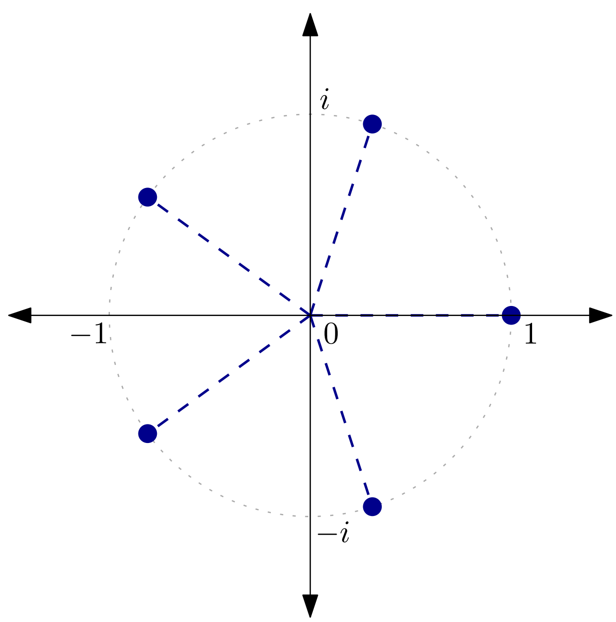
Středoškolská odborná činnost

Odmocniny z jedné v kombinatorice

Obor č. 1 – Matematika a statistika



Tomáš Pazourek

Jihomoravský kraj

Brno 2025

Středoškolská odborná činnost

Odmocniny z jedné v kombinatorice
Roots of Unity in Combinatorics

Obor č. 1 – Matematika a statistika

Autor: Tomáš Pazourek
Škola: Gymnázium Brno, tř. Kpt. Jaroše, p. o.
Kraj: Jihomoravský
Vedoucí práce: Zdeněk Pezlar

Brno 2025

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné. Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Brně dne: ....   Podpis: ....

Poděkování

Tímto děkuji především vedoucímu práce, Zdeňku Pezlarovi, za odborné vedení, cenné rady a připomínky poskytnuté v průběhu této práce. Velmi si vážím veškerého času, který mi ochotně věnoval. Také děkuji Pavlovi za motivaci v průběhu práce a Klárce i Martinovi za důkladnou kontrolu pravopisu.

Abstrakt

Cílem práce je uvést komplexní odmocniny z jedné jako výhodný nástroj na řešení problémů v kombinatorice a co nejvíce tyto úlohy zobecnit. Na základě jednoduché teorie jsou procházeny postupně složitější příklady. Ukazuje se, jak lze pomocí odmocnin z jedné řešit problém dláždění šachovnic, kde přispějeme značným zobecněním zejména případu s jedním prázdným políčkem. Také je dokázán vzorec pro součet každého n-tého Fibonacciho čísla, což je originální prací. Součty kombinačních čísel jsou navázány na počítání podmnožin, jejichž součet prvků je dělitelný určitým číslem. Příspěvek zde spočívá ve zobecnění této úlohy na určité dělitele a libovolné množiny. Jsou využívány zejména metody jako *Roots of Unity Filter* a generující funkce.

Klíčová slova

odmocniny z jedné; kombinatorika; komplexní čísla; Roots of Unity Filter; multisekce; dláždění šachovnic; polyomina; generující funkce; kombinatorické identity; Moivreova věta; Fibonacciho čísla

Abstract

This thesis aims to introduce complex roots of unity as a convenient tool for solving problems in combinatorics and to generalize these problems as much as possible. Based on simple theory, we study gradually more intricate examples. We show how roots of unity can be applied to solve chessboard tiling problems, where we contribute a significant generalization, especially in the case of one empty square. We also determine the sum of every n-th Fibonacci number, which is an original contribution. Sums of binomial coefficients are related to counting subsets whose sum of elements is divisible by a certain number. The contribution lies in generalizing this problem to specific divisors and arbitrary sets. Methods such as *Roots of Unity Filter* and generating functions are used.

Key words

roots of unity, combinatorics, complex numbers, Roots of Unity Filter, multisection, chessboard tiling, polyominoes, generating functions, combinatorial identities, De Moivre's theorem, Fibonacci numbers

Obsah

Úvod

Tato práce je zaměřená na aplikace odmocnin z jedné při řešení širokého spektra kombinatorických úloh, které zdánlivě vůbec nesouvisí s komplexními čísly. Snažíme se do co největší míry zobecnit tyto příklady. Podívejme se na úlohu 4.3.2 z 73. (loňského) ročníku Matematické olympiády [8], kterou jsem se rozhodl řešit právě pomocí odmocnin z jedné:

> Kolik neprázdných podmnožin množiny $\{0, 1, 2, \ldots, 9\}$ má součet prvků dělitelný třemi?

Tuto úlohu i její obecné varianty řešíme v kapitole 4. Řešení této úlohy jsem sepsal a odevzdal s využitím odmocnin z jedné, jak popisuji ve zmíněné kapitole. Tím se stala tato úloha výraznou motivací k sepsání celé této práce, a to spolu s videem [9], které uvedlo odmocniny z jedné právě v tomto kontextu.

První kapitola se věnuje teoretickému základu odmocnin z jedné. Nejprve jsou shrnuty základní vlastnosti komplexních čísel a odmocnin z jedné, jako je třeba rovnost 1.2.9, která říká, že pokud $\zeta = \cos(2\pi/n) + i \sin(2\pi/n)$ je n-tá odmocnina z jedné, potom platí

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0.$$

Následně je představen pojem multisekce, který bude v dalších kapitolách klíčový.

Druhá kapitola se soustředí na dláždění šachovnic polyominy. Zde jsou příspěvkem zejména významná zobecnění. Jednu z úloh zmínil Jakub Juránek ve své práci [5], na kterou tímto navážeme zobecněním pro libovolnou obdélníkovou šachovnici s chybějícím libovolným políčkem a obecným obdélníkovým polyominem.

Třetí kapitola je významná nalezením vzorce pro součet každého n-tého Fibonacciho čísla ve větě 3.2.12, což jsem v žádné literatuře nedohledal – známé jsou pouze identity pro součet každého a každého druhého členu posloupnosti. Kromě toho zmíníme součty kombinačních čísel jako výsledek potřebný k následující kapitole 4.

Ve čtvrté kapitole se počítají podmnožiny, jejichž součet prvků je dělitelný daným číslem. Kapitola přispěje řešením pro zcela libovolnou množinu zejména pro dělitele 3 a 5. Tyto výsledky jsou navíc založeny na součtech kombinačních čísel z třetí kapitoly. Výsledku se ve všech ostatních případech lze přiblížit využitím řady lemmat, čímž se výsledek postupně zjednoduší. Využito je zde pokročilejších metod, jako je *Roots of Unity Filter*, a věty o prvočíselných odmocninách z jedné a generující funkce.

V práci se ukazuje, jak lze odmocniny z jedné využít k řešení mnoha kombinatorických úloh, které je možné následně velmi značně zobecnit a najít řešení pro mnohem širší třídu problémů. V práci se také objevuje řada nových výsledků, které nebyly dosud publikovány.

Použité značení

$a \mid b$	a dělí b
$\mathbb{N} = \{1, 2, 3, \dots\}$	množina přirozených čísel
$\mathbb{Z}$	množina celých čísel
$\mathbb{Q}$	množina racionálních čísel
$\mathbb{R}$	množina reálných čísel
$\mathbb{C}$	množina komplexních čísel
$\gcd$	největší společný dělitel
F_n	n-té Fibonacciho číslo
L_n	n-té Lucasovo číslo
$\lfloor x \rfloor$	dolní celá část
$\lfloor x \rceil$	zaokrouhlení na nejbližší celé číslo
$\varphi(n)$	počet nesoudělných přirozených čísel menších než n
$\chi_m^r(n)$	součet každého kombinačního čísla $\binom{n}{j}$, kde $j \equiv r \pmod m$
$\mathcal{F}_m(n)$	součet všech Fibonacciho čísel F_j, kde $0 \leq j \leq n$ a $j \equiv n \pmod m$
$a^{(r)}$	počet podmnožin se součtem kongruentním r modulo m
$\mathcal{A}_m^r$	počet podmnožin se součtem kongruentním r modulo m
$\mathbb{Z}_d$	okruh zbytků modulo d
a^{-1}	multiplikativní inverze čísla a
$K[x]$	okruh polynomů nad tělesem K
$\Re(z)$	reálná složka komplexního čísla z
$\Im(z)$	imaginární složka komplexního čísla z

Kapitola 1

Teoretický základ odmocnin z jedné

V této kapitole se nejen zaměříme na teoretický základ komplexních čísel a odmocnin z jedné, ale také představíme jejich některé zásadní vlastnosti a definujeme si pojem multisekce. To představuje základ, z nějž budeme vycházet při řešení úloh v dalších kapitolách.

Komplexní čísla mají své kořeny v 16. století, kdy italský matematik Girolamo Cardano narazil při řešení rovnic třetího stupně na hodnoty, které nebyly reálné. Pro práci s těmito hodnotami zavedl imaginární jednotku i s vlastností $i^2 = -1$, čímž položil základ pro algebraický zápis komplexních čísel $z = x + yi$, kde x a y jsou reálná čísla.

Každé komplexní číslo můžeme zobrazit jako bod v komplexní rovině, která obsahuje reálnou osu (osa x) a imaginární osu (osa y). V rámci této kapitoly nejprve představíme základní formy zápisu komplexních čísel a poté vkročíme do pojmu komplexních odmocnin z jedné.

1.1 Algebraický a goniometrický zápis

Uveďme si dva způsoby zápisu komplexních čísel a také důležité vlastnosti komplexně sdruženého čísla i argumentu.

Komplexní čísla jsou většinou definována pomocí jejich reálné a imaginární složky, ale existuje i jiný užitečný tvar zápisu. Pokud $z \in \mathbb{C}$, pak lze psát

(i) v algebraickém tvaru, $z = a + bi$,

(ii) v goniometrickém tvaru, $z = r(\cos\varphi + i\sin\varphi)$,

kde $r = \sqrt{a^2 + b^2}$ představuje velikost (absolutní hodnotu) čísla z a úhel $\varphi \in [0, 2\pi)$ je jeho argument, který značíme $\arg z$.

Definice 1.1.1. *Absolutní hodnota* komplexního čísla $z = a + bi$ je reálné číslo $|z|$ splňující

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

Pokud napíšeme číslo v goniometrickém tvaru $z = r(\cos\varphi + i\sin\varphi)$, tak jeho absolutní hodnotu lze určit jako

$$|z| = \sqrt{r^2(\cos^2\varphi + \sin^2\varphi)} = \sqrt{r^2} = r.$$

Definice 1.1.2. *Sdružené číslo* komplexnímu číslu $z = a + bi$ definujme jako

$$\overline{z} = a - bi.$$

Uveďme podstatné vlastnosti násobení komplexních čísel a jejich sdružování.

Věta 1.1.3 ([3])**.** *Nechť z, w jsou komplexní čísla, pak*

(i) $z\overline{z} = |z|^2$;

(ii) $\overline{z + w} = \overline{z} + \overline{w}, \overline{z \cdot w} = \overline{z} \cdot \overline{w}$;

(iii) $|z| = |\overline{z}|$;

(iv) $|zw| = |z| \cdot |w|, |\frac{z}{w}| = \frac{|z|}{|w|}$;

(v) $\arg(zw) = \arg z + \arg w$.

1.2 Komplexní odmocniny z jedné

Vyjdeme z vlastnosti, kterou z definice splňuje každá n-tá odmocnina z jedné, a následně zjistíme algebraický tvar každého takového čísla. Využijeme přitom Moirvreovu větu 1.2.4. Dále definujeme pojem primitivní odmocniny z jedné a uvedeme některé jejich zásadní vlastnosti spolu s rovnostmi, které budeme dále využívat v následujících kapitolách.

Definice 1.2.1. Pro dané $n \in \mathbb{N}$ rozumíme n-tou *odmocninou z jedné* číslo $z \in \mathbb{C}$ splňující

$$z^n = 1.$$

Příklad 1.2.2. Pro příklad druhé odmocniny jsou 1 a -1. Čtvrté odmocniny pak umíme určit jako $1, i, -1, -i$.

Lemma 1.2.3. Pokud ζ je n-tá odmocnina z jedné, pak existuje $\varphi \in [0, 2\pi)$ takové, že

$$\zeta = \cos\varphi + i\sin\varphi.$$

Důkaz. Z definice platí rovnost $\zeta^n = 1$. Pokud srovnáme absolutní hodnoty a upravíme, tak platí $1 = |\zeta^n| = |\zeta|^n$ a odmocněním dostáváme $1 = |\zeta|$. Stačí nám psát v goniometrickém tvaru, kde $r = |\zeta| = 1$. □

Věta 1.2.4 (Moivreova věta)**.** *Pro každé reálné x a každé celé n platí*

$$(\cos x + i\sin x)^n = \cos nx + i\sin nx.$$

Důkaz. Pro celé n nazvěme $V(n)$ výrok $(\cos x + i \sin x)^n = \cos nx + i \sin nx$.

Pro $n \geq 0$ postupujme matematickou indukcí. Výrok $V(0)$ zjevně platí. Nyní předpokládejme, že $V(k)$ je pravdivé pro nějaké $k \geq 0$. Uvažme $V(k+1)$, kde po indukčním předpokladu použijeme sčítání argumentů z věty 1.1.3.

$$\begin{aligned}(\cos x + i \sin x)^{k+1} &= (\cos x + i \sin x)^k (\cos x + i \sin x)\\ &\overset{\text{IP}}{=} (\cos kx + i \sin kx)(\cos x + i \sin x)\\ &= \cos((k+1)x) + i \sin((k+1)x),\end{aligned}$$

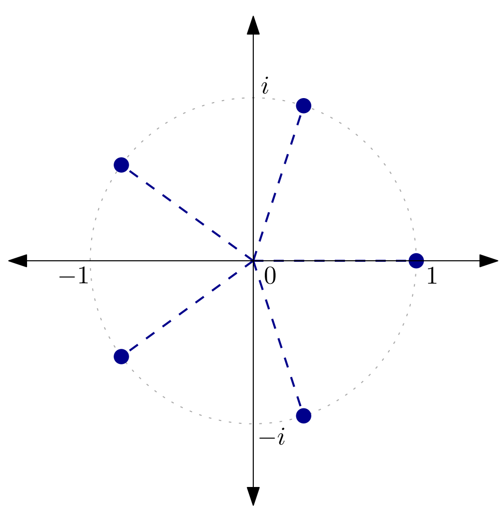
tudíž platí $V(n)$ pro každé $n \geq 0$. Konečně pro záporný exponent $n < 0$ pišme

$$\begin{aligned}(\cos x + i \sin x)^n &= \frac{1}{(\cos x + i \sin x)^{-n}} \overset{V(-n)}{=} \frac{1}{\cos(-nx) + i \sin(-nx)} =\\ &= \frac{\cos(-nx) - i \sin(-nx)}{\cos^2(-nx) + \sin^2(-nx)} = \cos(-nx) - i \sin(-nx) =\\ &= \cos(nx) + i \sin(nx),\end{aligned}$$

čímž jsme hotovi. □

Věta 1.2.5. *Je dáno n přirozené. Pokud ζ je n-tou odmocninou z jedné, pak existuje celé číslo $k \in \{0, 1, \ldots, n-1\}$ tak, že platí*

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



Obrázek 1.1: Páté odmocniny z jedné

Důkaz. Z lemmatu 1.2.3 pišme $\zeta = \cos \varphi + i \sin \varphi$. Vyjdeme opět z definice, že $1 = \zeta^n$. Umocnění zjednodušíme Moivreovou větou 1.2.4.

$$\zeta^n = (\cos \varphi + i \sin \varphi)^n = \cos n\varphi + i \sin n\varphi.$$

Srovnáme argumenty obou stran. Argument čísla $\zeta^n = 1$ je 0, zatímco na pravé straně se rovná $n\varphi$. Existuje tedy celé číslo k tak, že platí $n\varphi = 0 + 2k\pi$ čili

$$\varphi = \frac{2k\pi}{n}.$$

Vzhledem k periodicitě funkcí sin a cos získáme různé úhly právě pro $k \in \{0, \dots, n-1\}$. $\square$

Lemma 1.2.6. Množina všech n-tých odmocnin z jedné je multiplikativní s neutrálním prvkem 1.

Důkaz. Označme $\zeta = \cos(2k\pi/n) + i\sin(2k\pi/n)$ a $\xi = \cos(2\ell\pi/n) + i\sin(2\ell\pi/n)$. Potom ze sčítání argumentů komplexních čísel platí

$$\zeta \cdot \xi = \cos\left(2(k+\ell)\pi/n\right) + i\sin\left(2(k+\ell)\pi/n\right),$$

což je též n-tá odmocnina z jedné. $\square$

Zejména pokud si vezmeme $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$ a umocňujeme ji, tak z Moivreovy věty získáváme další odmocniny z jedné.

$$\zeta^k = \cos\left(2k\pi/n\right) + i\sin\left(2k\pi/n\right).$$

Definice 1.2.7. Libovolná n-tá odmocnina z jedné ζ je *primitivní*, pokud nejnižší přirozený exponent x splňující $\zeta^x = 1$ je $x = n$.

Poznámka. Tato úvaha je důležitá, protože některé n-té odmocniny z jedné jsou zároveň i menšími odmocninami, a stačí jim tedy i menší exponent. Například pokud si vezmeme devátou odmocninu z jedné $\zeta = \cos(2\pi/9) + i\sin(2\pi/9)$, pak $\zeta^3 = \cos(2\pi/3) + i\sin(2\pi/3)$ je sice také devátou odmocninou, ale současně je třetí (menší) odmocninou z jedné a platí rovnost $(\zeta^3)^3 = 1$. Mezi čísly ζ a ζ^3 je rozdíl v tom, kolik různých hodnot mohou jejich mocniny nabývat. Vzhledem k tomu, že ζ^3 má různé mocniny pouze $1, \zeta^3, \zeta^6$, tak ji nenazýváme primitivní devátou odmocninou, nýbrž je to primitivní třetí odmocnina. Dokonce platí, že ζ^a je primitivní devátou odmocninou, pokud a je nesoudělné s devíti.

Lemma 1.2.8. Pokud ζ je primitivní n-tou odmocninou z jedné, pak se mezi jejími mocninami $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ vyskytuje každá n-tá odmocnina z jedné právě jednou.

Důkaz. Předpokládejme, že se některá dvě čísla rovnají, $\zeta^x = \zeta^y$, kde $x, y \in \{0, \dots, n-1\}$. Potom vydělením rovnosti platí $\zeta^{x-y} = 1$. Vzhledem k tomu, že ζ je primitivní, tak platí dělitelnost $n \mid x - y$. To ale v množině $\{0, \dots, n-1\}$ splňuje jedině dvojice $x = y$. Navíc z lemmatu 1.2.6 se v řadě čísel nevyskytuje nic jiného než n-té odmocniny z jedné. $\square$

1.2.1 Zásadní identity

Věta 1.2.9. *Pokud $\zeta \neq 1$ je n-tou odmocninou z jedné, pak platí*

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0.$$

Důkaz. Jedná se o součet n členů geometrické řady s kvocientem $\zeta \neq 1$ a platí $\zeta^n = 1$.

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = \frac{\zeta^n - 1}{\zeta - 1} = \frac{1-1}{\zeta - 1} = 0.$$

□

Věta 1.2.10. *Je dáno přirozené n a primitivní n-tá odmocnina z jedné ζ. Potom platí*

$$f(\zeta) = (1+\zeta)(1+\zeta^2)\cdots(1+\zeta^n) = \begin{cases} 2, & \textit{pokud je } n \textit{ liché,} \\ 0, & \textit{pokud je } n \textit{ sudé.} \end{cases}$$

Důkaz. Známe n kořenů polynomu $z^n - 1$, a to navzájem různá čísla $1, \zeta, \zeta^2 \ldots, \zeta^{p-1}$, takže jej umíme napsat v součinovém tvaru.

$$z^n - 1 = (z-1)(z-\zeta)(z-\zeta^2)\cdots(z-\zeta^{p-1}).$$

Substitucí $z = -1$ získáme rovnost

$$\begin{aligned} (-1)^n - 1 &= (-1)^n(1+1)(1+\zeta)(1+\zeta^2)\cdots(1+\zeta^{n-1}), \\ 1 - (-1)^n &= (1+\zeta)(1+\zeta^2)\cdots(1+\zeta^{n-1})(1+\zeta^n). \end{aligned}$$

Levá strana se rovná 2, pokud je n liché, zatímco nule, pokud je n sudé. □

Důsledek 1.2.11. Jsou dána přirozená čísla n, k a primitivní n-tá odmocnina z jedné ζ. Označme $d = n/\gcd(n,k)$. Potom platí

$$f(\zeta^k) = (1+\zeta^k)(1+\zeta^{2k})\cdots(1+\zeta^{nk}) = \begin{cases} 2^{n/d} = 2^{\gcd(n,k)}, & \text{pokud je } d \text{ liché,} \\ 0, & \text{pokud je } d \text{ sudé.} \end{cases}$$

Důkaz. Číslo ζ^k je primitivní d-tou odmocninou z jedné, takže z věty 1.2.10 platí rovnost $(1+\zeta^k)(1+\zeta^{2k})\cdots(1+\zeta^{dk}) = 2$. Tento součin se v $f(\zeta^k)$ zopakuje dohromady $\frac{n}{d}$-krát čili $\gcd(n,k)$-krát. □

Úloha 1.2.12. Pro $a \in \mathbb{Z}$ a $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$ určete součet čísel

$$S_a = 1 + \zeta^a + \zeta^{2a} + \cdots + \zeta^{(n-1)a}.$$

Řešení. Rozlišme dva případy na základě dělitelnosti parametru a číslem n. Pokud $n \nmid a$, pak se jedná o geometrickou řadu s kvocientem $\zeta^a \neq 1$.

$$S_a = \sum_{k=0}^{n-1} \zeta^{ak} = \frac{\zeta^n - 1}{\zeta^a - 1} = \frac{1-1}{\zeta^a - 1} = 0.$$

Naopak pokud $n \mid a$, pak pišme $a = nm$ pro nějaké m. Platí $\zeta^{ak} = \zeta^{nmk} = 1^{mk} = 1$.

$$\sum_{k=0}^{n-1} \zeta^{ak} = \sum_{k=0}^{n-1} 1 = n.$$

Pokud a není dělitelné n, pak vyjde součet 0, jinak je součtem číslo n. $\square$

Tento příklad naznačuje obecnější trend spočívající v rozlišení, zda platí $\zeta^a = 1$, tedy zda je parametr dělitelný číslem n.

Následující věta nám pomůže dále.

Věta 1.2.13 (Eisensteinovo kritérium)**.** *Je-li $f(x) = a_0 + a_1x + \cdots + a_nx^n$ polynom s celočíselnými koeficienty a existuje prvočíslo p dělící všechny koeficienty kromě vedoucího, ale $p^2 \nmid a_0$, pak je f ireducibilní nad $\mathbb{Q}$.*

Máme-li prvočíslo p, pak p-té odmocniny mají navíc zvlášť výhodnou vlastnost. Následující věta naznačuje, jak při sčítání jejich mocnin získáme jistou lineární nezávislost mezi nimi.

Věta 1.2.14. *Pokud p je prvočíslo a $a_0, a_1, \ldots, a_{p-1}$ jsou racionální čísla splňující*

$$a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} = 0,$$

kde $\zeta = \cos(2\pi/p) + i\sin(2\pi/p)$, pak $a_0 = a_1 = \cdots = a_{p-1}$.

Důkaz. Nechť $P(x) = 1 + x + \cdots + x^{p-1}$. Ukážeme, že P je ireducibilní. Podívejme se tedy na jeho „posunutý polynom"

$$P(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \binom{p}{1} + \binom{p}{2}x + \cdots + \binom{p}{p-1}x^{p-2} + x^{p-1},$$

který má koeficienty tvaru $\binom{p}{k}$, což rozepsáním na podíl $p!/k!(p-k)!$ je zjevně dělitelné prvočíslem p (pro $0 < k < p$) a současně je konstantní člen roven p, tedy žádný kvadrát prvočísla jej nedělí. $P(x+1)$ proto splňuje Eisensteinovo kritérium 1.2.13, takže je ireducibilní nad $\mathbb{Q}$.

Předpokládejme nyní, že $P(x)$ je reducibilní. Potom existují nekonstantní polynomy s racionálními koeficienty R, S takové, že $P(x) = R(x) \cdot S(x)$, a tedy dosazením $x+1$ platí rovnost $P(x+1) = R(x+1) \cdot S(x+1)$, což je součinem dvou nekonstantních polynomů z $\mathbb{Q}[x]$. Sporem je tedy $P(x)$ též ireducibilní.

Dosazením ζ do P platí $P(\zeta) = (\zeta^p - 1)/(\zeta - 1) = 0$. Také polynom $a_0 + a_1x + \cdots + a_{p-1}x^{p-1}$ má ze zadání kořen ζ. Jelikož mají tyto dva polynomy společný dělitel a P je ireducibilní, tak P dělí oba z nich. Vzhledem k jejich shodnému stupni se polynomy liší pouze vynásobením konstantou. Všechny koeficienty u P jsou shodné, takže se neliší ani u polynomu $a_0 + a_1x + \cdots + a_{p-1}x^{p-1}$, což jsme chtěli ukázat. $\square$

1.3 Multisekce mocninné řady

Uvedeme si jednoduchý příklad, kde pomocí binomické věty sečteme každé druhé kombinační číslo. Dále tuto ideu zobecníme na mocninné řady – vyfiltrování všech členů kromě každého n-tého budeme nazývat multisekcí. Připomeneme si také tzv. Roots of Unity Filter, což je přímým důsledkem multisekce.

