě. Na cifrách s nejnižším významem bude dvojkový zápis čísla x_i. Na cifrách s vyšším významem budou počítadla. Pro počítadlo každé mince si vyhradíme pouze jednu cifru ve dvojkovém zápisu. Kdybychom nyní v reprezentaci použili dvě mince o hodnotě y_i, sečetly by se i jedničky na i-tém počítadle a jednička by „přetekla“ do sousedního počítadla.

Abychom tomu zabránili, dáme před počítadla jednotlivých mincí ještě počítadlo celkového počtu použitých mincí.

Zápis hodnoty mince y_i, odpovídající vektoru v_i, ve dvojkové soustavě nyní demonstruje následující výraz:

$$\underbrace{000\ldots001}_{\text{počítadlo použitých mincí}} \quad \underbrace{000\ldots\overbrace{1}^{i\text{-té místo}}\ldots000}_{n \text{ počítadel}} \ \underbrace{0101\ldots01}_{\text{dvojkový zápis } x_i}$$

Zápis pomocné mince y'_i, odpovídající vektoru v'_i, ve dvojkové soustavě je:

$$\underbrace{000\ldots001}_{\text{počítadlo použitých mincí}} \quad \underbrace{000\ldots\overbrace{1}^{i\text{-té místo}}\ldots000}_{n \text{ počítadel}}\underbrace{000\ldots000}_{\text{nuly}}$$

Částka c', jejíž reprezentaci v RepN hledáme, vypadá ve dvojkové soustavě následovně:

$$\underbrace{010\ldots101}_{\text{dvojkový zápis } n}\ \underbrace{111\ldots111}_{n \text{ počítadel}}\ \underbrace{0101\ldots01}_{\text{dvojkový zápis } c}$$

Každá mince má v počítadle celkového množství použitých mincí číslo 1. Částka c' má ve stejné části číslo n. Pro reprezentaci c' proto můžeme použít maximálně n mincí. Kdyby při sčítání došlo k přenosu z méně významných cifer, mohli bychom použít i méně než n mincí.

Každá mince má 1 na právě jednom z počítadel jednotlivých mincí. Pokud zajistíme, že nedojde k přenosu hodnot z méně významných cifer části dvojkového zápisu čísel x_i, pak potřebujeme alespoň n mincí pro vyplnění všech počítadel v c' jedničkami. Počítadlo použitých mincí zajišťuje, že využijeme maximálně n mincí. Pro zaplnění i-tého počítadla jednotlivých mincí proto potřebujeme buď minci y_i, nebo minci y'_i.

Největší částka, kterou umíme reprezentovat pomocí maximálně n mincí, je nx_{max}, kde x_{max} je největší z $x_0, x_1, \dots, x_{n-1}$. Aby dvojkový zápis nx_{max} nezasahoval do počítadel, vyhradíme si pro něj $d = \lceil \log_2 nx_{max} \rceil$ bitů.

Zadáním problému RepN budou mince $y_0, y_1, \dots, y_{n-1}$, $y'_0, y'_1, \dots, y'_{n-1}$ a částka c', kde

$$\begin{aligned} y_i &= x_i + 2^{i+d} + 2^{d+n} \\ y'_i &= 2^{i+d} + 2^{d+n} \\ c' &= c + \sum_{i=0}^{n-1} 2^{i+d} + n2^{d+n}. \end{aligned}$$

Vstup pro problém RepN je polynomiálně větší než vstup pro původní problém Rep1. Samotný algoritmus neprovádí žádný složitý výpočet. Jeho časová složitost je proto určena velikostí výstupu. Celý převod proto běží v polynomiálním čase. ☐

Problém RepN je tedy NP-těžký, tj. je alespoň tak těžký, jako všechny ostatní NP-úplné problémy. Problém RepN je zároveň ve třídě NP. Je totiž jednoduché v polynomiálním čase ověřit, že reprezentace částky n je platná.

Zjistili jsme tedy, že už základní problém zjištění, jestli je daná částka v systému mincí reprezentovatelná, patří mezi NP-úplné problémy. Dalším NP-úplným problémem, který jsme již zmínili, je nalezení Frobeniova čísla v systému mincí [21].

Grafový algoritmus, který jsme ukázali v části 1.3.2, se zdá být efektivní. I ten ale ve skutečnosti běží v exponenciálním čase vzhledem k délce zadání ve dvojkové soustavě. Počet kroků, který musí udělat, roste polynomiálně s hodnotou nejmenší mince v zadání. Hodnota mincí v zadání ale může růst exponenciálně vzhledem k délce zadání ve dvojkové soustavě.

2. Počet reprezentací částky

V této kapitole se podíváme na problém počtu reprezentací částky v systému mincí pomocí vytvořujících funkcí.

Počtem reprezentací částky a rozumíme počet různých n-tic, které jsou podle definice 1.1 reprezentací částky a.

Definice 2.1. *Vytvořující funkce posloupnosti* $\{a_n\}_{n=0}^{\infty}$ *je mocninná řada definovaná předpisem*

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots .$$

Vytvořující funkce představují jiný způsob pohledu na posloupnosti. Ze zápisu vytvořující funkce ve tvaru mocninné řady na první pohled vidíme prvky původní posloupnosti. Součet dvou vytvořujících funkcí sčítá koeficienty jednotlivých mocnin x. Odpovídá tedy sčítání dvou posloupností po složkách. Právě popsanou vlastnost zapíšeme pomocí následující věty.

Věta 2.2. *Mějme posloupnost* $\{a_n\}_{n=0}^{\infty}$ *s vytvořující funkcí* f *a posloupnost* $\{b_n\}_{n=0}^{\infty}$ *s vytvořující funkcí* g.

Vytvořující funkce posloupnosti $\{a_n + b_n\}_{n=0}^{\infty}$ *je* $f + g$.

Důkaz. Vyplývá z vlastností sčítání mocninných řad. □

Podíváme se ještě na operaci násobení.

Věta 2.3. *Mějme systém mincí a posloupnost* $\{a_n\}_{n=0}^{\infty}$ *takovou, že hodnota* a_i *vyjadřuje počet reprezentací částky* i *v systému mincí. Dále mějme druhý systém mincí, který nemá s prvním systémem žádnou společnou minci, a posloupnost* $\{b_n\}_{n=0}^{\infty}$ *takovou, že hodnota* b_j *vyjadřuje počet reprezentací částky* j *v druhém systému mincí. Nechť* f *je vytvořující funkce posloupnosti* $\{a_n\}_{n=0}^{\infty}$ *a* g *je vytvořující funkce posloupnosti* $\{b_n\}_{n=0}^{\infty}$.

Mějme dále posloupnost $\{c_n\}_{n=0}^{\infty}$ *takovou, že* c_i *je počet reprezentací částky* i *v systému mincí, který vznikl složením dvou dílčích podsystémů. Vytvořující funkce posloupnosti* $\{c_n\}_{n=0}^{\infty}$ *je rovna součinu vytvořujících funkcí* f *a* g.

Důkaz. Najdeme posloupnost, která má na n-tém místě hodnotu vyjadřující počet způsobů, jak rozměnit částku n v systému obsahujícím všechny mince z předchozích dvou systémů. Část částky n je pokaždé rozměněna pomocí mincí z prvního systému. Zbytek je rozměněn pomocí mincí z druhého systému. Pokud je pomocí prvního systému mincí rozměněna částka i, pak je pomocí druhého systému mincí rozměněna částka $n - i$ a počet způsobů, jak to udělat, je a_ib_{n-i}. Počet způsobů, jak v novém systému mincí rozměnit částku n, je tedy $c_n = \sum_{i=0}^{n} a_ib_{n-i}$.

Člen s x^n v součinu fg vypadá následovně:

$$\sum_{i=0}^{n} a_ix^ib_{n-i}x^{n-i} = \sum_{i=0}^{n} a_ib_{n-i}x^n$$

Součin f a g je tedy vytvořující funkcí posloupnosti $\{c_n\}_{n=0}^{\infty}$. □

Pro systémy s jedinou mincí je zjištění posloupnosti počtu způsobů reprezentace částky jednoduché. Například pro systém s jedinou mincí o hodnotě 3 je posloupnost počtu způsobů, jak reprezentovat částky

$$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, \dots).$$

První jednička přitom vyjadřuje, že částku 0 lze složit jediným způsobem. Obecně pro systémy s jedinou mincí o hodnotě c bude pro posloupnost počtu způsobů reprezentace $\{a_n\}_{n=0}^{\infty}$ platit

$$a_n = \begin{cases} 1 & \text{pokud } c \text{ dělí } n \\ 0 & \text{jinak.} \end{cases}$$

Vytvořující funkce této posloupnosti je

$$1 + x^c + x^{2c} + x^{3c} + \dots.$$

Věta 2.4. *Pro $x \in \mathbb{C}$ a $0 \leq |x| < 1$ a $c \in \mathbb{N}$ platí*

$$1 + x^c + x^{2c} + x^{3c} + \cdots = \frac{1}{1 - x^c}.$$

Důkaz. Připomeneme vzorec pro součet geometrické řady

$$1 + y + y^2 + y^3 + \cdots = \frac{1}{1 - y}.$$

Tvrzení věty nyní získáme dosazením $y = x^c$. □

Postupným skládáním systémů mincí pomocí násobení vytvořujících funkcí nyní umíme najít počet způsobů, jak reprezentovat částku v libovolném systému mincí.

Například pro systém mincí o hodnotách 3, 5 a 7 nyní stačí k nalezení posloupnosti počtu způsobů reprezentace jednotlivých částek vynásobit vytvořující funkce tří jednomincových systémů.

$$(1 + x^3 + x^6 + x^9 + \dots)(1 + x^5 + x^{10} + x^{15} + \dots)(1 + x^7 + x^{14} + x^{21} + \dots) =$$
$$= \frac{1}{1 - x^3} \frac{1}{1 - x^5} \frac{1}{1 - x^7}$$

Výsledný výraz dále potřebujeme upravit zpět do tvaru mocninné řady, ve které koeficient u x^n určuje n-tý prvek hledané posloupnosti. Tomuto problému se budeme věnovat v následujících částech.

2.1 Pro dvě mince

V této části se budeme zabývat hledáním počtu způsobů, jak reprezentovat libovolnou částku v systému mincí o dvou nesoudělných hodnotách. Při psaní této části čerpáme z publikace [4, kap. 1].

2.1.1 Odvození pomocí vytvořujících funkcí

Pomocí vytvořujících funkcí nyní odvodíme vztah pro nalezení počtu reprezentací částek pro systémy mincí o dvou mincích s nesoudělnými hodnotami.

Mějme systém mincí o nesoudělných hodnotách a, b. Posloupnost počtu reprezentací částek pro tento systém mincí označíme $\{c_n\}_{n=0}^{\infty}$.

K nalezení členů této posloupnosti využijeme součin vytvořujících funkcí posloupností jednomincových systémů s mincemi o hodnotách a a b. Hledáme tedy koeficienty $c_0, c_1, c_2, \ldots \in \mathbb{N}_0$ takové, že

$$\frac{1}{(1-x^a)(1-x^b)} = c_0 + c_1 x + c_2 x^2 + \ldots .$$

Nechť $p \in \mathbb{N}_0$ je libovolné pevně zvolené číslo. Hledání koeficientu c_p můžeme zjednodušit tak, že budeme hledat konstantní člen výrazu

$$f(x) = \frac{1}{(1-x^a)(1-x^b)x^p} = \frac{c_0}{x^p} + \frac{c_1}{x^{p-1}} + \cdots + c_p + c_{p+1}x + c_{p+2}x^2 + \ldots .$$

Připomeňme známou větu o rozkladu racionální funkce na parciální zlomky, kterou následně aplikujeme na funkci f.

Věta 2.5 (Rozklad na parciální zlomky)**.** *Každou funkci ve tvaru*

$$f(x) = \frac{p(x)}{(x-a_1)^{e_1}(x-a_2)^{e_2}\cdots(x-a_n)^{e_n}},$$

kde $p(x)$ je polynom stupně nejvýše $e_1 + e_2 + \cdots + e_n$ a $e_1, e_2, \ldots, e_n \in \mathbb{N}$, můžeme zapsat ve tvaru

$$f(x) = \sum_{k=1}^{n} \left(\frac{C_{k,1}}{x-a_k} + \frac{C_{k,2}}{(x-a_k)^2} + \cdots + \frac{C_{k,e_k}}{(x-a_k)^{e_k}} \right),$$

kde koeficienty $C_{k,j} \in \mathbb{C}$ jsou určeny jednoznačně.

Důkaz. Důkaz zde neuvádíme. Je k dispozici například v [13, věta 57]. □

K nalezení rozkladu funkce f potřebujeme nejprve najít všechny kořeny polynomu $(1-x^a)(1-x^b)x^p$ v oboru komplexních čísel.

Kořeny polynomu $1 - x^k$ jsou všechny k-té odmocniny z 1, tedy komplexní čísla $1, \xi_k, \xi_k^2, \ldots, \xi_k^{k-1}$, kde

$$\xi_k = \cos\frac{2\pi}{k} + i\sin\frac{2\pi}{k}.$$

Všechny kořeny polynomu $(1-x^a)(1-x^b)x^p$ a jejich násobnosti jsou tedy

- kořen $x = 0$ s násobností p,
- kořen $x = 1$ s násobností 2,
- kořeny $\xi_a, \xi_a^2, \ldots, \xi_a^{a-1}$ s násobností 1,
- kořeny $\xi_b, \xi_b^2, \ldots, \xi_b^{b-1}$ s násobností 1.

Kořeny ξ_a^k a ξ_b^l jsou pro všechna $k \in \{1, 2, \dots, a-1\}$ a $l \in \{1, 2, \dots, b-1\}$ různé, protože a a b jsou nesoudělná čísla.

