MASARYKOVA UNIVERZITA • PŘÍRODOVĚDECKÁ FAKULTA

Eduard Fuchs

DISKRÉTNÍ MATEMATIKA

PRO UČITELE

Brno 2011

ISBN 978–80–210–5459–2

PŘEDMLUVA

Prvotní impulzy, které posléze lidstvo přivedly k vybudování matematiky, byly bezpochyby dvojího druhu: *početní* a *geometrické*. Tyto impulzy také předznamenaly jeden z centrálních protikladů, které lze vypozorovat v celé dosavadní historii matematiky – vztah *diskrétního* a *spojitého*.

Typickými reprezentanty matematických objektů nacházejících se na straně diskrétního proudu jsou *přirozená*, respektive *celá čísla*, *konečné množiny*, *konečné geometrie* apod., spojitý směr reprezentují objekty jako *množina všech reálných čísel*, *přímka*, *eukleidovská rovina*, *spojitá funkce* apod.

Jak již název napovídá, zabývá se *diskrétní matematika* první z výše uvedených stránek našich modelů reality.

Je svým způsobem paradoxní, že poté, co matematika na sklonku 19. století zvládla v Cantorově *teorii množin* problematiku matematického nekonečna (více viz v [4] nebo na CD [3], patří mezi matematické disciplíny, které se ve 20. století rozvíjejí nejdynamičtěji, právě diskrétní matematika, jejíž značná část se zabývá studiem *konečných* množin.

To, že zejména v poslední třetině 20. století prodělala diskrétní matematika přímo bouřlivý rozvoj, bylo způsobeno řadou faktorů. Mezi klíčové patří:

- neustále se rozšiřující škála aplikací nejen v matematice samotné, především však mimo ni, a to nejen v „tradičních“ přírodovědných oblastech, ale zejména v nových a mnohdy nečekaných souvislostech;

- intenzívní rozvoj výpočetní techniky, která umožňuje provádět výpočty a analýzy, které se ještě před několika desetiletími zdály nemožné a nadlouho přesahující hranice lidských možností.

V předloženém textu jsou vyloženy úvodní partie centrálních disciplín moderní diskrétní matematiky – *kombinatoriky* a *teorie grafů* v rozsahu, který by měli ovládat středoškolští učitelé matematiky. K základnímu textu jsou připojeny dva dodatky. V prvním jsou uvedeny základní biografické údaje osobností, které jsou v textu zmiňovány, ve druhém jsou tabulky některých studovaných funkcí.

Za pomoc při přípravě sazby tohoto textu děkuji Mgr. M. Anderovi a Mgr. D. Kottovi, který navíc celý text pečlivě pročetl a přispěl k jeho závěrečným úpravám. Za veškeré chyby a nedostatky však samozřejmě plně odpovídá autor.

Čtenářům budu vděčný, když případné chyby a nedostatky, které v textu zjistí, zašlou na mou mailovou adresu: `fuchs@math.muni.cz`. Za jejich připomínky jim předem děkuji.

OBSAH

DISKRÉTNÍ MATEMATIKA

PRO UČITELE

doc. RNDr. Eduard Fuchs, CSc.

Vydala Masarykova univerzita roku 2011

Druhé vydání, 2011
Náklad: 300 výtisků
Tisk: Tiskárna Blansko - Těchov
Těchov 152
678 01 Blansko

ISBN 978-80-210-5459-2

muni
PRESS
ISBN 978-80-210-5459-2

Kapitola 1

KOMBINATORIKA

1 Co to je kombinatorika a kdy vznikla

Jak uvidíme, neexistuje na otázky v nadpise jednoduchá odpověď. Částečnou odpovědí na první část otázky je – v jistém smyslu – celá první kapitola.

Tak jak je obtížné sdělit, co to je vůbec matematika, je nesnadné charakterizovat i její jednotlivé části. Pokusme se alespoň stručně naznačit, co je předmětem kombinatoriky (nazývané též *kombinatorická analýza, kombinatorická teorie* apod.) a jakými metodami se v kombinatorice pracuje.

Často se podle autora jedné z prvních učebnic kombinatoriky E. Netta (kniha *Lehrbuch der Combinatorik* vyšla v roce 1901) říká, že „kombinatorika je část matematiky zabývající se rozdělováním, uspořádáváním, nebo výběrem prvků nějaké množiny". Z modernějšího hlediska je centrálním pojmem kombinatoriky tzv. *konfigurace*, což je pojem, který bychom mohli charakterizovat jako „zobrazení nějaké množiny objektů do konečné abstraktní množiny se zadanou strukturou" (viz Bergeovu knihu [1]). Uvedená formulace sice pěkně zní, čtenář z ní však patrně těžko pochopí, co to konfigurace vlastně je. Objasnění tohoto pojmu vyplyne z dalšího textu, neboť v něm budeme studovat řadu nejrozmanitějších konfigurací. Kromě těch nejelementárnějších, tj. *variací, permutací* a *kombinací* (čtenáři dobře známých již se střední školy), to budou např. *rozklady konečných množin, rozklady přirozených čísel na sčítance, rozdělování předmětů do přihrádek, latinské čtverce, bloková schémata, konečné afinní roviny* a další.

Jaký je hlavní okruh otázek s těmito konfiguracemi spojený? Konfigurace jsou nejčastěji studovány z následujících aspektů:

(1) *Existuje jistá konfigurace nebo nikoliv?* (Budeme například řešit, zda existují ortogonální latinské čtverce daného řádu, zda existuje jistá afinní

rovina a podobně.)

(2) *Kolik existuje předepsaných konfigurací?* (Středoškolská kombinatorika v podstatě spočívá v určení počtu variací, permutací a kombinací daného typu. My se však budeme zabývat i podstatně komplikovanějšími problémy.)

(3) *Lze najít metodu, jak vypsat všechny konfigurace daného typu?* (Je zřejmé, že jde o kvalitativně odlišnou úlohu než je problém popsaný v bodě (2).)

(4) *Jaké je „asymptotické" chování počtu daných konfigurací?* (Vzhledem k tomu, že budeme téměř neustále pracovat s konečnými množinami, bude počet konfigurací daného typu téměř vždy konečný. Proto by se mohlo zdát, že nejjednodušší určení počtu všech konfigurací spočívá prostě ve vypsání všech možností. To je však ve většině případů prakticky vyloučeno, neboť počet daných konfigurací je tak obrovský, že vypočítat všechny možnosti nelze – stačí si například jen uvědomit, jak rychle roste funkce $n!$. I když často známe např. rekurentní formuli pro počet $k(n)$ konfigurací daného typu (pro všechna $n \in \mathbb{N}$), roste funkce $k(n)$ tak rychle, že již pro poměrně malá n nelze $k(n)$ přesně vyčíslit ani pomocí počítačů. Pak se alespoň snažíme najít nějakou „jednoduchou" funkci, která popisuje, „jak rychle" $k(n)$ roste.)

(5) *Jak najít z konfigurací daného typu tu, která optimálně vyhovuje zadaným předpokladům?* (Úlohy tohoto typu mají řadu konkrétních aplikací v matematice i mimo ni. Uvedeným problémem se zabývá intenzivně rozvíjená část kombinatoriky – tzv. teorie „kombinatorických algoritmů".)

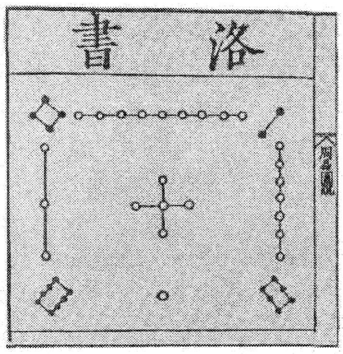
O většině uvedených aspektů se v dalším alespoň stručně zmíníme. Přesto zůstává řada závažných částí kombinatoriky, o nichž nemůžeme pojednat ani ve zkratce. Jmenujme za jiné alespoň *kombinatorickou teorii uspořádaných množin, Pólyovu teorii enumerace* či *teorii kódování.* K popsání uvedených teorií nemáme k dispozici dostatečný matematický aparát, ani nám to neumožňuje rozsah tohoto textu.

Metody v kombinatorice užívané můžeme rovněž popsat jen částečně. Jak alespoň naznačíme, užívá se v kombinatorice výrazně i těch nejkomplikovanějších metod algebry, reálné i komplexní analýzy i geometrie. Kromě toho si kombinatorika vytvořila i své specifické metody, z nichž se později zmíníme například o *metodě inkluze a exkluze* a o teorii *vytvořujících funkcí.*

Jak uvidíme, řadu kombinatorických problémů lze velmi snadno zformulovat, avšak jejich řešení je velmi často obtížné.

Prozatím jsme se pokusili alespoň naznačit, co to kombinatorika je. Nyní stručně k její historii.

První „kombinatorické“ výsledky či alespoň náznaky jsou až překvapivě staré. Pravděpodobně nejstarší „konfiguraci“ lze nalézt v jednom z nejstarších dochovaných textů v historii lidstva. V posvátné knize taoismu *I-tīng*, (tj. *Kniha proměn*) z roku přibližně 2200 př. Kr. jsou dvě konfigurace, nazývané *Lo-šu* a *Říční mapa*. Na obrázku 1.1 je konfigurace *Lo-šu*.



Obr. 1.1: Konfigurace „Lo-šu“ ve středověkém textu

Nahradíme-li znázorněné skupiny bodů čísly, obdržíme známý magický čtverec (nazývaný též *Saturn*):

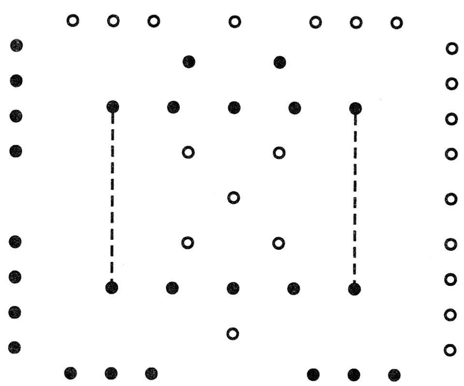
4	9	2
3	5	7
8	1	6

V tomto čtverci je součet čísel v každém řádku, sloupci i úhlopříčce roven číslu 15.

Druhá konfigurace, kterou podle pověsti měla na svém krunýři znázorněnu posvátná želva vylézající z řeky *Ho*, je znázorněna na obr. 1.2.

Znázorníme-li toto schéma čísly, obdržíme

			7			
			2			
		10		10		
8	3		5		4	9
		10		10		
			1			
			6			



Obr. 1.2: Konfigurace „Říční mapa“

Toto schéma je pozoruhodné svou „středovou symetrií“. Platí například

$$5+3=8,\ 5+1=6 \text{ atd.}, 3+10+2=8+7,\ 3+10+1=8+6 \text{ atd.}$$

Řada kombinatorických pojmů je doložena například ve staré indické matematice.

Kombinatorika jakožto matematická disciplína se však začíná konstituovat až cca v 16. až 17. století, prakticky – vcelku evidentně – současně se vznikem teorie pravděpodobnosti. Kombinatorické úvahy lze vysledovat v díle B. Pascala, P. Fermata a dalších. První publikovanou prací z kombinatoriky je Leibnizovo dílo *Disertatio de Arte Combinatoria* z roku 1666. V 18. století k rozvoji kombinatoriky zvlášť významně přispěl L. Euler. Opravdu bouřlivý rozvoj však kombinatorika prodělává až ve 20. století, zejména pak v posledních třiceti letech, kdy se v souvislosti s rozvojem výpočetní techniky rozvíjí celá tzv. **diskrétní** matematika, jejíž významnou součástí je právě kombinatorika.

2 Základní kombinatorické funkce

2.1. Definice. Funkci $n!$ (čti n faktoriál) definujeme pro všechna $n \in \mathbb{N}_0$ takto:

$$n! = \begin{cases} 1 & \text{pro } n = 0 \\ 1 \cdot 2 \cdot \ldots \cdot n & \text{pro } n > 0. \end{cases}$$

2.2. Poznámka. Podle výše uvedené definice tedy pro všechna $n \in \mathbb{N}_0$ platí:

$$(n+1)! = (n+1) \cdot n!$$

2.3. Příklad. Pro funkci $n!$ lze dokázat řadu vztahů, od elementárních po velmi komplikované. Například v matematické analýze se dokazuje, že

$$\sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{0!} + \frac{1}{1!} + \cdots + \frac{1}{n!} + \cdots = e.$$

(Připomeňme, že *součtem nekonečné řady* $\sum_{n=0}^{\infty} a_n$ rozumíme následující limitu (pokud existuje): $\lim_{n\to\infty} s_n$, kde $s_n = a_0 + a_1 + \cdots + a_n$.)

Odtud například plyne

$$\sum_{n=2}^{\infty} \frac{n-1}{n!} = \sum_{n=2}^{\infty} \frac{1}{(n-1)!} - \sum_{n=2}^{\infty} \frac{1}{n!} = \sum_{n=1}^{\infty} \frac{1}{n!} - (e-2) = (e-1) - (e-2) = 1.$$

2.4. Poznámka. Zobecněním funkce $n!$ na všechna kladná reálná čísla je tzv. *Eulerova funkce gama* definovaná takto:

$$\Gamma(x) = \int_0^{\infty} e^{-t} \cdot t^{x-1}\, dt, \qquad x > 0.$$

Lze dokázat, že pro každé přirozené číslo n platí: $\Gamma(n) = (n-1)!$. Funkce $\Gamma(x)$ je přitom spojitá v celém definičním oboru.

Hodnoty $n!$ rostou s rostoucím n „velmi rychle". Pro alespoň částečnou představu uvádíme v tabulce na straně 168 hodnoty $n!$ pro $n \in \{1, \dots, 25\}$.

K přibližnému výpočtu hodnot $n!$ pro velká n se nejčastěji užívá tzv. *Stirlingovy formule*

$$n! \sim \sqrt{2\pi n} \cdot e^{-n} \cdot n^n,$$

kde symbol $\sim$ značí, že podíl výrazů na obou stranách pro $n \to \infty$ konverguje k 1.

2.5. Definice. Buď $k \in \mathbb{N}$ libovolné. Funkci $(x)_k$ definujeme pro všechna reálná x takto:

$$(x)_k = x \cdot (x-1) \cdot (x-2) \cdot \ldots \cdot (x-k+1).$$

Dále klademe

$$(x)_0 = 1.$$

2.6. Definice. Buď $k \in \mathbb{N}$ libovolné. Funkci $(x)^{(k)}$ definujeme pro všechna reálná x takto:

$$(x)^{(k)} = x \cdot (x+1) \cdot (x+2) \cdot \ldots \cdot (x+k-1).$$

Dále klademe

$$(x)^{(0)} = 1.$$

2.7. Definice. Buď $k \in \mathbb{N}_0$ libovolné. Pro každé reálné číslo x definujeme

$$\binom{x}{k} = \frac{(x)_k}{k!} = \frac{x \cdot (x-1) \cdot (x-2) \cdot \ldots \cdot (x-k+1)}{k!}.$$

Pro celé záporné číslo k pokládáme

$$\binom{x}{k} = 0.$$

2.8. Poznámka. Symbol $\binom{x}{k}$ (čti „x nad k") se obvykle nazývá *binomický koeficient*. (Toto pojmenování je spojeno se jménem významného algebraika 16. století *Michaela Stifela*.) Pro $n, k \in \mathbb{N}_0$ se $\binom{n}{k}$ nazývá také *kombinační* *číslo*. O kombinatorickém významu funkcí $n!$, $(x)_k$, $(x)^{(k)}$ a $\binom{x}{k}$ budeme hovořit v následujících paragrafech.

2.9. Příklad. (a) Pro každé $x \in \mathbb{R}$ platí $\binom{x}{0} = 1$, zejména $\binom{0}{0} = 1$.

(b) $\binom{-4}{3} = \dfrac{(-4)\cdot(-5)\cdot(-6)}{6} = -20.$

(c) $\binom{\frac{1}{2}}{4} = \dfrac{(\frac{1}{2})\cdot(-\frac{1}{2})\cdot(-\frac{3}{2})\cdot(-\frac{5}{2})}{24} = -\dfrac{5}{128}.$

(d) Pro $n, k \in \mathbb{N}_0$, $n < k$ platí $\binom{n}{k} = 0$, neboť $(n)_k = 0$.

(e) Pro $n, k \in \mathbb{N}_0$, $n \geq k$ platí $\binom{n}{k} = \dfrac{(n)_k}{k!} = \dfrac{n!}{(n-k)!\cdot k!}.$

(f) Pro každé $n \in \mathbb{N}_0$ platí

$$\binom{-\frac{1}{2}}{n} = \frac{(-1)^n}{2^{2n}}\cdot\binom{2n}{n} = \frac{(-1)^n}{2^{2n-1}}\cdot\binom{2n-1}{n-1}.$$

Vskutku, pro $n = 0$ je tvrzení evidentní. Nechť je tedy $n > 0$. Pak

$$\begin{aligned}\binom{-\frac{1}{2}}{n} &= \frac{1}{n!}\cdot\left(-\frac{1}{2}\right)\cdot\left(-\frac{3}{2}\right)\cdot\ldots\cdot\left(-\frac{2n-3}{2}\right)\cdot\left(-\frac{2n-1}{2}\right) = \\ &= \frac{1}{n!}\cdot\frac{(-1)^n}{2^n}\cdot\frac{(2n)!}{2\cdot 4\cdot\ldots\cdot(2n-2)\cdot 2n} = \frac{(-1)^n}{2^{2n}}\cdot\frac{(2n)!}{(n!)^2} = \\ &= \frac{(-1)^n}{2^{2n}}\cdot\binom{2n}{n} = \frac{(-1)^n}{2^{2n-1}}\cdot\binom{2n-1}{n-1}.\end{aligned}$$

(g) Pro každé $n \in \mathbb{N}_0$ platí

$$\binom{\frac{1}{2}}{n} = \frac{(-1)^{n-1}}{n\cdot 2^{2n-1}}\cdot\binom{2n-2}{n-1}.$$

Vskutku, podle definice platí

$$\binom{\frac{1}{2}}{n} = \frac{1}{n!}\cdot\left(\frac{1}{2}\right)\cdot\left(-\frac{1}{2}\right)\cdot\ldots\cdot\left(-\frac{2n-3}{2}\right).$$

Dosadíme-li za součin

$$\frac{1}{n!}\cdot\left(-\frac{1}{2}\right)\cdot\left(-\frac{3}{2}\right)\cdot\ldots\cdot\left(-\frac{2n-3}{2}\right)$$

výraz z příkladu (f), dostáváme

$$\begin{aligned}\binom{\frac12}{n} &= \frac{(-1)^{n-1}}{2^{2n-1}}\cdot\binom{2n-1}{n-1}\cdot\frac{1}{2n-1} = \\ &= \frac{(-1)^{n-1}}{2^{2n-1}}\cdot\frac{(2n-1)!}{n!(n-1)!}\cdot\frac{1}{2n-1} = \frac{(-1)^{n-1}}{n\cdot 2^{2n-1}}\cdot\frac{(2n-2)!}{(n-1)!^2} = \\ &= \frac{(-1)^{n-1}}{n\cdot 2^{2n-1}}\cdot\binom{2n-2}{n-1}.\end{aligned}$$

Dosadíme-li do posledního vztahu $n+1$ místo n, obdržíme „symetričtější" vzorec (platný pro každé $n \in \mathbb{N}_0$):

$$\binom{\frac12}{n+1} = \frac{(-1)^n}{(n+1)\cdot 2^{2n+1}}\cdot\binom{2n}{n}.$$

2.10. Definice. Podle definice je $(x)_n = x\cdot(x-1)\cdot(x-2)\cdot\ldots\cdot(x-n+$ $+1)$ polynom n-tého stupně. Označíme-li koeficient u x^k symbolem $s(n,k)$, dostáváme

$$(x)_n = s(n,0) + s(n,1)x + s(n,2)x^2 + \cdots + s(n,n)x^n.$$

Koeficienty $s(n,k)$ se nazývají *Stirlingova čísla 1. druhu.*

2.11. Věta. *Pro Stirlingova čísla 1. druhu platí následující rekurentní formule:*

$$\begin{aligned}&s(n+1,k) = s(n,k-1) - n\cdot s(n,k),\\ &s(n,0) = 0, \quad s(n,n) = 1.\end{aligned}$$

Důkaz. Tvrzení $s(n,0) = 0$ a $s(n,n) = 1$ jsou zřejmá. Dokažme tedy první vztah. Podle definice platí

$$(x)_{n+1} = (x)_n\cdot(x-n),$$

takže, opět podle definice,

$$\cdots + s(n+1,k)x^k + \cdots = (\cdots + s(n,k-1)x^{k-1} + s(n,k)x^k + \ldots)(x-n).$$

Porovnáním koeficientů u x^k na levé a pravé straně poslední rovnosti obdržíme dokazovanou formuli. •

2.12. Poznámka. Rekurentní formule z věty 2.11 nám umožňuje, jak se čtenář může snadno přesvědčit, postupně počítat čísla $s(n, k)$. Některé hodnoty uvádíme v tabulce na straně 170.

2.13. Věta. *Pro každé celé číslo k a každé reálné číslo x platí:*

$$\binom{x}{k} + \binom{x}{k+1} = \binom{x+1}{k+1}.$$

Důkaz. Pro $k \leq 0$ je tvrzení splněno triviálně. Nechť tedy je $k \geq 1$. Pak

$$\binom{x}{k} + \binom{x}{k+1} = \frac{(x)_k}{k!} + \frac{(x)_{k+1}}{(k+1)!} = \frac{(k+1)(x)_k + (x)_{k+1}}{(k+1)!} =$$
$$= \frac{(k+1) \cdot x(x-1) \cdots (x-k+1) + x(x-1) \cdots (x-k)}{(k+1)!} =$$
$$= \frac{x(x-1) \cdots (x-k+1) \cdot (k+1+x-k)}{(k+1)!} =$$
$$= \frac{(x+1)_{k+1}}{(k+1)!} = \binom{x+1}{k+1}.$$

Tím je důkaz hotov. •

2.14. Poznámka. Z definice binomických koeficientů a z věty 2.13 plyne platnost následující rekurentní formule:

Pro $n, k \in \mathbb{N}$, $n \geq k$ platí

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}; \qquad \binom{n}{0} = \binom{n}{n} = 1.$$

Tato formule nám umožňuje postupně počítat hodnoty $\binom{n}{k}$. Tabulce hodnot $\binom{n}{k}$ se obvykle říká *Pascalův trojúhelník*. (Viz tabulku v příloze na straně 169.) Jak si čtenář jistě již při nejrůznějších příležitostech uvědomil, je většina pojmů nazvaných po dřívějších osobnostech, po nich pojmenována neoprávněně. Nejinak tomu je i v tomto případě, byť jde o název v evropské tradici obvyklý. Blaise Pascal (1623–1662) toto schéma popsal ve své slavné knize *Traité du triangle arithmétique* (tj. *Pojednání o aritmetickém trojúhelníku*), avšak prokazatelně dříve je znali například arabský astronom al-Tusi (1265), čínský matematik Chu Ši-Chie (1303) či indický matematik Narajána Pandita (1365). Dokonce i v evropské literatuře se toto schéma vyskytlo před Pascalem – v knize Petra Apiana (1495–1552). To však nic nemění na skutečnosti, že je toto schéma mnohdy užitečné, jak si ostatně čtenář jistě uvědomil již na střední škole.

Pro kombinační čísla lze dokázat řadu rovností, tzv. *kombinatorických identit*, které se v matematice uplatňují v nejneočekávanějších souvislostech. Důkazy některých těchto identit vyžadují důmyslných metod – viz např. knihu [8]. V následující větě shrneme jen několik nejelementárnějších.

2.15. Věta. *Buďte $n \geq k$ nezáporná celá čísla. Pak platí:*

(a) $\binom{n}{k} = \binom{n}{n-k}$,

(b) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$,

(c) $\sum_{k=0}^{n} k \cdot \binom{n}{k} = n \cdot 2^{n-1}$,

(d) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ *pro každé přirozené číslo n.*

Důkaz. (a) Tvrzení plyne přímo z definice. (Řádky Pascalova trojúhelníka jsou tedy „symetrické".)

(b) Indukcí. Pro $n = 0$ je tvrzení triviální. Nechť tedy formule platí pro dané $n \geq 0$. Pak

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = \binom{n+1}{0} + \sum_{k=1}^{n+1} \left[\binom{n}{k-1} + \binom{n}{k} \right] = 1 + \sum_{k=0}^{n} \binom{n}{k} + \sum_{k=1}^{n} \binom{n}{k} +$$

$$+ \binom{n}{n+1} = \sum_{k=0}^{n} \binom{n}{k} + \sum_{k=0}^{n} \binom{n}{k} = 2^n + 2^n = 2^{n+1}.$$

(c) Protože $\binom{n}{k} = \binom{n}{n-k}$, platí

$$k \cdot \binom{n}{k} + (n-k) \cdot \binom{n}{n-k} = n \cdot \binom{n}{k} = \frac{n}{2} \cdot \left[\binom{n}{k} + \binom{n}{n-k} \right].$$

Odtud

$$\sum_{k=0}^{n} k \cdot \binom{n}{k} = \frac{n}{2} \cdot \sum_{k=0}^{n} \cdot \binom{n}{k} = \frac{n}{2} \cdot 2^n = n \cdot 2^{n-1}.$$

(d) Přímým výpočtem dostáváme

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \binom{n}{0} + \sum_{k=1}^{n} (-1)^k \left[\binom{n-1}{k-1} + \binom{n-1}{k} \right] =$$

$$= \binom{n}{0} + \sum_{k=0}^{n-1} (-1)^{k+1} \binom{n-1}{k} + \sum_{k=1}^{n-1} (-1)^k \binom{n-1}{k} =$$

$$= -\sum_{k=1}^{n-1} (-1)^k \binom{n-1}{k} + \sum_{k=1}^{n-1} (-1)^k \binom{n-1}{k} = 0.$$

•

Často je užívána i následující formule.

2.16. Věta. *Pro každé reálné x a každé $n \in \mathbb{N}_0$ platí:*

$$\sum_{k=0}^{n} \binom{x+k}{k} = \binom{x}{0} + \binom{x+1}{1} + \binom{x+2}{2} + \cdots + \binom{x+n}{n} = \binom{x+n+1}{n}.$$

Důkaz. Indukcí. Pro $n = 0$ je rovnice správná. Nechť tedy uvedený vztah platí pro $n \geq 0$. Pak

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

$$= \binom{x+n+1}{n} + \binom{x+n+1}{n+1} = \binom{x+n+2}{n+1}.$$

•

Dosadíme-li ve větě 2.16 $n-k$ místo k a x místo $x+n$, dostaneme okamžitě tvrzení následujícího důsledku.

2.17. Důsledek.

$$\sum_{k=0}^{n} \binom{x-k}{n-k} = \binom{x}{n} + \binom{x-1}{n-1} + \binom{x-2}{n-2} + \cdots + \binom{x-n}{0} = \binom{x+1}{n}.$$

POZNÁMKY A CVIČENÍ

1. Dokažte, že

$$\sum_{k=1}^{n} (k \cdot k!) = (n+1)! - 1.$$

2. Dokažte, že pro Stirlingova čísla 1. druhu platí vztah

$$\sum_{k=1}^{n} s(n,k) = 0, \qquad n > 1.$$

3. Dokažte identitu

$$\sum_{k=0}^{n} (-1)^k \binom{x}{k} = \binom{n-x}{n} = (-1)^n \binom{x-1}{n} = \prod_{k=1}^{n} \left(1 - \frac{x}{k}\right).$$

4. Tzv. *Catalanovu posloupnost* 1, 2, 5, 14, 42, 132, 429, 1 430, 4 862, ... definovanou vztahem

$$c_n = \frac{\binom{2n}{n}}{n+1}$$

studoval již Euler. Dokažte, že platí:

a) $c_2 = 2c_1$

b) $c_3 = 3c_2 - c_1$

c) $c_4 = 4c_3 - 3c_2$

d) $c_5 = 5c_4 - 6c_3 + c_2$

e) $c_6 = 6c_5 - 10c_4 + 4c_3$

f) $c_7 = 7c_6 - 15c_5 + 10c_4 - c_3$

g) $c_n = \binom{2n-1}{n-1} - \binom{2n-1}{n+1} = \binom{2n}{n} - \binom{2n}{n-1}$

h) $c_{n+1} = \dfrac{(2n+2)\cdot(2n+1)}{(n+2)\cdot(n+1)} \cdot c_n$

3 Základní kombinatorické pojmy

Nejprve zavedeme označení, které budeme v dalším textu dodržovat.

