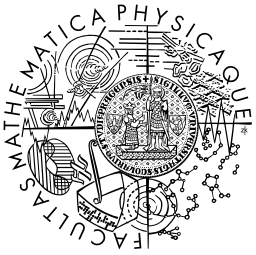


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

DIPLOMOVÁ PRÁCE

Jindřich Michalik

Kombinatorické posloupnosti čísel a dělitelnost

Katedra didaktiky matematiky

Vedoucí diplomové práce:	doc. RNDr. Antonín Slavík, Ph.D.
Studijní program:	Matematika
Studijní obor:	Učitelství matematiky – deskriptivní geometrie pro střední školy (MDUSSS)

Praha 2018

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

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

V ..... dne ..... Podpis autora

Název práce: Kombinatorické posloupnosti čísel a dělitelnost

Autor: Jindřich Michalik

Katedra: Katedra didaktiky matematiky

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

Abstrakt: Práce obsahuje přehled výsledků o číselně teoretických vlastnostech některých významných kombinatorických posloupností, konkrétně faktoriálů, kombinačních čísel, Fibonacciho a Catalanových čísel. Je zkoumána např. parita, prvočíselnost, dělitelnost mocninami prvočísel, nesoudělnost apod. Práce by měla být z velké části srozumitelná nadaným středoškolským studentům, výsledky jsou ilustrovány na příkladech.

Klíčová slova: kombinatorika, posloupnost, dělitelnost, faktoriál, kombinační číslo, Fibonacciho čísla, Catalanova čísla, Lucasova věta, Legendreův vzorec, Kummerova věta

Title: Combinatorial sequences and divisibility

Author: Jindřich Michalik

Department: Department of Mathematics Education

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

Abstract: This work contains an overview of the results concerning number-theoretic properties of some significant combinatorial sequences such as factorials, binomial coefficients, Fibonacci and Catalan numbers. These properties include parity, primality, prime power divisibility, coprimality etc. A substantial part of the text should be accessible to gifted high school students, the results are illustrated with examples.

Keywords: combinatorics, sequence, divisibility, factorial, binomial coefficient, Fibonacci numbers, Catalan numbers, Lucas' Theorem, Legendre's formula, Kummer's theorem

Děkuji doc. RNDr. Antonínu Slavíkovi, Ph.D. za odborné vedení, poskytnutí vhodné literatury, neobyčejnou pečlivost a vytrvalost.

Obsah

1 Úvod **2**

2 Faktoriál **3**
2.1 Definice faktoriálu 3
2.2 Dělitelé faktoriálu 3
2.3 Dělitelé faktoriálu: odhady a důsledky 7

3 Kombinační číslo **9**
3.1 Zavedení kombinačních čísel 9
3.2 Kombinatorické identity 9
3.3 Parita čísel v Pascalově trojúhelníku 10
3.4 Lucasova věta 13
3.5 Pascalův trojúhelník modulo 2 17
3.6 Kummerova věta 18
3.7 Kdy je kombinační číslo mocninou? 23

4 Fibonacciho čísla **25**
4.1 Rekurentní vzorec 25
4.2 Dělitelnost Fibonacciho čísel 26
4.3 Dláždění 27
4.4 Největší společný dělitel Fibonacciho čísel 31

5 Catalanova čísla **34**
5.1 Úvodní příklad 34
5.2 Rekurentní vzorec 36
5.3 Parita a prvočíselnost Catalanových čísel 38
5.4 Dělitelé Catalanových čísel 40

Seznam obrázků **45**

Seznam tabulek **46**

Literatura **47**

1. Úvod

Tato diplomová práce si klade za cíl sestavit přehled výsledků o číselně teoretických vlastnostech některých významných kombinatorických posloupností týkajících se dělitelnosti. Takovými vlastnostmi rozumíme např. prvočíselnost, lichost a sudost nebo obecněji dělitelnost daným prvočíslem, v návaznosti i dělitelnost danou mocninou daného prvočísla, nesoudělnost a podobně. V každé kapitole je použití odvozených vlastností ilustrováno na příkladech.

V kapitole 2 začínáme se základní posloupností kombinatoriky, posloupností faktoriálů. Pro $n \geq 3$ je faktorálem $n! = 1 \cdot 2 \cdot \ldots n$ zřejmě složené číslo, proto začínáme velmi rychle s vyšetřováním, jaká největší mocnina daného prvočísla p je dělitelem $n!$. Výsledkem je tzv. Legendreův vzorec (2.2.7), na který se mnohokrát odkazujeme v průběhu práce při dokazování nových vět nebo při řešení příkladů.

Kapitola 3 pojednává o kombinačních číslech. Často pracujeme s Pascalovým trojúhelníkem pro lepší představu o významu některých odvozených výsledků. Nejdříve se zabýváme lichostí/sudostí kombinačních čísel. Na získané výsledky navazuje Lucasova věta 3.4.7, díky které můžeme snadno zjistit zbytek po dělení daného kombinačního čísla $\binom{n}{k}$ daným prvočíslem p. Zajímavé je uspořádání sudých a lichých čísel v Pascalově trojúhelníku, o čemž pojednává sekce 3.5. Zjišťujeme, že při barevném odlišení pozic podle parity čísel, která se v Pascalově trojúhelníku nacházejí, získáme obrázek připomínající známý fraktál.

Dále v kapitole 3 zjišťujeme, jaká největší mocnina daného prvočísla p dělí dané kombinační číslo. Elegantní odpověď na tuto otázku dává Kummerova věta 3.6.2, z níž pramení mnoho důsledků a využijeme ji i v příkladech v kapitole 5. V závěru kapitoly se dozvíme, že kombinační číslo je zřídkakdy mocninou prvočísla.

Kapitola 4 pojednává o Fibonacciho číslech, pravděpodobně nejpopulárnější kombinatorické posloupnosti. Přestože se dají najít souvislosti mezi Fibonacciho čísly a kombinačními čísly např. v Pascalově trojúhelníku, lze tuto kapitolu číst samostatně a bez znalostí z přechozích dvou kapitol. Zabýváme se soudělností Fibonacciho čísel a kombinatoricky odvozujeme, že pro $n, m \geq 1$ je m-té Fibonacciho číslo F_m dělitelem $F_{m \cdot n}$. V návaznosti na tento výsledek odvozujeme větu, která výrazně usnadňuje určení největšího společného dělitele Fibonacciho čísel.

Poslední kapitola je věnována posloupnosti Catalanových čísel. Přes různá kombinatorická odvození se dostaneme jak k definici n-tého Catalanova čísla C_n pomocí kombinačního čísla, tak k rekurentnímu vzorci. Dále se zabýváme paritou a prvočíselností Catalanových čísel a zjišťujeme, že Catalanových prvočísel je konečný počet. V sekci 5.4 popisujeme dělitelnost C_n různými prvočísly. Výsledky přebíráme z článku [2] bez důkazů kvůli jejich rozsahu; přínos sekce 5.4 spočívá ve zpřehlednění těchto výsledků. Na závěr kapitoly zjišťujeme, jakou největší mocninou dvojky je dělitelné dané Catalanovo číslo a vylepšujeme výsledek z [2] pro dělitelnost číslem 3.

Od čtenáře očekáváme znalosti středoškolské matematiky. Mnoho důkazů a řešení příkladů využívá zápis čísel v různých číselných soustavách (nebo obecně v soustavě o základu daného prvočísla p), některé vyžadují práci se zbytky po dělení daným prvočíslem v podobě kongruencí.

2. Faktoriál

2.1 Definice faktoriálu

Na úvod kapitoly připomeneme definici faktoriálu pro přirozená čísla, tj.

$$n! = \prod_{k=1}^{n} k. \tag{2.1.1}$$

Faktoriál hraje v kombinatorice důležitou roli, neboť $n!$ je počet permutací n-prvkové množiny. Prvních deset faktoriálů přirozených čísel udává tabulka 2.1.

Pro některé účely se hodí dodefinovat hodnotu faktoriálu i pro $n = 0$ vztahem $0! = 1$. O užitečnosti této definice se přesvědčíme v navazujících kapitolách. V této kapitole budeme vycházet z knihy [7].

2.2 Dělitelé faktoriálu

Přistupme nyní ke zkoumání dělitelnosti faktoriálů. Z definice je ihned zřejmé, že každé přirozené číslo $k \leq n$ je dělitelem $n!$. Zamysleme se nyní, jak by vypadal prvočíselný rozklad čísla $n!$. Obecně je to součin

$$n! = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \ldots \cdot p_t^{k_t} = \prod_{i=1}^{t} p_i^{k_i}, \tag{2.2.1}$$

kde p_i jsou různá prvočísla a k_i příslušné exponenty pro každý index i.

Pro libovolné prvočíslo $p \leq n$ chceme zjistit, jaká největší mocnina p je dělitelem $n!$. Hledaný exponent budeme značit $\epsilon_p(n!)$.

Uveďme jednoduchý příklad:

Nechť je dáno $n = 10$ a $p = 2$. Chceme najít číslo $\epsilon_p(n!) = \epsilon_2(10!)$, tedy exponent u dvojky v prvočíselném rozkladu čísla 10!.

Jelikož je 10! podle definice součinem čísel $1, \ldots, 10$, můžeme najít $\epsilon_2(10!)$ tak, že posčítáme exponenty nejvyšších mocnin dvojky, které dělí čísla $1, \ldots, 10$. Tedy u každého z těchto deseti čísel zjistíme, kolik dvojek se nachází v jeho prvočíselném rozkladu. Tímto postupem získáme tabulku 2.2.

Zjišťujeme, že celkový počet dvojek v prvočíselných rozkladech všech deseti čísel dohromady je $1 + 2 + 1 + 3 + 1 = 8$. Tudíž 2^8 dělí 10!, ale 2^9 už ne.