Pro nalezení rozkladu funkce f na parciální zlomky hledáme konstanty

$$A_1, A_2, \dots, A_p, B_1, B_2, C_1, C_2, \dots, C_{a-1}, D_1, D_2, \dots, D_{b-1}$$

takové, že

$$\begin{aligned}\frac{1}{(1-x^a)(1-x^b)x^p} = \frac{A_1}{x} + \frac{A_2}{x^2} + \dots + \frac{A_p}{x^p} + \frac{B_1}{x-1} + \frac{B_2}{(x-1)^2} +& \\ + \frac{C_1}{x-\xi_a} + \frac{C_2}{x-\xi_a^2} + \dots + \frac{C_{a-1}}{x-\xi_a^{a-1}} +& \\ + \frac{D_1}{x-\xi_b} + \frac{D_2}{x-\xi_b^2} + \dots + \frac{D_{b-1}}{x-\xi_b^{b-1}}.&\end{aligned} \tag{2.1}$$

Z definice funkce f plyne, že platí $A_1 = c_{p-1}, A_2 = c_{p-2}, \dots, A_p = c_0$. Uvidíme, že pro nalezení c_p nejsou hodnoty těchto konstant podstatné.

Najdeme konstantu B_2. Obě strany rovnice (2.1) vynásobíme výrazem $(x-1)^2$, čímž získáme

$$\begin{aligned}\frac{(x-1)^2}{(1-x^a)(1-x^b)x^p} = \sum_{k=1}^{p} \frac{A_k(x-1)^2}{x^k} + B_1(x-1) + B_2 +& \\ + \sum_{k=1}^{a-1} \frac{C_k(x-1)^2}{x-\xi_a^k} + \sum_{k=1}^{b-1} \frac{D_k(x-1)^2}{x-\xi_b^k}.&\end{aligned}$$

Limita pravé strany pro x jdoucí k 1 je B_2. Platí proto

$$\begin{aligned}B_2 &= \lim_{x\to 1} \frac{(x-1)^2}{(1-x^a)(1-x^b)x^p} \\ &= \lim_{x\to 1} \frac{(x-1)^2}{(1-x)(1+x+\dots+x^{a-1})(1-x)(1+x+\dots+x^{b-1})x^p} = \frac{1}{ab}.\end{aligned}$$

Konstantu B_1 získáme podobným způsobem. Obě strany rovnice (2.1) vynásobíme $x-1$, čímž získáme

$$\begin{aligned}\frac{x-1}{(1-x^a)(1-x^b)x^p} = \sum_{k=1}^{p} \frac{A_k(x-1)}{x^k} + B_1 + \frac{B_2}{x-1} +& \\ + \sum_{k=1}^{a-1} \frac{C_k(x-1)}{x-\xi_a^k} + \sum_{k=1}^{b-1} \frac{D_k(x-1)}{x-\xi_b^k}.&\end{aligned}$$

Po odečtení $B_2/(x-1)$ od obou stran rovnice je limita pravé strany pro x jdoucí k 1 rovna B_1. Platí proto

$$\begin{aligned}B_1 &= \lim_{x\to 1} \frac{x-1}{(1-x^a)(1-x^b)x^p} - \frac{\frac{1}{ab}}{x-1} = \lim_{x\to 1} \frac{(x-1)^2 - \frac{1}{ab}(1-x^a)(1-x^b)x^p}{(1-x^a)(1-x^b)(x-1)x^p} \\ &= \lim_{x\to 1} \frac{(x-1)^2 - \frac{1}{ab}(1-x)(1+x+\dots+x^{a-1})(1-x)(1+x+\dots+x^{b-1})x^p}{(1-x)\underbrace{(1+x+\dots+x^{a-1})}_{\to a}(1-x)\underbrace{(1+x+\dots+x^{b-1})}_{\to b}(x-1)\underbrace{x^p}_{\to 1}}.\end{aligned}$$

Zkrátíme $(x-1)^2$ a pomocí věty o aritmetice limit [12, věta 106] získáme

$$B_1 = \frac{-1}{ab} \lim_{x \to 1} \frac{\frac{1}{ab}(1+x+\cdots+x^{a-1})(1+x+\cdots+x^{b-1})x^p - 1}{x-1}$$

Definujme funkci h předpisem

$$h(x) = \frac{1}{ab}(1+x+\cdots+x^{a-1})(1+x+\cdots+x^{b-1})x^p.$$

Platí $h(1)=1$, tedy

$$B_1 = \frac{-1}{ab} \lim_{x \to 1} \frac{h(x)-h(1)}{x-1} = \frac{-1}{ab} h'(1).$$

Vypočítáme derivaci funkce h podle pravidla o derivování součinu:

$$\begin{aligned} h'(x) = \frac{1}{ab}\big(&(1+2x+3x^2+\cdots+(a-1)x^{a-2})(1+x^2+x^3+\cdots+x^{b-1})x^p + \\ &+ (1+x^2+x^3+\cdots+x^{a-1})(1+2x+3x^2+\cdots+(b-1)x^{b-2})x^p + \\ &+ (1+x^2+x^3+\cdots+x^{a-1})(1+x^2+x^3+\cdots+x^{b-1})px^{p-1}\big) \end{aligned}$$

Hodnota B_1 je tedy

$$\begin{aligned} B_1 &= \frac{-1}{ab}\left(\frac{(1+2+\cdots+(a-1))b}{ab} + \frac{a(1+2+\cdots+(b-1))}{ab} + \frac{abp}{ab}\right) \\ &= \frac{-1}{ab}\left(\frac{a-1}{2} + \frac{b-1}{2} + p\right) = \frac{1}{ab} - \frac{1}{2a} - \frac{1}{2b} - \frac{p}{ab}. \end{aligned}$$

Koeficienty C_k získáme analogicky. Budeme hledat koeficient C_l. Vynásobením obou stran rovnice (2.1) výrazem $x - \xi_a^l$ získáme

$$\begin{aligned} \frac{x-\xi_a^l}{(1-x^a)(1-x^b)x^p} = &\sum_{k=1}^{p} \frac{A_k(x-\xi_a^l)}{x^k} + \frac{B_1(x-\xi_a^l)}{x-1} + \frac{B_2(x-\xi_a^l)}{(x-1)^2} + \\ &+ \sum_{k=1}^{l-1} \frac{C_k(x-\xi_a^l)}{x-\xi_a^k} + C_l + \sum_{k=l+1}^{a-1} \frac{C_k(x-\xi_a^l)}{x-\xi_a^k} + \sum_{k=1}^{b-1} \frac{D_k(x-\xi_a^l)}{x-\xi_b^k}. \end{aligned}$$

Limita pravé strany pro x jdoucí k ξ_l je C_l. Platí proto

$$\begin{aligned} C_l &= \lim_{x \to \xi_a^l} \frac{x-\xi_a^l}{(1-x^a)(1-x^b)x^p} = \frac{1}{\xi_a^{lp}(1-\xi_a^{lb})} \lim_{x \to \xi_a^l} \frac{x-\xi_a^l}{1-x^a} \\ &\overset{\text{L'H}}{=} \frac{1}{\xi_a^{lp}(1-\xi_a^{lb})} \frac{-1}{a\xi_a^{l(a-1)}} \end{aligned}$$

V druhém kroku výpočtu jsme použili L'Hospitalovo pravidlo na limitu ve tvaru „$\frac{0}{0}$“. Platí, že $\xi_a^a = 1$, neboť ξ_a je a-tá odmocnina jedničky. Proto

$$\xi_a^{lp}\xi_a^{l(a-1)} = \xi_a^{la}\xi_a^{lp-l} = \xi_a^{l(p-1)}.$$

Použitím popsaných úprav získáme

$$C_l = \frac{-1}{a\xi_a^{l(p-1)}(1-\xi_a^{lb})}.$$

Stejným postupem zjistíme, že

$$D_l = \frac{-1}{b\xi_b^{l(p-1)}(1-\xi_b^{la})}.$$

Uvažujme nyní funkci g definovanou předpisem

$$g(x) = c_p + c_{p+1}x + c_{p+2}x^2 + \cdots.$$

Naším cílem je najít hodnotu $c_p = g(0)$. Pro $x \neq 0$ platí

$$\begin{aligned} g(x) = f(x) - \frac{c_0}{x^p} - \cdots - \frac{c_{p-1}}{x} &= \frac{B_1}{x-1} + \frac{B_2}{(x-1)^2} + \\ &+ \frac{C_1}{x-\xi_a} + \frac{C_2}{x-\xi_a^2} + \cdots + \frac{C_{a-1}}{x-\xi_a^{a-1}} + \\ &+ \frac{D_1}{x-\xi_b} + \frac{D_2}{x-\xi_b^2} + \cdots + \frac{D_{b-1}}{x-\xi_b^{b-1}}. \end{aligned} \tag{2.2}$$

Na levé i na pravé straně předchozího vztahu jsou funkce spojité v nule, limitním přechodem $x \to 0$ tedy dospějeme k rovnosti

$$c_p = g(0) = -B_1 + B_2 - \frac{C_1}{\xi_a} - \frac{C_2}{\xi_a^2} - \cdots - \frac{C_{a-1}}{\xi_a^{a-1}} - \frac{D_1}{\xi_b} - \frac{D_2}{\xi_b^2} - \cdots - \frac{D_{b-1}}{\xi_b^{b-1}}.$$

Dosazením za konstanty B_i, C_j, D_k získáme

$$c_p = g(0) = \frac{1}{2a} + \frac{1}{2b} + \frac{p}{ab} + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\xi_a^{kp}(\xi_a^{kb}-1)} + \frac{1}{b}\sum_{k=1}^{b-1} \frac{1}{\xi_b^{kp}(\xi_b^{ka}-1)}. \tag{2.3}$$

Našli jsme výraz udávající počet způsobů reprezentace c_p částky p v systému s nesoudělnými hodnotami a, b.

Pokusíme se nalezený vzorec (2.3) dále zjednodušit. Začneme hledáním jednoduššího způsobu zápisu pro

$$\frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\xi_a^{kp}(\xi_a^{kb}-1)}. \tag{2.4}$$

Podíváme se na systém mincí o hodnotách a a 1. Počet způsobů, jak reprezentovat částku p, označíme c'_p. Každá reprezentace částky p použije k krát minci o hodnotě a a zbytek částky doplní mincemi o hodnotě 1. Počet způsobů reprezentace p je tedy roven počtu možností, jak zvolit $k \in \mathbb{N}_0$, aby $ka < p$ a tedy i $k < p/a$. Proto platí

$$c'_p = \left\lfloor \frac{p}{a} \right\rfloor + 1. \tag{2.5}$$

Symbol $\lfloor x \rfloor$ přitom označuje dolní celou část $x \in \mathbb{R}$, tj. největší celé číslo menší nebo rovné x.

Počet způsobů reprezentace částky p můžeme získat i dosazením $b = 1$ do vztahu (2.3):

$$c'_p = \frac{1}{2a} + \frac{1}{2} + \frac{p}{a} + \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\xi_a^{kp}(\xi_a^{k}-1)} \tag{2.6}$$

Z výrazů (2.5) a (2.6) vyjádříme

$$\frac{1}{a}\sum_{k=1}^{a-1}\frac{1}{\xi_a^{kp}(\xi_a^k-1)} = -\left\{\frac{p}{a}\right\}+\frac{1}{2}-\frac{1}{2a}. \tag{2.7}$$

Značení $\{x\}$ zde má význam desetinné části čísla x, tedy $\{x\} = x - \lfloor x \rfloor$.

Hledaný výraz (2.4) stále není ve stejném tvaru jako (2.7). Předtím, než ho do podobného tvaru upravíme, ukážeme některé vlastnosti čísla ξ_a. Z Moivreovy věty plyne

$$\xi_a^k = \cos\frac{2\pi k}{a} + i\sin\frac{2\pi k}{a}.$$

Z periodicity goniometrických funkcí proto dostáváme, že

$$\xi_a^k = \xi_a^{k \mod a}. \tag{2.8}$$

Lemma 2.6. *Mějme nesoudělná čísla $m, a \in \mathbb{N}$ a $k \in \{1, 2, \dots, a-1\}$. Potom*

$$mk \mod a \neq 0.$$

Důkaz. Předpokládejme pro spor, že $mk \mod a = 0$, tedy a dělí mk. Odtud a z předpokladu nesoudělnosti a a m plyne, že a dělí k.

Žádná z možných hodnot k ale není dělitelná a, čímž získáváme spor. □

Lemma 2.7. *Pro nesoudělná čísla $a, m \in \mathbb{N}_0$ platí*

$$\{\xi_a^k; k \in \{1, 2, \dots, a-1\}\} = \{\xi_a^{mk}; k \in \{1, 2, \dots, a-1\}\}.$$

Důkaz. Ze vztahu (2.8) vidíme, že stačí dokázat

$$\{k; k \in \{1, 2, \dots, a-1\}\} = \{mk \mod a; k \in \{1, 2, \dots, a-1\}\}.$$

Z vlastností zbytku po dělení plyne $mk \mod a \in \{0, 1, \dots, a-1\}$. Z lemmatu 2.6 dále plyne, že $mk \mod a \neq 0$. Zbývá tedy dokázat, že pro $u, v \in \{1, 2, \dots, a-1\}$ a $u \neq v$ platí

$$mu \mod a \neq mv \mod a.$$

Předpokládejme pro spor, že

$$mu \equiv mv \pmod a.$$

Z předchozí kongruence plyne, že a dělí $m(u-v)$. Protože a, m jsou nesoudělná, a dělí $u - v$ a platí

$$\begin{aligned} u &\equiv v \pmod a \\ u &= v + ka, \end{aligned}$$

pro $k \in \mathbb{Z}$. Odtud a z předpokladu $u, v \in \{1, 2, \dots, a-1\}$ plyne, že $u = v$. □

Důsledek 2.8. *Pro libovolnou funkci $h : \mathbb{C} \to \mathbb{C}$ a nesoudělná čísla $a, m \in \mathbb{N}$ platí*

$$\sum_{j=1}^{a-1} h(\xi_a^j) = \sum_{j=1}^{a-1} h(\xi_a^{jm}).$$

Lemma 2.9. *Mějme dvě nesoudělná čísla $a, b \in \mathbb{N}$ a číslo $b' \in \mathbb{N}$ takové, že*

$$bb' \equiv 1 \pmod{a}.$$

Potom jsou a a b' nesoudělná.