3.1. Označení. Počet prvků konečné množiny X značíme $|X|$. Symbolem $\mathcal{P}(X)$ označíme, jak je obvyklé, množinu všech podmnožin množiny X. Pro $k \in \mathbb{N}_0$ označme

$$\mathcal{P}_k(X) = \{A;\ A \subseteq X, |A| = k\}.$$

Mnoho kombinatorických úvah je založeno na následujícím zřejmém faktu.

3.2. Věta. *Buďte A, B konečné množiny. Pak* $|A \times B| = |A| \cdot |B|$.

3.3. Poznámka. Jinými slovy je věta 3.2 často formulována jako tzv. *pravidlo součinu* následovně:

Lze-li objekt X vybrat r způsoby a po každém takovém výběru lze objekt Y vybrat s způsoby, pak lze uspořádanou dvojici $[X, Y]$ vybrat $r \cdot s$ způsoby.

Jako aplikaci věty 3.2 uveďme tvrzení, které v roce 1935 odvodili maďarští matematikové P. Erdös a G. Szekeres.

3.4. Věta. *Každá posloupnost $a_1, a_2, \ldots, a_{mn+1}$, která obsahuje $mn + 1$ navzájem různých celých čísel nutně obsahuje klesající vybranou podposloupnost o více než m prvcích nebo rostoucí vybranou podposloupnost o více než n prvcích.*

Důkaz. Pro každé $i = 1, 2, \ldots, mn + 1$ označme k_i počet čísel v nejdelší klesající podposloupnosti s prvním prvkem a_i a analogicky nechť r_i značí počet prvků v nejdelší rostoucí podposloupnosti začínající prvkem a_i.

Předpokládejme, že tvrzení věty neplatí. Pak pro každé i platí $1 \leq k_i \leq \leq m$, $1 \leq r_i \leq n$, takže zobrazení $a_i \to [k_i, r_i]$ je zobrazením množiny $\{a_1, a_2, \ldots, a_{mn+1}\}$ do kartézského součinu $\{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}$. Ukážeme, že toto zobrazení je prosté.

Nechť je $i < j$. Pak platí $a_i < a_j$ nebo $a_i > a_j$ (neboť čísla a_i, a_j jsou podle předpokladu různá). Je-li $a_i < a_j$, pak platí zřejmě $r_i > r_j$, je-li $a_i > a_j$, platí zase $k_i > k_j$. V obou případech je $[k_i, r_i] \neq [k_j, r_j]$. To je však spor, neboť nemůže existovat injekce množiny o $mn + 1$ prvcích do množiny o mn prvcích. •

3.5. Definice. Buď $n \in \mathbb{N}$, $|X| = n$. Pro $k \in \mathbb{N}$, $k \leq n$ nazveme *variací k-té třídy v X* každý řetězec $(A, \leq)$, kde $A \in \mathcal{P}_k(X)$.

3.6. Věta. *Buďte $k \leq n$ přirozená čísla. Nechť $|X| = n$. Počet variací k-té třídy v X je roven číslu*

$$(n)_k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1).$$

Důkaz. Tvrzení plyne z pravidla součinu. První prvek lze vybrat n způsoby, druhý $n-1$ způsoby atd. •

3.7. Poznámka. Počet uspořádaných k-tic bez opakování z n prvků je tedy roven číslu $(n)_k$ pro libovolná $n, k \in \mathbb{N}$ (neboť pro $k > n$ je $(n)_k = 0$ podle definice).

3.8. Důsledek. *Buďte X, Y konečné množiny, $|X| = n$, $|Y| = k$. Pak pro množinu* $\operatorname{inj}(X^Y)$ *všech injekcí Y do X platí*

$$\left|\operatorname{inj}(X^Y)\right| = (n)_k.$$

3.9. Definice. Variace n-té třídy z n prvkové množiny se nazývají *permutace* této množiny.

Z věty 3.6 okamžitě plyne.

3.10. Věta. *Počet permutací n prvkové množiny je roven číslu $(n)_n = n!$.*

3.11. Poznámka. Je-li $X = \{1, 2, \ldots, n\}$, je podle definice 3.9 permutací množiny X každý řetězec $\{a_1 < a_2 < \cdots < a_n\}$, kde $a_i \in X$ pro každé i. Zapíšeme-li tento řetězec jako uspořádanou n-tici $[a_1, a_2, \ldots, a_n]$, můžeme danou permutaci ztotožnit se zobrazením $i \to a_i$. Toto zobrazení je obvyklé zapisovat ve tvaru

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

Jinými slovy, za permutace množiny X můžeme považovat bijekce množiny X na sebe.

Odtud a z věty 3.10 okamžitě plyne

3.12. Důsledek. *Buďte X, Y konečné množiny. Pak pro množinu* $\operatorname{bij}(Y^X)$ *všech bijekcí X na Y platí*

$$\left|\operatorname{bij}(Y^X)\right| = \begin{cases} 0 & \textit{je-li } |X| \neq |Y|, \\ |Y|! & \textit{je-li } |X| = |Y|. \end{cases}$$

3.13. Definice. Buď X konečná množina, $k \in \mathbb{N}_0$ buď libovolné. *Kombinací k-té třídy z X* rozumíme každou k prvkovou podmnožinu množiny X. (Množina $\mathcal{P}_k(X)$ je tedy množinou všech kombinací k-té třídy z X.)

Z vět 3.6 a 3.10 bezprostředně plyne

3.14. Věta. *Buď X konečná množina, $|X| = n$. Pak pro každé $k \in \mathbb{N}_0$ platí*

$$|\mathcal{P}_k(X)| = \frac{(n)_k}{k!} = \binom{n}{k}.$$

3.15. Příklad. *Kolika způsoby můžeme na šachovnici (o 64 polích) rozestavit 8 věží tak, aby se žádné dvě z nich vzájemně neohrožovaly?*

Tomu, kdo ví, jak se v šachu tahá věží, je zřejmé, že hledáme právě všechna taková rozestavění věží, kdy v každé řadě a v každém sloupci stojí právě jedna věž. Očíslujeme-li pevně řady a sloupce čísly $1, \dots, 8$, je poloha každé figury na šachovnici jednoznačně určena dvojicí $[i, j]$, kde i je číslo řady a j číslo sloupce. Odtud je zřejmé, že hledaných rozestavení je $8! = 40\,320$.

3.16. Příklad. (a) *Kolika způsoby můžeme rozestavit 6 dětí do kruhu?*

Do řady lze rozestavit 6 dětí $6! = 720$ způsoby. Protože z každé řady utvoříme evidentním způsobem kruh, je počet takto vzniklých kruhů rovněž 720. Vzhledem k tomu, že však nerozlišíme dva kruhy lišící se jen pootočením, je hledaný počet $\frac{720}{6} = 120$.

(b) *Kolik náhrdelníků lze utvořit ze 6 korálků 6 různých barev?*

Mohlo by se zdát, že podle (a) je správná odpověď 120. Protože však nerozlišíme dva náhrdelníky, z nichž jeden vznikl „převrácením" druhého, je hledaný počet $\frac{120}{2} = 60$.

3.17. Příklad. Buď A množina všech možných pořadí 16 oddílů v 1. fotbalové lize. Pro $x, y \in A$ položme $x \sim y \iff$ v x, y je stejné pořadí na prvních třech místech a stejné dva oddíly sestupují. Určete $|A/_\sim|$.

Ze zadání plyne, že $|A| = 16!$. Relace $\sim$ je zřejmě ekvivalence na A, takže má smysl se ptát po počtu prvků faktormnožiny $A/_\sim$.

Protože pořadí mužstev na prvních třech místech je možno určit $(16)_3$ způsoby a ze zbývajících mužstev můžeme dvě sestupující určit $\binom{13}{2}$ způsoby, platí

$$|A/_\sim| = (16)_3 \cdot \binom{13}{2} = 16 \cdot 15 \cdot 14 \cdot \frac{13 \cdot 12}{2} = 262\,080.$$

Prozatím jsme hovořili o variacích, permutací a kombinacích *bez opakování*. Nyní budeme uvažovat případy, kdy se prvky dané množiny mohou v uvedených výběrech opakovat.

3.18. Definice. Buď $X \neq \emptyset$ konečná množina, $|X| = n$. Nechť $k \in \mathbb{N}_0$ je libovolné. Uspořádanou k-tici prvků z množiny X, v níž se prvky mohou opakovat, nazýváme *k-variace s opakováním* z prvků množiny X. Počet všech k-variací s opakováním označme $V(n, k)$.

3.19. Poznámka. V této souvislosti je nutno **důrazně** upozornit na některé nesprávné (a časté) představy, které si řada studentů přináší již ze střední školy. Tyto omyly se týkají jak **opakování** tak **určování pořadí** prvků v dané variaci.

V řadě příkladů, ať již uměle vykonstruovaných či vzniklých při řešení faktických problémů, opakování prvků ve variaci **může a nemusí** znamenat skutečné opakování konkrétních objektů. Když je například v osudí deset cifer $0, 1, \dots, 9$ a tvoříme několikamístné číslo tak, že vytáhneme číslo z osudí a opět je do osudí vrátíme, může být samozřejmě vytaženo znovu. Ve vzniklé variaci se tedy opravdu opakuje týž objekt.

Častěji však užíváme variace *s opakováním* v případě, že se sice neopakuje stejný objekt, nás však zajímají jen některé vlastnosti objektů tvořících „základní" množinu, z níž variace tvoříme. Prvky, které mají stejnou vlastnost, pak nerozlišujeme, ač samozřejmě, „rozlišitelné" jsou. Vybereme-li například ve třídě (v níž je například 20 hochů a 10 dívek) 6 dětí a uspořádáme je do zástupu, obdržíme šestiprvkovou variaci, v níž se samozřejmě žádný prvek – žák neopakuje. Když se však například rozhodneme, že pro nás za jistých okolností bude podstatné pouze to, zda daný žák je hoch nebo dívka, avšak hochy, resp. dívky navzájem nebudeme rozlišovat, je možno **tutéž** šestici žáků považovat za variaci s opakováním, kde ovšem opakování neznačí opakování žáka, ale opakování vlastnosti „hoch" nebo „dívka". Jinak řečeno, variace s opakováním lze chápat jsko uspořádané k-tice prvků několika druhů, přičemž navzájem **nerozlišujeme** předměty téhož druhu, ačkoliv tyto předměty jinak mohou být rozlišitelné.

Druhý častý omyl u variací (ať již s opakováním či bez opakování) souvisí s „pořadím" prvků ve variacích.

Toto pořadí **může a nemusí** souviset s jejich vybíráním z dané množiny objektů.

Vytahujeme-li čísla z osudí a postupně je zapisujeme, je samozřejmě jejich pořadí určeno pořadím jejich vybrání z osudí. Když však vybereme ze třídy několik dětí a pak je seřadíme například podle výšky, nesouvisí obecně jejich pořadí v dané variaci vůbec s tím, v jakém pořadí jsme je ve třídě vybírali.

Proto je **zcela nesmyslné** tvrdit, že variace je skupina objektů, u nichž *záleží na pořadí, v jakém jsme je vybírali.*

3.20. Věta. *Pro každé* $n, k \in \mathbb{N}_0$ *platí* $V(n, k) = n^k$.

Důkaz. Indukcí vzhledem k číslu k. Tvrzení $V(n, 0) = n^0 = 1$ je zřejmé. Nechť tedy $V(n, k) = n^k$. Buď $[a_1, \dots, a_k]$ libovolná k-variace s opakováním. Je zřejmé, že počet $(k + 1)$-variací tvaru $[a_1, \dots, a_k, x]$ je roven číslu n. Odtud plyne, že $V(n, k + 1) = n \cdot V(n, k) = n \cdot n^k = n^{k+1}$. •

3.21. Příklad. Buďte X, Y konečné množiny. Nechť $X = \{a_1, \dots, a_k\}$. Přiřadíme-li každému zobrazení $f\colon X \to Y$ uspořádanou k-tici $[f(a_1), \dots, f(a_k)]$, vidíme okamžitě, že

$$\left|Y^X\right| = V(|X|, |Y|) = |Y|^{|X|}.$$

3.22. Definice. Buď $k \in \mathbb{N}$ libovolné. Buď dáno n předmětů k druhů. Nechť n_i značí počet předmětů i-tého druhu, $i = 1, \dots, k$. (Tj. $n_1 + \cdots + n_k = n$.) Symbolem $P(n_1, \dots, n_k)$ označme počet prvků množiny všech uspořádaných n-tic těchto předmětů. Tyto n-tice nazýváme *permutace s opakováním.*

Z věty 3.10 okamžitě plyne

3.23. Věta. *Pro každá čísla* $n_1, \dots, n_k \in \mathbb{N}_0$ *platí*

$$P(n_1, \dots, n_k) = \frac{(n_1 + \cdots + n_k)!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}.$$

3.24. Příklad. (a) *Kolik různých čísel lze utvořit z čísla* 3 855 835 *přeskupením cifer?*

Protože dané číslo obsahuje dvě cifry 3, tři cifry 5 a dvě cifry 8, je hledaný počet

$$P(2, 3, 2) = \frac{7!}{2! \cdot 3! \cdot 2!} = 210.$$

(b) Když Christian Huygens objevil Saturnův prstenec, zašifroval svůj objev, jak bylo v té době časté, do následujícího tzv. *anagramu*:

aaaaaaa ccccc d eeeee g h iiiiii llll mm nnnnnnnnn
oooo pp q rr s ttttt uuuuu

Náležitým uspořádáním písmen dostaneme zprávu *Annulo cingitur tenui, plano, nusquam cohaerente, ad eclipticam inclinato.* Česky: *Obklopen prstencem tenkým, plochým, nikde nezavěšeným, nakloněným k ekliptice.*

Určíme, za jak dlouho by počítač, který by vypsal milión permutací Huygensova anagramu za sekundu, vypsal všechny permutace.

Spočtěme, kolik je všech permutací daného anagramu. Z počtu jednotlivých písmen v anagramu plyne, že všech permutací je

$$P(7,5,1,5,1,1,7,4,2,9,4,2,1,2,1,5,5) = \frac{62!}{9!\cdot(7!)^2\cdot(5!)^4\cdot(4!)^2\cdot(2!)^3}.$$

Toto číslo je přibližně rovno číslu $3{,}573\cdot 10^{60}$. Počítač by tedy potřeboval více než 10^{54} sekund. O velikosti tohoto čísla si uděláme představu, když si uvědomíme, že trvání našeho vesmíru – tj. přibližně 15 miliard roků – je méně než 10^{17} sekund.

3.25. Poznámka. Zajímavé aplikace čísel $P(n_1,\dots,n_k)$ lze najít například v úvahách o tzv. *svazu k-tic.*

Buď k přirozené číslo. Symbolem $\mathbb{N}_0^k$ označme množinu všech uspořádaných k-tic $[a_1,\dots,a_k]$ nezáporných celých čísel. Definujeme-li na $\mathbb{N}_0^k$ relaci $\le$ takto:

$$[a_1,\dots,a_k]\le[b_1,\dots,b_k] \iff a_i\le b_i \text{ pro všechna } i=1,\dots,k,$$

je zřejmé, že relace $\le$ je uspořádání na množině $\mathbb{N}_0^k$. Přitom je evidentní, že $(\mathbb{N}_0^k,\le)$ je svaz, v němž

$$\begin{aligned}\sup\{a,b\} &= [\max(a_1,b_1),\dots,\max(a_k,b_k)],\\ \inf\{a,b\} &= [\min(a_1,b_1),\dots,\min(a_k,b_k)].\end{aligned}$$

Svaz $\mathbb{N}_0^k$ můžeme reprezentovat následujícím způsobem. Bod $[a_1,\dots,a_k]\in$ $\in\mathbb{N}_0^k$ znázorníme jako bod eukleidovského prostoru $\mathbb{E}_k$ a dva body $\mathbf{a}=$ $=[a_1,\dots,a_k]$, $\mathbf{b}=[b_1,\dots,b_k]$ spojíme šipkou směřující z $\mathbf{a}$ do $\mathbf{b}$ právě tehdy, když existuje index i takový, že

$$a_j=\begin{cases} b_j & \text{pro } j\neq i,\\ b_j+1 & \text{pro } j=i.\end{cases}$$

(Tzn., že z **a** do **b** vede šipka právě tehdy, když **a** pokrývá **b** ve svazu $(\mathbb{N}_0^k,\le)$.)

Nyní se pokusme určit počet „cest“ z bodu **a** do bodu **b** pro každé dva prvky $\mathbf{a},\mathbf{b}\in\mathbb{N}_0^k$, $\mathbf{a}\le\mathbf{b}$. (Cestou rozumějme posloupnost na sebe napojených šipek.)

032	→	022	→	012	→	002	→	001	→	000
032	→	022	→	012	→	011	→	001	→	000
032	→	022	→	012	→	011	→	010	→	000
032	→	022	→	021	→	011	→	001	→	000
032	→	022	→	021	→	011	→	010	→	000
032	→	022	→	021	→	020	→	010	→	000
032	→	031	→	021	→	011	→	001	→	000
032	→	031	→	021	→	011	→	010	→	000
032	→	031	→	021	→	020	→	010	→	000
032	→	031	→	030	→	020	→	010	→	000

Tab. 3.1: Cesty z bodu 032 do bodu 000

Tak například v $\mathbb{N}_0^3$ existuje 10 cest z bodu 032 do bodu 000 znázorněných v tabulce 3.1.

Buďte nyní $\mathbf{a} = [a_1, \ldots, a_k]$, $\mathbf{b} = [b_1, \ldots, b_k]$ libovolné dva prvky v $\mathbb{N}_0^k$, takové, že $\mathbf{a} \leq \mathbf{b}$. Označme $a_i - b_i = n_i$, $i = 1, \ldots, k$. Definujme pro $i = 1, \ldots, k$ zobrazení $\alpha_i \colon \mathbb{N}_0^k \to \mathbb{N}_0^k$ takto:

$$\alpha_i[x_1, \ldots, x_k] = [x_1, \ldots, x_{i-1}, x_i - 1, x_{i+1}, \ldots, x_k].$$

Nyní přiřaďme každé cestě z $\mathbf{a}$ do $\mathbf{b}$ odpovídající posloupnost zobrazení α_i. (Tak např. cestě z bodu 032 do bodu 000 uvedené na prvním řádku v tabulce 3.1 odpovídá posloupnost $\alpha_2, \alpha_2, \alpha_2, \alpha_3, \alpha_3$, poslední cestě pak posloupnost $\alpha_3, \alpha_3, \alpha_2, \alpha_2, \alpha_2$.) Je zřejmé, že popsané přiřazení je bijekcí množiny cest z $\mathbf{a}$ do $\mathbf{b}$ na množinu všech posloupností utvořených z α_i tak, že se v nich α_i vyskytuje n_i-krát. Odtud plyne, že hledaných cest je

$$P(n_1, \ldots, n_k) = \frac{\left(\sum\limits_{i=1}^{k}(a_i - b_i)\right)!}{(a_1 - b_1)! \cdot \ldots \cdot (a_k - b_k)!}.$$

3.26. Definice. Mějme dostatečný počet prvků n druhů. Skupinu k objektů, v níž nezáleží na pořadí a v níž navzájem nerozlišujeme předměty téhož druhu, nazýváme *k-kombinace s opakováním*. Počet těchto k-kombinací s opakováním označme $C(n, k)$.

3.27. Věta. *Pro každé $n, k \in \mathbb{N}_0$ platí* $C(n, k) = \binom{n+k-1}{k}$.

Důkaz. Pro $n = 0$ nebo $k = 0$ je tvrzení triviální. Nechť tedy $n \neq 0 \neq$ $\neq k$. Každou k-kombinaci s opakováním lze velmi jednoduše (a jednoznačně) popsat pomocí posloupnosti nul a jedniček takto: nechť je dána posloupnost $a_1, a_2, \dots, a_{k+n-1}$, v níž je k jedniček a $n - 1$ nul. Přiřaďme této posloupnosti k-kombinaci s opakováním, v níž je tolik předmětů 1. druhu, kolik je v dané posloupnosti jedniček před první nulou, tolik předmětů druhého druhu, kolik je v dané posloupnosti jedniček mezi první a druhou nulou atd. Zřejmě nyní platí:

$$C(n, k) = P(k, n-1) = \frac{(n+k-1)!}{k!(n-1)!} = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}.$$

●

3.28. Poznámka. Pro pojem kombinace **s opakováním** bychom mohli zopakovat téměř vše, co jsme již uvedli v poznámce 3.19.

I u kombinací s opakováním může a nemusí uvedené „opakování“ značit, že se opakuje týž předmět. Když se dohodneme, že objekty s jistou vlastností budeme **považovat za nerozlišitelné**, může opakování značit opakování objektů stejné vlastnosti, přestože jinak tyto objekty mohou samozřejmě být rozlišitelné.

Z důvodů uvedených v poznámce 3.19 je navíc nesmyslné tvrdit, že u kombinací *nezáleží na pořadí, v němž byly prvky vybírány*. Jak jsme viděli, nemusí na tomto pořadí záviset ani u variací.

Upozorňujeme ještě, že v definici 3.26 nelze slovo „skupina“ nahradit termínem „množina“. Skupina tří prvků (například písmen a, a, b) není totéž jako množina $\{a, a, b\}$, neboť ta má jen dva prvky; je to jen nešikovně napsaná množina, neboť v **množině** se žádný prvek opakovat nemůže. (Pro úplnost dodejme, že i množina $\{a, b\}$ je dvouprvková pouze tehdy, když a, b neznamenají týž objekt.)

3.29. Příklad. Buďte X, Y konečné řetězce. Zjistíme, *kolik existuje izotonních zobrazení X do Y.*

Nechť $X = \{x_1 < x_2 < \cdots < x_k\}$, $Y = \{y_1 < y_2 < \cdots < y_n\}$. Buď $f\colon X \to Y$ izotonní zobrazení. Pak platí $f(x_1) \leq f(x_2) \leq \ldots \leq f(x_k)$, takže izotonních zobrazení X do Y je tolik jako všech neklesajících k-tic prvků z Y. To, že k-ticím (v nichž se prvky mohou opakovat) předepíšeme pevně pořadí, je totéž, jako když pořadí prvků v k-ticích nerozlišujeme. Podle věty 3.27 je tedy izotonních zobrazení X do Y

$$C(|Y|, |X|) = \binom{|X| + |Y| - 1}{|X|}.$$

3.30. Příklad. (a) *Kolika způsoby můžeme mezi 4 chlapce rozdělit 50 stejných kuliček?*

Postupujeme jako v důkazu věty 3.27. Přidejme k 50 kuličkám 3 kamínky. Poskládáme-li kuličky s kamínky do řady, rozdělí 3 kamínky posloupnost na 4 úseky. Označíme-li chlapce A, B, C, D a chlapci A dáme všechny kuličky z prvního úseku, chlapci B všechny kuličky z druhého úseku atd., je ihned zřejmé, že všech rozdělení je

$$P(50, 3) = \binom{53}{3} = \frac{53 \cdot 52 \cdot 51}{3 \cdot 2} = 23\,426.$$

(b) Pozměňme příklad (a) tak, že budeme požadovat, aby *každý chlapec dostal alespoň jednu kuličku.*

Podle (a) tedy chceme zjistit, v kolika posloupnostech 50 kuliček a 3 kamínků nejsou žádné dva kamínky vedle sebe a rovněž není kamínek ani na prvním ani na posledním místě posloupnosti. Tento počet zjistíme jednoduchým obratem. Dáme-li každému chlapci předem jednu kuličku, zůstane jich 46, které pak již můžeme rozdělit libovolně. Hledaných rozdělení je tak

$$P(46, 3) = \binom{49}{3} = \frac{49 \cdot 48 \cdot 47}{3 \cdot 2} = 18\,424.$$

Následující úloha je velmi jednoduchá, v dalším se však na ni budeme několikrát odvolávat.

3.31. Příklad. *Mějme p prvků 1. druhu a q prvků 2. druhu. Kolik existuje permutací s opakováním těchto prvků takových, že žádné dva prvky 1. druhu nestojí vedle sebe?*

Hledaných permutací je zřejmě tolik, kolika způsoby lze rozmístit p prvků 1. druhu do $q - 1$ mezer mezi prvky 2. druhu a před první a za poslední z nich, tj. celkem na $q + 1$ míst. Tzn., že hledaný počet je $\binom{q+1}{p}$ pokud je $p \leq q + 1$ a je roven 0, pokud $p > q + 1$.

3.32. Příklad. *Buď dán $(c+m)$-úhelník $A_1 A_2 \ldots A_{c+m}$, kde $c, m \in \mathbb{N}$, $c+m \geq$ ≥ 3. Kolika způsoby lze obarvit jeho vrcholy tak, aby jich bylo c červených, m modrých a žádné dva sousední vrcholy nebyly červené?*

Označme hledaný počet obarvení $t(c, m)$. Je zřejmé, že pro $c > m$ je $t(c, m) = 0$. Nechť tedy $c \leq m$. Úlohu lehce vyřešíme pomocí úlohy 3.31. Označíme-li výsledek příkladu 3.31 symbolem $r(p, q)$, je zřejmě takových „přípustných" obarvení vrcholů, při nichž je vrchol A_1 červený, celkem

$r(c-1, m-2)$. Přípustných obarvení, při nichž je A_1 modrý, je $r(c, m-1)$. Odtud

$$t(c, m) = r(c-1, m-2) + r(c, m-1) = \binom{m-1}{c-1} + \binom{m}{c} = \frac{c+m}{m}\binom{m}{c}.$$

3.33. Příklad. *Muž prodávající Večerník (za 5 korun) u sebe nemá na začátku prodeje žádné peníze. Ihned se před ním utvořila fronta m + k lidí, přičemž m lidí má u sebe pouze desetikorunovou minci a k lidí pouze pětikorunu. Kolika způsoby se tito lidé mohou postavit do fronty tak, aby měl prodávající vždy nazpět na desetikorunu?* (Rozlišujeme rozestavení „pětikorun" a „desetikorun" a nikoliv jednotlivé lidi se stejnou mincí.)

Počet všech možných rozestavení „pětikorun" a „desetikorun" do fronty je počet příslušných permutací s opakováním, tj.

$$P(m, k) = \frac{(m+k)!}{m! \cdot k!} = \binom{m+k}{k}.$$

Dále je zřejmé, že úloha má alespoň jedno řešení právě tehdy, když $m \leq k$; jinak se totiž prodej nutně zastaví. V dalším tedy předpokládáme, že platí $0 \leq m \leq k$.

Každé rozestavení lidí ve frontě můžeme evidentně zapsat jako posloupnost m jedniček (označujících lidi s desetikorunou) a k pětek (označujících lidi s pětikorunou). Podle zadání hledáme počet „příznivých" permutací, tj. takových permutací $(a_1, \dots, a_{k+m})$ m jedniček a k pětek, které mají následující vlastnost: pro každé d takové, že $1 \leq d \leq m+k$ je mezi prvky $a_1, \dots, a_d$ alespoň tolik pětek jako jedniček.

Nejprve dokážeme, že počet *nepříznivých* případů je roven číslu

$$P(m-1, k+1) = \binom{m+k}{k+1}.$$

Nechť tedy $a_1, \dots, a_{k+m}$ je nějaká nepříznivá permutace. Nechť d_0 je nejmenší index takový, že mezi prvky $a_1, \dots, a_{d_0}$ je více jedniček než pětek. Pak zřejmě $d_0 = 2s+1$, přičemž mezi prvky $a_1, \dots, a_{2s}$ je s jedniček a s pětek. Připíšeme-li před zadanou permutaci jednu pětku, dostaneme tak permutaci m jedniček a $k+1$ pětek. V této permutaci stojí na prvním místě pětka a mezi prvními $2s+2$ členy je nyní $s+1$ jedniček a $s+1$ pětek.

Nyní v permutaci $5, a_1, \dots, a_{k+m}$ zaměňme na prvních $2s+2$ místech vzájemně pětky a jedničky. Původní nepříznivé permutaci $a_1, \dots, a_{k+m}$ tak popsaným způsobem přiřadíme permutaci m jedniček a $k+1$ pětek, v níž na prvním místě stojí cifra 1. Přitom je zřejmé, že různým nepříznivým permutacím jsou přiřazeny různé permutace uvedeného typu.