Ke stejnému závěru bychom však mohli dojít trochu odlišným postupem. Místo sledování, kolika dvojkami přispěje každý sloupec tabulky do výsledného součtu, se nyní podívejme na to, kolika dvojkami přispěje každý řádek. Začneme tím, že zjistíme, kolik z daných deseti čísel je dělitelných dvěma, a zapíšeme počet na konec řádku. Poté zjistíme, kolik z daných čísel je dělitelných čtyřmi, a opět zapíšeme do tabulky. Takto postupujeme dále po mocninách dvojky, dokud je

n	1	2	3	4	5	6	7	8	9	10
$n!$	1	2	6	24	120	720	5 040	40 320	362 880	3 628 800

Tabulka 2.1: Tabulka faktoriálů pro malá n

	1	2	3	4	5	6	7	8	9	10
dělitelné 2		X		X		X		X		X
dělitelné 4				X				X		
dělitelné 8								X		
dvojek celkem	0	1	0	2	0	1	0	3	0	1

Tabulka 2.2: Výpočet $\epsilon_2(10!)$ po sloupcích

počet větší než 0 (tedy v tomto případě do dělitelnosti číslem 8). Tímto způsobem vznikne poslední sloupec tabulky 2.3.

	1	2	3	4	5	6	7	8	9	10	počet dvojek
dělitelné 2		X		X		X		X		X	$5 = \lfloor\ 10/2\ \rfloor$
dělitelné 4				X				X			$2 = \lfloor\ 10/4\ \rfloor$
dělitelné 8								X			$1 = \lfloor\ 10/8\ \rfloor$
součet											8

Tabulka 2.3: Výpočet $\epsilon_2(10!)$ po řádcích

Připomínáme, že $\lfloor x \rfloor$ značí dolní celou část čísla x. Do prvního řádku posledního sloupce tabulky 2.3 zapisujeme počet čísel dělitelných dvěma. Takových čísel je přesně polovina, pokud je jejich počet dělitelný dvěma. Obecně je to však dolní celá část poloviny jejich počtu. Analogicky, počet čísel dělitelných čtyřmi je dolní celá část čtvrtiny jejich počtu atd.

Zjišťujeme, že

$$\epsilon_2(10!) = \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{4} \right\rfloor + \left\lfloor \frac{10}{8} \right\rfloor = 5 + 2 + 1 = 8. \tag{2.2.2}$$

Zobecněním předchozí úvahy ihned dostáváme následující větu.

Věta 2.2.1. ([7, str. 113]) *Pro libovolné přirozené n platí:*

$$\epsilon_2(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n}{8} \right\rfloor + ... = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor. \tag{2.2.3}$$

Součet (2.2.3) je vždy konečný a má nejvýše $\lfloor \log_2 n \rfloor$ nenulových členů, neboť pro $2^k > n$ je $\left\lfloor \frac{n}{2^k} \right\rfloor$ rovno nule.

Vidíme, že každý člen je dolní celou částí poloviny předchozího členu. Pro všechna n totiž platí

$$\left\lfloor \frac{n}{2^{k+1}} \right\rfloor = \left\lfloor \frac{\lfloor n/2^k \rfloor}{2} \right\rfloor. \tag{2.2.4}$$

Snadno to plyne např. ze zápisu čísel ve dvojkové soustavě, neboť dolní celá část z $n/2^k$ odpovídá posunu dvojkového zápisu o k pozic vpravo.

Například pro $n = 100$ dostáváme

$$\epsilon_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97. \tag{2.2.5}$$

Sledujme, co se při výpočtu dalších členů děje, zapíšeme-li je ve dvojkové soustavě:

$$\begin{aligned} 100 &= (1100100)_2 &&= 100 \\ \lfloor 100/2 \rfloor &= (110010)_2 &&= 50 \\ \lfloor 100/4 \rfloor &= (11001)_2 &&= 25 \\ \lfloor 100/8 \rfloor &= (1100)_2 &&= 12 \\ \lfloor 100/16 \rfloor &= (110)_2 &&= 6 \\ \lfloor 100/32 \rfloor &= (11)_2 &&= 3 \\ \lfloor 100/64 \rfloor &= (1)_2 &&= 1 \end{aligned}$$

Výpočet dolní celé části z poloviny libovolného čísla je ve dvojkové soustavě jednoduchý – stačí odebrat poslední cifru. Díky těmto vlastnostem čísel zapsaných ve dvojkové soustavě můžeme zformulovat následující větu.

Věta 2.2.2. ([7, str. 114]) *Pro libovolné přirozené n platí*

$$\epsilon_2(n!) = n - \nu_2(n), \tag{2.2.6}$$

kde $\nu_2(n)$ je počet jedniček v binární reprezentaci čísla n.

Proč tomu tak je? Uvedeme nejdříve příklad.

Číslo $100 = (1100100)_2$ je reprezentováno ve dvojkové soustavě třemi jedničkami o hodnotách 64, 32, 4. Dolní celou část poloviny čísla 100 můžeme počítat jako součet dolních celých částí těchto čísel, tedy $\lfloor \frac{100}{2} \rfloor = \lfloor \frac{64}{2} \rfloor + \lfloor \frac{32}{2} \rfloor + \lfloor \frac{4}{2} \rfloor$. Stejně postupujeme i při výpočtu dalších členů $\epsilon_2(100!)$, tedy $\lfloor \frac{100}{4} \rfloor = \lfloor \frac{64}{4} \rfloor + \lfloor \frac{32}{4} \rfloor + \lfloor \frac{4}{4} \rfloor$ atd. V řádcích tabulky 2.4 vidíme, jakou hodnotou přispěje každé z čísel 64, 32, 4, potažmo každá jednička z binárního zápisu čísla $100 = (1100100)_2$, ke konečnému součtu $\epsilon_2(100!)$.

	64	32	16	8	4	2	1	0
	32	16	8	4	2	1	0	0
	4	2	1	0	0	0	0	0
součet	**100**	50	25	12	6	3	1	0

Tabulka 2.4: Význam binárního zápisu pro dolní součty

Nyní můžeme přistoupit k důkazu věty 2.2.2.

Důkaz. Každá jednička v binárním zápisu čísla n má hodnotu 2^m, přičemž m je pozice této jedničky zprava s číslováním od nuly. Současně se však tato jednička projeví přičtením čísla $2^{m-1} + 2^{m-2} + ... + 2^0$ k hodnotě $\epsilon_2(n!)$. Platí $2^{m-1} + 2^{m-2} + ... + 2^0 = 2^m - 1$, tedy každá jednička v binárním zápisu čísla n přispěje hodnotou $2^m - 1$ k číslu $\epsilon_2(n!)$, a současně hodnotou 2^m k číslu n. Tím je rovnost (2.2.6) dokázána.

□

Zobecníme-li vztah (2.2.3) pro libovolné prvočíslo p, dostáváme tzv. Legendreův vzorec.

Věta 2.2.3. ([7, str. 114], [13, str. 9]) *Pro přirozené číslo n a prvočíslo p platí:*

$$\epsilon_p(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ... = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor . \tag{2.2.7}$$

Platnost Legendreova vzorce (2.2.7) můžeme odůvodnit stejným způsobem (tabulka 2.2), jen místo po mocninách dvojky postupujeme po mocninách prvočísla p. S pomocí Legendreova vzorce můžeme odvodit analogii vzorce (2.2.6) pro obecné prvočíslo p.

Věta 2.2.4. ([12, str. 115], [22])
Pro libovolné přirozené číslo n a prvočíslo p platí

$$\epsilon_p(n!) = \frac{n - \nu_p(n)}{p-1}, \tag{2.2.8}$$

kde $\nu_p(n)$ je ciferný součet při reprezentaci čísla n v číselné soustavě o základu p.

Důkaz.

Rozvinutý zápis čísla n v číselné soustavě o základu p je $n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$, tedy platí $\lfloor \frac{n}{p^i} \rfloor = n_k p^{k-i} + n_{k-1}p^{k-1-i} + \cdots + n_{i+1}p + n_i$. Vyjdeme-li ze vzorce (2.2.7), dostáváme postupně

$$\begin{aligned}
\epsilon_p(n!) &= \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor \\
&= \sum_{i=1}^{k} \left(n_k p^{k-i} + n_{k-1}p^{k-1-i} + \cdots + n_{i+1}p + n_i \right) \\
&= \sum_{i=1}^{k} \sum_{j=i}^{k} n_j p^{j-i} \\
&= \sum_{j=1}^{k} \sum_{i=1}^{j} n_j p^{j-i} \\
&= \sum_{j=1}^{k} n_j \cdot \frac{p^j - 1}{p-1} \\
&= \sum_{j=0}^{k} n_j \cdot \frac{p^j - 1}{p-1} \\
&= \frac{1}{p-1} \sum_{j=0}^{k} \left(n_j p^j - n_j \right) \\
&= \frac{1}{p-1} \cdot \left(n - \nu_p(n) \right),
\end{aligned} \tag{2.2.9}$$

čímž je věta dokázána.

□

Uveďme nyní příklad na použití vzorce (2.2.7).

Příklad 2.2.5. Zjistěte, kolika nulami končí číslo 100!.

Přirozené číslo n končí x nulami právě tehdy, když je dělitelné 10^x, ale ne 10^{x+1}. Jelikož se číslo 10 rozkládá na součin $2 \cdot 5$, musí být n dělitelné 2^x a současně 5^x. Nalezneme tedy největší mocninu dvojky, která dělí 100!, a největší mocninu pětky, která dělí 100!. Minimum z těchto dvou výsledků je hledané x.

$$\begin{aligned}
\epsilon_2(100!) &= \sum_{i=1}^{\infty} \left\lfloor \frac{100}{2^i} \right\rfloor \\
&= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor \\
&= 50 + 25 + 12 + 6 + 3 + 1 = 97 \\
\epsilon_5(100!) &= \sum_{i=1}^{\infty} \left\lfloor \frac{100}{5^i} \right\rfloor \\
&= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 20 + 4 = 24 \\
\min(97{,}24) &= 24
\end{aligned} \tag{2.2.10}$$

Zjistili jsme, že číslo 100! končí 24 nulami.

