MASARYKOVA UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA
ÚSTAV MATEMATIKY A STATISTIKY

Užití komplexních čísel v kombinatorice

Bakalářská práce

Jakub Juránek

Vedoucí práce: doc. RNDr. Jaromír Šimša, CSc. **Brno 2014**

Obsah

Úvod

Cílem této bakalářské práce je ukázat, že komplexní čísla se dají v kombinatorice užít nejen k určování konečných součtů tvořených kombinačními čísly. Tato mylná představa pramení z faktu, že na středních školách se jiné aplikace neprobírají. V této práci na několika příkladech názorně ukážeme, jak se dají využít při určování počtu prvků konkrétní množiny patřících do jisté zbytkové třídy a též – poněkud nečekaně – v kombinatorické geometrii, konkrétně při řešení úloh o pokrývání šachovnic.

Že mohou být zde vyložené aplikace užitečné i středoškolským studentům potvrzuje fakt, že některé z uvedených příkladů pocházejí z různých matematických seminářů a olympiád. Celá práce je tak cílena právě na středoškolského studenta a předpokládá u čtenáře pouze znalost středoškolské matematiky a zájem o dané téma. Může být tedy používána například na gymnáziích při přípravě na matematickou olympiádu, ovšem díky méně tradičním aplikacím není nezajímavá ani pro studenty matematiky na vysokých školách.

Práce je rozdělena do dvou kapitol, první teoretické a druhé praktické. První se věnuje teoretickým poznatkům o komplexních číslech, zbytkových třídách a je zakončena několika speciálními praktickými tvrzeními. Nejprve zavedeme komplexní čísla jako uspořádané dvojice reálných čísel a některé s nimi spojené pojmy, včetně jejich algebraického tvaru, a uvedeme a dokážeme jejich základní vlastnosti. V následujících dvou částech zavedeme goniometrický tvar komplexního čísla a popíšeme další vlastnosti, přičemž se výkladem zaměříme především na komplexní odmocniny z jedné. Poté se podíváme na zbytkové třídy a jejich souvislost s odmocninami z jedné a nakonec dokážeme několik speciálnějších tvrzení, která budeme potřebovat ve druhé kapitole. První kapitola je zpracována především dle [8] a [9].

Druhá kapitola pak podává praktický výklad o užití komplexních čísel v kombinatorice na několika konkrétních příkladech. Nejprve popíšeme právě ono známé určování různých konečných součtů tvořených kombinačními čísly, vycházející z faktu, že libovolné komplexní číslo můžeme vyjádřit jednak v algebraickém tvaru a umocnit ho užitím binomické věty, jednak v goniometrickém tvaru a umocnit užitím Moivreovy věty. Poté již přejdeme k tomu méně známému, totiž k určování počtu prvků konkrétní množiny patřících do jisté zbytkové třídy s využitím komplexních odmocnin z jedné. Vrcholem celé práce je pak poslední část věnovaná oblasti kombinatorické geometrie, a to problematice pokrývání šachovnic obecných rozměrů soustavami šachovnic menších zadaných rozměrů. Uvedené příklady vycházejí v první části z [5], ve druhé a třetí pak z [1].

Práce je sázena programem LaTeX.

Kapitola 1

Teoretický základ

Před tím, než ve druhé kapitole vyložíme některá užití komplexních čísel v kombinatorice, podívejme se na komplexní čísla a jejich vlastnosti trochu obecněji. V první části této kapitoly zavedeme komplexní čísla jako uspořádané dvojice reálných čísel a některé s nimi spojené pojmy, včetně jejich algebraického tvaru, a uvedeme a dokážeme jejich základní vlastnosti. V dalších dvou částech zavedeme goniometrický tvar komplexního čísla a popíšeme další vlastnosti, přičemž se výkladem zaměříme především na komplexní odmocniny z jedné. Poté se podíváme na zbytkové třídy a jejich souvislost s odmocninami z jedné a nakonec dokážeme několik speciálnějších tvrzení, která budeme potřebovat ve druhé kapitole. Problematika komplexních čísel je zpracována dle [8].

1.1 Komplexní číslo a jeho algebraický tvar

Definice 1.1. *Komplexním číslem* z rozumíme libovolnou uspořádanou dvojici reálných čísel, tedy $z := (x,y)$, kde $x,y \in \mathbb{R}$.
Množinu všech komplexních čísel značíme $\mathbb{C} := \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.
Reálnou částí komplexního čísla $z = (x,y)$ rozumíme číslo $\mathrm{Re}\, z := x \in \mathbb{R}$.
Imaginární částí komplexního čísla $z = (x,y)$ rozumíme číslo $\mathrm{Im}\, z := y \in \mathbb{R}$.
Komplexní číslo, které má nenulovou imaginární část, nazýváme *číslem imaginárním*.
Imaginární číslo, které má nulovou reálnou část, nazýváme *číslem ryze imaginárním*.

Definice 1.2. Nechť $z_1 = (x_1,y_1), z_2 = (x_2,y_2) \in \mathbb{C}$.
Řekneme, že čísla z_1, z_2 se rovnají, píšeme $z_1 = z_2$, jestliže $x_1 = x_2$ a současně $y_1 = y_2$.

Definice 1.3. Nechť $z_1 = (x_1,y_1), z_2 = (x_2,y_2) \in \mathbb{C}$.
Součet čísel z_1, z_2 značíme $z_1 + z_2$ a definujeme předpisem $z_1 + z_2 := (x_1 + x_2, y_1 + y_2)$.
Součin čísel z_1 , z_2 značíme $z_1 \cdot z_2$ a definujeme předpisem $z_1 \cdot z_2 := (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot \cdot y_2 + x_2 \cdot y_1)$.

Definice 1.4. Nechť $z = (x,y) \in \mathbb{C}$.
Číslo $-z := (-x,-y) \in \mathbb{C}$ nazveme *číslem opačným k číslu* z.

Definice 1.5. Nechť $z = (x,y) \in \mathbb{C}, z \neq (0,0)$.
Číslo $z^{-1} := \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2} \right) \in \mathbb{C}$ nazveme *převráceným číslem k číslu* z.

Věta 1.6. Pro libovolná $z, z_1, z_2, z_3 \in \mathbb{C}$ platí:

1. $z_1 + z_2 = z_2 + z_1$;
2. $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$;
3. $z + (0,0) = z$;
4. $z + (-z) = (0,0)$;
5. $z_1 \cdot z_2 = z_2 \cdot z_1$;
6. $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$;
7. $z \cdot (1,0) = z$;
8. $z \cdot z^{-1} = (1,0)$, je-li $z \neq (0,0)$;
9. $(z_1 + z_2) \cdot z_3 = z_1 \cdot z_3 + z_2 \cdot z_3$.

Důkaz. Nechť $z = (x,y), z_1 = (x_1,y_1), z_2 = (x_2,y_2), z_3 = (x_3,y_3)$.
Důkaz provedeme s využitím známých vlastností tělesa reálných čísel. U každého bodu uvedeme konkrétní využívanou vlastnost a konkrétní místo jejího použití označíme $\triangleq$.

1. Z komutativity sčítání reálných čísel plyne

$$\begin{aligned} z_1 + z_2 = (x_1,y_1) + (x_2,y_2) = (x_1 + x_2, y_1 + y_2) &\triangleq (x_2 + x_1, y_2 + y_1) = \\ &= (x_2,y_2) + (x_1,y_1) = z_2 + z_1. \end{aligned}$$

2. Z asociativity sčítání reálných čísel plyne

$$\begin{aligned} (z_1 + z_2) + z_3 &= \big((x_1,y_1) + (x_2,y_2)\big) + (x_3,y_3) = (x_1 + x_2, y_1 + y_2) + (x_3,y_3) = \\ &= \big((x_1 + x_2) + x_3, (y_1 + y_2) + y_3\big) \triangleq \big(x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)\big) = \\ &= (x_1,y_1) + (x_2 + x_3, y_2 + y_3) = (x_1,y_1) + \big((x_2,y_2) + (x_3,y_3)\big) = \\ &= z_1 + (z_2 + z_3). \end{aligned}$$

3. Z toho, že číslo 0 je neutrálním prvkem sčítání reálných čísel, plyne

$$z + (0,0) = (x,y) + (0,0) = (x + 0, y + 0) \triangleq (x,y) = z.$$

4. Z toho, že inverzním prvkem libovolného $a \in \mathbb{R}$ vzhledem k sčítání je číslo $-a \in \mathbb{R}$, plyne

$$z + (-z) = (x,y) + (-x,-y) = \big(x + (-x), y + (-y)\big) \triangleq (0,0).$$

5. Z komutativity sčítání a násobení reálných čísel plyne

$$\begin{aligned} z_1 \cdot z_2 = (x_1,y_1) \cdot (x_2,y_2) = (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1) &\triangleq \\ \triangleq (x_2 \cdot x_1 - y_2 \cdot y_1, x_2 \cdot y_1 + x_1 \cdot y_2) = (x_2,y_2) \cdot (x_1,y_1) &= z_2 \cdot z_1. \end{aligned}$$

6. Z komutativity sčítání a násobení reálných čísel a platnosti distributivního zákona plyne

$$\begin{aligned}(z_1\cdot z_2)\cdot z_3 &= \big((x_1,y_1)\cdot(x_2,y_2)\big)\cdot(x_3,y_3) = \\ &= (x_1\cdot x_2-y_1\cdot y_2, x_1\cdot y_2+x_2\cdot y_1)\cdot(x_3,y_3) = \\ &= \big((x_1\cdot x_2-y_1\cdot y_2)\cdot x_3-(x_1\cdot y_2+x_2\cdot y_1)\cdot y_3, \\ &\qquad (x_1\cdot x_2-y_1\cdot y_2)\cdot y_3+x_3\cdot(x_1\cdot y_2+x_2\cdot y_1)\big) \triangleq \\ &\triangleq \big(x_1\cdot(x_2\cdot x_3-y_2\cdot y_3)-y_1\cdot(x_2\cdot y_3+x_3\cdot y_2), \\ &\qquad x_1\cdot(x_2\cdot y_3+x_3\cdot y_2)+(x_2\cdot x_3-y_2\cdot y_3)\cdot y_1\big) = \\ &= (x_1,y_1)\cdot(x_2\cdot x_3-y_2\cdot y_3, x_2\cdot y_3+x_3\cdot y_2) = \\ &= (x_1,y_1)\cdot\big((x_2,y_2)\cdot(x_3,y_3)\big) = z_1\cdot(z_2\cdot z_3).\end{aligned}$$

7. Z toho, že číslo 1 je neutrálním prvkem násobení reálných čísel, a vlastnosti reálných čísel, že pro libovolné $a\in\mathbb{R}$ platí $a\cdot 0=0\cdot a=0$, plyne

$$z\cdot(1,0)=(x,y)\cdot(1,0)=(x\cdot 1-y\cdot 0, x\cdot 0+1\cdot y)\triangleq(x,y)=z.$$

8. Z toho, že inverzním prvkem libovolného $a\in\mathbb{R}, a\neq 0$, vzhledem k násobení je číslo $\frac{1}{a}\in\mathbb{R}$, při $z_1\neq(0,0)$ plyne

$$z\cdot z^{-1}=(x,y)\cdot\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)=\left(\frac{x^2+y^2}{x^2+y^2},\frac{-x\cdot y+x\cdot y}{x^2+y^2}\right)\triangleq(1,0).$$

9. Z komutativity a asociativity sčítání reálných čísel a platnosti distributivního zákona plyne

$$\begin{aligned}(z_1+z_2)\cdot z_3 &= \big((x_1,y_1)+(x_2,y_2)\big)\cdot(x_3,y_3) = \big(x_1+x_2,y_1+y_2\big)\cdot(x_3,y_3) = \\ &= \big((x_1+x_2)\cdot x_3-(y_1+y_2)\cdot y_3,(x_1+x_2)\cdot y_3+x_3\cdot(y_1+y_2)\big)\triangleq \\ &\triangleq \big((x_1\cdot x_3-y_1\cdot y_3)+(x_2\cdot x_3-y_2\cdot y_3), \\ &\qquad (x_1\cdot y_3+x_3\cdot y_1)+(x_2\cdot y_3+x_3\cdot y_2)\big) = \\ &= (x_1\cdot x_3-y_1\cdot y_3,x_1\cdot y_3+x_3\cdot y_1)+(x_2\cdot x_3-y_2\cdot y_3,x_2\cdot y_3+x_3\cdot y_2) = \\ &= (x_1,y_1)\cdot(x_3,y_3)+(x_2,y_2)\cdot(x_3,y_3) = z_1\cdot z_3+z_2\cdot z_3.\end{aligned}$$

□

Poznámka 1.7. První vlastnost z předchozí věty nám říká, že sčítání komplexních čísel je komutativní, a druhá, že je i asociativní. Třetí pak, že neutrálním prvkem sčítání komplexních čísel je číslo $(0,0)$, a čtvrtá, že opačné číslo $-z$ je inverzním prvkem k z vzhledem ke sčítání. Celkem tedy množina komplexních čísel se sčítáním tvoří komutativní grupu.
Pátá vlastnost nám říká, že násobení komplexních čísel je komutativní, a šestá, že je i asociativní. Sedmá pak, že neutrálním prvkem násobení komplexních čísel je číslo $(1,0)$, a osmá, že převrácené číslo z^{-1} je inverzním prvkem k $z\neq(0,0)$ vzhledem k násobení. Celkem tedy množina nenulových komplexních čísel $\mathbb{C}\setminus\{(0,0)\}$ s násobením tvoří též komutativní grupu.
To vše spolu s poslední vlastností, která nám říká, že komplexní čísla se sčítáním a násobením splňují distributivní zákon, znamená, že celkově komplexní čísla se sčítáním a násobením tvoří komutativní těleso.

Poznámka 1.8. Ztotožníme-li reálné číslo a s komplexním číslem $(a,0)$, dostaneme izomorfismus mezi tělesem $\mathbb{R}$ a podtělesem $\mathbb{R}\times\{0\} = \{(a,0) \mid a \in \mathbb{R}\}$ tělesa $\mathbb{C}$. Méně formálně lze psát $\mathbb{R} \subset \mathbb{C}$.
Ověřme, že $\mathbb{R}\times\{0\}$ je skutečně podtěleso $\mathbb{C}$:
pro libovolná reálná čísla $z_1 = (a,0), z_2 = (b,0) \in \mathbb{R}\times\{0\}$ platí:

1. $z_1 + z_2 = (a,0)\cdot(b,0) = (a+b,0) \in \mathbb{R}\times\{0\}$;
2. $z_1 \cdot z_2 = (a,0)\cdot(b,0) = (a\cdot b - 0\cdot 0, a\cdot 0 + a\cdot 0) = (a\cdot b,0) \in \mathbb{R}\times\{0\}$;
3. $-z_1 = (-a,0) \in \mathbb{R}\times\{0\}$;
4. $z_1 \neq (0,0)$: $z_1^{-1} = \left(\frac{a}{a^2+0^2}, \frac{-0}{a^2+0^2}\right) = \left(\frac{1}{a},0\right) \in \mathbb{R}\times\{0\}$;
5. $0 = (0,0) \in \mathbb{R}\times\{0\}$;
6. $1 = (1,0) \in \mathbb{R}\times\{0\}$. □

Definice 1.9. Nechť $n \in \mathbb{Z}$.
Pak *n-tou mocninou komplexního čísla z* rozumíme komplexní číslo z^n definované předpisem

$$z^n := \begin{cases} \underbrace{z\cdot z\cdot \ldots \cdot z}_{n} & \text{pro } n \in \mathbb{N}; \\ (1,0) & \text{pro } n = 0, z \neq (0,0); \\ \left(z^{-1}\right)^{-n} & \text{pro } n \in \mathbb{Z}^-, z \neq (0,0). \end{cases}$$

Poznámka 1.10. Z asociativity násobení komplexních čísel pro $z \in \mathbb{C}, z \neq (0,0), n \in \mathbb{N}$ libovolné, platí

$$z^{-n} = \left(z^{-1}\right)^n = (z^n)^{-1}.$$

Z komutativity a asociativity násobení komplexních čísel pro libovolná celá čísla m,n a libovolná komplexní čísla z, z_1, z_2, nenulová pokud jsou umocňována na nekladný exponent, platí:

$$z^m \cdot z^n = z^{m+n}, \quad (z_1\cdot z_2)^m = z_1^m \cdot z_2^m, \quad (z^m)^n = z^{mn}.$$

Poznámka 1.11. Pro dvě komplexní čísla též můžeme formálně definovat i jejich rozdíl a podíl.
Nechť $z_1 = (x_1,y_1), z_2 = (x_2,y_2) \in \mathbb{C}$.
Rozdíl čísel z_1, z_2 značíme $z_1 - z_2$ a definujeme předpisem $z_1 - z_2 := z_1 + (-z_2)$.
Podíl čísel z_1, z_2, kde $z_2 \neq (0,0)$, značíme $\frac{z_1}{z_2}$ a definujeme předpisem $\frac{z_1}{z_2} := z_1 \cdot z_2^{-1}$.

Věta 1.12. Nechť $z_1 = (x_1,y_1), z_2 = (x_2,y_2) \in \mathbb{C}$.
Pak platí

$$z_1 - z_2 = (x_1 - x_2, y_1 - y_2). \tag{1.1}$$

Je-li navíc $z_2 \neq (0,0)$, pak platí

$$\frac{z_1}{z_2} = \left(\frac{x_1x_2 + y_1y_2}{x_2^2 + y_2^2}, \frac{x_2y_1 - x_1y_2}{x_2^2 + y_2^2}\right). \tag{1.2}$$

Důkaz. Důkaz provedeme pouhým rozepsáním z definice.

$$z_1 - z_2 = z_1 + (-z_2) = (x_1,y_1) + (-x_2,-y_2) = (x_1 - x_2, y_1 - y_2)$$

$$\frac{z_1}{z_2} = z_1 \cdot z_2^{-1} = (x_1,y_1)\left(\frac{x_2}{x_2^2+y_2^2}, \frac{-y_2}{x_2^2+y_2^2}\right) = \left(\frac{x_1x_2+y_1y_2}{x_2^2+y_2^2}, \frac{x_2y_1-x_1y_2}{x_2^2+y_2^2}\right)$$

□

Poznámka 1.13. Protože počítání s komplexními čísly jako uspořádanými dvojicemi reálných čísel je poněkud nepraktické, využíváme rovnosti

$$(a,0)+(b,0)\cdot(0,1) = (a,0)+(b\cdot 0-0\cdot 1, b\cdot 1+0\cdot 0) = (a,0)+(0,b) = (a,b),$$

která nám při výše zmíněném ztotožnění reálných čísel $a = (a,0)$ a označení $\mathrm{i} := (0,1)$ dává možnost zápisu komplexního čísla $z = (a,b)$ ve tvaru

$$z = (a,b) = a + b\mathrm{i} = \mathrm{Re}\, z + \mathrm{i}\,\mathrm{Im}\, z.$$

Definice 1.14. Nechť $z \in \mathbb{C}, z = (x,y)$.
Zápis čísla z ve tvaru $z = x + yi$, resp. ve tvaru $z = \mathrm{Re}\, z + \mathrm{i}\,\mathrm{Im}\, z$, nazýváme *algebraickým tvarem komplexního čísla z*.
Číslo $\mathrm{i} := (0,1)$ nazýváme *imaginární jednotkou*.