Důkaz. Označíme c libovolného společného dělitele a a b'. Existují tedy $k, l \in \mathbb{Z}$ takové, že $a = kc$, $b' = lc$.

Obě strany druhé rovnosti vynásobíme b, čímž získáme

$$bb' = blc.$$

Z předpokladu věty a následného dosazení za a plyne

$$bb' = 1 + ua = 1 + ukc,$$

pro nějaké $u \in \mathbb{Z}$. Z toho získáme

$$1 = blc - ukc = c(bl - uk).$$

Zjistili jsme tedy, že libovolný společný dělitel c čísel a, b', dělí 1. Čísla a, b' jsou tedy nesoudělná. □

Lemma 2.10. *Mějme $a, m \in \mathbb{N}_0$ nesoudělná a $m > 0$. Potom existuje a' takové, že $aa' \equiv 1 \pmod{m}$ a platí*

$$a' \equiv a^{\varphi(m)-1} \pmod{m},$$

kde φ je Eulerova funkce [23, str. 19].

Důkaz. Podle Eulerovy věty [23, věta 3.10] platí

$$1 \equiv a^{\varphi(m)} = aa^{\varphi(m)-1} \pmod{m}.$$

Odtud plyne požadovaný vztah. □

Zavedeme funkci h s předpisem

$$h(x) = \frac{1}{x^p(x^b - 1)}.$$

Hledaný výraz (2.4) je roven

$$\frac{1}{a}\sum_{k=1}^{a-1} h(\xi_a^k).$$

Volme nyní b' takové, že $bb' \equiv 1 \pmod{a}$. Takové b' podle lemmatu 2.10 existuje, protože a, b jsou nesoudělná. Podle důsledku 2.8 platí

$$\frac{1}{a}\sum_{k=1}^{a-1} h(\xi_a^k) = \frac{1}{a}\sum_{k=1}^{a-1} h(\xi_a^{kb'}) = \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\xi_a^{kpb'}(\xi_a^k - 1)}.$$

Použitím vztahu (2.7), kde místo p píšeme pb', získáme

$$\frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\xi_a^{kp}(\xi_a^{kb} - 1)} = \frac{1}{a}\sum_{k=1}^{a-1} \frac{1}{\xi_a^{kpb'}(\xi_a^k - 1)} = -\left\{\frac{pb'}{a}\right\} + \frac{1}{2} - \frac{1}{2a}. \tag{2.9}$$

Stejným způsobem můžeme zjednodušit druhou sumu z výrazu (2.3): Zkoumáním systému mincí o hodnotách $1, b$ bychom došli k závěru, že

$$\frac{1}{b}\sum_{k=1}^{b-1}\frac{1}{\xi_b^{kp}(\xi_b^{ka}-1)} = -\left\{\frac{pa'}{b}\right\} + \frac{1}{2} - \frac{1}{2b}. \tag{2.10}$$

Dosazením získaných výrazů do (2.3) obdržíme následující větu.

Věta 2.11. *Počet reprezentací částky p v systému mincí o nesoudělných hodnotách $a, b \in \mathbb{N}$ je*

$$c_p = \frac{p}{ab} + 1 - \left\{\frac{pb'}{a}\right\} - \left\{\frac{pa'}{b}\right\},$$

kde $a', b' \in \mathbb{N}$ a

$$\begin{aligned} aa' &\equiv 1 \pmod{b} \\ bb' &\equiv 1 \pmod{a}. \end{aligned}$$

Důkaz. Větu jsme odvodili výše. □

Příklad 2.12. *Zjistěte počet reprezentací částky 42 v systému mincí o hodnotách 5 a 7.*

Řešení. Příklad vyřešíme dvěma způsoby. Nejprve odhadneme řešení prostým zkoušením. Potom najdeme počet způsobů použitím věty 2.11.

Po krátkém zkoušení zjistíme, že částku 42 můžeme reprezentovat pomocí šesti mincí o hodnotě 7, nebo pomocí jedné mince o hodnotě 7 a sedmi mincí o hodnotě 5. Našli jsme tedy dva způsoby, jak částku reprezentovat.

Dalším zkoušením bychom jistě přišli i na to, že žádný jiný způsob reprezentace není. Pojďme tuto skutečnost ověřit ještě pomocí věty 2.11.

Víme, že $a = 5, b = 7$ a $p = 42$. Platí $a' = 3$, neboť $\varphi(7) = 6$ a podle lemmatu 2.10

$$a' = a^{\varphi(b)-1} \mod b = 5^5 \mod 7 = 3.$$

Použitím stejného lemmatu zjistíme, že $b' = 3$, protože

$$7^3 \mod 5 = 3.$$

Zbývá tedy dosadit do vzorce ve větě 2.11 a vypočítat výsledek:

$$\begin{aligned} c_{42} &= \frac{42}{35} + 1 - \left\{\frac{42\cdot 3}{5}\right\} - \left\{\frac{42\cdot 3}{7}\right\} \\ &= \frac{42}{35} + 1 - \left\{\frac{126}{5}\right\} - \{6\cdot 3\} = \frac{42}{35} + 1 - \frac{1}{5} = 2 \end{aligned}$$

Počet způsobů, jak reprezentovat částku 42, je roven 2.

Příklad 2.13. *Zjistěte počet reprezentací částky 171 v systému mincí o hodnotách 9 a 30.*

Řešení. Čísla 9 a 30 nejsou nesoudělná. Nemůžeme proto použít větu 2.11.

Vydělíme-li hodnoty mincí jejich největším společným dělitelem tj. číslem 3, získáme systém mincí o nesoudělných hodnotách 3 a 10. Každá reprezentace částky $171/3 = 57$ v novém systému mincí je potom reprezentací částky 171 v původním systému mincí a naopak.

Počet reprezentací částky 171 v původním systému mincí je proto stejný jako počet reprezentací částky 57 v novém systému mincí. Vlastně jde o zobecnění věty 1.4.

Zbývá tedy určit počet reprezentací pro $a = 3, b = 10$ a $p = 57$. Podle lemmatu 2.10 platí $a' = 3^3 \mod 10 = 7$ a $b' = 10^1 \mod 3 = 1$. Použitím věty 2.11 získáme

$$c_{57} = \frac{57}{30} + 1 - \left\{\frac{57 \cdot 1}{3}\right\} - \left\{\frac{57 \cdot 7}{10}\right\} = \frac{57}{30} + 1 - \frac{9}{10} = 2.$$

Počet reprezentací částky 171 v systému mincí o hodnotách 9 a 30 je tedy 2.

Kdybychom v předchozím příkladu požadovali počet reprezentací částky, která není dělitelná třemi, mohli bychom podle věty 1.3 odpovědět, že počet reprezentací je roven 0.

2.1.2 Počet nereprezentovatelných částek a největší z nich

Pomocí vzorce pro získání počtu reprezentací částky z věty 2.11 nyní zjistíme počet nereprezentovatelných částek a největší nereprezentovatelnou částku v systému mincí o dvou nesoudělných hodnotách a, b.

Nejprve najdeme největší nereprezentovatelnou částku. Vlastně znovu zformulujeme větu 1.18. Pro důkaz ale tentokrát použijeme poznatky z této kapitoly.

Věta 2.14. *V systému mincí o nesoudělných hodnotách $a, b \in \mathbb{N}$ je největší nereprezentovatelná částka rovna*

$$ab - a - b.$$

Důkaz. Potřebujeme ukázat, že $ab - a - b$ není reprezentovatelná, a že každá větší částka reprezentovatelná je. Pro počet reprezentací c_{ab-a-b} platí

$$c_{ab-a-b} = \frac{ab - a - b}{ab} + 1 - \left\{\frac{(ab - a - b)b'}{a}\right\} - \left\{\frac{(ab - a - b)a'}{b}\right\}.$$

Nejprve upravíme

$$\left\{\frac{(ab - a - b)b'}{a}\right\} = \left\{b - 1 - \frac{bb'}{a}\right\} = \left\{b - 1 - ka - \frac{1}{a}\right\}.$$

Poslední rovnost využívá toho, že pro nějaké $k \in \mathbb{N}_0$ je $bb' = 1 + ka$. To vyplývá přímo ze zavedení b' pomocí kongruence. Dále si uvědomíme, že

$$\left\{b - 1 - ka - \frac{1}{a}\right\} = \left\{1 - \frac{1}{a}\right\} = 1 - \frac{1}{a}$$

Podobně bychom zjistili, že

$$\left\{\frac{(ab-a-b)a'}{b}\right\} = \left\{a-1-\frac{aa'}{b}\right\} = \left\{a-1-kb-\frac{1}{b}\right\} = 1-\frac{1}{b}.$$

Po dosazení získáme

$$c_{ab-a-b} = \frac{ab-a-b}{ab} + 1 - 1 + \frac{1}{a} - 1 + \frac{1}{b} = 0.$$

Zbývá dokázat, že každá větší částka je reprezentovatelná, tedy že pro $n \in \mathbb{N}$ platí $c_{ab-a-b+n} > 0$. Využijeme toho, že pro $m \in \mathbb{Z}$ platí

$$\left\{\frac{m}{a}\right\} \leq \frac{a-1}{a}.$$

Nyní odhadneme $c_{ab-a-b+n}$.

$$c_{ab-a-b+n} \geq \frac{ab-a-b+n}{ab} + 1 - \frac{a-1}{a} - \frac{b-1}{b} = \frac{n}{ab} > 0.$$

□

Nyní najdeme počet nereprezentovatelných částek v systému mincí o nesoudělných hodnotách a, b.

Lemma 2.15. *Pro $x \in \mathbb{R}$, $x \notin \mathbb{Z}$ platí $\{-x\} = 1 - \{x\}$.*

Důkaz. Výraz rozepíšeme pomocí definice $\{x\}$.

$$\{-x\} = -x - \lfloor -x \rfloor = -x - (-\lfloor x \rfloor - 1) = 1 - (x - \lfloor x \rfloor) = 1 - \{x\}$$

V druhém kroku využíváme toho, že pro $x \notin \mathbb{Z}$ platí $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$. □

Lemma 2.16. *Mějme systém dvou mincí o nesoudělných hodnotách $a, b \in \mathbb{N}$ a číslo $n \in \{1, 2, \dots, ab-1\}$, které není násobkem a ani b.*

Potom je právě jedna z částek n a $ab-n$ reprezentovatelná.

Důkaz. Dokážeme, že součet počtů reprezentací čísel n a $ab-n$ je 1, tedy

$$c_n + c_{ab-n} = 1.$$

Budeme upravovat výraz c_{ab-n}.

$$\begin{aligned} c_{ab-n} &= \frac{ab-n}{ab} + 1 - \left\{\frac{(ab-n)b'}{a}\right\} - \left\{\frac{(ab-n)a'}{b}\right\} \\ &= 2 - \frac{n}{ab} - \left\{b - \frac{nb'}{a}\right\} - \left\{a - \frac{na'}{b}\right\} \\ &= 2 - \frac{n}{ab} - \left\{-\frac{nb'}{a}\right\} - \left\{-\frac{na'}{b}\right\} \end{aligned}$$

Dále můžeme použít lemma 2.15, protože n není násobkem a ani b:

$$\begin{aligned} c_{ab-n} &= 2 - \frac{n}{ab} - \left\{-\frac{nb'}{a}\right\} - \left\{-\frac{na'}{b}\right\} = -\frac{n}{ab} + \left\{\frac{nb'}{a}\right\} + \left\{\frac{na'}{b}\right\} \\ &= 1 - \left(\frac{n}{ab} + 1 - \left\{\frac{nb'}{a}\right\} - \left\{\frac{na'}{b}\right\}\right) = 1 - c_n \end{aligned}$$

□

Nyní zopakujeme větu 1.9 a dokážeme jí pomocí poznatků z této kapitoly.

Věta 2.17. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná, pak počet všech nereprezentovatelných částek menších než ab je*

$$\frac{(a-1)(b-1)}{2}.$$

Důkaz. Všech částek $n \in \{1, 2, \ldots, ab-1\}$ je $ab-1$. Z nich $a-1$ je násobkem b a $b-1$ je násobkem a. Z nesoudělnosti a a b plyne, že žádné není společným násobkem a i b.

Částek $n \in \{1, 2, \ldots, ab-1\}$, které nejsou násobkem a ani b je proto

$$ab - 1 - (a-1) - (b-1) = a(b-1) - (b-1) = (a-1)(b-1).$$

Podle lemmatu 2.16 je právě polovina z nich nereprezentovatelná. □

2.2 Pro více mincí

V této části odvodíme způsob výpočtu počtu reprezentací libovolné částky v systému s více než dvěma mincemi. Neočekáváme přitom, že se nám podaří najít zcela obecný a efektivní způsob řešení této úlohy. Kdybychom takový způsob našli, dokázali bychom efektivně řešit NP-úplný problém reprezentovatelnosti z části 1.4.2, a tedy i všechny ostatní NP-úplné problémy.

2.2.1 Pomocí rozkladu na parciální zlomky

Postup, který jsme použili v předchozí části o dvoumincových systémech, funguje z velké části i pro systémy s více mincemi. Ukážeme, které části postupu lze použít i v obecném případě a které části narážejí na problémy. Při psaní této části opět čerpáme z publikace [4, kap. 1].