Zadaný příklad vyřešíme ještě jiným způsobem, a to pomocí vět 2.2.2 a 2.2.4. Opět potřebujeme zjistit hodnoty $\epsilon_2(100!)$ a $\epsilon_5(100!)$. Hodnotu $\epsilon_2(100!)$ zjistíme pomocí věty 2.2.2 (resp. už jsme ji zjistili). Po dosazení do (2.2.6) dostáváme

$$\epsilon_2(100!) = 100 - 3 = 97. \tag{2.2.11}$$

Hodnotu $\epsilon_5(100!)$ zjistíme pomocí věty 2.2.4. Ciferný součet čísla $100 = (400)_5$ při zápisu v pětkové soustavě je $\nu_5(100) = 4$. Po dosazení do (2.2.8) tedy dostáváme

$$\epsilon_5(100!) = \frac{100 - 4}{5 - 1} = 24. \tag{2.2.12}$$

Hledaným číslem je opět minimum z obou dosažených výsledků, tedy 24.

2.3 Dělitelé faktoriálu: odhady a důsledky

Jak rychle roste funkce $\epsilon_p(n!)$? Snadno můžeme dostat dobrý odhad odstraněním dolních celých částí jednotlivých členů ve vzorci (2.2.7) a sečtením nekonečné geometrické řady:

$$\begin{aligned}
\epsilon_p(n!) &< \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + ... \\
&= \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + ...\right) \\
&= \frac{n}{p}\left(\frac{p}{p-1}\right) \\
&= \frac{n}{p-1}
\end{aligned} \tag{2.3.1}$$

Pro $p = 2$ a $n = 100$ dostáváme horní odhad 100, což je celkem blízko skutečné hodnotě $\epsilon_p(n!) = 97$. Obecně roste $\epsilon_2(n!)$ srovnatelně rychle jako n. Plyne to ze vzorce (2.2.6) a z toho, že $\nu_2(n) \leq \lceil \log_2 n \rceil$ je pro velká n zanedbatelné oproti hodnotě n.

Pro $p = 2$ a $p = 3$ získáváme odhady $\epsilon_2(n!) \sim n$ a $\epsilon_3(n!) \sim n/2$, zdá se tedy logické, že by pro některá n mohlo být $\epsilon_3(n!)$ přesně poloviční oproti $\epsilon_2(n!)$. Skutečně takové případy jsou, a to například pro $n = 6$ a $n = 7$. Platí $6! = 2^4 \cdot 3^2 \cdot 5$; z prvočíselného rozkladu vidíme, že počet trojek je opravdu poloviční oproti počtu dvojek. To samé platí pro $7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. Není však dokázáno, zda je takových případů nekonečně mnoho.

Nerovnost (2.3.1) můžeme použít k odvození dalšího odhadu týkajícího se dělitelů faktoriálu. Snadno získáváme odhad pro $p^{\epsilon_p(n!)}$, což je největší mocnina p, která dělí $n!$:

$$p^{\epsilon_p(n!)} < p^{\frac{n}{p-1}} \tag{2.3.2}$$

Tuto nerovnost můžeme ještě zjednodušit (za cenu zhoršení horního odhadu), uvědomíme-li si, že pro každé reálné x platí $x \leq 2^{x-1}$; tudíž

$$p^{\epsilon_p(n!)} < p^{\frac{n}{p-1}} \leq (2^{p-1})^{\frac{n}{p-1}} = 2^n. \tag{2.3.3}$$

Odvodili jsme tedy, že největší mocnina libovolného prvočísla, která dělí $n!$, je vždy menší než 2^n.

3. Kombinační číslo

3.1 Zavedení kombinačních čísel

Na úvod kapitoly připomeneme definici kombinačního čísla. Pro nezáporné celé číslo n a nezáporné celé číslo $k \leq n$ definujeme kombinační číslo $\binom{n}{k}$ jako počet různých neuspořádaných k-tic, které lze sestavit z n různých prvků bez opakování. Pro takto definované číslo platí

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n \cdots (n-k+1)}{k!}, \tag{3.1.1}$$

a to i pro případ $n = 0$ nebo $k = 0$ díky definici $0! = 1$ z předchozí kapitoly. Pro $k > n$ definujme $\binom{n}{k} = 0$.

Všechna kombinační čísla $\binom{n}{k}$, kde $n \in \mathbb{N}_0$ a $0 \leq k \leq n$, lze uspořádat do trojúhelníkového schématu tak, že na n-tém řádku shora (s číslováním od nuly) najdeme po řadě zleva čísla $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$. Tuto strukturu nazýváme Pascalův trojúhelník (viz tabulku 3.1).

0						1							
1					1		1						
2				1		2		1					
3			1		3		3		1				
4		1		4		6		4		1			
5	1		5		10		10		5		1		
6	1	6		15		20		15		6		1	

Tabulka 3.1: Prvních 7 řádků Pascalova trojúhelníku

3.2 Kombinatorické identity

V této sekci předvedeme kombinatorické důkazy dvou identit, které budeme vzápětí potřebovat. Vycházíme převážně z kapitoly 5.2 knihy [3]. Obě identity lze snadno dokázat také přímo ze vztahu (3.1.1).

Věta 3.2.1. *Pro* $0 \leq k \leq n$ *platí*

$$k\binom{n}{k} = n\binom{n-1}{k-1}. \tag{3.2.1}$$

Důkaz. ([3, str. 75])

Kolika způsoby lze ze třídy o n studentech vybrat k-člennou komisi s určením jednoho z členů předsedou? K výsledku lze dospět dvěma způsoby, které odpovídají levé a pravé straně dokazovaného vztahu (3.2.1).

1. způsob:

Existuje $\binom{n}{k}$ způsobů, jak vybrat komisi. Potom je k možností, jak z této komise určit předsedu. Počet možností je tedy $k\binom{n}{k}$.

2. způsob:

Nejprve vybereme předsedu z n studentů. Poté ze zbývajících $n-1$ studentů vybereme $k-1$, kteří doplní komisi. Celkový počet možností je tedy $n\binom{n-1}{k-1}$.

□

Věta 3.2.2. *Pro $0 \leq k \leq n$ platí*

$$(n-k)\binom{n}{k} = n\binom{n-1}{k}. \tag{3.2.2}$$

Důkaz. Ze třídy o n studentech potřebujeme vybrat k-člennou komisi a jednoho zapisovatele, který nebude členem komise. Kolika způsoby to lze provést? Odpověď lze vyjádřit dvěma způsoby, které odpovídají levé a pravé straně dokazovaného vztahu (3.2.2).

1. způsob:

Vybereme komisi, což lze provést $\binom{n}{k}$ způsoby. Ze zbylých $n-k$ studentů vybereme zapisovatele. Celkový počet možností je tedy $(n-k)\binom{n}{k}$.

2. způsob:

Vybereme nejdříve z n studentů zapisovatele, poté ze zbylých $n-1$ studentů vybereme k-člennou komisi. Počet možností je tedy $n\binom{n-1}{k}$.

□

3.3 Parita čísel v Pascalově trojúhelníku

V této sekci odvodíme zajímavý fakt týkající se kombinačních čísel a jejich uspořádání v Pascalově trojúhelníku. Seznámíme se také se zajímavým způsobem, jak pro dané n a dané k zjistit paritu kombinačního čísla $\binom{n}{k}$. Budeme vycházet z kapitoly 5.5 knihy [3].

Při pohledu na Pascalův trojúhelník se zdá, že počet lichých čísel v každém řádku je vždy mocnina dvou. Silnější tvrzení poskytuje zajímavá věta, kterou nyní dokážeme.

Věta 3.3.1. ([3, str. 75]) *Pro nezáporné celé číslo n je počet lichých čísel v n-tém řádku Pascalova trojúhelníku roven 2^b, kde b je počet jedniček ve dvojkovém zápisu čísla n.*

Například v 76. řádku Pascalova trojúhelníku se podle této věty nachází $2^3 = 8$ lichých čísel, neboť $76 = 64+8+4 = (1001100)_2$. Jinými slovy, existuje 8 různých hodnot k, pro které je číslo $\binom{76}{k}$ liché.

Abychom dokázali větu 3.3.1, vymyslíme způsob, jak určit paritu čísla $\binom{n}{k}$ pro $0 \leq k \leq n$, a zjistíme, kolik z nich je lichých. Budeme potřebovat jednoduché lemma, které lze odvodit zkoumáním rovnosti $a = br$.

Lemma 3.3.2. ([3, str. 75]) *Buďte r,a,b celá čísla taková, že $r = \frac{a}{b}$. Pokud je a sudé a b liché, pak r je sudé. Pokud jsou a i b lichá, pak i r je liché.*

Následující lemma představuje rychlou metodu určení parity čísla $\binom{n}{k}$.

Lemma 3.3.3. ([3, str. 75]) *Pokud je n sudé a k liché, pak $\binom{n}{k}$ je sudé. Jinak platí*

$$\binom{n}{k} \equiv \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor} \pmod 2. \tag{3.3.1}$$

Tedy kromě případu, kdy n je sudé a k je liché, je parita čísel $\binom{n}{k}$ a $\binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor}$ stejná. Například

$$\binom{57}{37} \equiv \binom{28}{18} \equiv \binom{14}{9} \pmod 2. \tag{3.3.2}$$

Jelikož je číslo 14 sudé a číslo 9 liché, je podle lemmatu $\binom{14}{9}$ sudé, tím pádem i $\binom{57}{37}$ je sudé. Naproti tomu

$$\binom{57}{25} \equiv \binom{28}{12} \equiv \binom{14}{6} \equiv \binom{7}{3} \equiv \binom{3}{1} \equiv \binom{1}{0} \equiv 1 \pmod 2, \tag{3.3.3}$$

tedy $\binom{57}{25}$ je liché.

Důkaz lemmatu 3.3.3 rozdělíme na 4 případy.

Případ 1: n je sudé a k je liché.

Podle identity (3.2.1) platí

$$\binom{n}{k} = \frac{n\binom{n-1}{k-1}}{k}, \tag{3.3.4}$$

tedy zlomek na pravé straně rovnosti má sudého čitatele a lichého jmenovatele. Tedy podle lemmatu 3.3.2 je $\binom{n}{k}$ sudé.

Případ 2: n je sudé a k je sudé.