Poznámka 1.15. Komplexní čísla v algebraickém tvaru můžeme sčítat a násobit jako dvojčleny s proměnnou i splňující rovnost $\mathrm{i}^2 = (0,1)\cdot(0,1) = (0\cdot 0-1\cdot 1, 0\cdot 1+0\cdot 1) = $
$= (-1,0) = -1$. Ověříme to snadno rozepsáním.
Nechť $z_1 = (x_1,y_1), z_2 = (x_2,y_2) \in \mathbb{C}$. Pak

$$\begin{aligned} z_1+z_2 &= (x_1+y_1\mathrm{i})+(x_2+y_2\mathrm{i}) = (x_1+x_2)+(y_1+y_2)\mathrm{i} = (x_1+x_2, y_1+y_2); \\ z_1\cdot z_2 &= (x_1+y_1\mathrm{i})\cdot(x_2+y_2\mathrm{i}) = x_1x_2+x_1y_2\mathrm{i}+x_2y_1\mathrm{i}+y_1y_2\mathrm{i}^2 = \\ &= (x_1x_2-y_1y_2)+(x_1y_2+x_2y_1)\mathrm{i} = (x_1x_2-y_1y_2, x_1y_2+x_2y_1). \end{aligned}$$

Opačné číslo k číslu $z = x+y\mathrm{i} \in \mathbb{C}$ v algebraickém tvaru je $-z = -x-y\mathrm{i}$. Můžeme to psát i přímo jako vynásobení -1, tj. $-z = -(x+y\mathrm{i})$ a rozdíl psát jako běžný rozdíl dvojčlenů. Že je splněno zavedení rozdílu v Poznámce 1.11 a Větě 1.12 opět ověříme rozepsáním.
Nechť $z_1 = (x_1,y_1), z_2 = (x_2,y_2) \in \mathbb{C}$. Pak

$$\begin{aligned} z_1-z_2 &= (x_1+y_1\mathrm{i})-(x_2+y_2\mathrm{i}) = (x_1+y_1\mathrm{i})+(-x_2-y_2\mathrm{i}) = (x_1-x_2)+(y_1-y_2)\mathrm{i} = \\ &= (x_1-x_2, y_1-y_2). \end{aligned}$$

Algebraický tvar se dá s velkou výhodou využít k výpočtu podílu dvou komplexních čísel, neboť není potřeba si pamatovat složitý vzorec a stačí provést běžné rozšíření zlomku, o čemž se nyní přesvědčíme.
Nechť $z_1 = (x_1,y_1), z_2 = (x_2,y_2) \in \mathbb{C}, z_2 \neq (0,0)$. Pak

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{x_1+y_1\mathrm{i}}{x_2+y_2\mathrm{i}}\cdot\frac{x_2-y_2\mathrm{i}}{x_2-y_2\mathrm{i}} = \frac{x_1x_2-x_1y_2\mathrm{i}+x_2y_1\mathrm{i}-y_1y_2\mathrm{i}^2}{x_2^2-x_2y_2\mathrm{i}+x_2y_2\mathrm{i}-y_2^2\mathrm{i}^2} = \\ &= \frac{(x_1x_2+y_1y_2)+(x_2y_1-x_1y_2)\mathrm{i}}{x_2^2+y_2^2} = \left(\frac{x_1x_2+y_1y_2}{x_2^2+y_2^2}, \frac{x_2y_1-x_1y_2}{x_2^2+y_2^2}\right). \end{aligned}$$

Proto ani není nutné si pamatovat vzorec pro převrácené číslo z^{-1} k číslu $z = (x,y) \neq$
$\neq (0,0)$, neboť ho můžeme určit z faktu, že číslo $(1,0) = 1$ je neutrálním prvkem vzhledem k násobení, díky čemuž lze psát $z^{-1} = 1\cdot z^{-1} = \frac{1}{z}$. Dostáváme tak

$$z^{-1} = \frac{1}{z} = \frac{1}{x+y\mathrm{i}}\cdot\frac{x-y\mathrm{i}}{x-y\mathrm{i}} = \frac{x-y\mathrm{i}}{x^2-xy\mathrm{i}+xy\mathrm{i}-y^2\mathrm{i}^2} = \frac{x-y\mathrm{i}}{x^2+y^2} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right).$$

Definice 1.16. Nechť $z = (x, y) \in \mathbb{C}$.
Absolutní hodnotu komplexního čísla z značíme $|z|$ a rozumíme jí nezáporné reálné číslo definované předpisem $|z| := \sqrt{x^2 + y^2}$.

Definice 1.17. *Komplexní jednotkou* rozumíme každé takové komplexní číslo, jehož absolutní hodnota je rovna jedné.

Definice 1.18. Nechť $z = (x, y) \in \mathbb{C}$.
Číslo $\overline{z} := (x, -y)$ nazýváme *číslem komplexně sdruženým s číslem* z.

Věta 1.19. Pro libovolná komplexní čísla $z = x + y\mathrm{i}, z_1 = x_1 + y_1\mathrm{i}$, $z_2 = x_2 + y_2\mathrm{i}$ a libovolné celé číslo n platí:

1. $\overline{(\overline{z})} = z$;
2. $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$;
3. $z + \overline{z} = 2x$;
4. $z \cdot \overline{z} = |z|^2$;
5. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$;
6. $\overline{-z} = -\overline{z}$
7. $\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2}$;
8. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$;
9. $\overline{z^{-1}} = \overline{z}^{-1}$;
10. $\overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}$;
11. $\overline{z^n} = \overline{z}^n$, je-li $z \neq 0$.

Důkaz. Důkaz jednotlivých bodů provedeme přímým rozepsáním, s případným využitím předchozích bodů, pouze poslední bod dokážeme matematickou indukcí. Pro lepší přehlednost využijeme zápisy komplexních čísel v algebraickém tvaru namísto zápisů uspořádanými dvojicemi.

1. $\overline{(\overline{z})} = \overline{\overline{(x + y\mathrm{i})}} = \overline{x - y\mathrm{i}} = x + y\mathrm{i} = z$
2. $z = \overline{z} \Leftrightarrow x + y\mathrm{i} = x - y\mathrm{i} \Leftrightarrow y = 0 \Leftrightarrow z \in \mathbb{R}$
3. $z + \overline{z} = (x + y\mathrm{i}) + (x - y\mathrm{i}) = 2x$
4. $z \cdot \overline{z} = (x + yi) \cdot (x - yi) = x^2 - xy\mathrm{i} + xy\mathrm{i} - y^2 i^2 = x^2 + y^2 = |z|^2$
5. $\overline{z_1 + z_2} = \overline{(x_1 + y_1\mathrm{i}) + (x_2 + y_2\mathrm{i})} = \overline{(x_1 + x_2) + (y_1 + y_2)\mathrm{i}} =$
   $= (x_1 + x_2) - (y_1 + y_2)\mathrm{i} = (x_1 - y_1\mathrm{i}) + (x_2 - y_2\mathrm{i}) = \overline{z_1} + \overline{z_2}$
6. $\overline{-z} = \overline{-(x + y\mathrm{i})} = \overline{-x - y\mathrm{i}} = -x + y\mathrm{i} = -(x - y\mathrm{i}) = -\overline{z}$

7. $\overline{z_1 - z_2} = \overline{z_1 + (-z_2)} \overset{bod\ 5}{=} \overline{z_1} + \overline{-z_2} \overset{bod\ 6}{=} \overline{z_1} + (-\overline{z_2}) = \overline{z_1} - \overline{z_2}$

8. $\overline{z_1 \cdot z_2} = \overline{(x_1 + y_1\mathrm{i}) \cdot (x_2 + y_2\mathrm{i})} = \overline{x_1x_2 + x_1y_2\mathrm{i} + x_2y_1\mathrm{i} + y_1y_2\mathrm{i}^2} =$
$= \overline{(x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)\mathrm{i}} = (x_1x_2 - y_1y_2) - (x_1y_2 + x_2y_1)\mathrm{i} =$
$= (x_1 - y_1\mathrm{i}) \cdot (x_2 - y_2\mathrm{i}) = \overline{z_1} \cdot \overline{z_2}$

9. $$\overline{z^{-1}} = \overline{\left(\frac{1}{z}\right)} = \overline{\left(\frac{\overline{z}}{z \cdot \overline{z}}\right)} \overset{bod\ 4}{=} \overline{\left(\frac{\overline{z}}{|z|^2}\right)} \overset{bod\ 1}{=} \frac{z}{|z|^2} \overset{bod\ 4}{=} \frac{z}{z \cdot \overline{z}} = \frac{1}{\overline{z}} = \overline{z}^{-1}$$

10. $$\overline{\left(\frac{z_1}{z_2}\right)} = \overline{z_1 \cdot z_2^{-1}} \overset{bod\ 8}{=} \overline{z_1} \cdot \overline{z_2^{-1}} \overset{bod\ 9}{=} \overline{z_1} \cdot \overline{z_2}^{-1} = \frac{\overline{z_1}}{\overline{z_2}}$$

11. Důkaz rozdělíme na tři části podle signatury n.

    (a) Pro $n = 0$ je tvrzení $\overline{z^0} = \overline{1} \overset{bod\ 2}{=} 1 = \overline{z}^0$ zřejmé.

    (b) Pro $n \in \mathbb{N}$ důkaz provedeme matematickou indukcí. Pro $n = 1$ je tvrzení $\overline{z^1} = \overline{z} = \overline{z}^1$ zřejmé. Dále budeme předpokládat, že tvrzení platí pro $1, 2, \ldots, n$ a ukážeme, že platí i pro $n + 1$.

    $$\overline{z^{n+1}} = \overline{z^n \cdot z} \overset{bod\ 8}{=} \overline{z^n} \cdot \overline{z} \overset{IP}{=} \overline{z}^n \cdot \overline{z} = \overline{z}^{n+1}$$

    (c) Pro $n \in \mathbb{Z}^-$ dostaneme rozepsáním

    $$\overline{z^n} = \overline{(z^{-1})^{-n}} \overset{bod\ 11b}{=} \left(\overline{z^{-1}}\right)^{-n} \overset{bod\ 9}{=} (\overline{z}^{-1})^{-n} = \overline{z}^n.$$

□

Věta 1.20. Pro libovolná komplexní čísla $z = x + y\mathrm{i}, z_1 = x_1 + y_1\mathrm{i}, z_2 = x_2 + y_2\mathrm{i}$ a libovolné celé číslo n platí:

1. $|z| \geq 0$, přičemž $|z| = 0 \Leftrightarrow z = 0$;
2. $|z| = |-z| = |\overline{z}| = |\overline{-z}|$;
3. $|z^{-1}| = \frac{1}{|z|}$, je-li $z \neq 0$;
4. $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$;
5. $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$, je-li $z_2 \neq 0$;
6. $|z^n| = |z|^n$, je-li $z \neq 0$;
7. $|\mathrm{Re}\, z| \leq |z| \ \wedge\ |\mathrm{Im}\, z| \leq |z|$;
8. $|z_1| - |z_2| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|$.

Důkaz.

1. Plyne z definice $|z| = \sqrt{x^2+y^2}$, neboť odmocnina z nezáporného čísla, kterým kvadrát i součet kvadrátů jsou, je číslo nezáporné, přičemž se rovná nule právě tehdy, když je číslo pod odmocninou rovno nule, což nastává právě tehdy, když $x = 0$ a současně $y = 0$, tedy $z = 0$.

2. Z faktu, že pro reálná čísla platí $a^2 = (-a)^2$, postupně dostáváme

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

3.

$$\begin{aligned}|z^{-1}| = \left|\frac{1}{z}\right| = \left|\frac{1}{x+y\mathrm{i}}\cdot\frac{x-y\mathrm{i}}{x-y\mathrm{i}}\right| = \left|\frac{x-y\mathrm{i}}{x^2+y^2}\right| = \sqrt{\left(\frac{x}{x^2+y^2}\right)^2+\left(\frac{-y}{x^2+y^2}\right)^2} = \\ = \frac{\sqrt{x^2+y^2}}{x^2+y^2} = \frac{1}{\sqrt{x^2+y^2}} = \frac{1}{|z|}\end{aligned}$$

4.

$$\begin{aligned}|z_1\cdot z_2| = \left|(x_1x_2-y_1y_2)+(x_1y_2+x_2y_1)\mathrm{i}\right| = \sqrt{(x_1x_2-y_1y_2)^2+(x_1y_2+x_2y_1)^2} = \\ = \sqrt{x_1^2x_2^2-2x_1x_2y_1y_2+y_1^2y_2^2+x_1^2y_2^2+2x_1x_2y_1y_2+x_2^2y_1^2} = \\ = \sqrt{x_1^2x_2^2+y_1^2y_2^2+x_1^2y_2^2+x_2^2y_1^2} = \sqrt{x_1^2(x_2^2+y_2^2)+y_1^2(x_2^2+y_2^2)} = \\ = \sqrt{(x_1^2+y_1^2)\cdot(x_2^2+y_2^2)} = \sqrt{x_1^2+y_1^2}\cdot\sqrt{x_2^2+y_2^2} = |z_1|\cdot|z_2|\end{aligned}$$

5.

$$\left|\frac{z_1}{z_2}\right| = \left|z_1\cdot z_2^{-1}\right| \overset{bod\ 4}{=} \left|z_1\right|\cdot\left|z_2^{-1}\right| \overset{bod\ 3}{=} \frac{|z_1|}{|z_2|}$$

6. Důkaz rozdělíme na tři části podle signatury n.

   (a) Pro $n = 0$ je tvrzení $|z^0| = |1| = 1 = |z|^0$ zřejmé.

   (b) Pro $n \in \mathbb{N}$ důkaz provedeme matematickou indukcí. Pro $n = 1$ je tvrzení $|z^1| = |z| = |z|^1$ zřejmé. Dále budeme předpokládat, že tvrzení platí pro $1,2,\ldots,n$ a ukážeme, že platí i pro $n+1$.

$$\left|z^{n+1}\right| = |z^n\cdot z| \overset{bod\ 4}{=} |z^n|\cdot|z| \overset{IP}{=} |z|^n\cdot|z| = |z|^{n+1}$$

   (c) Pro $n \in \mathbb{Z}^-$ dostaneme rozepsáním

$$|z^n| = \left|(z^{-1})^{-n}\right| \overset{bod\ 6b}{=} \left|z^{-1}\right|^{-n} \overset{bod\ 3}{=} \left(\frac{1}{|z|}\right)^{-n} = |z|^n.$$

7. Plyne z vlastnosti reálných čísel, kde je kvadrát číslo nezáporné, tudíž $x^2 \leq x^2 + y^2$ a analogicky $y^2 \leq x^2 + y^2$. Obě strany nerovností jsou nezáporné, lze je tedy beze změny znaménka nerovnosti odmocnit, čímž dostaneme požadovaná tvrzení.

8. Tzv. trojúhelníkovou nerovnost v této práci dále nevyužíváme, proto ji pro úsporu místa nebudeme dokazovat. Uvádíme ji zde jen pro úplnost. Důkaz lze nalézt například v [2, strana 16]. □

1.2 Goniometrický tvar komplexního čísla

Poznámka 1.21. V této části budeme potřebovat některé vlastnosti goniometrických funkcí. Kromě faktu, že funkce sinus a kosinus mají periodu 2π, to budou některé vzorce, které zde uvedeme bez důkazů, jež lze nalézt například v [7]. Na začátek připomeňme tzv. goniometrickou jedničku, tedy poznatek, že pro libovolné $\alpha \in \mathbb{R}$ platí

$$\sin^2 \alpha + \cos^2 \alpha = 1. \tag{1.3}$$

Definice 1.22. Nechť $z \in \mathbb{C}, z \neq 0$.
Zápis čísla z ve tvaru $z = r(\cos\varphi + \mathrm{i}\sin\varphi)$, kde $r \in \mathbb{R}^+$ a $\varphi \in \mathbb{R}$, nazýváme *goniometrickým tvarem komplexního čísla* z.
Číslo φ nazýváme *argumentem komplexního čísla* z.
Pokud $\varphi \in \langle 0, 2\pi)$, nazýváme číslo φ *hlavním argumentem komplexního čísla* z.

Věta 1.23. Libovolné nenulové komplexní číslo z lze vyjádřit ve tvaru

$$z = r(\cos\varphi + \mathrm{i}\sin\varphi),$$

kde $r = |z|$ a číslo φ je určeno dvojicí rovností

$$\cos\varphi = \frac{\mathrm{Re}\, z}{|z|}, \qquad \sin\varphi = \frac{\mathrm{Im}\, z}{|z|},$$

přičemž číslo r je určeno jednoznačně a číslo φ je určeno až na násobek 2π.

Důkaz. Existence.
Pouhým dosazením uvedených hodnot r, $\cos\varphi$ a $\sin\varphi$ dostáváme

$$r(\cos\varphi + \mathrm{i}\sin\varphi) = |z|\left(\frac{\mathrm{Re}\, z}{|z|} + \mathrm{i}\frac{\mathrm{Im}\, z}{|z|}\right) = \mathrm{Re}\, z + \mathrm{i}\,\mathrm{Im}\, z = z.$$

Jednoznačnost.
Spočteme-li absolutní hodnotu čísla z v goniometrickém tvaru, dostaneme

$$|z| = \left|r\cos\varphi + \mathrm{i}r\sin\varphi\right| = \sqrt{(r\cos\varphi)^2 + (r\sin\varphi)^2} = \sqrt{r^2\left(\cos^2\varphi + \sin^2\varphi\right)} \overset{(1.3)}{=} \sqrt{r^2} \overset{r\geq 0}{=} r.$$

Že je každý argument φ určen zmíněnými rovnicemi pak plyne z porovnání reálných a imaginárních částí téhož komplexního čísla z v algebraickém a goniometrickém tvaru, tedy $\mathrm{Re}\, z = r\cos\varphi$ a $\mathrm{Im}\, z = r\sin\varphi$. Z průběhu goniometrických funkcí plyne, že v libovolném intervalu $\langle \alpha, \alpha + 2\pi)$ má první rovnice nejvýše dvě řešení, přičemž v případě dvou řešení je jejich sinus různý. □

Poznámka 1.24. Z předchozí věty plyne, že hlavní argument libovolného nenulového komplexního čísla z je určen jednoznačně.
Například v [8] se hlavním argumentem rozumí argument $\varphi \in \langle -\pi, \pi)$. Naše zavedení je středoškolsky výhodnější, neboť se tak vyhneme zde mírně nepřirozeným goniometrickým funkcím ze záporných čísel, jelikož právě na středních školách jsou studovány převážně na intervalu $\langle 0, 2\pi \rangle$. Dále je to výhodné i pro zápis řešení binomické rovnice, viz Věta 1.31, kde v případě, že α je hlavní argument a, je i množina řešení zapsána pomocí čísel s hlavními argumenty, navíc přirozeně postupně rostoucími od 0 do 2π.

Poznámka 1.25. Komplexní číslo v algebraickém tvaru lze znázornit jako bod v rovině s kartézskou soustavou souřadnic, přičemž jeho x-ová souřadnice je rovna jeho reálné části a y-ová souřadnice imaginární části. Tato rovina se nazývá Gaussovou rovinou a její zavedení nám umožňuje mnoho planimetrických problémů řešit pomocí komplexních čísel. Tím se ale v této práci nezabýváme, mnohé aplikace lze najít například v [2]. Přechod na goniometrický tvar pak v Gaussově rovině není nic jiného, než přechod od kartézských k polárním souřadnicím.