Věta 1.3.1 (Binomická věta)**.** *Pro nenulová $A, B \in \mathbb{C}$ a $n \in \mathbb{N}$ platí*

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^{n-k} B^k.$$

Úloha 1.3.2. Kolik podmnožin $\{1, 2, \ldots, n\}$ má sudý součet prvků?

Není složité si rozmyslet, že libovolných podmnožin je celkem 2^n, neboli

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n. \tag{1.1}$$

Tento výsledek lze získat rozepsáním rovnosti $(1+1)^n = 2^n$ podle binomické věty 1.3.1. Chtěli bychom znát $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots$, což se rovná počtu sudých podmnožin. Překvapivě se můžeme k výsledku dostat dalším využitím binomické věty. Stačí rozepsat rovnost $(1-1)^n = 0$, čímž získáváme střídavě sčítání a odčítání těchto kombinačních čísel.

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0. \tag{1.2}$$

Sečtením rovností (1.1) a (1.2) se nám podaří eliminovat liché podmnožiny tak, že nám zbývají pouze členy

$$2\binom{n}{0} + 2\binom{n}{2} + 2\binom{n}{4} + \cdots = 2^n + 0$$

čili výsledný počet 2^{n-1} získáme vydělením dvěma.

Využili jsme zde cykličnost funkce $(-1)^n$, kde -1 je primitivní druhá odmocnina z jedné. Pomocí ní jsme získali každé druhé kombinační číslo. V kapitole 4 ukážeme, jak lze stejným způsobem získat součet každého m-tého kombinačního čísla. Tento postup však vychází z tzv. multisekce libovolné mocninné řady.

Definice 1.3.3. *Multisekcí* mocninné řady f rozumíme další mocninnou řadu skládající se z určitých členů f takových, že mají konstantní rozestupy.

Máme-li mocninnou řadu $1 + 2x + 3x^2 + 4x^3 + 5x^4 + 6x^5 + 7x^6 + \ldots$, tak její multisekcí je například $1 + 4x^3 + 7x^6 + \ldots$, kde se vyskytuje pouze každý třetí člen.

Věta 1.3.4 (Multisekce)**.** *Je dána mocninná řada $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$ a přirozené číslo m. Potom platí*

$$a_0 + a_m x^m + a_{2m} x^{2m} + \cdots = \frac{f(x) + f(\zeta x) + f(\zeta^2 x) + \cdots + f(\zeta^{m-1} x)}{m},$$

kde $\zeta = \cos(2\pi/m) + i \sin(2\pi/m)$ je primitivní m-tou odmocninou z jedné.

Důkaz. Dosazením čísla ζx do mocninné řady se cyklicky střídají mocniny ζ.

$$f(\zeta x) = a_0 + \zeta a_1 x + \zeta^2 a_2 x^2 + \dots + a_m x^m + \zeta a_{m+1} x^{m+1} + \dots$$

Dosadíme obecně $\zeta^k x$, kde k je celé číslo.

$$f(\zeta^k x) = a_0 + \zeta^k a_1 x + \zeta^{2k} a_2 x^2 + \dots + a_m x^m + \zeta^k a_{m+1} x^{m+1} + \dots \tag{1.3}$$

Získaných m rovností pro $k = 0, 1, 2, \dots, m-1$ sečteme, čímž dostaneme mocninnou řadu, kde u x^j je koeficient

$$a_j(1 + \zeta^j + \zeta^{2j} + \dots + \zeta^{(m-1)j}).$$

Z výsledku příkladu 1.2.12 platí

$$1 + \zeta^j + \zeta^{2j} + \dots + \zeta^{(m-1)j} = \begin{cases} m, & \text{pro } m \mid j, \\ 0, & \text{jinak.} \end{cases}$$

Takže se ve výsledné mocninné řadě vyskytují pouze členy $a_j x^j$, kde $m \mid j$, a to s koeficientem m.

$$f(x) + f(\zeta x) + f(\zeta^2 x) + \dots + f(\zeta^{m-1} x) = m a_0 + m a_m x^m + m a_{2m} x^{2m} + \dots.$$

Vydělením číslem m získáme dokazovanou větu. □

Věta 1.3.5 (Roots of Unity Filter)**.** *Definujme* $\zeta = \cos(2\pi/m) + i \sin(2\pi/m)$ *pro přirozené číslo* m*. Pro mocninnou řadu* $f(x) = a_0 + a_1 x + a_2 x^2 + \dots$ *je součet každého* m*-tého koeficientu daný vztahem*

$$a_0 + a_m + a_{2m} + a_{3m} + \dots = \frac{f(1) + f(\zeta) + f(\zeta^2) + \dots + f(\zeta^{m-1})}{m}.$$

Důkaz. Plyne přímo z multisekce 1.3.4 po dosazení $x = 1$. □

Na podobném principu jako je multisekce 1.3.4 lze sečíst každý m-tý člen, přičemž začínáme u r-tého, kde $r \in \{0, 1, \dots, m-1\}$.

Stačí vynásobit každou funkční hodnotu konstantou tak, aby u správných členů vyšel nenulový koeficient.

Věta 1.3.6 (Obecná multisekce)**.** *Je dáno přirozené číslo* m *a* $r \in \{0, 1, \dots, m-1\}$*. Definujme* $\zeta = \cos(2\pi/m) + i \sin(2\pi/m)$*. Pro mocninnou řadu* $f(x) = a_0 + a_1 x + a_2 x^2 + \dots$ *je součet každého* m*-tého členu počínaje* r*-tým roven*

$$a_r + a_{m+r} x^{m+r} + \dots = \frac{f(x) + \zeta^{-r} f(\zeta x) + \zeta^{-2r} f(\zeta^2 x) + \dots + \zeta^{-(m-1)r} f(\zeta^{m-1} x)}{m}.$$

Důkaz probíhá analogicky jako u věty 1.3.5.

Věta 1.3.7 (Obecný Roots of Unity Filter)**.** *Je dáno přirozené číslo* m *a* $r \in \{0, \dots, m-1\}$*. Definujme* $\zeta = \cos(2\pi/m) + i \sin(2\pi/m)$*. Pro mocninnou řadu* $f(x) = a_0 + a_1 x + a_2 x^2 + \dots$ *je součet každého* m*-tého koeficientu počínaje* r*-tým roven*

$$a_r + a_{m+r} + a_{2m+r} + \dots = \frac{f(1) + \zeta^{-r} f(\zeta) + \zeta^{-2r} f(\zeta^2) + \dots + \zeta^{-(m-1)r} f(\zeta^{m-1})}{m}.$$

Důkaz. Plyne z věty 1.3.6 dosazením $x = 1$. □

Kapitola 2

Dláždění šachovnic polyominy

Dláždění je častým problémem olympiádní matematiky. Plochu chceme vyplnit určitým tvarem desek (zejména polyominy), případně ukázat, že takové vyplnění neexistuje. V této kapitole se zaměříme na dláždění obdélníkových i čtvercových šachovnic různými polyominy.

Touto kapitolou přispějeme k charakterizaci šachovnic, kterým zbyde jediné prostřední políčko po vyplnění polyominy $1 \times k$ a $k \times 1$. Andreescu a Dospinescu [1] i Jakub Juránek [5] řeší konkrétní rozměry šachovnice i polyomina. Přispěji dokázáním obecné věty 2.1.3.

Dále v podobném problému s obdélníkovou šachovnicí uvažujeme jediné prázdné políčko a hledáme jeho souřadnice. Určité zobecnění zmiňuje Jakub Juránek ve své práci [5], já na to navazuji obecnou obdélníkovou šachovnicí a libovolným polyominem ve větě 2.1.9.

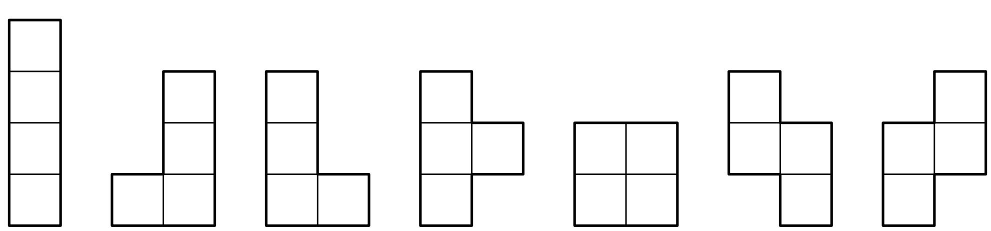
Kromě toho vyřešíme problém kompletního vyplnění šachovnice v následující sekci 2.2, kde navíc představíme známý *Rectangle Tiling Problem* 2.2.1 a také De Bruijnovy věty 2.2.2 uvažující kvádr a cihly ve více dimenzích.

Z kapitoly 1 zde využijeme zejména jednu zásadní vlastnost, a to rovnost 1.2.9,

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0,$$

kde $\zeta = \cos(2\pi/n) + i \sin(2\pi/n)$ je primitivní n-tou odmocninou z jedné.

Poznámka. Různých tetromin existuje sedm.



Obrázek 2.1: Různá tetromina. Zleva I-, J- L-, T-, O-, S-, Z-tetromino.

Podobně jako tetromina uvažujeme domina, trimina a obecně polyomina. Jedná se o souvislý útvar tvořený několika shodnými čtverci.

2.1 Chybějící políčka v šachovnici

Úloha 2.1.1 (Motivační)**.** Šachovnici o velikosti 8×8 jsme odebrali dvě protější rohová políčka. Rozhodněte, zda ji lze zcela pokrýt dominy.

Tato úloha je příkladem, kde dokazujeme, proč šachovnice nelze vyplnit. Standardně se řeší obarvováním. Pokud uvažujme bíločerné šachovnicové obarvení, pak každé domino zakryje jedno černé a jedno bíle pole. Na začátku je na šachovnici různý počet černých a bílých polí, tudíž ji nevyplníme.

Na této úloze budeme ilustrovat, jakým způsobem je možné místo barev využít čísla. Konkrétně nám budou stačit dvě čísla, 1 a -1.

Řešení. Předpokládejme, že je šachovnice skutečně pokrytá. Každému políčku přiřadíme buď číslo 1, nebo -1 tak, aby spolu sousedily vždy různé hodnoty (např. 1 na bílá a -1 na černá políčka). Docílíme toho, že každé položené domino zakrývá právě políčka 1 a -1 (v některém pořadí). Tudíž zakrývá políčka se součtem 0.

Protější rohy leží na diagonále, tudíž by byly očíslovány stejně. Bez újmy na obecnosti předpokládejme, že na chybějících políčkách bylo číslo 1. Součet všech čísel na šachovnici tedy není 0, ale je o $2 \cdot 1$ menší.

Součet čísel na upravené šachovnici je -2, avšak pokud by ji bylo možné pokrýt, byl by součet roven 0. □

2.1.1 Prázdné prostřední políčko

Zde vyplňujeme čtvercovou šachovnici, kde chybí právě prostřední políčko, pomocí obdélníkových polyomin, typicky šířky či délky 1. Začneme s úlohou s konkrétními rozměry šachovnice i polyomin, kterou řeší Andreescu a Dospinescu [1] i Jakub Juránek [5], ale obecnou větu dokážu až v 2.1.3.

Úloha 2.1.2. Šachovnici 13×13 chybí prostřední políčko. Ukažte, že tato šachovnice nelze pokrýt tetrominy 1×4 a 4×1.

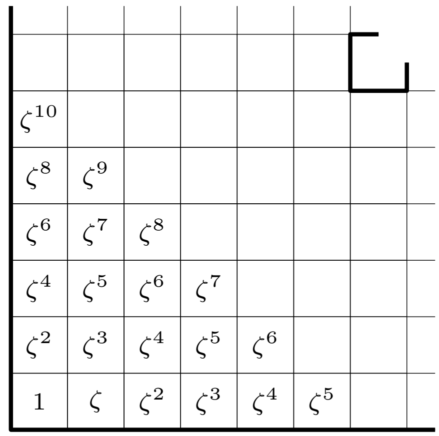
Při šachovnicovém očíslování nezískáme žádnou novou informaci, jelikož, na rozdíl od příkladu výše, je zde součet všech čísel v tabulce nulový. Proto je třeba využít složitější očíslování.

Každé tetromino pokrývá 4 políčka najednou, takže je možnost využít *komplexnější* očíslování. Čísla $1, i, -1, -i$ dávají součet 0 a současně stejnou vlastnost mají dvojice $1, -1$ a $i, -i$. Uvažujme následující očíslování.

Řešení. Předpokládejme, že je šachovnice vyplněná. Každému políčku přiřaďme jedno číslo takovým způsobem, že pokud je v a-tém sloupci a b-tém řádku (číslujme od 0), pak tomuto políčku přidělíme číslo i^{a+2b}, kde i je primitivní čtvrtá odmocnina z jedné.

Pokud je položené libovolné tetromino 4×1 (vodorovné), pak součet hodnot na pokrytých políčkách je

$$i^{a+2b} + i^{a+1+2b} + i^{a+2+2b} + i^{a+3+2b} = i^{a+2b} \cdot \frac{i^4 - 1}{i - 1} = 0.$$



Obrázek 2.2: Očíslování šachovnice 13×13 s chybějícím prostředním políčkem

Pro tetromino 1×4 (svislé) je součet hodnot

$$i^{a+2b} + i^{a+2b+2} + i^{a+2b+4} + i^{a+2b+6} = i^{a+2b} \cdot \frac{i^8 - 1}{i^2 - 1} = 0.$$

Označme S součet všech čísel v šachovnici včetně středu. Spočítáme S jako součet všech pokrytých políček (dohromady nula) plus číslo ve středovém políčku, což je $i^{6+2\cdot 6}$. Platí tedy $S = i^{18} = i^2 = -1$. Součet S také umíme spočítat jiným způsobem.

$$\begin{aligned} S &= \sum_{a=0}^{12} \sum_{b=0}^{12} i^{a+2b} = \sum_{a=0}^{12} \sum_{b=0}^{12} i^a \cdot i^{2b} = \sum_{a=0}^{12} \left(i^a \cdot \sum_{b=0}^{12} i^{2b} \right) \\ &= \left(\sum_{b=0}^{12} i^{2b} \right) \left(\sum_{a=0}^{12} i^a \right) = \frac{i^{26} - 1}{i^2 - 1} \cdot \frac{i^{13} - 1}{i - 1} = 1 \cdot 1 = 1. \end{aligned}$$

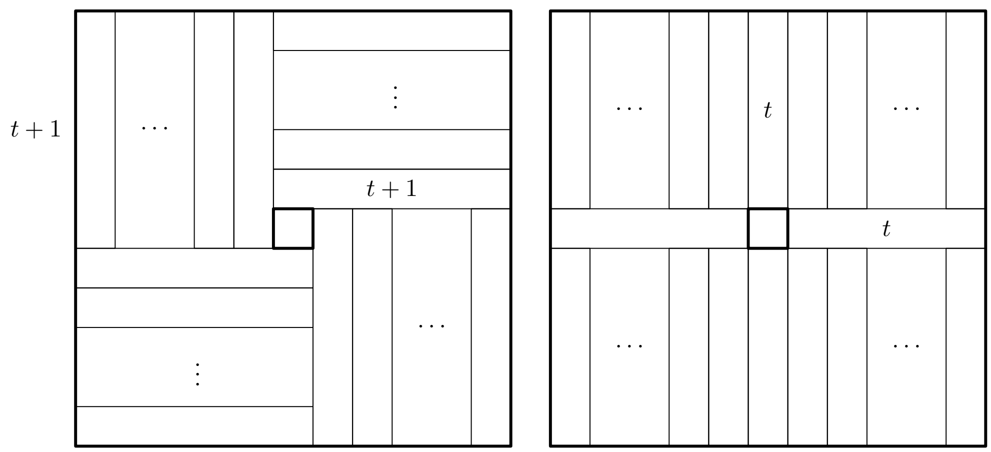
Spočítali jsme S dvěma různými způsoby, ale v obou případech vyšel jinak, $-1 \neq 1$. To je spor s předpokladem, že jsme mohli vyplnit tabulku. □

Pro tyto konkrétní hodnoty šachovnice nelze pokrýt. Podívejme se na obecnou velikost šachovnice a polyomina.

Věta 2.1.3 (Vlastní). *Máme šachovnici $n \times n$, kde $n > 1$ je liché, s chybějícím prostředním políčkem. K vyplnění jsou k dispozici obdélníky $1 \times k$ a $k \times 1$. Potom šachovnici lze zaplnit právě tehdy, když $2k$ dělí jedno z čísel $n - 1$ nebo $n + 1$.*

Důkaz. Pišme $n = 2t + 1$ pro $t \geq 0$ a číslujme souřadnice $(0,0), \ldots, (2t, 2t)$. Středové políčko je tedy (t, t).

Nejprve názorně pomocí obrázku ukažme konstrukce pro případy, kdy $k \mid t$ nebo $k \mid t+1$, a následně ukážeme, že pokud šachovnici nelze tímto způsobem *triviálně* vyplnit, pak ji nelze vyplnit vůbec.



Obrázek 2.3: Vyplnění šachovnice $(2t+1) \times (2t+1)$ obdélníky $1 \times k$, kde platí $k \mid (t+1)$ nebo $k \mid t$. Obdélník $1 \times (t+1)$ nebo $1 \times t$ získáme spojením několika obdélníků $1 \times k$.

Pokud $k = 1$, pak platí $k \mid t$. Pro $k = 2$ je jedno z po sobě jdoucích čísel t a $t+1$ dělitelné dvěma. Dále mějme $k > 2$ a definujme

$$\zeta = \cos(2\pi/k) + i \sin(2\pi/k)$$

jako primitivní k-tou odmocninu z jedné. Předpokládejme, že všechna políčka kromě prostředního jsou pokrytá.

Nejprve očíslujme každé políčko takovým způsobem, že políčku na (x, y) přiřadíme číslo ζ^{x+y}. Každý obdélník zakryje k po sobě jdoucích mocnin ζ, což se rovná nule. Součet všech čísel v šachovnici spočítáme jako

$$\sum_{x=0}^{2t} \sum_{y=0}^{2t} \zeta^x \zeta^y = \left(\sum_{x=0}^{2t} \zeta^x \right) \left(\sum_{y=0}^{2t} \zeta^y \right) = \left(\frac{\zeta^{2t+1} - 1}{\zeta - 1} \right)^2.$$

Číslo uprostřed šachovnice je $\zeta^{t+t} = \zeta^{2t}$. Zároveň se všechna pokrytá čísla sečtou na nulu, takže se ζ^{2t} rovná součtu všech čísel. Platí rovnost $(\zeta^{2t+1} - 1)^2 = \zeta^{2t}(\zeta - 1)^2$. Převedením na jednu stranu získáme

$$\begin{aligned} (\zeta^{2t+1} - 1)^2 - \zeta^{2t}(\zeta - 1)^2 &= 0 \\ (\zeta^{2t+1} - 1 + \zeta^t(\zeta - 1))(\zeta^{2t+1} - 1 - \zeta^t(\zeta - 1)) &= 0 \\ (\zeta^{2t+1} - 1 + \zeta^{t+1} - \zeta^t)(\zeta^{2t+1} - 1 - \zeta^{t+1} + \zeta^t) &= 0. \end{aligned}$$

Úpravou obou závorek na součin máme

$$(\zeta^t - 1)(\zeta^{t+1} + 1)(\zeta^t + 1)(\zeta^{t+1} - 1) = 0. \tag{2.1}$$

Nejprve se zabývejme variantou, kde k je liché. V tomto případě neexistuje celé číslo j takové, že $\zeta^j = -1$. Rovnost (2.1) tedy umíme vydělit $(\zeta^{t+1} + 1)(\zeta^t + 1) \neq 0$.

$$(\zeta^t - 1)(\zeta^{t+1} - 1) = 0.$$

Platí $\zeta^t = 1$ nebo $\zeta^{t+1} = 1$. V prvním případě $k \mid t$ a v druhém $k \mid t+1$.

Dále se zabývejme variantou pro sudé k a předpokládejme, že $k \nmid t$ a $k \nmid (t+1)$, ekvivalentně platí dvě rovnosti, $\zeta^t \neq 1$ a $\zeta^{t+1} \neq 1$.

Nyní očíslujme jiným způsobem. Do každého políčka na souřadnicích (x, y) vepišme číslo $(-1)^x \zeta^y$. Potom vertikální obdélník pokryje stejný počet čísel ζ^y jako $-\zeta^y$, tudíž zakryje v součtu nulu. Horizontální obdélník pokryje dohromady též 0 (stejně jako výše). Součet všech čísel je po tomto očíslování

$$\left(\sum_{x=0}^{2t} (-1)^x\right)\left(\sum_{y=0}^{2t} \zeta^y\right) = \left(\frac{(-1)^{2t+1} - 1}{-1-1}\right)\left(\frac{\zeta^{2t+1} - 1}{\zeta - 1}\right) = \frac{\zeta^{2t+1} - 1}{\zeta - 1},$$

což se rovná číslu $(-1)^t \zeta^t = (-\zeta)^t$ uprostřed, tudíž platí rovnost $(-\zeta)^t(\zeta - 1) = \zeta^{2t+1} - 1$. Převedením na jednu stranu rovnice platí

$$\begin{aligned} -\zeta^{2t+1} + (-\zeta)^t(\zeta - 1) + 1 &= 0, \\ (-\zeta)^{2t+1} - (-\zeta)^{t+1} - (-\zeta)^t + 1 &= 0, \\ ((-\zeta)^{t+1} - 1)((-\zeta)^t - 1) &= 0. \end{aligned}$$

(i) Pokud je t sudé, pak se rovnost zjednoduší na $(-\zeta^{t+1} - 1)(\zeta^t - 1) = 0$. Platí předpoklad, že $\zeta^t \neq 1$, takže vydělíme rovnost číslem $\zeta^t - 1 \neq 0$. Platí tedy $\zeta^{t+1} = -1$. Umocněním na druhou máme

$$\zeta^{2t+2} = 1, \tag{2.2}$$

takže platí $k \mid 2t + 2$.

(ii) V opačném případě je t liché, tedy $(\zeta^{t+1} - 1)(-\zeta^t - 1) = 0$. Z předpokladu $\zeta^{t+1} \neq 1$ zjednodušíme rovnost na $\zeta^t = -1$, takže umocněním

$$\zeta^{2t} = 1, \tag{2.3}$$

takže platí $k \mid 2t$.

Nakonec očíslujeme každé políčko (x, y) hodnotou ζ^{x+2y}. Vertikální obdélník s počátkem v (x, y) zakryje dohromady

$$\zeta^{x+2y}(1 + \zeta^2 + \zeta^4 + \cdots + \zeta^{2(k-1)}) = \zeta^{x+2y} \cdot \frac{\zeta^{2k} - 1}{\zeta^2 - 1} = 0,$$

jelikož $\zeta^2 \neq 1$ a $\zeta^k = 1$. Horizontální obdélník zakryje k po sobě jdoucích mocnin ζ, takže také přispívá nulou.

Součet všech čísel v šachovnici je

$$\left(\sum_{x=0}^{2t} \zeta^x\right)\left(\sum_{y=0}^{2t} \zeta^{2y}\right) = \left(\frac{\zeta^{2t+1} - 1}{\zeta - 1}\right)\left(\frac{\zeta^{4t+2} - 1}{\zeta^2 - 1}\right),$$

což se rovná číslu uprostřed, tj. ζ^{t+2t} neboli ζ^{3t}. Pokud vynásobíme rovnost jmenovateli, pak platí

$$\zeta^{3t}(\zeta - 1)(\zeta^2 - 1) = (\zeta^{2t+1} - 1)(\zeta^{4t+2} - 1). \tag{2.4}$$

(i) Nejprve předpokládejme, že t je liché. Z rovnosti (2.3) platí $\zeta^{2t} = 1$. Potom rovnost (2.4) výše se zjednoduší na

$$\begin{aligned} \zeta^t(\zeta-1)(\zeta^2-1) &= (\zeta-1)(\zeta^2-1). \\ (\zeta^t-1)(\zeta-1)(\zeta^2-1) &= 0. \end{aligned}$$

Platí ale $\zeta \neq 1, \zeta^2 \neq 1$ a z předpokladu také platí $\zeta^t \neq 1$. Tím pádem nelze v tomto případě vyplnit.

(ii) Nyní nám zbývá probrat sudé t. Z rovnosti (2.2) máme $\zeta^{2t+2} = 1$. Pak (2.4) se zjednoduší na

$$\begin{aligned} \zeta^{t-2}(\zeta-1)(\zeta^2-1) &= (\zeta^{-1}-1)(\zeta^{-2}-1), \\ \zeta^3 \cdot \zeta^{t-2}(\zeta-1)(\zeta^2-1) &= (1-\zeta)(1-\zeta^2), \\ \zeta^{t+1}(\zeta-1)(\zeta^2-1) &= (\zeta-1)(\zeta^2-1), \\ (\zeta^{t+1}-1)(\zeta-1)(\zeta^2-1) &= 0. \end{aligned}$$

Platí $\zeta \neq 1$ a $\zeta^2 \neq 1$ a z předpokladu také $\zeta^{t+1} \neq 1$, tudíž jsme i zde došli ke sporu – šachovnice nelze vyplnit.