Budeme vycházet ze základního vzorce (3.1.1) pro výpočet kombinačního čísla.

$$\begin{aligned}
\binom{n}{k} &= \frac{n(n-1)(n-2)\cdots(n-k+1)}{1\cdot 2\cdot 3\cdots k} \\
&= \frac{(n-1)(n-3)\cdots(n-k+1)}{1\cdot 3\cdot 5\cdots(k-1)} \cdot \frac{n(n-2)(n-4)\cdots(n-k+2)}{2\cdot 4\cdot 6\cdots k} \\
&= \frac{(n-1)(n-3)\cdots(n-k+1)}{1\cdot 3\cdot 5\cdots(k-1)} \cdot \frac{2^{\frac{k}{2}}\cdot \frac{n}{2}(\frac{n}{2}-1)(\frac{n}{2}-2)\cdots(\frac{n}{2}-\frac{k}{2}+1)}{2^{\frac{k}{2}}\cdot 1\cdot 2\cdot 3\cdots\frac{k}{2}} \\
&= \frac{(n-1)(n-3)\cdots(n-k+1)\cdot\binom{n/2}{k/2}}{1\cdot 3\cdot 5\cdots(k-1)}
\end{aligned} \tag{3.3.5}$$

Výsledný jmenovatel je jistě lichý, stejně tak i všechny činitele v čitateli kromě posledního. Podle lemmatu 3.3.2 mají tedy čísla $\binom{n}{k}$ a $\binom{n/2}{k/2}$ stejnou paritu. Dostáváme tedy požadovaný výsledek

$$\binom{n}{k} \equiv \binom{n/2}{k/2} = \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor} \pmod 2. \tag{3.3.6}$$

Případ 3: n je liché a k je liché.

S využitím identity (3.2.1) a lemmatu 3.3.2 dostáváme

$$\binom{n}{k} = \frac{n\binom{n-1}{k-1}}{k} \equiv \binom{n-1}{k-1} \pmod 2. \tag{3.3.7}$$

Jelikož jsou čísla $n-1$ a $k-1$ sudá, podle (3.3.6) platí

$$\binom{n-1}{k-1} \equiv \binom{(n-1)/2}{(k-1)/2} = \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor} \pmod 2. \tag{3.3.8}$$

Tedy pro lichá čísla n a k opět dostáváme požadovaný výsledek (3.3.1).

Případ 4: n je liché a k je sudé.

S použitím identity (3.2.2) a podobnou úvahou jako v případu 3 odvozujeme

$$\binom{n}{k} = \frac{n\binom{n-1}{k}}{n-k} \equiv \binom{n-1}{k} \equiv \binom{(n-1)/2}{k/2} = \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor} \pmod 2. \tag{3.3.9}$$

Tím je důkaz lemmatu 3.3.3 hotov.

Jak souvisí lemma 3.3.3 s větou 3.3.1? Připomeňme, že pokud má číslo x binární reprezentaci $(b_t b_{t-1} \dots b_1 b_0)_2$, kde $b_i \in \{0,1\}$, pak je jeho parita určena hodnotou b_0 a číslo $\lfloor x/2 \rfloor = b_t 2^{t-1} + b_{t-1} 2^{t-2} + \cdots + b_1$ má binární reprezentaci $(b_t b_{t-1} \dots b_2 b_1)_2$. Tento poznatek umožňuje snadné použití lemmatu 3.3.3 k určení parity $\binom{n}{k}$, pokud jsou čísla n a k zapsána ve dvojkové soustavě.

Příklad 3.3.4. ([3, str. 76]) Určete paritu čísla $\binom{76}{52}$.

Nejprve vyjádříme čísla 76 a 52 ve dvojkové soustavě:

$$\begin{aligned} 76 &= 64 + 8 + 4 = (1001100)_2 \\ 52 &= 32 + 16 + 4 = (0110100)_2 \end{aligned} \tag{3.3.10}$$

Na začátek zápisu čísla 52 ve dvojkové soustavě jsme přidali nulu, aby měly binární zápisy obou čísel stejnou délku. Vidíme, že binární reprezentace obou čísel končí číslicí 0, jedná se tedy o případ $\binom{\text{sudá}}{\text{sudá}}$. Opakovaným použitím lemmatu 3.3.3 dostáváme

$$\binom{(100110)_2}{(011010)_2} \equiv \binom{(10011)_2}{(01101)_2} \equiv \binom{(1001)_2}{(0110)_2} \equiv \binom{(100)_2}{(011)_2} \pmod 2. \tag{3.3.11}$$

Poslední kombinační číslo je typu $\binom{\text{sudá}}{\text{lichá}}$, proto podle lemmatu 3.3.3 je číslo $\binom{76}{52}$ sudé.

Obecně bude číslo $\binom{n}{k}$ sudé právě tehdy, pokud při postupném odebírání poslední cifry z binárního zápisu obou čísel n a k narazíme na případ $\binom{\text{sudá}}{\text{lichá}}$. To nastane v případě, že se některá číslice 1 z binárního zápisu k nachází přesně pod číslicí 0 z binárního zápisu n. Lze tedy například hned určit, že číslo $\binom{76}{12} = \binom{(1001100)_2}{(0001100)_2}$ je liché, neboť všechny číslice 1 z binárního zápisu čísla 12 se nacházejí pod číslicí 1 z binárního zápisu čísla 76.

Pro kolik hodnot k tedy bude číslo $\binom{76}{k}$ liché? Jelikož $76 = (1001100)_2$, k musí mít tvar $k = (x00yz00)_2$, kde x,y,z jsou číslice 0 nebo 1. Zřejmě existuje $2^3 = 8$ možností, jak volit číslice x,y,z, tedy pro právě 8 různých hodnot k je číslo $\binom{76}{k}$ liché. Obecněji, pokud b je počet jedniček v binární reprezentaci čísla n, pak existuje 2^b hodnot k, pro které je číslo $\binom{n}{k}$ liché. Věta 3.3.1 je dokázána.

Můžeme ještě zjistit, pro které hodnoty k je $\binom{76}{k}$ liché. Jsou to čísla

$$\begin{aligned} 64+8+4&=76,\\ 64+8&=72,\\ 64+4&=68,\\ 64&=64,\\ 8+4&=12,\\ 8&=8,\\ 4&=4,\\ 0&=0. \end{aligned} \tag{3.3.12}$$

3.4 Lucasova věta

Již víme, jak efektivně určit počet lichých čísel v n-tém řádku Pascalova trojúhelníku z binárního zápisu čísla n. V této sekci větu 3.3.1 zobecníme a pro dané n a dané prvočíslo p určíme počet čísel v n-tém řádku Pascalova trojúhelníku, která nejsou dělitelná p. Využijeme přitom zápisu čísla n v číselné soustavě o základu p. Dostaneme tím tvrzení známé pod názvem Lucasova věta.

Na úvod představíme jednoduchou, ale užitečnou větu o dělitelnosti kombinačních čísel.

Věta 3.4.1. ([3, str. 114]) *Nechť je dáno prvočíslo p. Potom je p dělitelem kombinačního čísla $\binom{p}{k}$ pro všechna přirozená čísla $k < p$.*

Důkaz. Podle (3.2.1) je

$$k\binom{p}{k} = p\binom{p-1}{k-1} \tag{3.4.1}$$

násobek p. Jelikož je p prvočíslo, je nesoudělné s k, tedy p dělí $\binom{p}{k}$.

□

Zobecněním dostáváme následující větu, kterou dokážeme stejným způsobem.

Věta 3.4.2. ([3, str. 120]) *Nechť je dáno prvočíslo p. Potom pro všechna $\alpha \in \mathbb{N}$ a pro všechna $1 \leq k < p^\alpha$ platí:*

$$\binom{p^\alpha}{k} \equiv 0 \,(\mathrm{mod}\, p). \tag{3.4.2}$$

Důkaz. Opět podle (3.2.1) je

$$k\binom{p^\alpha}{k} = p^\alpha\binom{p^\alpha - 1}{k-1}. \tag{3.4.3}$$

Je $1 \leq k < p^\alpha$, proto největší mocnina p, která dělí k, je nejvýše $p^{\alpha-1}$. Tedy p musí být dělitelem $\binom{p^\alpha}{k}$.

□

Definice 3.4.3. ([3, str. 121]) Polynomy s celočíselnými koeficienty

$$f(x) = \sum_{n\geq 0} a_n x^n,\ g(x) = \sum_{n\geq 0} b_n x^n \tag{3.4.4}$$

jsou kongruentní modulo p, pokud platí $a_n \equiv b_n \pmod p$ pro všechna n.

Poznámka 3.4.4. Kongruenci polynomů značíme pomocí $\equiv$, tj. píšeme $f \equiv g \pmod p$.

Poznámka 3.4.5. Sčítání a násobení polynomů zachovává kongruenci: pokud $f_1 \equiv g_1$ a $f_2 \equiv g_2$, pak $f_1 + f_2 \equiv g_1 + g_2$ a $f_1 \cdot f_2 \equiv g_1 \cdot g_2$ (důkazy těchto jednoduchých tvrzení přenecháváme čtenáři).

Lemmatu, které nyní představíme, se někdy přezdívá „prvákova binomická věta“ („freshman's binomial theorem“, [3, str. 120]).

Lemma 3.4.6. ([3, str. 121]) *Pro prvočíslo p a $\alpha \in \mathbb{N}_0$ platí*

$$(1+x)^{p^\alpha} \equiv 1 + x^{p^\alpha} \pmod p. \tag{3.4.5}$$

Důkaz. Kongruenci odvodíme pomocí binomické věty. Platí

$$(1+x)^{p^\alpha} = \sum_{k=0}^{p^\alpha} \binom{p^\alpha}{k} x^k \equiv 1 + x^{p^\alpha} \pmod p, \tag{3.4.6}$$

neboť podle věty 3.4.2 jsou všechny sčítance kongruentní s nulou modulo p, až na případy $k = 0$ a $k = p^\alpha$.