Mějme systém mincí o hodnotách $a_1, a_2, \ldots, a_n \in \mathbb{N}$. Předpokládejme navíc, že hodnoty mincí jsou po dvou nesoudělné. Vytvořující funkce posloupnosti počtu reprezentací částek $\{c_k\}_{k=0}^{\infty}$ je

$$\frac{1}{(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})}.$$

Počet reprezentací c_p částky p je roven konstantnímu členu výrazu

$$\begin{aligned} f(x) &= \frac{1}{x^p(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})} \\ &= \frac{c_0}{x^p} + \frac{c_1}{x^{p-1}} + \cdots + c_p + c_{p+1}x + c_{p+2}x^2 + \cdots. \end{aligned}$$

Pro úpravu funkce f do tvaru mocninné řady jí rozložíme na parciální zlomky. Kořeny polynomu $x^p(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})$ a jejich násobnosti jsou

- kořen 0 s násobností p,
- kořen 1 s násobností n,
- kořeny $\xi_{a_k}^j$ pro $k \in \{1, \ldots, n\}, j \in \{1, \ldots, a_k - 1\}$ s násobností 1.

Kořeny $\xi_{a_k}^j$ a $\xi_{a_l}^m$ jsou pro $j \in \{1, \dots, a_k - 1\}$, $m \in \{1, \dots, a_l - 1\}$ a $k \neq l$ různé, což plyne z předpokladu nesoudělnosti a_k a a_l.

Rozklad funkce f na parciální zlomky hledáme ve tvaru

$$\begin{aligned} f(x) = \frac{1}{x^p(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})} = \sum_{j=1}^{p} \frac{A_j}{x^j} + \sum_{k=1}^{n} \frac{B_k}{(x-1)^k} + \\ + \sum_{l=1}^{a_1-1} \frac{C_{1,l}}{x-\xi_{a_1}^l} + \sum_{l=1}^{a_2-1} \frac{C_{2,l}}{x-\xi_{a_2}^l} + \dots + \sum_{l=1}^{a_n-1} \frac{C_{n,l}}{x-\xi_{a_n}^l}. \end{aligned} \tag{2.11}$$

Z definice f plyne stejně jako v případě dvoumincového systému, že $A_j = c_{p-j}$. Koeficienty $C_{k,l}$ získáme podobně jako v případě dvoumincového systému. Celou rovnici vynásobíme výrazem $x - \xi_{a_k}^l$. Následným limitním přechodem zjistíme, že

$$\begin{aligned} C_{k,l} &= \lim_{x \to \xi_{a_k}^l} \frac{x - \xi_{a_k}^l}{x^p(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})} \\ &= \frac{1}{\xi_{a_k}^{lp}(1-\xi_{a_k}^{la_1})\cdots(1-\xi_{a_k}^{la_{k-1}})(1-\xi_{a_k}^{la_{k+1}})\cdots(1-\xi_{a_k}^{la_n})} \lim_{x \to \xi_{a_k}^l} \frac{x-\xi_{a_k}^l}{1-x^{a_k}} \\ &\overset{L'H}{=} \frac{-1}{\xi_{a_k}^{lp}(1-\xi_{a_k}^{la_1})\cdots(1-\xi_{a_k}^{la_{k-1}})(1-\xi_{a_k}^{la_{k+1}})\cdots(1-\xi_{a_k}^{la_n})a_k\xi_{a_k}^{l(a_k-1)}} \\ &= \frac{-1}{\xi_{a_k}^{l(p-1)}(1-\xi_{a_k}^{la_1})(1-\xi_{a_k}^{la_2})\cdots(1-\xi_{a_k}^{la_{k-1}})(1-\xi_{a_k}^{la_{k+1}})\cdots(1-\xi_{a_k}^{la_n})}. \end{aligned} \tag{2.12}$$

V druhém kroku jsme použili L'Hospitalovo pravidlo na výraz ve tvaru „$\frac{0}{0}$“.

Výpočet koeficientů $B_1, B_2, \dots, B_n$ je složitější. Podrobně ho zde rozepisovat nebudeme. Pro konkrétní hodnotu n bychom k jejich výpočtu mohli použít například program `Mathematica`. Například pro trojmincové systémy tímto způsobem postupně vypočítáme B_3, B_2 a B_1:

$$\begin{aligned} B_3 &= \lim_{x \to 1} \frac{(x-1)^3}{x^p(1-x^{a_1})(1-x^{a_2})(1-x^{a_3})} = \frac{-1}{a_1a_2a_3} \\ B_2 &= \lim_{x \to 1} \frac{(x-1)^2}{x^p(1-x^{a_1})(1-x^{a_2})(1-x^{a_3})} - \frac{B_3}{x-1} \\ &= \frac{a_1+a_2+a_3+2p-3}{2a_1a_2a_3} \\ B_1 &= \lim_{x \to 1} \frac{x-1}{x^p(1-x^{a_1})(1-x^{a_2})(1-x^{a_3})} - \frac{B_3}{(x-1)^2} - \frac{B_2}{x-1} \\ &= -\frac{a_1^2+3a_1(a_2+a_3+2p-2)+a_2^2+3a_2(a_3+2p-2)}{12a_1a_2a_3} - \\ &- \frac{a_3^2+6a_3p-6a_3+6p^2-12p+6}{12a_1a_2a_3} \end{aligned} \tag{2.13}$$

Podobně jako v případě dvoumincového systému nyní definujeme funkci g předpisem

$$g(x) = c_p + c_{p+1}x + c_{p+2} + \cdots,$$

pro kterou platí

$$g(x) = f(x) - \sum_{j=1}^{p} \frac{c_{p-j}}{x^j} = \sum_{k=1}^{n} \frac{B_k}{(x-1)^k} +$$
$$+ \sum_{l=1}^{a_1-1} \frac{C_{1,l}}{x - \xi_{a_1}^l} + \sum_{l=1}^{a_2-1} \frac{C_{2,l}}{x - \xi_{a_2}^l} + \cdots + \sum_{l=1}^{a_n-1} \frac{C_{n,l}}{x - \xi_{a_n}^l}.$$

Pomocí funkce g nyní najdeme c_p:

$$c_p = g(0) = \sum_{k=1}^{n} (-1)^k B_k - \sum_{l=1}^{a_1-1} \frac{C_{1,l}}{\xi_{a_1}^l} - \sum_{l=1}^{a_2-1} \frac{C_{2,l}}{\xi_{a_2}^l} - \cdots - \sum_{l=1}^{a_n-1} \frac{C_{n,l}}{\xi_{a_n}^l}. \tag{2.14}$$

Při hledání počtu reprezentací částky ve dvoumincovém systému jsme pokračovali zjednodušením sum obsahujících $\xi_{a_k}^l$. V obecném případě stejný postup neuspěje. Nalezené řešení navíc platí pouze pro systémy minci, jejichž hodnoty jsou po dvou nesoudělné.

Příklad 2.18. *Odvoďte vzorec pro získání počtu reprezentací částky p v systému mincí o hodnotách* $6, 9$ *a* 20.

Řešení. Ze vztahu (2.14) plyne

$$c_p = -B_1 + B_2 - B_3 - \sum_{l=1}^{a_1-1} \frac{C_{1,l}}{\xi_{a_1}^l} - \sum_{l=1}^{a_2-1} \frac{C_{2,l}}{\xi_{a_2}^l} - \sum_{l=1}^{a_3-1} \frac{C_{3,l}}{\xi_{a_3}^l}.$$

Dosazením za konstanty B_1, B_2 a B_3 ze vztahu 2.13 a za konstanty $C_{1,l}, C_{2,l}$ a $C_{3,l}$ ze vztahu 2.12 získáme

$$c_p = \frac{p^2}{a_1a_2a_3} + \frac{n}{2}\left(\frac{1}{a_1a_2} + \frac{1}{a_1a_3} + \frac{1}{a_2a_3}\right) +$$
$$+ \frac{1}{12}\left(\frac{3}{a_1} + \frac{3}{a_2} + \frac{3}{a_3} + \frac{a_1}{a_2a_3} + \frac{a_2}{a_1a_3} + \frac{a_3}{a_1a_2}\right) +$$
$$+ \frac{1}{a_1} \sum_{l=1}^{a_1-1} \frac{1}{(1-\xi_{a_1}^{la_2})(1-\xi_{a_1}^{la_3})\xi_{a_1}^{lp}} + \frac{1}{a_2} \sum_{l=1}^{a_2-1} \frac{1}{(1-\xi_{a_2}^{la_1})(1-\xi_{a_2}^{la_3})\xi_{a_2}^{lp}} +$$
$$+ \frac{1}{a_3} \sum_{l=1}^{a_3-1} \frac{1}{(1-\xi_{a_3}^{la_1})(1-\xi_{a_3}^{la_2})\xi_{a_3}^{lp}}.$$

Dosazením $a_1 = 6, a_2 = 9$ a $a_3 = 20$ získáme požadovaný vzorec.

V následující části odvodíme rekurentní vzorec pro výpočet počtu reprezentací libovolné částky.

2.2.2 Odvození rekurentního vzorce

Rekurentní vzorec pro získání počtu reprezentací libovolné částky odvodíme nejprve pro systémy se třemi mincemi o různých hodnotách $a, b, c \in \mathbb{N}$. Potom odvození zobecníme pro libovolné systémy mincí. Pro počet reprezentací částky

p v systému mincí budeme stejně jako v předchozích částech používat značení c_p. Tato část je inspirována příkladem rekurentního vzorce pro výpočet počtu reprezentací v [26, str. 99, 100]. Zobecňujeme a zjednodušujeme zde závěry z příkladu a uvádíme snazší odvození.

Pro hledání počtu reprezentací využijeme kombinatorickou úvahu a princip inkluze a exkluze.

Věta 2.19 (Princip inkluze a exkluze)**.** *Pro každý soubor $X_1, X_2, \ldots, X_n$ konečných množin platí*

$$\left|\bigcup_{i=1}^{n} X_i\right| = \sum_{\substack{A \subset \{1,2,\ldots,n\} \\ A \neq \emptyset}} (-1)^{|A|-1} \left|\bigcap_{i \in A} X_i\right| .$$

Důkaz. Větu zde nebudeme dokazovat. Pro důkaz se odkazujeme na [17, věta 2.6.2]. □

Dále zformulujeme jednodušší variantu věty 2.19, která se omezuje na tři množiny.

Důsledek 2.20. *Pro trojici konečných množin A, B, C platí*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| .$$

Pomocí principu inkluze a exkluze odvodíme rekurentní vzorec pro získání počtu reprezentací částky p v systému mincí o hodnotách $a, b, c \in \mathbb{N}$.

Věta 2.21. *Pro počet reprezentací částky $p > 1$ v systému mincí o různých hodnotách $a, b, c \in \mathbb{N}$ platí*

$$c_p = c_{p-a} + c_{p-b} + c_{p-c} - c_{p-a-b} - c_{p-a-c} - c_{p-b-c} + c_{p-a-b-c},$$

kde $c_k = 0$ pro $k < 0$ a $c_0 = 1$.

Důkaz. Nechť A je množina všech reprezentací částky p, které obsahují alespoň jednu minci o hodnotě a, B je množina reprezentací, které obsahují alespoň jednu minci o hodnotě b a C je množina reprezentací, které obsahují alespoň jednu minci o hodnotě c.

Množina obsahující všechny reprezentace nenulové částky p je $A \cup B \cup C$ a proto platí

$$c_p = |A \cup B \cup C| .$$

Pokud z každé reprezentace v množině A odebereme jednu minci o hodnotě a, získáme všechny reprezentace částky $p - a$. Pro velikost množiny A proto platí $|A| = c_{p-a}$. Pokud platí $p < a$, pak je množina A jistě prázdná. Proto budeme v této části uvažovat $c_k = 0$ pro $k < 0$. Zároveň si uvědomíme, že částku 0 můžeme reprezentovat jediným způsobem, platí proto $c_0 = 1$. Stejným způsobem zjistíme, že $|B| = c_{p-b}$ a $|C| = c_{p-c}$.

Množina $A \cap B$ obsahuje všechny reprezentace částky p s alespoň jednou mincí o hodnotě a a alespoň jednou mincí o hodnotě b. Stejnou úvahou jako v případě zjišťování $|A|$ získáme $|A \cap B| = c_{p-a-b}$. Tímto postupem dále získáme $|A \cap C| = c_{p-a-c}$, $|B \cap C| = c_{p-b-c}$ a $|A \cap B \cap C| = c_{p-a-b-c}$. Použitím principu inkluze a exkluze pro tři množiny získáme požadovaný vztah. □

Předchozí větu nyní zobecníme pro systémy o n mincích.

Poznámka. *V této kapitole jsme počet reprezentací částky p značili c_p, neboť šlo o prvek posloupnosti $\{c_n\}_{n=0}^{\infty}$. V následující větě budeme pro značení počtu reprezentací částky p používat $c(p)$ namísto c_p, protože na místě p se budou vyskytovat složitější výrazy, které by v dolním indexu vypadaly nepřehledně.*

Věta 2.22. *Mějme systém mincí o hodnotách $a_1, a_2, \ldots, a_n \in \mathbb{N}$, které jsou navzájem různé. Pro počet reprezentací částky p v tomto systému mincí $c(p)$ platí*

$$c(p) = \sum_{\substack{A \subset \{1,2,\ldots,n\} \\ A \neq \emptyset}} (-1)^{|A|+1} c\left(p - \sum_{k \in A} a_k\right),$$

kde $p \in \mathbb{N}$, $c(0) = 1$ a $c(k) = 0$ pro $k < 0$.

Důkaz. Mějme množiny $X_1, X_2, \ldots, X_n$ takové, že množina X_i se skládá z reprezentací částky p, které obsahují alespoň jednu minci o hodnotě a_i. Pro velikost této množiny platí $|X_i| = c(p - a_i)$, neboť odebráním jedné mince o hodnotě a_i z každé reprezentace v X_i získáme množinu všech reprezentací částky $p - a_i$.

Obecněji pro každou neprázdnou množinu $A \subset \{1, 2, \ldots, n\}$ platí

$$\left|\bigcap_{i \in A} X_i\right| = c\left(p - \sum_{k \in A} a_k\right).$$

Na levé straně je velikost množiny reprezentací p, které využívají alespoň jednu minci od každé z hodnot a_i pro $i \in A$. Odebráním těchto mincí a_i od každé z reprezentací získáme všechny reprezentace částky $p - \sum_{k \in A} a_k$.