Abychom to shrnuli, platí $t = \alpha k$ nebo $t = \alpha k - 1$ pro nějaké celé číslo α, přičemž platí rovnost $n = 2t + 1$. Pro dané $k \in \mathbb{N}$ lze šachovnici $n \times n$ bez prostředního políčka vyplnit obdélníky $1 \times k$ a $k \times 1$ právě pro

$$n = 2\alpha k \pm 1, \alpha \in \mathbb{N},$$

kde $n > 1$. To je ekvivalentní dělitelnosti $2k \mid (n \pm 1)$, což jsme chtěli ukázat. □

Byla třeba tři různá očíslování, ale dostali jsme se k výsledku — nelze-li šachovnici vyplnit *triviálně*,[1] pak nelze vyplnit vůbec. Toto tvrzení lze samozřejmě aplikovat i na samotnou úlohu 2.1.2, kde s ohledem na tento výsledek stačí nahlédnout, že příklad nemá řešení, jelikož $2 \cdot 4$ nedělí 12 ani 14.

2.1.2 Libovolné prázdné políčko

Nyní představíme úlohy, kde je stále jedno prázdné políčko, avšak v šachovnici není dáno uprostřed, ale kdekoli. Začneme s konkrétní úlohou 2.1.5, následně zobecníme rozměr čtvercové šachovnice, z čehož vyplyne tvrzení 2.1.8. Jakub Juránek zmiňuje určité zobecnění této úlohy ve své práci [5], na což navážeme obecnou větou 2.1.9.

Za použití odmocnin z jedné určíme, kde se po vyplnění může poslední prázdné pole vyskytovat. Abychom si usnadnili práci, nejdříve dokážeme následující lemma.

[1] tj. pomocí jedné z konstrukcí uvedených v příkladu výše

Lemma 2.1.4 (Jediné prázdné pole)**.** Nechť $k, A, B \in \mathbb{N}$, kde $k > 1$. Šachovnice $A \times B$, která má souřadnice číslované $(0,0), \ldots, (A-1, B-1)$, je vyplněná polyominy $k \times 1$ a $1 \times k$ až na jediné políčko na souřadnicích (x, y). Pokud definujeme $\zeta = \cos(2\pi/k) + i \sin(2\pi/k)$ jako primitivní k-tou odmocninu z jedné, pak pro každou dvojici celých čísel (a, b) splňující $a, b \not\equiv 0 \pmod{k}$ platí

$$(\zeta^a - 1)(\zeta^b - 1)\zeta^{ax+by} = (\zeta^{aA} - 1)(\zeta^{bB} - 1).$$

Důkaz. Očíslujme každé pole v šachovnici tak, že do políčka na souřadnicích (ℓ, m) vepíšeme číslo $\zeta^{a\ell+bm}$. Nejprve ukážeme, že při tomto očíslování každé položené polyomino zakryje čísla, která mají součet nula.

Každý horizontální obdélník s počátečními souřadnicemi (i, j) zakryje políčka, jejichž čísla mají součet

$$\zeta^{ai+bj}\left(1 + \zeta^a + \zeta^{2a} + \cdots + \zeta^{(k-1)a}\right) = \zeta^{ai+bj} \cdot \frac{\zeta^{ka} - 1}{\zeta^a - 1} = \zeta^{ai+bj} \cdot \frac{1 - 1}{\zeta^a - 1} = 0.$$

Jedná se o geometrickou řadu, jelikož $k \nmid a$. Stejně tak platí $k \nmid b$, takže analogickým výpočtem platí, že každý vertikální obdélník zakryje políčka s čísly, jejichž součet je nula.

Součet S všech čísel v šachovnici lze spočítat sečtením všech zakrytých čísel (dohromady nula) a čísla v prázdném políčku. Platí tedy $S = \zeta^{ax+by}$. Spočítejme S jiným způsobem.

$$S = \sum_{\ell=0}^{A-1}\sum_{m=0}^{B-1}\left(\zeta^{a\ell} \cdot \zeta^{bm}\right) = \left(\sum_{\ell=0}^{A-1}\zeta^{a\ell}\right)\left(\sum_{m=0}^{B-1}\zeta^{bm}\right) = \frac{\zeta^{aA} - 1}{\zeta^a - 1} \cdot \frac{\zeta^{bB} - 1}{\zeta^b - 1}.$$

Dosazením rovnosti $S = \zeta^{ax+by}$ tedy platí

$$\zeta^{ax+by} = \frac{\zeta^{aA} - 1}{\zeta^a - 1} \cdot \frac{\zeta^{bB} - 1}{\zeta^b - 1}.$$

Po vynásobení nenulovým číslem $(\zeta^a - 1)(\zeta^b - 1)$ jsme hotovi. □

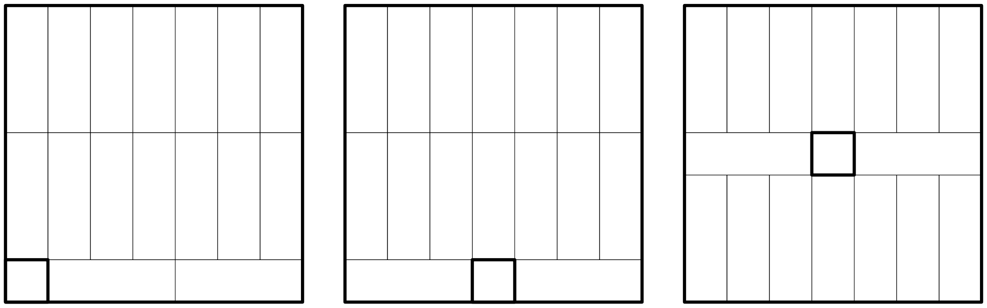
Úloha 2.1.5. Šachovnice 7×7 je pokryta šestnácti obdélníky o rozměrech 1×3 (můžeme je otáčet) tak, že pouze jedno políčko zůstane nepokryté. Jaké jsou možné pozice tohoto políčka?

Řešení. Souřadnice v šachovnici číslujme směrem z levého spodního rohu postupně $(0,0), \ldots, (6,6)$. Pokud definujeme $\zeta = \cos(2\pi/3) + i \sin(2\pi/3)$, pak z lemmatu 2.1.4 pro konkrétní hodnoty $A = B = 7, k = 3$ platí

$$(\zeta^a - 1)(\zeta^b - 1)\zeta^{ax+by} \overset{2.1.4}{=} (\zeta^{7a} - 1)(\zeta^{7b} - 1) = (\zeta^a - 1)(\zeta^b - 1),$$

kde a ani b není dělitelné třemi. Po vydělení nenulovým číslem $(\zeta^a - 1)(\zeta^b - 1)$ platí rovnost

$$\zeta^{ax+by} = 1$$



Obrázek 2.4: Možné pozice prázdného políčka v tabulce 7×7 vyplněné obdélníky 3×1

neboli $3 \mid ax + by$. Pokud dosadíme postupně dvě dvojice čísel $(a, b) = (1, 1)$ a $(2, 1)$, tak dostaneme dělitelnosti $3 \mid a + b$ a $3 \mid 2a + b$, jejichž odečtením platí $3 \mid a$. Dosazením do první dělitelnosti platí také $3 \mid b$. Obě souřadnice chybějícího políčka jsou dělitelné třemi, což odpovídá středům stran, rohům a středu tabulky. Konstrukcí ověříme, že tato políčka skutečně mohou zůstat nepokrytá, viz obrázek 2.4.

Vzhledem k symetrii čtverce získáme ostatní tři rohy a středy stran otočením celé tabulky o 90, 180 a 270 stupňů. Vyhovují tedy právě tato políčka. □

Pokrývejme stále triminy, ale podívejme se libovolnou velikost čtvercové šachovnice.

Lemma 2.1.6. Šachovnici $(3n+1) \times (3n+1)$, kde n je přirozené, vyplníme triminy 1×3 a 3×1 až na jedno políčko. Potom právě políčka se souřadnicemi

$$(3x, 3y), \quad x, y \in \mathbb{N}_0$$

mohou zůstat prázdná.

Toto lemma lze dokázat analogickou konstrukcí.

Lemma 2.1.7. Šachovnici $(3n + 2) \times (3n + 2)$ pro přirozené n vyplníme triminy 1×3 a 3×1 až na jedno políčko. Potom právě políčka se souřadnicemi

$$(3x + 2, 3y + 2), \quad x, y \in \mathbb{N}_0$$

mohou zůstat prázdná.

Důkaz. Postupujme jako v důkazu úlohy 2.1.5. Pokud (x, y) je prázdné, pak

$$(\zeta^a - 1)(\zeta^b - 1)\zeta^{ax+by} \overset{2.1.4}{=} (\zeta^{(3n+2)a} - 1)(\zeta^{(3n+2)b} - 1) = (\zeta^{-a} - 1)(\zeta^{-b} - 1).$$

Vynásobíme rovnost číslem ζ^{a+b}.

$$(\zeta^a - 1)(\zeta^b - 1)\zeta^{ax+by+a+b} = (1 - \zeta^a)(1 - \zeta^b).$$

Po vydělení číslem $(\zeta^a - 1)(\zeta^b - 1) \neq 0$ získáváme $\zeta^{ax+by+a+b} = 1$. Dosadíme hodnoty $(a, b) = (1, 1), (2, 1)$. Platí dvě dělitelnosti $3 \mid x + y - 1, 3 \mid x - y$ neboli $x \equiv y \equiv 2 \pmod 3$. Prázdné políčko je tedy na souřadnicích $(3x + 2, 3y + 2)$. □

Tvrzení 2.1.8 (Vlastní)**.** Šachovnici $n \times n$ jsme vyplnili triminy 3×1 a 1×3 tak, že jedno políčko zbylo prázdné. Toto prázdné políčko může být právě na souřadnicích[2]

$$\begin{cases} (3x, 3y), & \text{pokud } n = 3t + 1, \\ (3x + 2, 3y + 2), & \text{pokud } n = 3t + 2, \end{cases}$$

kde $x, y \in \mathbb{N}_0$.

Důkaz. Pokud je rozměr šachovnice dělitelný třemi, tak zjevně nezbyde jediné prázdné políčko. Případy $n \equiv 1, 2 \pmod 3$ řeší lemmata 2.1.6 a 2.1.7. □

Daný rozměr šachovnice i obdélníku jsme řešili v úloze 2.1.5. Následujícími úvahami jsme se seznámili s variabilním rozměrem čtvercové šachovnic, čímž se postupně dostáváme k nejobecnější úloze 2.1.9 zahrnující libovolný rozměr šachovnice i polyomina.

Věta 2.1.9 (Vlastní)**.** *Jsou dána čísla $A, B, k \in \mathbb{N}$, kde $k > 1$. Šachovnice $A \times B$ je vyplněná obdélníky $1 \times k$ a $k \times 1$ tak, že zbylo právě jedno prázné políčko. Potom platí kongruence $A \equiv B \equiv \pm 1 \pmod k$ a toto prázdné políčko může být právě na souřadnicích $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$, kde číslujeme od $(0, 0)$, splňujících*

$$(x, y) \equiv \begin{cases} (-1, -1) \pmod k, & \textit{pokud } A \equiv B \equiv -1 \pmod k, \\ (0, 0) \pmod k, & \textit{pokud } A \equiv B \equiv 1 \pmod k. \end{cases}$$

Jakub Juránek zmiňuje toto zobecnění ve své práci [5]. Přichází zejména na podmínku, že platí $AB \equiv 1 \pmod k$, a na určitou formu lemmatu 2.1.4 pro jediné prázdné políčko v šachovnici. Končí s větami:

> „Tyto nutné podmínky pouze výrazně zredukují počet pozic (r, s) vynechaného pole, [...] Zmíněná redukce tak může přinést citelnou úsporu strojového času."

Důkaz. Souřadnice v šachovnici očíslujeme postupně jako $(0, 0), (0, 1), \dots, (A - 1, B - 1)$. Z lemmatu 2.1.4 pro obecné hodnoty A, B, k a prázdné pole (x, y) platí

$$(\zeta^a - 1)(\zeta^b - 1)\zeta^{ax+by} = (\zeta^{aA} - 1)(\zeta^{bB} - 1), \tag{2.5}$$

kde k nedělí a ani b.

Nejprve vyřešíme úlohu pro $k = 2$. Do rovnosti (2.5) dosadíme dvojici $(a, b) = (1, 1)$. Platí tedy

$$(\zeta^n - 1)^2 = (\zeta - 1)^2 \cdot \zeta^{x+y}.$$

Zároveň zjednodušíme zápis tím, že $\zeta = -1$. Počet políček je lichý, aby zbylo jedno prázdné pole, takže $n \equiv 1 \pmod 2$ čili $\zeta^n = -1$. Zjednodušíme rovnici.

$$\begin{aligned} (-1 - 1)^2 &= (-1 - 1)^2 \cdot (-1)^{x+y}, \\ 1 &= (-1)^{x+y}. \end{aligned}$$

[2] číslujeme od $(0, 0)$

Odtud platí kongruence $x \equiv -y \equiv y \pmod 2$.

Dále předpokládejme, že $k > 2$. Dosadíme dvojici $(2, 1)$ do rovnice (2.5), protože k nedělí 2 ani 1. Platí tedy

$$(\zeta^2 - 1)(\zeta - 1)\zeta^{2x+y} = (\zeta^{2A} - 1)(\zeta^B - 1),$$
$$(\zeta + 1)(\zeta - 1)^2\zeta^{2x+y} = (\zeta^A + 1)(\zeta^A - 1)(\zeta^B - 1). \tag{2.6}$$

Též dosadíme dvojici $(a, b) = (1, 1)$.

$$(\zeta - 1)^2\zeta^{x+y} = (\zeta^A - 1)(\zeta^B - 1). \tag{2.7}$$

Nyní vydělíme rovnost (2.6) rovnicí (2.7).

$$(\zeta + 1)\zeta^x = \zeta^A + 1. \tag{2.8}$$

Podívejme se na rovnost absolutních hodnot. Jelikož $|\zeta^x| = 1$, tak pišme

$$|\zeta - (-1)| = |\zeta^A - (-1)|.$$

Čísla ζ a ζ^A tedy mají stejnou vzdálenost od -1 a navíc leží na jednotkové kružnici. Existují tedy nejvýše dvě různá čísla ζ^A. Zjevně vyhovuje ζ^1, ale také lze vidět rovnost $|1 + \zeta| = \left|\overline{1 + \zeta}\right| = |1 + \zeta^{-1}|$. Pokud obě možnosti pro A přepíšeme formou kongruence modulo k, pak platí

$$A \equiv \pm 1 \pmod k.$$

Vzhledem k tomu, že dvojice proměnných (A, x) a (B, y) jsou symetricky zaměnitelné, tak též platí kongruence

$$B \equiv \pm 1 \pmod k.$$

Rozlišíme nyní řešení podle zbytku čísla A po dělení k, ze symetrie vyjdou stejně dva případy pro B. Využívat k tomu budeme zejména rovnost (2.8).

(i) Pokud $k \mid (A + 1)$, pak platí $\zeta^{A+1} = 1$. Vynásobíme rovnost (2.8) číslem ζ a potom stačí dosadit. Platí $(\zeta + 1)\zeta^{x+1} = \zeta^{A+1} + \zeta = 1 + \zeta$, což vydělíme $1 + \zeta \neq 0$, a tedy dostáváme rovnost $\zeta^{x+1} = 1$. Platí tedy $x \equiv -1 \pmod k$.

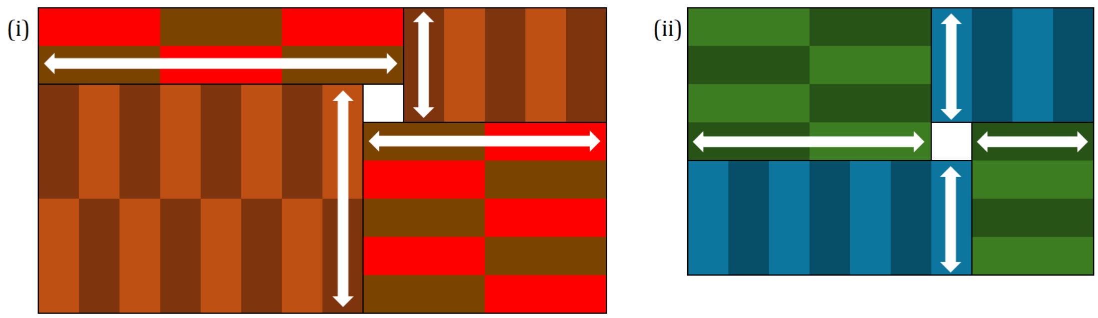
(ii) V druhém případě platí $k \mid (A-1)$. Platí $\zeta^A = \zeta$, což využijeme dosazením do rovnice (2.8). Platí tedy $(\zeta + 1)\zeta^x = \zeta^A + 1 = \zeta + 1$ a to nám stačí vydělit nenulovým $\zeta + 1$. Dostáváme rovnost $\zeta^x = 1$. Platí $x \equiv 0 \pmod k$.

Analogicky souřadnici y prázdného políčka určíme stejným způsobem, ale v závislosti na B. Pokud by A, B měli jinou hodnotu modulo k, pak by platilo $AB \equiv 1 \cdot (-1) \equiv -1 \pmod k$, což by naznačovalo, že prázdných políček je $k - 1 > 1$. Existují tedy dvě různé možnosti, kde v šachovnici zbyde poslední políčko (x, y).

$$(x, y) \equiv \begin{cases} (-1, -1) \pmod k, & \text{pokud } A \equiv B \equiv -1 \pmod k, \\ (0, 0) \pmod k, & \text{pokud } A \equiv B \equiv 1 \pmod k. \end{cases}$$

Poznamenejme, že případ $k = 2$ je zcela v souladu s těmito podmínkami, jelikož v každém případě platí $A \equiv B \equiv 1 \equiv -1 \pmod 2$ (obě jsou lichá) a současně jsme dokázali kongruenci $x \equiv y \pmod 2$, což odpovídá jedné z možností.

Oba případy ověříme konstrukcí na obrázku 2.5. □



Obrázek 2.5: Šachovnice $A \times B$ zaplněná obdélníky $1 \times k$ a $k \times 1$. Bílé šipky značí rozměr dělitelný k. (i) $A \equiv B \equiv -1 \pmod k$ a (ii) $A \equiv B \equiv 1 \pmod k$

2.1.3 Více prázdných políček

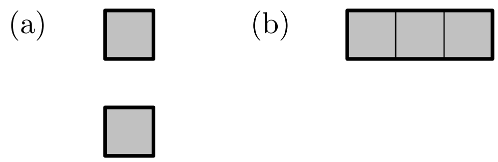
Šachovnici vyplníme tak, že zbydou alespoň dvě prázdná políčka. Zde není tak snadné obecně zjistit řešení, proto uvedeme pouze jeden příklad 2.1.11 s dvěma prázdnými políčky, čímž si nastíníme postup řešení.

Lemma 2.1.10 (Více prázdných políček)**.** Nechť $k, A, B \in \mathbb{N}$, kde $k > 1$. Šachovnice $A \times B$, která má souřadnice číslované $(0,0), \ldots, (A-1, B-1)$, je vyplněná polyominy $k \times 1$ a $1 \times k$ až na n políček na souřadnicích (x_j, y_j) pro $j \in \{1, \ldots, n\}$. Pokud definujeme $\zeta = \cos(2\pi/k) + i \sin(2\pi/k)$ jako primitivní k-tou odmocninu z jedné, pak pro každou dvojici celých čísel (a, b) splňující $a, b \not\equiv 0 \pmod k$ platí

$$(\zeta^a - 1)(\zeta^b - 1) \sum_{j=1}^{n} \zeta^{ax_j + by_j} = (\zeta^{aA} - 1)(\zeta^{bB} - 1).$$

Důkaz. Probíhá analogicky jako v lemmatu 2.1.4 až na to, že místo jediného prázdného políčka jich uvažujeme n. □

Úloha 2.1.11. Do šachovnice 8×9 umístíme trimina 3×1 a *rozbitá* trimina 1×3, které získáme odstraněním jejich středového políčka. Trimina a rozbitá trimina se nepřekrývají a nelze je otáčet. Dokažte, že existuje množina S obsahující právě 18 políček takových, že pokud v šachovnici pokryjeme 70 políček, tak zbývající dvě jsou v S.



Obrázek 2.6: (a) rozbité trimino 1×3, (b) trimino 3×1

Řešení. Souřadnice číslujme od levého spodního rohu postupně $(0,0), \dots, (7,8)$. Máme tedy 8 sloupců a 9 řádků. Do každého políčka v šachovnici vepíšeme číslo tak, že do políčka se souřadnicemi (j,k) vepíšeme číslo $\zeta^j \cdot i^k$, kde $\zeta = \cos(2\pi/3) + i \sin(2\pi/3)$ je primitivní třetí odmocnina z jedné a i je primitivní čtvrtá odmocnina z jedné.

Součet čísel v políčkách, které zakryje trimino s levou souřadnicí (a,b), je

$$\zeta^a i^b + \zeta^{a+1} i^b + \zeta^{a+2} i^b = \zeta^a i^b (1 + \zeta + \zeta^2) = 0.$$

Každé rozbité trimino (se souřadnicemi (a,b) spodního čtverce) zakryje dohromady

$$\zeta^a i^b + \zeta^a i^{b+2} = \zeta^a i^b + (-1)\zeta^a i^b = 0.$$

Označíme σ součet všech čísel. Potom platí

$$\sigma = \sum_{k=0}^{7} \sum_{l=0}^{8} \zeta^k \cdot i^l = \left(\sum_{k=0}^{7} \zeta^k \right) \left(\sum_{l=0}^{8} i^l \right) = \frac{\zeta^8 - 1}{\zeta - 1} \cdot \frac{i^9 - 1}{i - 1} = \frac{\zeta^2 - 1}{\zeta - 1} \cdot \frac{i - 1}{i - 1} =$$
$$= (\zeta + 1) \cdot 1 = -\zeta^2.$$

Pokud zbývají políčka $(a_1, b_1), (a_2, b_2)$, pak číslo σ spočítame jako součet všech trimin a rozbitých trimin (čili nula) plus dvě prázdná pole.

$$\sigma = \zeta^{a_1} i^{b_1} + \zeta^{a_2} i^{b_2}.$$

Číslo $\sigma \cdot \zeta$ se potom rovná

$$\zeta^{a_1+1} i^{b_1} + \zeta^{a_2+1} i^{b_2} = -1.$$

Označíme $z_1 = \zeta^{a_1+1} i^{b_1}$ a $z_2 = \zeta^{a_2+1} i^{b_2}$. Obě tato čísla jsou součinem odmocnin z jedné, takže leží na jednotkové kružnici. Číslo $z_1 + z_2 = -1$ je reálné, takže jejich imaginární část je opačná. Na jednotkové kružnici tomu odpovídá buď $z_1 = -z_2$, nebo $z_1 = \bar{z}_2$. V prvním případě ale $z_1 + z_2 = 0$, takže s ohledem na $\bar{z}_1 = 1/z_1$ nutně platí rovnost

$$-1 = z_1 + \bar{z}_1 = z_1 + \frac{1}{z_1}.$$

Pokud vynásobíme rovnost číslem z_1, potom

$$z_1^2 + z_1 + 1 = 0$$

čili $z_1^3 - 1 = (z_1 - 1)(z_1^2 + z_1 + 1) = 0$, odkud také plyne $z_2^3 = \overline{z_1}^3 = 1$. Dosazením dostáváme

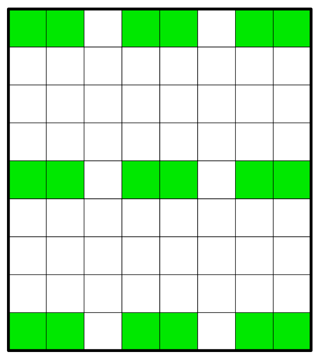
$$1 = z_1^3 = (\zeta^{a_1+1} i^{b_1})^3 = \zeta^{3a_1+3} i^{3b_1} = i^{-b_1},$$

tedy $4 \mid b_1$ a stejně tak $4 \mid b_2$. Rovnost $z_1 + z_2 = -1$ se zjednoduší na

$$\zeta^{a_1+1} + \zeta^{a_2+1} = -1,$$

což pro mocniny ζ platí právě, když sčítáme ζ a ζ^2 čili a_1 a a_2 dávají v některém pořadí zbytek 0 a 1 po dělení třemi.

Vybereme množinu S jako průnik sloupců $0, 1, 3, 4, 6, 7$ s řádky $0, 4, 8$. Z uvedených argumentů výše zbudou po pokrytí 70 políček vždy dvě z této množiny. □



Obrázek 2.7: Možné pozice (zeleně) prázdných dvou políček po zakrytí 70 políček šachovnice 8×9 triminy 3×1 a rozbitými triminy 1×3.

2.2 Kompletní vyplnění šachovnice a dělitelnost jejích rozměrů

Uvedeme úlohy, kde je vyplněná celá šachovnice obdélníky, nebo celý kvádr vícerozměrnými cihlami. Zde je snadnější zkoumat dělitelnost jednotlivých rozměrů kvádru i cihel. I díky tomu začneme hned obecnou úlohou 2.2.1, kde vyplňujeme obdélníkovou šachovnici polyominy s délkou či šířkou 1. Dále demonstrujeme určitý postup řešení v úloze 2.2.2, který aplikujeme ve známém *Rectangle Tiling Problem* v podsekci 2.2.1. Kromě toho uvedeme několik De Bruijnových vět v podsekci 2.2.2, které se elegantně dokazují odmocninami z jedné a uvažují kvádr i cihly ve více dimenzích.