□

Ilustrujme použití lemmatu 3.4.6 na příkladu. Zjistíme, pro která čísla k je kombinační číslo $\binom{82}{k}$ liché. Číslo 82 rozepíšeme jako součet mocnin dvojky, tj. $82 = 64 + 16 + 2$, a použijeme lemma 3.4.6 pro $p = 2$.

$$\begin{aligned}\sum_{k=0}^{82} \binom{82}{k} x^k &= (1+x)^{82} \\ &= (1+x)^{64}(1+x)^{16}(1+x)^2 \\ &\equiv (1+x^{64})(1+x^{16})(1+x^2) \\ &\equiv 1 + x^2 + x^{16} + x^{18} + x^{64} + x^{66} + x^{80} + x^{82} \pmod 2\end{aligned} \tag{3.4.7}$$

Číslo $\binom{82}{k}$ má stejnou paritu jako koeficient u x^k v posledním výrazu. Například $\binom{82}{18} \equiv 1 \pmod 2$ je liché, zatímco $\binom{82}{20} \equiv 0 \pmod 2$ je sudé. Hodnoty k, pro které je $\binom{82}{k}$ liché, jsou ty, které lze psát ve tvaru $64a+16b+2c$, kde $a,b,c \in \{0,1\}$.

Existuje tedy $2^3 = 8$ lichých hodnot $\binom{82}{k}$. Tedy obecně, pokud má n binární zápis $\sum_{i=0}^{t} b_i 2^i$, kde $b_i = 0$ nebo 1, počet lichých hodnot $\binom{n}{k}$ je

$$\prod_{i=0}^{t}(1 + b_i) = 2^b, \tag{3.4.8}$$

kde b je počet jedniček v binárním zápisu n. Vlastně jsme jiným způsobem dokázali větu 3.3.1.

Nyní jsme připraveni vyslovit a dokázat Lucasovu větu.

Věta 3.4.7. ([5, str. 589], [14, sekce XXI]) *Nechť je dáno prvočíslo p a čísla $n,k \in \mathbb{N}_0$, přičemž $n = \sum_{i\geq 0} b_i p^i$ a $k = \sum_{i\geq 0} c_i p^i$ pro $0 \leq b_i,c_i < p$ jsou zápisy čísel n, resp. k, v soustavě o základu p. Potom platí*

$$\binom{n}{k} \equiv \prod_{i\geq 0} \binom{b_i}{c_i} \pmod p. \tag{3.4.9}$$

Důkaz. Z binomické věty a lemmatu 3.4.6 plyne

$$\begin{aligned}
\sum_{k=0}^{n} \binom{n}{k} x^k &= (1+x)^n \\
&= (1+x)^{b_0 + b_1 p + b_2 p^2 + \cdots} \\
&= (1+x)^{b_0}(1+x)^{b_1 p}(1+x)^{b_2 p^2} \cdots \\
&\equiv (1+x)^{b_0}(1+x^p)^{b_1}(1+x^{p^2})^{b_2} \cdots \\
&\equiv \prod_{i\geq 0} \sum_{j_i=0}^{b_i} \binom{b_i}{j_i} x^{j_i p^i} \pmod p.
\end{aligned} \tag{3.4.10}$$

Jelikož $b_i < p$ a pro $b_i < j$ je $\binom{b_i}{j} = 0$, dostáváme

$$\sum_{k=0}^{n} \binom{n}{k} x^k = \prod_{i\geq 0} \sum_{j_i=0}^{p-1} \binom{b_i}{j_i} x^{j_i p^i} \pmod p. \tag{3.4.11}$$

Koeficient u členu x^k na levé straně (3.4.11) je $\binom{n}{k}$. Zjistíme, jak vypadá koeficient u x^k na pravé straně. Po roznásobení součinu má každý člen tvar

$$\binom{b_0}{j_0} x^{j_0} \binom{b_1}{j_1} x^{j_1 p} \binom{b_2}{j_2} x^{j_2 p^2} \cdots . \tag{3.4.12}$$

Aby byl ve vybraném členu exponent u x roven k, musí platit

$$k = j_0 + j_1 p + j_2 p^2 + \cdots . \tag{3.4.13}$$

Jelikož je $0 \leq j_i \leq p-1$, existuje pouze jeden způsob, jak rovnosti dosáhnout: (3.4.13) musí být zápis k v soustavě o základu p, tedy $j_i = c_i$. Koeficient u x^k na pravé straně (3.4.11) je tedy $\binom{b_0}{c_0}\binom{b_1}{c_1}\ldots$. Jelikož jsou koeficienty u x^k na obou stranách (3.4.11) kongruentní modulo p, dostáváme

$$\binom{n}{k} \equiv \binom{b_0}{c_0}\binom{b_1}{c_1}\binom{b_2}{c_2}\ldots \pmod p, \tag{3.4.14}$$

což jsme měli dokázat.

□

Pomocí Lucasovy věty lze snadno zjistit, jaký je zbytek $\binom{n}{k}$ při dělení libovolným prvočíslem p. Zamysleme se například nad případem $n = 97$, $k = 35$ a $p = 5$.

$$\begin{aligned} 97 &= 3 \cdot 5^2 + 4 \cdot 5 + 2 = (342)_5 \\ 35 &= 1 \cdot 5^2 + 2 \cdot 5 + 0 = (120)_5 \end{aligned} \tag{3.4.15}$$

Podle Lucasovy věty je

$$\binom{97}{35} \equiv \binom{3}{1}\binom{4}{2}\binom{2}{0} = 18 \equiv 3 \,(\mathrm{mod}\, 5). \tag{3.4.16}$$

Naproti tomu pro $k = 38 = 1 \cdot 5^2 + 2 \cdot 5 + 3 = (123)_5$ je

$$\binom{97}{38} \equiv \binom{3}{1}\binom{4}{2}\binom{2}{3} = 0 \equiv 0 \,(\mathrm{mod}\, 5). \tag{3.4.17}$$

Všimněme si, že se číslice 3 nachází pod číslicí 2 v zápisech čísel $38 = (123)_5$, resp. $97 = (342)_5$, v pětkové soustavě. V (3.4.17) tím pádem vzniká činitel $\binom{2}{3} = 0$, proto je $\binom{97}{38}$ dělitelné pěti. Nadešel čas představit zajímavý důsledek Lucasovy věty, který je zobecněním věty 3.3.1.

Věta 3.4.8. ([5, str. 590]) *Nechť je dáno prvočíslo p a čísla n,$k \in \mathbb{N}_0$, přičemž $n = \sum_{i=0} b_i p^i$ a $k = \sum_{i=0} c_i p^i$ pro $0 \leq b_i$,$c_i < p$ jsou zápisy čísel n, resp. k, v soustavě o základu p. Potom počet hodnot k, pro které platí*

$$\binom{n}{k} \not\equiv 0 \,(\mathrm{mod}\, p), \tag{3.4.18}$$

je

$$\prod_{i=0} (b_i + 1). \tag{3.4.19}$$

Důkaz.

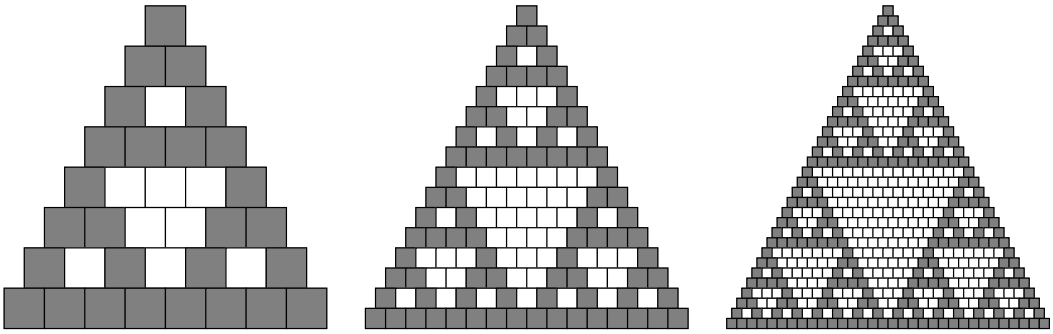
Podle Lucasovy věty nastává (3.4.18) právě tehdy, když je součin na pravé straně (3.4.9) nenulový. To je ekvivalentní s tím, že pro každé i platí

$$\binom{b_i}{c_i} \not\equiv 0 \,(\mathrm{mod}\, p). \tag{3.4.20}$$

Jelikož pro každé i platí $b_i < p$, existuje $b_i + 1$ možných hodnot c_i, pro které platí (3.4.20).

□

Jelikož je $97 = (342)_5$, díky větě 3.4.8 víme, že v 97. řádku Pascalova trojúhelníku je $(3 + 1) \cdot (4 + 1) \cdot (2 + 1) = 60$ čísel, která nejsou dělitelná pěti.



Obrázek 3.1: Barevně odlišená parita čísel v Pascalově trojúhelníku

													1																		
												1		**1**																
											1		0		**1**															
P_n										**1**		**1**		**1**		**1**														
						1		0		0		0		**1**																
					1		**1**		0		0		**1**		**1**															
				1		0		**1**		0		**1**		0		**1**														
P_{n+1}	**1**		**1**		**1**		**1**		**1**		**1**		**1**		**1**		**1**													

Tabulka 3.2: Rozmístění lichých čísel v Pascalově trojúhelníku

3.5 Pascalův trojúhelník modulo 2

Zmíníme ještě zajímavou vlastnost Pascalova trojúhelníku, která se týká parity jeho čísel; nahradíme-li lichá a sudá čísla v Pascalově trojúhelníku dvěma barvami, získáme obrázek, který připomíná fraktál známý jako Sierpinského trojúhelník [15].

Nahraďme pro představu každé číslo v Pascalově trojúhelníku jeho zbytkem po dělení dvěma. Získáváme tak trojúhelník, ve kterém se nachází pouze čísla 1 a 0. Označíme-li P_n prvních 2^n řádků tohoto trojúhelníku (započítáváme i nultý řádek), potom P_{n+1} je trojúhelník, který se skládá ze tří kopií P_n a vnitřního trojúhelníku obsahujícího pouze nuly, viz tabulku 3.2; tuto skutečnost vzápětí dokážeme. Kopie trojúhelníku P_n vlevo dole a vpravo dole budeme pro jednoduchost nazývat ekvivalentní trojúhelníku P_n.