Poznámka 1.26. Před dalším výkladem připomeňme známe součtové vzorce goniometrických funkcí. Pro libovolná $\alpha, \beta \in \mathbb{R}$ platí:

$$\begin{aligned}
\sin(\alpha+\beta) &= \sin\alpha\cos\beta + \cos\alpha\sin\beta;\\
\sin(\alpha-\beta) &= \sin\alpha\cos\beta - \cos\alpha\sin\beta;\\
\cos(\alpha+\beta) &= \cos\alpha\cos\beta - \sin\alpha\sin\beta;\\
\cos(\alpha-\beta) &= \cos\alpha\cos\beta + \sin\alpha\sin\beta.
\end{aligned}$$

Věta 1.27. Nechť z_1, z_2 jsou nenulová komplexní čísla v goniometrickém tvaru,
$z_1 = r_1(\cos\varphi_1 + \mathrm{i}\sin\varphi_1), z_2 = r_2(\cos\varphi_2 + \mathrm{i}\sin\varphi_2)$.
Pak platí:

1. $z_1 \cdot z_2 = r_1 r_2\big[\cos(\varphi_1+\varphi_2) + \mathrm{i}\sin(\varphi_1+\varphi_2)\big]$;
2. $\frac{z_1}{z_2} = \frac{r_1}{r_2}\big[\cos(\varphi_1-\varphi_2) + \mathrm{i}\sin(\varphi_1-\varphi_2)\big]$.

Důkaz.

1. $$\begin{aligned}
z_1 \cdot z_2 &= \big[r_1(\cos\varphi_1 + \mathrm{i}\sin\varphi_1)\big]\cdot\big[r_2(\cos\varphi_2 + \mathrm{i}\sin\varphi_2)\big] =\\
&= r_1 r_2\big[\cos\varphi_1\cos\varphi_2 + \mathrm{i}\cos\varphi_1\sin\varphi_2 + \mathrm{i}\sin\varphi_1\cos\varphi_2 + \mathrm{i}^2\sin\varphi_1\sin\varphi_2\big] =\\
&= r_1 r_2\big[(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + \mathrm{i}(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)\big] =\\
&= r_1 r_2\big[\cos(\varphi_1+\varphi_2) + \mathrm{i}\sin(\varphi_1+\varphi_2)\big]
\end{aligned}$$

2. $$\begin{aligned}
\frac{z_1}{z_2} &= \frac{r_1(\cos\varphi_1 + \mathrm{i}\sin\varphi_1)}{r_2(\cos\varphi_2 + \mathrm{i}\sin\varphi_2)}\cdot\frac{\cos\varphi_2 - \mathrm{i}\sin\varphi_2}{\cos\varphi_2 - \mathrm{i}\sin\varphi_2} =\\
&= \frac{r_1}{r_2}\cdot\frac{\cos\varphi_1\cos\varphi_2 - \mathrm{i}\cos\varphi_1\sin\varphi_2 + \mathrm{i}\sin\varphi_1\cos\varphi_2 - \mathrm{i}^2\sin\varphi_1\sin\varphi_2}{\cos^2\varphi_2 - \mathrm{i}\cos\varphi_2\sin\varphi_2 + \mathrm{i}\sin\varphi_2\cos\varphi_2 - \mathrm{i}^2\sin^2\varphi_2} =\\
&= \frac{r_1}{r_2}\cdot\frac{(\cos\varphi_1\cos\varphi_2 + \sin\varphi_1\sin\varphi_2) + \mathrm{i}(\sin\varphi_1\cos\varphi_2 - \cos\varphi_1\sin\varphi_2)}{\sin^2\varphi_2 + \cos^2\varphi_2} =\\
&= \frac{r_1}{r_2}\big[\cos(\varphi_1-\varphi_2) + \mathrm{i}\sin(\varphi_1-\varphi_2)\big]
\end{aligned}$$

□

Věta 1.28 (Moivreova). Pro libovolné nenulové komplexní číslo $z = r(\cos\varphi + \mathrm{i}\sin\varphi)$ a libovolné celé číslo n platí

$$z^n = r^n\big[\cos(n\varphi) + \mathrm{i}\sin(n\varphi)\big].$$

Důkaz. Důkaz rozdělíme na tři části podle signatury n.

1. Pro $n = 0$ je tvrzení $z^0 = r^0(\cos 0 + \mathrm{i}\sin 0) = 1(1 + 0\mathrm{i}) = 1$ zřejmé.

2. Pro $n \in \mathbb{N}$ důkaz provedeme matematickou indukcí. Pro $n = 1$ je tvrzení $z^1 = r^1\big[\cos(1\varphi) + \mathrm{i}\sin(1\varphi)\big] = r(\cos\varphi + \mathrm{i}\sin\varphi) = z$ zřejmé. Dále budeme předpokládat, že tvrzení platí pro $1, 2, \ldots, n$ a ukážeme, že platí i pro $n+1$.

$$\begin{aligned} z^{n+1} = z \cdot z^n &\overset{IP}{=} \{r(\cos\varphi + \mathrm{i}\sin\varphi)\} \cdot \{r^n\big[\cos(n\varphi) + \mathrm{i}\sin(n\varphi)\big]\} \overset{V\,1.27}{=} \\ &\overset{V\,1.27}{=} r^{n+1}\Big[\cos\big((n+1)\varphi\big) + \mathrm{i}\sin\big((n+1)\varphi\big)\Big] \end{aligned}$$

3. Pro $n \in \mathbb{Z}^-$ dostaneme rozepsáním

$$\begin{aligned} z^n = \frac{1}{z^{-n}} &\overset{\text{část } 2}{=} \frac{1}{r^{-n}\big[\cos(-n\varphi) + \mathrm{i}\sin(-n\varphi)\big]} \cdot \frac{\cos(-n\varphi) - \mathrm{i}\sin(-n\varphi)}{\cos(-n\varphi) - \mathrm{i}\sin(-n\varphi)} = \\ &= r^n \frac{\cos(-n\varphi) - \mathrm{i}\sin(-n\varphi)}{\cos^2(-n\varphi) + \sin^2(-n\varphi)} = r^n\big[\cos(-n\varphi) - \mathrm{i}\sin(-n\varphi)\big] = \\ &= r^n\big[\cos(n\varphi) + \mathrm{i}\sin(n\varphi)\big] \end{aligned}$$

□

Definice 1.29. *Binomickou rovnicí* s neznámou $z \in \mathbb{C}$ rozumíme rovnici tvaru $z^n = a$, kde $a \in \mathbb{C}$ a $n \in \mathbb{N}$ jsou daná čísla a $z \in \mathbb{C}$ je neznámá.
Libovolný kořen z této rovnice nazýváme (komplexní) *n-tou odmocninou* z a a píšeme $z = \sqrt[n]{a}$ nebo $z = a^{\frac{1}{n}}$.

Poznámka 1.30. V oboru reálných čísel se $\sqrt[n]{a}$ definuje pouze pro $a \in \mathbb{R}_0^+$ a kvůli jednoznačnosti (pro sudá n) se dodává podmínka $\sqrt[n]{a} \in \mathbb{R}_0^+$. V oboru komplexních čísel hodnoty $\sqrt[n]{a}$ existují pro libovolné $a \in \mathbb{C}$, ale jednoznačně existuje pouze $\sqrt[n]{0} = 0$ pro libovolné n a $\sqrt[1]{a} = a$ pro libovolné a. Jak vypadají všechny n-té odmocniny z nenulového komplexního čísla nám řekne následující věta, ve které s výhodou využijeme goniometrického tvaru odmocňovaného čísla i výsledné odmocniny.

Věta 1.31. Množina kořenů binomické rovnice $z^n = a$, kde $a \neq 0$ má goniometrický tvar $a = |a| \cdot (\cos\alpha + \mathrm{i}\sin\alpha)$, je tvaru

$$K = \left\{ \sqrt[n]{|a|} \cdot \left[\cos\left(\frac{\alpha}{n} + k\frac{2\pi}{n}\right) + \mathrm{i}\sin\left(\frac{\alpha}{n} + k\frac{2\pi}{n}\right)\right]; \quad k = 0, 1, \ldots, n-1 \right\}.$$

Důkaz. Ukažme, že libovolný prvek množiny K je řešením dané binomické rovnice. Umocníme-li jej totiž na n, dostaneme užitím Moivreovy věty

$$\left(\sqrt[n]{|a|}\cdot\left[\cos\left(\frac{\alpha}{n}+k\frac{2\pi}{n}\right)+\mathrm{i}\sin\left(\frac{\alpha}{n}+k\frac{2\pi}{n}\right)\right]\right)^n \overset{V\,1.28}{=}$$
$$\overset{V\,1.28}{=} |a|\cdot\left[\cos\left(\alpha+k2\pi\right)+\mathrm{i}\sin\left(\alpha+k2\pi\right)\right] = |a|\cdot(\cos\alpha+\mathrm{i}\sin\alpha) = a,$$

tedy je řešením dané binomické rovnice.
Prvky množiny K jsou zřejmě po dvou různé. Máme tedy n různých řešení binomické rovnice, která je speciálním případem polynomiální rovnice stupně n, tudíž jsou to podle Základní věty algebry (viz [9, strana 93]) všechna její řešení. □

1.3 Komplexní odmocniny z jedné

Poznámka 1.32. Dosadíme-li do Věty 1.31 $a = 1 = 1(\cos 0 + \mathrm{i}\sin 0)$, dostaneme všech n různých komplexních n-tých odmocnin z jedné, které dále označme

$$\varepsilon_k^{(n)} = \cos\left(k\frac{2\pi}{n}\right)+\mathrm{i}\sin\left(k\frac{2\pi}{n}\right), \quad k = 1,2,\ldots,n,$$

přitom jsme $k = 0$ nahradili $k = n$, což bude v dalším vhodnější tvar. Mohli jsme to udělat, neboť $\cos\left(0\frac{2\pi}{n}\right)+\mathrm{i}\sin\left(0\frac{2\pi}{n}\right) = \cos\left(n\frac{2\pi}{n}\right)+\mathrm{i}\sin\left(n\frac{2\pi}{n}\right) = 1+0\mathrm{i} = 1$, z čehož též vidíme, že jednička jako jediná n-tá odmocnina z jedné v nezáporných reálných číslech je i jednou z n-tých odmocnin z jedné v komplexních číslech. Rozepsáním příslušné binomické rovnice na kořenové činitele pak dostáváme rovnost polynomů

$$z^n - 1 = (z-1)\left(z-\varepsilon_1^{(n)}\right)\left(z-\varepsilon_2^{(n)}\right)\ldots\left(z-\varepsilon_{n-1}^{(n)}\right).$$

Horní exponent (n) budeme v dalším, kdy nebude hrozit pochybnost o n, pro lepší zápis mocnin často vynechávat. S využitím Moivreovy věty navíc můžeme psát

$$\varepsilon_k = \cos\left(k\frac{2\pi}{n}\right)+\mathrm{i}\sin\left(k\frac{2\pi}{n}\right) = \left[\cos\left(\frac{2\pi}{n}\right)+\mathrm{i}\sin\left(\frac{2\pi}{n}\right)\right]^k = \varepsilon_1^k,$$

tedy $\varepsilon_1 = \sqrt[n]{1}, \varepsilon_1^2 = \sqrt[n]{1},\ldots,\varepsilon_1^n = 1 = \sqrt[n]{1}$, přičemž jsme takto dostali všechny hodnoty $\sqrt[n]{1}$ pomocí hodnoty ε_1. Dosazením do výše odvozené rovnosti dostáváme důležitý rozklad

$$z^n - 1 = (z-1)\left(z-\varepsilon_1\right)\left(z-\varepsilon_1^2\right)\ldots\left(z-\varepsilon_1^{n-1}\right).$$

Věta 1.33. Nechť $\varepsilon = \sqrt[n]{1}, \varepsilon_1 = \sqrt[n]{1}, \varepsilon_2 = \sqrt[n]{1}$ a $m \in \mathbb{Z}$. Pak platí:

1. $\varepsilon^{-1} = \sqrt[n]{1}$;
2. $\overline{\varepsilon} = \sqrt[n]{1}$;
3. $-\varepsilon = \sqrt[n]{1}$, je-li n sudé;
4. $\varepsilon^m = \sqrt[n]{1}$;
5. $\varepsilon_1\cdot\varepsilon_2 = \sqrt[n]{1}$.

Důkaz. Rozepsáním dostaneme:

1. $(\varepsilon^{-1})^n = (\varepsilon^n)^{-1} = 1^{-1} = 1$;
2. $\overline{\varepsilon}^n \overset{V1.19}{=} \overline{\varepsilon^n} = \overline{1} = 1$;
3. $(-\varepsilon)^n = (-1)^n \varepsilon^n = (-1)^n \cdot 1 = (-1)^n \overset{2|n}{=} 1$;
4. $(\varepsilon^m)^n = (\varepsilon^n)^m = 1^m = 1$;
5. $(\varepsilon_1 \cdot \varepsilon_2)^n = \varepsilon_1^n \cdot \varepsilon_2^n = 1 \cdot 1 = 1$. □

Poznámka 1.34. Z goniometrického tvaru odmocniny z jedné ihned vidíme, že její absolutní hodnota je rovna jedné. Každá komplexní odmocnina z jedné je tedy komplexní jednotkou. Ovšem naopak každá komplexní jednotka není odmocninou z jedné. Ukážeme si nutnou a dostatečnou podmínku pro to, aby byla.

Věta 1.35. Komplexní jednotka $\varepsilon = \cos\alpha + \mathrm{i}\sin\alpha$ je komplexní n-tou odmocninou z jedné pro vhodné $n \in \mathbb{N}$ právě tehdy, když existuje $k \in \mathbb{Q}$ takové, že $\alpha = k\pi$.

Důkaz. Existuje-li takové $k \in \mathbb{Q}, k = \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{N}$, že $\alpha = k\pi = \frac{a}{b}\pi$, dostaneme při volbě $n = 2b$ rovnost

$$\varepsilon^n = \varepsilon^{2b} = [\cos\alpha + \mathrm{i}\sin\alpha]^n = \left[\cos\frac{a}{b}\pi + \mathrm{i}\sin\frac{a}{b}\pi\right]^{2b} = \cos 2a\pi + \mathrm{i}\sin 2a\pi = 1.$$

Komplexní jednotka ε je tedy například $(2b)$-tou odmocninou z jedné.
Je-li naopak komplexní jednotka $\varepsilon = \cos\alpha + \mathrm{i}\sin\alpha$ n-tou odmocninou z jedné, pro nějaké $n \in \mathbb{N}$, musí podle Moivreovy věty pro takové n existovat $a \in \mathbb{Z}$ tak, že $\alpha n = 2\pi a$, odkud $\alpha = k\pi$ pro $k = \frac{2a}{n} \in \mathbb{Q}$. □

Definice 1.36. *Primitivní n-tou odmocninou z jedné* rozumíme libovolnou n-tou odmocninu z jedné ε takovou, že její mocniny ε^k, $k = 1, 2, \ldots, n$, jsou právě všechny n-té odmocniny z jedné.

Poznámka 1.37. Dle definice je n-tá odmocnina ε primitivní právě tehdy, když $\varepsilon, \varepsilon^2, \ldots, \varepsilon^n$ jsou všechny n-té odmocniny z jedné. Protože n-tých odmocnin z jedné je právě n, nastane to právě tehdy, když hodnoty $\varepsilon, \varepsilon^2, \ldots, \varepsilon^n = 1$ jsou po dvou různé.
Z Poznámky 1.32 plyne, že $\varepsilon_1^{(n)}$ je primitivní n-tá odmocnina z jedné pro libovolné přirozené číslo n. Naopak číslo 1, které je n-tou odmocninou z jedné pro libovolné $n \in \mathbb{N}$, je primitivní pouze v případě $\sqrt[n]{1}$ pro $n = 1$.

Věta 1.38. Nechť ε je libovolná primitivní n-tá odmocnina z jedné a nechť $t \in \mathbb{Z}$.
Pak $\varepsilon^t = 1$ právě tehdy, když číslo t je dělitelné číslem n.

Důkaz. Vyjádřeme číslo t podobně jako při dělení celých čísel se zbytkem, zde ovšem $t = nl + k, l \in \mathbb{Z}, k \in \{1, 2, \ldots, n\}$, a upravujme $\varepsilon^t = \varepsilon^{nl+k} = \left(\varepsilon^n\right)^l \varepsilon^k = \varepsilon^k$. Protože pro $k = n$ je $\varepsilon^k = \varepsilon^n = 1$ a z definice primitivní odmocniny z jedné jsou mocniny ε^k po dvou různé, dostáváme ekvivalenci mezi $\varepsilon^t = 1$ a $k = n$, což je ekvivalentní právě podmínce $n \mid t$. □

Věta 1.39. Daná n-tá odmocnina z jedné

$$\varepsilon_k = \cos\left(k\frac{2\pi}{n}\right) + \mathrm{i}\sin\left(k\frac{2\pi}{n}\right), \quad \text{kde } k \in \{1,2,\ldots,n\},$$

je primitivní právě tehdy, když číslo k je nesoudělné s číslem n.

Důkaz. Z definice je odmocnina ε_k primitivní právě tehdy, když hodnoty

$$\varepsilon_k, \varepsilon_k^2, \ldots, \varepsilon_k^n = 1$$

jsou navzájem různé. To znamená, že pro každá dvě čísla $p,q \in \mathbb{N}$,

$$1 \leq p < q \leq n, \tag{1.4}$$

musí být

$$\varepsilon_k^p \neq \varepsilon_k^q \quad \text{neboli} \quad \varepsilon_k^{q-p} \neq 1.$$

Poněvadž $\varepsilon_k = \varepsilon_1^k$, můžeme nutnou a dostatečnou podmínku, aby daná ε_k byla primitivní, vyjádřit ve tvaru

$$\varepsilon_1^{k(q-p)} \neq 1 \quad \text{pro všechna} \quad p,q \in \mathbb{N}, 1 \leq p < q \leq n.$$

Rovnost $\varepsilon_1^{k(q-p)} = 1$ je dle Věty 1.38, neboť ε_1 je primitivní n-tá odmocnina z jedné, ekvivalentní s tím, že n dělí $k(q-p)$.
Pro případ, kdy je k nesoudělné s n, připomeňme pravidlo, že pro libovolná $a,b,c \in \mathbb{Z}$ platí

$$a \mid b \cdot c \ \wedge \ (a,b) = 1 \quad \Longrightarrow \quad a \mid c,$$

což by v našem případě $n \mid k(q-p)$ znamenalo, že $n \mid p-q$. To je však ve sporu s (1.4), což dokazuje, že ε_k je primitivní.
Jsou-li naopak k a n soudělná, existují $m,l \in \mathbb{N}, m < n$, taková, že $mk = ln$, a tedy existují $p,q \in \mathbb{N}$ vyhovující (1.4), pro něž $q-p = m$. Pro tato p,q je $\varepsilon_1^{k(q-p)} = 1$ a ε_k není tedy primitivní. □

Důsledek 1.40. Nechť p je prvočíslo a nechť $\varepsilon = \sqrt[p]{1}$.
Pak ε je primitivní právě tehdy, když $\varepsilon \neq 1$.