Množiny $X_1, X_2, \ldots, X_n$ jsme zvolili tak, aby pro $p > 0$ platilo

$$c(p) = \left|\bigcup_{i=1}^{n} X_i\right|.$$

Použitím principu inkluze a exkluze 2.19 získáváme požadovanou rovnost. ☐

Podle věty 2.22 platí pro dvoumincové systémy o hodnotách a, b

$$c(p) = c(p-a) + c(p-b) - c(p-a-b)$$

a pro trojmincové systémy o různých hodnotách a, b, c jsme odvodili vzorec

$$c(p) = c(p-a)+c(p-b)+c(p-c)-c(p-a-b)-c(p-a-c)-c(p-b-c)+c(p-a-b-c).$$

Příklad 2.23. *Zjistěte počty reprezentací částek od 0 do 63 v systému mincí o hodnotách 6,9 a 20.*

Řešení. Použitím rekurzivního vzorce pro systémy mincí o třech různých hodnotách získáme tabulku počtů reprezentací 2.1.

p	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
c_p	1	0	0	0	0	0	1	0	0	1	0	0	1	0	0	1
p	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
c_p	0	0	2	0	1	1	0	0	2	0	1	2	0	1	2	0
p	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
c_p	1	2	0	1	3	0	2	2	1	1	3	0	2	3	1	2
p	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
c_p	3	1	2	3	1	2	4	1	3	3	2	2	5	1	3	4

Tabulka 2.1: Počty reprezentací v systému mincí o hodnotách $6, 9$ a 20

Z tabulky 2.1 také vidíme, že Frobeniovo číslo systému mincí o hodnotách 6,9 a 20 je rovno 43. Následujících šest po sobě jdoucích částek je totiž reprezentovatelných. Přidáním vhodného počtu mincí o hodnotě 6 k jedné z nich proto umíme reprezentovat každou větší částku. Ke stejnému závěru jsme došli i použitím grafového algoritmu v části 1.3.2.

3. Nalezení minimální reprezentace

V této kapitole se budeme zabývat problémy motivovanými následující otázkou:

Otázka. *Máme systém mincí o hodnotách $x_1, x_2, \dots, x_n$. Je-li dána částka a reprezentovatelná v tomto systému, jaké nejmenší množství mincí je potřeba k získání částky a?*

V celé kapitole budeme bez újmy na obecnosti předpokládat, že mince jsou seřazené podle velikosti tak, aby $x_1 > x_2 > x_3 > \dots > x_n$. Abychom mohli řešit problémy podobné úvodní otázce, zavedeme nejprve několik základních pojmů:

Reprezentaci částky jsme definovali na začátku kapitoly 2 v definici 1.1. Mince jsme seřadili podle velikosti, v reprezentaci $(a_1, a_2, \dots, a_n)$ je proto a_1 počet mincí s největší hodnotou.

Definice 3.1. *Máme-li reprezentace $A = (a_1, a_2, \dots, a_n)$ a $B = (b_1, b_2, \dots, b_n)$, pak řekneme, že A je lexikograficky větší než B a píšeme $A >_{lex} B$, pokud*

$$\exists i \in \{1, 2, \dots, n\}\ a_i > b_i \wedge \forall k \in \{1, \dots, i-1\}\ a_i = b_i.$$

Dále řekneme, že A je lexikograficky větší nebo rovno B a píšeme $A \geq_{lex} B$, pokud

$$A >_{lex} B \vee A = B.$$

Definice 3.2. *Počet mincí reprezentace $A = (a_1, a_2, \dots, a_n)$ značíme $|A|$, tj.*

$$|A| = \sum_{i=1}^{n} a_i.$$

Definice 3.3. *Reprezentace A částky a v systému mincí $x_1, x_2, \dots, x_n$ se nazývá minimální, je-li složena z nejmenšího možného počtu mincí a zároveň je ze všech takových reprezentací lexikograficky největší. Značíme ji $M(a)$.*

Reprezentací částky a s nejmenším počtem mincí může být v systému více. Například v systému mincí o hodnotách $20, 14, 8$ a 1 má částka 28 reprezentace $(0, 2, 0, 0)$ a $(1, 0, 1, 0)$. Obě se skládají z nejmenšího možného počtu mincí. Druhá z nich je ale lexikograficky větší. Proto v tomto systému mincí platí

$$M(28) = (1, 0, 1, 0).$$

3.1 Hladový algoritmus

V České republice platíme pomocí systému „mincí“ o hodnotách

$$1, 2, 5, 10, 20, 50, 100, 200, 500, 1000, 2000 \text{ a } 5000.$$

K nalezení minimální reprezentace libovolné částky v našem systému mincí můžeme použít tzv. hladový algoritmus (greedy algorithm). Hladový algoritmus vezme největší možnou minci nepřesahující částku, jejíž reprezentaci hledáme. Se zbylou částkou celý postup opakuje. Mohli bychom ho popsat následujícím pseudokódem (algoritmus 1).

Algoritmus 1 Hladový algoritmus

```
1: function HLADOVY(a, x_1, x_2, ..., x_n)          ▷ částka a a systém mincí
2:     R ← (0, 0, ..., 0)        ▷ inicializuj reprezentaci na nulový vektor délky n
3:     while a > 0 do
4:         i ← index mince největší hodnoty menší nebo rovné a
5:         R_i ← R_i + 1                    ▷ přidej 1 na i-té místo reprezentace
6:         a ← a − x_i
7:     end while
8:     return R
9: end function
```

Rychlost popsaného algoritmu můžeme vylepšit tím, že v každé iteraci cyklu nebudeme brát jednu nejcennější minci, ale vezmeme jich největší možné množství $\lfloor x/x_i \rfloor$. Řádky 5 a 6 algoritmu tedy pozměníme takto:

$R_i \leftarrow R_i + \lfloor x/x_i \rfloor$ ▷ přidej $\lfloor x/x_i \rfloor$ na i-té místo reprezentace

$a \leftarrow a - \lfloor x/x_i \rfloor x_i$

Cyklus algoritmu nyní proběhne maximálně n krát, celková složitost algoritmu je tedy lineární vzhledem k velikosti vstupu. K popsání časové složitosti můžeme použít také asymptotickou notaci $O(n)$.

Pro nalezení minimální reprezentace částky 631 algoritmus vybere největší možnou bankovku (minci) 500. Se zbytkem nerozměněné částky 131 postup opakuje. Částku 631 tímto způsobem rozmění na mince

$$500, 100, 20, 10 \text{ a } 1.$$

Skutečné měny jsou obvykle sestavené tak, aby se pro nalezení minimální reprezentace dal použít hladový algoritmus. Můžeme ale vymyslet systém mincí, pro který hladový algoritmus nenajde vždy minimální reprezentaci. Například v systému mincí o hodnotách $1, 3, 6, 12, 24, 30$ a 60 je reprezentace částky 48 pomocí dvou mincí 24 minimální. Hladový algoritmus ji ale složí ze tří mincí $30, 12$ a 6.

V systému mincí o hodnotách $12, 24$ a 30 dokonce hladový algoritmus částku 48 vůbec neumí reprezentovat. Nejprve vezme postupně mince 30 a 12, pro zbylou částku 6 už nemá žádnou minci, kterou by mohl použít. Částka 48 je přitom v uvedeném systému mincí reprezentovatelná pomocí dvou mincí 24.

Situaci si trochu zjednodušíme tím, že se omezíme na systémy mincí, ve kterých jsou reprezentovatelné všechny částky, tj. systémy mincí obsahující minci o hodnotě 1. I v tom případě je problém nalezení minimální reprezentace částky a NP-úplný problém [16].

3.2 Optimalita hladového algoritmu

V této kapitole si ukážeme, jak efektivně zjistit, jestli v daném systému mincí můžeme použít hladový algoritmus k hledání minimální reprezentace libovolné částky. Algoritmus a důkaz jeho správnosti popsal Pearson v publikaci [19], ze které vycházíme.

Definice 3.4. *Hladovou reprezentací částky a v systému mincí $x_1, x_2, \ldots, x_n$ rozumíme lexikograficky největší ze všech možných reprezentací a. Značíme jí $G(a)$.*

Naše definice hladové reprezentace odpovídá reprezentaci, kterou získáme použitím výše popsaného hladového algoritmu. Opakovaným přidáváním největší možné mince je zajištěno, že hodnotnějších mincí je v reprezentaci maximální možné množství.

Pokud hladový algoritmus vrátí reprezentaci s nejmenším počtem mincí, pak je podle definice 3.3 zřejmé, že se jedná o minimální reprezentaci tj.

$$|G(a)| = |M(a)| \Rightarrow G(a) = M(a).$$

Definice 3.5. *Máme reprezentace $A = (a_1, a_2, \ldots, a_n)$ a $B = (b_1, b_2, \ldots, b_n)$. Řekneme, že $A \leq B$, pokud pro všechna $i \in \{1, \ldots, n\}$ platí $a_i \leq b_i$.*

Předchozí definici bychom mohli popsat i tak, že $A \leq B$, pokud existuje vektor $D = (d_1, d_2, \ldots, d_n)$ takový, že pro všechna $i \in \{1, \ldots, n\}$ platí $d_i \geq 0$ a

$$A + D = B.$$

Náš algoritmus bude pro systém mincí $x_1, x_2, \ldots, x_n$ hledat nejmenší číslo w takové, že $M(w) \neq G(w)$. Pokud ho najde, pak pro tento systém nelze obecně použít hladový algoritmus pro hledání minimální reprezentace. V opačném případě hladový algoritmus použít lze.

Předtím než algoritmus popíšeme, dokážeme několik vlastností hladových a minimálních reprezentací.

Věta 3.6. *Nechť pro reprezentace $A = (a_1, a_2, \ldots, a_n)$ a $B = (b_1, b_2, \ldots, b_n)$ platí $A \leq B$.*

1. *Pokud je B hladovou reprezentací nějaké částky, pak je i A hladovou reprezentací.*

2. *Pokud je B minimální reprezentací nějaké částky, pak je i A minimální reprezentací.*

Důkaz. Nechť $A' = (a'_1, a'_2, \ldots, a'_n)$ je libovolnou reprezentací částky $\sum_{i=1}^{n} a_i x_i$. Protože A' a A reprezentují stejnou částku, platí

$$\sum_{i=1}^{n} a'_i x_i = \sum_{i=1}^{n} a_i x_i.$$

Ekvivalentními úpravami rovnice dostaneme

$$\sum_{i=1}^{n} b_i x_i - \sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} a'_i x_i = \sum_{i=1}^{n} b_i x_i.$$

Obě strany reprezentují stejnou částku. Pravá strana rovnice odpovídá reprezentaci B. Levá strana odpovídá reprezentaci $B - A + A'$. Předpokládáme-li, že B je hladová, pak platí

$$B - A + A' \leq_{lex} B.$$

Výraz na levé straně nerovnosti je platnou reprezentací, neboť z předpokladu $A \leq B$ plyne, že $B - A$ má všechny složky větší nebo rovny 0. Odečtením

$B - A$ od obou stran nerovnice nezměníme lexikografické uspořádání a získáme tím $A' \leq_{lex} A$. Dokázali jsme, že A je lexikograficky větší než libovolná jiná reprezentace stejné částky A'. Je to tedy reprezentace hladová.

Předpokládáme-li, že B je minimální, pak

$$|B| - |A| + |A'| \geq |B|.$$

Odečtením $|B| - |A|$ od obou stran rovnice získáme $|A'| \geq |A|$. Dokázali jsme, že A nemá větší počet mincí než libovolná jiná reprezentace stejné částky A'. Pro libovolnou další reprezentaci $A'' = (a''_1, a''_2, \ldots, a''_n)$ s nejmenším množstvím mincí, která reprezentuje stejnou částku jako A, platí:

$$\begin{aligned} |A| &= |A''| \\ |B| - |A| + |A''| &= |B| \\ |B - A + A''| &= |B| \end{aligned}$$

Protože $B - A + A''$ i B reprezentují stejnou částku, obsahují stejný počet mincí a B je minimální, platí

$$\begin{aligned} B - A + A'' &\leq_{lex} B \\ A'' &\leq_{lex} A. \end{aligned}$$

Reprezentace s nejmenším možným množstvím mincí A je tedy lexikograficky větší než libovolná jiná reprezentace s nejmenším množstvím mincí A''. Je proto minimální. □

Věta 3.7. *Nechť je w nejmenší částka, pro kterou není hladová reprezentace minimální, tj. $G(w) \neq M(w)$. Potom má na každém místě alespoň jedna z $G(w), M(w)$ číslo 0.*

Důkaz. Označíme $G(w) = (g_1, g_2, \ldots, g_n)$ a $M(w) = (m_1, m_2, \ldots, m_n)$. Předpokládejme pro spor, že pro nějaké $i \in \{1, \ldots, n\}$ platí $g_i > 0$ a $m_i > 0$. Zvolíme vektor D s hodnotou $\min\{g_i, m_i\}$ na i-tém místě a s nulami všude jinde. Reprezentace $G(w) - D$ je podle věty 3.6 hladová reprezentace částky

$$w - x_i \min\{g_i, m_i\}.$$

Podle stejné věty je $M(w) - D$ minimální. Z předpokladu $G(w) \neq M(w)$ plyne, že $M(w) - D$ je různá od $G(w) - D$. To je spor s předpokladem, že w je nejmenší částka, pro kterou se hladová a minimální reprezentace liší. □

Pro nejmenší částku w s rozdílnou hladovou a minimální reprezentací tedy například platí, že $M(w)$ má na první pozici číslo 0. Kdyby to tak nebylo, musela by mít na první pozici číslo 0 reprezentace $G(w)$. Minimální reprezentace $M(w)$ by potom byla lexikograficky větší než $G(w)$, což je spor s definicí $G(w)$.