Chceme dokázat, že pokud vybereme libovolné číslo v P_n, potom čísla na odpovídajících pozicích v trojúhelnících ekvivalentních P_n vlevo a vpravo dole v trojúhelníku P_{n+1} mají stejnou hodnotu (mod 2) jako vybrané číslo v P_n. Podívejme se na kombinační číslo $\binom{r}{c}$, tedy c-té číslo v r-tém řádku v trojúhelníku P_n. Jelikož P_n má 2^n řádků, obě čísla r, c musí být menší než 2^n. Ve dvojkové soustavě mohou být tedy zapsána jako

$$\begin{aligned} r &= r_{n-1} \dots r_2 r_1 r_0 \\ c &= c_{n-1} \dots c_2 c_1 c_0. \end{aligned} \tag{3.5.1}$$

Trojúhelník P_n má 2^n řádků a v jeho posledním řádku se nachází 2^n čísel. Proto číslu $\binom{r}{c}$ v P_n odpovídá číslo $\binom{2^n+r}{c}$ v levém dolním ekvivalentním trojúhelníku a číslo $\binom{2^n+r}{2^n+c}$ v pravém dolním ekvivalentním trojúhelníku.

Podle Lucasovy věty platí:

$$\begin{aligned}\binom{2^n+r}{c} &\equiv \binom{1\,r_{n-1}\dots r_0}{0\,c_{n-1}\dots c_0} \equiv \binom{1}{0}\binom{r_{n-1}}{c_{n-1}}\dots\binom{r_0}{c_0}\\ &\equiv \binom{r_{n-1}}{c_{n-1}}\dots\binom{r_0}{c_0} \equiv \binom{r}{c} (\mathrm{mod}\, 2)\\ \binom{2^n+r}{2^n+c} &\equiv \binom{1\,r_{n-1}\dots r_0}{1\,c_{n-1}\dots c_0} \equiv \binom{1}{1}\binom{r_{n-1}}{c_{n-1}}\dots\binom{r_0}{c_0}\\ &\equiv \binom{r_{n-1}}{c_{n-1}}\dots\binom{r_0}{c_0} \equiv \binom{r}{c} (\mathrm{mod}\, 2)\end{aligned} \tag{3.5.2}$$

Zbývá dokázat, že P_n a dva jemu ekvivalentní trojúhelníky obklopují trojúhelník skládající se ze sudých čísel. Zaměřme se na první řádek Pascalova trojúhelníku pod trojúhelníkem P_n, tj. řádek s pořadovým číslem $r = 2^n$. V něm se nachází $2^n + 1$ čísel, konkrétně jsou to čísla $\binom{r}{c}$ pro $0 \le c \le 2^n$. Na začátku i na konci řádku se nachází číslo 1. Jsou to vrchní čísla v levém dolním, resp. pravém dolním, trojúhelníku ekvivalentním P_n. Všechna zbývající čísla v tomto řádku mají ve svém dvojkovém zápisu alespoň jednu jedničku a jsou menší než 2^n. S využitím Lucasovy věty odvozujeme

$$\binom{2^n}{c} \equiv \binom{1\;0\dots0}{0\;c_{n-1}\dots c_0} \equiv \binom{1}{0}\binom{0}{c_{n-1}}\dots\binom{0}{1}\dots\binom{0}{c_0} \equiv 0 \pmod 2, \tag{3.5.3}$$

tedy všechna čísla kromě prvního a posledního jsou v tomto řádku sudá.

Co se děje v následujícím řádku? Jelikož je $\binom{r+1}{c} = \binom{r}{c} + \binom{r}{c-1}$, tj. c-té číslo v $r+1$-tém řádku je součtem $c-1$-tého a c-tého čísla v řádku předchozím, musí všechna čísla z tohoto řádku patřící do zkoumaného vnitřního trojúhelníka být též sudá. Jejich počet je o 1 menší. Stejným způsobem lze dokázat, že i všechny další řádky vnitřního trojúhelníku obsahují pouze sudá čísla. V posledním řádku trojúhelníku P_{n+1} už se nachází jen lichá čísla.

3.6 Kummerova věta

V úvodu této sekce předvedeme větu, která dává odpověď na otázku, jakou největší mocninou prvočísla p je dělitelné kombinační číslo $\binom{n}{m}$. K jejímu důkazu využijeme vzorec (2.2.8) z předchozí kapitoly.

Než tak učiníme, připomeňme symbol $\epsilon_p(n!)$, který byl definován v kapitole 2 a označuje největší mocninu prvočísla p, která dělí číslo $n!$. Podobně pro libovolné přirozené číslo n budeme $\epsilon_p(n)$ značit největší mocninu p, která dělí n. Je zřejmé, že pro přirozená a, b platí tyto vztahy:

$$\begin{aligned}\epsilon_p(a \cdot b) &= \epsilon_p(a) + \epsilon_p(b),\\ \epsilon_p(a/b) &= \epsilon_p(a) - \epsilon_p(b) \;\; (\text{pokud } a/b \in \mathbb{N}).\end{aligned} \tag{3.6.1}$$

Dále připomeňme symbol $\nu_p(n)$ označující ciferný součet čísla n při reprezentaci v soustavě o základu p.

Věta 3.6.1. *Nechť je dáno prvočíslo p. Potom platí*

$$\epsilon_p\left(\binom{n}{m}\right) = \frac{\nu_p(n-m) + \nu_p(m) - \nu_p(n)}{p-1}. \tag{3.6.2}$$

Důkaz. S pomocí vztahů (2.2.8) a (3.6.1) odvozujeme

$$\begin{aligned}\epsilon_p\left(\binom{n}{m}\right) &= \epsilon_p\left(\frac{n!}{(n-m)!\cdot m!}\right)\\ &= \epsilon_p(n!) - \epsilon_p((n-m)!) - \epsilon_p(m!)\\ &= \frac{n-\nu_p(n)}{p-1} - \frac{n-m-\nu_p(n-m)}{p-1} - \frac{m-\nu_p(m)}{p-1}\\ &= \frac{\nu_p(n-m)+\nu_p(m)-\nu_p(n)}{p-1}.\end{aligned} \tag{3.6.3}$$

□

Rozmyslíme si, že číslo na pravé straně vztahu (3.6.2) se dá interpretovat i jako počet přenosů při sčítání čísel m a $n-m$ v soustavě o základu p. Výsledná věta, kterou nyní uvádíme, je známa jako věta Kummerova.

Věta 3.6.2. ([12, str. 115], [10]) *Nechť je dáno prvočíslo p a přirozená čísla n, m, přičemž $n \geq m$. Potom platí, že číslo $\epsilon_p\left(\binom{n}{m}\right)$ je rovno počtu přenosů při sčítání čísel m a $n-m$ zapsaných v číselné soustavě o základu p.*

Důkaz. Pro účely důkazu připusťme zápis čísel v soustavě o základu p začínající nulou. Položme $r = n - m$. Nechť tedy

$$\begin{aligned}n &= n_d n_{d-1} \ldots n_0,\\ m &= m_d m_{d-1} \ldots m_0,\\ r &= r_d r_{d-1} \ldots r_0\end{aligned} \tag{3.6.4}$$

jsou zápisy čísel n, m, r v soustavě o základu p.

Pokud na j-té pozici dochází při sčítání $m + r$ k přenosu, definujme $c_j = 1$, jinak $c_j = 0$. Formálněji, zavedeme-li $c_{-1} = 0$, pro $0 \leq j \leq d$ definujeme

$$\begin{aligned}&c_j = 1, \quad \text{pokud} \quad m_j + r_j + c_{j-1} \geq p,\\ &c_j = 0 \quad \text{jinak.}\end{aligned} \tag{3.6.5}$$

Poznamenejme, že musí být $c_d = 0$.

Potom pro $j \geq 0$ dostáváme

$$n_j = m_j + r_j + c_{j-1} - pc_j. \tag{3.6.6}$$

S využitím věty 3.6.1 odvozujeme

$$\begin{aligned}
\epsilon_p\left(\binom{n}{m}\right) &= \frac{\nu_p(m)+\nu_p(r)-\nu_p(n)}{p-1} \\
&= \frac{\sum_{j=0}^{d}(m_j+r_j-n_j)}{p-1} \\
&= \frac{\sum_{j=0}^{d}(-c_{j-1}+pc_j)}{p-1} \\
&= \frac{\sum_{j=0}^{d}(-c_{j-1}+c_j+(p-1)c_j)}{p-1} \\
&= \frac{c_d-c_{-1}+\sum_{j=0}^{d}((p-1)c_j)}{p-1} \\
&= \sum_{j=0}^{d} c_j,
\end{aligned} \tag{3.6.7}$$

což je celkový počet přenosů při sčítání $r+m$.

□

Poznámka 3.6.3. Počet přenosů při sčítání čísel $n-m$ a m je roven počtu „výpůjček“ při odečítání čísla m od čísla n [16]. Označme opět $r=n-m$ a nechť (3.6.4) jsou zápisy čísel n, m, r v soustavě o základu p. Pokud na j-té pozici dochází při odečítání $n-m$ k výpůjčce, definujme $b_j=1$, jinak $b_j=0$. Jelikož $n \geq m$, musí být $b_d=0$. Pro $j \geq 0$ dostáváme $r_j = n_j - m_j - b_{j-1} + pb_j$, po úpravě $n_j = m_j + r_j + b_{j-1} - pb_j$. Srovnáním se vztahem (3.6.6) dostáváme $c_{j-1} - pc_j = b_{j-1} - pb_j$. Jelikož pro $j \geq 0$ jsou b_j,$c_j \in \{0,1\}$ a $p>1$, musí být $b_j = c_j$. Tedy při odčítání $n-m$ dochází k výpůjčce právě na těch pozicích, na kterých dochází k přenosu při sčítání $m+r$.

Zajímavé nestandardní důkazy Kummerovy věty a vzorce (2.2.8) lze najít v [20].

Kummerovu větu můžeme využít při řešení různých příkladů na dělitelnost a při dokazování dalších vět o dělitelnosti kombinačních čísel. Začněme s řešením příkladu, který se objevil v Matematické olympiádě v SSSR [16].

Příklad 3.6.4. ([16, str. 4]) Ukažte, že číslo $\binom{1000}{500}$ není dělitelné sedmi.