Důkaz. Tvrzení plyne z předchozí věty, neboť pro libovolné prvočíslo p platí $(p,k) = 1$ pro všechna $k = 1,2,\ldots,p-1$ a $(p,p) = p$, přičemž $\varepsilon_p^{(p)} = 1$. □

Věta 1.41. Nechť ε je libovolná primitivní n-tá odmocnina z jedné a nechť $t \in \mathbb{N}_0$.
Jestliže číslo t není dělitelné číslem n, pak platí:

$$1 + \varepsilon^t + \varepsilon^{2t} + \cdots + \varepsilon^{(n-1)t} = 0.$$

Jestliže je naopak číslo t dělitelné číslem n, pak platí:

$$1 + \varepsilon^t + \varepsilon^{2t} + \cdots + \varepsilon^{(n-1)t} = n.$$

Důkaz. Pokud $n \nmid t$, pak, dle Věty 1.38, $\varepsilon^t \neq 1$ a lze tudíž využít vzorce pro součet členů geometrické posloupnosti, odkud

$$1+\varepsilon^t+\varepsilon^{2t}+\cdots+\varepsilon^{(n-1)t}=\frac{\varepsilon^{nt}-1}{\varepsilon^t-1}=\frac{0}{\varepsilon^t-1}=0.$$

Pokud $n \mid t$, pak, dle Věty 1.38, $\varepsilon^t = 1$, odkud

$$1+\varepsilon^t+\varepsilon^{2t}+\cdots+\varepsilon^{(n-1)t}=1+1+1+\cdots+1=n.$$

□

Poznámka 1.42. Tvrzení předchozí věty pro $t = 1$ lze vidět přímo z příslušné binomické rovnice. Podle vzorce pro rozdíl dvou n-tých mocnin, $n \geq 2$, platí

$$z^n-1=(z-1)\left(1+z+z^2+\cdots+z^{n-1}\right),$$

tudíž z toho, že ε je n-tá odmocnina z jedné, tedy $\varepsilon^n - 1 = 0$, přičemž $\varepsilon \neq 1$, dostaneme

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

Tuto pro nás velmi důležitou vlastnost komplexních odmocnin z jedné v dalším mnohokrát využijeme, přičemž ji vždy pro zapamatování raději připomeneme.

Poznámka 1.43. Označme $\left\{\sqrt[n]{1}\right\}$ množinu všech n-tých odmocnin z jedné, tedy

$$\left\{\sqrt[n]{1}\right\}=\left\{\varepsilon_1^{(n)},\varepsilon_2^{(n)},\ldots,\varepsilon_n^{(n)}=1\right\}.$$

Tato množina je zřejmě podmnožinou množiny všech nenulových komplexních čísel, je uzavřená vůči násobení, což plyne z Věty 1.33 bodu 5, obsahuje neutrální prvek vůči násobení $1=\varepsilon_n^{(n)}$ a ke každému prvku obsahuje i prvek inverzní, což plyne z Věty 1.33 bodu 1. Celkem je $\left\{\sqrt[n]{1}\right\}$ s násobením podgrupou grupy $\mathbb{C}\setminus\{0\}$ s násobením. Množina $\left\{\sqrt[n]{1}\right\}$ s násobením je tedy sama grupou, přičemž

$$\left(\varepsilon_k^{(n)}\right)^{-1}=\varepsilon_{n-k}^{(n)}.$$

Množinu $\left\{\sqrt[n]{1}\right\}$ můžeme též vygenerovat pomocí jedné, libovolně vybrané hodnoty ε primitivní n-té odmocniny z jedné, tedy

$$\left\{\sqrt[n]{1}\right\}=\left\{\varepsilon,\varepsilon^2,\ldots,\varepsilon^n=1\right\}.$$

V této reprezentaci jsou inverzní prvky tvaru

$$\left(\varepsilon^k\right)^{-1}=\varepsilon^{n-k}\quad\text{pro všechna}\quad k=1,2,\ldots,n.$$

1.4 Zbytkové třídy

V této části podáme stručný výklad o zbytkových třídách a izomorfních zobrazeních grup. Je zpracována podle [9, části 1.3 a 1.6], kde je možno nalézt i důkazy zde zmíněných tvrzení, které tu pro stručnost uvádět nebudeme. Na závěr této části ukážeme souvislost mezi odmocninami z jedné a zbytkovými třídami, kterou budeme v příkladech využívat.

Definice 1.44. Nechť n je přirozené číslo.
Dvě celá čísla a, b se nazývají *kongruentní podle modulu n*, jestliže $n \mid a-b$.
Píšeme $a \equiv b \pmod{n}$.

Definice 1.45. Nechť n je přirozené číslo.
Množiny $[a]_n = \{kn+a \mid k \in \mathbb{Z}\}$, kde $a \in \mathbb{Z}$, se nazývají *zbytkové třídy podle modulu n*.
Množinu všech zbytkových tříd podle modulu n označujeme symbolem $\mathbb{Z}_n$.

Věta 1.46. Pro dvě zbytkové třídy podle téhož modulu n platí $[a]_n = [b]_n$ právě tehdy, když $a \equiv b \pmod{n}$.

Poznámka 1.47. Z předchozí věty plyne, že $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

Definice 1.48. Nechť n je přirozené číslo.
Na množině $\mathbb{Z}_n$ všech zbytkových tříd podle modulu n definujeme operaci sčítání předpisem

$$[a]_n + [b]_n = [a+b]_n.$$

Věta 1.49. Množina $\mathbb{Z}_n$ s operací sčítání tvoří komutativní grupu pro libovolné přirozené číslo n. Přičemž roli neutrálního prvku hraje zbytková třída $[0]_n$ a roli inverzního prvku k libovolné zbytkové třídě $[a]_n$ třída $[-a]_n = [n-a]_n$.

Definice 1.50. Nechť množina G_1 s operací $\star$ a množina G_2 s operací $\diamond$ jsou dvě grupy.
Nechť $f\colon G_1 \to G_2$ je bijektivní zobrazení.
Řekneme, že f je *izomorfismus* grupy G_1 na grupu G_2, jestliže pro libovolné dva prvky $a, b \in G_1$ platí

$$f(a) \diamond f(b) = f(a \star b).$$

Grupy G_1, G_2 se nazývají *izomorfní*, jestliže existuje izomorfismus $G_1 \to G_2$.
Píšeme $G_1 \cong G_2$.

Věta 1.51. Nechť $f\colon G_1 \to G_2$ je izomorfismus grup.
Pak inverzní zobrazení $f^{-1}\colon G_2 \to G_1$ je rovněž izomorfismus.
Odtud $G_1 \cong G_2 \Leftrightarrow G_2 \cong G_1$.

Věta 1.52. Nechť n je přirozené číslo.
Pak grupa $\mathbb{Z}_n$ se sčítáním je izomorfní s grupou $\{\sqrt[n]{1}\}$ s násobením.

Důkaz. Nechť ε je primitivní n-tá odmocnina z jedné a $\{\sqrt[n]{1}\} = \{\varepsilon, \varepsilon^2, \ldots, \varepsilon^n = 1\}$.
Uvažme zobrazení $f\colon \mathbb{Z}_n \to \{\sqrt[n]{1}\}$ definované předpisem

$$f([a]_n) = \varepsilon^a$$

a ukažme, že se jedná o izomorfismus.
Protože ε je primitivní a $|\mathbb{Z}_n| = \left|\{\sqrt[n]{1}\}\right| = n$, jde o bijektivní zobrazení. Rozepsáním

$$f([a]_n + [b]_n) = f([a+b]_n) = \varepsilon^{a+b} = \varepsilon^a \cdot \varepsilon^b = f([a]_n) \cdot f([b]_n)$$

dostáváme, že f je izomorfismus a $\mathbb{Z}_n \cong \left\{\sqrt[n]{1}\right\}$. □

Poznámka 1.53. Izomorfismus f z důkazu předchozí věty budeme často užívat v příkladech, kdy příslušnost uvažovaného celého čísla k nějaké zbytkové třídě budeme s výhodou reprezentovat odpovídající mocninou komplexní jednotky ε.

1.5 Pomocná tvrzení

Na závěr první kapitoly dokážeme několik tvrzení, která využijeme ve druhé kapitole v příkladech.
První pomocné tvrzení se bude týkat jedné vlastnosti kombinačních čísel. Dokážeme ji užitím známé rovnosti

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}, \tag{1.5}$$

na které je také založen rekurentní výpočet binomických koeficientů uspořádaných do Pascalova trojúhelníku (viz [3, strana 169]).

Lemma 1.54. Pro libovolná $n, s \in \mathbb{N}_0$ platí

$$\sum_{k=0}^{s} \binom{n+k}{k} = \binom{n+s+1}{s}.$$

Důkaz. Důkaz provedeme matematickou indukcí přes s. Pro $s = 0$ je tvrzení zřejmé, neboť

$$\binom{n}{0} = 1 = \binom{n+1}{0}.$$

Předpokládejme, že tvrzení platí pro $0, 1, \ldots, s-1$ a ukažme, že platí i pro s. Pak

$$\sum_{k=0}^{s} \binom{n+k}{k} = \sum_{k=0}^{s-1} \binom{n+k}{k} + \binom{n+s}{s} \overset{IP}{=} \binom{n+s}{s-1} + \binom{n+s}{s} \overset{(1.5)}{=} \binom{n+s+1}{s},$$

čímž je tvrzení dokázáno. □

V následujícím budeme využívat pojmy a tvrzení z algebry mnohočlenů, které lze nalézt např. v [9].

Lemma 1.55. Nechť p je prvočíslo. Pak polynom $f(x) = x^{p-1} + \cdots + x + 1$ je ireducibilní nad $\mathbb{Q}$.

Důkaz. Pro $p = 2$ je tvrzení zřejmé. Dále tedy nechť $p \geq 3$. K důkazu užijeme tvrzení, které nám říká, že polynom $f(x)$ je ireducibilní nad $\mathbb{Q}$ právě tehdy, když je nad $\mathbb{Q}$ ireducibilní polynom $f(ax+b)$, kde $a,b \in \mathbb{Q}, a \neq 0$. Uvažme tedy polynom $f(x+1)$:

$$f(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1 = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + p,$$

kde každý koeficient a_{p-1-s} pro $s = 1, \ldots, p-2$ je dán rovností

$$a_{p-1-s} = \sum_{k=0}^{s} \binom{p-1-s+k}{k}.$$

Dosadíme-li do vzorce z Lemmatu 1.54 za $n = p-1-s$, dostaneme

$$a_{p-1-s} = \sum_{k=0}^{s} \binom{p-1-s+k}{k} = \binom{p}{s} \quad \text{pro každé} \quad s = 1, \ldots, p-2.$$

Protože však $p \mid \binom{p}{s}$ pro $s = 1, \ldots, p-2$, tedy $p \mid a_n$ pro $n = 1, \ldots, p-2$ a současně $p \mid p$, $p \nmid 1$ a $p^2 \nmid p$, tak podle Eisensteinova kritéria (viz [9, strana 101]) je polynom $f(x+1)$, a tedy i polynom $f(x)$ ireducibilní nad $\mathbb{Q}$. □

Následující věta je společně s rovností z Poznámky 1.42 základním kamenem řešení řady příkladů, které uvedeme ve druhé kapitole této práce.

Věta 1.56. Nechť p je prvočíslo a nechť ε značí primitivní p-tou odmocninu z jedné, tedy $\varepsilon = \sqrt[p]{1}, \varepsilon \neq 1$.
Nechť čísla $a_0, a_1, \ldots, a_{p-1} \in \mathbb{Q}$ jsou taková, že

$$a_0 + a_1\varepsilon + \cdots + a_{p-1}\varepsilon^{p-1} = 0.$$

Pak platí

$$a_0 = a_1 = \cdots = a_{p-1}.$$

Důkaz. Uvažme polynomy $a_0 + a_1 x + \cdots + a_{p-1}x^{p-1}$ a $1 + x + \cdots + x^{p-1}$. Tyto dva polynomy mají společný kořen ε, nejsou tedy nesoudělné. Protože je však polynom $1 + x + \cdots + x^{p-1}$ podle Lemmatu 1.55 ireducibilní nad $\mathbb{Q}$, musí dělit polynom $a_0 + a_1 x + \cdots + a_{p-1}x^{p-1}$. To je zřejmě ekvivalentní podmínce $a_0 = a_1 = \cdots = a_{p-1}$, čímž je tvrzení dokázáno. □

Lemma 1.57. Pro libovolné $n \in \mathbb{N}$ a libovolné $q \in \mathbb{C}, q \neq 1$, platí

$$R_1(q,n) := 1q + 2q^2 + \cdots + nq^n = \frac{nq^{n+2} - (n+1)q^{n+1} + q}{(q-1)^2}. \tag{1.6}$$

Důkaz. Tuto identitu je možno dokázat více způsoby, zde si ukážeme dva z nich. Další je možno najít v [4, příklad 2.27]. Nejprve běžný způsob známý především z důkazu vzorce pro součet členů geometrické posloupnosti, tedy odečtením $R_1(q,n)$ od jeho q-násobku:

$$R_1(q,n) = q + 2q^2 + 3q^3 + \cdots + nq^n \tag{1.7a}$$
$$q \cdot R_1(q,n) = q^2 + 2q^3 + \cdots + (n-1)q^n + nq^{n+1} \tag{1.7b}$$

(1.7b) − (1.7a):

$$(q-1)\cdot R_1(q,n) = nq^{n+1} - (q+q^2+\cdots+q^n) = nq^{n+1} - \frac{q^{n+1}-q}{q-1} =$$
$$= \frac{nq^{n+2}-(n+1)q^{n+1}+q}{q-1}$$

Odtud již po vydělení číslem $q-1$ plyne (1.6). □

Druhý způsob, který si zde uvedeme, bude užitím diferenčního a sumačního počtu, jehož základy jsou vyloženy v [6].

$$R_1(q,n) = q+2q^2+3q^3+\cdots+nq^n$$
$$R_1(q,n+1) = q+2q^2+3q^3+\cdots+nq^n+(n+1)q^{n+1}$$
$$\Delta R_1(q,n) = R_1(q,n+1)-R_1(q,n) = (n+1)q^{n+1}$$
$$R_1(q,n) = \sum(n+1)q^{n+1} = (an+b)q^{n+1}+c$$
$$(n+1)q^{n+1} = \Delta[(an+b)q^{n+1}+c] = [a(q-1)n+aq+b(q-1)]q^{n+1}$$

Porovnáním koeficientů u stejných mocnin n dostaneme

$$a = \frac{1}{q-1}, \quad b = -\frac{1}{(q-1)^2},$$

tedy

$$R_1(q,n) = \left[\frac{n}{q-1} - \frac{1}{(q-1)^2}\right]q^{n+1} + c = \frac{nq^{n+2}-(n+1)q^{n+1}}{(q-1)^2} + c.$$

Podmínka $R_1(q,1) = q$ nám dá

$$c = \frac{q}{(q-1)^2},$$

odkud již plyne (1.6). □

Lemma 1.58. Nechť $p > 2$ je prvočíslo a nechť ε značí primitivní p-tou odmocninu z jedné, tedy $\varepsilon = \sqrt[p]{1}, \varepsilon \neq 1$.
Pak platí rovnost polynomů

$$(x^p+1)^2 = (x+\varepsilon)\left(x+\varepsilon^2\right)\cdots\left(x+\varepsilon^{2p}\right). \tag{1.8}$$

Důkaz. Uvažme binomickou rovnici $z^p = -1$. Protože p je liché, je

$$\left(-\varepsilon^k\right)^p = (-1)^p(\varepsilon^p)^k = -1\cdot 1 = -1$$

pro každé $k = 1,2,\ldots,p$. Máme tedy p různých kořenů rovnice $z^p+1=0$, což jsou podle Základní věty algebry všechna řešení této binomické rovnice. Rozepsáním na součin kořenových činitelů dostaneme polynomickou rovnost

$$x^p+1 = (x+1)(x+\varepsilon)\cdots\left(x+\varepsilon^{p-1}\right).$$

Umocníme-li tuto rovnost na druhou a využijeme-li periodičnosti mocnin ε, tedy rovností $\left(x+\varepsilon^k\right)^2 = \left(x+\varepsilon^k\right)\left(x+\varepsilon^{k+p}\right)$ pro každé $k = 1,2,\ldots,p$, dostaneme dokazovanou rovnost (1.8). □

Lemma 1.59. Nechť $p > 2$ je prvočíslo a nechť ε značí primitivní p-tou odmocninu z jedné, tedy $\varepsilon = \sqrt[p]{1}, \varepsilon \neq 1$.
Pak platí

$$\frac{1}{\varepsilon - 1} = -\frac{1}{p}\big(\varepsilon^{p-2} + 2\varepsilon^{p-3} + \cdots + (p-2)\varepsilon + p - 1\big). \tag{1.9}$$

Důkaz. Uvažme polynom $x^{p-2} + 2x^{p-3} + \cdots + (p-2)x + p - 1$. Vynásobíme-li ho polynomem $x - 1$, dostaneme

$$\begin{aligned}\big(x^{p-2} + 2x^{p-3} + \cdots + (p-2)x + p - 1\big)(x-1) = \\ = x^{p-1} + 2x^{p-2} + \cdots + (p-2)x^2 + (p-1)x - \\ - x^{p-2} - 2x^{p-3} - \ldots - (p-2)x - (p-1) \\ = (x^{p-1} + x^{p-2} + \cdots + x + 1) - p.\end{aligned} \tag{1.10}$$

Dosadíme-li do (1.10) $x = \varepsilon$, dostaneme vzhledem k $\varepsilon^{p-1} + \varepsilon^{p-2} + \cdots + \varepsilon + 1 = 0$ rovnost

$$\big(\varepsilon^{p-2} + 2\varepsilon^{p-3} + \cdots + (p-2)\varepsilon + p - 1\big)(\varepsilon - 1) = -p,$$

která po vydělení $-p(\varepsilon - 1)$ přejde v dokazovaný vzorec (1.9). □

Kapitola 2

Praktické užití

2.1 Konečné součty kombinačních čísel

Jediné známější uplatnění komplexních čísel v kombinatorice je jejich užití při určování různých konečných součtů tvořených kombinačními čísly. Vychází se přitom z faktu, že libovolné komplexní číslo můžeme vyjádřit jednak v algebraickém tvaru a umocnit ho užitím binomické věty, jednak v goniometrickém tvaru a umocnit užitím Moivreovy věty. Tato problematika je v našem textu zpracována podle [4, část 1.7.].
Binomická věta nám umožňuje n-tou mocninu součtu dvou čísel rozepsat na součet s kombinačními čísly. Je-li $n \in \mathbb{N}$ a $A, B \in \mathbb{C}$, pak ji lze vyjádřit vzorcem:

$$(A+B)^n = \binom{n}{0}A^n + \binom{n}{1}A^{n-1}B + \binom{n}{2}A^{n-2}B^2 + \cdots + \binom{n}{n-1}AB^{n-1} + \binom{n}{n}B^n \quad (2.1)$$

Pro začátek uveďme dva vzorce pro součty kombinačních čísel, které plynou ze samotné binomické věty po volbě $A = 1, B = 1$, resp. $A = 1, B = -1$.

$$2^n = (1+1)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} \quad (2.2)$$

$$0 = \big(1+(-1)\big)^n = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots + (-1)^{n-1}\binom{n}{n-1} + (-1)^n\binom{n}{n} \quad (2.3)$$

Sečteme-li, resp. odečteme-li tyto dvě rovnosti a vydělíme-li výsledek dvěma, dostaneme identity

$$\frac{(2.2)+(2.3)}{2}: \quad \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots = 2^{n-1}, \quad (2.4)$$

$$\frac{(2.2)-(2.3)}{2}: \quad \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots = 2^{n-1}, \quad (2.5)$$

kde součty končí $\binom{n}{n}$, resp. $\binom{n}{n-1}$, případně $\binom{n}{n-1}$, resp. $\binom{n}{n}$, podle toho, zda je číslo n sudé, případně liché. V dalším již poslední člen zdůrazňovat nebudeme a budeme takto značit součet všech kombinačních čísel $\binom{n}{k}$ tvořených podle zřejmého pravidla až po k nejvyšší možné, při úmluvě, že kombinační číslo $\binom{n}{k}$ máme definované pouze pro $k = 0, 1, \ldots, n$.