Věta 3.8. *Uvažujme nejmenší w, pro které $M(w) \neq G(w)$. Nechť $i, j \in \{1, \ldots, n\}$ jsou takové, že první nenulová hodnota $M(w)$ je na i-tém místě a poslední nenulová hodnota $M(w)$ je na j-tém místě.*

Platí, že $M(w)$ se shoduje s $G(x_{i-1} - 1)$ na pozicích 1 až $j - 1$. Na pozici j je $M(w)$ o jedna větší než $G(x_{i-1} - 1)$. Na všech zbývajících pozicích je $M(w)$ nulová.

Důkaz. Z věty 3.7 plyne, že reprezentace $G(w)$ musí mít na i-tém místě hodnotu 0. Zřejmě $i \geq 2$ a na nějakém předchozím místě musí mít $G(w)$ nenulovou hodnotu, protože jinak by byla $M(w)$ lexikograficky větší. Mince jsou seřazeny podle velikosti od největší. Platí proto $x_{i-1} \leq w$ a tedy i

$$x_{i-1} - 1 < w. \tag{3.1}$$

Označíme $G(x_{i-1} - 1) = (v_1, v_2, \ldots, v_n)$. Protože

$$x_{i-1} > x_{i-1} - 1 \geq x_i,$$

první krok hladového algoritmu vezme minci o hodnotě x_i a proto $v_i \neq 0$. Pro $M(w) = (m_1, m_2, \ldots, m_n)$ platí z předpokladu věty $m_i \neq 0$. Z i-té pozice obou reprezentací proto můžeme odečíst hodnotu 1, čímž dostaneme minimální reprezentaci částky $w - x_i$ a hladovou reprezentaci částky $x_{i-1} - 1 - x_i$. Protože $w - x_i < w$, platí $M(w - x_i) = G(w - x_i)$. Podle (3.1) je navíc

$$x_{i-1} - 1 - x_i < w - x_i$$

a tedy i

$$G(x_{i-1} - 1 - x_i) <_{lex} G(w - x_i) = M(w - x_i).$$

Vrácením 1 k i-tému místu obou reprezentací nezměníme lexikografické uspořádání a dostáváme tak nerovnost

$$G(x_{i-1} - 1) <_{lex} M(w). \tag{3.2}$$

Minimální reprezentace $M(w)$ má na j-tém místě nenulovou hodnotu. Odečtením 1 od této hodnoty získáme podle věty 3.6 minimální reprezentaci částky $w - x_j$. Ta je menší než w, její hladová reprezentace je proto stejná jako minimální. Na místech 1 až $i - 1$ zůstaly hodnoty 0. Hladový algoritmus pro částku $w - x_j$ tedy v prvním kroku nemohl vybrat žádnou z mincí $x_1, \ldots, x_{i-1}$. Platí proto $w - x_j < x_{i-1}$ a odtud i

$$w - x_j \leq x_{i-1} - 1. \tag{3.3}$$

Podle (3.3) platí $G(w - x_j) \leq_{lex} G(x_{i-1} - 1)$. Složením s (3.2) dostáváme

$$G(w - x_j) \leq_{lex} G(x_{i-1} - 1) <_{lex} M(w).$$

Protože $G(w - x_j) = M(w - x_j)$, tak se $G(w - x_j)$ liší od $M(w)$ pouze o 1 v j-tém místě. Aby mohlo $G(x_{i-1} - 1)$ ležet lexikograficky mezi nimi, musí mít na všech místech od 1 do $j - 1$ stejné hodnoty jako $M(w)$. Na všech místech od $j + 1$ do n má $M(w)$ nuly. Aby bylo $G(i - 1 - 1)$ lexikograficky menší než $M(w)$, zbývá jediné j-té místo na kterém může být nižší. Zároveň na tomto místě musí být nižší jen o 1, jinak by lexikograficky kleslo pod $G(w - x_j)$. □

Pokud tedy pro daný systém mincí známe čísla i a j, dokážeme použitím hladového algoritmu pomocí věty 3.8 určit minimální reprezentaci w a tedy i částku w.

Čísla i a j ale neznáme. Vlastně ani nevíme, jestli existují. Nevíme totiž, zda existuje w splňující $M(w) \neq G(w)$. Možností, jak zvolit i a j, je pouze $O(n^2)$

Algoritmus 2 Algoritmus rozhodující, jestli hladový algoritmus v daném systému mincí najde pro libovolnou částku její minimální reprezentaci.

function OPTIMALITAHLADOVEHO($x_1, x_2, \ldots, x_n$)
  for $i \leftarrow 1$ **to** n **do**
    for $j \leftarrow i$ **to** n **do** ▷ volíme dvojice $i \leq j$
      $R \leftarrow$HLADOVY($x_{i-1} - 1, x_1, x_2, \ldots, x_n$)
      $R_j \leftarrow R_j + 1$
      for $k \leftarrow j + 1$ **to** n **do**
        $R_k \leftarrow 0$ ▷ vynulujeme pozice od $j + 1$
      end for
      $w' \leftarrow \sum_{l=1}^{n} R_l x_l$ ▷ částka, kterou reprezentuje R
      $G \leftarrow$ HLADOVY($w', x_1, x_2, \ldots, x_n$)
      if $|R| < |G|$ **then**
        return hladový algoritmus nenajde minimální reprezentaci w'
      end if
    end for
  end for
  return hladový algoritmus najde minimální reprezentaci libovolné částky
end function

(řádově maximálně n^2). Můžeme tedy postupně zkoušet všechny možnosti. Celý postup ukazuje algoritmus 2.

Při každé volbě i a j nalezneme pomocí hladového algoritmu a věty 3.8 reprezentaci R a odpovídající částku w'. Pokud je nyní $|R| < |G(w')|$, pak jsme našli reprezentaci w', která má menší počet mincí než hladová reprezentace. V opačném případě pokračujeme zkoušením následující kombinace i a j.

Pokud při zkoušení všech možných i, j nenastala ani jednou druhá možnost, pak hladový algoritmus pro tento systém mincí vždy najde minimální reprezentaci.

Při každém výběru i, j použijeme maximálně dvakrát hladový algoritmus a dvakrát sečteme počet mincí nějaké reprezentace. Jednou navíc zjistíme částku, kterou reprezentuje reprezentace R. Hladový algoritmus popsaný v části 3.1 provede $O(n)$ kroků. Zjištění reprezentovatelné částky a počtu mincí zabere také $O(n)$ kroků.

Celý postup pro zjištění optimality hladového algoritmu proto poběží v čase $O(n^3)$.

I pokud jsme v algoritmu 2 nalezli reprezentaci R částky w' takovou, že $|R| < |G|$, stále si nejsme jisti, jestli je R minimální reprezentací w' ani jestli je w' skutečně nejmenší částka, pro kterou hladový algoritmus nenajde minimální reprezentaci. Pro nalezení w a jeho minimální reprezentace $M(w)$ z věty 3.8 bychom museli najít všechny reprezentace R takové, že $|R| < |G|$ a vybrat z nich tu, která reprezentuje nejmenší částku.

Příklad 3.9. *Mějme systém mincí o hodnotách $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ rovnajících se postupně 60, 30, 24, 12, 6, 3, 1. Rozhodněte, jestli je v tomto systému mincí hladová reprezentace libovolné částky zároveň reprezentací minimální.*

Řešení. Zvolíme-li $i = j = 3$, pak platí

$$G(x_{i-1} - 1) = G(29) = (0, 0, 1, 0, 1, 2).$$

Reprezentace R získaná algoritmem 2 pro tuto volbu i a j je $R = (0, 0, 2, 0, 0, 0)$. Jde o reprezentaci částky $w' = 48$.

$$G(w') = G(48) = (0, 1, 0, 1, 0, 1, 0).$$

Došli jsme tedy (stejně jako v sekci 3.1) k závěru, že v tomto systému mincí pro některé částky není hladová reprezentace reprezentací minimální. Příkladem takové částky je 48.

Kdybychom ve stejném systému mincí zvolili $i = 4$, $j = 5$, pak vypočteme

$$G(x_{i-1} - 1) = G(23) = (0, 0, 0, 1, 1, 1, 2).$$

Reprezentace R získaná algoritmem 2 pro tuto volbu i a j je $R = (0, 0, 0, 1, 2, 0, 0)$. Číslo w' je tedy rovno 24 a

$$G(w') = G(24) = (0, 0, 1, 0, 0, 0).$$

Pro tuto volbu i, j jsme tedy nenašli číslo w pro které $|G(w)| > |M(w)|$. Reprezentace R dokonce zjevně není minimální reprezentací částky 24.

4. Úlohy o hledání mincí

Tato kapitola představuje sbírku zajímavých úloh, které ke svému řešení nevyžadují vysokoškolskou matematiku.

4.1 Vážení mincí

V této části ukážeme několik úloh, k jejichž řešení budeme používat vážení mincí. V každé úloze předpokládáme, že na váhu je možné položit libovolné množství mincí zároveň. V úlohách, kde mluvíme o rovnoramenných vahách, máme na mysli váhy sloužící k porovnání hmotnosti předmětů položených na levé straně vah s hmotností předmětů položených na pravé straně vah.

Příklad 4.1. *Máme deset hromádek po deseti mincích. Jedna hromádka obsahuje samé falešné mince. Známe hmotnost pravé mince a víme, že falešná mince je o gram těžší než pravá mince.*

K dispozici máme obyčejnou váhu, která ukazuje hmotnost závaží, které na ní vložíme. Kolik vážení potřebujeme, abychom zjistili, na které hromádce jsou falešné mince? [8, str. 26–27]

Řešení. Stačí nám jedno vážení. Na váhu položíme jednu minci z první hromádky, dvě mince z druhé hromádky, tři mince ze třetí hromádky a tak dále. Poslední desátou hromádku na váhu položíme celou. Kdyby byly všechny mince pravé, ukázala by váha hmotnost

$$(1 + 2 + \cdots + 10)m = 55m \text{ gramů},$$

kde m je hmotnost jedné pravé mince vyjádřená v gramech. Pokud je j-tá hromádka falešná, pak váha ukáže $55m + j$ gramů. Podle počtu přebytečných gramů proto poznáme, která hromádka je falešná.

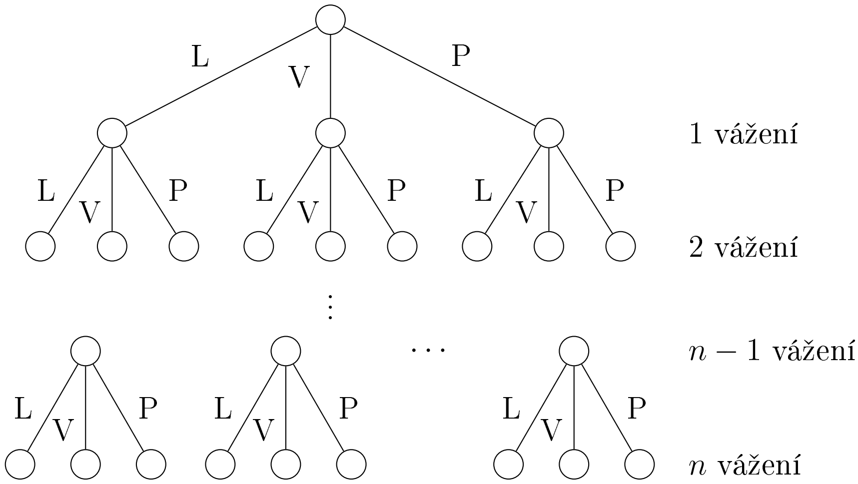
Příklad 4.2. *Máme 3^n mincí, z nichž jedna je falešná a ostatní jsou pravé. Všechny pravé mince mají stejnou hmotnost. Falešná mince je těžší než pravé mince. Jaký minimální počet vážení na rovnoramenných vahách potřebujeme, abychom s jistotou našli falešnou minci?*

Řešení. Všechny mince můžeme rozdělit na tři stejně velké hromádky velikosti 3^{n-1}. Pomocí rovnoramenné váhy porovnáme hmotnosti prvních dvou hromádek. Falešná mince se jistě nachází v těžší z prvních dvou hromádek. Pokud při vážení zůstanou váhy vyvážené, pak je falešná mince ve třetí hromádce.

Nyní máme 3^{n-1} mincí, z nichž jedna je falešná a ostatní jsou pravé. Můžeme proto opakovat stejný postup. Po n krocích zbude pouze falešná mince.

Ukázali jsme, že mezi 3^n mincemi dokážeme najít falešnou pomocí n vážení na rovnoramenných vahách. Nyní dokážeme, že je to minimální možné množství vážení.

Uvažujme libovolný postup vedoucí k nalezení falešné mince, který je založen na opakovaném vážení. Jeho průběh můžeme znázornit pomocí stromu na obrázku 4.1. Každý vrchol stromu odpovídá nějakému stavu, ve kterém se nacházíme po jistém počtu vážení. Začínáme v kořenovém vrcholu a po každém vážení se



Obrázek 4.1: Strom možných průběhů vážení na rovnoramenných vahách

posouváme o jednu úroveň níže podle toho, jak dopadlo poslední vážení. Písmena L, P, V postupně odpovídají případům, kdy je levá strana těžší, pravá strana je těžší, resp. kdy jsou obě strany vyvážené. Každý stav pak odpovídá posloupnosti písmen L, P, V. Pokud např. první dvě vážení skončila převážením vah na levou stranu, nacházíme se ve stavu LL.

Po prvním vážení jsme v jednom ze tří možných stavů. Každé další vážení ztrojnásobí počet možných stavů, po k váženích se tedy nacházíme v některém z 3^k stavů.

Zadání úlohy si můžeme představit tak, že falešná mince se nachází na jednom z 3^n možných míst. Aby náš postup dokázal rozlišit všechny možné případy, potřebujeme alespoň n vážení na rovnoramenných vahách.

Libovolný postup k nalezení falešné mince musí váhy použít alespoň n-krát. Náš postup využívá právě n vážení, je tedy optimální.

K maximálnímu množství stavů, které dokážeme rozlišit pomocí n vážení bychom mohli dojít i jiným způsobem.