Úloha 2.2.1. Mějme obdélníkovou šachovnici, kterou lze vyplnit polyominy $1 \times x$ a $y \times 1$. Dokažte, že potom lze vyplnit pouze jedním typem polyomina.

Řešení. Uvažujme rozměry šachovnice $A \times B$. Pokud $x = 1$ nebo $y = 1$, pak máme k dispozici monomino 1×1, kterým vyplníme libovolnou šachovnici. Dále řešme případ $x, y > 1$.

Definujme primitivní x-tou odmocninu z jedné jako $\zeta = \cos(2\pi/x) + i\sin(2\pi/x)$ a primitivní y-tou odmocninu z jedné, $\varepsilon = \cos(2\pi/y) + i\sin(2\pi/y)$. Pomocí jejich mocnin zaplníme celou šachovnici takovým způsobem, že do políčka na souřadnicích (j,k) vepíšeme číslo $\zeta^j \cdot \varepsilon^k$.

ε^3	$\zeta\varepsilon^3$			
ε^2	$\zeta\varepsilon^2$	$\zeta^2\varepsilon^2$		
ε	$\zeta\varepsilon$	$\zeta^2\varepsilon$	$\zeta^3\varepsilon$	
1	ζ	ζ^2	ζ^3	

Obrázek 2.8: Očíslování šachovnice $A \times B$, kde do políčka (j,k) vepíšeme $\zeta^j\varepsilon^k$.

Předpokládejme, že šachovnice je vyplněná. Nejprve ukažme, že čísla v každém polyominu o velikostech $1 \times x$ a $y \times 1$ dávají součet 0. Polyomino $1 \times x$ začínající na (j,k) zakryje v součtu

$$\zeta^j\varepsilon^k + \zeta^{j+1}\varepsilon^k + \cdots + \zeta^{j+x-1}\varepsilon^k = \zeta^j\varepsilon^k(1 + \zeta + \cdots + \zeta^{x-1}) = \zeta^j\varepsilon^k \cdot 0 = 0.$$

Polyomino $y \times 1$ začínající na (j,k) zakryje v součtu

$$\zeta^j\varepsilon^k + \zeta^j\varepsilon^{k+1} + \cdots + \zeta^j\varepsilon^{k+y-1} = \zeta^j\varepsilon^k(1 + \varepsilon + \cdots + \varepsilon^{y-1}) = \zeta^j\varepsilon^k \cdot 0 = 0.$$

Označme S součet všech čísel v šachovnici. Vzhledem k rovnostem výše platí $S = 0$. Jiným způsobem jej spočítáme jako

$$S = \sum_{j=0}^{A}\sum_{k=0}^{B} \zeta^j \cdot \varepsilon^k = \left(\sum_{j=0}^{A} \zeta^j\right)\left(\sum_{k=0}^{B} \varepsilon^k\right) = \frac{\zeta^A - 1}{\zeta - 1} \cdot \frac{\varepsilon^B - 1}{\varepsilon - 1}.$$

Vynásobením nenulovým číslem $(\zeta - 1)(\varepsilon - 1)$ máme rovnost

$$0 = (\zeta^A - 1)(\varepsilon^B - 1),$$

tudíž jedno z čísel ζ^A a ε^B se rovná jedné. Pokud $\zeta^A = 1$, pak $x \mid A$. Jinak platí $\varepsilon^B = 1$, takže $y \mid B$.

Jelikož jednička dělí libovolné přirozené číslo, tak je tato podmínka v souladu i s případy zmíněnými na začátku, tj. $x = 1$ nebo $y = 1$.

Šachovnici $A \times B$ lze vyplnit polyominy $1 \times x$ a $y \times 1$ právě, pokud $x \mid A$ nebo $y \mid B$. Vyplníme ji jednoduše, a to použitím pouze jednoho druhu polyomina. Pokud $x \mid A$, tak každý řádek zaplníme celým počtem A/x polyomin $1 \times x$. Pokud $y \mid B$, tak každý sloupec zaplníme pomocí B/y polyomin $y \times 1$. $\square$

Úloha 2.2.2 (Vlastní)**.** Máme danou obdélníkovou šachovnici vyplněnou obdélníkovými polyominy s celočíselnými délkami stran. Dokažte, že pokud každé polyomino má alespoň jednu délku strany dělitelnou číslem $N \in \mathbb{N}$, pak celá šachovnice má jednu délku strany dělitelnou N.

Řešení. Nechť má šachovnice rozměry $A \times B$. Nechť $\zeta = \cos(2\pi/N) + i \sin(2\pi/N)$ je primitivní N-tá odmocnina z jedné. Pak vepíšeme do každého políčka číslo tak, aby na pozici (x, y) bylo číslo ζ^{x+y}.

ζ^3	ζ^4			
ζ^2	ζ^3	ζ^4		
ζ	ζ^2	ζ^3	ζ^4	
1	ζ	ζ^2	ζ^3	

Obrázek 2.9: Očíslování šachovnice $A \times B$ takové, že do políčka (x, y) vepíšeme číslo ζ^{x+y}.

Mějme obdélník o rozměrech $w \times h$ s levým spodním rohem na souřadnicích (a, b), pak součet σ políček, které pokrývá, je

$$\sigma = \sum_{j=a}^{a+w-1} \sum_{k=b}^{b+h-1} \zeta^{j+k} = \left(\sum_{j=a}^{a+w-1} \zeta^j \right) \left(\sum_{k=b}^{b+h-1} \zeta^k \right).$$

Označíme $\sigma = \sigma_w \cdot \sigma_h$ jednotlivé činitele. Vzhledem k symetrii předpokládejme, že první rozměr, w, je dělitelný N. Sečtením geometrické řady platí

$$\sigma_w = \zeta^a \cdot \frac{\zeta^w - 1}{\zeta - 1} = \zeta^a \cdot \frac{1 - 1}{\zeta - 1} = 0.$$

Dosazením máme

$$\sigma = \sigma_w \cdot \sigma_h = 0 \cdot \sigma_h = 0.$$

Označme S součet všech čísel v šachovnici. Potom z rovnosti výše platí $S = 0$. Součet spočítáme jiným způsobem, a to

$$S = \sum_{j=0}^{A-1} \sum_{k=0}^{B-1} \zeta^{j+k} = \left(\sum_{j=0}^{A-1} \zeta^j \right) \left(\sum_{k=0}^{B-1} \zeta^k \right) = \frac{\zeta^A - 1}{\zeta - 1} \cdot \frac{\zeta^B - 1}{\zeta - 1},$$

vynásobením $(\zeta - 1)^2 \neq 0$ a dosazením $S = 0$ získáme rovnost

$$(\zeta^A - 1)(\zeta^B - 1) = 0,$$

tudíž jedno z čísel ζ^A, ζ^B je 1. Vzhledem k tomu, že ζ je N-tá odmocnina z jedné, tak A nebo B je násobek N, což jsme chtěli dokázat. $\square$

Poznámka. Je třeba zmínit, že obdélník $jN \times k$ i $k \times jN$ je možné vyplnit jk kopiemi obdélníků $1 \times N$ nebo $N \times 1$. S ohledem na výsledek řešení příkladu 2.2.1, kde $x = y = N$, jednoduše dojdeme k závěru, že číslo N dělí jeden z rozměrů šachovnice.

Velmi podobný postup řešení má následující příklad.

2.2.1 Rectangle Tiling Problem

Věta 2.2.3 (Rectangle Tiling Problem)**.** *Obdélník je vyplněný menšími obdélníky, kde každý má aspoň jednu celočíselnou délku strany. Potom vyplněný obdélník má jednu stranu celočíselnou.*

Tento problém poprvé zmínil Hugh Mongomery na konferenci v roce 1985, kde nastínil důkaz níže obsahující dvojité integrály. Když tak učinil, začaly se uvádět mnohé elementárnější důkazy z různých zemí. V roce 2018 byl publikován článek [10], kde je zmíněno dokonce 14 různých důkazů této věty.

Přestože zde uvažujeme libovolné neceločíselné rozměry, tak postup řešení je velmi podobný jako v úloze 2.2.2.

Důkaz. Uvažujme kartézský souřadnicový systém, kde šachovnice má své vrcholy v bodech na souřadnicích $(0, 0), (A, 0), (B, 0), (A, B)$.

Každému bodu (x, y) v rovině přiřadíme číslo

$$e^{2\pi i(x+y)} = \cos\left(2\pi(x + y)\right) + i \sin\left(2\pi(x + y)\right).$$

Nyní je ale nutné součet každého obdélníčku spočítat spojitě, nikoli diskrétně. Mějme obdélník o rozměrech $w \times h$, kde $w, h \in \mathbb{R}^+$, s levým dolním rohem na souřadnicích (a, b). Potom integrací jeho obsahu dostáváme

$$\begin{aligned} I &= \int_a^{a+w} \int_b^{b+h} e^{2\pi i(x+y)} \,\mathrm{d}x \,\mathrm{d}y = \\ &= \int_a^{a+w} e^{2\pi i x} \,\mathrm{d}x \cdot \int_b^{b+h} e^{2\pi i y} \,\mathrm{d}y = \\ &= I_w \cdot I_h, \end{aligned}$$

kde I_w, I_h jsme po řadě označili dva činitele. Vzhledem k symetrii předpokládejme, že celočíselný je rozměr w. Platí tedy

$$\begin{aligned} I_w &= \int_a^{a+w} e^{2\pi i x} \,\mathrm{d}x = \\ &= (2\pi i e^{2\pi i(a+w)} - 2\pi i e^{2\pi i a}) = \\ &= 2\pi i \cdot e^{2\pi i a} \cdot (e^{2\pi i w} - 1) = \\ &= 2\pi i \cdot e^{2\pi i a} \cdot (1 - 1) = \\ &= 0. \end{aligned}$$

Dosazením máme

$$I = I_w \cdot I_h = 0 \cdot I_h = 0.$$

Každý obdélník samotný se integruje na nulu. Tabulka je celá vyplněná takovými obdélníky, tudíž integrací celého jejího obsahu získáme součet několika nul.

$$\int_0^A \int_0^B e^{2\pi i(x+y)} \,\mathrm{d}x \,\mathrm{d}y = 0.$$

Analogickým způsobem integrace získáme

$$\int_0^A \int_0^B e^{2\pi i(x+y)} \,\mathrm{d}x \,\mathrm{d}y = -4\pi^2 \cdot (e^{2\pi i A} - 1)(e^{2\pi i B} - 1),$$

tedy

$$(e^{2\pi i A} - 1)(e^{2\pi i B} - 1) = 0.$$

Z toho již přímo plyne $e^{2\pi i A} = 1$ nebo $e^{2\pi i B} = 1$. Jeden z rozměrů tabulky je proto celočíselný, což jsme chtěli dokázat. □

Vraťme se k úloze 2.2.2, kde uvažujeme tabulku $A \times B$. Když zmenšíme tabulku na rozměry $A/N \times B/N$, tak se změní právě ty délky, které byli dělitelné N, na celočíselné. Tímto jsme převedli problém na obecnou úlohu 2.2.3.

2.2.2 De Bruijnova věta

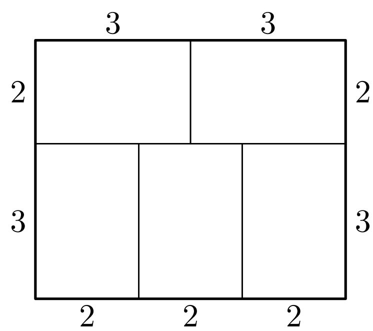
Nicolaas Govert de Bruijn byl nizozemský matematik, který přispěl mimo jiné i ke kombinatorice. Jeho poznatky v tomto oboru si zde představíme. Otázku s kvádry $1 \times 2 \times 4$ si N. G. de Bruijn položil, když jeho syn ve věku sedmi let zjistil, že nemůže vyplnit svoji krychli $6 \times 6 \times 6$ pomocí kostek $1 \times 2 \times 4$. [2]

Také cihly na stavbu mají obvykle rozměr $1 \times 2 \times 4$, aby je bylo možné spolu poskládat různými způsoby. Je zajímavé, že takový rozměr cihel není výhodou, pokud potřebujeme zcela vyplnit krychli či kvádr. Lze dokázat (a obecnější výsledek je uveden níže), že pokud určitý kvádr nelze vyplnit triviálně (tj. se všemi cihlami v rovnoběžné poloze), pak jej není možné vyplnit vůbec.

Příklad 2.2.4. Mějme krychlovou krabici o rozměrech $10 \times 10 \times 10$. Tuto krabici není možné triviálně vyplnit cihlami $1 \times 2 \times 4$, protože 4 nedělí 10. Podle právě zmíněné věty ji nelze vyplnit vůbec, aniž bychom cihly lámali. Výsledek je ještě zajímavější, pokud si uvědomíme, že celkový počet potřebných cihel by bylo celé číslo (konkrétně 125).

Poznamenejme také, že toto tvrzení neplatí pro některé jiné rozměry cihel.

Příklad 2.2.5. Cihly s rozměry $1 \times 2 \times 3$ dokážou zaplnit krabici $1 \times 5 \times 6$, zatímco triviálním způsobem zaplnit nelze, viz obrázek 2.10.



Obrázek 2.10: Krabice $1 \times 5 \times 6$ zaplněná cihlami $1 \times 2 \times 3$ netriviálním způsobem.

Dále se budeme snažit určit, které cihly mají zmíněnou vlastnost cihly $1 \times 2 \times 4$. Důkaz bude probíhat očíslováním odmocninami z jedné (podobným způsobem jako v ostatních úlohách s tabulkou).

Uvažujme zde obecně n dimenzí a jako rozměry n-dimenzionálních krychlí a cihel uvažujme přirozená čísla.

Definice 2.2.6. Kvádr $A_1 \times \cdots \times A_n$ nazývejme *násobkem* cihly $a_1 \times \cdots \times a_n$, pokud existují celá čísla $q_1, q_2, \ldots, q_n$ taková, že $q_1 a_1, \ldots, q_n a_n$ jsou permutací $A_1, \ldots, A_n$. Jako příklad násobku cihly $1 \times 2 \times 4$ uvedeme krabici $6 \times 8 \times 7$.

Definice 2.2.7. Cihlu $a_1 \times \cdots \times a_n$ nazvěme *harmonickou*, pokud existuje permutace $a'_1, \ldots, a'_n$ čísel $a_1, \ldots, a_n$ taková, že platí dělitelnost $a'_1 \mid a'_2 \mid \cdots \mid a'_n$. Například cihla $2 \times 1 \times 6 \times 2$ je harmonická.

Ukažme, že harmonické krychle mají zmíněnou vlastnost krychle $1 \times 2 \times 4$ (věta 2.2.9) a že neharmonické krychle tuto vlastnost nemají (věta 2.2.10). Tedy pokud cihla není harmonická, pak existuje krychle, kterou lze vyplnit, ale ne triviálně. A každou krychli vyplněnou harmonickými cihlami lze vyplnit triviálně.

Nejdříve ale dokažme následující větu.

Věta 2.2.8 (De Bruijn, [2])**.** *Pokud lze kvádr $A_1 \times \cdots \times A_n$ vyplnit cihlami $a_1 \times \cdots \times a_n$, pak alespoň jedno z A_i je násobkem a_1, alespoň jedno z A_i je násobkem a_2 atd. (To však neimplikuje, že kvádr je násobkem bloku, např. kvádr $1 \times 5 \times 6$ a cihla $1 \times 2 \times 3$.)*

Důkaz. Stačí dokázat, že existuje i takové, že $a_1 \mid A_i$. Každou cihlu $C = a_1 \times \cdots \times a_n$ umíme rozdělit na několik cihel $C' = a_1 \times 1 \times \cdots \times 1$. Jelikož kvádr umíme vyplnit cihlami C, tak ji lze vyplnit i cihlami C'. Dále rozdělíme každou cihlu C' na a_1 jednotkových krychliček. Celá krychle jich potom obsahuje $A_1 \cdots A_n$. Dejme jim souřadnice $(k_1, \ldots, k_n)$, kde $1 \leq k_j \leq A_j$ pro $j = 1, 2, \ldots, n$.

Definujme $\zeta = \cos(2\pi/a_1) + i \sin(2\pi/a_1)$ jako a_1-tou odmocninu z jedné a uvažujme součet

$$\sigma(A) = \sum_{k=1}^{A} \zeta^k.$$

Potom pišme

$$S = \sum_{k_1=1}^{A_1} \cdots \sum_{k_n=1}^{A_n} \zeta^{k_1+\cdots+k_n} = \sum_{k_1=1}^{A_1} \cdots \sum_{k_n=1}^{A_n} (\zeta^{k_1} \cdots \zeta^{k_n}) = \sigma(A_1) \cdots \sigma(A_n). \tag{2.9}$$

Každý sčítanec v této n-násobné sumě odpovídá právě jedné krychličce, konkrétně sčítanec $\zeta^{k_1+\cdots+k_n}$ odpovídá krychličce na souřadnicích $(k_1, \dots, k_n)$. Uvažujme libovolnou cihlu γ o rozměrech C' skládající se z a_1 krychliček v řadě. Cihla γ má jedinou proměnnou souřadnici, a to v j-tém rozměru, kde $1 \leq j \leq n$. V j-tém rozměru zasahuje právě do souřadnic

$$k_j, k_j + 1, \dots, k_j + (a_1 - 1)$$

pro nějaké k_j. Nechť $(k_1, \dots, k_j, \dots, k_n)$ jsou souřadnice „počáteční" krychličky cihly γ. Krychličky na těchto souřadnicích přispějí do součtu S sčítancem

$$w_\gamma = \sum_{k=0}^{a_1-1} \zeta^{k_1+\cdots+(k_j+k)\cdots+k_n} = \zeta^{k_1+\cdots+k_n} \cdot \sum_{k=0}^{a_1-1} \zeta^k.$$

Sečteme jako geometrickou řadu a s ohledem na rovnost $\zeta^{a_1} = 1$ platí

$$w_\gamma = \zeta^{k_1+\cdots+k_n} \cdot \frac{\zeta^{a_1} - 1}{\zeta - 1} = \zeta^{k_1+\cdots+k_n} \cdot \frac{1-1}{\zeta - 1} = 0.$$

Tedy čísla na pozicích krychliček každé cihly γ mají součet $w_\gamma = 0$. Součet všech čísel v krychli se tedy také vynuluje, $S = 0$. Dosazením do rovnosti 2.9 potom získáváme

$$\sigma(A_1) \cdots \sigma(A_n) = 0,$$

tudíž existuje A_i takové, že $\sigma(A_i) = 0$. Platí

$$\sigma(A_i) = \zeta + \zeta^2 + \cdots + \zeta^{A_i} = \frac{\zeta(\zeta^{A_i} - 1)}{\zeta - 1},$$

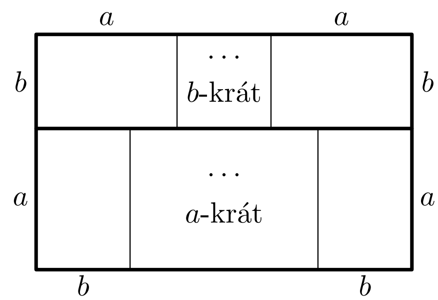
tedy $\zeta^{A_i} = 1$, odkud jistě platí, že $a_1 \mid A_i$, což jsme chtěli dokázat. □

Věta 2.2.9 (De Bruijn, [2]). *Pokud harmonickými cihlami $a_1 \times \cdots \times a_n$ vyplníme kvádr, pak je jejím násobkem.*

Důkaz. Uvažujme rozměry krychle $A_1, \dots, A_n$ a využijme indukci na dimenzi n. Pokud platí $n = 1$, pak úsečku délky A_1 vyplníme cihlou délky a_1, pokud $a_1 \mid A_1$, a tedy „krychle" je násobkem cihly. Předpokládejme nyní, že dokazované tvrzení platí pro $n - 1$ dimenzí, a dokažme, že platí i pro n dimenzí.

Bez újmy na obecnosti, nechť platí $a_1 \mid a_2 \mid \cdots \mid a_{n-1} \mid a_n$. Z předchozí věty 2.2.8 jistě existuje A_i takové, že $a_n \mid A_i$. Indexujme souřadnice krychle tak, že platí $a_n \mid A_n$.

Mějme $(n-1)$-dimenzionální stěnu $A_1 \times \cdots \times A_{n-1}$, která je vyplněná cihlami o $n - 1$ dimenzích, takže mají velikost buď $a_2 \times \cdots \times a_n$, $a_1 \times a_3 \times \cdots \times a_n, \dots$, nebo $a_1 \times \cdots \times a_{n-1}$.



Obrázek 2.11: Kvádr $(a+b) \times ab$ zaplněný cihlami $a \times b$.

Každá taková cihla lze rozdělit na cihly $C = a_1 \times \cdots \times a_{n-1}$ díky tomu, že platí zmíněné dělitelnosti, a každá cihla ve stěně je proto násobkem cihly C. Jelikož je cihla C harmonická, tak z indukčního předpokladu je kvádr $A_1 \times \cdots \times A_{n-1}$ jejím násobkem. Jelikož i poslední rozměr A_n je násobkem rozměru a_n, tak celý kvádr $A_1 \times \cdots \times A_n$ je násobkem cihly $a_1 \times \cdots \times a_n$. Tím jsme dokončili indukční krok, a jsme hotovi. □

Věta 2.2.10 (De Bruijn, [2])**.** *Pro každou neharmonickou cihlu $a_1 \times \cdots \times a_n$ existuje kvádr, který dokážeme těmito cihlami zaplnit a zároveň není jejím násobkem.*

Důkaz. Jelikož pro $n = 1$ je každá cihla harmonická, tak mějme $n > 1$. Dále uspořádejme rozměry tak, aby $a_1 \le a_2 \le \cdots \le a_n$, a označme $C = a_1 \times \cdots \times a_n$ rozměry cihly. Dále nechť k je největší číslo splňující $a_{k-1} \nmid a_k$ (takže $2 \le k \le n$ a platí $a_k \mid a_{k+1} \mid \cdots \mid a_n$).

Kvádr $(a+b) \times ab$ lze zaplnit cihlami $a \times b$, viz obrázek 2.11. Takže kvádr o rozměrech

$$a_1 \times \cdots \times a_{k-2} \times (a_{k-1} + a_k) \times a_{k-1}a_k \times a_{k+1} \times \cdots \times a_n$$

je možné zaplnit cihlami $a_1 \times \cdots \times a_n$. (Jedná se o rozměry cihly, kde jsme upravili dva rozměry tak, že je k sobě lze poskládat jako na obrázku.)

Ukažme, že se nejedná o násobek C. Nechť j je nejmenší index splňující $a_j = a_{k-1}$. Platí tedy $a_{j-1} < a_j = \cdots = a_{k-1}$. Pak žádné z čísel $a_1, \ldots, a_{j-1}, a_{k-1} + a_k$ není násobkem žádného z čísel $a_j, \ldots, a_{k-1}, a_k, \ldots, a_n$. (Číslo $a_{k-1} + a_k$ není násobkem a_{k-1} ani a_k, takže ani žádným násobkem a_k. Vzhledem k volbě k jsou $a_{k+1}, \ldots, a_n$ násobky a_k.)

Pokud by kvádr byl násobkem cihly C, pak existuje nejvíce $j-1$ indexů i takových, že A_i není násobkem žádného z čísel $a_j, \ldots, a_n$. Proto zkonstruovaný kvádr není násobkem cihly C. Tímto jsme hotovi. □

Kapitola 3

Kombinatorické a číselné identity

Originálním výsledkem této kapitoly je vzorec pro součet každého n-tého Fibonacciho čísla, obsahující zaokrouhlení na nejbližší celé číslo – věta 3.2.12.

Nejprve ale v sekci 3.1 uvedeme sčítání kombinačních čísel, jelikož tyto výsledky budou potřeba v následující kapitole (např. v podsekci 4.4.1) a současně nám pomohou představit využití *Roots of Unity Filter*, díky čemuž bude sčítání Fibonacciho čísel v sekci 3.2 jednodušeji uchopitelné.

3.1 Součty kombinačních čísel

Tyto součty lze interpretovat jako součet každého m-tého čísla na n-tém řádku Pascalova trojúhelníku.

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}
$$

Obrázek 3.1: Prvních 7 řádků Pascalova trojúhelníku se zvýrazněným každým druhým číslem na posledním řádku

Známým způsobem využití komplexních čísel v rámci kombinatoriky je k určení různých součtů konečně mnoha kombinačních čísel. Vycházíme přitom z faktu, že každé komplexní číslo lze po umocnění vyjádřit nejen pomocí binomické věty, ale i dle Moivreovy věty. Úvodní text této sekce je zpracován podle [4].