Nejjednodušší součty s využitím komplexních čísel dostaneme, zvolíme-li ve vzorci (2.1) $A = 1$ a $B = \mathrm{i}$. Protože

$$\mathrm{i}^{4k} = 1,\ \mathrm{i}^{4k+1} = \mathrm{i},\ \mathrm{i}^{4k+2} = -1,\ \mathrm{i}^{4k+3} = 1 \ \text{ pro všechna } \ k \in \mathbb{N}_0,$$

dostaneme z binomické věty

$$(1+\mathrm{i})^n = \binom{n}{0} + \binom{n}{1}\mathrm{i} - \binom{n}{2} - \binom{n}{3}\mathrm{i} + \cdots + \binom{n}{n-1}\mathrm{i}^{n-1} + \binom{n}{n}\mathrm{i}^n. \tag{2.6}$$

Z goniometrického tvaru čísla $1+\mathrm{i} = \sqrt{2}\left(\cos\frac{\pi}{4} + \mathrm{i}\sin\frac{\pi}{4}\right)$ dostaneme pro jeho n-tou mocninu z Moivreovy věty druhé vyjádření

$$(1+\mathrm{i})^n = \left[\sqrt{2}\left(\cos\frac{\pi}{4} + \mathrm{i}\sin\frac{\pi}{4}\right)\right]^n = \left(\sqrt{2}\right)^n\left(\cos\frac{n\pi}{4} + \mathrm{i}\sin\frac{n\pi}{4}\right). \tag{2.7}$$

Porovnáním reálných a imaginárních částí obou vyjádření téže mocniny dostaneme

$$\mathrm{Re}\,(2.6) = \mathrm{Re}\,(2.7): \quad \binom{n}{0} - \binom{n}{2} + \binom{n}{4} + \ldots = \left(\sqrt{2}\right)^n \cos\frac{n\pi}{4}, \tag{2.8}$$

$$\mathrm{Im}\,(2.6) = \mathrm{Im}\,(2.7): \quad \binom{n}{1} - \binom{n}{3} + \binom{n}{5} + \ldots = \left(\sqrt{2}\right)^n \sin\frac{n\pi}{4}. \tag{2.9}$$

Sečtením a odečtením identit (2.4), resp. (2.5), a (2.8), resp. (2.9), a následným vydělením dvěma dostaneme následující čtyři identity.

$$\frac{(2.4)+(2.8)}{2}: \quad \binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \ldots = 2^{n-2} + \left(\sqrt{2}\right)^{n-2}\cos\frac{n\pi}{4}$$

$$\frac{(2.5)+(2.9)}{2}: \quad \binom{n}{1} + \binom{n}{5} + \binom{n}{9} + \ldots = 2^{n-2} + \left(\sqrt{2}\right)^{n-2}\sin\frac{n\pi}{4}$$

$$\frac{(2.4)-(2.8)}{2}: \quad \binom{n}{2} + \binom{n}{6} + \binom{n}{10} + \ldots = 2^{n-2} - \left(\sqrt{2}\right)^{n-2}\cos\frac{n\pi}{4}$$

$$\frac{(2.5)-(2.9)}{2}: \quad \binom{n}{3} + \binom{n}{7} + \binom{n}{11} + \ldots = 2^{n-2} - \left(\sqrt{2}\right)^{n-2}\sin\frac{n\pi}{4}$$

Pro odvození dalších identit označme

$$\omega = \cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3} = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2},$$

tedy ω je primitivní třetí odmocnina z jedné. Umocníme-li ω na n-tou, jednak v algebraickém tvaru podle binomické věty, jednak v goniometrickém podle Moivreovy věty, dostaneme rovnosti

$$\omega^n = \left(-\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}\right)^n = \binom{n}{0}\frac{(-1)^n}{2^n} + \binom{n}{1}\frac{(-1)^{n-1}\sqrt{3}}{2^n}\mathrm{i} - \binom{n}{2}\frac{(-1)^{n-2}\left(\sqrt{3}\right)^2}{2^n} - \\ - \binom{n}{3}\frac{(-1)^{n-3}\left(\sqrt{3}\right)^3}{2^n}\mathrm{i} + \ldots,$$

$$\omega^n = \left[\cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3}\right]^n = \cos\frac{2n\pi}{3} + \mathrm{i}\sin\frac{2n\pi}{3},$$

u kterých porovnáme reálné a imaginární části

$$\begin{aligned}
\cos\frac{2n\pi}{3} &= \binom{n}{0}\frac{(-1)^n}{2^n} - \binom{n}{2}\frac{(-1)^{n-2}\left(\sqrt{3}\right)^2}{2^n} + \binom{n}{4}\frac{(-1)^{n-4}\left(\sqrt{3}\right)^4}{2^n} - \\
&\quad - \binom{n}{6}\frac{(-1)^{n-6}\left(\sqrt{3}\right)^6}{2^n} + \dots \\
&= \frac{(-1)^n}{2^n}\left[\binom{n}{0} - 3\binom{n}{2} + 3^2\binom{n}{4} - 3^3\binom{n}{6} + \dots\right], \\
\sin\frac{2n\pi}{3} &= \binom{n}{1}\frac{(-1)^n\sqrt{3}}{2^n} - \binom{n}{3}\frac{(-1)^{n-3}\left(\sqrt{3}\right)^3}{2^n} + \binom{n}{5}\frac{(-1)^{n-5}\left(\sqrt{3}\right)^5}{2^n} - \\
&\quad - \binom{n}{7}\frac{(-1)^{n-7}\left(\sqrt{3}\right)^7}{2^n} + \dots \\
&= \frac{(-1)^{n-1}\sqrt{3}}{2^n}\left[\binom{n}{1} - 3\binom{n}{3} + 3^2\binom{n}{5} - 3^3\binom{n}{7} + \dots\right],
\end{aligned}$$

odkud dostáváme identity

$$\begin{aligned}
\binom{n}{0} - 3\binom{n}{2} + 3^2\binom{n}{4} - 3^3\binom{n}{6} + \dots &= (-1)^n 2^n \cos\frac{2n\pi}{3}, \\
\binom{n}{1} - 3\binom{n}{3} + 3^2\binom{n}{5} - 3^3\binom{n}{7} + \dots &= (-1)^{n-1}\frac{2^n}{\sqrt{3}}\sin\frac{2n\pi}{3}.
\end{aligned}$$

Spolu s ω uvažme nyní další vhodná komplexní čísla v algebraickém i goniometrickém tvaru:

$$\begin{aligned}
\omega &= -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2} = \cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3} \\
\omega^2 &= -\frac{1}{2} - \mathrm{i}\frac{\sqrt{3}}{2} = \cos\left(-\frac{2\pi}{3}\right) + \mathrm{i}\sin\left(-\frac{2\pi}{3}\right) \\
1+\omega &= \frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2} = \cos\frac{\pi}{3} + \mathrm{i}\sin\frac{\pi}{3} \\
1+\omega^2 &= \frac{1}{2} - \mathrm{i}\frac{\sqrt{3}}{2} = \cos\left(-\frac{\pi}{3}\right) + \mathrm{i}\sin\left(-\frac{\pi}{3}\right)
\end{aligned}$$

Umocněme na n-tou čísla $(1+1), (1+\omega)$ a $(1+\omega^2)$, tedy čísla jedna plus některá ze tří třetích odmocnin z jedné, opět v algebraickém i goniometrickém tvaru:

$$\begin{aligned}
(1+1)^n &= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \binom{n}{4} + \binom{n}{5} + \dots \\
(1+1)^n &= 2^n \\
(1+\omega)^n &= \binom{n}{0} + \binom{n}{1}\omega + \binom{n}{2}\omega^2 + \binom{n}{3} + \binom{n}{4}\omega + \binom{n}{5}\omega^2 + \dots \\
(1+\omega)^n &= \cos\frac{n\pi}{3} + \mathrm{i}\sin\frac{n\pi}{3}
\end{aligned}$$

$$(1+\omega^2)^n = \binom{n}{0} + \binom{n}{1}\omega^2 + \binom{n}{2}\omega + \binom{n}{3} + \binom{n}{4}\omega^2 + \binom{n}{5}\omega + \dots$$
$$(1+\omega^2)^n = \cos\left(-\frac{n\pi}{3}\right) + \mathrm{i}\sin\left(-\frac{n\pi}{3}\right) = \cos\frac{n\pi}{3} - \mathrm{i}\sin\frac{n\pi}{3}$$

Součet těchto tří mocnin $S_1 = (1+1)^n + (1+\omega)^n + (1+\omega^2)^n$ je, při využití rovnosti $1+\omega+\omega^2 = 0$, v algebraickém tvaru

$$\begin{aligned} S_1 &= \binom{n}{0}(1+1+1) + \binom{n}{1}(1+\omega+\omega^2) + \binom{n}{2}(1+\omega^2+\omega) + \\ &\quad + \binom{n}{3}(1+1+1) + \binom{n}{4}(1+\omega+\omega^2) + \binom{n}{5}(1+\omega^2+\omega) + \dots \\ &= 3\left[\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \dots\right] \end{aligned}$$

a v goniometrickém tvaru

$$S_1 = 2^n + \cos\frac{n\pi}{3} + \mathrm{i}\sin\frac{n\pi}{3} + \cos\frac{n\pi}{3} - \mathrm{i}\sin\frac{n\pi}{3} = 2^n + 2\cos\frac{n\pi}{3},$$

odkud porovnáním dostáváme identitu

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \dots = \frac{1}{3}\left[2^n + 2\cos\frac{n\pi}{3}\right].$$

Vynásobíme-li druhý, resp. třetí sčítanec, ω^2, resp. ω, dostaneme v algebraickém vyjádření zjevné tvary, v goniometrickém pak

$$\omega^2(1+\omega)^n = \left[\cos\frac{4\pi}{3} + \mathrm{i}\sin\frac{4\pi}{3}\right]\left[\cos\frac{n\pi}{3} + \mathrm{i}\sin\frac{n\pi}{3}\right] = \cos\frac{(n+4)\pi}{3} + \mathrm{i}\sin\frac{(n+4)\pi}{3},$$
$$\begin{aligned} \omega(1+\omega^2)^n &= \left[\cos\left(-\frac{4\pi}{3}\right) + \mathrm{i}\sin\left(-\frac{4\pi}{3}\right)\right]\left[\cos\left(-\frac{n\pi}{3}\right) + \mathrm{i}\sin\left(-\frac{n\pi}{3}\right)\right] = \\ &= \cos\left(-\frac{(n+4)\pi}{3}\right) + \mathrm{i}\sin\left(-\frac{(n+4)\pi}{3}\right) = \cos\frac{(n+4)\pi}{3} - \mathrm{i}\sin\frac{(n+4)\pi}{3}. \end{aligned}$$

Nový součet $S_2 = (1+1)^n + \omega^2(1+\omega)^n + \omega(1+\omega^2)^n$ je v algebraickém tvaru

$$\begin{aligned} S_2 &= \binom{n}{0}(1+\omega^2+\omega) + \binom{n}{1}(1+1+1) + \binom{n}{2}(1+\omega+\omega^2) + \\ &\quad + \binom{n}{3}(1+\omega^2+\omega) + \binom{n}{4}(1+1+1) + \binom{n}{5}(1+\omega+\omega^2) + \dots \\ &= 3\left[\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \dots\right] \end{aligned}$$

a v goniometrickém tvaru

$$\begin{aligned} S_2 &= 2^n + \cos\frac{(n+4)\pi}{3} + \mathrm{i}\sin\frac{(n+4)\pi}{3} + \cos\frac{(n+4)\pi}{3} - \mathrm{i}\sin\frac{(n+4)\pi}{3} = \\ &= 2^n + 2\cos\frac{(n+4)\pi}{3}, \end{aligned}$$

odkud porovnáním dostáváme identitu

$$\binom{n}{1}+\binom{n}{4}+\binom{n}{7}+\cdots=\frac{1}{3}\left[2^n+2\cos\frac{(n+4)\pi}{3}\right].$$

Proveďme nyní to samé, jen druhý, resp. třetí sčítanec, vynásobme ω, resp. ω^2.

$$\omega(1+\omega)^n=\left[\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}\right]\left[\cos\frac{n\pi}{3}+\mathrm{i}\sin\frac{n\pi}{3}\right]=\cos\frac{(n+2)\pi}{3}+\mathrm{i}\sin\frac{(n+2)\pi}{3}$$

$$\begin{aligned}\omega(1+\omega^2)^n&=\left[\cos\left(-\frac{2\pi}{3}\right)+\mathrm{i}\sin\left(-\frac{2\pi}{3}\right)\right]\left[\cos\left(-\frac{n\pi}{3}\right)+\mathrm{i}\sin\left(-\frac{n\pi}{3}\right)\right]=\\&=\cos\left(-\frac{(n+2)\pi}{3}\right)+\mathrm{i}\sin\left(-\frac{(n+2)\pi}{3}\right)=\cos\frac{(n+2)\pi}{3}-\mathrm{i}\sin\frac{(n+2)\pi}{3}\end{aligned}$$

Nový součet $S_3=(1+1)^n+\omega(1+\omega)^n+\omega^2(1+\omega^2)^n$ je v algebraickém tvaru

$$\begin{aligned}S_3&=\binom{n}{0}(1+\omega+\omega^2)+\binom{n}{1}(1+\omega^2+\omega)+\binom{n}{2}(1+1+1)+\\&\quad+\binom{n}{3}(1+\omega+\omega^2)+\binom{n}{4}(1+\omega^2+\omega)+\binom{n}{5}(1+1+1)+\ldots\\&=3\left[\binom{n}{2}+\binom{n}{5}+\binom{n}{8}+\ldots\right]\end{aligned}$$

a v goniometrickém tvaru

$$\begin{aligned}S_3&=2^n+\cos\frac{(n+2)\pi}{3}+\mathrm{i}\sin\frac{(n+2)\pi}{3}+\cos\frac{(n+2)\pi}{3}-\mathrm{i}\sin\frac{(n+2)\pi}{3}=\\&=2^n+2\cos\frac{(n+2)\pi}{3},\end{aligned}$$

odkud porovnáním dostáváme poslední identitu

$$\binom{n}{2}+\binom{n}{5}+\binom{n}{8}+\cdots=\frac{1}{3}\left[2^n+2\cos\frac{(n+2)\pi}{3}\right].$$

2.2 Počty prvků ve zbytkových třídách

Jak jsme zmínili již v první kapitole, lze díky izomorfnosti grupy zbytkových tříd $\mathbb{Z}_n$ se sčítáním a grupy n-tých odmocnin z jedné $\left\{\sqrt[n]{1}\right\}$ s násobením s výhodou reprezentovat příslušnost čísla k nějaké zbytkové třídě podle daného modulu n mocninou pevně zvolené primitivní n-té odmocniny z jedné. Zde si ukážeme několik příkladů využívajících nejen vlastností odmocnin z jedné, ale i dříve uvedených pomocných tvrzení. Tato méně tradiční problematika je v našem textu zpracována dle [1, Chapter 7].

Příklad 1. Kolik n-ciferných číslech složených z cifer $1,3,4,6,7,9$ má ciferný součet dělitelný sedmi?

Řešení. Označme $a_n^{(k)}$ počet n-ciferných čísel složených z cifer $1,3,4,6,7,9$, jejichž ciferný součet je kongruentní s k modulo 7. Námi hledaný počet je pak $a_n^{(0)}$. Dále označme ε primitivní sedmou odmocninu z jedné. Pomocí ε budeme reprezentovat příslušnost čísel k jednotlivým zbytkovým třídám modulo 7: číslům kongruentním s $0,1,2,\ldots,6$ budou po řadě odpovídat mocniny $\varepsilon^0 = 1, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^6$.
Uvažme nyní sumu

$$\sum_{k=0}^{6} a_n^{(k)} \varepsilon^k,$$

v níž jsou jednotlivá n-ciferná čísla s ciferným součtem kongruentním s k modulo 7 reprezentována svým počtem $a_n^{(k)}$ a mocninou ε^k.
Ke stejnému součtu se dostaneme, budeme-li přes všechna jednotlivá n-ciferná čísla z těchto cifer sčítat mocniny ε s exponentem rovným nikoliv zbytku k ciferného součtu po dělení sedmi, nýbrž rovným přímo ciferném součtu $c_1 + c_2 + \cdots + c_n$, neboť $\varepsilon^7 = 1$, a tedy $\varepsilon^{c_1+c_2+\cdots+c_n} = \varepsilon^k$. Dostaneme tak rovnost komplexních čísel

$$\sum_{k=0}^{6} a_n^{(k)} \varepsilon^k = \sum_{c_1,c_2,\ldots,c_n \in \{1,3,4,6,7,9\}} \varepsilon^{c_1+c_2+\cdots+c_n}.$$

Protože $\varepsilon^{c_1+c_2+\cdots+c_n} = \varepsilon^{c_1} \cdot \varepsilon^{c_2} \cdot \ldots \cdot \varepsilon^{c_n}$, můžeme si tuto sumu představit jako součet všech součinů čísel z uspořádaných n-tic složených z $\varepsilon^1, \varepsilon^3, \varepsilon^4, \varepsilon^6, \varepsilon^7, \varepsilon^9$, přičemž každé pořadí s opakováním je tam právě jednou. To ale není nic jiného, než rozepsání mocniny $\left(\varepsilon^1 + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 + \varepsilon^9\right)^n$ roznásobením na jednotlivé členy. Tedy

$$\sum_{c_1,c_2,\ldots,c_n \in \{1,3,4,6,7,9\}} \varepsilon^{c_1+c_2+\cdots+c_n} = \left(\varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 + \varepsilon^9\right)^n.$$

Protože $\varepsilon^7 = 1$, $\varepsilon^9 = \varepsilon^2$ a $1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^5 + \varepsilon^6 = 0$, dostaneme

$$\varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 + \varepsilon^9 = 1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 = -\varepsilon^5.$$

Docházíme tak k rovnosti komplexních čísel

$$\sum_{k=0}^{6} a_n^{(k)} \varepsilon^k = \left(-\varepsilon^5\right)^n,$$

s neznámými celočíselnými koeficienty $a_n^{(k)}$.
Nyní musíme rozlišit jednotlivé případy v závislosti na tom, jaký zbytek dává n po dělení číslem 7. Rozebereme tedy 7 případů, kdy $n = 7r + s, s \in \{0,1,\ldots,6\}$.
Ve všech případech provedeme následující úpravu:

$$\left(-\varepsilon^5\right)^n = (-1)^n \left(\varepsilon^5\right)^n = (-1)^n \left(\varepsilon^5\right)^{7r+s} = (-1)^n \left(\varepsilon^7\right)^{5r} \varepsilon^{5s} = (-1)^n \varepsilon^{5s}$$

i.) $n \equiv 0 \pmod 7$, tj. $n = 7r+0, r \in \mathbb{N}$.

$$\sum_{k=0}^{6} a_n^{(k)} \varepsilon^k = (-1)^n \varepsilon^0 = (-1)^n \quad \text{neboli} \quad \sum_{k=0}^{6} a_n^{(k)} \varepsilon^k - (-1)^n = 0.$$

Rozepsáním sumy

$$a_n^{(0)} - (-1)^n + a_n^{(1)}\varepsilon^1 + a_n^{(2)}\varepsilon^2 + a_n^{(3)}\varepsilon^3 + a_n^{(4)}\varepsilon^4 + a_n^{(5)}\varepsilon^5 + a_n^{(6)}\varepsilon^6 = 0$$

vidíme, že můžeme použít Větu 1.56, ze které plyne

$$a_n^{(0)} - (-1)^n = a_n^{(1)} = a_n^{(2)} = a_n^{(3)} = a_n^{(4)} = a_n^{(5)} = a_n^{(6)}.$$

Protože se těchto sedm hodnot rovná, je jejich součet roven sedminásobku první hodnoty:

$$7\left[a_n^{(0)} - (-1)^n\right] = \sum_{k=0}^{6} a_n^{(k)} - (-1)^n$$

Suma $\sum_{k=0}^{6} a_n^{(k)}$ reprezentuje součet počtů n-ciferných čísel tvořených ciframi $1,3,4,6,7,9$, jež postupně dávají zbytek $0,1,\ldots,6$ po dělení číslem 7. Udává tedy celkový počet n-ciferných čísel z těchto cifer. Protože žádná z nich není nula, je takových n-ciferných čísel právě 6^n.
Nyní už jen dosadíme za sumu do poslední rovnosti a vyjádříme $a_n^{(0)}$.

$$7\left[a_n^{(0)} - (-1)^n\right] = 6^n - (-1)^n, \quad \text{odkud} \quad a_n^{(0)} = \frac{6^n - (-1)^n}{7} + (-1)^n.$$

ii.) $n \equiv 1 \pmod 7$, tj. $n = 7r+1, r \in \mathbb{N}_0$.
Budeme postupovat analogicky dle výše uvedených úvah, které již zapisovat nebudeme.

$$\sum_{k=0}^{6} a_n^{(k)} \varepsilon^k = (-1)^n \varepsilon^5$$

$$a_n^{(0)} = a_n^{(1)} = a_n^{(2)} = a_n^{(3)} = a_n^{(4)} = a_n^{(5)} - (-1)^n = a_n^{(6)}$$

$$7a_n^{(0)} = \sum_{k=0}^{6} a_n^{(k)} - (-1)^n = 6^n - (-1)^n \;\Rightarrow\; a_n^{(0)} = \frac{6^n - (-1)^n}{7}$$

Je zřejmé, že rovněž v ostatních případech $n \equiv 2, 3, 4, 5$ a $6 \pmod 7$ dostaneme stejné vyjádření počtu, neboť číslo $(-1)^n$ se jen bude v rozepsané sumě přesouvat postupně k $a_n^{(3)}$, $a_n^{(1)}$, $a_n^{(6)}$, $a_n^{(4)}$ a $a_n^{(2)}$, ovšem další kroky výpočtu již budou shodné.