Nyní ukážeme, že *každá* posloupnost m jedniček a $k+1$ pětek s jedničkou na začátku je přiřazena některé nepříznivé permutaci.

Buď tedy $b_0, b_1, \dots, b_{k+m}$ libovolná permutace m jedniček a $k+1$ pětek, $b_0 = 1$. Protože platí $m \le k$ (podle předpokladu), existuje nejmenší index d_0 takový, že mezi členy $b_0, b_1, \dots, b_{d_0}$ je stejný počet jedniček jako pětek. Zaměníme-li v posloupnosti $b_0, b_1, \dots, b_{d_0}$ vzájemně jedničky a pětky a pak vynecháme první cifru (tj. pětku), dostaneme zřejmě onu nepříznivou permutaci, jíž je přiřazena daná permuatce $b_0, b_1, \dots, b_{k+m}$.

Zjistili jsme tak, že počet všech nepříznivých rozestavení fronty kupujících je roven počtu všech permutací, v nichž je m jedniček a $k+1$ pětek a v nichž na prvním místě stojí jednička. Vynecháme-li tuto první jedničku, dostaneme právě všechny permutace $m-1$ jedniček a $k+1$ pětek, jichž je $P(m-1, k+1) = \binom{m+k}{k+1}$. Protože všech permutací je, jak jsme již uvedli, $P(m,k) = \binom{m+k}{k} = \binom{m+k}{m}$, je počet všech příznivých permutací $\binom{m+k}{m} - \binom{m+k}{m-1} = \frac{k-m+1}{k+1}\binom{m+k}{m}$.

Je-li zejména $m = k$, tj. ve frontě je stejný počet lidí s desetikorunou jako s pětikorunou, může stát fronta bez zdržování celkem

$$\frac{1}{k+1}\binom{2k}{k}$$

způsoby.

Poznámky a cvičení

1. Kolika způsoby můžeme na šachovnici vybrat

(a) dvě pole (2 016)

(b) dvě pole různých barev (1 024)

(c) dvě pole neležící ve stejné řadě ani ve stejném sloupci (1 568)

(d) dvě pole různé barvy splňující podmínku (c) (768)

2. Nechť $p_1, \dots, p_n$ jsou navzájem různá prvočísla, $k_1, \dots, k_n$ buďte libovolná přirozená čísla. Určete součet všech dělitelů čísla

$$q = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}.$$

(Mezi dělitele počítáme i čísla 1 a q.)

$$\left(\frac{p_1^{k_1+1}-1}{p_1-1}\cdot\ldots\cdot\frac{p_n^{k_n+1}-1}{p_n-1}\right)$$

3. Kolik existuje šesticiferných čísel, v nichž se vyskytují tři liché a tři sudé cifry?

(281 250)

4. Stěny každé ze tří hracích kostek jsou očíslovány čísly 1, 4, 13, 40, 121 a 364. Kolik různých součtů lze získat při hodu těmito kostkami? (56)

5. Máme čtyři bílé koule, čtyři černé koule a čtyři červené koule. Kolika způsoby je můžeme rozdělit do 6 rozlišitelných přihrádek? (2 000 376)

6. Havajská abeceda má 12 písmen: samohlásky *a, e, i, o, u*, souhlásky *h,k,l,m,n,p,w*.

a) Dokažte, kolik lze utvořit slov o čtyřech písmenech.

b) Kolik z uvedených slov má na druhém a čtvrtém místě samohlásku a na zbývajících místech souhlásku?

c) Kolik slov má na druhém a čtvrtém místě samohlásku?

7. Každý člověk má dva (biologické) rodiče, 4 prarodiče atd. Kolik předků má každý z nás ve 20 předešlých generacích (cca v posledním půl tisíciletí)?

8. *Palindrom* je posloupnost symbolů, která je stejná, čteme-li je zepředu i zezadu (například „tabat“). Určete počet sedmiciferných a osmiciferných palindromů (v dekadickém zápisu), nesmí-li se žádná číslice užít více než dvakrát.

9. Dokažte, že každé palindromické číslo sudé délky je dělitelné číslem 11.

10. Určete celkový počet přirozených čísel, v jejichž dekadickém zápisu se neopakuje žádná cifra.

11. V městské radě je 10 zástupců levice a 11 zástupců pravice. Levici zastupují 4 ženy, pravici 3 ženy. Určete, kolika způsoby lze sestavit osmičlenný výbor, v němž má být stejný počet zástupců levice i pravice a stejný počet mužů i žen.

4 Rozklady konečných množin

Víme, že *rozkladem na množině* A rozumíme systém $\overline{A}$ neprázdných po dvou disjunktních množin, jejichž sjednocením je množina A. Prvky systému $\overline{A}$ nazýváme *třídy rozkladu* $\overline{A}$. Systém $\mathcal{K}(A)$ všech rozkladů na množině A uspořádáme relací $\leq$ definovanou pomocí *zjemnění*, tj. pro $\overline{X}, \overline{Y} \in \mathcal{K}(A)$ platí

$$\overline{X} \leq \overline{Y} \iff (U \in \overline{X}, V \in \overline{Y}, U \cap V \neq \emptyset \Rightarrow U \subseteq V).$$

Snadno lze dokázat, že $(\mathcal{K}(A), \leq)$ je úplný svaz izomorfní s úplným svazem $(\mathcal{E}(A), \subseteq)$ všech ekvivalencí na množině A.

V tomto paragrafu určíme $|\mathcal{K}(A)|$ pro konečnou množinu A a určíme počet rozkladů na třídy o jistých předepsaných vlastnostech.

4.1. Definice. Označme B_n počet všech rozkladů na n prvkové množině, $n \in \mathbb{N}$. Čísla B_n se nazývají *Bellova čísla.*

Bellova čísla se často vyskytují v řadě aplikací. Nejprve odvodíme rekurentní formuli pro jejich výpočet.

4.2. Věta.

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k, \qquad B_0 = 1.$$

Důkaz. Předpokládejme, že známe čísla $B_1, \ldots, B_n$ a chceme určit číslo B_{n+1}. Buď X libovolná množina o n prvcích. Buď $a \notin X$ libovolný prvek. Položíme-li $X_1 = X \cup \{a\}$, je $|X_1| = n + 1$.

Buď $\overline{X_1}$ libovolný rozklad množiny X_1. Prvek a leží v některé třídě rozkladu $\overline{X_1}$. Tato třída může mít $1, 2, \ldots, n + 1$ prvků.

Spočtěme, kolik je na $\overline{X_1}$ rozkladů takových, že prvek a leží ve třídě o k prvcích. Zbývajících $k - 1$ prvků v této třídě můžeme z množiny X_1 vybrat $\binom{n}{k-1}$ způsoby. Máme-li utvořenu třídu obsahující prvek a, můžeme na zbývajících $n - k + 1$ prvcích zvolit libovolný rozklad. Podle předpokladu je těchto rozkladů B_{n-k+1}. Podle pravidla součinu odtud plyne, že prvek a leží v k-prvkové třídě $(k = 1, \ldots, n + 1)$ v

$$\binom{n}{k-1} B_{n-k+1} = \binom{n}{n-k+1} B_{n-k+1}$$

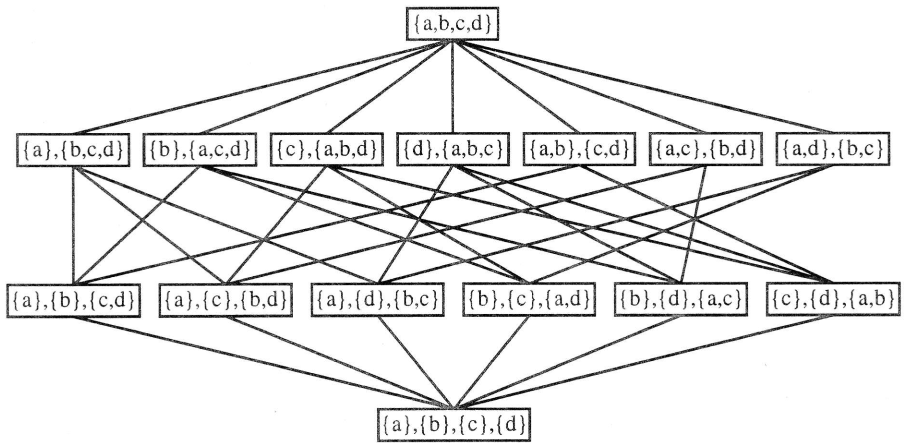
rozkladech. B_0 přitom značí počet rozkladů, kdy a leží ve třídě o mohutnosti $n+1$, tj. $B_0 = 1$.

Počet všech rozkladů na X_1 je roven součtu všech výše uvedených možností. To je však právě dokazovaná formule. •

4.3. Příklad. Z rekurentní formule 4.2 okamžitě plyne:

$$B_0 = 1,\ B_1 = 1,\ B_2 = 2,\ B_3 = 5,\ B_4 = 15,\ B_5 = 52,\ B_6 = 203, \ldots$$

4.4. Poznámka. Podle příkladu 4.3 existuje na 4-prvkové množině $\{a, b, c, d\}$ celkem 15 rozkladů. S uspořádáním popsaným v úvodu paragrafu tvoří tyto rozklady úplný svaz, jehož hasseovský diagram je na obr. 4.3.



Obr. 4.3: Svaz rozkladů čtyřprvkové množiny

Podle počtu prvků v jednotlivých třídách výše uvedeného rozkladu je největší prvek prvkem „typu“ 4, nejmenší prvek je prvkem typu 1+1+1+1, pod největším prvkem leží rozklady typu 1+3, respektive 2+2 a konečně nejmenší prvek pokrývají prvky typu 1+1+2.

Tento intuitivně zcela zřejmý popis nyní precizujeme.

4.5. Definice. Buď A konečná množina. Nechť rozklad $\overline{A}$ obsahuje λ_i tříd mohutnosti i, $(i = 1, \ldots, k)$ a neobsahuje třídu o mohutnosti větší než k. Pak říkáme, že $\overline{A}$ je *rozklad typu*

$$\underbrace{1+1+\cdots+1}_{\lambda_1} + \underbrace{2+2+\cdots+2}_{\lambda_2} + \cdots + \underbrace{k+k+\cdots+k}_{\lambda_k}$$

nebo též typu

$$1^{\lambda_1} 2^{\lambda_2} \ldots k^{\lambda_k}.$$

4.6. Příklad. Rozklad množiny $\{1, 2, 3, 4, 5, 6\}$ na třídy $\{1\}$, $\{2, 4\}$, $\{3, 6\}$, a $\{5\}$ je rozklad typu 1+1+2+2 nebo též typu $1^2 2^2$.

4.7. Věta. *Počet rozkladů typu $1^{\lambda_1} 2^{\lambda_2} \dots k^{\lambda_k}$ na n-prvkové množině je roven číslu*

$$\frac{n!}{(1!)^{\lambda_1} \cdot (2!)^{\lambda_2} \dots (k!)^{\lambda_k} \cdot \lambda_1! \cdot \lambda_2! \dots \lambda_k!}$$

pokud $\lambda_1 + 2\lambda_2 + \dots + k\lambda_k = n$. Je-li $\lambda_1 + 2\lambda_2 + \dots + k\lambda_k \neq n$, je počet rozkladů uvedeného typu roven nule.

Důkaz. Je zřejmé, že rozklad typu $1^{\lambda_1} 2^{\lambda_2} \dots k^{\lambda_k}$ na n-prvkové množině existuje právě tehdy, když $\lambda_1 + 2\lambda_2 + \dots + k\lambda_k = n$, neboť počet prvků jednotlivých tříd je roven počtu prvků celé množiny (třídy rozkladu jsou po dvou disjunktní). Určeme tedy počet rozkladů daného typu za předpokladu $\lambda_1 + 2\lambda_2 + \dots + k\lambda_k = n$.

Každý rozklad typu $1^{\lambda_1} 2^{\lambda_2} \dots k^{\lambda_k}$ vznikne tak, že v následujícím schématu

$$\underbrace{\{x\}, \dots, \{x\}}_{\lambda_1}, \underbrace{\{x, x\}, \dots, \{x, x\}}_{\lambda_2}, \dots, \underbrace{\{\overbrace{x, x, \dots, x}^{k}\}, \dots, \{\overbrace{x, x, \dots, x}^{k}\}}_{\lambda_k}$$

místo x vepíšeme postupně nějakou permutaci prvků dané n-prvkové množiny. Těchto permutací je $n!$. Různé permutace však neudávají nutně různé rozklady. Především udávají týž rozklad permutace, lišící se jen pořadím tříd o stejné mohutnosti. Protože tříd o mohutnosti i je λ_i, můžeme z těchto tříd utvořit $\lambda_i!$ různých permutací. Celkový počet $n!$ všech permutací je proto nutno vydělit číslem $\lambda_1! \cdot \lambda_2! \cdot \dots \cdot \lambda_k!$. Pořadí prvků v každé třídě rozkladu, která má i prvků, lze zapsat $i!$ možnostmi. Protože těchto tříd je λ_i, můžeme pořadí prvků ve všech těchto třídách zapsat celkem $\underbrace{i! \cdot i! \cdot \dots \cdot i!}_{\lambda_i} = (i!)^{\lambda_i}$ způsoby, aniž se změní množiny, tvořící jednotlivé třídy. Celkový počet permutací je tak nutno vydělit ještě číslem $(1!)^{\lambda_1} \cdot (2!)^{\lambda_2} \cdot \dots \cdot (k!)^{\lambda_k}$. Odtud již plyne dokazované tvrzení. •

4.8. Příklad. Na čtyřprvkové množině má podle věty 4.7 existovat

$$\frac{4!}{(1!)^2 \cdot (2!)^1 \cdot 2! \cdot 1!} = 6$$

rozkladů typu $1^2 2^1$. Na obrázku 4.3 vidíme, že tomu tak opravdu je.

4.9. Definice. Buďte $n \geq m$ přirozená čísla. Označme $S(n, m)$ počet rozkladů n-prvkové množiny na m tříd. Čísla $S(n, m)$ se nazývají *Stirlingova čísla 2. druhu*. Dále definitoricky klademe $S(0, 0) = 1$, $S(0, n) = 0$ pro $n \in \mathbb{N}$.

4.10. Příklad. Z obrázku 4.3 je vidět, že například $S(4, 2) = 7$.

4.11. Věta. *Buďte X, Y neprázdné konečné množiny, $|X| = n$, $|Y| = k$, $n \geq k$. Pak pro množinu* surj (Y^X) *všech surjekcí X na Y platí*

$$\left|\operatorname{surj}(Y^X)\right| = k! \cdot S(n, k).$$

Důkaz. Buď $f : X \to Y$ surjekce. Tato surjekce určuje rozklad množiny X na k tříd; jednotlivé třídy jsou úplné vzory prvků množiny Y. Každý rozklad množiny X na k tříd přitom určuje $k!$ surjekcí X na Y. Odtud plyne tvrzení. •

4.12. Věta.

$$\begin{aligned} &S(n+1, k) = S(n, k-1) + k \cdot S(n, k) \quad \textit{pro } 1 < k < n, \\ &S(n, n) = S(n, 1) = 1. \end{aligned}$$

Důkaz. Představme si všechny rozklady $(n+1)$-prvkové množiny $\{a_1, \ldots, a_{n+1}\}$ na k tříd. V některých rozkladech tvoří prvek a_{n+1} jednoprvkovou třídu. Těchto rozkladů je $S(n, k-1)$. Ve všech ostatních rozkladech je prvek a_{n+1} prvkem některé třídy o více prvcích. Prvek a_{n+1} je tedy v těchto rozkladech přidán k některé třídě rozkladu množiny $\{a_1, \ldots, a_n\}$ na k tříd. Těchto rozkladů je $S(n, k)$ a prvek a_{n+1} můžeme přidat ke kterékoliv z uvedených k tříd. Odtud plyne dokazovaná formule. •

4.13. Poznámka. Rekurentní formule z věty 4.12 nám umožňuje postupně počítat hodnoty čísel $S(n, k)$. V tabulce na straně 171 uvádíme některé hodnoty Stirlingových čísel druhého druhu. Této tabulce se také říká *Stirlingův trojúhelník.*

Z Pascalova a Stirlingova trojúhelníka lze snadno odvodit tabulku 4.2, shrnující výsledky tvrzení 3.8, 3.12 a 4.11 o zobrazeních n-prvkové množiny do množiny k-prvkové.

V diagonále následující tabulky je tučně vytištěn počet $n!$ bijekcí mezi n-prvkovými množinami. Nad diagonálou ($n < k$) je uveden počet injekcí $(k)_n = n!\binom{n}{k}$ a pod diagonálou ($n > k$) je počet surjekcí $k! \cdot S(n, k)$.

	$k=1$	2	3	4	5	6	...
$n=1$	**1**	2	3	4	5	6	...
2	1	**2**	6	12	20	30	...
3	1	6	**6**	24	60	120	...
4	1	14	36	**24**	120	360	...
5	1	30	150	240	**120**	720	...
6	1	62	540	1560	1800	**720**	...
$\vdots$							

Tab. 4.2: Tabulka počtu injekcí, surjekcí a bijekcí

4.14. Věta. *Pro všechna reálná x a každé přirozené n platí*

$$x^n = \sum_{k=1}^{n} S(n,k)(x)_k.$$

Důkaz. Nechť $|A| = m \leq |X| = n$. Počet zobrazení X do A je podle příkladu 3.21 roven číslu m^n. Buď nyní $f : X \to A$ libovolné zobrazení. Pak je f surjekce X na množinu $f(X) = A_1$. Je-li $|f(X)| = k$, existuje podle věty 4.11 celkem $k! \cdot S(n,k)$ surjekcí množiny X na množinu A_1. Avšak k-prvkových podmnožin v A je $\binom{m}{k}$. Odtud plyne, že existuje $\binom{m}{k} \cdot k! \cdot S(n,k)$ surjekcí X na k-prvkovou podmnožinu v A. Dokázali jsme tak, že

$$m^n = \sum_{k=1}^{n} \binom{m}{k} \cdot k! \cdot S(n,k) = \sum_{k=1}^{n} (m)_k \cdot S(n,k).$$

Polynomy n-tého stupně x^n a $\sum_{k=1}^{n} S(n, k(x)_k$ se tedy shodují v $n+1$ hodnotách $0, 1, \ldots, n$. Jak z matematické analýzy víme, plyne odtud rovnost těchto polynomů. •

4.15. Věta.

$$S(n+1,k) = \sum_{i=0}^{n} \binom{n}{i} S(i, k-1).$$

Důkaz. Představme si rozklady $(n+1)$-prvkové množiny $\{a_1, \ldots, a_{n+1}\}$ na k tříd. Když v každém z těchto rozkladů vyškrtneme třídu obsahující prvek a_{n+1}, zůstanou nám právě všechny rozklady všech množin $K \subseteq \{a_1, \ldots, a_n\}$ na $k-1$ tříd. Odtud plyne dokazovaná formule. •

4.16. Poznámka. Z definice je zřejmá souvislost Bellových čísel se Stirlingovými čísly 2. druhu; platí

$$B_n = S(n,1) + S(n,2) + \cdots + S(n,n) = \sum_{k=1}^{n} S(n,k).$$

Odtud a z věty 4.15 lze snadno odvodit rekurentní formuli z věty 4.2. Když pro jednoduchost položíme $S(n,k) = 0$ pro $k > n$ (jak je to ostatně vyznačeno již v tabulce ma straně 171), platí

$$\begin{aligned} B_{n+1} &= \sum_{k=1}^{\infty} S(n+1,k) = \sum_{k=1}^{\infty}\sum_{i=0}^{n} \binom{n}{i} \cdot S(i,k-1) = \\ &= \sum_{i=0}^{n} \binom{n}{i} \left(\sum_{k=1}^{\infty} S(i,k-1) \right) = \sum_{i=0}^{n} \binom{n}{i} B_i . \end{aligned}$$

Pro Bellova čísla je známa řada důležitých vztahů. Na ukázku si odvoďme alespoň dva z nejběžnějších.

4.17. Věta. *Pro každé reálné číslo t platí*

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n = e^{(e^t - 1)}.$$

Důkaz. Uvedený vztah odvodil E. T. Bell již v roce 1934. My však uvedeme elegantní důkaz, který v roce 1964 uveřejnil americký matematik G. C. Rota.

Označme F množinu všech reálných funkcí $\varphi(x)$ definovaných vztahem

$$\varphi(x) = \sum_{n=0}^{\infty} \alpha_n \cdot (x)_n, \quad \text{kde } \sum_{n=0}^{\infty} |\alpha_n| < \infty.$$

Definujeme-li sčítání funkcí z F a násobení těchto funkcí reálnými čísly obvyklým způsobem, utvoříme zřejmě z F vektorový prostor.

Připomeňme si, že když V je nějaký vektorový prostor a $f : V \to \mathbb{R}$ je zobrazení (takovým zobrazením se říká *funkcionál*), nazývá se f *lineární funkcionál*, jestliže pro každé vektory $\underline{u}$, $\underline{v}$ a každá reálná čísla α, β platí

$$f(\alpha\underline{u} + \beta\underline{v}) = \alpha f(\underline{u}) + \beta f(\underline{v}).$$

Nyní ukážeme, že zobrazení $L\colon F \to \mathbb{R}$ definované vztahem $L(\varphi) = \sum_{n=0}^{\infty} \alpha_n$ je lineární funkcionál. Skutečně:

$$L(\beta\varphi + \gamma\varphi') = \sum_{n=0}^{\infty} (\beta\alpha_n + \gamma\alpha_n') = \beta \sum_{n=0}^{\infty} \alpha_n + \gamma \sum_{n=0}^{\infty} \alpha_n' = \beta L(\varphi) + \gamma L(\varphi').$$

Z věty 4.14 dále plyne (vzhledem k tomu, že zřejmě $x^n \in F$):

$$L(x^n) = L\left(\sum_{k=1}^{n} S(n,k)(x)_k\right) = \sum_{k=1}^{n} S(n,k) = B_n.$$

Z matematické analýzy víme, že pro každé reálné číslo x platí $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.

Odtud plyne, že $e^x \in F$, neboť řada $\sum_{n=0}^{\infty} \frac{1}{n!}$ konverguje. Nyní můžeme snadno spočítat hodnotu $L(e^{tx})$. Platí

$$L\left(e^{tx}\right) = L\left(\sum_{n=0}^{\infty} \frac{t^n x^n}{n!}\right) = \sum_{n=0}^{\infty} L\left(\frac{t^n x^n}{n!}\right) = \sum_{n=0}^{\infty} \frac{t^n}{n!} L(x^n) = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n.$$

Položíme-li nyní $e^t = 1 + u$, obdržíme

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n &= L\left[(1+u)^x\right] = L\left(\sum_{n=0}^{\infty} \binom{x}{n} u^n\right) = L\left(\sum_{n=0}^{\infty} \frac{(x)_n}{n!} u^n\right) = \\ &= \sum_{n=0}^{\infty} \frac{u^n}{n!} = e^u = e^{(e^t - 1)}.\end{aligned}$$

•

4.18. Poznámka. V uvedeném důkazu jsme využili zobecněné binomické věty. Podrobněji o ní budeme, současně s dalšími podrobnostmi o mocninných řadách, hovořit v paragrafu 9.

V následující větě ukážeme rozvoj Bellových čísel v nekonečnou řadu.

4.19. Věta. (G. Dobinski)

$$B_{n+1} = \frac{1}{e}\left(1^n + \frac{2^n}{1!} + \frac{3^n}{2!} + \frac{4^n}{3!} + \dots\right) = \frac{1}{e} \sum_{k=1}^{\infty} \frac{k^n}{(k-1)!}.$$

Důkaz. Platí

$$e = \sum_{k=0}^{\infty} \frac{1}{k!} = \sum_{k=n}^{\infty} \frac{1}{(k-n)!} = \sum_{k=n}^{\infty} \frac{(k)_n}{k!} = \sum_{k=0}^{\infty} \frac{(k)_n}{k!},$$

(neboť pro $k = 0, \dots, n-1$ je $(k)_n = 0$). Pro funkcionál L definovaný v důkazu věty 4.17 platí:

$$L\left[(x)_n\right] = 1 = \frac{1}{e} \sum_{k=0}^{\infty} \frac{(k)_n}{k!}.$$

Pro funkci $\varphi(x) = \sum_{n=0}^{\infty} \alpha_n (x)_n$ odtud plyne

$$L[\varphi(x)] = \sum_{n=0}^{\infty} \alpha_n \sum_{k=0}^{\infty} \frac{1}{e} \frac{(k)_n}{n!} = \frac{1}{e} \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=0}^{\infty} \alpha_n (x)_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{\varphi(k)}{k!}.$$

Položíme-li $\varphi(x) = x^{n+1}$, obdržíme dokazovanou formuli. •

Poznámky a cvičení

1. Povšimněme si zajímavé skutečnosti: čísla

$$\begin{aligned} 2+1 &= 3 \\ 2 \times 3 + 1 &= 7 \\ 2 \times 3 \times 5 + 1 &= 31 \\ 2 \times 3 \times 5 \times 7 + 1 &= 211 \\ 2 \times 3 \times 5 \times 7 \times 11 + 1 &= 2\,311 \end{aligned}$$

jsou prvočísla, avšak

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031 = 59 \times 509$$

prvočíslo není. Uvedená faktorizace čísla 30 031 je však **jediná**, jeho předchůdce 30 030 však má 31 faktorizací. Popište, jak tento počet souvisí s tím, že $31 = S(6, 2)$.

2. Dokažte, že

a) $S(n, 2) = 2^{n-1} - 1$

b) $S(n, n-1) = \binom{n}{2}$

c) $S(n+1, m) = S(n, m-1) + m \cdot S(n, m)$

d) $S(n, m) = \sum_k \binom{n-1}{k} S(k, m-1)$

5 Princip inkluze a exkluze

Účinným prostředkem při řešení řady kombinatorických úloh je tzv. *princip inkluze a exkluze* (česky bychom mohli říci *princip vylučování a zapojování prvků*). Před jeho formulací si ukážeme, v čem spočívá jeho podstata.

Buďte M_1, M_2 libovolné konečné množiny. Pak zřejmě platí

$$|M_1 \cup M_2| = |M_1| + |M_2| - |M_1 \cap M_2|\,.$$

Pro tři množiny je zřejmé, že mohutnost jejich sjednocení obecně neobdržíme, když od součtu jejich mohutností odečteme mohutnosti průniků všech dvojic těchto množin. Některé prvky bychom totiž mohli odečíst dvakrát – a sice ty prvky, které leží v průniku všech tří těchto množin. Zřejmě tak platí

$$\begin{aligned} |M_1 \cup M_2 \cup M_3| &= |M_1| + |M_2| + |M_3| - |M_1 \cap M_2| - |M_1 \cap M_3| - \\ &\quad - |M_2 \cap M_3| + |M_1 \cap M_2 \cap M_3|\,. \end{aligned}$$

Zobecněním popsaného procesu obdržíme následující princip inkluze a exkluze.

5.1. Věta. *Buď dána konečná množina M. Nechť prvky množiny M mohou mít vlastnosti $\alpha_1, \alpha_2, \dots, \alpha_n$. Symbolem $M(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_k}, \alpha'_{j_1}, \alpha'_{j_2}, \dots, \alpha'_{j_p})$ označme počet všech prvků množiny M, které mají vlastnosti $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_k}$ a nemají žádnou z vlastností $\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_p}$ (bez ohledu na to, mají-li nebo nemají vlastnosti, které ve výčtu $\alpha_{i_1}, \alpha_{i_2}, \dots\ \alpha_{i_k}, \alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_p}$ nejsou uvedeny). Pak platí*

$$\begin{aligned} M(\alpha'_1, \alpha'_2, \dots, \alpha'_n) &= |M| - \sum_{i=1}^{n} M(\alpha_i) + \sum_{i<j} M(\alpha_i, \alpha_j) - \\ &- \sum_{i<j<k} M(\alpha_i, \alpha_j, \alpha_k) + \dots + (-1)^n M(\alpha_i, \alpha_2, \dots, \alpha_n). \end{aligned}$$

Důkaz. Indukcí vzhledem k počtu vlastností.