Definice 3.1.1 (Kombinační číslo)**.** Pro $n \in \mathbb{N}$ a $k \in \mathbb{Z}$ definujme kombinační číslo $\binom{n}{k}$ jako celé číslo splňující

$$\binom{n}{k} = \begin{cases} \frac{n!}{(n-k)!k!}, & \text{pro } 0 \le k \le n, \\ 0, & \text{jinak.} \end{cases}$$

Definice 3.1.2 (Konečný součet kombinačních čísel)**.** Pro dané $m \in \mathbb{N}$ a $r \in \{0, \dots, m-1\}$ definujme konečný součet kombinačních čísel jako

$$\chi_m^r(n) = \binom{n}{r} + \binom{n}{r+m} + \binom{n}{r+2m} + \dots$$

Binomická věta nám umožňuje vyjádřit kladnou celočíselnou mocninu libovolného dvojčlenu jako konečný součet obsahující kombinační čísla.

Věta 3.1.3 (Binomická věta)**.** *Pro nenulová $A, B \in \mathbb{C}$ a $n \in \mathbb{N}$ platí*

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^{n-k} B^k.$$

Sumou lze sčítat přes všechna celá čísla $k \geq 0$, jelikož pro $k > n$ platí $\binom{n}{k} = 0$.

$$(A+B)^n = \binom{n}{0} A^n + \binom{n}{1} A^{n-1} B + \binom{n}{2} A^{n-2} B^2 + \dots$$

Vhodným užitím binomické věty získáme součty některých kombinačních čísel. Uveďme dva příklady.

$$2^n = (1+1)^n = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n},$$
$$0 = (1-1)^n = \binom{n}{0} - \binom{n}{1} + \dots + \binom{n}{n}(-1)^n.$$

Sečtením, resp. odečtením rovností a vydělením dvěma dostáváme dvě rovnosti.

$$\chi_2^0(n) = \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots = 2^{n-1}, \tag{3.1}$$
$$\chi_2^1(n) = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \dots = 2^{n-1}, \tag{3.2}$$

Abychom získali další identity, dosaďme do binomické věty 3.1.3 hodnoty $A = 1$ a $B = i$.

$$(1+i)^n = \binom{n}{0} + \binom{n}{1} i - \binom{n}{2} - \binom{n}{3} i + \dots + \binom{n}{n} i^n.$$

Dle Moivreovy věty spočítáme levou stranu.

$$(1+i)^n = \left[\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)\right]^n = (\sqrt{2})^n \cdot \left(\cos\frac{n\pi}{4} + i\sin\frac{n\pi}{4}\right).$$

Porovnáním reálných a imaginárních složek dostáváme dvě rovnosti.

$$\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \dots = (\sqrt{2})^n \cos\frac{n\pi}{4}, \tag{3.3}$$
$$\binom{n}{1} - \binom{n}{3} + \binom{n}{5} - \dots = (\sqrt{2})^n \sin\frac{n\pi}{4}. \tag{3.4}$$

Sečtením a odečtením identit (3.1) a (3.3), resp. (3.2) a (3.4) a následně vydělením dvěma obdržíme čtyři rovnosti.

$$\begin{aligned}
\chi_4^0(n) &= \binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots &= 2^{n-2} + \left(\sqrt{2}\right)^{n-2} \cdot \cos \tfrac{n\pi}{4}, \\
\chi_4^1(n) &= \binom{n}{1} + \binom{n}{5} + \binom{n}{9} + \cdots &= 2^{n-2} + \left(\sqrt{2}\right)^{n-2} \cdot \sin \tfrac{n\pi}{4}, \\
\chi_4^2(n) &= \binom{n}{2} + \binom{n}{6} + \binom{n}{10} + \cdots &= 2^{n-2} - \left(\sqrt{2}\right)^{n-2} \cdot \cos \tfrac{n\pi}{4}, \\
\chi_4^3(n) &= \binom{n}{3} + \binom{n}{7} + \binom{n}{11} + \cdots &= 2^{n-2} - \left(\sqrt{2}\right)^{n-2} \cdot \sin \tfrac{n\pi}{4}.
\end{aligned}$$

Věta 3.1.4. *Je dáno přirozené číslo n. Pro součet každého třetího kombinačního čísla platí*

$$\chi_3^r(n) = \binom{n}{r} + \binom{n}{r+3} + \binom{n}{r+6} + \cdots = \frac{2^n + 2\cos\frac{(n+4r)\pi}{3}}{3}.$$

Řešení. Pišme polynom

$$f(x) = (1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \ldots$$

Pro $r \in \{0, 1, 2\}$ chceme ponechat každý člen na místě r modulo 3. Stejně jako v minulé kapitole využijeme Roots of Unity Filter. Pro primitivní třetí odmocninu z jedné ζ, definovanou jako $\zeta = \cos(2\pi/3) + i\sin(2\pi/3)$, platí

$$\chi_3^r(n) = \frac{f(1) + \zeta^{2r} f(\zeta) + \zeta^r f(\zeta^2)}{3}, \tag{3.5}$$

kde $\chi_3^r(n)$ je součet všech kombinačních čísel tvaru $\binom{n}{3k+r}$, kde k je celé číslo. Definujme též $\varepsilon = \cos(\pi/3) + i\sin(\pi/3)$ jako primitivní šestou odmocninu z jedné. Spočítejme tyto tři funkční hodnoty pomocí rovností $-1 = \varepsilon^3$, $\zeta = \varepsilon^2$ a $1 + \zeta + \zeta^2 = 0$. Dosazením jednoduše platí $f(1) = 2^n$ a také

$$\begin{aligned}
f(\zeta) &= (1+\zeta)^n = (-\zeta^2)^n = \varepsilon^n, \\
f(\zeta^2) &= (1+\zeta^2)^n = (-\zeta)^n = \varepsilon^{-n}.
\end{aligned}$$

Dosazením do rovnice (3.5) platí

$$\chi_3^r(n) = \frac{2^n + \zeta^{2r}\varepsilon^n + \zeta^r\varepsilon^{-n}}{3} = \frac{2^n + \varepsilon^{n+4r} + \varepsilon^{-n-4r}}{3}.$$

Pro komplexní číslo z na jednotkové kružnici platí $z + \frac{1}{z} = 2\Re(z)$. Nahlédnutím k algebraickému zápisu mocnin ε dle Moivreovy věty tedy platí

$$\chi_3^r(n) = \frac{2^n + 2\cos\frac{(n+4r)\pi}{3}}{3}.$$

□

Důsledek 3.1.5. Pro součet každého třetího kombinačního čísla platí

$$\chi_3^0(n) = \binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \ldots = \frac{1}{3}\left[2^n + 2\cos\left(\frac{n\pi}{3}\right)\right],$$
$$\chi_3^1(n) = \binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \ldots = \frac{1}{3}\left[2^n + 2\cos\left(\frac{(n+4)\pi}{3}\right)\right],$$
$$\chi_3^2(n) = \binom{n}{2} + \binom{n}{5} + \binom{n}{8} + \ldots = \frac{1}{3}\left[2^n + 2\cos\left(\frac{(n+2)\pi}{3}\right)\right].$$

Důkaz. Pro $r = 0, 1$ platí přímo z předchozí věty. Pokud $r = 2$, pak vzhledem k periodě kosinu platí $\cos\frac{(n+4r)\pi}{3} = \cos\frac{(n+8)\pi}{3} = \cos\frac{(n+2)\pi}{3}$. Tímto získáváme všechny tři rovnosti. □

Sice nejsme schopni dojít k explicitnímu vzorci pro každé χ_m^r obecně, ale dokážeme ho určit jako následující součet kosinů.

Věta 3.1.6. *Mějme přirozená čísla n, m a $r \in \{0, \ldots, m-1\}$. Pro součet každého m-tého kombinačního čísla počínaje r-tým platí*

$$\chi_m^r(n) = \sum_{k\in\mathbb{Z}} \binom{n}{km+r} = \frac{1}{m}\left(2^n + 2\sum_{j=1}^{\left\lfloor\frac{m-1}{2}\right\rfloor}\left(2\cos\frac{\pi j}{m}\right)^n \cos\frac{\pi(n-2r)j}{m}\right).$$

Důkaz. Nechť $\zeta = \cos(2\pi/m) + i\sin(2\pi/m)$ a označme $\sigma_j = \zeta^{-rj}(1+\zeta^j)^n$. Dle Roots of Unity Filtru platí

$$m \cdot \chi_m^r(n) = \sigma_0 + \sigma_1 + \cdots + \sigma_{m-1}$$

Není třeba uvažovat případný nulový sčítanec $\sigma_{m/2}$, jelikož platí rovnost $1 + \zeta^{m/2} = 0$, takže i $\sigma_{m/2} = 0$. Můžeme tedy psát formou sumy bez tohoto členu. Pokud pomocí dolní celé části označíme $m' = \left\lfloor\frac{m-1}{2}\right\rfloor$ a rozmyslíme si, že platí $\sigma_{m-j} = \sigma_{-j} = \overline{\sigma_j}$, tak platí

$$m \cdot \chi_m^r(n) = \sum_{j=0}^{m} \sigma_j = \sigma_0 + \sum_{j=1}^{m'} (\sigma_j + \sigma_{m-j}) = \sigma_0 + \sum_{j=1}^{m'} (\sigma_j + \overline{\sigma_j})$$

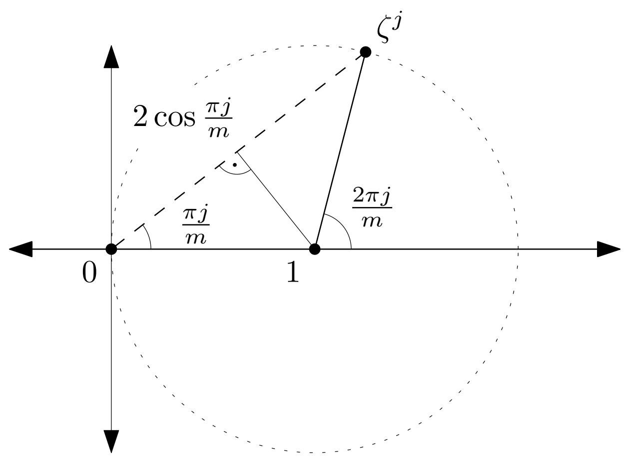
Dosazením platí $\sigma_0 = 2^n$. Každá dvojice sčítanců je součet dvou komplexně sdružených čísel. Jelikož pro každé $z \in \mathbb{C}$ platí $z + \overline{z} = 2\Re(z)$, tak pišme

$$\chi_m^r(n) = \frac{1}{m}\left(2^n + 2\sum_{j=1}^{m'} \Re(\sigma_j)\right). \tag{3.6}$$

Nyní spočítáme $\sigma_j = \zeta^{-rj}(1+\zeta^j)^n$ v goniometrickém tvaru. Platí rovnosti

(i) $|\sigma_j| = |\zeta^{-rj}(1+\zeta^j)^n| = |1+\zeta^j|^n$,

(ii) $\arg\sigma_j = \arg\left(\zeta^{-rj}(1+\zeta^j)^n\right) = -2\pi rj/m + n\cdot\arg(1+\zeta^j)$, takže zbývá dopočítat absolutní hodnotu a argument čísla $1 + \zeta^j$. Jelikož pro každý index j platí $1 < j < m/2$, tak $1 + \zeta^j$ má kladnou imaginární část jako na obrázku 3.2. Obě čísla 0 i ζ^j leží na kružnici s poloměrem 1 a středem v čísle 1. Argumentem čísla ζ^j je z definice $2\pi j/m$, takže z věty o obvodovém a středovém úhlu zmíněné kružnice platí rovnost argumentu $\arg(1+\zeta^j) = \pi j/m$. Vzdálenost od počátku čísla $1+\zeta^j$ se díky tomuto úhlu rovná hodnotě $|1 + \zeta^j| = 2\cos(\pi j/m)$.



Obrázek 3.2: Geometrická reprezentace čísla $1 + \zeta^j$, kde ζ je m-tá odmocnina z jedné.

Pišme tedy

$$\sigma_j = \left(2\cos\frac{\pi j}{m}\right)^n \left[\cos\left(\frac{\pi(n-2r)j}{m}\right) + i\sin\left(\frac{\pi(n-2r)j}{m}\right)\right].$$

Reálná část σ_j je nyní zjevná. Dosazením do rovnice (3.6) získáváme výsledek. □

3.2 Konečné součty Fibonacciho čísel

Ačkoliv vzorec pro součet prvního až n-tého Fibonacciho čísla lze snadno dokázat například indukcí (stejně jako součet každého druhého Fibonacciho čísla), tak jiné součty tak jednoduché nejsou.

Vzhledem k tomu, že alespoň pomocí Roots of Unity Filtru umíme vyjádřit součet každého několikátého členu posloupnosti, tak se pokusíme najít vzorec pro součet každého m-tého Fibonacciho čísla. Nakonec se ukáže, že z původního výrazu s odmocninami jsme schopni určit vzorec, a to pro každé $m \in \mathbb{N}$.

Výsledkem této sekce je tedy získání vzorce pro součet každého m-tého Fibonacciho čísla, a to pro každé přirozené m. V řešení se překvapivě objeví jak dolní celá část, tak i zaokrouhlení na nejbližší celé číslo.

Definice 3.2.1 (Fibonacciho posloupnost)**.** Fibonacciho posloupnost $F_0, F_1, F_2, \ldots$ definujme s počátečními členy $F_0 = 0, F_1 = 1$ a dále pro každé $n \geq 0$ pišme

$$F_{n+2} = F_{n+1} + F_n.$$

Definice 3.2.2 (Konečný součet Fibonacciho čísel)**.** Nechť $m, n \in \mathbb{N}$. Pro součet každého m-tého Fibonacciho čísla, kde končíme F_n, využívejme značení $\mathcal{F}_m(n)$, pro které platí

$$\mathcal{F}_m(n) = F_r + F_{r+m} + F_{r+2m} + \cdots + F_{n-m} + F_n,$$

kde $r = n \bmod m$, takže platí $0 \leq r \leq m - 1$.

Vzorce pro součet každého a každého druhého Fibonacciho čísla, tj. pro $m = 1, 2$, jsou vypsány v následující větě.

Věta 3.2.3. *Pro každé přirozené n platí*

$$\mathcal{F}_1(n) = F_0 + F_1 + F_2 + \cdots + F_n = F_{n+2} - 1,$$

$$\mathcal{F}_2(n) = \begin{cases} F_0 + F_2 + F_4 + \cdots + F_n = F_{n+1} - 1, \\ F_1 + F_3 + F_5 + \cdots + F_n = F_{n+1}. \end{cases}$$

Všimněme si, že pro sčítání každého druhého Fibonacciho čísla je nutné rozlišit dva součty na základě dělitelnosti n dvěma, jelikož v obou případech začínáme jiným členem posloupnosti. U dalších získaných vzorců bude nutné počítat se všemi různými počátečními členy součtu.

Začneme s $m = 3$ a ukážeme, že i když se může zdát, že bude nutné rozlišovat na tři vzorce, tak ve skutečnosti stačí pouze jeden – následující věta prozradí proč.

Věta 3.2.4 (Vlastní)**.** *Pro každé přirozené n platí*

$$\mathcal{F}_3(n) = \left\lfloor \frac{F_{n+2}}{2} \right\rfloor.$$

Důkaz této věty vychází z lemmatu 3.2.6, ale nejdříve potřebujeme znát explicitní tvar konečné generující funkce Fibonacciho čísel. Tento tvar je dán následující větou.

Věta 3.2.5 (Vlastní)**.** *Pro každé přirozené N a každé $x \in \mathbb{C}$ splňující $1 - x - x^2 \neq 0$ platí*

$$F_0x^0 + F_1x + F_2x^2 + \cdots + F_Nx^N = \frac{x - F_{N+1}x^{N+1} - F_Nx^{N+2}}{1 - x - x^2}.$$

Důkaz. Definujme součet výše jako $G_N(x) = \sum_{n=0}^{N} F_nx^n$. Pokud ze sumy odděláme první dva sčítance $F_0x^0 + F_1x^1 = x$, tak platí $G_N(x) = x + \sum_{n=0}^{N-2} F_{n+2}x^{n+2}$. Když dosadíme rekurenci $F_{n+2} = F_{n+1} + F_n$, tak platí

$$G_N(x) = x + \sum_{n=0}^{N-2}(F_{n+1} + F_n)x^{n+2} = x + x\sum_{n=1}^{N-1} F_nx^n + x^2\sum_{n=0}^{N-2} F_nx^n.$$

Obě sumy vyjádříme pomocí $G_N(x)$, jelikož se až na některé sčítance rovnají. První sumu získáme, pokud od tohoto čísla odečteme $xF_0 + F_N x^N = F_N x^N$, a podobně druhou sumu získáme, když od $G_N(x)$ odečteme $F_{N-1}x^{N-1} + F_N x^N$. Platí tedy

$$G_N(x) = x + x\left(G_N(x) - F_N x^N\right) + x^2\left(G_N(x) - F_{N-1}x^{N-1} - F_N x^N\right).$$

Roznásobíme a členy s G_N převedeme na levou stranu rovnosti. Vytknutím potom platí

$$(1 - x - x^2)G_N(x) = x - (F_N + F_{N-1})x^{N+1} - F_N x^{N+2} = x - F_{N+1}x^{N+1} - F_N x^{N+2}.$$

Za předpokladu, že $1 - x - x^2 \neq 0$ vydělíme rovnost, čímž jsme hotovi. $\square$

Dokazovaná věta 3.2.4 je přímým důsledkem následující lemmatu, které rozlišuje tři případy podle zbytku n po dělení třemi.

Lemma 3.2.6. Pro součet každého třetího Fibonacciho čísla platí

(i) $F_0 + F_3 + F_6 + \cdots + F_n = \frac{1}{2}\left(F_{n+2} - 1\right)$,

(ii) $F_1 + F_4 + F_7 + \cdots + F_n = \frac{1}{2}F_{n+2}$,

(iii) $F_2 + F_5 + F_8 + \cdots + F_n = \frac{1}{2}\left(F_{n+2} - 1\right)$.

Důkaz. Definujme primitivní třetí odmocninu z jedné $\zeta = \cos(2\pi/3) + i\sin(2\pi/3)$ a určeme zbytek $r = n \bmod 3$. Potom z Roots of Unity Filtru platí

$$F_r + F_{3+r} + \cdots + F_n = \frac{G_n(1) + \zeta^{-r}G_n(\zeta) + \zeta^{-2r}G_n(\zeta^2)}{3}. \tag{3.7}$$

Pro první vzorec předpokládejme, že $r = 0$. Potom z explicitního vyjádření 3.2.5 spočítáme funkční hodnoty.

$$\begin{aligned}
G_n(1) &= \frac{1 - F_{n+1} - F_n}{1 - 1 - 1^2} = -1 + F_n + F_{n+1},\\
G_n(\zeta) &= \frac{\zeta - F_{n+1}\zeta^{n+1} - F_n\zeta^{n+2}}{1 - \zeta - \zeta^2} = \frac{\zeta - F_{n+1}\zeta - F_n\zeta^2}{2},\\
G_n(\zeta^2) &= \frac{\zeta^2 - F_{n+1}\zeta^{2(n+1)} - F_n\zeta^{2(n+2)}}{1 - \zeta^2 - \zeta^4} = \frac{\zeta^2 - F_{n+1}\zeta^2 - F_n\zeta}{2}.
\end{aligned}$$

Využijeme vztahu $1 + \zeta + \zeta^2 = 0$. Sečtením pravých stran rovností máme $\frac{3}{2}\left(F_{n+2} - 1\right)$, odkud vydělením třemi získáme první identitu. Dále předpokládejme, že $r = 1$. Podobně spočítáme funkční hodnoty a dosadíme do rovnosti (3.7), čímž získáme druhou identitu,

$$F_1 + F_4 + \cdots + F_n = \frac{1}{3}\cdot\frac{3}{2}\left(F_{n+1} + F_n\right) = \frac{1}{2}F_{n+2}.$$

Pro poslední identitu stačí odečíst první dvě rovnosti od součtu všech Fibonacciho čísel, který se rovná $\mathcal{F}_1(n) = F_{n+2} - 1$. $\square$

3.2.1 Obecný součet členů Fibonacciho posloupnosti

Podíváme se, jakého tvaru je libovolný součet Fibonacciho čísel, $\mathcal{F}_m(n)$. I když pro dané m existuje m různých vzorců na základě zbytku n po dělení m, tak tyto vzorce jsou natolik podobné, že se liší jen o malou konstantu. Díky tomu jsme schopni pomocí zaokrouhlení určit jednotný vztah.

Věta 3.2.7 (Obecný vzorec, vlastní)**.** *Obecný součet Fibonacciho čísel je pro dvojici čísel $m, n \in \mathbb{N}$ daný vzorcem*

$$\mathcal{F}_m(n) = F_n\, \mathcal{Z}_2 + F_{n+1}\, \mathcal{Z}_1 - \mathcal{Z}_{1-n},$$

kde pro primitivní m-tou odmocninu z jedné, $\zeta = \cos(2\pi/m) + i \sin(2\pi/m)$, platí

$$\mathcal{Z}_\alpha = \frac{1}{m} \sum_{k=0}^{m-1} \frac{-\zeta^{\alpha k}}{1 - \zeta^k - \zeta^{2k}}.$$

Důkaz. Pro celé číslo k pišme $\sigma_k = \zeta^{-kr} G_n(\zeta^k)$. Nechť $r = n \mod m$, pak nahlédnutím k Roots of Unity Filtru pro mocninnou řadu G_n se hledaný součet rovná

$$\mathcal{F}_m(n) = F_r + F_{m+r} + F_{2m+r} + \cdots + F_n = \frac{\sigma_0 + \sigma_1 + \cdots + \sigma_{m-1}}{m}, \tag{3.8}$$

kde pomocí explicitního vzorce 3.2.5 vyjádříme každé z čísel σ_k jako

$$\sigma_k = \zeta^{-kr} G_n(\zeta^k) = \zeta^{-kr} \cdot \frac{\zeta^k - \zeta^{k(r+2)} F_n - \zeta^{k(r+1)} F_{n+1}}{1 - \zeta^k - \zeta^{2k}} = \frac{\zeta^{k(1-r)} - \zeta^{2k} F_n - \zeta^k F_{n+1}}{1 - \zeta^k - \zeta^{2k}}.$$

Rozdělením na tři sčítance a sečtením podle rovnosti (3.8) se zde vyskytnou čísla $\mathcal{Z}_\alpha$ (přičemž platí $\mathcal{Z}_{1-r} = \mathcal{Z}_{1-n}$) čímž získáme přímo dokazovaný vzorec. □

Abychom mohli pokračovat v úpravě čísel $\mathcal{Z}_\alpha$, potřebujeme znát explicitní vzorec Fibonacciho a Lucasových čísel. Lucasova čísla definujeme stejně jako Fibonacciho, až na počáteční členy – $L_0 = 2, L_1 = 1$ – dále platí $L_n = L_{n-1} + L_{n-2}$.

Poznámka. První členy Lucasovy posloupnosti jsou

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123.$$

Věta 3.2.8 (Explicitní vzorec Fibonacciho a Lucasových čísel)**.** *Pro každé $n \in \mathbb{N}_0$ platí*

$$F_n = \frac{\varphi^n - \tilde{\varphi}^n}{\sqrt{5}}, \qquad L_n = \varphi^n + \tilde{\varphi}^n,$$

kde $\varphi = \frac{1+\sqrt{5}}{2}$ a $\tilde{\varphi} = \frac{1-\sqrt{5}}{2}$.

Věta 3.2.9 (Honsberger, [6])**.** *Pro všechny dvojice přirozených čísel m, n platí rovnost*

$$F_{m+n} = F_{m-1} F_n + F_m F_{n+1}.$$

Věta 3.2.10 (Vlastní). *Obecný součet Fibonacciho čísel pro dvojici čísel $m, n \in \mathbb{N}$, kde $r = n \bmod m$, je daný vzorcem*

$$\mathcal{F}_m(n) = \frac{F_{m+n} + (-1)^{m+1} F_n}{L_m - 1 + (-1)^{m+1}} + \frac{(-1)^r F_{m-r} + F_r}{L_m - 1 + (-1)^{m+1}},$$

Důkaz. Definujme $r = n \bmod m$. Potom platí rovnost $\mathcal{Z}_{1-n} = \mathcal{Z}_{1-r}$ a z definice je součet Fibonacciho čísel $\mathcal{F}_m(r)$ roven pouze prvnímu členu, F_r. Pišme tedy

$$F_r = \mathcal{F}_m(r) = F_r\,\mathcal{Z}_2 + F_{r+1}\,\mathcal{Z}_1 - \mathcal{Z}_{1-n},$$

což odečteme od rovnosti 3.2.7, čímž dostaneme

$$\mathcal{F}_m(n) = F_n\,\mathcal{Z}_2 + F_{n+1}\,\mathcal{Z}_1 - (F_r\,\mathcal{Z}_2 + F_{r+1}\,\mathcal{Z}_1 - F_r). \tag{3.9}$$

Dále zjistíme hodnotu čísel $\mathcal{Z}_1$ a $\mathcal{Z}_2$.