Shrnutí: počet $a_n^{(0)}$ n-ciferných čísel složených z cifer $1,3,4,6,7,9$ jejichž ciferný součet je dělitelný sedmi, je pro dané $n \in \mathbb{N}$ roven

$$a_n^{(0)} = \frac{6^n - (-1)^n}{7} + (-1)^n \quad \text{pro } n \equiv 0 \pmod 7;$$

$$a_n^{(0)} = \frac{6^n - (-1)^n}{7} \quad \text{pro } n \not\equiv 0 \pmod 7.$$

■

Příklad 2. Hodíme n-krát po sobě obvyklou hrací kostkou. Jaká je při daném n pravděpodobnost, že součet padlých čísel bude dělitelný pěti?

Řešení. Na začátek podotkněme, že házíme klasickou kostkou s čísly $1,2,3,4,5,6$, přičemž každé číslo má stejnou pravděpodobnost, že padne, a pro výpočet užíváme klasickou pravděpodobnost, která je rovna podílu počtu všech příznivých ku počtu všech možných výsledků.
Označme $a_n^{(k)}$ počet sérií n-hodů kostkou po sobě, dále říkejme n-hodů, u nichž součet padlých čísel je kongruentní s k modulo 5. Číslo $a_n^{(0)}$ pak označuje počet všech příznivých n-hodů. Dále označme ε primitivní pátou odmocninu z jedné. Pomocí ε budeme reprezentovat příslušnost padlých čísel k jednotlivým zbytkovým třídám modulo 5: číslům kongruentním s $0,1,2,3,4$ budou po řadě odpovídat mocniny $\varepsilon^0 = 1, \varepsilon^1, \varepsilon^2, \varepsilon^3, \varepsilon^4$.
Uvažme nyní sumu

$$\sum_{k=0}^{4} a_n^{(k)} \varepsilon^k,$$

v níž jsou jednotlivé n-hody se součtem padlých čísel kongruentním s k modulo 5 reprezentovány svým počtem $a_n^{(k)}$ a mocninou ε^k.
Ke stejnému součtu se dostaneme, budeme-li přes všech 6^n jednotlivých n-hodů sčítat mocniny ε s exponentem rovným nikoliv zbytku k součtu padlých čísel po dělení pěti, nýbrž rovným přímo součtu $c_1 + c_2 + \cdots + c_n$ padlých čísel, neboť $\varepsilon^5 = 1$, a tedy $\varepsilon^{c_1+c_2+\cdots+c_n} = \varepsilon^k$.
Dostaneme tak rovnost komplexních čísel

$$\sum_{k=0}^{4} a_n^{(k)} \varepsilon^k = \sum_{c_1,c_2,\ldots,c_n \in \{1,2,3,4,5,6\}} \varepsilon^{c_1+c_2+\cdots+c_n}.$$

Protože $\varepsilon^{c_1+c_2+\cdots+c_n} = \varepsilon^{c_1} \cdot \varepsilon^{c_2} \cdot \ldots \cdot \varepsilon^{c_n}$, můžeme si tuto sumu představit jako součet všech součinů čísel z uspořádaných n-tic složených z $\varepsilon^1, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6$, přičemž každé pořadí s opakováním je tam právě jednou. To ale není nic jiného, než rozepsání mocniny $\left(\varepsilon^1 + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^5 + \varepsilon^6\right)^n$ roznásobením na jednotlivé členy. Platí tedy rovnost

$$\sum_{c_1,c_2,\ldots,c_n \in \{1,2,3,4,5,6\}} \varepsilon^{c_1+c_2+\cdots+c_n} = \left(\varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^5 + \varepsilon^6\right)^n.$$

Protože $\varepsilon^5 = 1$, $\varepsilon^6 = \varepsilon$ a $1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = 0$, dostaneme

$$\varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^5 + \varepsilon^6 = 1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon = \varepsilon.$$

Docházíme tak k rovnosti komplexních čísel

$$\sum_{k=0}^{4} a_n^{(k)} \varepsilon^k = \varepsilon^n,$$

s neznámými celočíselnými koeficienty $a_n^{(k)}$ splňujícími podmínku

$$a_n^{(0)} + a_n^{(1)} + a_n^{(2)} + a_n^{(3)} + a_n^{(4)} = \sum_{k=0}^{4} a_n^{(k)} = 6^n,$$

neboť počet všech n-hodů je právě 6^n.
Nyní musíme rozlišit jednotlivé případy v závislosti na tom, jaký zbytek dává n po dělení číslem 5. Rozebereme tedy 5 případů, kdy $n = 5r+s, s \in \{0,1,\ldots,4\}$. Uvážíme při tom, že z periodičnosti mocnin ε plyne $\varepsilon^n = \varepsilon^{5r+s} = \varepsilon^s$.
i.) $n \equiv 0 \pmod 5$, tj. $n = 5r+0, r \in \mathbb{N}$.

$$\sum_{k=0}^{4} a_n^{(k)} \varepsilon^k = \varepsilon^0 = 1 \quad \text{neboli} \quad \sum_{k=0}^{4} a_n^{(k)} \varepsilon^k - 1 = 0.$$

Rozepsáním sumy

$$a_n^{(0)} - 1 + a_n^{(1)}\varepsilon^1 + a_n^{(2)}\varepsilon^2 + a_n^{(3)}\varepsilon^3 + a_n^{(4)}\varepsilon^4 = 0$$

vidíme, že můžeme použít Větu 1.56, ze které plyne

$$a_n^{(0)} - 1 = a_n^{(1)} = a_n^{(2)} = a_n^{(3)} = a_n^{(4)}.$$

Protože se těchto pět hodnot rovná, je jejich součet roven pětinásobku první hodnoty:

$$5\left[a_n^{(0)} - 1\right] = \sum_{k=0}^{4} a_n^{(k)} - 1 = 6^n - 1,$$

kde jsme využili výše zmíněného poznatku o počtu všech n-hodů.
Z této rovnosti pro $a_n^{(0)}$ dostáváme vyjádření

$$a_n^{(0)} = \frac{6^n + 4}{5}.$$

Hledaná pravděpodobnost P_n je tak v případě $n = 5r, r \in \mathbb{N}$, rovna

$$P_n = \frac{a_n^{(0)}}{6^n} = \frac{1}{5} + \frac{4}{5 \cdot 6^n}.$$

ii.) $n \equiv 1 \pmod 5$, tj. $n = 5r+1, r \in \mathbb{N}_0$.
Budeme postupovat analogicky dle výše uvedených úvah, které již zapisovat nebudeme.

$$\sum_{k=0}^{4} a_n^{(k)} \varepsilon^k = \varepsilon.$$

$$a_n^{(0)} = a_n^{(1)} - 1 = a_n^{(2)} = a_n^{(3)} = a_n^{(4)}.$$

$$5a_n^{(0)} = \sum_{k=0}^{4} a_n^{(k)} - 1 = 6^n - 1 \;\Rightarrow\; a_n^{(0)} = \frac{6^n - 1}{5}$$

$$P_n = \frac{a_n^{(0)}}{6^n} = \frac{1}{5} - \frac{1}{5 \cdot 6^n}.$$

Je zřejmé, že rovněž v ostatních případech $n = 5r+s$, kde $s \in \{2,3,4\}$ dostaneme stejné vyjádření pravděpodobnosti, neboť číslo -1 se jen bude v rozepsané sumě přesouvat postupně k $a_n^{(2)}, a_n^{(3)}, a_n^{(4)}$, ovšem další kroky výpočtu již budou shodné.

Shrnutí: pravděpodobnost P_n toho, že součet padlých čísel při n hodech kostkou bude dělitelný pěti, je pro dané $n \in \mathbb{N}$ rovna

$$P_n = \frac{1}{5} + \frac{4}{5 \cdot 6^n} \quad \text{pro } n \equiv 0 \pmod 5;$$
$$P_n = \frac{1}{5} - \frac{1}{5 \cdot 6^n} \quad \text{pro } n \not\equiv 0 \pmod 5.$$

Vidíme, že s rostoucím n tato pravděpodobnost rychle konverguje k očekávatelné hodnotě $0,2$, přičemž pro n dělitelná pěti konverguje shora, pro ostatní n zdola. Význačné odchylky jsou ale pouze u $P_1 \doteq 0,167$ a $P_2 \doteq 0,194$. Od $n = 3$ je již odchylka menší než $0,001$ a od $n = 12$ dokonce než 10^{-10}. ■

Příklad 3. Nechť $p > 2$ je prvočíslo. Kolik existuje p-prvkových podmnožin množiny $A = \{1, 2, \ldots, 2p\}$ takových, že součet jejích prvků je dělitelný p?

Řešení. Označme $a_p^{(k)}$ počet p-prvkových podmnožin B množiny A takových, že součet $m(B)$ jejích prvků je kongruentní s k modulo p, tedy $|B| = p$ a $m(B) \equiv k \pmod p$. Námi hledaný počet je pak $a_p^{(0)}$. Dále označme ε primitivní p-tou odmocninu z jedné. Pomocí ε budeme reprezentovat příslušnost podmnožin k jednotlivým zbytkovým třídám modulo p: podmnožinám se součtem prvků kongruentním s $k \in \{0, 1, \ldots, p-1\}$ bude odpovídat mocnina ε^k.
Uvažme nyní sumu

$$\sum_{k=0}^{p-1} a_p^{(k)} \varepsilon^k,$$

v níž jsou jednotlivé p-prvkové podmnožiny se součtem prvků kongruentním s k modulo p reprezentovány svým počtem $a_p^{(k)}$ a mocninou ε^k.
Ke stejnému součtu se dostaneme, budeme-li přes všechny jednotlivé p-prvkové podmnožiny B množiny A sčítat mocniny ε s exponentem rovným nikoliv zbytku k součtu $m(B)$ po dělení číslem p, nýbrž rovným přímo součtu $m(B)$, neboť $\varepsilon^p = 1$, a tedy $\varepsilon^{m(B)} = \varepsilon^k$. Dostaneme tak rovnost komplexních čísel

$$\sum_{k=0}^{p-1} a_p^{(k)} \varepsilon^k = \sum_{B \subset A, |B|=p} \varepsilon^{m(B)}.$$

Jelikož součet prvků $m(B)$ je tvořen vždy p různými sčítanci od 1 do $2p$ a každá taková možná p-tice se v sumě vyskytuje právě jednou, můžeme tuto sumu přes podmnožiny B nahradit sumou přes všechny možné kombinace p čísel od 1 do $2p$:

$$\sum_{B \subset A, |B|=p} \varepsilon^{m(B)} = \sum_{1 \le c_1 < c_2 < \cdots < c_p \le 2p} \varepsilon^{c_1 + c_2 + \cdots + c_p}.$$

Po úpravě $\varepsilon^{c_1+c_2+\cdots+c_p} = \varepsilon^{c_1} \cdot \varepsilon^{c_2} \cdot \ldots \cdot \varepsilon^{c_p}$ vidíme, že v sumě máme všechny součiny p po dvou různých mocnin ε s exponenty od 1 do $2p$. Tato suma tak není nic jiného, než koeficient u x^p v polynomu

$$(x + \varepsilon)\left(x + \varepsilon^2\right) \cdots \left(x + \varepsilon^{2p}\right).$$

Z Lemmatu 1.58 plyne, že

$$(x+\varepsilon)\left(x+\varepsilon^2\right)\cdots\left(x+\varepsilon^{2p}\right)=\left(x^p+1\right)^2=x^{2p}+2x^p+1,$$

tudíž koeficient u x^p je 2.
Celkem

$$\sum_{k=0}^{p-1}a_p^{(k)}\varepsilon^k=2.$$

S užitím Věty 1.56 dostáváme

$$a_p^{(0)}-2=a_p^{(1)}=\cdots=a_p^{(p-1)}.$$

Všech p-prvkových podmnožin B $2p$-prvkové množiny A je právě $\binom{2p}{p}$, takže

$$a_p^{(0)}+a_p^{(1)}+\cdots+a_p^{(p-1)}=\binom{2p}{p}.$$

Dosadíme-li sem za $a_p^{(1)},\ldots,a_p^{(p-1)}$ hodnotu $a_p^{(0)}-2$, dostaneme

$$a_p^{(0)}+\left(a_p^{(0)}-2\right)+\cdots+\left(a_p^{(0)}-2\right)=\binom{2p}{p},\quad\text{odkud}\quad a_p^{(0)}=2+\frac{1}{p}\left[\binom{2p}{p}-2\right].\ \blacksquare$$

Příklad 4. Nechť $p>2$ je prvočíslo, nechť m,n jsou přirozené násobky p a n je liché. Pro každou funkci $f\colon\{1,2,\ldots,m\}\to\{1,2,\ldots,n\}$ splňující $\sum_{i=1}^{m}f(i)\equiv 0\pmod p$ uvažme součin $\prod_{i=1}^{m}f(i)$. Dokažte, že součet všech těchto součinů odpovídajících všem takovým funkcím f je dělitelný číslem $\left(\frac{n}{p}\right)^m$.

Řešení. Pro $k=0,1,\ldots,p-1$ označme $s_p^{(k)}$ součet všech součinů $\prod_{i=1}^{m}f(i)$ všech funkcí $f\colon\{1,2,\ldots,m\}\to\{1,2,\ldots,n\}$ takových, že $\sum_{i=1}^{m}f(i)\equiv k\pmod p$. Uvažovaný součet je pak $s_p^{(0)}$. Dále označme ε primitivní p-tou odmocninu z jedné. Pomocí ε budeme reprezentovat příslušnost funkcí k jednotlivým zbytkovým třídám modulo p: funkcím se součtem funkčních hodnot kongruentním s $k\in\{0,1,\ldots,p-1\}$ bude odpovídat mocnina ε^k.
Uvažme nyní sumu

$$\sum_{k=0}^{p-1}s_p^{(k)}\varepsilon^k,$$

v níž jsou jednotlivé funkce se součtem funkčních hodnot kongruentním s k modulo p reprezentovány součtem $s_p^{(k)}$ součinů svých funkčních hodnot a mocninou ε^k.
Ke stejnému součtu se dostaneme, budeme-li přes všechny jednotlivé funkce f sčítat součiny $a_1a_2\ldots a_m$ jejich funkčních hodnot vynásobené mocninou ε s exponentem rovným

nikoliv zbytku k součtu funkčních hodnot po dělení číslem p, nýbrž rovným přímo součtu $a_1+a_2+\cdots+a_m$ funkčních hodnot, neboť $\varepsilon^p=1$, a tedy $\varepsilon^{a_1+a_2+\cdots+a_m}=\varepsilon^k$. Dostaneme tak rovnost komplexních čísel

$$\sum_{k=0}^{p-1} s_p^{(k)}\varepsilon^k = \sum_{a_1,a_2,\ldots,a_m\in\{1,2,\ldots,n\}} a_1a_2\cdots a_m\varepsilon^{a_1+a_2+\cdots+a_m}.$$

Protože $a_1a_2\cdots a_m\varepsilon^{a_1+a_2+\cdots+a_m}=\left(a_1\varepsilon^{a_1}\right)\left(a_2\varepsilon^{a_2}\right)\cdots\left(a_m\varepsilon^{a_m}\right)$, můžeme si tuto sumu představit jako součet všech součinů čísel z uspořádaných m-tic složených z $1\varepsilon^1,2\varepsilon^2,\ldots,n\varepsilon^n$, přičemž každé pořadí s opakováním je tam právě jednou. To ale není nic jiného, než rozepsání mocniny $\left(\varepsilon+2\varepsilon^2+\cdots+n\varepsilon^n\right)^m$ roznásobením na jednotlivé členy. Tedy

$$\sum_{a_1,a_2,\ldots,a_m\in\{1,2,\ldots,n\}} a_1a_2\cdots a_m\varepsilon^{a_1+a_2+\cdots+a_m} = \left(\varepsilon+2\varepsilon^2+\cdots+n\varepsilon^n\right)^m.$$

Dosadíme-li do identity z Lemmatu 1.57

$$1q+2q^2+\cdots+nq^n=\frac{nq^{n+2}-(n+1)q^{n+1}+q}{(q-1)^2}$$

komplexní číslo $q=\varepsilon\neq 1$, dostaneme s ohledem na $\varepsilon^n=1$ rovnost

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

ze které po umocnění na m-tou s ohledem na $\varepsilon^m=1$ vychází

$$\left(\varepsilon+2\varepsilon^2+\cdots+n\varepsilon^n\right)^m=\left(\frac{n\varepsilon}{\varepsilon-1}\right)^m=\frac{n^m}{(\varepsilon-1)^m}.$$

Celkem

$$\sum_{k=0}^{p-1} s_p^{(k)}\varepsilon^k=\frac{n^m}{(\varepsilon-1)^m}.$$

K rozvinutí získaného zlomku do mocnin čísla ε využijeme speciálního mnohočlenu z Lemmatu 1.59, který umocníme na m-tou. Z binomické věty plyne, že existují celá čísla b_j, $j=1,2,\ldots,m(p-2)$, taková, že platí rovnost polynomů

$$\left(x^{p-2}+2x^{p-3}+\cdots+(p-2)x+p-1\right)^m=b_0+b_1x+\cdots+b_{m(p-2)}x^{m(p-2)}.$$