(a) Pro jednu vlastnost je formule evidentně správná, neboť jistě platí

$$M(\alpha'_1) = |M| - M(\alpha_1).$$

(b) Nechť dokazovaná formule platí pro $n-1$ vlastností, tj. platí

$$M(\alpha'_1, \alpha'_2, \ldots, \alpha'_{n-1}) = |M| - \sum_{i=1}^{n-1} M(\alpha_i) + \sum_{i<j} M(\alpha_i, \alpha_j) - \cdots + \\ +(-1)^{n-1} M(\alpha_i, \alpha_2, \ldots, \alpha_{n-1}). \qquad (5.1)$$

Odtud však plyne, že pro prvky, které mají vlastnost α_n, platí

$$M(\alpha'_1, \alpha'_2, \ldots, \alpha'_{n-1}, \alpha_n) = M(\alpha_n) - \sum_{i=1}^{n-1} M(\alpha_i, \alpha_n) + \cdots + \\ +(-1)^{n-1} M(\alpha_i, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n). \qquad (5.2)$$

Když nyní od 5.1 odečteme rovnost 5.2, dostaneme na pravé straně pravou stranu dokazované formule. Na levé straně obdržíme rozdíl

$$M(\alpha'_1, \alpha'_2, \ldots, \alpha'_{n-1}) - M(\alpha'_1, \alpha'_2, \ldots, \alpha'_{n-1}, \alpha_n),$$

což je ovšem právě $M(\alpha'_1, \alpha'_2, \ldots, \alpha'_{n-1}, \alpha'_n)$. ●

5.2. Příklad. V jistém závodě zhotovili následující přehled o svých zaměstnancích:

V závodě pracuje celkem 250 mužů a 200 žen. Předepsanou kvalifikaci má 160 mužů a 140 žen. Do práce dojíždí 180 mužů a 100 žen. Kvalifikovaných mužů dojíždí 150, kvalifikovaných žen 20.

Dokážeme, že uvedené hlášení je nepravdivé.

V závodě pracuje celkem 450 zaměstnanců. Označme nyní možné vlastnosti zaměstnanců následovně: α_1 značí příslušnost k mužskému pohlaví, α_2 dosažení předepsané kvalifikace, α_3 dojíždění. Z hlášení plyne, že $M(\alpha_1) = 250$, $M(\alpha_2) = 300$, $M(\alpha_3) = 280$, $M(\alpha_1, \alpha_2) = 160$, $M(\alpha_1, \alpha_3) = 180$, $M(\alpha_2, \alpha_3) = 170$ a konečně $M(\alpha_1, \alpha_2, \alpha_3) = 150$. Spočtěme $M(\alpha'_1, \alpha'_2, \alpha'_3)$, tj. počet nekvalifikovaných nedojíždějících žen. Podle principu inkluze a exkluze platí:

$$M(\alpha'_1, \alpha'_2, \alpha'_3) = 450 - 250 - 300 - 280 + 160 + 180 + 170 - 150 = -20,$$

což není možné. Proto musí být alespoň jeden údaj v hlášení nepravdivý.

5.3. Věta. (Speciální případ principu inkluze a exkluze) *Nechť ve větě 5.1 pro každé $k = 1, \ldots, n$ a pro každou kombinaci vlastností $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ závisí číslo $M(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}) = M(k)$ pouze na počtu těchto vlastností. Pak platí*

$$M(\alpha'_1, \ldots, \alpha'_n) = |M| - \binom{n}{1} M(1) + \binom{n}{2} M(2) - \binom{n}{3} M(3) + \ldots \\ \cdots + (-1)^n \binom{n}{n} M(n).$$

Důkaz. Důkaz je zcela zřejmý. •

5.4. Příklad. Zabývejme se následujícím problémem, v matematické literatuře známým pod názvem „Problème des Rencontres".

Označme S_n množinu všech permutací množiny $\{1, 2, \dots, n\}$, tj. množinu všech bijekcí $f\colon \{1, \dots, n\} \to \{1, \dots, n\}$. (Víme, že $|S_n| = n!$.) Naším úkolem je zjistit, kolik z těchto permutací nemá ani jeden pevný bod. (Připomeňme si, že x je pevný bod zobrazení f, když $f(x) = x$.)

Buď $f \in S_n$. Řekneme, že f má vlastnost α_i $(i = 1, \dots, n)$, jestliže $f(i) = i$. Naším úkolem je tedy určení čísla $M(\alpha'_1, \dots, \alpha'_n)$. Přitom je zřejmé, že můžeme aplikovat větu 5.3 a platí

$$M(1) = (n-1)!, \quad M(2) = (n-2)!, \quad \dots \quad , \quad M(k) = (n-k)! \quad \text{atd.}$$

Proto

$$\begin{aligned} M(\alpha'_1, \dots, \alpha'_n) &= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \\ &\quad + \dots + (-1)^n \binom{n}{n}(n-n)! = \sum_{k=0}^{n} (-1)^k \binom{n}{k}(n-k)! = \\ &= \sum_{k=0}^{n} (-1)^k \frac{n!}{(n-k)! \cdot k!}(n-k)! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \\ &= \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!}\right). \end{aligned}$$

5.5. Příklad. Pomocí příkladu 5.4 snadno vyřešíme následující tzv. *problém šatnářky.*

> *Představme si, že do šatny odevzdalo n osob svůj klobouk. Jaká je pravděpodobnost q_n toho, že když všichni ztratili lístek od šatny a šatnářka jim klobouky při odchodu vydávala zcela nahodile, dostal alespoň jeden člověk svůj klobouk?*

K šatně mohlo n osob přicházet celkem v $n!$ pořadích. (Přitom samozřejmě předpokládáme, že všechna pořadí jsou stejně pravděpodobná.) Z příkladu 5.4 okamžitě plyne, že pravděpodobnost toho, že nikdo nedostane svůj klobouk, je rovna číslu

$$p_n = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!}.$$

Pravděpodobnost toho, že alespoň jeden člověk svůj klobouk dostane, je proto

$$q_n = 1 - p_n = \frac{1}{1!} - \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{(-1)^{n+1}}{n!}.$$

5.6. Poznámka. Jak jsme uvedli již v důkazu věty 4.17, platí pro každé reálné číslo x vztah $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$. Zejména tedy platí

$$e^{-1} = \frac{1}{e} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots = \lim_{n\to\infty} p_n.$$

Odtud plyne, že $\lim_{n\to\infty} q_n = 1 - \frac{1}{e} (\doteq 0{,}632\,121\ \ldots)$. Navíc posloupnost $(q_n)_{n=1}^{\infty}$ konverguje „velmi rychle“, neboť například

$$q_1 = 1;\ q_2 = 0{,}5;\ q_3 = 0{,}\overline{6};\ q_4 = 0{,}625;\ q_5 = 0{,}6\overline{3};\ \ldots;\ q_8 = 0{,}632\,11\ldots$$

Odtud plyne překvapující zjištění, že *pravděpodobnost q_n se s rostoucím n prakticky nemění.*

5.7. Příklad. Metodou inkluze a exkluze lze vyřešit i jiný známý kombinatorický problém, tzv. *úlohu o hostech* (v literatuře běžně nazývanou *Problème des Ménages*).

Formulace tohoto problému je jednoduchá: *Kolika způsoby můžeme rozsadit kolem kulatého stolu n manželských párů tak, aby se muži a ženy pravidelně střídali a žádní dva manželé přitom neseděli vedle sebe?*

Nejprve se dohodněme, která rozesazení budeme považovat za různá. Úlohu vyřešíme nejprve tak, ža dvě rozesazení budeme považovat za různá, existuje-li alespoň jedna židle, která je v těchto rozesazeních obsazena různými osobami. Když tento výsledek vydělíme číslem $2n$, nerozlišujeme rozesazení, z nichž jedno vzniklo „pootočením“ druhého.

Všechna rozesazení rozdělme do $2 \cdot n!$ disjunktních skupin podle toho, jak se rozesadí ženy. Nyní určíme počet rozesazení v těchto skupinách.

Nechť jsou tedy ženy již jistým způsobem rozesazeny. Hledáme počet $r(n)$ všech rozesazení mužů, při nichž žádný muž nesedí vedle své ženy.

Všech možných rozesazení mužů je $n!$. Označme α_i následující vlastnost těchto rozesazení: i-tý muž sedí vedle své ženy. Pak platí:

$$r(n) = n! - \sum_{i=1}^{n} M(\alpha_i) + \sum_{i<j} M(\alpha_i, \alpha_j) - \sum_{i<j<k} M(\alpha_i, \alpha_j, \alpha_k) + \ldots$$
$$\cdots + (-1)^n M(\alpha_1, \ldots, \alpha_n).$$

Uvědomme si, že v tomto případě nemůžeme užít speciálního případu principu inkluze a exkluze. Pro různé k-tice vlastností $\alpha_{i_1}, \ldots, \alpha_{i_k}$ jsou totiž čísla $M(\alpha_{i_1}, \ldots, \alpha_{i_k})$ obecně značně odlišná. Je totiž zřejmé, že sedí-li příslušné ženy

„pohromadě“, mají jejich muži podstatně méně možností k rozesazení, než když jsou jejich ženy rozptýleny. Formální popis těchto závislostí je značně komplikovaný a tak výpočet jednotlivých hodnot $M(\alpha_{i_1}, \dots, \alpha_{i_k})$ je prakticky vyloučený. Naštěstí je snadné spočítat součet $\sum_{i_1 < \dots < i_k} M(\alpha_{i_1}, \dots, \alpha_{i_k})$. Tato suma udává počet všech rozesazení, kdy každá k-tice mužů sedí vedle svých žen (bez ohledu na to, jak jsou rozmístěni další muži).

Kolem stolu je rozmístěno $2n$ židlí a mezi nimi je $2n$ mezer. Představme si, že některá k-tice mužů sedí vedle svých žen a označme k mezer mezi těmi židlemi, na nichž sedí příslušné manželské páry. Žádné dvě z těchto mezer nyní nemohou být vedle sebe, protože v tom případě by některý muž musel mít z obou stran svou ženu nebo by některá žena měla z obou stran svého muže.

Z uvedeného plyne, že počet všech rozesazení, kdy některá k-tice mužů sedí vedle svých žen, je roven počtu způsobů, jak z $2n$ mezer vybrat k-tici tak, aby žádné dvě vybrané mezery nebyly vedle sebe. Toto číslo však umíme jednoduše spočítat podle příkladu 3.32; číslo

$$t(k, 2n-k) = \frac{2n}{2n-k}\binom{2n-k}{k}$$

udává počet rozesazení, kdy právě k mužů sedí vedle svých žen. Při určování čísel $M(\alpha_{i_1}, \dots, \alpha_{i_k})$ však zbývajících $n-k$ mužů může být rozesazeno jakkoliv, tj.

$$\sum_{i_1 < \dots < i_k} M(\alpha_{i_1}, \dots, \alpha_{i_k}) = (n-k)!\frac{2n}{2n-k}\binom{2n-k}{k},$$

takže

$$\begin{aligned} r(n) &= n! - (n-1)!\frac{2n}{2n-1}\binom{2n-1}{1} + (n-2)!\frac{2n}{2n-2}\binom{2n-2}{2} - \dots + \\ &\quad +(-1)^n(n-n)!\frac{2n}{n}\binom{n}{n} = \sum_{k=0}^{n}(-1)^k(n-k)!\frac{2n}{2n-k}\binom{2n-k}{k}. \end{aligned}$$

Číslo $r(n)$ udává počet řešení při zadaném rozesazení žen. Řešením úlohy o hostech je tedy číslo

$$2 \cdot n! \sum_{k=0}^{n}(-1)^k(n-k)!\frac{2n}{2n-k}\binom{2n-k}{k}.$$

Že nemá naději na úspěch snaha najít všechna řešení jejich výčtem, plyne z toho, že již například pro $n = 6$ je těchto možností 115 200.

Metodou inkluze a exkluze lze snadno řešit i některé problémy z teorie čísel. Na ukázku odvodíme tzv. *Eulerovu funkci* $\varphi(n)$.

5.8. Příklad. Pro každé přirozené číslo $n > 1$ označme $\varphi(n)$ počet těch přirozených čísel menších než n, která jsou s číslem n nesoudělná.

Odvodíme formuli pro výpočet hodnot funkce $\varphi(n)$.

Víme, že každé přirozené číslo n lze jednoznačně rozložit na součin prvočinitelů. Nechť tedy

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}$$

je tento rozklad (tj. $p_1, \ldots, p_k$ jsou všechna navzájem různá prvočísla dělící číslo n).

Pro každé $i = 1, \ldots, k$ označme α_i vlastnost: přirozené číslo je dělitelné prvočíslem p_i. Je zřejmé, že mezi čísly $1, \ldots, n$ je čísel s vlastností α_i právě $\dfrac{n}{p_i}$.

Podle principu inkluze a exkluze platí

$$\begin{aligned}\varphi(n) &= n - \sum_i M(\alpha_i) + \sum_{i<j} M(\alpha_i, \alpha_j) - \cdots + (-1)^k M(\alpha_1, \ldots, \alpha_k) = \\ &= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \cdots + (-1)^k \frac{n}{p_i \cdot \ldots \cdot p_k},\end{aligned}$$

neboť mezi čísly $i = 1, \ldots, n$ je zřejmě $\dfrac{n}{p_{i_1} \cdot \ldots \cdot p_{i_s}}$ dělitelných čísly $p_{i_1} \ldots p_{i_s}$. Dále je však zřejmé, že platí

$$\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) = 1 - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \ldots$$
$$\cdots + (-1)^k \frac{n}{p_i \cdot \ldots \cdot p_k}.$$

Dokázali jsme tak, že

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Známe-li tedy rozklad čísla n na součin prvočinitelů, lze hodnotu $\varphi(n)$ snadno spočítat. Například $1\,000\,000 = 10^6 = 2^6 \cdot 5^6$, takže

$$\varphi(1\,000\,000) = 1\,000\,000 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 400\,000.$$

5.9. Příklad. Pomocí principu inkluze a exkluze odvodíme formuli pro výpočet $\left|\operatorname{surj}(Y^X)\right|$.

Nechť tedy jsou X, Y konečné množiny, $|X| = n$, $|Y| = k$. Nechť $Y = \{y_1, \ldots, y_k\}$. Podle příkladu 3.21 víme, že $\left|Y^X\right| = k^n$.

Řekneme, že prvek $f \in Y^X$ má vlastnost α_i, jestliže $y_i \notin f(X)$. Pak

$$\begin{aligned}\left|\operatorname{surj}(Y^X)\right| &= k^n - \binom{k}{1}M(1) + \binom{k}{2}M(2) - \cdots + (-1)^k M(k) = \\ &= \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n.\end{aligned}$$

Ve větě 4.11 jsme však odvodili, že

$$\left|\operatorname{surj}(Y^X)\right| = k! \cdot S(n,k).$$

Porovnáním uvedených dvou formulí pro výpočet počtu surjekcí jedné konečné množiny na druhou obdržíme následující formuli pro Stirlingova čísla 2. druhu:

$$S(n,k) = \frac{1}{k!}\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n.$$

Poznámky a cvičení

1. Funkce f definovaná na podmnožině množiny $\mathbb{N}$ se nazývá *multiplikativní*, když její definiční obor je uzavřený vzhledem k násobení a pro každá dvě nesoudělná čísla x, y platí $f(x \cdot y) = f(x) \cdot f(y)$. Dokažte, že Eulerova funkce $\varphi(n)$ (viz 5.8) je multiplikativní.

2. *Möbiova funkce* $\mu(n)$ je pro $n \in \mathbb{N}$ definována následovně: $\mu(n)$ nabývá hodnoty 1, pokud je n součinem sudého počtu navzájem různých prvočísel, hodnoty -1, pokud je n součinem lichého počtu navzájem různých prvočísel a konečně je rovno 0 v ostatních případech.

Dokažte, že

$$\varphi(n) = n \cdot \sum_{d \mid n} \frac{\mu(d)}{d},$$

kde se sčítá přes všechny **dělitele čísla** n (včetně 1 a n).

3. Dokažte, že Möbiova funkce je multiplikativní.

4. V počítačové učebně je 30 počítačů, z nichž 20 běží pod operačním systémem Windows, osm má 21" monitor, 25 má instalován CD-ROM, 20 má alespoň dva z těchto atributů a 6 má všechny tři.

a) Kolik počítačů má alespoň jednu z uvedených vlastností?

b) Kolik počítačů nemá žádnou z nich?

c) Kolik počítačů má právě jednu z vlastností?

6 Rozklady přirozených čísel na sčítance

V tomto paragrafu se budeme zabývat následujícím problémem: *Buďte n, k přirozená čísla. Kolika způsoby lze číslo n rozložit na k přirozených sčítanců?*

Je zřejmé, že pro $k > n$ je tento počet roven nule, pro $k = 1$ nebo $k = n$ je pak roven jedné. Pro $2 \leq k \leq n - 1$ je těchto možností více. Musíme se však dohodnout, která rozložení čísla n budeme považovat za různá. Konkrétně jde o to, zda nám záleží nebo nezáleží na pořadí sčítanců.

Nejprve vyřešíme jednodušší případ, kdy pořadí sčítanců rozlišujeme.

6.1. Definice. *Kompozicí* čísla n na k sčítanců rozumíme každou uspořádanou k-tici $[x_1, \dots, x_k]$ přirozených čísel takovou, že

$$x_1 + x_2 + \cdots + x_k = n.$$

Počet všech kompozicí čísla n na k sčítanců označme $K(n, k)$.
(Termín *kompozice* zavedl Percy A. MacMahon.)

6.2. Věta. *Pro každá přirozená čísla n, k platí*

$$K(n, k) = \binom{n-1}{k-1}.$$

Důkaz. Postupujeme analogicky jako v příkladu 3.30. Mějme n jedniček a přidejme k nim $k - 1$ nul. Všech permutací těchto jedniček a nul je $P(n, k - 1) = \binom{n+k-1}{k-1}$. Je-li $a_1, \dots, a_{n+k-1}$ některá z těchto permutací, rozdělí ji $k - 1$ nul na k úseků. Označme x_i počet jedniček v i-tém úseku. Dostaneme tak k-tici $[x_1, \dots, x_k]$ takovou, že $x_1+x_2+\cdots+x_k = n$. Tato k-tice však obecně není kompozicí čísla n, neboť některá x_i mohou být rovna nule. Abychom zajistili, že všechna x_i jsou nenulová, umístíme do každého úseku jednu jedničku předem a zbývajících $n - k$ jedniček pak můžeme rozdělit libovolně, tj. $P(n - k, k - 1)$ způsoby.

Dokázali jsme tak, že

$$K(n, k) = P(n - k, k - 1) = \frac{(n - k + k - 1)!}{(n - k)! \cdot (k - 1)!} = \binom{n-1}{k-1}.$$

•

6.3. Poznámka. V průběhu důkazu věty 6.2 jsme ukázali, že kompozicí čísla n na nejvýše k sčítanců je $P(n-k, k-1) = \binom{n+k-1}{k-1}$.

6.4. Příklad. Podle věty 6.2 lze číslo $n = 7$ rozložit na tři sčítance celkem $K(7,3) = \binom{6}{2} = 15$ způsoby.

Příslušné kompozice jsou následující:

$5+1+1$	$4+2+1$	$3+2+2$	$3+3+1$
$1+5+1$	$2+1+4$	$2+3+2$	$3+1+3$
$1+1+5$	$1+2+4$	$2+2+3$	$1+3+3$
	$4+1+2$		
	$2+4+1$		
	$1+4+2$		

Pokud bychom však pořadí sčítanců nebrali v úvahu, lze číslo 7 rozložit na tři sčítance čtyřmi způsoby (sloupce v hořejším rozpisu).

Jak uvidíme, je situace s určením počtu rozkladů čísla n na k sčítanců bez ohledu na jejich pořadí podstatně komplikovanější.

6.5. Definice. Buďte n, k přirozená čísla. *Rozkladem* čísla n na k sčítanců rozumíme každou (neuspořádanou) k-tici přirozených čísel $x_1, \ldots, x_k$ takovou, že

$$x_1 + \cdots + x_k = n.$$

Počet všech rozkladů čísla n na k sčítanců označme $p(n,k)$.

6.6. Poznámka. To, že v rozkladu $x_1 + \cdots + x_k$ čísla n na k sčítanců na pořadí těchto sčítanců nezáleží je totéž, jako když se dohodneme na jistém přesně stanoveném pořadí, v jakém budeme tyto rozklady zapisovat. Nadále budeme proto rozklady psát tak, že $x_1 \geq x_2 \geq \ldots \geq x_k$.

Předpokládejme nyní, že

$$n = x_1 + x_2 + \cdots + x_k$$

je rozklad čísla n na k sčítanců. Pak

$$n - k = (x_1 - 1) + (x_2 - 1) + \cdots + (x_k - 1)$$

je rozklad čísla $n-k$ na k nebo méně sčítanců (neboť některá x_i se mohla rovnat jedné). Přitom uvedené přiřazení $(x_1, \ldots, x_k) \to (x_1 - 1, \ldots, x_k - 1)$ je evidentně bijekcí množiny všech rozkladů čísla n na k sčítanců na množinu všech rozkladů čísla $n-k$ na nejvýše k sčítanců.

Dokázali jsme tak, že platí následující věta.

6.7. Věta.

$$p(n,k) = \sum_{i=1}^{k} p(n-k,i); \qquad p(n,1) = p(n,n) = 1.$$

6.8. Poznámka. Uvedená rekurentní formule nám umožňuje postupně počítat všechny hodnoty $p(n,k)$. Tyto hodnoty pro čísla $n,k = 1,\dots,10$ uvádíme v tabulce na straně 169.

6.9. Poznámka. Číslo $q(n,k) = \sum_{i=1}^{k} p(n,i)$ udává počet rozkladů čísla n na nejvýše k sčítanců. Přitom lze číslo $q(n,k)$ najít přímo mezi čísly $p(x,y)$. Podle věty 6.7 totiž zřejmě platí

$$q(n,k) = p(n+k,k),$$

takže například $q(6,3) = p(9,3) = 7$.

V roce 1942 dokázal F. C. Auluck, že pro velká n je $q(n,k)$ přibližně rovno číslu $\frac{1}{k!}\binom{n-1}{k-1}$. To potvrzuje vcelku očekávanou skutečnost, že počet kompozic čísla n na k sčítanců je přibližně $k!$ krát větší než počet rozkladů čísla n na nejvýše k sčítanců.

Číslo $p(n) := q(n,n)\ \left(= \sum_{k=1}^{n} p(n,k)\right)$ udává počet **všech** rozkladů čísla n. Podle výše uvedeného platí

$$p(n) = p(2n,n),$$

takže i čísla $p(n)$ lze zjistit z tabulky čísel $p(n,k)$. (Kromě toho je $p(n)$ samozřejmě rovno součtu všech čísel v n-tém sloupci této tabulky.)

Tabulka čísel $p(n)$ je uvedena v příloze na straně 170.

Z tabulky čísel $p(n)$ je zřejmé, že již pro poměrně malé hodnoty n je výpočet hodnot $p(n)$ pomocí rekurentní formule pro $p(n,k)$ zdlouhavý a komplikovaný. (O výhodnějším způsobu výpočtu hodnot $p(n)$ se zmíníme v paragrafu 9 – viz větu 9.6.)

Vzhledem k tomu, že není znám jednoduchý explicitní vzorec pro přímý výpočet čísel $p(n,k)$, respektive $p(n)$, byly odvozeny alespoň vztahy popisující asymptotické chování těchto čísel. Tak například Hardy a Ramanujan odvodili, že

$$\lg p(n) \sim \pi\sqrt{\frac{2n}{3}} - \lg\frac{4n}{\sqrt{3}}.$$

V roce 1937 odvodil H. Rademacher, že $p(n)$ lze vyjádřit jako součet jisté konvergentní nekonečné řady. Pro ukázku jeho výsledek uveďme:

$$p(n) = \sum_{q=1}^{\infty} L_q(n) \cdot \psi_q(n),$$

kde

$$\psi_q(n) = \pi\sqrt{\frac{q}{2}} \cdot \frac{d}{dn} \frac{\sinh\left[\pi\sqrt{\frac{2}{3}} \cdot \frac{\sqrt{n-\frac{1}{24}}}{q}\right]}{\sqrt{n-\frac{1}{24}}}$$

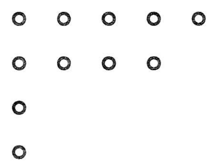
a

$$L_q(n) = \sum_{p} w_{p,q} \cdot e^{-\frac{2np\pi i}{q}},$$

kde $w_{p,q}$ je 24. odmocnina z jedné a p probíhá všechna celá čísla nesoudělná s q menší nebo rovna číslu q.

6.10. Poznámka. V řadě úvah o rozkladech přirozených čísel na sčítance jsou velmi užitečné tzv. *Ferrersovy diagramy*, v nichž každému sčítanci odpovídá řádek bodů v rovině. I bez přesné definice je jistě vše zřejmé z následujícího příkladu:

$5 + 4 + 1 + 1 \quad \longrightarrow$

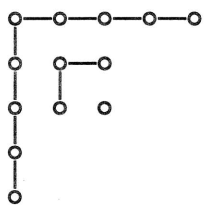


Je-li α rozklad čísla n, pak tzv. *adjungovaný rozklad* α^* k rozkladu α obdržíme tak, že Ferrersův diagram rozkladu α přečteme, jednoduše řečeno, po sloupcích. Tak například adjungovaný rozklad k výše uvedenému rozkladu $5 + 4 + 1 + 1$ je rozklad $4 + 2 + 2 + 2 + 1$.

Platí-li $\alpha = \alpha^*$, nazývá se rozklad α *samoadjungovaný*.

Pokusme se nyní zjistit, *kolik má číslo n samoadjungovaných rozkladů.* Nejprve uvažme následující jednoduchý příklad.

Samoadjungovaným rozkladem čísla 13 je například rozklad 5+3+3+1+1. Ferrersův diagram tohoto rozkladu je následující:



Když sečteme v uvedeném diagramu navzájem propojené body, obdržíme rozklad 9+3+1. Zamyslíme-li se nad tím, jak rozklad 9+3+1 vznikl, uvědomíme si jistě okamžitě, že jde zákonitě o rozklad s navzájem různými lichými sčítanci (pokud byl samozřejmě původní rozklad samoadjungovaný). Když si nyní navíc uvědomíme, že obrácením uvedeného postupu zase naopak každému rozkladu čísla n na navzájem různé liché sčítance přiřadíme evidentně samoadjungovaný rozklad čísla n, přičemž popsané zobrazení je zřejmě bijektivní, je jasné, že jsme dokázali následující tvrzení.

6.11. Věta. *Počet samoadjungovaných rozkladů čísla n je roven počtu rozkladů čísla n na navzájem různé liché sčítance.*

Pomocí Ferrersových diagramů lze okamžitě – pouhou záměnou řádků a sloupců – odvodit i další tvrzení.

6.12. Věta. *Počet rozkladů čísla n na sčítance nepřevyšující číslo k je stejný jako počet rozkladů čísla n na nejvýše k sčítanců.*

Na množině Y všech rozkladů (všech přirozených čísel) je obvyklé definovat vhodné uspořádání následujícím způsobem. (Pro formální jednoduchost nyní ztotožníme rozklad $a_1 \geq a_2 \geq \ldots \geq a_k$ s posloupností $(a_1, \ldots, a_k, 0, \ldots, 0, \ldots)$.)

6.13. Definice. Buď Y množina všech nerostoucích posloupností nezáporných celých čísel, jejichž součtem je přirozené číslo (tj. všechny členy každé posloupnosti jsou od jistého indexu $i \geq 2$ rovny nule). Definujeme relaci $\leq$ na Y tak, že pro libovolná $\alpha = (a_n)_{n=1}^{\infty}$, $\beta = (b_n)_{n=1}^{\infty}$ platí:

$$\alpha \leq \beta \iff a_i \leq b_i \text{ pro každé } i \in \mathbb{N}.$$

Okamžitě z definice je zřejmé, že platí následující věta.