Jelikož $1000-500=500$, chceme provést sčítání čísel $500+500$ v sedmičkové soustavě. Číslo 500 má v sedmičkové soustavě zápis 1313. Při sčítání $1313+1313$ nedochází k žádnému přenosu, tedy podle Kummerovy věty je $\epsilon_7\left(\binom{1000}{500}\right)=0$.

Tento příklad lze zřejmě řešit také přímo pomocí vzorce (3.6.2). Číslo 1000 má v sedmičkové soustavě zápis 2626, tedy dostáváme

$$\begin{aligned}
\epsilon_7\left(\binom{1000}{500}\right) &= \frac{\nu_7(1000-500)+\nu_7(500)-\nu_7(1000)}{6} \\
&= \frac{8+8-16}{6} = 0.
\end{aligned} \tag{3.6.8}$$

Věta 3.6.5. ([16, str. 8]) *Nechť je dáno prvočíslo p. Potom počet kombinačních čísel z $\binom{n}{0},\binom{n}{1},\ldots,\binom{n}{n}$, která jsou násobky p, je $n+1-(n_0+1)(n_1+1)\ldots(n_r+1)$, kde $n_0,\ldots,n_r$ jsou číslice při zápisu n v soustavě o základu p.*

Důkaz. Nechť jsou $n = n_0 + n_1 p + \cdots + n_r p^r (n_r \neq 0)$ a $a = a_0 + a_1 p + \cdots + a_r p^r$ rozvinuté zápisy n a a v soustavě o základu p. Podle Kummerovy věty a poznámky 3.6.3 p nedělí $\binom{n}{a}$ právě tehdy, když $n_i \geq a_i$ pro všechna $i \in \{0,\ldots,r\}$. Počet kombinačních čísel z $\binom{n}{0},\binom{n}{1},\ldots,\binom{n}{n}$, která nejsou násobkem p, je tedy $(n_0+1)(n_1+1)\ldots(n_r+1)$, neboť pro libovolné i lze a_i vybrat n_i+1 způsoby. Ostatní kombinační čísla jsou násobky p.

□

Věta 3.6.5 představuje zobecnění dříve dokázané věty 3.3.1, kterou získáme volbou $p = 2$.

Věta 3.6.6. ([16, str. 10]) *Je-li $n > 1$, pak největším společným dělitelem kombinačních čísel $\binom{n}{1}$, $\binom{n}{2}$, $\ldots$, $\binom{n}{n-1}$ je p, pokud je n mocninou prvočísla p, jinak 1.*

Důkaz. Označme d největšího společného dělitele kombinačních čísel $\binom{n}{1}$, $\binom{n}{2}$, $\ldots$, $\binom{n}{n-1}$ pro $n > 1$. Jelikož $\binom{n}{1} = n$, d musí být dělitelem n. Nechť je p libovolné prvočíslo, které dělí n.

Nejprve uvažme případ, že n je mocninou p, pišme $n = p^r$. Potom zápis čísla n v soustavě o základu p je $10\ldots0$ s počtem cifer $r+1$. Nechť má číslo $a \in \{1,\ldots,p^r-1\}$ v soustavě o základu p zápis $a_k\ldots a_1 a_0 0\ldots0$, $a_0 \neq 0$, počet nul na konci tohoto čísla označme s (tedy a je ve tvaru $p^s \cdot q$ pro nějaké q nesoudělné s p). Potom má číslo $n-a$ v soustavě o základu p zápis $(p-1)\ldots(p-1)(p-1-a_k)\ldots(p-1-a_1)(p-a_0)0\ldots0$. Toto číslo má r cifer a končí s nulami.

Při přičtení čísla a k číslu $n-a$ dochází přesně k $r-s$ přenosům, podle Kummerovy věty je tedy $\epsilon_p\left(\binom{n}{a}\right) = r-s$.

Pokud zvolíme $a = p^{r-1}$, pak $\epsilon_p\left(\binom{n}{a}\right) = r-(r-1) = 1$, proto $d \leq p$. Pro toto i kterékoli jiné $a \in \{1,\ldots,p^r-1\}$ je $s < r$, tedy $\epsilon_p\left(\binom{n}{a}\right) > 0$, a proto $d = p$.

Nyní zvážíme případ, že n není mocninou p, tedy lze psát $n = p^r \cdot m$, přičemž $m > 1$ a čísla p, m jsou nesoudělná. Potom zápis čísla n v soustavě o základu p je $m_k\ldots m_1 m_0 0\ldots0$, kde $m_0 \geq 1$ a počet nul na konci tohoto čísla je r.

Uvažme číslo $b = p^r$. Jeho zápis v soustavě o základu p je $10\ldots0$, počet nul je r. Číslo $n-b$ má tedy zápis $m_k\ldots m_1(m_0-1)0\ldots0$.

Při přičtení čísla b k číslu $n-b$ nedochází k žádnému přenosu, podle Kummerovy věty tedy kombinační číslo $\binom{n}{b}$ není dělitelné p. Tj. žádný prvočíselný dělitel n nedělí d, proto $d = 1$.

□

Poznámka 3.6.7. V článku [11] je podrobně popsáno, jak najít největšího společného dělitele kombinačních čísel $\binom{n}{r},\ldots,\binom{n}{s}$ pro $r \leq s \leq n$.

Příklad 3.6.8. ([16, str. 5]) Ukažte, že kombinační číslo $\binom{2n}{n}$ je násobkem $n+1$.

K řešení využijeme Kummerovu větu. Je-li p libovolný prvočíselný dělitel čísla $n+1$ a $\epsilon_p(n+1) = l$, pak číslo $n+1$ má v soustavě o základu p zápis

$a_k \dots a_1 a_0 0 \dots 0$, kde $a_0 \neq 0$ a počet nul za a_0 je roven l. Číslo n má v soustavě o základu p zápis $a_k \dots a_1 (a_0 - 1)(p-1) \dots (p-1)$ (na konci čísla je l číslic $p-1$).

Při sčítání $n + n$ v soustavě o základu p dochází k alespoň l přenosům, tj.

$$\epsilon_p(n+1) \leq \epsilon_p(\binom{2n}{n}). \tag{3.6.9}$$

Ukázali jsme, že exponent libovolného prvočísla p v prvočíselném rozkladu čísla $\binom{2n}{n}$ je větší nebo roven exponentu tohoto prvočísla v rozkladu čísla $n+1$; odtud již plyne dokazované tvrzení.

Poznámka 3.6.9. Číslo $C_n = \frac{1}{n+1}\binom{2n}{n}$ se nazývá n-té Catalanovo číslo. Ukázali jsme, že takto definované číslo je vždy celé. Tuto skutečnost lze dokázat i kombinatorickou úvahou; viz kapitolu 5, kde se Catalanovým číslům a jejich významu v kombinatorice věnujeme podrobněji.

Příklad 3.6.10. ([16, str. 6]) Ukažte, že pro $n > 1$ je $\binom{2n}{n}$ sudé a 4 není dělitelem $\binom{2n}{n}$ právě tehdy, když n je mocninou dvojky.

Zjistíme, pro která $n > 1$ je $\epsilon_2(\binom{2n}{n}) = 1$. Platí $\nu_2(2n) = \nu_2(n)$, tedy podle (3.6.2) je

$$\epsilon_2\left(\binom{2n}{n}\right) = 2\nu_2(n) - \nu_2(2n) = \nu_2(n) \geq 1, \tag{3.6.10}$$

tj. kombinační číslo $\binom{2n}{n}$ je sudé. Navíc platí:

$$\epsilon_2\left(\binom{2n}{n}\right) = 1 \quad \Leftrightarrow \quad \nu_2(n) = 1 \quad \Leftrightarrow \quad n \text{ je mocninou dvojky.} \tag{3.6.11}$$

Příklad 3.6.11. ([4, str. 201]) Ukažte, že pro prostřední binomické koeficienty platí:

$$\begin{aligned} &\binom{2n}{n} \equiv (-1)^{\nu_3(n)} \pmod 3, \\ &\qquad \text{pokud se v trojkovém zápisu čísla } n \text{ vyskytují pouze číslice 0, 1,} \\ &\binom{2n}{n} \equiv 0 \pmod 3 \quad \text{jinak.} \end{aligned} \tag{3.6.12}$$

Pokud má číslo n ve svém trojkovém zápisu číslici 2, pak při sčítání tohoto čísla sama se sebou dochází k přenosu, tedy podle Kummerovy věty je dělitelné třemi. Tím je dokázána druhá část tvrzení. Pokud trojkový zápis obsahuje pouze číslice 0, 1, pak $2n$ má v trojkovém zápisu číslice 2 právě na těch pozicích, kde má n číslice 1. Tedy podle Lucasovy věty

$$\binom{2n}{n} \equiv \binom{2}{1}^{\nu_3(n)} \equiv (-1)^{\nu_3(n)} \pmod 3. \tag{3.6.13}$$

Výsledek z předchozího příkladu se dá celkem snadno zobecnit pro zbytky při dělení libovolným prvočíslem p. K tomuto účelu zavedeme operátor $\nu_{p,j}(n)$, který značí počet číslic v zápisu $(n)_p$ majících hodnotu j (předpokládáme $0 \leq j < p$). Nyní můžeme zformulovat větu, jejíž důkaz lze provést analogicky s řešením příkladu 3.6.11.

Věta 3.6.12. ([4, str. 201]) *Nechť je dáno prvočíslo p a nechť S je množina všech $s \in \mathbb{N}$, pro která platí, že všechny číslice v zápisu $(s)_p$ mají hodnotu nejvýše $p/2$. Potom*

$$\begin{aligned} \binom{2n}{n} &\equiv \prod_j \binom{2j}{j}^{\nu_{p,j}(n)} \pmod{p}, \quad \text{pokud} \quad n \in S, \\ \binom{2n}{n} &\equiv 0 \pmod{p} \quad \text{jinak.} \end{aligned} \tag{3.6.14}$$

3.7 Kdy je kombinační číslo mocninou?

Kummerova věta říká, jakou nevětší mocninou daného prvočísla p je dělitelné kombinační číslo $\binom{n}{k}$. V této sekci zjistíme, ve kterých případech je kombinační číslo $\binom{n}{k}$ rovno mocnině nějakého prvočísla. V článku [9] dokázal autor, že k této skutečnosti dochází zřídkakdy, konkrétně pouze pro $k = 1$ nebo $k = n - 1$, pokud n je mocninou prvočísla. Později se podařilo Wolfgangu Stahlovi větu dokázat elegantně s využitím Legendreova vzorce.