Odtud po dosazení $x=\varepsilon$ a využití periodičnosti mocnin ε dostaneme

$$\left(\varepsilon^{p-2}+2\varepsilon^{p-3}+\cdots+(p-2)\varepsilon+p-1\right)^m=c_0+c_1\varepsilon+\cdots+c_{p-1}\varepsilon^{p-1},$$

kde $c_i = \sum_{i \equiv j \pmod p} b_j$ je celé číslo pro každé $i = 0, 1, \ldots, p-1$.
Využijeme-li nyní vzorec z Lemmatu 1.59 umocněný na m-tou, dostáváme

$$\begin{aligned}\frac{1}{(\varepsilon-1)^m} &= \left(-\frac{1}{p}\right)^m \left(\varepsilon^{p-2} + 2\varepsilon^{p-3} + \cdots + (p-2)\varepsilon + p - 1\right)^m \\ &= \left(-\frac{1}{p}\right)^m \left(c_0 + c_1\varepsilon + \cdots + c_{p-1}\varepsilon^{p-1}\right),\end{aligned}$$

z čehož po vynásobení n^m máme rovnost

$$\sum_{k=0}^{p-1} s_p^{(k)} \varepsilon^k = \frac{n^m}{(\varepsilon-1)^m} = \left(-\frac{n}{p}\right)^m \left(c_0 + c_1\varepsilon + \cdots + c_{p-1}\varepsilon^{p-1}\right).$$

Označme $r = \left(-\frac{n}{p}\right)^m$. Je zřejmé, že dělitelnost celými čísly $\left(\frac{n}{p}\right)^m$ a r je ekvivalentní, můžeme tedy dokazovat, že $r \mid s_p^{(0)}$.
Rovnost

$$\sum_{k=0}^{p-1} s_p^{(k)} \varepsilon^k = r\left(c_0 + c_1\varepsilon + \cdots + c_{p-1}\varepsilon^{p-1}\right),$$

v níž, jak víme, nejen neznámé součty $s_p^{(k)}$, ale i koeficienty c_j, jsou celá čísla, můžeme upravit na

$$\left(s_p^{(0)} - rc_0\right) + \left(s_p^{(1)} - rc_1\right)\varepsilon + \cdots + \left(s_p^{(p-1)} - rc_{p-1}\right)\varepsilon^{p-1} = 0$$

a užít Větu 1.56, podle které platí

$$s_p^{(0)} - rc_0 = s_p^{(1)} - rc_1 = \cdots = s_p^{(p-1)} - rc_{p-1}.$$

Označíme-li $k = s_p^{(0)} - rc_0 = \cdots = s_p^{(p-1)} - rc_{p-1}$, pak z případného $r \mid k$ již vyplyne potřebné $r \mid s_p^{(0)}$. Naším cílem je tak dokázat, že $r \mid k$. Z definice čísla k plyne, že jeho p-násobek má vyjádření

$$pk = s_p^{(0)} + s_p^{(1)} + \cdots + s_p^{(p-1)} - r\left(c_0 + c_1 + \cdots + c_{p-1}\right).$$

Stejnou úvahou jako při součtu $\sum_{k=0}^{p-1} s_p^{(k)} \varepsilon^k = \left(\varepsilon + 2\varepsilon^2 + \cdots + n\varepsilon^n\right)^m$, akorát bez mocnin ε, dospějeme k rovnosti

$$s_p^{(0)} + s_p^{(1)} + \cdots + s_p^{(p-1)} = (1 + 2 + \cdots + n)^m = \left(\frac{n(n+1)}{2}\right)^m.$$

Ze zavedení čísel c_i plyne, že $c_0 + c_1 + \cdots + c_{p-1} = b_0 + b_1 + \cdots + b_{m(p-2)}$, a z uvažovaného polynomu při $x = 1$ dostaneme $b_0 + b_1 + \cdots + b_{m(p-2)} = (1 + 2 + \cdots + p - 1)^m$.
Porovnáním vychází

$$c_0 + c_1 + \cdots + c_{p-1} = \left(\frac{p(p-1)}{2}\right)^m.$$

Dosadíme-li dvě odvozené rovnosti do původního vyjádření pk, dostaneme

$$pk = \left(\frac{n(n+1)}{2}\right)^m - r\left(\frac{p(p-1)}{2}\right)^m \Rightarrow k = r\left[(-1)^m\left(\frac{n+1}{2}\right)^m - \left(\frac{p-1}{2}\right)^m\right]p^{m-1}.$$

Vzhledem k předpokladu, že p a n jsou lichá čísla, odtud již plyne, že $r \mid k$, což, jak víme, dokazuje požadované tvrzení. ■

2.3 Pokrývání šachovnic

V této části kapitoly věnované ukázkám kombinatorického užití komplexních čísel se podíváme, jak tato čísla můžeme – poněkud nečekaně – uplatnit při řešení úloh o pokrývání šachovnic obecných rozměrů soustavami šachovnic menších zadaných rozměrů. Omezíme se přitom na případy, kdy budeme čtvercové či obdélníkové šachovnice, s případnými vynechanými poli, pokrývat pouze obdélníčky, jejichž jeden rozměr je roven jedné a budeme je moci klást na šachovnici jen v jednom směru. Budeme tedy hovořit o šachovnicích $m \times n$ o m řádcích a n sloupcích a obdélníčcích $1 \times x$ ve vodorovném a $y \times 1$ ve svislém směru. Tato problematika vychází z [1, Chapter 7], odkud jsou převzaty a rozpracovány Příklady 5 a 6, a námi je poté dále rozvedena k větší obecnosti v Příkladech 7 a 8. Jedná se o přesun od zjišťování existence zaplnění pro konkrétní velikost šachovnice a zadané pozice vynechaných polí ke hledání všech možných pozic vynechaných polí na obdélníkové šachovnici obecných rozměrů.

Příklad 5. Určete nutnou a dostatečnou podmínku na čísla $m,n,x,y \in \mathbb{N}$ k tomu, aby bylo možné zaplnit šachovnici $m \times n$ obdélníčky $1 \times x$ a $y \times 1$.

Řešení. V případě $x = 1$ nebo $y = 1$ lze zřejmě zaplnit obdélníčky 1×1 šachovnici libovolných rozměrů. Dále tedy řešme případ $x \neq 1$ a $y \neq 1$.
Označme ε_1 primitivní y-tou odmocninu z jedné a ε_2 primitivní x-tou odmocninu z jedné. Pomocí jejich mocnin zaplňme celou šachovnici, a to tak, že do pole na souřadnicích (k,j) vepišme číslo $\varepsilon_1^k\varepsilon_2^j$.
Nejprve ukažme, že čísla v každém obdélníčku $1 \times x$ či $y \times 1$ dávají součet 0. Připomeňme, že dle Věty 1.41 platí $1+\varepsilon_2+\cdots+\varepsilon_2^{x-1} = 0$ a $1+\varepsilon_1+\cdots+\varepsilon_1^{y-1} = 0$.
Obdélníček $1 \times x$ začínající na pozici (k,j):

$$\varepsilon_1^k\varepsilon_2^j + \varepsilon_1^k\varepsilon_2^{j+1} + \cdots + \varepsilon_1^k\varepsilon_2^{j+x-1} = \varepsilon_1^k\varepsilon_2^j\left(1+\varepsilon_2+\cdots+\varepsilon_2^{x-1}\right) = \varepsilon_1^k\varepsilon_2^j \cdot 0 = 0$$

Obdélníček $y \times 1$ začínající na pozici (k,j):

$$\varepsilon_1^k\varepsilon_2^j + \varepsilon_1^{k+1}\varepsilon_2^j + \cdots + \varepsilon_1^{k+y-1}\varepsilon_2^j = \varepsilon_1^k\varepsilon_2^j\left(1+\varepsilon_1+\cdots+\varepsilon_1^{y-1}\right) = \varepsilon_1^k\varepsilon_2^j \cdot 0 = 0$$

Z právě dokázané vlastnosti plyne: Abychom mohli požadovaným způsobem zaplnit celou šachovnici, musí být součet všech mn čísel do této šachovnice vepsaných nulový.
Součet S všech čísel vepsaných do šachovnice lze vyjádřit jako

$$S = \left(\varepsilon_1+\varepsilon_1^2+\cdots+\varepsilon_1^m\right)\left(\varepsilon_2+\varepsilon_2^2+\cdots+\varepsilon_2^n\right),$$

neboť součin k-tého sčítance ε_1^k z prvního činitele a j-tého sčítance ε_2^j z druhého činitele je roven právě číslu $\varepsilon_1^k\varepsilon_2^j$ zapsanému na pozici (k,j). Vidíme, že jde o součin dvou součtů m a n po sobě jdoucích členů geometrických posloupností, první má úvodní člen i kvocient ε_1, druhá má úvodní člen i kvocient ε_2, přičemž díky $x \neq 1$ a $y \neq 1$ je $\varepsilon_1 \neq 1$ a $\varepsilon_2 \neq 1$. Užijeme tedy vzorec pro součet členů geometrické posloupnosti a dostaneme

$$S = \varepsilon_1 \cdot \frac{\varepsilon_1^m - 1}{\varepsilon_1 - 1} \cdot \varepsilon_2 \cdot \frac{\varepsilon_2^n - 1}{\varepsilon_1 - 1}.$$

Má-li být součet S nulový, musí být $\varepsilon_1^m - 1 = 0$ nebo $\varepsilon_2^n - 1 = 0$, tedy $\varepsilon_1^m = 1$ nebo $\varepsilon_2^n = 1$. Protože jsou ε_1 a ε_2 primitivní, je to podle Věty 1.38 ekvivalentní s tím, že $x \mid n$ nebo $y \mid m$. Dostali jsme tak nutnou podmínku k tomu, aby bylo možné zaplnit šachovnici $m \times n$ obdélníčky $1 \times x$ a $y \times 1$. Jde však i o podmínku dostatečnou, neboť v případě $x \mid n$, resp. $y \mid m$, můžeme celou šachovnici zřejmě zaplnit pouze obdélníčky $1 \times x$, resp. $y \times 1$. Protože jednička dělí libovolné přirozené číslo, je tato podmínka v souladu i se speciálními případy $x = 1$ nebo $y = 1$.
Podmínka $x \mid n$ nebo $y \mid m$ je tedy nutná a dostatečná k tomu, aby bylo možné zaplnit šachovnici $m \times n$ obdélníčky $1 \times x$ a $y \times 1$. ■

Příklad 6. Můžeme zaplnit šachovnici 13×13, ze které jsme odstranili středové pole, obdélníčky 1×4 a 4×1?

Řešení. Budeme postupovat podobně jako v předchozím příkladě. Využijeme zde mocnin primitivní čtvrté odmocniny z jedné (pro jednoduchost zvolme hodnotu i), kterými vyplníme celou šachovnici 13×13 tak, že do pole na souřadnicích (k,j) vepíšeme číslo i^{k+2j}.[1]
Je to obdoba řešení z Příkladu 5 pro $\varepsilon_1 = \mathrm{i}$ a $\varepsilon_2 = \mathrm{i}^2 = -1$. Protože $\varepsilon_2 = -1$ je primitivní druhá odmocnina z jedné, zkoumáme vlastně obecnější zaplnění obdélníčky 1×2 a 4×1, z jehož případné neexistence vyplyne i neexistence požadovaného zaplnění obdélníčky 1×4 a 4×1.
Nejprve ukážeme, že čísla v každém obdélníčku 1×2 či 4×1 dávají součet 0.
Obdélníček 1×2 začínající na pozici (k,j):

$$\mathrm{i}^{k+2j} + \mathrm{i}^{k+2j+2} = \mathrm{i}^{k+2j}\left(1 + \mathrm{i}^2\right) = \mathrm{i}^{k+2j} \cdot (1-1) = \mathrm{i}^{k+2j} \cdot 0 = 0$$

Obdélníček 4×1 začínající na pozici (k,j):

$$\mathrm{i}^{k+2j} + \mathrm{i}^{k+2j+1} + \mathrm{i}^{k+2j+2} + \mathrm{i}^{k+2j+3} = \mathrm{i}^{k+2j}\left(1 + \mathrm{i} + \mathrm{i}^2 + \mathrm{i}^3\right) = \mathrm{i}^{k+2j} \cdot 0 = 0$$

Z právě dokázané vlastnosti plyne: Abychom mohli požadovaným způsobem zaplnit šachovnici bez středového pole, musí být součet všech $13^2 - 1 = 168$ čísel do této upravené šachovnice vepsaných nulový. To je ekvivalentní s tím, že je součet všech 169 čísel vepsaných do celé šachovnice roven číslu vepsanému do středového pole.
Součet S všech čísel vepsaných do celé šachovnice má hodnotu

$$S = \left(\mathrm{i} + \mathrm{i}^2 + \cdots + \mathrm{i}^{13}\right)\left(\mathrm{i}^2 + \mathrm{i}^4 + \cdots + \mathrm{i}^{26}\right) = \mathrm{i} \cdot \frac{\mathrm{i}^{13} - 1}{\mathrm{i} - 1} \cdot \mathrm{i}^2 \cdot \frac{\mathrm{i}^{26} - 1}{\mathrm{i}^2 - 1} =$$
$$= \mathrm{i} \cdot \frac{\mathrm{i} - 1}{\mathrm{i} - 1} \cdot (-1) \cdot \frac{-1 - 1}{-1 - 1} = -\mathrm{i}.$$

[1] Při vepisování čísla i^{k+j}, což necháváme na vyzkoušení čtenáři, by nebyla porušena nutná podmínka, takže existenci zaplnění bychom našim výpočtem nemohli vyloučit.

Středové pole je na pozici $(7,7)$, je v něm tedy číslo

$$\mathrm{i}^{7+14} = \mathrm{i}^{21} = \mathrm{i}.$$

Zjistili jsme, že součet všech čísel vepsaných do celé šachovnice je různý od čísla vepsaného do středového pole $(-\mathrm{i} \neq \mathrm{i})$, z čehož plyne, že šachovnici 13×13 bez středového pole nelze zaplnit nejen obdélníčky 1×4 a 4×1, ale ani obdélníčky 1×2 a 4×1. ■

Nyní se podívejme na zaplňování čtvercové šachovnice bez jednoho pole obecněji.
Budeme ji zaplňovat obdélníčky $1 \times x$ a $x \times 1$, bude tedy vhodné vyjádřit rozměry šachovnice jako $(xm+y) \times (xm+y)$, kde $x,m \in \mathbb{N}, y \in \{0,1,\ldots,x-1\}$. Vynechané pole bude na zadané pozici (r,s), $r,s \in \{1,2,\ldots,xm+y\}$. Dodejme, že rozměry šachovnice by mohly být i menší než x, tedy s hodnotou $m = 0$, není ale těžké rozmyslet, že by pak jediná vyhovující šachovnice byla 1×1, kde je ono jediné pole vynecháno.
Abychom vůbec mohli o takovémto zaplnění uvažovat, musí být počet polí upravené šachovnice dělitelný číslem x. Podmínku $x \mid \left[(xm+y)^2 - 1\right]$ vyřešíme pomocí kongruencí:

$$\begin{aligned} (xm+y)^2 &\equiv 1 \pmod{x} \\ x^2m^2 + 2xmy + y^2 &\equiv 1 \pmod{x} \\ y^2 &\equiv 1 \pmod{x} \end{aligned}$$

Dostáváme tedy první nutnou podmínku ve tvaru jednoduché kongruence $y^2 \equiv 1 \pmod{x}$.
Dále využijeme samotného vepisování komplexních čísel do jednotlivých polí šachovnice. Zde si nejprve musíme uvědomit, že podmínka nulového součtu všech čísel vepsaných do upravené šachovnice, neboli rovnosti součtu všech čísel vepsaných do celé šachovnice a čísla vepsaného do odstraněného pole je též pouze podmínkou nutnou.
Označíme ε primitivní x-tou odmocninu z jedné a celou šachovnici zaplníme mocninami ε tak, že do pole na souřadnicích (k,j) vepíšeme číslo ε^{ak+bj}, kde a,b jsou pevně zvolená čísla z množiny $\{1,2,\ldots,x-1\}$.
To, že čísla v každém obdélníčku $1 \times x$ či $x \times 1$ dávají součet 0, ukážeme s využitím Věty 1.41 na obdélníčku $1 \times x$ začínajícím na pozici (k,j):

$$\varepsilon^{ak+bj} + \varepsilon^{ak+b(j+1)} + \cdots + \varepsilon^{ak+b(j+x-1)} = \varepsilon^{ak+bj}\left(1 + \varepsilon^b + \cdots + \varepsilon^{(x-1)b}\right) \overset{x \mid b}{=} \varepsilon^{ak+bj} \cdot 0 = 0$$

Stejným rozepsáním bychom to dokázali i pro libovolný obdélníček $x \times 1$.
Tímto dostáváme dalších $(x-1)^2$ nutných podmínek, že se totiž součet všech čísel ε^{ak+bj} vepsaných do celé šachovnice (který zde obecně upravovat nebudeme) musí rovnat číslu ε^{ar+bs} pro všechny možné dvojice (a,b), kterých je právě $(x-1)^2$. (Netvrdíme však, že jsou to navzájem nezávislé podmínky.)
Ovšem ani při splnění všech těchto $(x-1)^2+1$ nutných podmínek nemůžeme tvrdit, že požadované zaplnění existuje. Tyto nutné podmínky pouze výrazně zredukují počet pozic (r,s) vynechaného pole, které pro možné zaplnění vůbec přicházejí v úvahu. Na ně pak můžeme aplikovat nějaký počítačový algoritmus, který nám takové zaplnění buď najde, nebo po vyzkoušení všech možností rozhodne, že takové zaplnění neexistuje. Zmíněná redukce tak může přinést citelnou úsporu strojového času.
Dle předchozího obecného návodu nyní kompletně rozeberme situaci pro $x = 4$.

Příklad 7. Jaká je možná pozice (r,s) jediného vynechaného pole na čtvercové šachovnici, při které lze takto upravenou šachovnici zaplnit obdélníčky 1×4 a 4×1?