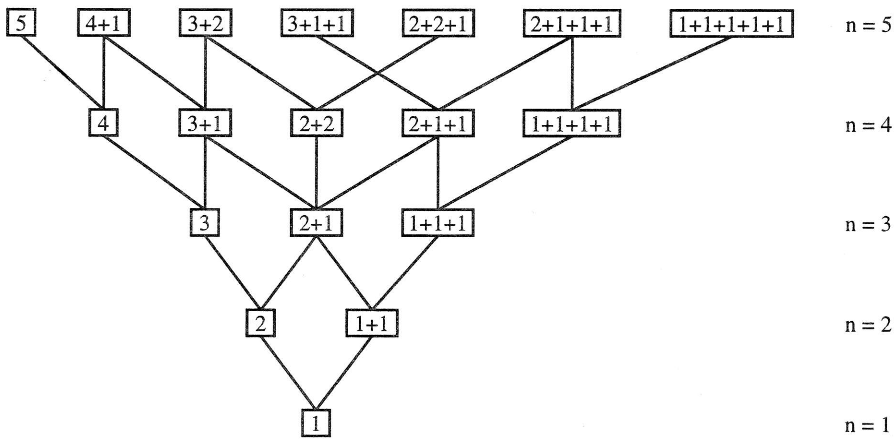
6.14. Věta. *Relace $\leq$ definovaná v 6.13 je uspořádání na množině Y a $(Y, \leq)$ je svaz, v němž*

$$\begin{aligned} \alpha \vee \beta &= (\max\{a_1, b_1\}, \max\{a_2, b_2\}, \ldots) \\ \alpha \wedge \beta &= (\min\{a_1, b_1\}, \min\{a_2, b_2\}, \ldots). \end{aligned}$$

6.15. Poznámka. Svaz $(Y, \leq)$ je obvykle nazýván *Youngův svaz.*

Část tohoto svazu je na obr. 6.4.

Počet prvků „výšky“ n v $(Y, \leq)$ je zřejmě $p(n)$. Snadná je též odpověď na otázku, kolik prvků prvek $\alpha \in Y$ pokrývá a kolika prvky je pokryt. Je zřejmé, že když rozklad α obsahuje k **různých** sčítanců, pak α pokrývá k prvků a je pokryt $k+1$ prvky.



Obr. 6.4: Youngův svaz

Poznámky a cvičení

1. Srinivasa Ramanujan dokázal řadu vlastností čísel $p(n, k)$ a $p(n)$, například skutečnost, že pro každé $n \in \mathbb{N}_0$ je $p(5n + 4)$ násobkem 5. Ověřte tuto skutečnost pro $n = 0, 1, 2$.

2. Označme $t(n)$ počet rozkladů čísla n, jejichž každý sčítanec je mocninou čísla 2 (včetně $2^0 = 1$).

(a) Vypočtěte $t(n)$ pro $1 \leq n \leq 6$.

(b) Dokažte, že $t(2n + 1) = t(2n)$.

(c) Dokažte, že $t(n)$ je sudé pro všechna $n > 1$.

3. Již Galileo Galilei řešil problém, proč při házení kostkami nepadá stejně často součet 9 a 10.

a) Ukažte, že čísla 9 a 10 mají stejný počet rozkladů na tři sčítance, které jsou nejvýše rovny 6.

b) Zdůvodněte, proč přesto nepadá součet 9 stejně často jako součet 10.

4. Dokažte, že $p(2r + k, r + k) = p(2s + k, s + k)$ pro každé $r, s \in \mathbb{N}$.

5. Dokažte, že číslo $p(r + k, k)$ je rovno:

a) počtu rozkladů čísla $r + \binom{k+1}{2}$ na k navzájem různých sčítanců;

b) počtu rozkladů čísla r na sčítance nejvýše rovné k.

6. Pomocí Ferrersových diagramů dokažte rovnost $p(n) = p(2n, n)$.

7. Hardy a Ramanujan v r. 1919 dokázali, že

$$p(n) \doteq \frac{1}{4n\sqrt{3}} \cdot e^{\pi \cdot \sqrt{\frac{2n}{3}}}.$$

Porovnejte hodnotu $p(70)$ podle tohoto tvaru s přesnou hodnotou (viz tabulku na straně 170).

čítanců;

).

tou (viz

7 Rozdělování do přihrádek

V tomto paragrafu v podstatě jen shrneme některé výsledky odvozené již dříve, přeformulujeme je však do jazyka tzv. „přihrádkové“ kombinatoriky. Mnohé úlohy lze totiž převést na následující problém: *kolika způsoby lze n předmětů rozdělit do k přihrádek?*

Vzhledem k tomu, že jak předměty, tak přihrádky mohou být vzájemně rozlišitelné, respektive nerozlišitelné, a na rozmístění mohou být kladeny další omezující podmínky (např. aby všechny přihrádky byly neprázdné, aby počet prvků v různých přihrádkách byl různý apod.), lze úloh tohoto typu zformulovat celou řadu. Řešení některých z nich může být velmi komplikované.

Četné aplikace těchto výsledků lze najít i mimo matematiku, např. ve statistické fyzice.

Ještě před řešením úloh uvedeného typu si zformulujeme následující evidentní tvrzení, známé jako *Dirichletův princip.*

7.1. Věta. *Při každém rozdělení n předmětů do k přihrádek, kde $k < n$, existuje alespoň jedna přihrádka obsahující alespoň dva předměty.*

Jakkoliv je Dirichletův princip jednoduchý, umožňuje řešení řady úloh. Řadu zajímavých příkladů lze najít například v [7].

7.2. Příklad. *Dokažte, že když v obdélníku o rozměrech 6 cm $\times$ 4 cm vybereme libovolně 25 bodů, pak mezi nimi existují alespoň dva, které mají vzdálenost menší než 1,5 cm.*

Leží-li dva body v jednotkovém čtverci, je jejich vzdálenost rovna nejvýše $\sqrt{2}$, což je méně než 1,5. Kdybychom tedy chtěli 25 bodů rozmístit tak, aby každé dva měly vzdálenost alespoň 1,5 cm, mohli bychom do každého čtverce o straně 1 cm ležícího v daném obdélníku umístit nejvýše jeden bod. Obdélník však lze pokrýt nejvýše 24 takovými čtverci. Podle věty 7.1 tedy mezi libovolnými 25 body jsou alespoň dva ze stejného čtverce.

7.3. Věta. *Buďte k, n libovolná přirozená čísla. Pak lze n rozlišitelných předmětů rozmístit do k rozlišitelných přihrádek právě k^n způsoby.*

Důkaz. Je-li $X = \{x_1, \ldots, x_n\}$ množina n předmětů a $Y = \{y_1, \ldots, y_k\}$ množina k přihrádek, pak je evidentní, že rozdělení předmětů do přihrádek je totéž jako zobrazení množiny X do množiny Y. (Prvek x_i se zobrazí na tu přihrádku, do které je umístěn.) Odtud a z věty 3.21 okamžitě plyne tvrzení. •

Při popsaných rozmístěních předmětů do přihrádek existují samozřejmě přihrádky, které mohou zůstat prázdné. Chceme-li předměty X rozmístit do přihrádek Y tak, aby žádná přihrádka nezůstala prázdná, je to zřejmě totéž, jako sestrojit surjekci X na Y. Odtud, z věty 4.11 a z příkladu 5.9 plyne následující tvrzení.

7.4. Věta. *Buď dáno n rozlišitelných předmětů a k rozlišitelných přihrádek, $n \geq k$. Počet rozdělení těchto předmětů do přihrádek, při nichž žádná přihrádka nezůstane prázdná, je roven číslu*

$$k!S(n,k) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n.$$

Podobně z důsledku 3.8 plyne

7.5. Věta. *Buď dáno n rozlišitelných předmětů a k rozlišitelných přihrádek, $k \geq n$. Počet rozdělení předmětů do přihrádek, při nichž každá přihrádka obsahuje nejvýše jeden prvek, je roven číslu*

$$(k)_n = k \cdot (k-1) \cdot \ldots \cdot (k-n+1).$$

Nyní uvažujme případ, kdy máme opět k rozlišitelných přihrádek avšak n vzájemně nerozlišitelných předmětů. Uvědomíme-li si, že za předměty můžeme vzít například cifry 1 (v počtu n) a přihrádky můžeme označit $x_1, \ldots, x_k$, je okamžitě zřejmé, že tato úloha je ekvivalentní s určením počtu kompozicí čísla n. Chceme-li přitom, aby v každé přihrádce bylo alespoň r předmětů, můžeme nejprve do každé přihrádky r předmětů vložit a zbývajících $n - kr$ předmětů pak rozdělit libovolně. Odtud, z věty 6.2 a poznámky 6.3 okamžitě plyne následující tvrzení.

7.6. Věta. *Buďte k, n libovolná přirozená čísla. Pak lze n nerozlišitelných předmětů rozmístit do k rozlišitelných přihrádek právě*

$$\binom{n+k-1}{k-1}$$

způsoby.

Chceme-li, aby v každé přihrádce bylo alespoň r předmětů, je těchto možností

$$\binom{n-kr+k-1}{k-1}.$$

Mají-li zejména být všechny přihrádky neprázdné, je možností celkem

$$\binom{n-1}{k-1}.$$

Nyní uvažme případ, kdy jsou přihrádky nerozlišitelné. Nechť tedy je dáno k nerozlišitelných přihrádek a n rozlišitelných předmětů. Rozdělit tyto předměty do přihrádek tak, aby právě p těchto přihrádek bylo neprázdných, evidentně značí utvořit rozklad na množině předmětů na právě p tříd. Podle definice 4.9 udává počet těchto rozkladů Stirlingovo číslo 2. druhu $S(n, p)$.

Odtud okamžitě plyne

7.7. Věta. *Počet rozmístění n rozlišitelných předmětů do k nerozlišitelných přihrádek je roven číslu*

$$S(n, 1) + S(n, 2) + \cdots + S(n, k) = \sum_{i=1}^{k} S(n, i).$$

Chceme-li zejména, aby všechny přihrádky byly neprázdné, je těchto možností právě $S(n, k)$.

Zbývá nám poslední možný případ, kdy jsou nerozlišitelné i předměty i přihrádky. Protože za předměty můžeme vzít cifry 1 a za přihrádky sčítance, jejichž pořadí nerozlišujeme, je tento případ evidentně popsán pomocí rozkladů přirozených čísel. Odtud a z věty 6.9 okamžitě plyne následující tvrzení.

7.8. Věta. *Je-li dáno n nerozlišitelných předmětů, lze je do k nerozlišitelných přihrádek rozdělit*

$$p(n, 1) + p(n, 2) + \cdots + p(n, k) = \sum_{i=1}^{k} p(n, i) = p(n + k, k)$$

způsoby.

Chceme-li, aby všechny přihrádky byly neprázdné, je těchto možností právě $p(n, k)$.

7.9. Poznámka. Uvedené výsledky můžeme shrnout do tabulky 7.3, v níž je uveden počet všech rozdělení (bez jakýchkoliv omezujících předpokladů).

7.10. Příklad. Ilustrujme si rozdíly mezi počty možností v jednotlivých případech například pro 10 předmětů a 4 přihrádky.

(a) $k^n = 4^{10} = 1\,048\,576$,

(b) $\binom{n+k-1}{k-1} = \binom{13}{3} = 286$,

Počet všech rozmístění		n předmětů	
		rozlišitelných	nerozlišitelných
k přihrádek	rozlišitelných	k^n	$\binom{n+k-1}{k-1}$
	nerozlišitelných	$\sum_{i=1}^{k} S(n,i)$	$\sum_{i=1}^{k} p(n,i)$

Tab. 7.3: Umísťování předmětů do přihrádek

(c) $\sum_{i=1}^{k} S(n,i) = S(10,1) + S(10,2) + S(10,3) + S(10,4) =$

$= 1 + 511 + 9\,330 + 34\,105 = 43\,947,$

(d) $\sum_{i=1}^{k} p(n,i) = p(10,1) + p(10,2) + p(10,3) + p(10,4) = 23\,.$

Poznámky a cvičení

1. Do 15 přihrádek je rozmístěno 100 míčků. Dokažte, že alespoň dvě přihrádky obsahují stejný počet míčků.

2. Dokažte, že v každé skupině (alespoň dvou) lidí existují alespoň dva lidé, kteří znají stejný počet členů skupiny. (Návod: Uvažujte množinu lidí, kteří neznají nikoho).

3. Ukažte, že mezi sedmi různými přirozenými čísly vždy existují čísla x, y taková, že $x + y$ nebo $x - y$ je dělitelné deseti.

4. Máme čtyři bílé koule, čtyři černé koule a čtyři červené koule. Kolika způsoby je můžeme rozdělit do 6 rozlišitelných přihrádek? (2 000 376)

8 Řešení rekurentních formulí

S rekurentními formulemi jsme se setkali již několikrát. Tak například ve větě 4.2 jsme odvodili rekurentní formuli pro výpočet Bellových čísel B_n, ve větě 6.7 pak rekurentní formuli pro výpočet počtu $p(n, k)$ rozkladů čísla n na k sčítanců.

Mezi právě uvedenými formulemi je – kromě jiného – jeden zásadní rozdíl. Čísla B_n závisejí na jediné hodnotě (tj. n), čísla $p(n, k)$ na dvou hodnotách (tj. n, k). V tomto paragrafu se budeme zabývat formulemi prvního z uvedených typů, tj. formulemi pro výpočet členů posloupnosti pomocí předcházejících členů.

Předpokládejme, že je tedy dána rekurentní formule pro výpočet hodnot $f(n)$. Obecně nám taková formule umožňuje výpočet členu $f(n+1)$, známe-li hodnoty $f(1), \ldots, f(n)$ (respektive $f(0), \ldots, f(n)$ apod.). Jednotlivé formule se však mohou lišit tím, kolik předcházejících členů fakticky potřebujeme k výpočtu členu následujícího. Tak například ve formuli 4.2 pro výpočet čísel B_n potřebujeme k určení B_n **všechny** členy předcházející. Ve formuli $f(n+2) = f(n+1) + f(n)$ potřebujeme jen předcházející dva členy.

Má tedy smysl následující definice.

8.1. Definice. Řekneme, že rekurentní formule pro výpočet hodnot $f(n)$ je *řádu* $k \in \mathbb{N}$, jestliže pro každé $n \in \mathbb{N}$ lze $f(n+k)$ určit pomocí $f(n)$, $f(n+1)$, $\ldots$, $f(n+k-1)$, přičemž k je nejmenší přirozené číslo s uvedenou vlastností.

8.2. Příklad. (a) $f(n+3) = f(n+2) - \log f(n)$ je formule 3. řádu,

(b) $f(n+2) = f(n+1) + f(n)$ je formule 2. řádu,

(c) $T_{n+1} = \sum_{k=0}^{n} T_k$ není formule konečného řádu.

8.3. Definice. Buď dána rekurentní formule k-tého řádu pro výpočet čísel $f(n)$, $n \in \mathbb{N}$. Řekneme, že posloupnost $(a_n)_{n=1}^{\infty}$ je *řešením* této rekurentní formule, jestliže pro každé $i \in \mathbb{N}$ dostaneme po dosazení čísel a_{i+j} za $f(n+j)$, $j = 0, \ldots, k$, identitu.

8.4. Příklad. Posloupnost $(2^n)_{n=1}^{\infty}$ je řešením rekurentní formule 2. řádu

$$f(n+2) = 3 \cdot f(n+1) - 2 \cdot f(n),$$

neboť pro všechna $n \in \mathbb{N}$ platí

$$2^{n+2} = 3 \cdot 2^{n+1} - 2 \cdot 2^n.$$

8.5. Poznámka. Rekurentní formule k-tého řádu zřejmě může obecně mít nekonečně mnoho řešení, neboť prvních k členů posloupnosti, která je řešením, můžeme volit zcela libovolně. Stejně tak se ovšem může stát, že rekurentní formule nemá řešení žádné.

Nyní se bude zabývat otázkou, zda lze alespoň v některých případech pro danou rekurentní formuli určit člen $f(n)$, aniž bychom museli počítat postupně všechny členy předcházející. Uvidíme, že se nám to podaří pro speciální typ formulí – pro tzv. lineární rekurentní formule s konstantními koeficienty.

8.6. Definice. Rekurentní formule tvaru

$$f(n+k) = a_1 \cdot f(n+k-1) + a_2 \cdot f(n+k-2) + \cdots + a_k \cdot f(n), \qquad (8.1)$$

kde $a_1, \ldots, a_k$ jsou reálná čísla, $a_k \neq 0$, se nazývá *lineární rekurentní formule k-tého řádu s konstantními koeficienty.*

8.7. Věta. *Jsou-li posloupnosti* $(f_1(n))_{n=1}^{\infty}, (f_2(n))_{n=1}^{\infty}, \ldots, (f_s(n))_{n=1}^{\infty}$ *řešením formule 8.1, je také jejich libovolná lineární kombinace*

$$\left(c_1 f_1(n) + c_2 f_2(n) + \cdots + c_s f_s(n)\right)_{n=1}^{\infty}$$

řešením formule 8.1.

Důkaz. Je zřejmé, že stačí dokázat, že každá lineární kombinace libovolných dvou řešení formule 8.1 je opět řešením formule 8.1. Nechť tedy $(g(n))_{n=1}^{\infty}$, $(h(n))_{n=1}^{\infty}$ jsou řešení formule 8.1, tj. platí

$$\begin{aligned} g(n+k) &= a_1 g(n+k-1) + a_2 g(n+k-2) + \cdots + a_k g(n) \\ h(n+k) &= a_1 h(n+k-1) + a_2 h(n+k-2) + \cdots + a_k h(n) \end{aligned}$$

pro všechna $n \in \mathbb{N}$. Potřebujeme dokázat, že pro libovolná čísla $c_1, c_2 \in \mathbb{R}$ je $(r(n))_{n=1}^{\infty}$, kde $r(n) = c_1 g(n) + c_2 h(n)$, také řešením formule 8.1.

Pro každé $n \in \mathbb{N}$ platí:

$$
\begin{aligned}
r(n+k) = c_1 g(n+k) + c_2 h(n+k) = c_1[a_1 g(n+k-1) + \cdots + a_k g(n)] +\\
+ c_2[a_1 h(n+k-1) + \cdots + a_k h(n)] =\\
= a_1[c_1 g(n+k-1) + c_2 h(n+k-1)] + \cdots + a_k[c_1 g(n) + c_2 h(n)] =\\
= a_1 r(n+k-1) + \cdots + a_k r(n),
\end{aligned}
$$

což znamená, že $(r(n))_{n=1}^{\infty}$ je řešením formule 8.1. •

8.8. Poznámka. Zdůrazněme, že větu 8.7 jsme dokázali pro **speciální typ** rekurentních formulí. Snadno lze ukázat, že když formule není lineární, pak lineární kombinace daných řešení vůbec **nemusí být** řešením dané formule.

8.9. Příklad. Mějme dánu rekurentní formuli 2. řádu

$$f(n+2) = 5 \cdot f(n+1) - 6 \cdot f(n).$$

Pouhým dosazením lze snadno ověřit, že posloupnosti $(2^n)_{n=1}^{\infty}$ a $(3^n)_{n=1}^{\infty}$ jsou lineárně nezávislá řešení dané formule. Nyní ukážeme, že **každé** řešení $(g(n))_{n=1}^{\infty}$ zadané formule je vhodnou lineární kombinací uvedených dvou řešení, tj. existují konstanty $c_1, c_2 \in \mathbb{R}$ takové, že pro každé $n \in \mathbb{N}$ platí:

$$g(n) = \left(c_1 \cdot 2^n + c_2 \cdot 3^n\right)_{n=1}^{\infty}.$$

Jak tyto konstanty nalezneme? Protože řád dané formule je 2, je řešení $(g(n))_{n=1}^{\infty}$ jednoznačně určeno volbou hodnot $g(1)$ a $g(2)$. Nechť tedy $g(1) = a$, $g(2) = b$. Potřebujeme dokázat, že existují konstanty c_1, c_2 takové, že

$$
\begin{aligned}
2c_1 + 3c_2 &= a\\
4c_1 + 9c_2 &= b
\end{aligned}
$$

Tento systém rovnic má však právě jedno řešení

$$c_1 = \frac{3a-b}{2}, \quad c_2 = \frac{b-2a}{3}.$$

8.10. Poznámka. Je zřejmé, že množina všech posloupností reálných čísel se sčítáním definovaným po složkách a s obvyklým násobením reálnými čísly tvoří vektorový prostor nekonečné dimenze na $\mathbb{R}$. Z věty 8.7 plyne, že všechna řešení lineární rekurentní formule daného řádu tvoří podprostor tohoto prostoru. V příkladu 8.9 jsme ukázali, že dimenze vektorového prostoru všech řešení zadané rekurentní formule druhého řádu je 2; posloupnosti $(2^n)_{n=1}^{\infty}$ a $(3^n)_{n=1}^{\infty}$ tvoří bázi tohoto vektorového prostoru.

Postup uvedený v příkladu 8.9 lze snadno zobecnit na případ lineární rekurentní formule s konstantními koeficienty libovolného řádu $k \in \mathbb{N}$. Libovolné řešení $(g(n))_{n=1}^{\infty}$ takové rekurentní formule je totiž jednoznačně určeno hodnotami $g(1), g(2), \dots, g(k)$. Existují-li lineárně nezávislá řešení

$$(f_1(n))_{n=1}^{\infty}, (f_2(n))_{n=1}^{\infty}, \dots (f_k(n))_{n=1}^{\infty},$$

pak jistě existují konstanty $c_1, c_2, \dots, c_k \in \mathbb{R}$ takové, že pro každé $n \in \mathbb{N}$ platí:

$$g(n) = c_1 f_1(n) + \dots + c_k f_k(n).$$

K tomu totiž stačí ukázat, že systém rovnic

$$\begin{aligned} c_1 f_1(1) + c_2 f_2(1) + \dots + c_k f_k(1) &= g(1) \\ c_1 f_1(2) + c_2 f_2(2) + \dots + c_k f_k(2) &= g(2) \\ &\vdots \\ c_1 f_1(k) + c_2 f_2(k) + \dots + c_k f_k(k) &= g(k) \end{aligned}$$

má řešení. Z lineární nezávislosti posloupností

$$(f_1(n))_{n=1}^{\infty}, (f_2(n))_{n=1}^{\infty}, \dots, (f_k(n))_{n=1}^{\infty}$$

však snadno plyne, že daný systém rovnic má **právě jedno** řešení $c_1, c_2, \dots, c_k$.

V dalším (viz důsledek 8.19) ukážeme, že takový systém lineárně nezávislých řešení vskutku existuje.

Celkem se takto snadno odvodí následující tvrzení.

8.11. Věta. *Dimenze podprostoru všech řešení lineární rekurentní formule s konstantními koeficienty je rovna řádu této formule.*

8.12. Poznámka. Je-li dána nějaká rekurentní formule, může a nemusí se stát, že existuje posloupnost $(g(n, c_1, c_2, \dots, c_k))_{n=1}^{\infty}$ obsahující parametry $c_1, c_2, \dots, c_k$ tak, že platí:

(a) Dosadíme-li za parametry $c_1, c_2, \dots, c_k$ **libovolná** reálná čísla, je vzniklá posloupnost řešením dané rovnice.

(b) **Každé řešení** dané rekurentní formule lze získat vhodnou volbou parametrů $c_1, c_2, \dots, c_k$ ve výše uvedené rekurentní posloupnosti.

Pokud posloupnost $(g(n, c_1, c_2, \dots, c_k))_{n=1}^{\infty}$ s uvedenými vlastnostmi existuje, nazývá se **obecné řešení** dané rekurentní formule.

Z výše uvedeného tedy plyne, že platí:

8.13. Věta. *Nechť je dána lineární rekurentní formule*

$$f(n+k) = a_1 \cdot f(n+k-1) + a_2 \cdot f(n+k-2) + \cdots + a_k \cdot f(n)$$

řádu k s konstantními koeficienty. Nechť

$$(f_1(n))_{n=1}^{\infty}, \ldots, (f_k(n))_{n=1}^{\infty}$$

jsou lineárně nezávislá řešení dané formule. Pak je posloupnost $(g(n))_{n=1}^{\infty}$, kde pro každé $n \in \mathbb{N}$ platí

$$g(n) = c_1 f_1(n) + \cdots + c_k f_k(n),$$

obecným řešením dané rekurentní formule.

Otázkou nyní zůstává, zda alespoň v některých případech obecné řešení najdeme.

Buď nyní dána lineární rekurentní formule k-tého řádu s konstantními koeficienty

$$f(n+k) = a_1 f(n+k-1) + \cdots + a_k f(n).$$

Zjišťujeme, zda pro některé $r \in \mathbb{R}$ je posloupnost $(r^n)_{n=1}^{\infty}$ řešením této formule.

Pokud je posloupnost $(r^n)_{n=1}^{\infty}$ řešením, musí pro každé $n \in \mathbb{N}$ platit

$$r^{n+k} = a_1 r^{n+k-1} + \cdots + a_k r^k.$$

Pokud je $r = 0$, je tato rovnost splněna triviálně. Je-li $r \neq 0$, musí tedy platit

$$r^k = a_1 r^{k-1} + \cdots + a_k.$$

Odtud a z věty 8.7 plyne

8.14. Věta. *Je-li reálné číslo r řešením rovnice*

$$x^k = a_1 x^{k-1} + \cdots + a_k,$$

je každá posloupnost $(cr^n)_{n=1}^{\infty}$, $c \in \mathbb{R}$ libovolné, řešením rekurentní formule 8.1.

8.15. Poznámka. Rovnice $x^k = a_1 x^{k-1} + \cdots + a_k$ se nazývá *charakteristická rovnice* formule

$$f(n+k) = a_1 f(n+k-1) + \cdots + a_k f(n).$$

Charakteristickou rovnicí rekurentní formule k-tého řádu je tedy algebraická rovnice k-tého řádu. Tato algebraická rovnice má tedy k kořenů (počítáme-li každý kořen tolikrát, jaká je jeho násobnost).

Uvědomme si přitom, že když je formule 8.1 k-tého řádu, je koeficient a_k nenulový, takže také všechny kořeny charakteristické rovnice jsou nenulové.

Odtud plyne následující věta

8.16. Věta. *Buď* $f(n+k) = a_1 f(n+k-1) + \cdots + a_k f(n)$, $a_k \neq 0$, *lineární rekurentní formule k-tého řádu s konstantními koeficienty. Nechť charakteristická rovnice*

$$x^k = a_1 x^{k-1} + \cdots + a_k$$

má jednoduché navzájem různé reálné kořeny $r_1, \ldots, r_k$. Pak obecné řešení dané rekurentní formule je tvaru

$$\left(c_1 r_1^n + c_2 r_2^n + \cdots + c_k r_k^n\right)_{n=1}^{\infty}.$$

Důkaz. Posloupnost $\left(c_1 r_1^n + c_2 r_2^n + \cdots + c_k r_k^n\right)_{n=1}^{\infty}$ je řešením dané formule podle vět 8.14 a 8.7. Podle poznámky 8.15 jsou všechna čísla r_i, $i = 1, \ldots, k$ různá od nuly. Posloupnosti $\left(r_i^n\right)_{n=1}^{\infty}$, $i = 1, \ldots, k$ jsou evidentně lineárně nezávislé. Zbývá tak pouze dokázat, že každé řešení dané rekurentní formule lze získat vhodnou volbou konstant c_i. To dokážeme analogicky jako v poznámce 8.10.