Každé vážení na rovnoramenné váze může skončit třemi způsoby. Pokud výsledek každého vážení zapíšeme jako jednu cifru čísla v trojkovém zápisu, pak n vážení odpovídá n-cifernému číslu v trojkové soustavě. Vlastně jde o zápis výsledků vážení na obrázku 4.1, ve kterém místo znaků L, P a V využíváme znaky 0, 1 a 2.

Čísel s maximálně n ciframi je v trojkové soustavě 3^n. Pomocí n vážení proto nemůžeme reprezentovat více než 3^n různých stavů.

Užitečnost trojkové soustavy v úlohách s rovnoramennými vahami ukazuje i následující úloha.

Příklad 4.3. *Máme dvanáct mincí, z nichž jedenáct je pravých a jedna je falešná. Všechny pravé mince mají stejnou hmotnost. Falešná mince je těžší nebo lehčí než pravé mince.*

Máme k dispozici rovnoramenné váhy. Dokážeme pomocí tří vážení najít falešnou minci a určit, jestli je těžší nebo lehčí než ostatní mince? [7, kapitola 11]

Řešení. V druhém sloupci tabulky 4.1 jsou čísla od 1 do 12 zapsaná v trojkové soustavě. Ve třetím sloupci stejné tabulky jsou čísla v trojkové soustavě, která vzniknou z čísel v prvním sloupci souběžným nahrazením všech 0 za 2 a naopak.

1	**001**	221
2	002	**220**
3	**010**	212
4	**011**	211
5	**012**	210
6	020	**202**
7	021	**201**
8	022	**200**
9	100	**122**
10	101	**121**
11	102	**120**
12	110	**112**

Tabulka 4.1: Označení dvanácti mincí v trojkové soustavě.

Každou minci označíme jedním z čísel v druhém nebo třetím sloupci tabulky 4.1. Pro označení vybereme to číslo, které má jako první dvojici různých cifer jednu z možností 01, 12 nebo 20. V tabulce jsou podle tohoto kritéria tučně zvýrazněná označení jednotlivých mincí.

Všimneme si, že čtyři mince v našem označení mají první cifru 0, čtyři mince začínají cifrou 1 a zbylé čtyři cifrou 2. Totéž platí pro cifry na druhém a třetím místě.

Dále si můžeme všimnout, že v tabulce 4.1 jsou všechna trojková čísla s maximálně třemi ciframi kromě 000, 111 a 222.

Pro první vážení tedy položíme na levou stranu rovnoramenných vah všechny mince, které začínají cifrou 0. Na pravou stranu položíme všechny mince, které začínají cifrou 2.

Pokud se váhy převáží vpravo, znamená to, že falešná mince je buď těžší a je mezi mincemi na pravé straně, nebo lehčí a je mezi mincemi na levé straně. Víme tedy, že první cifra falešné mince je 2 v případě, že je těžší než pravé mince a 0 v případě, že je lehčí než pravé mince. Označíme si první cifru falešné mince 2 a pokud na konci všech vážení zjistíme, že falešná mince byla lehčí než mince pravé, tak nahrazením všech 0 za 2 a 2 za 0 získáme skutečné označení falešné mince.

Pokud váhy zůstanou vyvážené, pak falešná mince není na levé ani pravé straně a první cifra falešné mince je jistě 1.

Pokud se váhy převáží vlevo, pak je falešná mince buď těžší a začíná cifrou 0, nebo je lehčí a začíná cifrou 2. Podobnou úvahou jako v případě převážení vah vpravo si první cifru falešné mince prozatím označíme 0.

V druhém vážení položíme na levou stranu všechny mince s prostřední cifrou 0. Na pravou stranu položíme všechny mince s prostřední cifrou 2.

Pokud se váhy převáží vpravo, pak je falešná mince těžší a má prostřední cifru 2, nebo je falešná mince lehčí a má prostřední cifru 0. Prostřední cifru prozatím označíme 2.

Pokud váhy zůstanou vyvážené, pak falešná mince není na levé ani pravé straně a prostřední cifra má jistě hodnotu 1. Pokud se váhy převáží vlevo, označíme prostřední cifru 0.

Stejný postup provedeme i pro třetí cifru.

Kdybychom předem věděli, že falešná mince je těžší než pravé, pak by označení získané uvedeným postupem skutečně patřilo falešné minci. Kdybychom předem věděli, že falešná mince je lehčí než pravé, pak bychom nahrazením cifer 0 za 2 a 2 za 0 získali označení falešné mince.

Tuto informaci ale nemáme, musíme proto z obou možností vybrat tu správnou. Z obou možností označuje nějakou minci právě jedna z nich. V druhém a třetím sloupci tabulky 4.1 jsou totiž uvedeny obě možnosti, ale pouze jedna z nich je zvýrazněna tučně. Podle toho, která z možností to je, navíc zjistíme, jestli je falešná mince těžší nebo lehčí než pravé mince.

Kdybychom v předchozím příkladu nepotřebovali vědět, jestli je falešná mince těžší nebo lehčí než ostatní, dokázali bychom pomocí tří vážení najít falešnou minci i mezi třinácti mincemi. Jednu z nich bychom nechali stranou a hledali bychom falešnou minci mezi zbývajícími dvanácti. Kdyby bylo těchto dvanáct mincí pravých, váha by při každém vážení zůstala ve vyvážené poloze a postup by označil neexistující minci 111 za falešnou. V tom případě bychom věděli, že falešná musí být třináctá mince.

Ukážeme si ještě variantu úlohy s další přidanou mincí, o které víme, že je pravá.

Příklad 4.4. *Máme třináct mincí, z nichž dvanáct je pravých a jedna je falešná. Navíc máme jednu minci, o které předem víme, že je pravá. Všechny pravé mince mají stejnou hmotnost. Falešná mince je těžší nebo lehčí než mince pravé.*

Máme k dispozici rovnoramenné váhy. Dokážeme pomocí tří vážení najít falešnou minci a určit, jestli je těžší nebo lehčí než ostatní mince? [7, kapitola 11]

Řešení. Celý postup bude stejný, jako v příkladu o dvanácti mincích. Třináctou minci, o které nevíme jestli je falešná, označíme 000. Čtrnáctou minci, která je zaručeně pravá, označíme 222. Při každém vážení je nyní na levé straně navíc třináctá mince a na pravé straně je navíc čtrnáctá mince. Pokud je falešná mince mezi prvními dvanácti, pak je při každém vážení na obou stranách váhy navíc jedna pravá mince. V takovém případě tedy najdeme falešnou minci podle původního postupu pro 12 mincí. Pokud je falešná mince ta třináctá, pak pokud je těžší, váhy se vždy převáží vlevo a původní postup označí správně za falešnou minci 000. Pokud je falešná mince třináctá a je lehčí, pak se váhy převáží vždy vpravo a původní postup označí za falešnou minci 222.

Postup z příkladu o dvanácti mincích tedy zůstává nezměněný. Pokud označí falešnou minci jako 000, pak je falešná mince ta třináctá a je těžší než ostatní mince. Pokud označí falešnou minci jako 222, pak je falešná mince také ta třináctá, ale je lehčí než ostatní mince.

Pokud bychom nepotřebovali zjistit, zda je falešná mince těžší, nebo lehčí, pak bychom zvládli vyřešit i podobný problém se čtrnácti mincemi a jednou zaručeně pravou mincí. Použili bychom stejný postup jako v předchozím případě, jenom bychom jednu minci ponechali stranou. Pokud předchozí postup v takovém případě označí za falešnou neexistující minci 111, pak je falešná mince, kterou jsme nechali stranou.

Příklad 4.5. *Máme deset mincí. Každá z nich má jednu ze dvou různých hmotností. Jinak jsou nerozlišitelné. Dokážeme pomocí maximálně tří vážení na rovnoramenných vahách rozhodnout, jestli má všech deset mincí stejnou hmotnost?* [1]

Řešení. Nejprve si ukážeme, jak bychom postupovali, kdybychom mohli použít čtyři vážení. Prvně porovnáme hmotnost dvou libovolných mincí. Pokud mají rozdílnou hmotnost, jsme hotovi a odpovídáme, že všech deset mincí nemá stejnou hmotnost.

Pokud mají dvě mince stejnou hmotnost, pak v druhém vážení porovnáme tuto dvojici mincí s libovolnou jinou dvojicí mincí. Pokud dvojice nemají stejnou hmotnost, pak opět odpovíme záporně. Pokud mají dvojice stejnou hmotnost, pokračujeme. Zvážíme čtveřice již vážených s dosud nezváženou čtveřicí.

Tímto způsobem umíme pomocí n kroků zjistit, jestli má 2^n mincí stejnou hmotnost. V případě deseti mincí pomocí tří vážení zjistíme, jestli má prvních 8 mincí stejnou hmotnost. V posledním vážení porovnáme libovolné dvě již zvážené mince s posledními dvěma nezváženými.

Nyní vyřešíme úlohu pomocí tří vážení. Deset mincí si očíslujeme od 1 do 10. Rozdělíme je na hromádky. První hromádka bude obsahovat pouze minci 1. Druhá hromádka bude obsahovat mince 2 a 3. Třetí hromádka bude obsahovat mince 4, 5 a 6. Čtvrtá hromádka bude obsahovat zbylé mince 7, 8, 9 a 10.

Dále označíme a počet těžkých mincí v první hromádce, b počet těžkých mincí v druhé hromádce, c počet těžkých mincí ve třetí hromádce a d počet těžkých mincí ve čtvrté hromádce.

Nejprve pomocí rovnoramenných vah porovnáme hmotnost první a čtvrté hromádky s hmotností druhé a třetí hromádky. Pokud se váhy převáží na jednu nebo na druhou stranu, pak víme, že některé mince nemají stejnou hmotnost. Pokud váhy zůstanou vyvážené, pak platí

$$a + d = b + c. \tag{4.1}$$

Dále porovnáme hmotnost první a druhé hromádky se třetí hromádkou. Pokud se váhy převáží na libovolnou stranu, opět jsme skončili se závěrem že některé mince nemají stejnou hmotnost. V opačném případě víme, že

$$a + b = c. \tag{4.2}$$

Nakonec porovnáme hmotnost první a třetí hromádky s hmotností čtvrté hromádky. Pokud se váhy převáží na nějakou stranu, opět víme, že některé mince nemají stejnou hmotnost. V opačném případě platí

$$a + c = d. \tag{4.3}$$

Sečtením rovností (4.2) a (4.3) získáme

$$2a + b = d. \tag{4.4}$$

Dále sečteme rovnosti (4.1) a (4.4), čímž obdržíme

$$3a = c.$$

Dosazením za c do rovnice (4.2) a následnými úpravami získáme

$$2a = b.$$

Nakonec dosadíme za c do rovnice (4.3). Získáme tím

$$4a = d.$$

Proměnná a vyjadřuje počet těžkých mincí na jednoprvkové hromádce s jedinou mincí 1. Může proto nabývat hodnoty 0 nebo 1. Pokud platí $a = 0$, pak $b = c = d = 0$ a z deseti mincí není žádná těžká. Pokud platí $a = 1$, pak $b = 2$, $c = 3$ a $d = 4$ a všechny mince jsou těžké.

Pokud při našich váženích váhy zůstaly pokaždé vyvážené, pak mají všechny mince stejnou hmotnost. V opačném případě mince stejnou hmotnost nemají.

4.2 Zlaté, kouzelné a jiné mince

V této části se budeme zabývat úlohami, ve kterých k rozlišení mincí nebudeme používat váhy, ale nějaký jiný systém.

Příklad 4.6. *Z osmi mincí jsou čtyři kouzelné. Kouzelné mince jsou od obyčejných nerozlišitelné. Jediný, kdo mince umí rozlišit je kouzelník. Naším úkolem je vytvořit dvě hromádky tak, aby v každé byly dvě kouzelné mince a dvě obyčejné.*

Každý den můžeme kouzelníkovi předložit dvě vytvořené hromádky. On nám sdělí, zda jsme úkol splnili. Jaký nejmenší možný počet dní potřebujeme, abychom s jistotou správně rozdělili mince? [6, str. 7]

Řešení. Hromádku obsahující x kouzelných mincí a y obyčejných mincí budeme označovat (x, y). Začínáme tedy s jedinou hromádkou $(4, 4)$ a naším cílem je rozdělit mince na dvě hromádky $(2, 2)$.

První den máme jedinou možnost – rozdělit mince do dvou hromádek o čtyřech mincích náhodně. Pokud jsme se do správného rozdělení netrefili, určitě nastala jedna z variant:

1. Jedna z hromádek obsahuje tři kouzelné mince a druhá jednu kouzelnou minci. Získali jsme tedy hromádky $(3, 1)$ a $(1, 3)$.

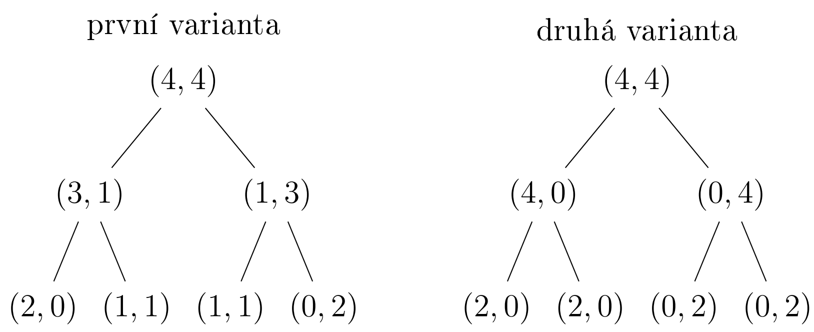
2. Jedna z hromádek obsahuje čtyři kouzelné mince a druhá samé obyčejné. Získali jsme tedy hromádky $(4, 0)$ a $(0, 4)$.

V každém případě obě hromádky o čtyřech mincích rozdělíme na hromádky o dvou mincích. Vzniknou tím čtyři hromádky o dvou mincích. Pokud nastala první varianta, pak vzniknou hromádky $a = (2, 0)$, $b = (1, 1)$, $c = (1, 1)$ a $d = (0, 2)$. Složením a s hromádkou d a b s hromádkou c vzniknou dvě hledané hromádky $(2, 2)$.