Jelikož platí $\varphi\tilde{\varphi} = -1, \varphi + \tilde{\varphi} = 1$, tak rozložíme $1 - x - x^2 = (1 - \varphi x)(1 - \tilde{\varphi} x)$, a tedy i každý člen sumy ve výrazech $\mathcal{Z}_1, \mathcal{Z}_2$ na parciální zlomky.

$$\mathcal{Z}_1 = \frac{1}{m} \sum_{k=0}^{m-1} \frac{-\zeta^k}{1 - \zeta^k - \zeta^{2k}} = \frac{1}{m} \sum_{k=0}^{m-1} \left(\frac{\frac{-1}{\sqrt{5}}}{1 - \zeta^k \varphi} + \frac{\frac{1}{\sqrt{5}}}{1 - \zeta^k \tilde{\varphi}} \right)$$

Z následujícího zlomku nejdříve oddělíme číslo 1 a následně rozložíme stejným způsobem.

$$\mathcal{Z}_2 = \frac{1}{m} \sum_{k=0}^{m-1} \frac{-\zeta^{2k}}{1 - \zeta^k - \zeta^{2k}} = \frac{1}{m} \sum_{k=0}^{m-1} \left(1 + \frac{\frac{1}{\sqrt{5}}(1 - \varphi)}{1 - \zeta^k \varphi} + \frac{\frac{1}{\sqrt{5}}(\tilde{\varphi} - 1)}{1 - \zeta^k \tilde{\varphi}} \right)$$

Pokud rozdělíme sumy na každý zlomek zvlášť, tak jsme schopni takovou sumu sečíst za využití Roots of Unity Filtru – pro každé x, kde $x^m \neq 1$, platí

$$1 + \zeta^k x + (\zeta^k x)^2 + \cdots + (\zeta^k x)^{m-1} = \frac{1 - (\zeta^k x)^m}{1 - \zeta^k x} = \frac{1 - x^m}{1 - \zeta^k x}.$$

Pokud sečteme tuto rovnost pro každé $k \in \{0, \ldots, m-1\}$, tak u každé kladné mocniny v součtu najdeme součet $1 + \zeta^k + \cdots + \zeta^{k(m-1)} = 0$. Platí tedy

$$m = \sum_{k=0}^{m-1} \frac{1 - x^m}{1 - \zeta^k x} = (1 - x^m) \cdot \sum_{k=0}^{m-1} \frac{1}{1 - \zeta^k x}.$$

Vydělením rovnosti číslem $m(1 - x^m)$ se suma (vydělená m) rovná číslu $1/(1 - x^m)$. Konkrétně budeme využívat tuto rovnost pro $x = \varphi$ a $x = \tilde{\varphi}$. Sečteme tedy zlomky nejdříve pro $\mathcal{Z}_1$ a převedeme zpět na společného jmenovatele, čímž dostaneme

$$\mathcal{Z}_1 = \frac{1}{\sqrt{5}} \left(\frac{-1}{1 - \varphi^m} + \frac{1}{1 - \tilde{\varphi}^m} \right) = \frac{\frac{-1}{\sqrt{5}}(\varphi^m - \tilde{\varphi}^m)}{1 - (\varphi^m + \tilde{\varphi}^m) + (\varphi\tilde{\varphi})^m} = \frac{-F_m}{1 - L_m + (-1)^m}.$$

Využili jsme zde jak explicitních vztahů pro Fibonacciho a Lucasova čísla, tak i toho, že $\varphi\tilde{\varphi} = -1$. Podobně pro $\mathcal{Z}_2$ platí

$$\mathcal{Z}_2 = 1 + \frac{1}{\sqrt{5}}\left(\frac{1-\varphi}{1-\varphi^m} + \frac{\tilde{\varphi}-1}{1-\tilde{\varphi}^m}\right) = 1 + \frac{\frac{1}{\sqrt{5}}(\varphi^m - \tilde{\varphi}^m) + \frac{-\varphi\tilde{\varphi}}{\sqrt{5}}(\varphi^{m-1} - \tilde{\varphi}^{m-1}) - \frac{1}{\sqrt{5}}(\varphi - \tilde{\varphi})}{1 - (\varphi^m + \tilde{\varphi}^m) + (\varphi\tilde{\varphi})^m}.$$

Zde navíc využijeme vztahu $\varphi - \tilde{\varphi} = \sqrt{5}$ a také známé identity $L_m = F_{m+1} + F_{m-1}$. Po úpravě získáme

$$\mathcal{Z}_2 = 1 + \frac{F_m + F_{m-1} - 1}{1 - L_m + (-1)^m} = \frac{-F_{m-1} + (-1)^m}{1 - L_m + (-1)^m}.$$

Pokud nyní dosadíme za $\mathcal{Z}_1$ a $\mathcal{Z}_2$, tak dokážeme upravit výraz

$$F_n \mathcal{Z}_2 + F_{n+1} \mathcal{Z}_1 = \frac{F_n(-F_{m-1} + (-1)^m) + F_{n+1}(-F_m)}{1 - L_m + (-1)^m} = \frac{-F_n F_{m-1} - F_{n+1} F_m + (-1)^m F_n}{1 - L_m + (-1)^m}$$

Z Honsbergerovy identity platí $F_n F_{m-1} + F_{n+1} F_m = F_{m+n}$, takže po dosazení získáme

$$F_n \mathcal{Z}_2 + F_{n+1} \mathcal{Z}_1 = \frac{F_{m+n} + (-1)^{m+1} F_n}{L_m - 1 + (-1)^{m+1}} \tag{3.10}$$

a analogicky vyjde i $F_r \mathcal{Z}_2 + F_{r+1} \mathcal{Z}_1$, takže po odečtení F_r vyjde

$$F_r \mathcal{Z}_2 + F_{r+1} \mathcal{Z}_1 - F_r = \frac{F_{m+r} + (-1)^{m+1} F_r}{L_m - 1 + (-1)^{m+1}} - F_r = \frac{F_{m+r} - F_r L_m + F_r}{L_m - 1 + (-1)^{m+1}}.$$

Lze dokázat, že platí $F_r L_m = F_{m+r} - (-1)^r F_{m-r}$, což dosadíme do výrazu a po úpravě získáme

$$F_r \mathcal{Z}_2 + F_{r+1} \mathcal{Z}_1 - F_r = \frac{(-1)^r F_{m-r} + F_r}{L_m - 1 + (-1)^{m+1}}. \tag{3.11}$$

Pokud tyto dvě rovnice nyní dosadíme do vzorečku (3.9), tak dostaneme přímo dokazované tvrzení. □

Definice 3.2.11 (Zaokrouhlení)**.** Pro libovolné $x \in \mathbb{R}$ značme $\lfloor x \rceil$ jako zaokrouhlení na nejbližší celé číslo. Platí rovnost $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor$.

Toto řešení však obsahuje mnoho členů – co kdybychom využili zaokrouhlení? Ukáže se, že je možné získat ještě jednodušší výsledek, a to pro $m = 5$ a libovolně velké $m \geq 7$.

Věta 3.2.12 (Vlastní)**.** *Nechť n je přirozené. Pro $m = 5$ nebo $m \geq 7$ platí rovnost*

$$\mathcal{F}_m(n) = \left\lfloor \frac{(-1)^{m+1} F_n + F_{n+m}}{L_m - 1 - (-1)^m} \right\rceil.$$

Důkaz. Dokážeme, že pokud $r = n \bmod m$, pak pro $m = 5$ nebo $m \geq 7$ platí nerovnost

$$\left| \frac{(-1)^r F_{m-r} + F_r}{L_m - 1 + (-1)^{m+1}} \right| < \frac{1}{2}.$$

Vzhledem k tomu, že $\mathcal{F}_m(n)$ je celé číslo, tak pokud připustíme předpoklad výše, pak platí

$$\mathcal{F}_m(n) = \left\lfloor \mathcal{F}_m(n) - \frac{(-1)^r F_{m-r} + F_r}{L_m - 1 + (-1)^{m+1}} \right\rceil = \left\lfloor \frac{(-1)^{m+1} F_n + F_{n+m}}{L_m - 1 - (-1)^m} \right\rceil.$$

Odhadneme čitatel i jmenovatel. Jednak platí $L_m - 1 + (-1)^{m+1} \geq L_m - 2 > 0$, jednak je absolutní hodnota čitatele nejvýše $F_{m-r} + F_r$. Pokud $r = 0$, pak se čitatel rovná nejvýše F_m. Ve všech ostatních případech platí nerovnosti $F_{m-r} \leq F_{m-1}$ a $F_r \leq F_{m-1}$. Za předpokladu, že jsou oba indexy různé, je jedno z čísel nejvýše F_{m-2}. Jinak jsou indexy $m - r$ a r shodné neboli $r = m/2 \leq m - 2$, takže by obě čísla F_{m-r}, F_r byla nejvýše F_{m-2}. V obou případech tedy platí nerovnost

$$F_{m-r} + F_r \leq F_{m-2} + F_{m-1} = F_m$$

Dosazením nerovností platí

$$\left| \frac{(-1)^r F_{m-r} + F_r}{L_m - 1 + (-1)^{m+1}} \right| \leq \frac{F_m}{L_m - 2}$$

Pro $m = 5$ snadno ověříme, že opravdu platí nerovnost

$$\frac{F_5}{L_5 - 1 + (-1)^{5+1}} = \frac{5}{11} < \frac{1}{2}.$$

Předpokládejme nyní, že pro $m \geq 7$ nerovnost neplatí, $\frac{1}{2} \leq \left| \frac{(-1)^r F_{m-r} + F_r}{L_m - 1 + (-1)^{m+1}} \right| \leq \frac{F_m}{L_m - 2}$. Úpravou získáme

$$L_m - 2F_m \leq 2,$$

Pokud využijeme identitu $L_m = F_{m-1} + F_{m+1}$, tak z rekurentního vzorce a úpravou získáme nerovnost $F_{m-3} \leq 2$. Vzhledem k tomu, že Fibonacciho posloupnost je neklesající a jelikož platí $m - 3 \geq 4$, tak $F_{m-3} \geq F_4 > 2$, což je spor. Platí tedy dokazovaná nerovnost, a tudíž i věta. □

Poznámka. Ve větě 3.2.12 jsme dále ukázali, že pro $m = 5$ a všechna $m \geq 7$ existuje vzorec zahrnující zaokrouhlení. Pro zbývající čísla $m = 4$ a $m = 6$ ukážeme, že tyto vzorce také obsahují zaokrouhlení.

Věta 3.2.13. *Pro součet každého čtvrtého Fibonacciho čísla platí*

$$\mathcal{F}_4(n) = \left\lfloor \frac{F_{n+4} - F_n - 1}{5} \right\rceil.$$

Důkaz. Pro $m = 4$ platí $L_4 = 7$, takže z věty 3.2.10 vyjde

$$\mathcal{F}_4(n) = \frac{F_{n+4} - F_n}{5} + \frac{(-1)^r F_{4-r} + F_r}{5}.$$

Konstantní člen je pro $r = 0, 1, 2, 3$ po řadě roven $\frac{3}{5}, \frac{-1}{5}, \frac{2}{5}, \frac{1}{5}$. Pokud odečteme $\frac{1}{5}$, pak můžeme zaokrouhlit na nejbližší celé číslo. □

Věta 3.2.14. *Pro součet každého šestého Fibonacciho čísla platí*

$$\mathcal{F}_6(n) = \left\lfloor \frac{F_{n+3} - 1}{4} \right\rceil.$$

Důkaz. Pro $m = 6$ platí $L_6 = 18$, takže z podobně jako výše z věty 3.2.10 platí

$$\mathcal{F}_6(n) = \frac{F_{n+6} - F_n}{16} + \frac{(-1)^r F_{6-r} + F_r}{16}.$$

Druhý sčítanec je pro $r = 0, ..., 5$ po řadě roven $\frac{8}{16}, \frac{-4}{16}, \frac{5}{16}, 0, \frac{4}{16}, \frac{4}{16}$. Pokud odečteme $1/4$, pak můžeme opět zaokrouhlit na nejbližší celé číslo. Pišme tedy

$$\mathcal{F}_6(n) = \left\lfloor \frac{F_{n+6} - F_n - 4}{16} \right\rceil.$$

Navíc platí

$$F_{n+6} = 2F_{n+4} + F_{n+3} = 3F_{n+3} + 2F_{n+2} = 3F_{n+3} + F_{n+2} + F_{n+1} + F_n = 4F_{n+3} + F_n,$$

takže $F_{n+6} - F_n = 4F_{n+3}$ a po zkrácení čtyř dostaneme výsledek. □

Kapitola 4

Počítání podmnožin se součtem prvků

Odmocniny z jedné nám umožňují počítat podmnožiny, jejichž součet je dělitelný určitým číslem. Významnou motivací pro tuto kapitolu byla úloha 4.3.2 z loňského ročníku Matematické olympiády [8]:

> Kolik neprázdných podmnožin množiny $\{0, 1, 2, \ldots, 9\}$ má součet prvků dělitelný třemi?

V této kapitole se budeme zabývat zejména následující úlohou.

Úloha 4.0.1. Je dána konečná množina $S \subset \mathbb{Z}$ a celá čísla $0 \leq r < m$. Kolik jejích podmnožin dává součet prvků zbytek r po dělení m?

Celé řešení této obecné úlohy (sekce 4.4 a dále) je vlastní prací. Nejdříve ale vyřešíme úlohy pro některé konkrétní množiny.

Pokud uvažujeme libovolnou množinu prvků, tak kompaktní explicitní řešení úlohy zde najdeme pro hodnoty dělitele $m = 1, 2, 3, 4, 6, 8, 12 \ldots$, tedy konkrétně čísla tvaru $m = 2^\alpha$ a $m = 3 \cdot 2^\alpha$, kde $\alpha \geq 0$. Také ukážeme, že řešením pro $m = 5$ (a každé další prvočíslo) je součet alespoň p^{p-3} čísel, z nichž každé je různým součinem $p - 2$ čísel tvaru χ_m^r neboli součtů každého m-tého kombinačního čísla.

Významnou roli při hledání bude kromě součtu kombinačních čísel hrát *Roots of Unity Filter* a také třeba věta 1.2.14 o prvočíselných odmocninách z jedné. Tyto věty využijeme především v kombinaci s generujícími funkcemi, které nyní krátce uvedeme.

4.1 Úvod do generujících funkcí

Jedním zásadním pojmem, který zde budeme využívat na manipulaci s posloupnostmi čísel, jsou *generující funkce*. Místo nekonečných posloupností, se kterými je obtížné pracovat, se dívejme na jednoduchou funkci, kterou tuto řadu reprezentujme. Konkrétně například funkcí

$$f(x) = 1 + 3x + 5x^2 + 7x^3 + \cdots$$

určíme posloupnost $1, 3, 5, 7, \ldots$, a to pomocí koeficientů mocninné řady f.

Definice 4.1.1. Pokud je f generující funkcí, pak její zápis pomocí mocninné řady

$$f(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + c^4x^4 + \cdots$$

nazývejme *generující řadou*. Říkejme, že funkce f generuje posloupnost čísel

$$c_0, c_1, c_2, c_3, c_4, \ldots$$

Příklad 4.1.2. Připomeňme si rovnost

$$1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \cdots + \frac{x^n}{n!} + \cdots = e^x.$$

Můžeme tedy využít funkci e^x, abychom popsali tuto nekonečnou řadu koeficientů. V tomto případě máme posloupnost

$$1, 1, \frac{1}{2}, \frac{1}{6}, \frac{1}{24}, \ldots, \frac{1}{n!}, \ldots,$$

jejíž generující funkcí je e^x.

Více lze vyhledat v literatuře [7]. Zde budeme využívat generující funkce hlavně v kontextu kombinatorických úloh, a to konkrétně pro součty podmnožin.

Úmluva. Za součet prvků prázdné množiny považujme nulu.

Příklad 4.1.3. Mějme množinu $S = \{2\}$. Existují právě dvě podmnožiny, $\emptyset, \{1\}$ (se součty 0 a 1), což je generováno funkcí $1 + x$. Pokud nyní přidáme do množiny další prvek, $S = \{1, -1\}$, tak do každé dříve určené podmnožiny prvek vložíme, či nikoli. Počty podmnožin s určitým součtem nyní generuje funkce $(1+x)(1+x^{-1}) = 2+x+x^{-1}$, a to pro $\emptyset, \{1\}, \{-1\}, \{1, -1\}$. Pokud bychom přidali rovnou více prvků, $S = \{-1, 1, 2, 3, 4\}$, tak počet podmnožin S se součtem j získáme, když se podíváme na koeficient u x^j ve funkci

$$(1 + x^{-1})(1 + x)(1 + x^2)(1 + x^3)(1 + x^4).$$

4.2 Známé úlohy

Úloha 4.2.1. Hodíme n běžnými šestistěnnými hracími kostkami s čísly $1, \ldots, 6$. Určete pravděpodobnost, že součet čísel na kostkách je dělitelný pěti.

Řešení. Každá kostka přispěje k součtu jedním z čísel 1 až 6. Hodíme-li n kostkami, pak se jedná o n totožných nezávislých dějů, kde každý z nich má generující funkci $x+x^2+\cdots+x^6$.

$$f(x) = (x + x^2 + \cdots + x^6)^n = \sum_{i\geq 0} a_i x^i.$$

Potom koeficient a_k je počtem způsobů, že nám padl součet k.

Nechť $\zeta = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$ je primitivní pátá odmocnina z jedné. Z Roots of Unity Filtru platí $5a^{(0)} = f(1) + f(\zeta) + \cdots + f(\zeta^4)$, kde $a^{(0)} = a_0 + a_5 + \ldots$ Pro každé k platí rovnost

$$f(\zeta^k) = (\zeta^k + \zeta^{2k} + \cdots + \zeta^{6k})^n = \begin{cases} 6^n, & \text{pokud } 5 \mid k, \\ \zeta^{kn}, & \text{pokud } 5 \nmid k. \end{cases}$$

Takže pokud $5 \mid n$, pak $a^{(0)} = \frac{1}{5}(6^n + 4)$, jinak $\zeta^n \neq 1$, takže součet funkčních hodnot obsahuje geometrickou řadu $5a^{(0)} = 6^n + \zeta^n + \zeta^{2n} + \cdots + \zeta^{4n} = 6^n - 1 + \frac{\zeta^{5n}-1}{\zeta^n-1}$, takže platí $a^{(0)} = \frac{1}{5}(6^n - 1)$.

Pravděpodobnost P_n hodu součtu dělitelným pěti získáme vydělením všemi možnými hody čili 6^n. Platí tedy

$$P_n = \begin{cases} \frac{1}{5} + \frac{4}{5\cdot 6^n}, & \text{pokud } 5 \mid n, \\ \frac{1}{5} - \frac{1}{5\cdot 6^n}, & \text{pokud } 5 \nmid n. \end{cases}$$

□

I pokud zjišťujeme ciferný součet, tak lze chytře využít odmocniny z jedné spolu s generující funkcí.

Úloha 4.2.2. Určete počet čísel složených z n cifer, kde každá je buď 1, 3, 4, 6, 7, nebo 9, jejichž ciferný součet je dělitelný sedmi.

Řešení. Každá číslice přispěje svojí hodnotou k cifernému součtu. Vzhledem k tomu, že žádná cifra není nulová, tak každá kombinace vytvoří n-ciferné číslo. Generující funkce popisující počet čísel s daným ciferným součtem je tedy

$$f(x) = (x + x^3 + x^4 + x^6 + x^7 + x^9)^n = \sum_{i\geq 0} a_i x^i.$$

Nechť $\zeta = \cos(\frac{2\pi}{7}) + i\sin(\frac{2\pi}{7})$ je sedmá odmocnina z jedné. Dosazením $\zeta^0 = 1$ je výraz v součinu roven $f(1) = 6^n$ a pro ζ^k, kde $7 \nmid k$, platí

$$\begin{aligned} f(\zeta^k) &= (\zeta^k + \zeta^{3k} + \zeta^{4k} + \zeta^{6k} + \zeta^{7k} + \zeta^{9k})^n = \\ &= (1 + \zeta^k + \zeta^{2k} + \zeta^{3k} + \zeta^{4k} + \zeta^{6k})^n = (-\zeta^{5k})^n = (-1)^n(\zeta^{5n})^k. \end{aligned}$$

Sečtením pro $k \in \{0, \ldots, 6\}$ máme

$$7a^{(0)} = \sum_{k=0}^{6} f(\zeta^k) = 6^n + (-1)^n \sum_{k=1}^{6} (\zeta^{5n})^k,$$

kde $a^{(0)} = a_0 + a_7 + \dots$ Pokud $7 \mid n$, tak platí $\zeta^{5n} = 1$, takže suma se rovná 6. V opačném případě $7 \nmid n$ čili $\zeta^7 \neq 1$, takže se suma rovná $\zeta^{5n} + \cdots + (\zeta^{5n})^6 = -1$. Počet hledaných čísel je

$$a^{(0)} = \begin{cases} \frac{1}{7}(6^n + 6(-1)^n), & \text{pokud } 7 \mid n, \\ \frac{1}{7}(6^n - (-1)^n), & \text{pokud } 7 \nmid n. \end{cases}$$

□

4.3 Jednoduché množiny

V rámci této sekce vyřešíme zejména úlohu 4.3.2 ze 73. (loňského) ročníku Matematické olympiády.

V následujících úlohách volíme množinu $\{1, 2, 3, \dots, n\}$, u které zkoumáme počet podmnožin, jejichž součet je dělitelný postupně dvěma, 4.3.1, třemi, číslem n, 4.3.4, přirozenou mocninou dvojky, 4.3.6, či libovolným prvočíslem v úloze 4.3.5.

Úloha 4.3.1. Kolik podmnožin množiny $\{1, 2, 3, \dots, n\}$ má sudý součet prvků?

Řešení. Pokud se podíváme na libovolnou podmnožinu, tak každý prvek $k = 1, 2, \dots, n$ přispívá buď nulou nebo k. Generující funkce pro samostatný prvek k je tedy $1 + x^k$. Uvažujme nyní generující funkci

$$f(x) = (1 + x)(1 + x^2) \cdots (1 + x^n),$$

kde po roznásobení odpovídá koeficient u x^i počtu podmnožin se součtem i. Pišme

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$$

Hledáme nyní $a^{(0)} = a_0 + a_2 + a_4 + \dots$ Abychom sečetli pouze sudé pozice naší posloupnosti, dosadíme postupně hodnoty 1 a -1 do funkce.

$$f(1) = a_0 + a_1 + a_2 + a_3 + \dots,$$
$$f(-1) = a_0 - a_1 + a_2 - a_3 + \dots$$

Sečtením a vydělením dvěma získáme rovnost

$$a^{(0)} = \frac{f(1) + f(-1)}{2}.$$

Nahlédnutím k definici platí $f(1) = 2^n$ a $f(-1) = (1 - 1)(1 + 1) \cdots = 0$. Dosazením je počet všech podmnožin se sudým počtem prvků právě 2^{n-1}.

Podmnožin s lichým součtem je zbytek neboli také polovina všech. Pokud označíme $a^{(r)}$ je počet podmnožin $\{1, 2, \dots, n\}$ se součtem r modulo 2, pak

$$a^{(0)} = a^{(1)} = 2^{n-1}.$$

□

Podobným způsobem vyřešíme úlohu z loňského domácího kola Matematické olympiády kategorie B. Využívat zde budeme třetí odmocniny z jedné.

Úloha 4.3.2. Kolik neprázdných podmnožin množiny $\{0, 1, 2, \ldots, 9\}$ má součet prvků dělitelný třemi? (MO B 73-I-1, [8])

Řešení. Uvažujme generující funkci v součinovém tvaru

$$f(x) = (1+1)(1+x)(1+x^2)\cdots(1+x^9),$$

kterou roznásobíme do tvaru

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots$$

Koeficient a_n udává počet podmnožin se součtem prvků n. Definujme primitivní třetí odmocninu z jedné jako $\zeta = \cos(2\pi/3) + i\sin(2\pi/3)$. Dosadíme tedy do f čísla $1, \zeta, \zeta^2$.

$$\begin{aligned} f(1) &= a_0 + a_1 + a_2 + a_3 + a_4 + \ldots, \\ f(\zeta) &= a_0 + a_1\zeta + a_2\zeta^2 + a_3 + a_4\zeta + \ldots, \\ f(\zeta^2) &= a_0 + a_1\zeta^2 + a_2\zeta + a_3 + a_4\zeta^2 + \ldots. \end{aligned}$$

Sečtením těchto tří rovností získáme u $a_0, a_3, \ldots$ koeficient 3, zatímco ostatních vyjde koeficient $1 + \zeta + \zeta^2 = (\zeta^3 - 1)/(\zeta - 1) = 0$. Vydělme třemi.

$$a_0 + a_3 + a_6 + a_9 + \cdots = \frac{f(1) + f(\zeta) + f(\zeta^2)}{3}. \tag{4.1}$$

Dle věty 1.2.10 platí rovnost

$$(1+\zeta)(1+\zeta^2) = 1,$$

a navíc nahlédnutím k definici platí rovnosti $f(1) = 2^{10}$,

$$\begin{aligned} f(\zeta) &= (1+1)(1+\zeta)(1+\zeta^2)\cdots(1+\zeta^9) = 2^4(1+\zeta)^3(1+\zeta^2)^3 = 2^4, \\ f(\zeta^2) &= (1+1)(1+\zeta^2)(1+\zeta^4)\cdots(1+\zeta^{18}) = 2^4(1+\zeta)^3(1+\zeta^2)^3 = 2^4. \end{aligned}$$

Dosazením těchto hodnot do rovnosti (4.1) platí

$$a_0 + a_3 + a_6 + a_9 + \cdots = \frac{2^{10} + 2^4 + 2^4}{3} = \frac{2^{10} + 2^5}{3}.$$

Úloha však nepřipouští prázdnou množinu (se součtem 0), která je jedna. Vyhovujících podmnožin je tedy

$$(a_0 + a_3 + a_6 + a_9 + \ldots) - 1 = \frac{2^{10} + 2^5}{3} - 1 = 351.$$

□

Tento způsob sečtení funkčních hodnot tak, že nám zůstal každý druhý či třetí člen, není nic jiného, než jednoduchý příklad Roots of Unity Filteru. V následujících úlohách začneme pracovat s Roots of Unity Filterem jako s obecným nástrojem pro sečtení každého n-tého koeficientu v posloupnosti.