Buď $(g(n))_{n=1}^{\infty}$ libovolné řešení zadané rekurentní formule. Toto řešení je jednoznačně určeno hodnotami $g(1), \ldots, g(k)$. Zvolme tedy tyto hodnoty libovolně, ale pevně. Je potřeba dokázat, že systém k rovnic o k neznámých $c_1, \ldots, c_k$

$$\begin{aligned} c_1 r_1 + c_2 r_2 + \cdots + c_k r_k &= g(1) \\ c_1 r_1^2 + c_2 r_2^2 + \cdots + c_k r_k^2 &= g(2) \\ &\vdots \\ c_1 r_1^k + c_2 r_2^k + \cdots + c_k r_k^k &= g(k) \end{aligned}$$

má řešení. Protože však jsou všechna čísla r_i nenulová, je determinant

$$\begin{vmatrix} r_1 & r_2 & \ldots & r_k \\ r_1^2 & r_2^2 & \ldots & r_k^2 \\ \vdots & \vdots & & \vdots \\ r_1^k & r_2^k & \ldots & r_k^k \end{vmatrix}$$

rovněž nenulový, takže daný systém rovnic má právě jedno řešení. •

8.17. Příklad. Vyřešme rekurentní formuli z příkladu 8.2(b):

$$f(n+2) = f(n+1) + f(n).$$

Charakteristická rovnice je tvaru

$$x^2 = x + 1.$$

Její kořeny jsou

$$x_{1,2} = \frac{1 \pm \sqrt{5}}{2},$$

takže obecné řešení je tvaru

$$\left(c_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^n\right)_{n=1}^{\infty}$$

Hledejme takové řešení $(g(n))_{n=1}^{\infty}$ zadané formule, že $g(1) = 1$, $g(2) = 1$. Pak musí platit

$$\begin{aligned} c_1 \frac{1+\sqrt{5}}{2} + c_2 \frac{1-\sqrt{5}}{2} &= 1 \\ c_1 \left(\frac{1+\sqrt{5}}{2}\right)^2 + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^2 &= 1. \end{aligned}$$

Tento systém rovnic má právě jedno řešení $c_1 = -c_2 = \frac{1}{\sqrt{5}}$. Odtud plyne, že

$$g(n) = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Toto řešení $(g(n))_{n=1}^{\infty}$ je tzv. *Fibonacciova posloupnost*

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots;$$

členy této posloupnosti jsou tzv. *Fibonacciova čísla*, která hrají důležitou roli v různých částech matematiky i v řadě pozoruhodných aplikací. Poznamenejme pouze, že posloupnost Fibonacciových čísel je obvyklé značit symbolem $(F_n)_{n=0}^{\infty}$.

Ve větě 8.16 jsme popsali, jak lze nalézt obecné řešení v případě, že charakteristická rovnice má pouze jednoduché reálné kořeny. Dobře však víme, že algebraická rovnice může mít i kořeny imaginární a násobnost kořenů může být větší než jedna. V dalším popíšeme obecně alespoň ten případ, kdy všechny kořeny charakteristické rovnice jsou reálné.

8.18. Věta. *Nechť charakteristická rovnice formule 8.1 má reálný nenulový p-násobný kořen r. Pak jsou posloupnosti*

$$\left(r^n\right)_{n=1}^{\infty}, \left(n \cdot r^n\right)_{n=1}^{\infty}, \ldots, \left(n^{p-1} \cdot r^n\right)_{n=1}^{\infty}$$

lineárně nezávislá řešení formule 8.1.

Důkaz. Je zřejmé, že pro $r \neq 0$ jsou posloupnosti $(r^n)_{n=1}^{\infty}, \ldots, \left(n^{p-1} \cdot r^n\right)_{n=1}^{\infty}$ lineárně nezávislé. Zbývá tak dokázat, že všechny tyto posloupnosti jsou řešením formule 8.1.

Nechť tedy r je p-násobný kořen charakteristické rovnice. Potřebujeme dokázat, že pro $s = 1, \ldots, p-1$ je $(n^s \cdot r^n)_{n=1}^{\infty}$ řešením formule 8.1, tj. že platí

$$(n+k)^s r^{n+k} = a_1(n+k-1)^s r^{n+k-1} + a_2(n+k-2)^s r^{n+k-2} + \cdots + a_k n^s r^n.$$

Vydělíme-li tuto rovnici r^n, obdržíme

$$(n+k)^s r^k = a_1(n+k-1)^s r^{k-1} + a_2(n+k-2)^s r^{k-2} + \cdots + a_k n^s.$$

Dokažme pro jednoduchost tento vztah pouze pro $s = 1$. Předpokládejme tedy, že číslo $r \neq 0$ je alespoň dvojnásobným kořenem rovnice

$$x^k = a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_k.$$

Z algebry víme, že dvojnásobný kořen polynomu je nutně kořenem derivace tohoto polynomu, takže r je kořenem rovnice

$$kx^{k-1} = a_1(k-1)x^{k-2} + a_2(k-2)x^{k-3} + \cdots + a_{k-1}.$$

Odtud plyne, že platí

$$kr^{k-1} = a_1(k-1)r^{k-2} + a_2(k-2)r^{k-3} + \cdots + a_{k-1}.$$

Za těchto předpokladů potřebujeme dokázat správnost následující rovnosti:

$$(n+k)r^k = a_1(n+k-1)r^{k-1} + a_2(n+k-2)r^{k-2} + \cdots + a_k(n+k-k).$$

Upravme tuto rovnost následovně:

$$nr^k + kr^k = n \cdot [a_1 r^{k-1} + a_2 r^{k-2} + \cdots + a_k] + a_1(k-1)r^{k-1} + \\ + a_2(k-2)r^{k-2} + \cdots + a_k(k-k).$$

Rovnost výrazů stojících u n na obou stranách rovnosti nyní plyne z toho, že r je kořenem charakteristické rovnice, rovnost zbývajících členů plyne z toho, že kořen r je alespoň dvojnásobný. •

Z věty 8.18 okamžitě plyne

8.19. Důsledek. *Buď*

$$f(n+k) = a_1 f(n+k-1) + a_2 f(n+k-2) + \cdots + a_k f(n)$$

lineární rekurentní formule k-tého řádu s konstantními koeficienty. Nechť jsou všechny kořeny $r_1, \dots, r_j$ charakteristické rovnice této formule reálné. Nechť kořen r_1 je p_1-násobný, r_2 je p_2-násobný, ..., r_j je p_j-násobný (tj. $p_1 + \dots + p_j = k$). Pak obecným řešením dané rekurentní formule je posloupnost, jejíž n-tý člen je roven výrazu

$$r_1^n \cdot (c_{11} + c_{12}n + \dots + c_{1p_1}n^{p_1-1}) + r_2^n \cdot (c_{21} + c_{22}n + \dots + c_{2p_2}n^{p_2-1}) + \dots$$
$$\dots + r_j^n \cdot (c_{j1} + c_{j2}n + \dots + c_{jp_j}n^{p_j-1}).$$

8.20. Příklad. Najděte obecné řešení formule

$$f(n+4) = 3f(n+3) + 3f(n+2) - 11f(n+1) + 6f(n).$$

Charakteristická rovnice této formule je

$$x^4 = 3x^3 + 3x^2 - 11x + 6.$$

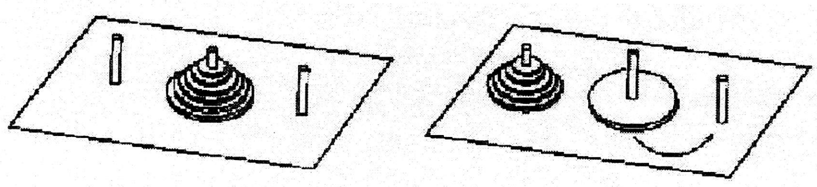
Snadno lze ověřit, že tato rovnice má dvojnásobný kořen 1 a jednoduché kořeny -2 a 3. Obecným řešením zadané formule je tedy posloupnost $(g(n))_{n=1}^{\infty}$, kde

$$g(n) = c_1 \cdot 1^n + c_2 n \cdot 1^n + c_3(-2)^n + c_4 3^n = c_1 + c_2 n + c_3(-2)^n + c_4 3^n.$$

Poznámky a cvičení

1. Název „Fibonacciova čísla“ pro členy posloupnost $1, 1, 2, 3, 5, 8, \dots$ zavedl francouzský matematik Eduard Lucas. Tzv. *Lucasova posloupnost* $(L_n)_{n=0}^{\infty}$ je definována stejnou rekurentní formulí $L_{n+2} = L_{n+1} + L_n$, avšak $L_0 = 1$, $L_1 = 3$. Vypočtěte L_{10}, L_{20}.

2. Známý hlavolam *Hanojská věž* uveřejnil v r. 1833 tajemný francouzský profesor „Claus“. Až v r. 1884 publikoval H. de Parville článek v časopise *La Natur*, v němž uvedl, že „Claus“ je anagram, který užil výše zmiňovaný Eduard „Lucas“. Hlavolam tvoří tři vertikální tyčky, na nichž je navlečeno n kruhových disků s otvory uprostřed. Tyto disky mají navzájem různé poloměry a jsou poskládány do věže tak, že poloměr každého disku je větší než poloměr kteréhokoliv disku nad ním (viz obrázek 8.5). Hlavolam spočívá v tom, přenést věž na jinou tyčku tak, že v každém kroku lze přenést pouze jeden disk z jedné tyčky na druhou a nikdy přitom nesmí být položen větší disk na menší.



Obr. 8.5: Hlavolam *Hanojská věž*

Parville v uvedeném článku uvádí legendu, podle níž mniši v utajovaném tibetském klášteře pracují na přemístění věže tvořené 64 zlatými disky. Ve chvíli, kdy práci dokončí, nastane konec světa. Kdy tato skutečnost nastane?

Označme H_n **minimální** počet kroků potřebných k přemístění věže.

a) Dokažte, že $(H_n)_{n=0}^{\infty}$ je řešením rekurentní formule $H_0 = 0$, $H_{n+1} = 2H_n + 1$.

b) Najděte obecné řešení uvedené formule.

c) Vypočtěte, kolik století by trvalo přemístění věže ze 64 disků, kdyby se na úkolu pracovalo nepřetržitě a přemístění každého disku by trvalo jednu sekundu.

3. Dokažte, že pro členy Fibonacciovy posloupnosti $(F_n)_{n=1}^{\infty}$ platí:

(a) $F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1$

(b) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$

(c) $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n \cdot F_{n+1}$

4. Dokažte, že *Fibonacciova posloupnost* $(F_n)_{n=0}^{\infty}$ splňuje:

a) $F_4 = F_2 + 2F_1 + F_0$

b) $F_5 = F_3 + 2F_2 + F_1$

c) $F_6 = F_3 + 3F_2 + 3F_1 + F_0$

d) $F_7 = F_4 + 3F_3 + 3F_2 + F_1$

e) $F_n = \sum_{k=1}^{n}(-1)^{n+k}\binom{n}{k}(F_{2k} - 1)$

f) $F_{k+n} = F_k F_n + F_{k-1} F_{n-1}$

g) F_k dělí čísla F_{2k+1} a F_{3k+2}

5. Takzvaná $(3n+1)$-*funkce* $g\colon \mathbb{N} \to \mathbb{N}$ je definována vztahem

$$g(n) = \begin{cases} \dfrac{n}{2}, & \text{pro } n \text{ sudé} \\[2ex] \dfrac{3n+1}{2}, & \text{pro } n \text{ liché.} \end{cases} \tag{8.2}$$

Zdá se pravděpodobné, že pro každé $n \in \mathbb{N}$ dospěje posloupnost $g(n)$, $g^2(n), g^3(n), \ldots$ k číslu 1. (Zatím to je prokázáno pro všechna $n < 2^{40}$.) Prověřte tuto vlastnost pro počáteční hodnoty 341, 96, 104, 336, 133.

6. Buď $n \in \mathbb{N}$ pevné. Pro každé $x \in \mathbb{N}_0$ položme

$$g(x) = 1^x + 2^x + \cdots + (n-1)^x.$$

Ukažte, že:

a) $g(0) = n - 1$

b) $g(1) = \frac{1}{2}n^2 - \frac{1}{2}n$

c) $g(2) = \frac{1}{3}n^3 - \frac{1}{2}n^2 + \frac{1}{6}n$

d) $g(3) = \frac{1}{4}n^4 - \frac{1}{2}n^3 + \frac{1}{4}n$

e) $g(4) = \frac{1}{5}n^5 - \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n$

7. k-té *Bernoulliovo číslo* b_k (pojmenované po Jacobu Bernoullim) je definováno jako koeficient u členu n ve funkci $g(k)$ (viz cvičení 1). Jacob Bernoulli dokázal, že

$$g(k) = \sum_{i=0}^{k} \frac{1}{i+1} \binom{k}{i} b_{k-i} n^{i+1}.$$

Pomocí této identity ověřte vyjádření čísla $g(4)$ ve cvičení 1(e). (Tabulka Bernoulliových čísel je uvedena v tabulce na straně 171.)

8. Bernoulliova čísla splňují vztah

$$\sum_{k=0}^{n} \binom{n+1}{k} b_k = 0, \qquad n \geq 1.$$

Pomocí tohoto vztahu a Pascalova trojúhelníka (strana 169) ukažte, že $b_5 = 0$, $b_6 = \frac{1}{42}$, $b_7 = 0$, $b_8 = -\frac{1}{30}$, $b_{10} = \frac{5}{66}$, $b_{12} = -\frac{691}{2\,730}$.

9. Nechť pro $x \in \mathbb{R}$ značí $[x]$ celou část čísla x, tj. největší celé číslo n takové, že $n \leq x$. Nechť S_n je množina všech permutací n–prvkové množiny $\{1, 2, \dots, n\}$. Řekneme, že permutace $p \in S_n$ je *fluktuační*, když platí:

$$p(2k-1) < p(2k) \text{ pro } 1 \leq k \leq \left[\frac{n}{2}\right],$$

$$p(2k+1) > p(2k) \text{ pro } 1 \leq k \leq \left[\frac{n-1}{2}\right].$$

Tak například v S_4 existují následující fluktuační permutace: $(1, 3, 2, 4)$, $(1, 4, 2, 3)$, $(2, 3, 1, 4)$, $(2, 4, 1, 3)$, $(3, 4, 1, 2)$. Označme ξ_n počet fluktuačních permutací v S_n, $\xi_0 = 1$. Tato čísla se nazývají *Eulerova*. Platí:

$$(\xi_n)_{n=0}^{\infty} = 1, 1, 1, 2, 5, 16, 61, \dots$$

a) Vypište 16 fluktuačních permutací v S_5.

b) Platí rekurentní formule:

$$\xi_{n+1} = \frac{1}{2} \cdot \sum_{k=0}^{n} \binom{n}{k} \xi_k \xi_{n-k}$$

Ukažte, že $\xi_7 = 272$.

9 Vytvořující funkce

9.1. Poznámka. (O nekonečných řadách funkcí.) Předpokládejme znalost nekonečných číselných řad. Shrneme zde některé elementární poznatky teorie nekonečných řad funkcí.

Nechť $(f_n(x))_{n=1}^{\infty}$ je posloupnost funkcí definovaných na množině $M \subseteq \mathbb{R}$. *Nekonečnou řadou funkcí* nazýváme symbol

$$\sum_{n=1}^{\infty} f_n(x) = f_1(x) + f_2(x) + \cdots + f_n(x) + \dots .$$

Řekneme, že tato řada *konverguje v bodě* $x_0 \in M$, jestliže konverguje číselná řada $\sum_{n=1}^{\infty} f_n(x_0)$.

Řekneme, že řada funkcí $\sum_{n=1}^{\infty} f_n(x)$ *konverguje na množině* K, jestliže konverguje v každém bodě $x \in K$.

Součtem řady $\sum_{n=1}^{\infty} f_n(x)$ na množině K nazýváme funkci $f(x)$ definovanou takto:

$$\text{pro každé } x_0 \in K \text{ platí } f(x_0) = \sum_{n=1}^{\infty} f_n(x_0).$$

Mocninnou řadou nazýváme řadu funkcí tvaru

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \dots ,$$

kde $a_0, a_1, a_2, \dots$ jsou reálná (respektive komplexní) čísla – tzv. *koeficienty řady*. Jistě existuje $\limsup_{n\to\infty} \sqrt[n]{|a_n|} = u$ (může být i $u = +\infty$). Číslo $r = \frac{1}{u}$ (kde $\frac{1}{0} = \infty$, $\frac{1}{\infty} = 0$) nazýváme *poloměr konvergence* mocninné řady $\sum_{n=0}^{\infty} a_n x^n$. Snadno lze dokázat, že tato mocninná řada konverguje na intervalu $(-r, r)$ a diverguje v každém bodě $x \in \mathbb{R}$, $|x| > r$.

V matematické analýze se dokazuje, že například

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \dots \text{ pro každé } x \in \mathbb{R} \text{ (tj. } r = \infty).$$

Odtud například plyne, že

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots, \qquad \frac{1}{e} = e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots,$$

což jsou vztahy, které jsme použili již v příkladu 2.3.

Zobecněním známé binomické věty je následující tvrzení:

Pro každé reálné číslo α platí

$$(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n = \binom{\alpha}{0} + \binom{\alpha}{1}x + \binom{\alpha}{2}x^2 + \dots + \binom{\alpha}{n}x^n + \dots ,$$

přičemž poloměr konvergence uvedené řady je $r = 1$ (tj. uvedená rovnost platí pro všechna $x \in (-1, 1)$).

Tak například

$$\sqrt{1+x} = (1+x)^{\frac{1}{2}} = \binom{\frac{1}{2}}{0} + \binom{\frac{1}{2}}{1}x + \binom{\frac{1}{2}}{2}x^2 + \dots + \binom{\frac{1}{2}}{n}x^n + \dots .$$

Podle příkladu 2.9 (c) tedy platí

$$\sqrt{1+x} = 1 + \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n \cdot 2^{2n-1}} \binom{2n-2}{n-1} x^n .$$

Je-li $\sum\limits_{n=0}^{\infty} a_n x^n$ mocninná řada a r její poloměr konvergence, lze uvnitř intervalu $(-r, r)$ tuto řadu derivovat a integrovat člen po členu, tj. pro každé $x \in (-r, r)$ platí

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)' = \sum_{n=0}^{\infty} (a_n x^n)' = \sum_{n=1}^{\infty} n \cdot a_n x^{n-1},$$

přičemž zderivovaná řada má stejný poloměr konvergence jako řada původní.

Dále pro každý interval $[a, b] \subseteq (-r, r)$ platí

$$\int_a^b \left(\sum_{n=0}^{\infty} a_n x^n\right) dx = \sum_{n=0}^{\infty} \left(\int_a^b a_n x^n dx\right).$$

Mocninné řady $\sum\limits_{n=0}^{\infty} a_n x^n$, $\sum\limits_{n=0}^{\infty} b_n x^n$ podle definice považujeme za sobě rovné, jestliže pro každé $n \in \mathbb{N}$ platí $a_n = b_n$.

Konečně součet, součin a podíl mocninných řad definujeme následovně:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} c_n x^n, \qquad \text{kde } c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0,$$

$$\frac{\sum\limits_{n=0}^{\infty} a_n x^n}{\sum\limits_{n=0}^{\infty} b_n x^n} = \sum_{n=0}^{\infty} d_n x^n,$$

kde $\sum\limits_{n=0}^{\infty} d_n x^n$ je ta mocninná řada, pro kterou platí

$$\sum_{n=0}^{\infty} b_n x^n \cdot \sum_{n=0}^{\infty} d_n x^n = \sum_{n=0}^{\infty} a_n x^n.$$

9.2. Definice. *Vytvořující funkcí* posloupnosti $(a_n)_{n=0}^{\infty}$ nazýváme mocninnou řadu $\sum\limits_{n=0}^{\infty} a_n x^n$ (na množině, kde tato řada konverguje).

9.3. Příklad. (a) Víme, že pro $x \in (-1, 1)$ platí

$$1 + x + x^2 + \cdots + x^n + \cdots = \frac{1}{1-x} \qquad \text{(geometrická řada).}$$

To znamená, že $\dfrac{1}{1-x}$ je vytvořující funkce posloupnosti $1, 1, 1, 1, \ldots$.

(b) Najdeme vytvořující funkci posloupnosti $1, 2, 3, 4, \ldots$.
Podle poznámky 9.1 víme, že pro $x \in (-1, 1)$ platí

$$\begin{aligned}(1 + x + x^2 + \cdots + x^n + \ldots)' &= 1 + 2x + 3x^2 + \cdots + nx^{n-1} + \cdots = \\ &= \left(\frac{1}{1-x}\right)' = \frac{1}{(1-x)^2}.\end{aligned}$$

Vytvořující funkcí posloupnosti $(n)_{n=1}^{\infty}$ je tak funkce $\dfrac{1}{(1-x)^2} = \sum\limits_{n=1}^{\infty} nx^{n-1}$.

(c) Víme, že pro každé $n \in \mathbb{N}$ a každé $x \in \mathbb{R}$ platí

$$(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k \qquad \text{(binomická věta).}$$

To znamená, že funkce $(1+x)^n$ je vytvořující funkcí konečné posloupnosti

$$\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n} \qquad \text{(tj. řádku Pascalova trojúhelníka).}$$

Vytvořující funkce jsou mocným nástrojem k řešení řady kombinatorických úloh, především těch, které vedou na rekurentní formule. K řešení komplikovanějších případů bychom však potřebovali hlubší znalosti o řadách funkcí. Proto se omezíme jen na několik jednodušších příkladů.

9.4. Příklad. *Řezem* v řetězci (tj. úplně uspořádané množině) $A \neq \emptyset$ rozumíme uspořádanou dvojici $[X, Y]$ neprázdných podmnožin množiny A takových, že $X \cap Y = \emptyset$, $X \cup Y = A$ a pro každé dva prvky $x \in X$, $y \in Y$ platí $x \leq y$ (tj. $x < y$). Je zřejmé, že v konečném n-prvkovém řetězci $A = \{a_1 < a_2 < \dots < a_n\}$ existuje $n-1$ řezů, protože „dolní třídou“ X může být právě jen některá z množin $\{a_1 < a_2 < \dots < a_i\}$, kde i může nabýt hodnot $1, \dots, n-1$.

Dělením řetězce $A = \{a_1 < a_2 < \dots < a_n\}$ nazveme každou posloupnost sestrojenou následovně: v prvním kroku utvořme nějaký řez $[X, Y]$ v A. Ve druhém kroku utvořme řez ve třídě X i Y, pokud tyto třídy nejsou jednoprvkové. Ve třetím kroku utvoříme řez v každé z nově vzniklých tříd obsahujících alespoň dva prvky atd. Posloupnost ukončíme v okamžiku, kdy jsou všechny vzniklé třídy jednoprvkové.

Je-li například $A = \{a_1 < a_2 < a_3 < a_4 < a_5\}$, je dělením na A například posloupnost

$$\begin{aligned} t_1 &= [\{a_1, a_2\}, \{a_3, a_4, a_5\}] \\ t_2 &= [\{a_1\}, \{a_2\}, \{a_3\}, \{a_4, a_5\}] \\ t_3 &= [\{a_1\}, \{a_2\}, \{a_3\}, \{a_4\}, \{a_5\}] \end{aligned}$$

Náš úkol nyní zní: *Kolik existuje dělení na konečném řetězci?*

Označme R_n počet dělení $(n+1)$-prvkového řetězce. Představme si první krok nějakého dělení tohoto řetězce. Jak jsme již uvedli, můžeme tento krok utvořit n způsoby (dolní třída může obsahovat $1, \dots, n$ prvků). Podle toho, kolik prvků dolní třída tohoto prvního řezu obsahuje, rozdělíme všechna dělení do n skupin. Do k-té skupiny patří dělení, v nichž dolní třída 1. řezu obsahuje k prvků. Spočtěme nyní počet dělení patřících do k-té skupiny. Protože dolní třída obsahuje k prvků, existuje na ní R_{k-1} řezů. Horní třída prvního řezu obsahuje

$n+1-k$ prvků, proto na ní existuje R_{n-k} řezů. Odtud zřejmě plyne rekurentní formule

$$R_n = R_0 R_{n-1} + R_1 R_{n-2} + \cdots + R_{n-1} R_0, \qquad R_0 = 1.$$

Vzhledem k tomu, že uvedená formule není konečného řádu, nemůžeme ji vyřešit pomocí metod odvozených v paragrafu 8. Ukážeme však, jak lze řešení nalézt pomocí vytvořující funkce posloupnosti $(R_n)_{n=0}^{\infty}$.

Vytvořující funkcí je v tomto případě funkce

$$F(x) = \sum_{n=0}^{\infty} R_n x^n.$$

Platí

$$F^2(x) = F(x) \cdot F(x) = \sum_{n=0}^{\infty} R_n x^n \cdot \sum_{n=0}^{\infty} R_n x^n = \sum_{n=0}^{\infty} c_n x^n,$$

kde

$$c_n = R_0 R_n + R_1 R_{n-1} + \cdots + R_n R_0 = R_{n+1},$$

tj.

$$F^2(x) = \sum_{n=0}^{\infty} R_{n+1} x^n.$$

Definujeme-li nyní funkci $G(x)$ vztahem $G(x) = x \cdot F(x)$, platí

$$G^2(x) = x^2 \cdot F^2(x) = x^2 \cdot \sum_{n=0}^{\infty} R_{n+1} x^n.$$

Platí tak

$$\begin{aligned} G(x) &= x \cdot \sum_{n=0}^{\infty} R_n x^n = R_0 x + R_1 x^2 + R_2 x^3 + \ldots \\ G^2(x) &= x^2 \cdot \sum_{n=0}^{\infty} R_{n+1} x^n = R_1 x^2 + R_2 x^3 + \ldots . \end{aligned}$$

Odtud

$$G^2(x) = G(x) - R_0 x = G(x) - x \qquad \text{(neboť } R_0 = 1\text{)}.$$

Z rovnice

$$G^2(x) - G(x) + x = 0$$

plyne

$$G(x) = \frac{1 \pm \sqrt{1-4x}}{2}.$$

Protože v bodě $x = 0$ řada $\sum_{n=0}^{\infty} R_n x^n$ konverguje, existuje $G(0)$. Z posledního vztahu plyne

$$G(0) = \frac{1 \pm \sqrt{1}}{2} = \begin{cases} 1, \\ 0, \end{cases}$$

přičemž podle definice musí být $G(0) = 0$. Tzn., že

$$G(x) = \frac{1 - \sqrt{1-4x}}{2}.$$

Funkci $\sqrt{1-4x}$ však umíme rozvinout v mocninnou řadu. Podle poznámky 9.1 platí

$$\sqrt{1-4x} = (1-4x)^{\frac{1}{2}} = \sum_{n=0}^{\infty} (-1)^n \binom{\frac{1}{2}}{n} (4x)^n,$$

tj.

$$\begin{aligned} G(x) &= \frac{1}{2}\left[1 - \sum_{n=0}^{\infty} (-1)^n \binom{\frac{1}{2}}{n} (4x)^n\right] = \\ &= \frac{1}{2}\left[1 - \left(1 + \sum_{n=1}^{\infty} (-1)^{2n-1} \cdot \frac{4^n}{n \cdot 2^{2n-1}} \binom{2n-2}{n-1} x^n\right)\right] = \\ &= \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} x^n = \sum_{n=0}^{\infty} \frac{1}{n+1} \binom{2n}{n} x^{n+1}. \end{aligned}$$

Protože $G(x) = x \cdot F(x)$, plyne odtud

$$\sum_{n=0}^{\infty} R_n x^{n+1} = \sum_{n=0}^{\infty} \frac{1}{n+1} \binom{2n}{n} x^{n+1},$$

tj.

$$R_n = \frac{1}{n+1} \binom{2n}{n}.$$

9.5. Poznámka. Na příkladu 9.4 lze názorně demonstrovat, jak lze často úlohy na první pohled zcela odlišné převést na řešení téže rekurentní formule.

V příkladu 3.33 jsme řešili problém, kolika způsoby se mohou lidé postavit do fronty na Večerník tak, aby měl prodávající vždy nazpět. Zjistili jsme, že když má k lidí desetikorunu a k lidí pětikorunu, je těchto možností

$$\frac{1}{k+1} \binom{2k}{k}.$$

Nyní všechny „příznivé" permutace k jedniček a k pětek (viz příklad 3.33) rozdělme do k tříd takto: permutace $a_1, \dots, a_{2k}$ patří do s-té třídy právě tehdy, když s je nejmenší přirozené číslo takové, že mezi ciframi $a_1, \dots, a_{2s}$ je právě s jedniček a s pětek (například permutace 55151151 patří do 3. třídy). Je zřejmé, že když příznivá permutace patří do s-té třídy a $s < k$, pak cifra na místě $2s + 1$ musí být 5; jinak by daná permutace nebyla příznivá.