Pokud nastala druhá varianta, vzniknou hromádky $a' = (2, 0)$, $b' = (2, 0)$, $c' = (0, 2)$ a $d' = (0, 2)$. Složením a' s hromádkou c' a b' s hromádkou d' vzniknou dvě hledané hromádky $(2, 2)$.

Obě varianty, které mohly nastat, ilustruje obrázek 4.2.

Bohužel nevíme, která varianta nastala, ani kolik kouzelných mincí je ve které ze čtyř hromádek. Pouze víme, že spojením vhodných dvojic hromádek o dvou mincích vzniknou hledané hromádky $(2, 2)$. Vyzkoušíme tedy všechny možnosti. Máme tři možnosti, jak k první hromádce připojit jinou. Jednu možnost jsme vyzkoušeli už první den. Zbývá tedy vyzkoušet ještě dvě další.



Obrázek 4.2: Dělení kouzelných mincí na hromádky.

Ke splnění úkolu nám stačí tři dny.

V menším množství dní mince s jistotou správně rozdělit nelze. První den nemáme žádné informace a musíme proto mince rozdělit do dvou hromádek náhodně. Rozborem všech možností následného rozdělení mincí v druhém dni bychom mohli ukázat, že ať mince v druhém dni rozdělíme jakkoliv, na začátku mohly být seřazeny tak, že rozdělení nebude správné.

Pokud nechceme rozebírat všechny možnosti, můžeme si uvědomit, že při rozdělení mincí na dvě hromádky můžou nastat tři možnosti:

1. První hromádka obsahuje všechny mince jednoho druhu.
2. První hromádka obsahuje jednu minci jednoho druhu a tři mince druhého druhu.
3. První hromádka obsahuje dvě kouzelné a dvě obyčejné mince.

Abychom mohli druhý den s jistotou rozdělit mince správně, museli bychom mít od kouzelníka dostatek informací k rozlišení těchto případů. Jedinou informací, kterou od kouzelníka máme, je jedna odpověď ano/ne z prvního dne. Pomocí jedné hodnoty ano/ne tři možnosti nemůžeme rozlišit, proto ať zvolíme jakoukoliv strategii, nemůžeme si být jistí, že druhý den rozdělíme mince správně.

Ukázali jsme, že ke splnění úkolu vždy stačí nejvýše tři dny, a že dva dny nemusejí stačit.

Příklad 4.7. *Ze sta mincí je padesát kouzelných. Kouzelné mince jsou od obyčejných nerozlišitelné. Jediný, kdo mince umí rozlišit je kouzelník. Naším úkolem je vytvořit dvě hromádky tak, aby v každé bylo dvacet pět kouzelných mincí a dvacet pět obyčejných mincí.*

Každý den můžeme kouzelníkovi předložit dvě vytvořené hromádky. On nám sdělí, zda jsme úkol splnili. Bude nám ke splnění úkolu jistě stačit padesát dní? [6, str. 7]

Řešení. Ukážeme, že padesát dní vždy stačí. První den rozdělíme mince do dvou hromádek po padesáti mincích náhodně. Pokud jsme mince nerozdělili správně už napoprvé, znamená to, že v první hromádce je n kouzelných mincí, kde $n \neq 25$. V druhé hromádce je tedy $50 - n$ kouzelných mincí. Zbylé mince v obou hromádkách jsou obyčejné.

Mince v hromádkách z prvního dne označíme čísly od 1 do 50. Druhý den vyměníme první minci z první hromádky za první minci z druhé hromádky. Počet kouzelných mincí v první hromádce mohl zůstat stejný jako předchozí den, jedna kouzelná mince mohla přibýt, případně mohla jedna kouzelná mince ubýt.

Pokud jsme druhého dne hromádky stále nerozdělili správně, vyměníme ještě druhou minci z první hromádky za druhou minci z druhé hromádky. Oproti stavu z prvního dne budou mít hromádky třetí den vyměněnou první a druhou minci.

Stejný postup opakujeme i v dalších dnech. V i-tém dni budou oproti prvnímu dni vyměněny všechny mince od 1 do $i-1$ včetně. V každém dni se počet kouzelných mincí v první hromádce změní oproti předchozímu dni maximálně o 1.

Kdybychom takto pokračovali 51 dní, byly by na konci obě hromádky prohozené. V první hromádce by proto bylo $50-n$ kouzelných mincí. Do tohoto stavu jsme se dostali postupným přidáváním a odebíráním maximálně jedné kouzelné mince v první hromádce. V některém z prvních padesáti dnů se tedy počty kouzelných mincí v obou hromádkách musely shodovat.

Řešení předchozí úlohy se snadno zobecní na případ, kdy máme $2n$ mincí a polovina z nich je kouzelná. K rozdělení na dvě hromádky obsahující $n/2$ kouzelných a $n/2$ obyčejných mincí pak stačí n dnů.

Úloha má samozřejmě smysl pouze pro n sudé.

Příklad 4.8. *Máme k dispozici n mincí tří různých druhů: bronzové, stříbrné a zlaté. Mince jsou od sebe nerozeznatelné. Máme stroj, který dostane dvě mince a řekne, jestli jsou stejného druhu. Neřekne ale z jakého.*

Každý den můžeme pomocí stroje provést libovolné množství porovnání. Žádná mince se ale v jednom dni nesmí účastnit dvou porovnání. Jaký nejmenší možný počet dní potřebujeme, abychom našli alespoň jednu zlatou minci pokud víme, že více než polovina mincí je zlatých? [2]

Řešení. První den o mincích nemáme žádnou informaci. Porovnáme proto co nejvíce náhodně zvolených dvojic. Následně vyřadíme každou dvojici, ve které jsou mince různého druhu. Zbavíme se tím maximálně tolika zlatých mincí, jako mincí ostatních druhů. V každé ze zbylých dvojic jsou obě mince stejného druhu. Mezi zbylými mincemi je proto stále více než polovina zlatých mincí.

Druhý den dvojice spárujeme do skupinek po čtyřech mincích. Z každé dvojice vybereme jednu minci a vybrané mince porovnáme. Pokud jsou mince stejného druhu, získali jsme čtveřici stejného druhu. Pokud jsou mince různého druhu, celou čtveřici vyřadíme. Opět tím odstraníme méně nebo stejně zlatých mincí než mincí jiného druhu. Mezi zbylými mincemi je proto stále více než polovina zlatých.

V každé čtveřici jsou ještě dvě mince, které jsme druhý den neporovnávali. Čtveřice mincí spárujeme do skupin po osmi. V každé skupině porovnáme dosud neporovnanou minci z první čtveřice s dosud neporovnanou mincí z druhé čtveřice. Pokud mají rozdílný druh, celou skupinu vyřadíme. Skupiny se stejným druhem ponecháme. Mezi zbylými mincemi je stále více než polovina zlatých mincí.

V každé z nově vzniklých skupin mincí jsou dvě mince, které se v druhém dni ještě neúčastnily porovnání. Celý postup tedy můžeme opakovat tak dlouho, dokud nezbude jedna velká skupina. V každém běhu porovnávání jsme zdvojnásobili velikost porovnávaných skupin. Poslední velká skupina proto obsahuje 2^k mincí.

Pokud je n liché, pak při prvním párování mincí zbyla jedna mince, která se porovnávání nemohla účastnit. Podobně pokud je počet vzniklých dvojic po prvním dni lichý, pak se jedna dvojice nemohla účastnit dalšího porovnávání. Podobně při párování čtveřic mohla zbýt jedna čtveřice atd. K poslední velké skupině jsme dospěli po $k-1$ párováních. Celkem mohlo zbýt maximálně

$$2^0 + 2^1 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$$

mincí mimo velkou skupinu. Víme, že velká skupina obsahuje všechny mince jednoho druhu a že více než polovina nevyhozených mincí je zlatá. Velká skupina se proto skládá ze samých zlatých mincí. Pro nalezení jedné zlaté mince proto stačí vybrat libovolnou z velké skupiny.

Zjistili jsme, že ve dvou dnech umíme najít zlatou minci. Nyní ukážeme, že v jednom dni to nejde.

První den umíme porovnávat pouze dvojice. Ať zvolíme jakoukoliv strategii porovnávání, po prvním dni bude pro každou minci platit jedna z možností:

1. Mince se účastnila porovnání s jinou mincí stejného druhu.

2. Mince se účastnila porovnání s jinou mincí jiného druhu.

3. Mince se žádného porovnání neúčastnila.

O žádné minci po prvním dni nevíme nic jiného, než která ze tří uvedených možností pro ni platí. Na základě těchto informací nedokážeme o žádné minci s jistotou říci, že je zlatá. Pro každou zvolenou minci totiž můžeme najít příklad zadání, ve kterém tato mince není zlatá.

Ukázali jsme, že ve dvou dnech umíme najít zlatou minci, zatímco jeden den nestačí. Nejmenší možné množství dní, ve kterých jsme schopni najít zlatou minci, je proto 2.

Závěr

Na závěr zmíníme několik odkazů na další související literaturu. Geometrický přístup k reprezentovatelnosti z části 1.2.2 můžeme v některých případech využít i pro hledání počtu reprezentací částky. V [18, kapitola 2] je popsaný způsob získání počtu reprezentací částky s pomocí Pickovy věty.

V části 1.3.2 jsme ukázali grafový algoritmus pro výpočet Frobeniova čísla. Při hledání nejkratší cesty grafem jsme použili Dijkstrův algoritmus. Více informací o Dijkstrově algoritmu a o různých vylepšeních rychlosti výpočtu Frobeniova čísla najdeme v [24, str. 536–542] a [5]. Pokud nechceme Frobeniovo číslo počítat, můžeme alespoň odhadnout jeho velikost. Přehled odhadů je například v [3].

V kapitole 3 jsme hledali lexikograficky největší z reprezentací, které využívají nejmenší možné množství mincí. Kdybychom upustili od požadavku na lexikograficky největší reprezentaci, mohli bychom hledat počet reprezentací, které využívají nejmenší možné množství mincí. Řešení tohoto problému se pro systémy s maximálně třemi mincemi nachází v [15].

Seznam použité literatury

[1] A Trick with Ten Coins. 2006, [cit. 19. 6. 2016].
URL <http://mathforum.org/wagon/fall06/p1065.html>

[2] Will A Real Gold Coin Please Stand Up? 2009, [cit. 2. 6. 2016].
URL <http://mathfactor.uark.edu/2009/03/yoak-will-a-real-gold-coin-please-stand-up/>

[3] Aliev, I. M.; Gruber, P. M.: An optimal lower bound for the Frobenius problem. *Journal of Number Theory*, ročník 123, č. 1, 2007: s. 71–79.

[4] Beck, M.; Robins, S.: *Computing the continuous discretely. Integer-point enumeration in polyhedra*. New York: Springer, 2007.

[5] Beihoffer, D.; Hendry, J.; Nijenhuis, A.; aj.: Faster algorithms for Frobenius numbers. *Electron. J. Combin*, ročník 12, č. 1, 2005.

[6] Galperin, G.: Emmisary. 2011, [cit. 2. 6. 2016].
URL <http://www.msri.org/attachments/media/news/emissary/EmissarySpring2011.pdf>

[7] Gardner, M.: *Martin Gardner's sixth book of mathematical games from Scientific American*. W. H. Freeman, 1971.

[8] Gardner, M.: *Hexaflexagons and other mathematical diversions: The first Scientific American book of puzzles and games*. University of Chicago Press, 1988.

[9] Garey, M. R.; Johnson, D. S.: *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York: W. H. Freeman & Co., 1979.

[10] Hetland, M. L.: Some Hardness Proofs. 2011, [cit. 15. 5. 2016].
URL <http://www.idi.ntnu.no/~mlh/algkon/hard.pdf>

[11] Honsberger, R.: *Mathematical gems II*. Washington, D.C.: The Mathematical Association of America, 1976.

[12] Jarník, V.: *Diferenciální počet I*. Praha: Academia, 1974.

[13] Jarník, V.: *Integrální počet I*. Praha: Academia, 1984.

[14] Kellerer, H.; Pferschy, U.; Pisinger, D.: *Knapsack Problems*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004.

[15] Lance Bryant, L. J., James Hamblin: A Variation on the Money-Changing Problem. *The American Mathematical Monthly*, ročník 119, č. 5, 2012: s. 406–414.

[16] Lueker, G. S.: Two NP-complete problems in nonnegative integer programming. 1975, report č. 178, Princeton University. Department of Computer Science.

[17] Matoušek, J.; Nešetřil, J.: *Kapitoly z diskrétní matematiky*. Praha: Matfyzpress, 2002.

[18] Michael, T.: *How to guard an art gallery and other discrete mathematical adventures*. JHU Press, 2009.

[19] Pearson, D.: A Polynomial-time Algorithm for the Change-making Problem. *Operations Research Letters*, ročník 33, č. 3, 2005: s. 231–234.

[20] Petković, M.: *Famous puzzles of great mathematicians*. Providence: American Mathematical Society, 2009.

[21] Ramírez-Alfonsín, J. L.: Complexity of the Frobenius problem. *Combinatorica*, ročník 16, č. 1, 1996: s. 143–147.

[22] Skiena, S. S.: *The algorithm design manual - Second edition*. Springer Science & Business Media, 2008.

[23] Stanovský, D.: *Základy algebry*. Praha: Matfyzpress, 2010.

[24] Wagon, S.: *Mathematica in Action: Problem Solving Through Visualization and Computation*. Springer Publishing Company, Inc., třetí vydání, 2010.

[25] Wei, Y.-S.: The Diophantine Frobenius Problem. [cit. 25. 7. 2016]. URL `<http://dosen.narotama.ac.id/wp-content/uploads/2012/03/The-Diophantine-Frobenius-Problem.pdf>`

[26] Wilf, H. S.: *generatingfunctionology*. Academic Press, Inc., 1994.