Definice 4.3.3 (Eulerova funkce)**.** Eulerovou funkcí φ myslíme funkci $\varphi : \mathbb{N} \to \mathbb{N}$, kde $\varphi(n)$ se rovná počtu přirozených čísel menších než n, která jsou nesoudělná s n.

Úloha 4.3.4. Označme $a^{(0)}$ počet podmnožin $\{1, 2, 3, \ldots, n\}$, jejichž součet prvků je dělitelný n. Dokažte, že platí

$$a^{(0)} = \frac{1}{n} \sum_{d|n,\ 2\nmid d} \varphi(d) \cdot 2^{n/d}.$$

Řešení. Definujme generující funkci

$$f(x) = (1 + x)(1 + x^2) \cdots (1 + x^n) = a_0 + a_1 x + a_2 x^2 + \ldots$$

Koeficient a_j je roven počtu podmnožin se součtem j. Zjevně platí $a^{(0)} = a_0 + a_n + a_{2n} + \ldots$ Označme $\zeta = \cos(2\pi/n) + i \sin(2\pi/n)$. Z Roots of Unity Filtru platí rovnost

$$a^{(0)} = \frac{1}{n} \sum_{j=1}^{n} f(\zeta^j). \tag{4.2}$$

Platí $f(\zeta^j) = (1 + \zeta^j)(1 + x^{2j}) \cdots (1 + x^{nj})$, takže pokud označíme $d = n/\gcd(n, k)$, pak z věty 1.2.11 přímo platí rovnost

$$f(\zeta^j) = \begin{cases} 2^{n/d}, & \text{pokud } d \text{ je liché,} \\ 0, & \text{pokud } d \text{ je sudé.} \end{cases}$$

Číslo ζ^j je d-tou primitivní odmocninou z jedné, pokud j je tvaru $k \cdot (n/d)$, kde k a d jsou nesoudělná čísla a $k \in \{1, \ldots, d\}$. Takových čísel j proto existuje $\varphi(d)$. Za všechny liché primitivní d-té odmocniny z jedné se přičte k výsledku $\varphi(d)2^{n/d}$. Platí tedy

$$a^{(0)} = \frac{1}{n} \sum_{j=1}^{n} f(\zeta^j) = \frac{1}{n} \sum_{d|n, 2\nmid d} \varphi(d) \cdot 2^{n/d}.$$

□

Úloha 4.3.5. Je dáno prvočíslo $p > 2, r \in \{0, \ldots, p-1\}$ a $n \in \mathbb{N}$. Označme $a^{(r)}$ počet podmnožin $\{1, 2, 3, \ldots, np\}$, jejichž součet dává zbytek r po dělení prvočíslem p. Dokažte, že potom platí

$$a^{(r)} = \begin{cases} \frac{1}{p}\left(2^{pn} + (p-1) \cdot 2^n\right) & \text{pro } r = 0, \\ \frac{1}{p}\left(2^{pn} - 2^n\right) & \text{pro } r \in \{1, \ldots, p-1\}. \end{cases}$$

Řešení. Označme $\zeta = \cos(2\pi/p) + i\sin(2\pi/p)$ primitivní p-tou odmocninu z jedné a pišme generující funkci

$$f(x) = (1+x)(1+x^2)\cdots(1+x^{np}) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$$

Číslo a_j odpovídá počtu podmnožin se součtem j. Definujme p čísel $a^{(0)}, \dots, a^{(p-1)}$ takových, že $a^{(j)} = a_j + a_{p+j} + a_{2p+j} + a_{3p+j} + \dots$ S touto definicí dosadíme číslo ζ do funkce, čímž se nám seskupí každý p-tý člen.

$$f(\zeta) = a^{(0)} + \zeta a^{(1)} + \zeta^2 a^{(2)} + \dots + \zeta^{p-1}a^{(p-1)}. \tag{4.3}$$

Rozepišme polynom $z^p - 1$ pomocí kořenových činitelů a dosaďme $z = -1$. Platí tedy vztah $(-1)^p - 1 = (-1-1)(-1-\zeta)\cdots(-1-\zeta^{p-1})$ čili

$$(1+1)(1+\zeta)(1+\zeta^2)\cdots(1+\zeta^{p-1}) = 2.$$

Platí tedy $f(\zeta) = \left((1+\zeta)(1+\zeta^2)\cdots(1+\zeta^{p-1})(1+1)\right)^n = 2^n$. Spolu s rovností (4.3) tedy máme

$$(a^{(0)} - 2^n) + \zeta a^{(1)} + \zeta^2 a^{(2)} + \dots + \zeta^{p-1}a^{(p-1)} = 0. \tag{4.4}$$

Z věty 1.2.14 platí $a^{(0)} - 2^n = a^{(1)} = a^{(2)} = \dots = a^{(p-1)}$. Určíme také součet všech koeficientů jako $a^{(0)} + \dots + a^{(p-1)} = f(1) = 2^{np}$, takže existuje

$$a^{(0)} = \frac{2^{np} - 2^n}{p} + 2^n = \frac{2^{np} + (p-1)\cdot 2^n}{p}$$

podmnožin se součtem dělitelným p, zatímco pouze

$$a^{(1)} = \dots = a^{(p-1)} = \frac{2^{np} - 2^n}{p}$$

podmnožin se součtem, který je kongruentní nenulovému zbytku modulo p. □

Úloha 4.3.6 (Vlastní)**.** Je dáno α přirozené a $n \geq 2^{\alpha-1}$. Dokažte, že pro každý zbytek $r \in \{0, 1, 2, \dots, 2^\alpha - 1\}$ existuje stejný počet podmnožin $\{1, 2, 3, \dots, n\}$ se součtem kongruentním r modulo 2^α.

Řešení. Pišme generující funkci

$$f(x) = (1+x)(1+x^2)\cdots(1+x^n) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$$

Pro zbytek $r \in \{0, 1, \dots, 2^n - 1\}$ definujme číslo $a^{(r)} = a_r + a_{r+2^n} + \dots$ a primitivní 2^n-tou odmocninu z jedné $\zeta = \cos(2\pi/2^n) + i\sin(2\pi/2^n)$. Z Roots of Unity Filtru platí rovnost

$$a^{(r)} = \frac{f(1) + \zeta^{-r}f(\zeta) + \zeta^{-2r}f(\zeta^2) + \dots + \zeta^{-(2^\alpha-1)r}f(\zeta^{2^\alpha-1})}{2^\alpha}. \tag{4.5}$$

Dokážeme, že $f(\zeta) = \cdots = f(\zeta^{2^\alpha - 1}) = 0$. Pro dané $r \in \{1, \ldots, 2^\alpha - 1\}$ pišme $r = 2^\beta \cdot R$ tak, že R je liché. Pro $k = 2^{\alpha-\beta-1}$ platí rovnost

$$\zeta^{rk} = \zeta^{(2^\beta R)(2^{\alpha-\beta-1})} = \zeta^{2^{\alpha-1} R} = (-1)^R = -1.$$

Číslo r není násobkem 2^α, takže $\beta \leq \alpha - 1$, a tedy k je celé číslo. Také je β nezáporné číslo, tudíž $k \leq 2^{\alpha-1} \leq n$. Činitel $1 + \zeta^{rk} = 0$ se vyskytuje ve funkční hodnotě

$$f(\zeta^r) = (1 + \zeta^r)(1 + \zeta^{2r}) \cdots (1 + \zeta^{kr}) \cdots (1 + \zeta^{nr}) = 0.$$

Pro každé $r \in \{0, \ldots, m-1\}$ dosazením do rovnosti (4.5) máme

$$a^{(r)} = \frac{f(1)}{2^\alpha} = \frac{2^n}{2^\alpha} = 2^{n-\alpha}.$$

Pro dané $\alpha \in \mathbb{N}$, $n \geq 2^{\alpha-1}$ a zbytek r existuje $2^{n-\alpha}$ podmnožin $\{1, \ldots, n\}$ se součtem r modulo 2^α. □

4.4 Obecná množina

Nyní se pokusíme řešit úlohu 4.0.1 obecně. Je dáno číslo m a také množina celých čísel S. Naším cílem je najít čísla $a^{(0)}, \ldots, a^{(m-1)}$, kde $a^{(r)}$ značí počet podmnožin, jejichž součet prvků je kongruentní r modulo m.

Definice 4.4.1 (Řešení obecné úlohy)**.** Jsou dána čísla $m, r \in \mathbb{N}$ a m čísel $s_0, \ldots, s_{m-1}$. Je dána množina obsahující s_j prvků kongruentních j modulo m, kde $j \in \{0, \ldots, m-1\}$. Počet jejích podmnožin se součtem prvků kongruentním r modulo m nazývejme řešením úlohy a popisujme jej funkcí $\mathcal{A}_m^r : \mathbb{N}_0^m \to \mathbb{N}_0$ definovanou jako

$$\mathcal{A}_m^r (s_0, \ldots, s_{m-1}) = a^{(r)}.$$

Poznámka. Počet vyhovujících podmnožin je jednoznačně dán hodnotami s_j, nezáleží tak na konkrétních číslech v množině.

V průběhu řešení dokážeme několik lemmat, která nám umožní postupně zjednodušovat výsledek. Začneme s následující jednoduchou vlastností.

Lemma 4.4.2 (Redukce nulových prvků)**.** Nechť $s_0, \ldots, s_{m-1} \in \mathbb{N}_0$. Řešení úlohy označme $\mathcal{A}_m^r (s_0, \ldots, s_{m-1})$, tedy počet podmnožin S (kde v S je s_γ prvků γ modulo m), jejichž součet je kongruentní r modulo m. Potom platí

$$\mathcal{A}_m^r (s_0, \ldots, s_{m-1}) = 2^{s_0} \cdot \mathcal{A}_m^r (0, s_1, \ldots, s_{m-1}).$$

Důkaz. Stačí dokázat rovnost $\mathcal{A}_m^r (s_0, \ldots, s_{m-1}) = 2\,\mathcal{A}_m^r (s_0 - 1, s_1, \ldots, s_{m-1})$, z indukce potom vyplývá původní tvrzení. Přidejme do množiny jeden prvek 0 mod m. Každá vyhovující podmnožina je nyní vyhovující současně s novým prvkem i bez něj. Naopak žádná nevyhovující podmnožina se nestane vyhovující, pokud do ní přidáme tento prvek. Počet řešení se tak zdvojnásobí, což jsme chtěli ukázat. □

Lemma 4.4.3 (Obecný vzorec)**.** Definujme $m \in \mathbb{N}$ a m-tici čísel $s_0, \dots, s_{m-1} \in \mathbb{N}_0$. Označíme $\zeta = \cos(2\pi/m) + i \sin(2\pi/m)$. Dále nechť $\mathcal{A}_m^r(s_0, \dots, s_{m-1})$ je počtem podmnožin S (kde v S je s_γ prvků γ modulo m), jejichž součet je kongruentní r modulo m, pak platí

$$\mathcal{A}_m^r(s_0, \dots, s_{m-1}) = \frac{1}{m} \sum_{k=0}^{m-1} \zeta^{-rk} \prod_{j=0}^{m-1} (1 + \zeta^{jk})^{s_j}.$$

Důkaz. Pišme generující funkci

$$f(x) = \prod_{s \in S} (1 + x^s) = \dots + a_{-2}x^{-2} + a_{-1}x^{-1} + a_0 + a_1 x + a_2 x^2 + \dots,$$

Po roznásobení odpovídá koeficient a_j počtu podmnožin se součtem j čili

$$a^{(r)} = \dots + a_{r-2m} + a_{r-m} + a_r + a_{r+m} + a_{r+2m} + \dots$$

Pro primitivní m-tou odmocninu z jedné ζ platí Roots of Unity Filter.

$$a^{(r)} = \frac{f(1) + \zeta^{-r} f(\zeta) + \zeta^{-2r} f(\zeta^2) + \dots + \zeta^{-(m-1)r} f(\zeta^{m-1})}{m}. \tag{4.6}$$

Pokud dosadíme číslo ζ^k do součinového tvaru f, pak dostaneme

$$f(\zeta^k) = \prod_{s \in S} (1 + \zeta^{ak}) = \prod_{j=0}^{m-1} (1 + \zeta^{jk})^{s_j}, \tag{4.7}$$

kde s_j je počtem prvků kongruentních j modulo m. Pišme rovnost (4.6) formou sumy a dosaďme vztah (4.7).

$$m \cdot a^{(r)} = \sum_{k=0}^{m-1} \zeta^{-rk} f(\zeta^k) = \sum_{k=0}^{m-1} \zeta^{-rk} \prod_{j=0}^{m-1} (1 + \zeta^{jk})^{s_j}. \tag{4.8}$$

Po vydělení m jsme hotovi. □

Nyní se podívejme na konkrétní množinu prvků, a to takovou, že obsahuje pouze prvky od jediného nenulového zbytku modulo m.

Důsledek 4.4.4 (Jediný nenulový zbytek)**.** Definujme přirozená čísla m, r a γ tak, že γ je nesoudělné s m. Označme $\mathcal{A}_m^r(0, \dots, s_\gamma, \dots, 0)$ počet podmnožin S (kde v S je jediných s_γ nenulových zbytků γ modulo m), jejichž součet prvků je r modulo m. Potom platí

$$\mathcal{A}_m^r(0, \dots, s_\gamma, \dots, 0) = \chi_m^{r\gamma^{-1}}(s_\gamma),$$

kde γ^{-1} značí multiplikativní inverzi čísla γ modulo m a $\chi_m^r(n) = \binom{n}{r} + \binom{n}{r+m} + \binom{n}{r+2m} + \dots$

Důkaz. Označme $\zeta = \cos(2\pi/m) + i\sin(2\pi/m)$ primitivní m-tou odmocninu z jedné. Z lemmatu 4.4.3 pro jedinou nenulovou hodnotu s_γ platí

$$\mathcal{A}_m^r(0,\dots,s_\gamma,\dots,0) = \frac{1}{m}\sum_{k=0}^{m-1}\zeta^{-rk}(1+\zeta^{\gamma k})^{s_\gamma} = \frac{1}{m}\sum_{k=0}^{m-1}\zeta^{-rk}(1+x^\gamma)^{s_\gamma}.$$

Binomickou větou rozšíříme mocninu, přičemž implicitně předpokládejme, že $\chi_m^r = \chi_m^r(s_\gamma)$.

$$\sum_{k=0}^{m-1}\zeta^{-rk}(1+x^\gamma)^{s_\gamma} = \sum_{k=0}^{m-1}\zeta^{-rk}\left(\chi_m^0 + \zeta^{k\gamma}\chi_m^1 + \dots + \zeta^{(m-1)k\gamma}\chi_m^{m-1}\right) =$$
$$= \sum_{k=0}^{m-1}\left(\zeta^{k(-r)}\chi_m^0 + \zeta^{k(\gamma-r)}\chi_m^1 + \dots + \zeta^{k((m-1)\gamma-r)}\chi_m^{m-1}\right) = m\,\chi_m^\alpha,$$

kde α splňuje rovnost $\alpha\gamma \equiv r \pmod{m}$ neboli $\alpha \equiv r\gamma^{-1} \pmod{m}$. Vzhledem k tomu, že čísla m, γ jsou nesoudělná, tak je zaručeno, že α existuje a je jednoznačně dáno jako zbytek modulo m. □

Poznámka. V tento moment je zjevné, že řešení úlohy s podmnožinami má mnoho společného se součty kombinačních čísel z předchozí kapitoly.

Pokud dále připustíme pouze prvočíselný dělitel p, tak umíme napsat následující lemma, které je založené na větě 1.2.14 o prvočíselných odmocninách z jedné.

Lemma 4.4.5 (Obecný vzorec pro prvočíslo)**.** Nechť p je prvočíslo a $s_0,\dots,s_{p-1} \in \mathbb{N}_0$. Pokud $\mathcal{A}_p^r(s_0,\dots,s_{p-1})$ značí počet podmnožin S (kde v S je s_γ prvků γ modulo p) se součtem prvků r modulo p, pak platí

$$\mathcal{A}_p^r(s_0,\dots,s_{p-1}) = \frac{1}{p}\left(2^{|S|} - \sum_{k=0}^{p-1} d_k\right) + d_r,$$

kde p-tici čísel $d_0,\dots,d_{p-1}$ splňuje rovnost

$$d_0 + \zeta d_1 + \zeta^2 d_2 + \dots + \zeta^{p-1}d_{p-1} = (1+\zeta^0)^{s_0}(1+\zeta^1)^{s_1}\cdots(1+\zeta^{p-1})^{s_{p-1}}.$$

Důkaz. Definujme generující funkci

$$f(x) = \prod_{s\in S}(1+x^s) = \dots + a_{-2}x^{-2} + a_{-1}x^{-1} + a_0 + a_1x + a_2x^2 + \dots,$$

kde po roznásobení odpovídá koeficient a_j počtu podmnožin se součtem j. Tím definujme čísla $a^{(0)},\dots,a^{(p-1)}$ tak, že $a^{(r)} = \dots + a_{r-2p} + a_{r-p} + a_r + a_{r+p} + a_{r+2p} + \dots$

Dále označme $\zeta = \cos(2\pi/p) + i\sin(2\pi/p)$ jako primitivní p-tou odmocninu z jedné. Do roznásobeného tvaru funkce f dosadíme číslo ζ, čímž se nám seskupí každý p-tý koeficient.

Platí tedy $f(\zeta) = a^{(0)} + \zeta a^{(1)} + \zeta^2 a^{(2)} + \cdots + \zeta^{p-1} a^{(p-1)}$. Podobně dosadíme ζ do součinového tvaru. Platí proto

$$f(\zeta) = \prod_{s \in S} (1 + \zeta^s) = \prod_{k=0}^{p-1} (1 + \zeta^k)^{s_k} = d_0 + \zeta d_1 + \zeta^2 d_2 + \cdots + \zeta^{p-1} d_{p-1},$$

kde $d_0, \ldots, d_{p-1}$ jsou racionální koeficienty při roznásobení tohoto součinu. Pokud sem dosadíme první vyjádření $f(\zeta)$, tak platí rovnost

$$(a^{(0)} - d_0) + (a^{(1)} - d_1)\zeta + \cdots + (a^{(p-1)} - d_{p-1})\zeta^{p-1} = 0.$$

Z lemmatu 1.2.14 přímo platí rovnosti $a^{(0)} - d_0 = a^{(1)} - d_1 = \cdots = a^{(p-1)} - d_{p-1}$. Pokud označíme $\Omega = a^{(r)} - d_r$, pak pišme $p\Omega$ jako

$$p\Omega = (a^{(0)} - d_0) + (a^{(1)} - d_1) + \cdots + (a^{(p-1)} - d_{p-1}) = \sum_{k=0}^{p-1} a^{(k)} - \sum_{k=0}^{p-1} d_k = 2^{|S|} - \sum_{k=0}^{p-1} d_k.$$

Pokud vyjádříme $a^{(r)} = \Omega + d_r$ a v tomto kontextu označíme $\mathcal{A}_m^r(s_0, \ldots, s_{p-1}) = a^{(r)}$, tak získáme dokazovanou rovnost. □

Poznámka. Úloha se nám lemmatem 4.4.5 pro prvočíselný dělitel zjednodušila na roznásobení jediného součinu.

Věta 4.4.6 (Redukce množiny pro prvočíslo)**.** *Nechť p je prvočíslo a $s_0, \ldots, s_{p-1} \in \mathbb{N}_0$. Označme $\mathcal{A}_p^r(s_0, \ldots, s_{p-1})$ počet podmnožin množiny s s_γ prvky γ modulo p, jejichž součet prvků je kongruentní r modulo p. Potom pro každé celé číslo $c \geq -\min(s_0, ..., s_{p-1})$ platí*

$$\mathcal{A}_p^r(s_0, s_1 + c, \ldots, s_{p-1} + c) = \mathcal{A}_p^r(s_0, \ldots, s_{p-1}) + 2^S \cdot \frac{2^{c(p-1)} - 1}{p},$$

kde píšeme $S = s_0 + \cdots + s_{p-1}$.

Důkaz. Označme $\zeta = \cos(2\pi/p) + i \sin(2\pi/p)$. Z lemmatu 4.4.5 platí

$$\mathcal{A}_p^r(s_0, s_1 + c, \ldots, s_{p-1} + c) = \frac{1}{p} \left(2^{S + c(p-1)} - \sum_{k=0}^{p-1} d_k \right) + d_r,$$

kde čísla $d_0, \ldots, d_{p-1}$ splňují

$$\begin{aligned} d_0 + \zeta d_1 + \cdots + \zeta^{p-1} d_{p-1} &= (1 + \zeta^0)^{s_0} (1 + \zeta^1)^{s_1 + c} \cdots (1 + \zeta^{p-1})^{s_{p-1} + c} \\ &= (1 + \zeta^0)^{s_0} (1 + \zeta^1)^{s_1} \cdots (1 + \zeta^{p-1})^{s_{p-1}}, \end{aligned}$$

přičemž jsme nahlédnuli k rovnosti $(1 + \zeta) \cdots (1 + \zeta^{p-1}) = 1$. Pro stejná čísla $d_0, \ldots, d_{p-1}$ tedy platí

$$\mathcal{A}_p^r(s_0, \ldots, s_{p-1}) = \frac{1}{p} \left(2^S - \sum_{k=0}^{p-1} d_k \right) + d_r.$$

Odečtením těchto dvou rovností se eliminuje $\sum_{k=0}^{p-1} d_k$ i d_r, takže získáme dokazované tvrzení. □

Poznámka. V tento moment máme všechno potřebné ke kompletnímu vyřešení případu pro dělitelnost třemi v podsekci 4.4.1.

4.4.1 Vyřešený případ pro dělitelnost třemi

Jelikož 3 je prvočíslo a existují pouze dva nenulové zbytky modulo 3, tak vždy dokážeme menší ze zbytků redukovat díky lemmatu 4.4.6. Ve chvíli, kdy uvažujeme jediný nenulový zbytek, tak lze počet podmnožin přímo spočítat z lemmatu 4.4.4.

Věta 4.4.7 (Vlastní)**.** *Jsou dána nezáporná celá čísla a, b, c, r, kde $r \in \{0, 1, 2\}$. V množině je celkem $a + b + c$ prvků, z nichž a je dělitelných třemi, b prvků dává zbytek 1 a c prvků dává zbytek 2 po dělení třemi. Označme $\mathcal{A}_3^r(a, b, c)$ počet podmnožin, jejichž součet prvků dává zbytek r po dělení třemi. Platí*

$$\mathcal{A}_3^r(a, b, c) = \frac{1}{3}\left(2^{a+b+c} + 2^{a+1} \cos\frac{(c - b + 2r)\pi}{3}\right).$$

Důkaz. Vzhledem k lemmatu 4.4.2 platí $\mathcal{A}_3^r(a, b, c) = 2^a \mathcal{A}_3^r(0, b, c)$. Nyní rozdělíme řešení podle toho, které z čísel b, c je větší.

(i) Pokud $b \geq c$, z lemmatu 4.4.6 pro $p = 3$ platí

$$\mathcal{A}_3^r(0, b, c) = \mathcal{A}_p^3(0, b - c, 0) + \frac{2^{b+c} - 2^{b-c}}{3}$$

a z lemmatu 4.4.4 pro jediný zbytek 1 modulo 3 platí $\mathcal{A}_3^r(0, b - c, 0) = \chi_3^r(b - c)$, jelikož platí $1 \equiv 1^{-1} \pmod 3$.

(ii) Pokud naopak $b < c$, tak platí

$$\mathcal{A}_3^r(0, b, c) = \mathcal{A}_p^3(0, 0, c - b) + \frac{2^{b+c} - 2^{c-b}}{3}$$

a z lemmatu 4.4.4 pro jediný zbytek 2 modulo 3 platí $\mathcal{A}_3^r(0, 0, c - b) = \chi_3^{2r}(c - b)$, jelikož $2 \equiv 2^{-1} \pmod 3$.

Pokud nahlédneme k výsledku úlohy 3.1.4, tak platí

$$\chi_3^r(n) = \binom{n}{r} + \binom{n}{r+3} + \cdots = \frac{1}{3}\left(2^n + 2\cos\frac{(n + 4r)\pi}{3}\right).$$

V prvním případě dosadíme $n = b - c$. Platí

$$\mathcal{A}_3^r(0, b, c) = \chi_3^r(b - c) + \frac{2^{b+c} - 2^{b-c}}{3} = \frac{1}{3}\left(2^{b+c} + 2\cos\frac{(b - c + 4r)\pi}{3}\right)$$

Jelikož platí $\cos(x) = \cos(-x + 2\pi r)$, tak se argument kosinu zde změní na $(c - b + 2r)\pi/3$, což chceme. Druhý případ dopadne analogicky – dosadíme $n = c - b$ a upravíme argument odečtením 2π,

$$\mathcal{A}_3^r(0, b, c) = \frac{1}{3}\left(2^{c+b} + 2\cos\frac{(c - b + 8r)\pi}{3}\right) = \frac{1}{3}\left(2^{b+c} + 2\cos\frac{(c - b + 2r)\pi}{3}\right)$$

Nyní už stačí každé řešení vynásobit 2^a, čímž přidáme prvky dělitelné třemi. □

4.4.2 Rozšíření pro všechny dělitele

Lemma 4.4.8 (Redukce sudých dělitelů)**.** Definujme celá čísla $\alpha \geq 0$ a $m \geq 1$. Nechť $s_0, \dots, s_{m-1} \in \mathbb{N}$. Označme $\mathcal{A}_m^r(s_0, \dots, s_{m-1})$ počet podmnožin S (kde v S je s_γ prvků γ modulo m) se součtem prvků r modulo m. Pak platí

$$\mathcal{A}^r_{2^\alpha m}(s_0, \dots, s_{2^\alpha m-1}) = \frac{1}{2^\alpha} \mathcal{A}^r_m \left(s^{(0)}, \dots, s^{(m-1)}\right),$$

kde píšeme $s^{(j)} = s_j + s_{j+m} + \dots + s_{j+(2^\alpha-1)m}$.