Nyní zjistíme, kolik permutací je obsaženo v s-té třídě. Buď tedy

$$a_1, \dots, a_{2s}, \dots, a_{2k}$$

permutace s-té třídy. Pak mezi členy $a_1, \dots, a_{2s}$ je s jedniček a s pětek, přičemž pro každé $r < s$ je mezi členy $a_1, \dots, a_{2r}$ více pětek než jedniček. Snadno však lze dokázat, že takových permutací $a_1, \dots, a_{2s}$ je celkem $\frac{1}{s}\binom{2s-2}{s-1}$. Mezi členy $a_{2s+1}, \dots, a_{2k}$ je nyní $k - s$ jedniček a $k - s$ pětek. Přitom permutace $a_{2s+1}, \dots, a_{2k}$ musí být evidentně rovněž příznivá. Počet těchto příznivých permutací je podle příkladu 3.33

$$\frac{1}{k-s+1} \cdot \binom{2k-2s}{k-s}.$$

Odtud ovšem plyne, že v s-té třídě je celkem

$$\frac{1}{s} \cdot \binom{2s-2}{s-1} \cdot \frac{1}{k-s+1} \cdot \binom{2k-2s}{k-s}$$

permutací. Vzhledem k tomu, že počet všech příznivých permutací je, jak jsme již uvedli,

$$\frac{1}{k+1}\binom{2k}{k},$$

plyne odtud identita

$$\sum_{s=1}^{k} \frac{k+1}{s(k-s+1)} \binom{2s-2}{s-1}\binom{2k-2s}{k-s} = \binom{2k}{k}.$$

Zavedeme-li nyní označení

$$\frac{1}{s+1} \cdot \binom{2s}{s} = T_s,$$

lze uvedenou identitu přepsat na tvar

$$T_0 T_{k-1} + T_1 T_{k-2} + \cdots + T_{k-1} T_0 = T_k,$$

což je formule, kterou jsme ve zcela jiné souvislosti řešili v příkladu 9.4. Řešení příkladů 3.33 a 9.4 je proto zákonitě stejné.

Nyní ukážeme, jak vypadají vytvořující funkce posloupností, udávajících počty rozkladů přirozených čísel, o nichž jsme hovořili v paragrafu 6.

9.6. Věta. *Pro vytvořující funkci posloupnosti* $(p(n))_{n=1}^{\infty}$ *platí*

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} \frac{1}{1-x^n} \qquad (\textit{pro } |x| < 1),$$

položíme-li definitoricky $p(0) = 1$.

Důkaz. Potřebujeme dokázat, že

$$1 + p(1)x + p(2)x^2 + \cdots + p(n)x^n + \cdots = \frac{1}{x-1} \cdot \frac{1}{1-x^2} \cdot \ldots \cdot \frac{1}{1-x^n} \cdot \ldots$$

Buďte $a_i \in \mathbb{R}$ libovolná čísla, $i = 1, 2, \ldots$. Víme, že když $\left|a_i x^i\right| < 1$, pak platí

$$\frac{1}{1-a_i x^i} = 1 + a_i x^i + a_i^2 x^{2i} + \cdots + a_i^n x^{ni} + \ldots \qquad \text{(součet geometrické řady).}$$

Odtud plyne

$$\frac{1}{(1-a_1x)\cdot(1-a_2x^2)\cdot\ldots\cdot(1-a_kx^k)\cdot\ldots} = (1 + a_1x + a_1^2x^2 + a_1^3x^3 + \ldots)\cdot$$

$$\cdot(1 + a_2x^2 + a_2^2x^4 + a_2^3x^6 + \ldots)\cdot\ldots\cdot(1 + a_kx^k + a_k^2x^{2k} + a_k^3x^{3k} + \ldots)\cdot\cdots =$$

$$= 1 + a_1x + (a_1^2 + a_2)x^2 + \cdots + (a_1^{r_1}a_2^{r_2}\ldots a_k^{r_k} + \ldots)x^n + \ldots .$$

V koeficientu u x^n určuje každý sčítanec $a_1^{r_1}a_2^{r_2}\ldots a_k^{r_k}$ právě jeden rozklad čísla n, totiž

$$\underbrace{(1+1+\cdots+1)}_{r_1} + \underbrace{(2+2+\cdots+2)}_{r_2} + \cdots + \underbrace{(k+k+\cdots+k)}_{r_k} = n.$$

(Například koeficient u x^2 je roven součtu $a_1^2 + a_1^0a_2^1$, jehož sčítanci určují po řadě rozklady $1+1$ a 2 čísla 2.)

Když nyní položíme $a_1 = a_2 = \cdots = 1$, obdržíme dokazované tvrzení. •

9.7. Poznámka. (a) Poloměr konvergence vytvořující funkce $\sum\limits_{n=0}^{\infty} p(n)x^n$ je tedy roven 1.

(b) Inverzní funkcí k vytvořující funkci $\sum\limits_{n=0}^{\infty} p(n)x^n$ je nekonečný součin

$$\prod_{n=1}^{\infty}(1-x^n) = (1-x)\cdot(1-x^2)\cdot\ldots\cdot(1-x^n)\cdot\cdots = \sum_{n=0}^{\infty} c_n x^n.$$

Koeficienty c_n mají rovněž jednoduchou kombinatorickou interpretaci. Platí

$$c_n = A(n) - B(n),$$

kde $A(n)$ je počet rozkladů čísla n na sudý počet navzájem různých sčítanců a $B(n)$ je počet rozkladů čísla n na lichý počet navzájem různých sčítanců.

(c) Již Euler, který první odvodil vytvořující funkci posloupnosti $(p(n))_{n=1}^{\infty}$, dokázal, že „většina" koeficientů c_n je rovna nule. Přesněji řečeno, odvodil následující vztah, dnes běžně nazývaný *Eulerova identita*:

$$\prod_{n=1}^{\infty}(1 - x^n) = 1 + \sum_{k=1}^{\infty}(-1)^k \cdot \left(x^{\frac{3k^2-k}{2}} + x^{\frac{3k^2+k}{2}}\right).$$

Důkaz této identity, který je nejvýhodnější provádět pomocí Ferrersových diagramů, zde uvádět nebudeme.

(d) Eulerovu identitu lze zřejmě v řeči rozkladů přirozených čísel interpretovat – při označení uvedeném v (b) – takto: *Nechť přirozené číslo n lze psát ve tvaru* $\dfrac{3k^2 \pm k}{2}$, *kde k je vhodné přirozené číslo. Pak* $A(n) = B(n)$. *Je-li přirozené číslo n výše uvedeného tvaru, pak* $A(n) - B(n) = (-1)^k$.

9.8. Poznámka. Ideu použitou v důkazu věty 9.6 lze samozřejmě použít v řadě analogických případů. Chceme-li například zjistit počet rozkladů čísla n na sčítance, z nichž každý je roven některému z čísel $s_1, \dots, s_k$, přičemž sčítanci jsou navzájem různí, utvoříme výraz

$$(1 + x^{s_1})(1 + x^{s_2}) \dots (1 + x^{s_k}).$$

Po roznásobení obdržíme evidentně výraz, v němž koeficient u x^n udává počet hledaných rozkladů.

9.9. Poznámka. Vytvořující funkcí posloupnosti $(p(n, k))_{n=1}^{\infty}$ je funkce

$$G(x) = \frac{x^k}{(1 - x)(1 - x^2) \dots (1 - x^k)}.$$

Vytvořující funkci posloupnosti udávají počty rozkladů čísla n na liché sčítance je funkce

$$H(x) = \frac{1}{(1 - x)(1 - x^3)(1 - x^5) \dots}.$$

Konečně vytvořující funkcí posloupnosti udávající počet rozkladů čísla n na navzájem různé sčítance, je funkce

$$K(x) = (1 + x)(1 + x^2)(1 + x^3) \cdots = \prod_{k=1}^{\infty}(1 + x^k).$$

Ukažme si, jak lze pomocí uvedených vytvořujících funkcí snadno odvozovat tvrzení o rozkladech přirozených čísel. Platí například

$$\begin{aligned} H(x) &= \frac{1}{(1-x)(1-x^3)(1-x^5)\dots} = \\ &= \frac{(1-x^2)(1-x^4)(1-x^6)(1-x^8)\dots}{(1-x)(1-x^2)(1-x^3)(1-x^4)\dots} = \\ &= \frac{[(1-x)(1+x)]\cdot\left[(1-x^2)(1+x^2)\right]\cdot\left[(1-x^3)(1+x^3)\right]\cdot\dots}{(1-x)(1-x^2)(1-x^3)(1-x^4)\dots} = \\ &= (1+x)(1+x^2)(1+x^3)\cdots = K(x). \end{aligned}$$

Dokázali jsme tak právě, že platí následující věta.

9.10. Věta. *Počet rozkladů čísla n na navzájem různé sčítance je roven počtu rozkladů čísla n na liché sčítance.*

Poznámky a cvičení

1. Dokažte, že vytvořující funkce Fibonacciovy posloupnosti je

$$g(x) = \sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2}.$$

2. Buď (B_n) posloupnost Bellových čísel.

a) Dokažte, že řada $\sum_{n=0}^{\infty} B_n x^n$ diverguje pro všechna $x \neq 0$.

b) Dokažte, že řada $\sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$ absolutně konverguje na $\mathbb{R}$.

10 Bloková schémata, latinské čtverce a konečné roviny

Jedním z centrálních pojmů moderní kombinatoriky jsou tzv. *bloková schémata*, nazývaná též *konfigurace*, *designy* i jinak. Teorie blokových schémat je intenzívně rozvíjena a je velmi složitá. Proto se zmíníme jen o nejzákladnějších pojmech a zavedeme některé jednoduché typy.

10.1. Definice. Buďte v, b, k, r, λ přirozená čísla, A konečná množina, $|A| = v$. Systém podmnožin

$$X_1, X_2, \ldots, X_b$$

množiny A se nazývá *blokové schéma typu* (v, b, k, r, λ) v množině A, jestliže $|X_1| = |X_2| = \cdots = |X_b| = k$, každý prvek $a \in A$ je prvkem právě r množin X_i a pro každé dva různé prvky $a, b \in A$ je $\{a, b\}$ podmnožinou právě λ množin X_i.
Množiny X_i se nazývají *bloky* daného blokového schématu.

Je samozřejmé, že nemusí existovat blokové schéma libovolného předepsaného typu. Jak však ukážeme v příkladu 10.2, může blokové schéma existovat.

10.2: Příklad. Buď $A = \{1, 2, 3, 4, 5, 6, 7\}$. Blokovým schématem typu $(7, 7, 3, 3, 1)$ je například systém množin

$$\begin{array}{lllllllll} X_1 & = & \{1,2,4\} & X_4 & = & \{4,5,7\} & X_7 & = & \{1,3,7\} \\ X_2 & = & \{2,3,5\} & X_5 & = & \{1,5,6\} & & & \\ X_3 & = & \{3,4,6\} & X_6 & = & \{2,6,7\} & & & \end{array}$$

10.3. Věta. *Existuje-li blokové schéma typu* (v, b, k, r, λ), *platí*

$$bk = vr, \quad r(k-1) = \lambda(v-1).$$

Důkaz. První rovnice je evidentní; levá i pravá strana zřejmě udává číslo $|X_1| + \cdots + |X_b|$. Ve druhé rovnici sečítáme počty dvojic obsahujících daný prvek $a_i \in A$. Prvek a_i je obsažen v r blocích a v každém z nich tvoří dvojice se zbývajícími $k - 1$ prvky. Současně však a_i tvoří λ dvojic s každým z $v - 1$ zbývajících prvků. •

10.4. Definice. Blokové schéma typu $(v, b, 3, r, \lambda)$ se nazývá *systémem trojic*. Pro $\lambda = 1$ se systém trojic nazývá *Steinerův*.

10.5. Poznámka. Steinerovým systémem trojic je například blokové schéma z příkladu 10.2. Je to tedy takový systém tříprvkových podmnožin dané konečné množiny, že každé dva prvky se současně vyskytují v právě jedné z podmnožin.

J. Steiner v roce 1853 zformuloval tento problém následovně: *Pro která přirozená čísla n lze rozdělit n písmen do trojic tak, aby se každá (neuspořádaná) dvojice písmen vyskytovala v právě jedné trojici?*

Protože se ve Steinerových trojicích každé písmeno vyskytuje s každým jiným písmenem právě jednou, musí být číslo $n-1$ sudé, tj. $n \equiv 1 (\mathrm{mod}\ 2)$. (Stačí si totiž uvědomit, že každé písmeno je ve trojici s dalšími dvěma písmeny.)

Dále víme, že každá trojice obsahuje tři dvojice a každá dvojice se v trojicích vyskytne právě jednou. Odtud plyne, že celkový počet dvojic, což je číslo $\binom{n}{2} = \dfrac{n(n-1)}{2}$, musí být násobek tří. Celkově odtud plyne, že číslo n musí být tvaru $6k+1$, respektive $6k+3$, $k \in \mathbb{N}$ (tj. $n \equiv 1, 3 (\mathrm{mod}\ 6)$).

V roce 1859 dokázal M. Riess, že tato nutná podmínka je současně postačující, tj. platí následující tvrzení, které uvedeme bez důkazu.

10.6. Věta. *Blokové schéma typu $(n, b, 3, r, 1)$ existuje právě tehdy, když*

$$n = 6k+1 \quad \textit{nebo} \quad n = 6k+3, \qquad k \in \mathbb{N}_0, n \geq 3.$$

Buď dán Steinerův systém trojic typu $(n, b, 3, r, 1)$. Jak jsme již uvedli v poznámce 10.5, je počet všech dvojic roven číslu $\frac{n(n-1)}{2}$. Každá trojice obsahuje tři dvojice, takže počet b všech bloků je roven číslu $\frac{n(n-1)}{6}$. Podle věty 10.3 dále platí $r \cdot 2 = n - 1$, tj. $r = \frac{n-1}{2}$.

Odtud a z věty 10.6 plyne

10.7. Věta. *Na n-prvkové množině existuje systém Steinerových trojic právě tehdy, když $n = 6k+1$ nebo $n = 6k+3$ ($k \in \mathbb{N}_0, n \geq 3$). V tom případě je těchto trojic $\dfrac{n(n-1)}{6}$ a každý prvek se vyskytuje v $\dfrac{n-1}{2}$ trojicích.*

10.8. Příklad. Uveďme Steinerovy systémy trojic pro nejmenší tři možné hodnoty n, tj. $n = 3$, $n = 7$ a $n = 9$.

$n = 3$:	1 2 3			
$n = 7$:	1 2 3	1 6 7	2 5 7	3 5 6
	1 4 5	2 4 6	3 4 7	
$n = 9$:	1 2 3	1 7 9	2 7 8	3 6 9
	1 4 5	2 4 9	3 4 8	4 6 7
	1 6 8	2 5 6	3 5 7	5 8 9

10.9. Poznámka. Úlohu vedoucí na Steinerův systém trojic (s dalšími podmínkami) zformuloval ještě před Steinerem v roce 1847 anglický matematik R. T. Kirkman. Jde o známý *Kirkmanův problém 15 dívek*: *15 školaček chodí denně na procházku seřazeno do pěti trojic. Lze je řadit do trojic tak, aby každá s každou šla během 7 dnů ve trojici právě jednou?*

Kladná odpověď je vcelku jednoduchá. Rozpis procházek může být následující:

1 2 3	1 4 7	1 5 13	1 6 8	1 9 10
4 5 6	2 5 10	2 4 12	2 11 13	2 7 14
7 8 9	6 11 14	6 7 15	4 10 15	3 5 15
10 11 12	9 12 15	8 10 14	5 9 14	4 8 11
13 14 15	3 8 13	3 9 11	3 7 12	6 12 13

1 11 15	1 12 14
2 6 9	2 8 15
3 4 14	3 6 10
5 8 12	4 9 13
7 10 13	5 7 11

Jde o Steinerův systém trojic s parametry $v = 15, b = 35, k = 3, r = 7, \lambda = 1$, přičemž musí být splněna ještě další podmínka: trojice musí být rozděleny na sedm tříd po pěti trojicích tak, aby byl každý prvek v každé třídě právě jednou.

Dodnes není známo, pro která n má Kirkmanův problém, přesněji řečeno jeho příslušné přeformulování, řešení.

Úzkou souvislost s teorií blokových schémat mají tzv. **latinské čtverce**.

10.10. Definice. Buď dána libovolná n-prvková množina A ($n \in \mathbb{N}$). *Latinským čtvercem řádu n* rozumíme čtvercovou tabulku o n řádcích a n sloupcích takovou, že v každém řádku a každém sloupci je permutace všech prvků množiny A.

10.11. Příklad.

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

1	2	3	4	5
2	1	4	5	3
3	4	5	1	2
4	5	2	3	1
5	3	1	2	4

jsou latinské čtverce řádu 5.

10.12. Poznámka. Je zřejmé, že existují latinské čtverce každého řádu $n \in \mathbb{N}$. Z každého latinského čtverce řádu $n > 1$ můžeme snadno utvořit další latinské čtverce například tak, že změníme pořadí řádků, respektive sloupců, nebo provedeme nějakou permutaci prvků množiny A nebo eventuálně uvedené postupy zkombinujeme.

Řekneme, že dva latinské čtverce jsou *ekvivalentní*, jestliže výše uvedeným způsobem lze jeden převést na druhý.

Lehce lze dokázat, že každý latinský čtverec 5. řádu je ekvivalentní právě s jedním z latinských čtverců z příkladu 10.11.

Latinské čtverce se vyskytují v nejrůznějších souvislostech. Utvoříme-li například obvyklou tabulku násobení v libovolné konečné grupě, obdržíme zřejmě latinský čtverec.

Latinské čtverce mají rovněž jednoduchou geometrickou interpretaci. Považujme každé z n^2 míst v latinském čtverci za „bod" a představme si následující „spojnice" bodů: (1) řádky latinského čtverce, (2) sloupce latinského čtverce, (3) body v nichž je vepsán stejný prvek. Tyto spojnice tvoří tzv. 3-*síť* s n^2 uzly. Každá spojnice je tvořena n body, spojnice téhož „typu" se neprotínají a každým bodem prochází právě jedna spojnice každého ze tří uvedených typů.

Naopak každou 3-síť lze interpretovat jako latinský čtverec.

10.13. Definice. Buďte dány dva latinské čtverce n-tého řádu utvořené z prvků množiny A. Označme a_{ij}, respektive b_{ij}, prvek ležící v průsečíku i-tého řádku a j-tého sloupce prvního, respektive druhého latinského čtverce. Protože $|A^2| = n^2$, lze všechny prvky množiny A^2 vepsat do schématu utvořeného z n řádků a n sloupců.
Řekneme, že dané dva čtverce (a_{ij}) a (b_{ij}) jsou *ortogonální*, když ve čtverci (a_{ij}, b_{ij}) je každý prvek z A^2 právě jednou.

10.14. Příklad. Čtverce

$$\begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix} \qquad \text{a} \qquad \begin{matrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{matrix}$$

jsou zřejmě ortogonální, neboť když z nich utvoříme popsaným způsobem čtverec

$$\begin{matrix} 12 & 23 & 31 \\ 21 & 32 & 13 \\ 33 & 11 & 22 \end{matrix}$$

jsou v tomto čtverci všechny prvky kartézského součinu $\{1,2,3\} \times \{1,2,3\}$ (přičemž prvek $[i, j]$ jsme zapsali stručně jako ij).

Je zřejmé, že neexistují ortogonální latinské čtverce 2. řádu. Jediné latinské čtverce 2. řádu jsou totiž čtverce

$$\begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array} \qquad \text{a} \qquad \begin{array}{cc} 2 & 1 \\ 1 & 2 \end{array}$$

a ty nejsou ortogonální, neboť ve čtverci

$$\begin{array}{cc} 12 & 21 \\ 21 & 12 \end{array}$$

nejsou všechny prvky součinu $\{1,2\} \times \{1,2\}$.

Problematiku existence ortogonálních latinských čtverců 6. řádu zpopularizoval Euler, když v roce 1782 zformuloval slavnou *úlohu o 36 důstojnících*:

Sestavte 36 důstojníků 6 různých hodností ze 6 různých pluků do čtverce tak, aby v žádné řadě ani žádném zástupu nestáli dva důstojníci stejné hodnosti ani dva důstojníci ze stejného pluku.

Je zřejmé, že tato Eulerova úloha vede na konstrukci dvou ortogonálních latinských čtverců 6. řádu. Protože se konstrukce těchto čtverců Eulerovi nedařila, vyslovil hypotézu, že *neexistují dva ortogonální latinské čtverce řádu* $n = 4k + 2$, $k = 0, 1, 2, \ldots$. (Podrobnosti viz ve cvičení 3 na konci této kapitoly.)

Pravdivost této hypotézy pro $k = 0$ jsme ukázali výše. Samotný Euler se nedožil vyřešení tohoto problému pro $k > 0$. Teprve v roce 1900 dokázal francouzský matematik G. Tarry, že **neexistují dva ortogonální latinské čtverce 6. řádu**.

Vzhledem k tomu, že latinských čtverců 6. řádu je téměř 25 000 000 a Tarry své tvrzení odvodil jistým systematickým výčtem, je jeho výkon opravdu pozoruhodný. (O počtu latinských čtverců řádu n viz kapitolu 2, poznámku 8.16).

Eulerova hypotéza byla dlouho považována za správnou. Vyvrácena byla až v roce 1959, kdy R. C. Bose a S. Shrikhande sestrojili dva ortogonální latinské čtverce 22. řádu.

Později Bose, Srikhande a E. T. Parker dokázali dokonce následující tvrzení:

10.15. Věta. *Pro každé přirozené $n > 2$ kromě $n = 6$ existují ortogonální latinské čtverce n-tého řádu.*

Důkaz. Důkaz nebudeme provádět, neboť přesahuje rámec tohoto textu. K jeho provedení je třeba řady tvrzení o blokových schématech. •

10.16. Příklad. Ukažme dva ortogonální latinské čtverce 10. řádu.

00	49	17	96	28	83	75	61	52	34
76	11	59	27	90	38	84	02	63	45
85	70	22	69	37	91	48	13	04	56
58	86	71	33	09	47	92	24	15	60
93	68	80	72	44	19	57	35	26	01
67	94	08	81	73	55	29	46	30	12
39	07	95	18	82	74	66	50	41	23
21	32	43	54	65	06	10	77	88	99
42	53	64	05	16	20	31	89	97	78
14	25	36	40	51	62	03	98	79	87

Z tohoto příkladu tedy plyne nesprávnost Eulerovy hypotézy již pro $k = 2$.

Důležitou částí kombinatoriky, těsně propojenou s teorií blokových schémat, jsou tzv. *konečné geometrie.* Ukažme souvislost některých pojmů konečných geometrií s teorií latinských čtverců.

10.17. Definice. Buď $A \neq \emptyset$ konečná množina, $\mathcal{R} \subseteq \mathcal{P}(A)$. Nechť platí:

(1) Pro každé $x, y \in A$, $x \neq y$, existuje právě jedna množina $P \in \mathcal{R}$ tak, že $\{x, y\} \subseteq P$.

(2) Pro každou množinu $P \in \mathcal{R}$ a pro každý prvek $x \in A$, $x \notin P$, existuje právě jedna množina $Q \in \mathcal{R}$ taková, že $x \in Q$ a $P \cap Q = \emptyset$.

(3) Existují tři navzájem různé prvky $x, y, z \in A$ takové, že $\{x, y, z\}$ není podmnožinou žádné množiny $P \in \mathcal{R}$.

Pak se dvojice $(A, \mathcal{R})$ nazývá *konečná afinní rovina.* Prvky množiny A se nazývají *body* a prvky množiny $\mathcal{R}$ *přímky* této roviny.

Ve shodě s obvyklou geometrickou terminologií zavedeme následující definici.

10.18. Definice. Dvě disjunktní přímky nazveme *rovnoběžkami. Směrem* v afinní rovině nazveme systém všech rovnoběžek s danou přímkou.
Skutečnost, že přímky P, Q jsou rovnoběžné, budeme značit symbolem $P \parallel Q$.

10.19. Věta. *Nechť P, Q, R jsou přímky v konečné afinní rovině. Nechť $P \parallel Q$, $Q \parallel R$, $P \neq R$. Pak $R \parallel P$.*

Důkaz. Připusťme, že existuje $a \in P \cap R$. Pak by bodem a procházely dvě rovnoběžky s přímkou Q, což není možné. •

10.20. Věta. *Všechny přímky v konečné afinní rovině mají stejný počet bodů.*

Důkaz. I. Nejprve dokážeme, že stejný počet bodů mají všechny přímky téhož směru.

Nechť tedy v konečné afinní rovině $(A, \mathcal{R})$ existuje přímka P tvořená n body $a_1, \dots, a_n$. Buď $b \in A$ libovolný bod neležící na přímce P (existence takového bodu plyne z vlastnosti (3)). Podle (2) prochází tímto bodem právě jedna rovnoběžka Q s přímkou P. Nyní dokážeme, že $|Q| = n$.

Pro každý bod $a_i \in P$ existuje podle (1) právě jedna přímka R_i taková, že $\{a_i, b\} \subseteq R_i$. Pro $a_i \neq a_j$ je zřejmě $R_i \neq R_j$. (Kdyby totiž $R_i = R_j$, ležely by body a_i, a_j, b na téže přímce, avšak a_i, a_j určují přímku P a $b \notin P$.)

Zvolme $a_i \in P$ libovolně. Podle (2) prochází každým bodem $a_j \in P$, $a_j \neq a_i$, právě jedna přímka disjunktní s R_i. Označme tuto přímku S_j. Kdyby byly přímky S_j a Q rovnoběžné, musela by se přímka S_j rovnat přímce P, protože bodem a_j prochází jediná rovnoběžka s Q. To by však znamenalo, že $a_i \in R_i \cap S_j$, což je spor s předpokladem.

Přímka S_j proto protne přímku Q v jednom bodě s_j různém od b (neboť $S_j \cap R_j = \{a_j\}$). Pro $j \neq k$ přitom zřejmě platí $s_j \neq s_k$. Na přímce Q tak leží body b, s_j, $j \neq i$. Přitom je zřejmé, že na Q nemůže ležet žádný další bod. (Předpokládejme totiž, že existuje na Q další bod c. Podle (2) existuje přímka C tak, že $c \in C$, $C \cap R_i = \emptyset$, tj. $C \neq Q$, neboť $b \in Q \cap R_i$. Je-li $c \neq s_j$, je $C \neq S_j$. Pak ale C protne přímku P v bodě různém od a_i pro všechna i, což je spor.)

Dokázali jsme tak, že $|Q| = n$.

II. Nechť nyní A, B jsou dvě různé přímky, které nejsou rovnoběžné. Připusťme, že A je tvořena n body $a_1, \dots, a_n$ a na B leží navzájem různé body $b_1, \dots, b_{n+1}$. Zvolme označení tak, že průsečík přímek A, B je $a_1 = b_1$. Podle definice bodem b_{n+1} prochází rovnoběžka C s přímkou A. Tato rovnoběžka má podle první části důkazu n bodů; označme je $c_1, \dots, c_n = b_{n+1}$.

Označme S_1 přímku procházející body b_1, c_1 a zvolme na B libovolný bod $b_i \neq b_1$. Tímto bodem prochází jediná rovnoběžka S_i s přímkou S_1. Tato rovnoběžka nutně protne přímky A, B. Kdyby totiž byly například přímky A a S_i rovnoběžné, procházely by bodem a_1 dvě rovnoběžky s přímkou S_i, a to přímky A a S_1.

Označme $S_i \cap A = a_i^\star$, $S_i \cap B = b_i^\star$. Pro $i \neq j$ však podle tvrzení 10.19 platí $a_i^\star \neq a_j^\star$, $b_i^\star \neq b_j^\star$. To však není možné, neboť na přímce B je víc bodů než na přímkách A a C.

Přímky A, B tedy musí obsahovat stejný počet bodů. •

10.21. Definice. *Řádem* konečné afinní roviny rozumíme počet bodů ležících na přímkách v této rovině.

Snadno lze dokázat následující tvrzení.

10.22. Věta. *Konečná afinní rovina řádu n má n^2 bodů a $n^2 + n$ přímek. Na každé přímce leží n bodů a každým bodem prochází $n + 1$ přímek. Všechny přímky lze rozdělit do $n + 1$ směrů a každý směr obsahuje n rovnoběžek.*

Nyní je ovšem přirozená otázka, zda nějaká afinní konečná rovina vůbec existuje.