Řešení. Zachováme označení $(xm+y)\times(xm+y)$ rozměrů celé šachovnice, popsané v předchozím textu. První podmínka $y^2\equiv 1 \pmod 4$ nám dává, že $y=1$ nebo $y=3$. Opět zvolme pro jednoduchost $\varepsilon=\mathrm{i}$ a vepišme do pole na pozici (k,j) mocninu i^{ak+bj}, kde $a,b\in\{1,2,3\}$ jsou pevně zvolená. Řešme nyní zvlášť případy pro obě možná y.
i.) $y=1$, tj. šachovnice $(4m+1)\times(4m+1)$
Nejprve spočtěme součet všech čísel vepsaných do celé šachovnice:

$$S=\left(\mathrm{i}^a+\mathrm{i}^{2a}+\cdots+\mathrm{i}^{(4m+1)a}\right)\left(\mathrm{i}^b+\mathrm{i}^{2b}+\cdots+\mathrm{i}^{(4m+1)b}\right)=$$
$$=\mathrm{i}^a\cdot\frac{\mathrm{i}^{(4m+1)a}-1}{\mathrm{i}^a-1}\cdot\mathrm{i}^b\cdot\frac{\mathrm{i}^{(4m+1)b}-1}{\mathrm{i}^b-1}=\mathrm{i}^a\cdot\frac{\mathrm{i}^a-1}{\mathrm{i}^a-1}\cdot\mathrm{i}^b\cdot\frac{\mathrm{i}^b-1}{\mathrm{i}^b-1}=\mathrm{i}^a\cdot 1\cdot\mathrm{i}^b\cdot 1=\mathrm{i}^{a+b}$$

Pro možnou polohu vynechaného pole jsme dostali podmínku $\mathrm{i}^{ar+bs}=\mathrm{i}^{a+b}$, která má platit pro všechny možné dvojice $a,b\in\{1,2,3\}$. Tuto podmínku vyřešíme pomocí kongruencí:

$$\begin{aligned}\mathrm{i}^{ar+bs}&=\mathrm{i}^{a+b}\\ ar+bs&\equiv a+b \pmod 4\\ a(r-1)+b(s-1)&\equiv 0 \pmod 4\end{aligned}$$

Je zřejmé, že tato podmínka je splněna pro $r\equiv 1 \pmod 4 \wedge s\equiv 1 \pmod 4$. Ukážeme, že je to jediná možnost, a to tak, že uvážíme některé konkrétní dvojice (a,b):

$$(a,b)=(1,1): \quad (r-1)+(s-1)\equiv 0 \pmod 4 \tag{2.10}$$
$$(a,b)=(2,1): \quad 2(r-1)+(s-1)\equiv 0 \pmod 4 \tag{2.11}$$
$$(a,b)=(1,2): \quad (r-1)+2(s-1)\equiv 0 \pmod 4 \tag{2.12}$$

$$(2.11)-(2.10): \quad (r-1)\equiv 0 \pmod 4 \qquad (2.12)-(2.10): \quad (s-1)\equiv 0 \pmod 4$$
$$r\equiv 1 \pmod 4 \qquad\qquad s\equiv 1 \pmod 4$$

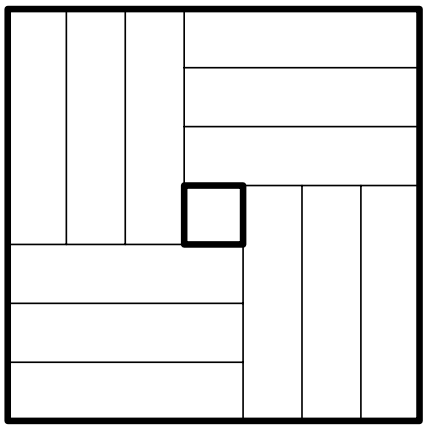
Tedy $r\equiv 1 \pmod 4 \wedge s\equiv 1 \pmod 4$ jsou jediné možné polohy vynechaného pole.
Jak jsme upozorňovali již dříve, nemáme stále jistotu, že požadované zaplnění pro všechny nalezené polohy vynechaného pole opravdu existuje. V tomto případě však můžeme vhodné zaplnění snadno popsat.
Libovolnou šachovnici $(4m+1)\times(4m+1)$ zaplníme tak, že nejprve zaplníme sloupec s vynechaným polem od něj obdélníčky 4×1 a poté od toho sloupce vyskládáme zbytek šachovnice obdélníčky 1×4. Obojí je možné právě díky tomu, že $r\equiv 1 \pmod 4$ a $s\equiv 1 \pmod 4$.
ii.) $y=3$, tj. šachovnice $(4m+3)\times(4m+3)$
Nejprve spočtěme součet všech čísel vepsaných do celé šachovnice, tentokráte s využitím Věty 1.41, kde $4\nmid a$ a $4\nmid b$:

$$S=\left(\mathrm{i}^a+\mathrm{i}^{2a}+\cdots+\mathrm{i}^{(4m+3)a}\right)\left(\mathrm{i}^b+\mathrm{i}^{2b}+\cdots+\mathrm{i}^{(4m+3)b}\right)$$
$$=\left[m\cdot\left(\mathrm{i}^a+\mathrm{i}^{2a}+\mathrm{i}^{3a}+\mathrm{i}^{4a}\right)+\left(\mathrm{i}^a+\mathrm{i}^{2a}+\mathrm{i}^{3a}\right)\right]\left[m\cdot\left(\mathrm{i}^b+\mathrm{i}^{2b}+\mathrm{i}^{3b}+\mathrm{i}^{4b}\right)+\right.$$
$$\left.+\left(\mathrm{i}^b+\mathrm{i}^{2b}+\mathrm{i}^{3b}\right)\right]=[m\cdot 0+(-1)]\,[m\cdot 0+(-1)]=(-1)\cdot(-1)=1$$

Pro možnou polohu vynechaného pole jsme dostali podmínku $\mathrm{i}^{ar+bs} = 1$, která má platit pro všechny možné dvojice $a, b \in \{1,2,3\}$. Tuto podmínku opět vyřešíme pomocí kongruencí:

$$\begin{aligned} \mathrm{i}^{ar+bs} &= 1 \\ ar+bs &\equiv 0 \pmod 4 \end{aligned}$$

Stejně snadno jako v prvním případě lze ukázat (nebudeme to zde popisovat), že pouze zřejmé řešení $r \equiv 0 \pmod 4 \wedge s \equiv 0 \pmod 4$ jsou jediné možné polohy vynechaného pole.



Obrázek 2.1: Zaplnění šachovnice 7×7 bez středového pole.

Uvedený obrázek 2.1 ukazuje příklad vhodného zaplnění pro nejmenší $m = 1$, kdy zaplňujeme šachovnici 7×7 bez středového pole. Rozšíření na větší šachovnice $(4m+3) \times (4m+3)$ pak provedeme tak, že nejprve podle obrázku 2.1 zaplníme část 7×7 „kolem“ vynechaného pole na pozici (r,s) a poté zbytek šachovnice snadno zaplníme prvně obdélníčky 4×1 „nad“ a „pod“ zaplněnou částí 7×7 a pak obdélníčky 1×4 „vlevo“ a „vpravo“ od zaplněné části $(4m+3) \times 7$. Oba poslední kroky jsou možné právě díky podmínkám $r \equiv 0 \pmod 4$ a $s \equiv 0 \pmod 4$. ■

Popsanou metodou je možné řešit i problematiku zaplňování obdélníkových šachovnic zadanými obdélníčky různých délek, což potvrzuje závěrečný příklad.

Příklad 8. Jaká je možná pozice (r,s) jediného vynechaného pole na šachovnici $m \times n$, $m \geq 3$ a $n \geq 2$, při které lze takto upravenou šachovnici zaplnit obdélníčky 1×2 a 3×1?

Řešení. Označme ε_1 primitivní třetí odmocninu z jedné a ε_2 primitivní druhou odmocninu z jedné ($\varepsilon_2 = -1$). Zaplňme celou šachovnici mocninami ε_1 a ε_2 tak, že do pole na pozici (k,j) vepišme číslo $\varepsilon_1^k \varepsilon_2^j$, takže součet čísel v každém z obdélníčků 1×2 a 3×1 bude nulový. Podmínka rovnosti součtu všech čísel vepsaných do celé šachovnice a čísla ve vynechaném poli je pak tvaru

$$\left(\varepsilon_1 + \varepsilon_1^2 + \cdots + \varepsilon_1^m\right)\left(\varepsilon_2 + \varepsilon_2^2 + \cdots + \varepsilon_2^n\right) = \varepsilon_1^r \varepsilon_2^s.$$

Protože na pravé straně rovnosti je zřejmě číslo nenulové, dostáváme z výsledku Příkladu 5 podmínku $2 \nmid n$ a současně $3 \nmid m$. Tedy $n \equiv 1 \pmod 2$ a $m \equiv 1$, nebo $2 \pmod 3$. Z podmínky $n \equiv 1 \pmod 2$ a Věty 1.41 plyne, že je druhý činitel $\varepsilon_2 + \varepsilon_2^2 + \cdots + \varepsilon_2^n$ roven ε_2. Další postup musíme rozdělit podle toho, zda je m kongruentní s 1, či 2 modulo 3.

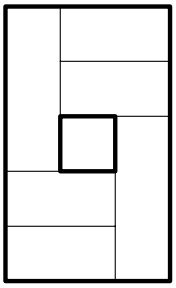
i.) $m \equiv 1 \pmod 3$, tj. šachovnice $(3k+1) \times (2l+1)$, $k,l \in \mathbb{N}$

V tomto případě pro první činitel platí $\varepsilon_1 + \varepsilon_1^2 + \cdots + \varepsilon_1^m = \varepsilon_1$. Podmínka pro polohu vynechaného pole je tak tvaru $\varepsilon_1\varepsilon_2 = \varepsilon_1^r\varepsilon_2^s$, neboli $\varepsilon_1^{1-r} = \varepsilon_2^{s-1}$. Poslední je rovnost některé hodnoty $\sqrt[3]{1}$ a některé hodnoty $\sqrt[2]{1}$. Protože společná hodnota těchto odmocnin je zřejmě jediná a je rovna jedné, je daná rovnost ekvivalentní podmínce $r \equiv 1 \pmod 3 \wedge s \equiv 1 \pmod 2$. Ukažme, že pro každou pozici (r,s) vynechaného pole splňující nalezenou podmínku požadované zaplnění existuje.

Libovolnou šachovnici $(3k+1) \times (2l+1)$ zaplníme tak, že nejprve zaplníme sloupec s vynechaným polem od něj obdélníčky 3×1 a poté od toho sloupce vyskládáme zbytek šachovnice obdélníčky 1×2. Obojí je možné právě díky tomu, že $r \equiv 1 \pmod 3$ a $s \equiv 1 \pmod 2$.

ii.) $m \equiv 2 \pmod 3$, tj. šachovnice $(3k+2) \times (2l+1)$, $k,l \in \mathbb{N}$

V tomto případě pro první činitel platí $\varepsilon_1 + \varepsilon_1^2 + \cdots + \varepsilon_1^m = \varepsilon_1 + \varepsilon_1^2 = -1 = \varepsilon_2$, a proto je podmínka pro polohu vynechaného pole tvaru $\varepsilon_2^2 = \varepsilon_1^r\varepsilon_2^s$, neboli $1 = \varepsilon_1^r\varepsilon_2^s$. Odtud se stejně jako v první části odvodí podmínka $r \equiv 0 \pmod 3 \wedge s \equiv 0 \pmod 2$. Opět ukažme, že pro každou pozici (r,s) vynechaného pole splňující nalezenou podmínku požadované zaplnění existuje.



Obrázek 2.2: Zaplnění šachovnice 5×3 bez středového pole.

Pro nejmenší uvažovanou šachovnici 5×3 bez středového pole je možné zaplnění znázorněno na obrázku 2.2. Rozšíření na větší šachovnice $(3k+2) \times (2l+1)$ pak provedeme tak, že nejprve podle obrázku 2.2 zaplníme část 5×3 „kolem“ vynechaného pole v pozici (r,s) a poté zbytek šachovnice snadno zaplníme prvně obdélníčky 3×1 „nad“ a „pod“ zaplněnou částí 5×3 a pak obdélníčky 1×2 „vlevo“ a „vpravo“ od zaplněné části $(3k+2) \times 3$. Oba poslední kroky jsou možné právě díky podmínkám $r \equiv 0 \pmod 3$ a $s \equiv 0 \pmod 2$. ■

Na úplný závěr této části se v krátkosti podíváme na ještě obecnější případ, ve kterém budeme obdélníčky $1 \times x$ a $y \times 1$ zaplňovat šachovnici $m \times n$, ve které bude vynecháno p polí na pozicích $(r_1,s_1),(r_2,s_2),\ldots,(r_p,s_p)$.

Podmínku na počet polí šachovnice tentokráte dostaneme ve tvaru, že musí existovat řešení $(c_1,c_2) \in \mathbb{N}_0^2$ diofantické rovnice

$$c_1x + c_2y = mn - p.$$

Označme ε_1 primitivní y-tou odmocninu z jedné a ε_2 primitivní x-tou odmocninu z jedné. Zaplňme celou šachovnici mocninami ε_1 a ε_2 tak, že do pole na pozici (k,j) vepíšeme číslo $\varepsilon_1^{ak}\varepsilon_2^{bj}$, kde a,b jsou pevně zvolená čísla, přičemž $a \in \{1,2,\ldots,y-1\}$ a $b \in \{1,2,\ldots,x-1\}$.
Nyní s využitím Věty 1.41 ukážeme, že čísla v každém obdélníčku $1 \times x$ či $y \times 1$ dávají součet 0.
Obdélníček $1 \times x$ začínající na pozici (k,j):

$$\varepsilon_1^{ak}\varepsilon_2^{bj} + \varepsilon_1^{ak}\varepsilon_2^{b(j+1)} + \cdots + \varepsilon_1^{ak}\varepsilon_2^{b(j+x-1)} = \varepsilon_1^{ak}\varepsilon_2^{bj}\left(1 + \varepsilon_2^{b} + \cdots + \varepsilon_2^{(x-1)b}\right) \overset{x\nmid b}{=} \varepsilon_1^{ak}\varepsilon_2^{bj} \cdot 0 = 0$$

Obdélníček $y \times 1$ začínající na pozici (k,j):

$$\varepsilon_1^{ak}\varepsilon_2^{bj} + \varepsilon_1^{a(k+1)}\varepsilon_2^{bj} + \cdots + \varepsilon_1^{a(k+y-1)}\varepsilon_2^{bj} = \varepsilon_1^{ak}\varepsilon_2^{bj}\left(1 + \varepsilon_1^{a} + \cdots + \varepsilon_1^{(y-1)a}\right) \overset{y\nmid a}{=} \varepsilon_1^{ak}\varepsilon_2^{bj} \cdot 0 = 0$$

Podmínek rovností pro součet všech čísel vepsaných do celé šachovnice a čísel na vynechaných polích je dle všech možných dvojic (a,b) právě $(x-1)(y-1)$ (opět netvrdíme, že jsou navzájem nezávislé) a vypadají následovně:

$$\left(\varepsilon_1^{a} + \varepsilon_1^{2a} + \cdots + \varepsilon_1^{ma}\right)\left(\varepsilon_2^{b} + \varepsilon_2^{2b} + \cdots + \varepsilon_2^{nb}\right) = \varepsilon_1^{ar_1}\varepsilon_2^{bs_1} + \varepsilon_1^{ar_2}\varepsilon_2^{bs_2} + \cdots + \varepsilon_1^{ar_p}\varepsilon_2^{bs_p}$$

Na závěr ještě jednou připomeňme, že těchto $(x-1)(y-1)+1$ podmínek je pouze nutných a jejich splnění nám ještě existenci požadovaného zaplnění negarantuje. Slouží nám tedy pouze k úspoře strojového času, neboť algoritmy ověřující tyto podmínky mohou mít řádově nižší složitost než algoritmy zkoušející všechny možnosti zaplnění. Ty tak můžeme díky odvozeným podmínkám aplikovat jen na ty zbylé „nadějné“ případy.

Závěr

Cílem této práce bylo ukázat různá užití komplexních čísel v kombinatorice. K tomu je nutné nejprve seznámit čtenáře s potřebnými teoretickými poznatky, čemuž se věnuje první kapitola. V jejích prvních dvou částech zavádíme komplexní čísla jako uspořádané dvojice reálných čísel, a poté zavádíme i jejich algebraický a goniometrický tvar. Též ukazujeme a dokazujeme mnohé jejich základní vlastnosti. Speciálně chceme zmínit úplně rozepsaný důkaz toho, že komplexní čísla jako uspořádané dvojice reálných čísel splňují vlastnosti komutativního tělesa, kterýžto bývá v literatuře často odbyt tím, že se snadno ukáže s využitím vlastností čísel reálných. Další část je pak věnována komplexním odmocninám z jedné, přičemž je dána odpověď na přirozenou, a přitom méně tradiční, otázku, kdy je komplexní jednotka komplexní n-odmocninou z jedné pro nějaké přirozené n. Největší pozornost je zaměřena na primitivní odmocniny z jedné, a to nejen na to, kdy je zvolená odmocnina primitivní, ale i na fakt, že množina všech n-tých odmocnin z jedné s násobením generovaná libovolnou primitivní odmocninou je grupou, která je, jak je ukázáno v další části, izomorfní s grupou všech zbytkových tříd modulo n se sčítáním. První kapitola je pak zakončena částí s několika ryze praktickými, a ne úplně obvyklými, tvrzeními, která uplatníme ve druhé kapitole. Všechna tato tvrzení jsou dokázána, čímž je čtenář ochráněn od neoblíbených prostých konstatování během výpočtů. Zejména zmiňme asi nejpodstatnější větu celé práce, tj. Větu 1.56, a nový způsob důkazu vzorce z Lemmatu 1.57 pomocí diferenčního počtu.

Druhá kapitola pak podává praktický výklad o užití komplexních čísel v kombinatorice na několika konkrétních příkladech. Nejprve se věnujeme onomu středoškolsky známému určování konečných součtů tvořených kombinačními čísly, kdy vhodné komplexní číslo vyjádříme jednak v algebraickém tvaru a umocníme užitím binomické věty, jednak v goniometrickém tvaru a umocníme užitím Moivreovy věty. V další části je poté na čtyřech příkladech, jejichž řešení je rozepsáno krok po kroku, ukázáno, jak lze využít výše zmiňované izomorfnosti ke stanovení počtu prvků konkrétní množiny patřících do jisté zbytkové třídy. Vrcholem celé práce je pak poslední část věnovaná oblasti kombinatorické geometrie, úlohám o pokrývání šachovnic obecných rozměrů soustavami šachovnic menších zadaných rozměrů. V této části ukazujeme nejen, jak je možné rozhodovat o existenci zaplnění pro konkrétní velikosti šachovnice a obdélníčků a zadané pozice vynechaných polí, ale i jak hledat všechny možné pozice vynechaných polí pro konkrétní velikosti obdélníčků na obdélníkové šachovnici obecných rozměrů.

Jsme si vědomi toho, že problematika užití komplexních čísel v kombinatorice touto prací nebyla plně vyčerpána. O to nám však ani nešlo. Cílem této práce bylo ukázat, že komplexní čísla mohou být v kombinatorice užitečným nástrojem, který lze užít v mnohých, mnohdy až nečekaných, situacích.

Seznam použité literatury

[1] ANDREESCU, Titu a Gabriel DOSPINESCU. *Problems from the Book*. Allen: XYZ Press, 2008, 554 s. ISBN 978-0-9799269-0-7.

[2] BOHÁČ, Pavel. *Základy geometrie komplexních čísel*. Brno, 2013. 143 s. Rigorózní práce. Masarykova univerzita, Přírodovědecká fakulta.

[3] FUCHS, Eduard. *Diskrétní matematika pro učitele*. 2. vyd. Brno: Masarykova univerzita, 2011, 178 s. ISBN 97-880-210-5459-2.

[4] HERMAN, Jiří, Radan KUČERA, a Jaromír ŠIMŠA. *Metody řešení matematických úloh I*. 2. přeprac. vyd. Brno: Masarykova univerzita, 1996. 278 s. ISBN 80-210-1202-1.

[5] HERMAN, Jiří, Radan KUČERA, a Jaromír ŠIMŠA. *Metody řešení matematických úloh II*. 3. přeprac. vyd. Brno: Masarykova univerzita, 2004. 355 s. ISBN 80-210-3569-2.

[6] KOBZA, Aleš. *Diferenční rovnice ve středoškolské matematice*. Brno, 2001. 53 s. Diplomová práce. Masarykova univerzita, Přírodovědecká fakulta.

[7] ODVÁRKO, Oldřich. *Matematika pro gymnázia: goniometrie*. 1. vyd. Praha: Prometheus, 1994, 127 s. ISBN 80-858-4957-7.

[8] RÁB, Miloš. *Komplexní čísla v elementární matematice*. 2. přeprac. vyd. Brno: Masarykova univerzita, 1996. vii, 209 s. ISBN 80-210-1475-X.

[9] ROSICKÝ, Jiří. *Algebra*. 4. přeprac. vyd. Brno: Masarykova univerzita, 2007, 133 s. ISBN 80-210-2964-4.