Důkaz. Stačí dokázat rovnost $\mathcal{A}^r_{2m}(s_0, \dots, s_{2m-1}) = \frac{1}{2} \mathcal{A}^r_m(s_0 + s_m, \dots, s_{m-1} + s_{2m-1})$, potom tvrzení vyplývá z indukce.

Vyjdeme z rovnosti 1.2.11, a to konkrétně pokud máme sudou (k-tou) primitivní odmocninu z jedné ξ, tak platí

$$g(\xi) = (1+\xi)(1+\xi^2)\dots(1+\xi^k) = 0.$$

Definujme nyní $\zeta = \cos(\pi/m) + i \sin(\pi/m)$ primitivní $2m$-tou primitivní odmocninu z jedné a také m-tou primitivní odmocninu z jedné $\omega = \cos(2\pi/m) + i\sin(2\pi/m)$. Platí tedy $\zeta^2 = \omega$. Z lemmatu 4.4.3 pišme

$$2m \cdot \mathcal{A}^r_{2m}(s_0, \dots, s_{2m-1}) = \sum_{k=1}^{2m} \zeta^{-rk} f(\zeta^k),$$

kde $f(\zeta^k) = \prod_{j=0}^{2m-1}(1+\zeta^{jk})^{s_j} = g(\zeta^k) \cdot \prod_{j=0}^{2m-1}(1+\zeta^{jk})^{s_j-1}$, jelikož předpokládáme, že $s_j > 0$. Pokud ζ^k je sudou primitivní odmocninou, tak $f(\zeta^k) = 0$. Speciálně když k je liché, tak jistě $f(\zeta^k) = 0$ čili

$$\sum_{k=1}^{2m} \zeta^{-rk} f(\zeta^k) = \sum_{k=1}^{m} \zeta^{-r(2k)} f(\zeta^{(2k)}) = \sum_{k=1}^{m} \omega^{-rk} f(\omega^k).$$

Platí ovšem $f(\omega^k) = \prod_{j=0}^{2m-1}(1+\omega^{jk})^{s_j} = \prod_{j=0}^{m-1}(1+\omega^{jk})^{s_j+s_{j+m}}$, takže

$$\sum_{k=1}^{m} \omega^{-rk} f(\omega^k) = m \cdot \mathcal{A}^r_m(s_0 + s_m, \dots, s_{m-1} + s_{2m-1}).$$

Po vydělení rovnosti $2m \cdot \mathcal{A}^r_{2m}(s_0, \dots, s_{2m-1}) = m \cdot \mathcal{A}^r_m(s_0 + s_m, \dots, s_{m-1} + s_{2m-1})$ číslem $2m$ jsme hotovi. □

Vzhledem k lemmatu 4.4.8 zjevně nezáleží na tom, zda v původní množině prvek dává zbytek r nebo $r + m/2$ modulo m, pokud je m sudé. Také nám to dává nadhled, že podmnožin se součtem r mod m je stejný počet jako se součtem $r + m/2$ mod m.

Poznámka. Pokud uvažujeme úlohu s dělitelem $3 \cdot 2^\alpha$, kde $\alpha \geq 0$, pak jsme schopni redukovat množinu a dělitel na číslo 3, kde už známe řešení.

Lemma 4.4.9 (Redukce soudělných prvků)**.** Nechť $m, r \in \mathbb{N}$ a $s_0, \dots, s_{m-1} \in \mathbb{N}_0$. Označme $\mathcal{A}_m^r(s_0, \dots, s_{m-1})$ počet podmnožin S (kde v S je s_γ prvků γ modulo m) se součtem prvků r modulo m. Předpokládejme, že každý prvek v S je dělitelný číslem $d \in \mathbb{N}$, kde $d > 1$, $d \mid m$. Pak platí

$$\mathcal{A}_m^r(s_0, \dots, s_{m-1}) = \begin{cases} 0, & \text{pokud } d \nmid r, \\ \mathcal{A}_{m/d}^{r/d}\left(s_0, s_d, s_{2d}, \dots, s^{m-d}\right), & \text{pokud } d \mid r. \end{cases}$$

Důkaz. Každá podmnožina má součet prvků dělitelný d, takže pokud $d \nmid r$, tak nevyhovuje žádná podmnožina. Předpokládejme dále, že $d \mid r$.

Je dána množina $S = \{a_1, \dots, a_n\}$ a definujme $S' = \{a_1/d, \dots, a_n/d\}$. Pro S vyhovuje podmnožina $\{a_1, \dots, a_n\} \subseteq S$ právě tehdy, když

$$a_1 + a_2 + \dots + a_n \equiv r \pmod{m},$$

každý prvek je dělitelný d, takže ekvivalentně vydělíme. Platí tak

$$a_1/d + a_2/d + \dots + a_n/d \equiv r/d \pmod{m/d},$$

což znamená, že podmnožina $\{a_1/d, \dots, a_n/d\} \subseteq S'$ vyhovuje (pro r/d modulo m/d). Jelikož jsme postupovali ekvivalentně, tak množině S vyhovuje stejný počet podmnožin jako množině S', což jsme chtěli dokázat. □

Lemma 4.4.10 (Kvadrát prvočísla)**.** Nechť $p > 2$ je prvočíslo a $s_1, \dots, s_{p^2-1} \in \mathbb{N}_0$. Pokud $\mathcal{A}_{p^2}^r(s_0, \dots, s_{p^2-1})$ značí počet podmnožin S (kde v S je s_γ prvků γ modulo p^2) se součtem prvků r modulo p^2, pak platí

$$\begin{aligned} \mathcal{A}_{p^2}^r(s_0, s_1 + 1, \dots, s_{p^2-1} + 1) = \mathcal{A}_{p^2}^r(s_0, \dots, s_{p^2-1}) + \frac{2^{p-1} - 1}{p} \mathcal{A}_p^r\left(s^{(0)}, \dots, s^{(p-1)}\right) \\ + 2^S \cdot \frac{2^{p^2-1} - 2^{p-1}}{p^2}, \end{aligned}$$

kde píšeme $s^{(j)} = s_j + s_{j+p} + \dots + s_{j+(p-1)p}$ a $S = s_0 + \dots s_{p^2-1}$.

Důkaz. Pro p^2-tou primitivní odmocninu z jedné ζ vzhledem k lemmatu 4.4.3 pišme

$$p^2 \cdot \mathcal{A}_{p^2}^r(s_0, s_1 + 1, \dots, s_{p^2-1} + 1) - 2^{S+p^2-1} = \sum_{k=1}^{p^2-1} \zeta^{-rk} \prod_{j=0}^{p^2-1} (1 + \zeta^{jk})^{s_j+1}.$$

Označme $g(\zeta^k) = \prod_{j=1}^{p^2-1}(1 + \zeta^{jk})$. Přitom uvažujeme $p^2 \nmid k$. Jelikož potom pro jediné hodnoty $k = \ell p$ platí $\gcd(k, p^2) = p \neq 1$, tak z věty 1.2.11 platí

$$g(\zeta^k) = \begin{cases} 2^{p-1}, & \text{pokud } k = \ell p, \\ 1, & \text{jinak.} \end{cases}$$

Platí tedy

$$\sum_{k=1}^{p^2-1} \zeta^{-rk} \prod_{j=0}^{p^2-1} (1+\zeta^{jk})^{s_j+1} = \sum_{k=1}^{p^2-1} \zeta^{-rk} g(\zeta^k) \prod_{j=0}^{p^2-1} (1+\zeta^{jk})^{s_j} =$$

$$= \sum_{k=1}^{p^2-1} \zeta^{-rk} \prod_{j=0}^{p^2-1} (1+\zeta^{jk})^{s_j} + (2^{p-1}-1) \sum_{\ell=1}^{p-1} \zeta^{-r(\ell p)} \prod_{j=0}^{p^2-1} (1+\zeta^{j(\ell p)})^{s_j}$$

První suma se rovná $p^2 \cdot \mathcal{A}^r_{p^2}(s_0, s_1, \ldots, s_{p^2-1}) - 2^S$. Pokud nyní definujeme $\omega = \zeta^p$ jako primitivní p-tou odmocninu, tak druhá suma se rovná

$$\sum_{\ell=1}^{p-1} \omega^{-r\ell} \prod_{j=0}^{p^2-1} (1+\omega^{j\ell})^{s_j} = \sum_{\ell=1}^{p-1} \omega^{-r\ell} \prod_{j=0}^{p-1} (1+\omega^{j\ell})^{s^{(j)}} = p\, \mathcal{A}^r_p \left(s^{(0)}, \ldots, s^{(p-1)}\right) - 2^S$$

Pokud označíme $A_1 = \mathcal{A}^r_{p^2}(s_0, s_1+1, \ldots, s_{p^2-1}+1)$, $\quad A_2 = \mathcal{A}^r_{p^2}(s_0, s_1, \ldots, s_{p^2-1})$ a $A_3 = \mathcal{A}^r_p \left(s^{(0)}, \ldots, s^{(p-1)}\right)$, tak platí

$$p^2 A_1 - 2^{S+p^2-1} = p^2 A_2 - 2^S + (2^{p-1}-1)(pA_3 - 2^S),$$

$$p^2 A_1 = p^2 A_2 + (2^{p-1}-1)(pA_3) + 2^{S+p^2-1} - 2^{S+p-1}.$$

Vydělíme celou rovnost p^2. Platí $A_1 = A_2 + \frac{2^{p-1}-1}{p} A_3 + 2^S \cdot \frac{2^{p^2-1}-2^{p-1}}{p^2}$, což jsme chtěli ukázat. □

Důsledek 4.4.11. Nechť $s_1, \ldots, s_8 \in \mathbb{N}_0$ a $r \in \mathbb{Z}_9$. Pokud $\mathcal{A}^r_m(s_0, \ldots, s_{m-1})$ značí počet podmnožin množiny s s_γ prvky γ modulo m, jejichž součet prvků je kongruentní r modulo m, pak platí

$$\mathcal{A}^r_9(s_0, s_1+1, \ldots, s_8+1) = \mathcal{A}^r_9(s_0, \ldots, s_8) + \mathcal{A}^r_3\left(s^{(0)}, s^{(1)}, s^{(2)}\right) + 7 \cdot 2^{S+2}.$$

kde píšeme $s^{(j)} = s_j + s_{j+3} + s_{j+6}$ a $S = s_0 + \ldots s_8$.

Důkaz. Platí po úpravě lemmatu 4.4.10 pro prvočíslo $p = 3$. □

Věta 4.4.12 (Výsledek pro prvočíslo)**.** *Definujme prvočíslo $p > 2$, čísla $s_1, \ldots, s_{p-1} \in \mathbb{N}_0$ a $r \in \mathbb{Z}_p$. Pokud $\mathcal{A}^r_p(s_0, \ldots, s_{p-1})$ značí počet podmnožin množiny s s_γ prvky γ modulo p, jejichž součet prvků je kongruentní r modulo p, pak platí*

$$\mathcal{A}^r_p(0, s_1, \ldots, s_{p-1}) = \sum_{\substack{r_2, \ldots, r_{p-1} \in \mathbb{Z}_p, \\ r_1 = r - 2r_2 - 3r_3 - \cdots - (p-1)r_{p-1}}} \chi^{r_1}_p(s_1) \cdot \chi^{r_2}_p(s_2) \cdots \chi^{r_{p-1}}_p(s_{p-1}),$$

kde $\chi^\rho_p(n) = \binom{n}{\rho} + \binom{n}{\rho+p} + \binom{n}{\rho+2p} + \ldots$

Důkaz. Pro prvočíslo p platí

$$\mathcal{A}_p^r(0, s_1, \ldots, s_{p-1}) = \frac{1}{p}\left(2^{|S|} - \sum_{k=0}^{p-1} d_k\right) + d_r,$$

kde čísla $d_0, \ldots, d_{p-1}$ splňují

$$d_0 + \zeta d_1 + \zeta^2 d_2 + \cdots + \zeta^{p-1} d_{p-1} = (1+\zeta^1)^{s_1} \cdots (1+\zeta^{p-1})^{s_{p-1}}. \tag{4.9}$$

Pokud nebudeme využívat rovnosti, že součet několika odmocnin z jedné se rovná nule, tak po roznásobení pravé strany rovnosti najdeme $2^{s_1} \cdots 2^{s_{p-1}} = 2^{|S|}$ členů. Nahlédnutím k levé straně rovnosti se toto číslo rovná součtu všech d_k, takže platí $d_0 + \cdots + d_{p-1} = 2^{|S|}$. Dosazením do první rovnosti je výsledek roven $\mathcal{A}_p^r(0, s_1, \ldots, s_{p-1}) = d_r$.

Roznásobíme každou závorku v součinu (4.9) pomocí binomické věty, čímž získáme součet kombinačních čísel, která jsou postupně násobená mocninami ζ. Pokud seskupíme každé p-té kombinační číslo, tak pro $j \in \{1, \ldots, p-1\}$ platí

$$(1+\zeta^j)^{s_j} = \chi_p^0(s_j) + \zeta^j\, \chi_p^1(s_j) + \cdots + \zeta^{(p-1)j}\, \chi_p^{p-1}(s_j).$$

Roznásobením součinu těchto čísel pro $j \in \{1, \ldots, p-1\}$ se d_r vzhledem k (4.9) rovná součtu takových čísel, že součin jejich mocnin ζ se rovná číslu ζ^r. Uvažujeme tedy všechna taková čísla $\chi_p^{r_1}(s_1) \cdot \chi_p^{r_2}(s_2) \cdots \chi_p^{r_{p-1}}(s_{p-1})$, že $r_1 + 2r_2 + 3r_3 + \cdots + (p-1)r_{p-1} \equiv r \pmod p$, pro libovolnou kombinaci $r_1, \ldots, r_{p-1} \in \{0, \ldots, p-1\}$. Vzhledem k tomu, že r_1 je libovolný prvek modulo p, tak existuje sčítanec pro kteroukoli $(p-2)$-tici čísel $(r_2, \ldots, r_{p-1}) \in (\mathbb{Z}_p)^{p-2}$, jelikož zvolíme r_1 jako $r_1 \equiv r - 2r_2 - 3r_3 - \cdots - (p-1)r_{p-1} \pmod p$. Pokud napíšeme výsledek formou sumy, tak získáme dokazovanou rovnost. □

Poznámka. Pro libovolné prvočíslo tedy dokážeme přímo spočítat řešení, ale zahrnuje to součet p^{p-2} čísel, z nichž každé je součtem každého p-tého kombinačního čísla.

4.4.3 Maticový tvar řešení pro dělitelnost pěti

Mějme čísla $s_0, \ldots, s_4$. Nejprve platí $\mathcal{A}_5^r(s_0, \ldots, s_4) = 2^{s_0}\, \mathcal{A}_5^r(0, s_1, \ldots, s_4)$. Umíme také eliminovat jedno z dalších čísel, přičemž ale nechejme všechny vstupy nezáporné. Například pokud platí $s_4 = \min\{s_1, \ldots, s_4\}$, pak zjednodušíme řešení následovně.

$$\mathcal{A}_5^r(0, s_1, \ldots, s_4) = \mathcal{A}_5^r(0, s_1 - s_4, s_2 - s_4, s_3 - s_4, 0) + \frac{1}{5}\left(2^{s_1+\cdots+s_4} - 2^{s_1+s_2+s_3-3s_4}\right).$$

Lemma 4.4.13 (Vlastní)**.** Jsou dána nezáporná celá čísla $s_0, \ldots, s_4$ a $r \in \{0, \ldots, 4\}$. V množině je celkem $s_0 + \cdots + s_4$ prvků, přičemž s_j prvků dává zbytek j po dělení pěti. Označme $\mathcal{A}_5^r(s_0, \ldots, s_4)$ počet podmnožin, jejichž součet prvků dává zbytek r po dělení pěti. Pro hodnoty $(s_0, \ldots, s_4) = (0, a, b, c, 0)$ platí rovnost

$$\mathcal{A}_5^r(0, a, b, c, 0) = \begin{pmatrix} \chi_5^0(b) & \ldots & \chi_5^4(b) \end{pmatrix} \begin{pmatrix} \chi_5^r(a) & \chi_5^{r+2}(a) & \ldots & \chi_5^{r+3}(a) \\ \chi_5^{r+3}(a) & \chi_5^r(a) & \ldots & \chi_5^{r+1}(a) \\ \chi_5^{r+1}(a) & \chi_5^{r+3}(a) & \ldots & \chi_5^{r+4}(a) \\ \chi_5^{r+4}(a) & \chi_5^{r+1}(a) & \ldots & \chi_5^{r+2}(a) \\ \chi_5^{r+2}(a) & \chi_5^{r+4}(a) & \ldots & \chi_5^r(a) \end{pmatrix} \begin{pmatrix} \chi_5^0(c) \\ \chi_5^1(c) \\ \chi_5^2(c) \\ \chi_5^3(c) \\ \chi_5^4(c) \end{pmatrix},$$

kde $\chi_5^\rho(n) = \binom{n}{\rho} + \binom{n}{\rho+5} + \binom{n}{\rho+10} + \dots$

Důkaz. Z věty 4.4.12 platí

$$\mathcal{A}_5^r(0,a,b,c,0) = \sum_{\substack{r_2,r_3,r_4\in\mathbb{Z}_5,\\ r_1=r-2r_2-3r_3-4r_4}} \chi_5^{r_1}(a)\cdot\chi_5^{r_2}(b)\cdot\chi_5^{r_3}(c)\cdot\chi_5^{r_4}(0).$$

Pokud $r_4 = 0$, pak $\chi_5^{r_4}(0) = \binom{0}{0} = 1$. Pro jiné r_4 jsou všechna příslušná kombinační čísla nulová, takže platí $\chi_5^{r_4}(0) = 0$, takže je hodnota součinu nulová, takže stačí v sumě uvažovat $r_4 = 0$. Dosadíme $r_1 = r - 2r_2 - 3r_3 - 4r_4 \equiv r + 3r_2 + 2r_3 \pmod 5$, takže platí

$$\mathcal{A}_5^r(0,a,b,c,0) = \sum_{r_2,r_3\in\mathbb{Z}_5} \chi_5^{r+3r_2+2r_3}(a)\cdot\chi_5^{r_2}(b)\cdot\chi_5^{r_3}(c).$$

Jelikož zde máme pouze dvě proměnné r_2, r_3, tak je možné využít násobení matic. Lze ověřit, že po vynásobení daných tří matic získáme sčítance tvaru $\chi_5^{r+3r_2+2r_3}(a)\cdot\chi_5^{r_2}(b)\cdot\chi_5^{r_3}(c)$, což jsme chtěli ukázat. □

Věta 4.4.14 (Vlastní)**.** *Jsou dána nezáporná celá čísla $s_0,\dots,s_4$ a $r\in\{0,\dots,4\}$. V množině je celkem $s_0+\dots+s_4$ prvků, přičemž s_j prvků dává zbytek j po dělení pěti. Označme $\mathcal{A}_5^r(s_0,\dots,s_4)$ počet podmnožin, jejichž součet prvků dává zbytek r po dělení pěti. Za předpokladu $s_4 = \min(s_1,\dots,s_4)$. Potom platí rovnost*

$$\mathcal{A}_5^r(s_0,\dots,s_4) = 2^{s_0}\cdot\begin{pmatrix}\Phi^0 & \dots & \Phi^4\end{pmatrix}\begin{pmatrix}\chi^r & \chi^{r+2} & \dots & \chi^{r+3}\\ \chi^{r+3} & \chi^r & \dots & \chi^{r+1}\\ \chi^{r+1} & \chi^{r+3} & \dots & \chi^{r+4}\\ \chi^{r+4} & \chi^{r+1} & \dots & \chi^{r+2}\\ \chi^{r+2} & \chi^{r+4} & \dots & \chi^r\end{pmatrix}\begin{pmatrix}\Psi^0\\ \Psi^1\\ \Psi^2\\ \Psi^3\\ \Psi^4\end{pmatrix} + \frac{1}{5}\left(2^S - 2^{S-4s_4}\right),$$

kde značíme $\chi^r = \chi_5^r(s_1-s_4)$, $\Phi^r = \chi_5^r(s_2-s_4)$ a $\Psi^r = \chi_5^r(s_3-s_4)$ a $S = s_0+\dots+s_4$.

Dále píšeme $\chi_5^\rho(n) = \binom{n}{\rho} + \binom{n}{\rho+5} + \binom{n}{\rho+10} + \dots$

Závěr

V této práci bylo shromážděno několik známých způsobů, jak využít odmocniny z jedné a hlavně byly aplikovány na značné zobecnění úloh.

Cílem této práce bylo představit odmocniny z jedné jako výhodný nástroj pro řešení kombinatorických problému a co nejvíce je zobecnit. Nakonec se jednalo o dláždění šachovnic, sčítání Fibonacciho čísel i kombinačních čísel a také pomocí nich počítat podmnožiny, jejichž součet prvků je dělitelný daným číslem. Zobecnit tyto úlohy se podařilo značně. Zmíněné úlohy jsou řešeny prostřednictvím nástrojů jako je zejména *Roots of Unity Filter* a generující funkce.

V rámci dláždění šachovnic tato práce přispěla zobecněním zejména problému s jedním prázdným políčkem kdekoli v šachovnici. Navíc se ukázalo, o kolik více je prostudované téma kompletního vyplnění šachovnice, a to i ve více než dvou rozměrech. Dále tato práce přispěla výpočtem vzorce pro součet každého n-tého Fibonacciho čísla zahrnující zaokrouhlení na nejbližší celé číslo. Kromě toho, součty kombinačních čísel byly využity pro určení počtů podmnožin se součtem prvků dělitelným určitým číslem. Obecné řešení bylo nalezeno pro libovolnou množinu celých čísel, zejména pro dělitele 3 a 5. Dále bylo ukázáno, že řešení pro prvočíselné dělitele větší než 3 sestává z mnoha sčítanců a nevychází kompaktně. Pro ostatní dělitele lze množinu čísel značně zjednodušit a přiblížit se obecnému řešení.

Úspěšně bylo demonstrováno využití odmocnin z jedné na všech daných typech úloh. Podařilo se zobecnit problém dláždění s prázdným políčkem v šachovnici. Podařilo se určit součet každého n-tého Fibonacciho čísla. Obecné řešení úlohy se součty podmnožin se velmi úspěšně spočítalo pro skupinu dělitelů. Pro ostatní dělitele se značně podařilo přiblížit k obecnému řešení. Další možné rozšíření této práce by mohlo spočívat

(i) v nalezení dalších odlišných typů úloh, které jsou elegantně řešitelné odmocninami z jedné a případně tyto úlohy zobecnit,

(ii) v navázání na problém dláždění šachovnic s více než jedním prázdným políčkem nebo s jiným zajímavým polyominem,

(iii) v pokračování zobecnění počítání podmnožin, což by mohlo zahrnovat nalezení dalších užitečných tvrzení, která by případně dokázala zobecnit řešení pro další dělitele či určitou skupinu množin,

(iv) ve výpočtu multisekcí jiných posloupností než Fibonacciho čísel.

Literatura

[1] Titu Andreescu and Gabriel Dospinescu. *Problems from the book.* XYZ Press, 2010.

[2] Nicholas G de Bruijn. Filling boxes with bricks. *The American Mathematical Monthly*, 76(1):37–40, January 1969.

[3] Zichao He, Zhuoxi Hou, and Yining Zhang. Proving combinatorial identities using complex numbers. *Highlights in Science, Engineering and Technology*, 47:1–8, May 2023.

[4] Jiří Herman, Radan Kučera, and Jaromír Šimša. *Metody řešení matematických úloh I.* Masarykova univerzita, Brno, 3. vyd. edition, 2011.

[5] Jakub Juránek. Užití komplexních čísel v kombinatorice [online], 2014 [cit. 2025-02-14]. SUPERVISOR : Jaromír Šimša.

[6] Donald Ervin Knuth. *The art of computer programming*, volume 3. Pearson Education, 1997.

[7] Oscar Levin. *Discrete mathematics: An open introduction.* University of Northern Colorado, 2019.

[8] 73. ročník matematické olympiády (2023/2024), zadání úloh domácího kola. Dostupné z: https://www.matematickaolympiada.cz/media/3563277/abc73.pdf.

[9] Grant Sanderson. Olympiad level counting (generating functions) [online], 2022.

[10] Stan Wagon. Fourteen proofs of a result about tiling a rectangle. *The American Mathematical Monthly*, 94(7):601–617, 1987.