První směr	I	1	2	3	4
	II	5	7	6	8
	III	10	11	9	12
	IV	15	14	16	13
Druhý směr	V	13	1	5	9
	VI	14	10	2	6
	VII	11	15	7	3
	VIII	4	8	12	16
Třetí směr	IX	6	16	1	11
	X	12	5	15	2
	XI	8	9	3	14
	XII	13	4	10	7
Čtvrtý směr	XIII	7	12	14	1
	XIV	2	13	8	11
	XV	16	3	10	5
	XVI	9	6	4	15
Pátý směr	XVII	1	8	10	15
	XVIII	2	7	9	16
	XIX	3	6	12	13
	XX	4	5	11	14

Tab. 10.4: Konečná afinní rovina 4. řádu

10.23. Příklad. V tabulce 10.4 je popsána konečná afinní rovina 4. řádu. Podle věty 10.22 musí obsahovat 16 bodů (jsou označeny arabskými číslicemi) a 20 přímek (jsou označeny římskými číslicemi). Každý z pěti směrů obsahuje čtyři přímky.

10.24. Poznámka. Sportovně založený čtenář může postřehnout, že afinní rovina 4. řádu uvedená v tabulce 10.4 je rozpisem rozjížděk při klasické ploché dráze, kdy 16 jezdců absolvuje 20 rozjížděk tak, že každý jezdec jede s každým právě v jedné rozjížďce.

Tabulka 10.4 je důkazem, že konečné afinní roviny vskutku existují. Tím však vůbec není zodpovězena otázka, zda existuje konečná afinní rovina libovolného řádu $n \in \mathbb{N}$. Alespoň částečnou odpověď na tuto otázku nám dává teorie latinských čtverců.

Jak latinské čtverce souvisejí s afinními rovinami si ukážeme na rovině uvedené v tabulce 10.4. (Porovnej následující konstrukci s definicí 3–sítě v poznámce 10.12.)

Seřaďme nejprve 16 bodů dané roviny do následující tabulky:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Na první pohled je vidět, že řádky v této tabulce jsou přímky 1. směru a sloupce přímky 2. směru v dané rovině. Nyní si ukážeme, jak lze zapsat přímky dalších tří směrů.

Uvažujme 3. směr, tj. přímky IX – XII. V uvedené čtvercové tabulce pak na místa bodů první z těchto přímek, tj. přímky číslo IX, vepišme číslo 1. (Tj. nahradíme jedničkou čísla 1,6,11,16.) Podobně cifrou 2 nahradíme body přímky číslo X (tj. vepíšeme dvojku místo čísel 2,5,12,15). Když tuto úpravu provedeme analogicky i pro přímky číslo XI a XII, obdržíme čtverec

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Nyní si uvědomme, že jsme zákonitě obdrželi latinský čtverec 4. řádu. Vzhledem k tomu, že přímky 3. směru se neprotínají (jsou to rovnoběžky), nemůže se stát, aby jedno a totéž místo mělo být obsazeno různými ciframi.

Protože každá přímka 3. směru protne každou přímku 1. směru (zapsanou v některém řádku čtvercové tabulky) právě jednou a rovněž každou přímku 2. směru (zapsanou v některém sloupci) protne právě v jednom bodě, je v každém řádku a každém sloupci vzniklého čtverce opravdu permutace čísel 1, 2, 3, 4, takže vzniklý čtverec je nutně latinský.

Když nyní provedeme analogickou úvahu i pro přímky 4. a 5. směru, obdržíme latinské čtverce

$$\begin{matrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{matrix} \qquad \text{a} \qquad \begin{matrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{matrix}$$

Popsaným způsobem jsme pomocí roviny 4. řádu sestrojili tři latinské čtverce 4. řádu. Jak se čtenář může snadno přesvědčit, jsou každé dva z těchto čtverců vzájemně ortogonální. Současně je snadné si uvědomit, že ortogonalita těchto čtverců je zákonitá.

Popsanou konstrukci však nyní můžeme snadno obrátit. Budou-li dány libovolné tři vzájemně ortogonální latinské čtverce 4. řádu, sestrojíme z nich zpětně snadno afinní rovinu 4. řádu.

Uvedenou úvahu můžeme zcela analogicky provést pro každé přirozené n a tak dokázat následující tvrzení.

10.25. Věta. *Konečná afinní rovina řádu $n \geq 3$ existuje právě tehdy, když existuje $n-1$ latinských čtverců n-tého řádu, z nichž každé dva jsou ortogonální.*

Jak jsme již uvedli, neexistují ani dva ortogonální latinské čtverce 6. řádu. Proto z věty 10.25 okamžitě plyne

10.26. Důsledek. *Neexistuje konečná afinní rovina 6. řádu.*

(Kdyby sportovní činovníci znali tento výsledek, pravděpodobně by nikdy nevznikla tzv. „dlouhá plochá dráha“, při níž jezdí v jedné rozjížďce 6 jezdců. Pro tuto soutěž podle důsledku 10.26 nelze sestrojit analogický „spravedlivý“ rozpis jako pro klasickou plochou dráhu.)

10.27. Poznámka. Dodnes není obecně známo, pro která n konečná afinní rovina n-tého řádu existuje. Jsou známy jen některé dílčí výsledky. Tak například metodami analytické geometrie lze odvodit tvrzení:

Je-li $n = p^k$, kde p je prvočíslo a k přirozené číslo, pak existuje konečná afinní rovina řádu n.

Podstatně komplikovanější je důkaz následujícího tvrzení:

Nechť číslo n není součtem čtverců dvou přirozených čísel a nechť $n \equiv 1 (mod\ 4)$ nebo $n \equiv 2 (mod\ 4)$. Pak neexistuje afinní rovina řádu n.

Podle uvedeného tvrzení neexistuje například afinní rovina 14. řádu. Je však řada případů, kdy pro dané n neumíme rozhodnout, zda afinní rovina řádu n existuje. Nejmenším takovým číslem je $n = 10$.

Ke konstrukci afinní roviny 10. řádu bychom potřebovali mít k dispozici 9 vzájemně ortogonálních latinských čtverců 10. řádu. Podle příkladu 10.16 dva ortogonální latinské čtverce 10. řádu existují. Ani pomocí počítačů však dodnes nebyla nalezena ani jedna trojice vzájemně ortogonálních latinských čtverců 10. řádu. Existence afinní roviny 10. řádu tak dodnes nebyla ani dokázána ani vyvrácena. Pro velkou obtížnost tohoto problému se mu často říká matematický „problém století", i když mnohé jiné problémy jsou známější a populárnější.

Kromě konečných afinních rovin jsou intenzivně studovány i konečné *projektivní* roviny, jejichž definice je v některých rysech obdobná.

10.28. Definice. Buď $A \neq \emptyset$ konečná množina (její prvky budeme opět nazývat *body*), a množina $\mathcal{R} \subseteq \mathcal{P}(A)$ (její body budeme opět nazývat *přímky*). Nechť platí:

(1) Pro každé $x, y \in A$, $x \neq y$, existuje právě jedna množina $P \in \mathcal{R}$ tak, že $\{x, y\} \subseteq P$.

(2) Každé dvě různé přímky se protínají v jediném bodě.

(3) Existují čtyři navzájem různé prvky, z nichž žádné tři neleží na téže přímce.

Pak se dvojice $(A, \mathcal{R})$ nazývá *konečná projektivní rovina.*

Základní vlastnosti projektivních rovin se odvíjejí od následujícího tvrzení, jehož důkaz je elementární a proto jej přenecháme čtenáři.

10.29. Věta. *V konečné projektivní rovině existují čtyři navzájem různé přímky, z nichž žádné tři se neprotínají v témže bodě.*

Z definice 10.28 a z věty 10.29 plyne základní vlastnost projektivních rovin, tzv. *princip duality*:

10.30. Věta. *Každé tvrzení v teorii konečných projektivních rovin zůstane v platnosti, když v něm vzájemně zaměníme pojmy bod a přímka.*

Snadné je odvodit i následující tvrzení.

10.31. Věta. *V každé projektivní rovině platí:*

(1) *všechny přímky mají stejný počet bodů;*

(2) *každým bodem prochází stejný počet přímek;*

(3) *počet bodů na přímkách je stejný jako počet přímek procházejících jednotlivými body.*

Má tedy smysl následující definice.

10.32. Definice. Nechť každá přímka konečné projektivní roviny obsahuje $n + 1$ bodů. Pak se číslo n nazývá *řád* dané roviny.

Z věty 10.31 a z definice 10.32 je zřejmé následující tvrzení.

10.33. Věta. *Konečná projektivní rovina řádu n má $n^2 + n + 1$ bodů a $n^2 + n + 1$ přímek.*

10.34. Poznámka. Konečná projektivní rovina 2. řádu by měla, pokud existuje, obsahovat 7 bodů a 7 přímek. Čtenář snadno ověří, že takovou rovinou je například Steinerův systém trojic pro $n = 7$ v příkladu 10.8.

Odpověď na otázku, pro která n existuje konečná projektivní rovina tohoto řádu je stejná jako u afinních rovin: *konečná projektivní rovina n-tého řádu existuje právě tehdy, když existuje $n - 1$ navzájem ortogonálních latinských čtverců řádu n.*

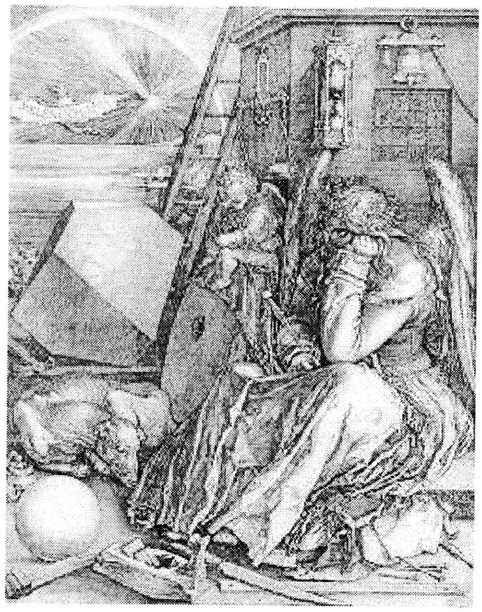
Poznámky a cvičení

1. Zkonstruujte dva latinské čtverce pátého řádu, které mají shodný právě jeden řádek.

2. Dokažte, že mezi latinskými čtverci řádu n jich může existovat nejvýše $n - 1$ navzájem ortogonálních.

3. Existuje zajímavá souvislost latinských čtverců se čtverci *magickými*, o nichž jsme se již několikrát zmínili.

Připomeňme, že *magickým čtvercem řádu n* rozumíme tabulku o n řádcích a n sloupcích, do níž jsou zapsána čísla $1, 2, \dots, n^2$ tak, že součet čísel ve všech řádcích, sloupcích a obou diagonálách je stejný. Snadno



Obr. 10.6: Dürerův obraz *Melancolia*

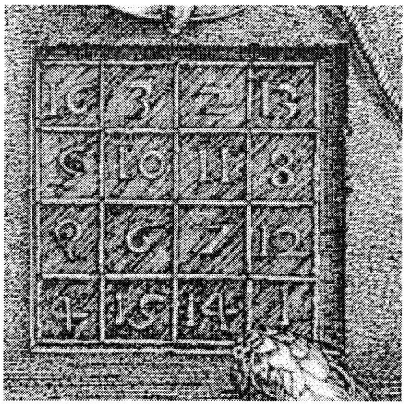
se ukáže, že uvedený součet v tomto případě musí být $\dfrac{n \cdot (n^2+1)}{2}$. Vynecháme-li požadavek, aby daný součet byl v diagonálách, dostaneme definici tzv. *polomagického čtverce.*

Není divu, že magické čtverce přitahovaly svými fascinujícími vlastnostmi lidi již před mnoha staletími. Již v úvodním paragrafu jsme se zmínili o magickém čtverci nazývaném *Saturn*, který vznikne přepsáním konfigurace *Lo-šu* (viz obrázek 1.1).

Magické čtverce se objevovaly například i ve výtvarném umění. Uveďme za mnohé obraz Albrechta Dürera *Melancolia* (viz obrázek 10.6; na obrázku 10.7 je detail magického čtverce).

Již ve 13. století popsal čínský matematik Jang-Hui řadu konstrukcí magických čtverců 3. až 10. řádu. Řada těchto konstrukcí byla velmi důmyslná. Uveďme na ukázku například konstrukci magického čtverce 9. řádu, nazývaného *Veliký Lo-šu.*

Očíslujme řádky a sloupce čtverce Lo-šu čísly 0, 1, 2. Dostaneme tak



Obr. 10.7: Detail Dürerova obrazu *Melancolia*

	0	1	2
0	4	9	2
1	3	5	7
2	8	1	6

Označme číslo v i-tém řádku a j-tém sloupci tohoto čtverce symbolem $L(i, j)$, (takže například $L(1, 2) = 7$). Čtverec „Veliký Lo-šu" dostaneme tak, že při analogickém očíslování jeho řádků a sloupců čísly $0, 1, 2, \ldots, 8$ jsou jeho prvky $G(i, j)$ vytvořeny podle pravidla:

$$G(3a + b, 3c + d) = L(a, c) + 9 \cdot [L(b, d) - 1], \quad a, b, c, d = 0, 1, 2.$$

Např.:

$$G(7, 2) = L(2, 0) + 9 \cdot [L(1, 2) - 1] = 8 + 9 \cdot (7 - 1) = 62$$

Dostaneme tak

	0	1	2	3	4	5	6	7	8
0	31	76	13	36	81	18	29	74	11
1	22	40	58	27	45	63	20	38	56
2	67	4	49	72	9	54	65	2	47
3	30	75	12	32	77	14	34	79	16
4	21	39	57	23	41	59	25	43	61
5	66	3	48	68	5	50	70	7	52
6	35	80	17	28	73	10	33	78	15
7	26	44	62	19	37	55	24	42	60
8	71	8	53	64	1	46	69	6	51

Jiný zajímavý magický čtverec zkonstruoval známý vědec a politik Benjamin Franklin. Je to čtverec 8. řádu

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

Tento čtverec je tzv. *supermagický*: když ho rozdělíme na 4 bloky o 4 řádcích a 4 sloupcích, je každý z těchto bloků *pseudomagický*: součet každého řádku a každého sloupce v těchto blocích je 130, avšak jednotlivé bloky nejsou složeny z čísel 1,2, . . . , 16.

Intenzívně se magickými čtverci zabýval v 18. století Euler. Slavný se stal jeho magický čtverec 8. řádu

1	48	31	50	33	16	63	18
30	51	46	3	62	19	14	35
47	2	49	32	15	34	17	64
52	29	4	45	20	61	36	13
5	44	25	56	9	40	21	60
28	53	8	41	24	57	12	37
43	6	55	26	39	10	59	22
54	27	42	7	58	23	38	11

Tento čtverec totiž, kromě toho, že je magický, ukazuje postup šachového koně, který přeskáče celou šachovnici (když z pole n skáče na pole $n+1$). (Srovnej s příkladem 6.10 ve 2. kapitole.)

Euler také odvodil mimořádně zajímavou souvislost mezi magickými a latinskými čtverci.

Často je mu připisována následující konstrukce magických čtverců **lichého** řádu, kterou však již v 17. století popsal francouzský velvyslanec v tehdejším Siamu S. de la Loubére. Tato konstrukce čtverce n-tého řádu pro liché n je následující.

Vepíšeme číslo 1 doprostřed prvního řádku. Máme-li již vepsáno číslo n, napíšeme číslo $n+1$ o jeden řádek výš a jeden sloupec doprava, přičemž „nad" prvním řádkem je poslední řádek a „vpravo" od posledního sloupce je první sloupec. Pokud je číslo $n + 1$ již obsazeno, napíšeme $n + 1$ **pod** číslo n.

Ilustrujme to na příkladu čtverce 5. řádu. Předepsaným postupem dostáváme

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

Euler ukázal, že když v takto vzniklém magickém čtverci n-tého řádu odečteme od každého čísla jedničku a výsledek vyjádříme nikoliv dekadicky, ale v soustavě o základu n (přičemž číslo 1 napíšeme jako 01, 2 jako 02 atd.), dostaneme popis ortogonálních latinských čtverců n-tého řádu.

Tak například z výše uvedeného magického čtverce dostaneme (neboť 16 dekadicky je 31 v pětkové soustavě apod.)

31	43	00	12	24
42	04	11	23	30
03	10	22	34	41
14	21	33	40	02
20	32	44	01	13

Uvedeným postupem lze tedy sestrojit ortogonální latinské čtverce pro každé liché n. Tyto úvahy Eulera pravděpodobně přivedly k formulaci úlohy o 36 důstojnících.

Dodatek 1: Biografie

V tomto dodatku uvádíme základní biografické údaje osobností, které jsou v textu zmíněny. Podrobnější životopisy včetně obrazových materiálů lze nalézt např. na CD-ROM [3].

d'ALEMBERT Jean Baptiste Le Rond (1717–1783)
Francouzský matematik a fyzik, osvícenský filozof, jeden z encyklopedistů.

BELL Eric Temple (1883–1960)
Americký matematik skotského původu.

BERNOULLI Jacob I. (1654–1705)
Švýcarský matematik a fyzik, první z plejády slavných Bernoulliů.

BETTI Enrico (1823–1892)
Italský matematik.

BORŮVKA Otakar (1899–1995)
Významný český matematik, profesor univerzity v Brně.

CATALAN Eugène Charles (1814–1894)
Belgický matematik.

CAYLEY Arthur (1821–1895)
Anglický matematik.

DESCARTES René (latinsky Renatus CARTESIUS) (1596–1650)
Francouzský filozof, matematik, fyzik a přírodovědec, jeden ze zakladatelů novověké filozofie a vědy.

DIRICHLET Peter Gustav Lejeune (1805–1859)
Německý matematik.

DÜRER Albrecht (1471–1528)
Německý malíř a grafik.

ERDÖS Paul (1913–1996)
Maďarský matematik.

EUKLEIDÉS z Alexandrie (asi 340–270 př. Kr.)
Starořecký matematik, autor nejvýznamnější matematické knihy dosavadní historie.

EULER Leonhard (1707–1783)
Švýcarský matematik, fyzik a fyziolog, jeden z nejvýznamnějších matematiků všech dob.

FERMAT Pierre (1601–1665)
Francouzský matematik a právník.

FERRERS Norman Macleod (1829–1903)
Anglický matematik.

FIBONACCI (vl. jménem Leonardo Pisánský) (asi 1170–po 1240)
První velký matematik evropského středověku.

FRANKLIN Benjamin (1706–1790)
Americký státník, přírodovědec a filozof. Vzděláním samouk se vlastní pílí vypracoval na jednoho z předních osvícenských myslitelů.

FULKERSON Delbert Ray (1924–1976)
Americký matematik.

GALILEI Galileo (1564–1642)
Italský fyzik, astronom, matematik a filozof, zakladatel experimentálních metod zkoumání přírody, kritik scholastiky, představitel renesančního mechanistického pojetí přírody.

HALL Phillip (1904–1982)
Anglický matematik.

HAMILTON William Rowan, sir (1805–1865)
Irský matematik a astronom.

HARDY Godfrey Harold (1877–1947)
Anglický matematik, největší světový odborník v teorii čísel první poloviny 20. století.

HASSE Helmut (1898–1979)
Německý matematik.

HEAWOOD Percy John (1861–1955)
Anglický matematik.

HUYGENS Christian (1629–1695)
Nizozemský matematik a fyzik.

JANG Hui (asi 1238–asi 1298)
Čínský matematik.

KEMPE Alfred Bray (1849–1922)
Anglický matematik.

KIRCHHOFF Gustave-Robert (1824–1887)
Německý fyzik a mechanik.

KIRKMAN Thomas Penyngton (1806–1895)
Anglický kněz. Ve volných chvílích se zabýval matematikou.

KÖNIG Dénes (1884–1944)
Maďarský matematik.

KURATOWSKI Kazimierz (1896–1980)
Polský matematik.

LAPLACE Pierre Simon (1749–1827)
Francouzský matematik, fyzik a astronom.

LEIBNIZ Gottfried Wilhelm von (1646–1716)
Německý matematik, filozof, právník, historik, jazykovědec, diplomat, vynálezce a polyhistor, zakladatel moderní matematické analýzy.

LUCAS Francois Edouard Anatole (1842–1891)
Francouzský matematik.

MacMAHON Percy Alexander (1854–1929)
Anglický matematik.

MENGER Karl (1902–1985)
Rakousko-americký matematik.

MÖBIUS August Ferdinand (1790–1869)
Německý matematik a astronom.

de MORGAN Augustus (1806–1909)
Skotský matematik a logik.

NETTO Eugen Otto Erwin (1848–1919)
Německý matematik.

ORE Oystein (1899–1968)
Americký matematik norského původu.

OZANAM Jacques (1640–1717)
Francouzský matematik, chemik a teolog.

PARKER Ernest Tilden (1926–1991)
Americký matematik.

PASCAL Blaise (1623–1662)
Francouzský matematik, fyzik a filozof.

PETERSEN Julius Peter Christian (1839–1910)
Dánský matematik.

PLATÓN (427–347 př. Kr.)
Starořecký filozof, jeden z největších antických myslitelů.

PÓLYA Gyergy (1887–1985)
Maďarský matematik.

RADEMACHER Hans (1892–1969)
Německý matematik.

RAMANUJAN Srinivasa Aaiangar (1887–1920)
Indický matematik.

ROTA Gian-Carlo (1932–1999)
Americký matematik italského původu.

SCHLÄFLI Ludwig (1814–1895)
Švýcarský matematik.

STEINER Jacob (1796–1863)
Německý matematik.

STIFEL Michael (1487–1567)
Německý matematik.

STIRLING James (1692–1770)
Skotský matematik.

TAIT Peter Guthrie (1831–1901)
Skotský matematik a filozof.

TARRY Gaston (1843–1913)
Francouzský matematik–amatér.

TARSKI Alfred (1901–1977)
Americký matematik a logik polského původu.

YOUNG John Wesley (1879–1932)
Americký matematik.

DODATEK 2: TABULKY

$n!$	n
1	1
2	2
6	3
24	4
120	5
720	6
5 040	7
40 320	8
362 880	9
3 628 800	10
39 916 800	11
479 001 600	12
6 227 020 800	13
87 178 291 200	14
1 307 674 368 000	15
	⋮
2 432 902 008 176 640 000	20
	⋮
15 511 210 043 330 985 984 000 000	25

Tab. 1.1: Tabulka hodnot n !

$\binom{n}{k}$	$k=0$	1	2	3	4	5	6	7	8	9	10
$n=0$	1	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0
2	1	2	1	0	0	0	0	0	0	0	0
3	1	3	3	1	0	0	0	0	0	0	0
4	1	4	6	4	1	0	0	0	0	0	0
5	1	5	10	10	5	1	0	0	0	0	0
6	1	6	15	20	15	6	1	0	0	0	0
7	1	7	21	35	35	21	7	1	0	0	0
8	1	8	28	56	70	56	28	8	1	0	0
9	1	9	36	84	126	126	84	36	9	0	0
10	1	10	45	120	210	252	210	120	45	10	1
$\vdots$											

Tab. 1.2: Pascalův trojúhelník

$p(n,k)$	$n=1$	2	3	4	5	6	7	8	9	10
$k=1$	1	1	1	1	1	1	1	1	1	1
2	0	1	1	2	2	3	3	4	4	5
3	0	0	1	1	2	3	4	5	7	8
4	0	0	0	1	1	2	3	5	6	9
5	0	0	0	0	1	1	2	3	5	7
6	0	0	0	0	0	1	1	2	3	5
7	0	0	0	0	0	0	1	1	2	3
8	0	0	0	0	0	0	0	1	1	2
9	0	0	0	0	0	0	0	0	1	1
10	0	0	0	0	0	0	0	0	0	1
$\vdots$										

Tab. 1.3: Počet $p(n,k)$ rozkladů čísla n na k sčítanců

n	$p(n)$	n	$p(n)$	n	$p(n)$	n	$p(n)$
1	1	21	792	41	44 583	...	
2	2	22	1 002	42	53 174	70	4 087 968
3	3	23	1 255	43	63 261	...	
4	5	24	1 575	44	75 175	80	15 796 476
5	7	25	1 958	45	89 134	...	
6	11	26	2 436	46	105 558	90	56 634 173
7	15	27	3 010	47	124 754	...	
8	22	28	3 718	48	147 273	100	190 569 292
9	30	29	4 565	49	173 525	...	
10	42	30	5 604	50	204 226	110	607 163 746
11	56	31	6 842	51	239 943	...	
12	77	32	8 349	52	281 589	120	1 844 349 560
13	101	33	10 143	53	329 931	...	
14	135	34	12 310	54	386 155	125	3 163 127 352
15	176	35	14 833	55	451 276	...	
16	231	36	17 977	56	526 823	200	3 972 999 029 388
17	297	37	21 637	57	614 154		
18	385	38	26 015	58	715 220		
19	490	39	31 185	59	831 820		
20	627	40	37 338	60	966 467		

Tab. 1.4: Počet $p(n)$ rozkladů čísla n

$s(n,k)$	$k=0$	1	2	3	4	5	6
$n=1$	0	1	0	0	0	0	0
2	0	-1	1	0	0	0	0
3	0	2	-3	1	0	0	0
4	0	-6	11	-6	1	0	0
5	0	24	-50	35	-10	1	0
6	0	-120	274	-225	85	-15	1
$\vdots$							

Tab. 1.5: Tabulka hodnot Stirlingových čísel prvního druhu

$S(n,k)$	$k=1$	2	3	4	5	6	7	8	9	10
$n=1$	1	0	0	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0	0
3	1	3	1	0	0	0	0	0	0	0
4	1	7	6	1	0	0	0	0	0	0
5	1	15	25	10	1	0	0	0	0	0
6	1	31	90	65	15	1	0	0	0	0
7	1	63	301	350	140	21	1	0	0	0
8	1	127	966	1701	1050	266	28	1	0	0
9	1	255	3025	7770	6951	2646	462	36	1	0
10	1	511	9330	34105	42525	22827	5580	750	45	1
$\vdots$										

Tab. 1.6: Tabulka hodnot Stirlingových čísel druhého druhu

k	b_k
2	0,166 67
4	0,033 33
6	0,023 81
8	0,033 33
10	0,075 76
12	0,253 11
14	1,166 67
16	7,092 16
18	54,971 18
20	529,124 24
22	6 192,123 19
24	86 580,253 11
26	1 425 517,166 67
28	27 298 231,067 82
30	601 580 873,900 64

Tab. 1.7: Bernoulliova čísla

n	$t(n)$	n	$t(n)$
1	1	14	3 159
2	1	15	7 741
3	1	16	19 320
4	2	17	48 629
5	3	18	123 867
6	6	19	317 955
7	12	20	823 065
8	23	21	2 144 505
9	47	22	5 623 756
10	106	23	14 828 074
11	235	24	39 299 897
12	551	25	104 636 890
13	1 301	26	279 793 450

Tab. 1.8: Počet t_n neizomorfních stromů na n uzlech

Rejstřík

LITERATURA

[1] C. BERGE: *Principles of Combinatorics,* Academic Press, New York – San Francisco – London 1971

[2] J. B. DENCE - T. P. DENCE: *Elements of the Theory of Numbers,* AcademicPress, London 1998

[3] E. FUCHS: *Diskrétní matematika a teorie množin pro učitele,* CD-ROM, Brno 2000

[4] E. FUCHS: *Teorie množin pro učitele,* Brno 2000

[5] J. E. GRAVER, M. E. WATKINS: *Combinatorics with Emphasis on the Theory of Graphs,* Springer - Verlag, New York – Heidelberg – Berlin 1977

[6] M. HALL, JR.: *Combinatorial Theory,* Blaisdel P.C., Waltham – Toronto – London 1967; ruský překlad 1970

[7] J. HERMAN, R. KUČERA, J. ŠIMŠA: *Metody řešení matematických úloh II,* Brno 1997

[8] J. KAUCKÝ: *Kombinatorické identity,* Veda, Bratislava 1975

[9] J. NEČAS: *Grafy a jejich použití,* SNTL, Praha 1978

[10] R. MERRIS: *Combinatorics,* PWS Publishing Company, Boston – London – Tokyo 1996

[11] J. NEŠETŘIL: *Teorie grafů,* SNTL, Praha 1979

[12] J. SEDLÁČEK: *Úvod do teorie grafů,* Academia, Praha 1981

[13] P. ŠIŠMA: *Teorie grafů 1736–1963,* Prometheus, Praha 1997

[14] N. J. VILENKIN: *Kombinatorika,* SNTL, Praha – Moskva 1977