Věta 3.7.1. ([19]) *Nechť jsou dána přirozená čísla n, k a prvočíslo p. Potom může být $\binom{n}{k}$ přirozenou mocninou p pouze pro $k = 1$ nebo $k = n - 1$.*

Důkaz. Zřejmě nemůže být $\binom{n}{k}$ přirozenou mocninou p pro $k \geq n$; zbývá dokázat, že $\binom{n}{k}$ není přirozenou mocninou p pro $1 < k < n - 1$.

Uvědomme si, že pro reálná x, y je

$$\lfloor x + y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \leq 1. \tag{3.7.1}$$

Určeme $m \in \mathbb{N}$ tak, aby pro daná čísla n, p platilo $p^m \leq n < p^{m+1}$. Potom podle (2.2.7) a (3.7.1) je

$$\epsilon_p(\binom{n}{k}) = \epsilon_p\left(\frac{n!}{k! \cdot (n-k)!}\right) = \sum_{i=1}^{m} \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{n-k}{p^i} \right\rfloor \right) \leq m. \tag{3.7.2}$$

Pro $1 < k < n - 1$ platí $p^m \leq \binom{n}{1} < \binom{n}{k}$, tj. $\binom{n}{k}$ nemůže být menší mocninou p než p^{m+1}; současně nemůže být $\binom{n}{k}$ větší mocninou p než p^m podle (3.7.2). □

V článku [18] dokázal autor větu 3.7.1 s využitím Kummerovy věty. Proveďme totéž!

Příklad 3.7.2. Použijte Kummerovu větu k důkazu věty 3.7.1.

Zvolme $m \in \mathbb{N}$ tak, aby pro daná čísla n, p platilo $p^m \leq n < p^{m+1}$. Číslo p^m má v soustavě o základu p stejný počet cifer jako n (tedy $m + 1$), tj. při sčítání čísel $k \in \{1, \ldots, n-1\}$ a $n - k$ dochází k nejvýše m přenosům. Podle Kummerovy věty je tedy

$$\epsilon_p\left(\binom{n}{k}\right) \leq m \quad \Rightarrow \quad p^{\epsilon_p(\binom{n}{k})} \leq p^m \leq n. \tag{3.7.3}$$

Pro $1 < k < n - 1$ je $n < \binom{n}{k}$, tedy $p^{\epsilon_p(\binom{n}{k})} < \binom{n}{k}$, proto $\binom{n}{k}$ není mocninou p.

Sekci uzavřeme tvrzením od Pála Erdőse, který dokázal, že kombinační číslo je zřídkakdy mocninou přirozeného čísla (s exponentem > 1), konkrétně $\binom{n}{k}$ může být mocninou pouze pro $3 < k < n - 3$. Důkaz pro jeho rozsah neuvádíme, můžeme jej nalézt například v knize [1].

Věta 3.7.3. ([1, str. 14]) *Rovnice* $\binom{n}{k} = m^l$ *nemá žádné celočíselné řešení pro* $l > 1$ *a* $3 < k < n - 3$.

4. Fibonacciho čísla

4.1 Rekurentní vzorec

Kapitolu o Fibonacciho číslech uvedeme notoricky známou úlohou s králíky, která řešitele na Fibonacciho posloupnost přímo navede (vycházíme z knihy [8]). Mějme pár čerstvě narozených králíků opačného pohlaví. Zajímá nás, jak početnou rodinu (resp. kolik párů) získáme z tohoto jednoho počátečního páru za jeden rok, platí-li tyto zásady:

1) Každý narozený pár (jeden samec a jedna samice) dospěje za 1 měsíc.

2) Dva měsíce po narození páru (tj. 1 měsíc po dosažení dospělosti) a každý další měsíc porodí samice z tohoto páru jeden nový pár králíků (opět samce a samici).

3) Během celého roku nezemře žádný králík.

Pokud budeme řešit úlohu tak, že každý měsíc zapíšeme počet nově narozených párů králíků, počet dospělých párů a celkový počet párů, dostaneme tabulku 4.1. Počet nově narozených párů je vždy roven počtu dospělých párů z předchozího měsíce a počet dospělých párů je roven celkovému počtu párů z předchozího měsíce. To znamená, že celkový počet párů po n měsících, kde $n \geq 2$, je součtem počtu párů po $n-1$ a $n-2$ měsících. Odtud snadno zjistíme, že celkový počet párů po jednom roce je 233.

	Počet nově narozených párů	Počet dospělých párů	Celkový počet párů
Start	1	0	1
Po 1 měsíci	0	1	1
Po 2 měsících	1	1	2
Po 3 měsících	1	2	3
Po 4 měsících	2	3	5
Po 5 měsících	3	5	8
Po 6 měsících	5	8	13
Po 7 měsících	8	13	21
Po 8 měsících	13	21	34
Po 9 měsících	21	34	55
Po 10 měsících	34	55	89
Po 11 měsících	55	89	144
Po 1 roce	89	144	233

Tabulka 4.1: Řešení úlohy s králíky

Posloupnost čísel ve druhém (popřípadě třetím) sloupci tabulky 4.1 je známa jako Fibonacciho posloupnost (druhý a třetí sloupec se liší jen posunutím, definice Fibonacciho posloupnosti jsou v literatuře nejednotné – někdy se začíná nulou, jindy jedničkou). Toto jméno jí však dal Édouard Lucas až v roce 1876. Přezdívka

$F_0 = 0$	$F_5 = 5$	$F_{10} = 55$	$F_{15} = 610$	$F_{20} = 6\,765$
$F_1 = 1$	$F_6 = 8$	$F_{11} = 89$	$F_{16} = 987$	$F_{21} = 10\,946$
$F_2 = 1$	$F_7 = 13$	$F_{12} = 144$	$F_{17} = 1597$	$F_{22} = 17\,711$
$F_3 = 2$	$F_8 = 21$	$F_{13} = 233$	$F_{18} = 2584$	$F_{23} = 28\,657$
$F_4 = 3$	$F_9 = 34$	$F_{14} = 377$	$F_{19} = 4181$	$F_{24} = 46\,368$

Tabulka 4.2: Prvních 25 Fibonacciho čísel

Fibonacci vznikla zkrácením sousloví Filius Bonaccii (v překladu z latiny Bonacciho syn – ten zpopularizoval posloupnost ve své knize Liber Abaci).

Fibonacciho posloupnost $\{F_n\}_{n=0}^{\infty}$ je jednoznačně určena dvěma počátečními členy a rekurentním vzorcem:

$$\begin{aligned} &(1)\ F_0 = 0, F_1 = 1 \\ &(2)\ F_n = F_{n-1} + F_{n-2}, n \geq 2 \end{aligned} \tag{4.1.1}$$

S užitím rekurentní definice nalezneme prvních 25 Fibonacciho čísel, viz tabulku 4.2.

4.2 Dělitelnost Fibonacciho čísel

V této sekci se podíváme na některé jednoduché vlastnosti Fibonacciho čísel týkající se dělitelnosti. Začneme velmi důležitým tvrzením o nesoudělnosti dvou po sobě jdoucích Fibonacciho čísel. Při pozorování tabulky 4.2 přirozeně dojdeme k hypotéze, že každá dvě po sobě jdoucí Fibonacciho čísla jsou nesoudělná, tj. největší společný dělitel dvou po sobě jdoucích Fibonacciho čísel je 1. Největšího společného dělitele dvou přirozených čísel m, n budeme nadále značit NSD(m,n), platí tedy např. NSD(F_5,F_6) = NSD(5, 8) = 1.

Věta 4.2.1. ([8, str. 8]) *Pro $n \in \mathbb{N}_0$ platí* NSD(F_n,F_{n+1}) = 1.

Důkaz. Snadno se přesvědčíme, že věta platí pro $n = 0$, tedy NSD(F_0,F_1) = NSD(0,1) = 1. Předpokládejme nyní, že tvrzení neplatí, tj. existuje nejmenší $r > 0$, pro které NSD(F_r,F_{r+1}) > 1. Existuje tedy přirozené $d > 1$, které je dělitelem čísel F_r i F_{r+1}. Pro Fibonacciho čísla platí $F_{r+1} = F_r + F_{r-1}$, z čehož vyplývá, že pokud d dělí F_r i F_{r+1}, potom musí být i dělitelem čísla F_{r-1}. Tedy platí NSD(F_{r-1},F_r) > 1, což je v rozporu s předpokladem, že r je nejmenší číslo, pro které tvrzení neplatí.

□

Stejným způsobem můžeme snadno odvodit velmi podobnou vlastnost Fibonacciho čísel, kterou též zformulujeme jako větu.

Věta 4.2.2. ([8, str. 8]) *Pro $n \in \mathbb{N}_0$ platí* NSD(F_n,F_{n+2}) = 1.

Dokážeme ještě jednu vlastnost Fibonacciho čísel týkající se dělitelnosti:

Věta 4.2.3. ([8, str. 9]) *Součet šesti po sobě jdoucích Fibonacciho čísel je vždy dělitelný* 4. *Navíc pro pevně zvolené $n \in \mathbb{N}_0$ platí:*

$$\sum_{r=0}^{5} F_{n+r} = F_n + F_{n+1} + F_{n+2} + F_{n+3} + F_{n+4} + F_{n+5} = 4F_{n+4} \tag{4.2.1}$$

Důkaz.

$$\begin{aligned}\sum_{r=0}^{5} F_{n+r} &= F_n + F_{n+1} + F_{n+2} + F_{n+3} + F_{n+4} + F_{n+5} \\ &= (F_n + F_{n+1}) + F_{n+2} + F_{n+3} + F_{n+4} + (F_{n+3} + F_{n+4}) \\ &= 2F_{n+2} + 2F_{n+3} + 2F_{n+4} = 2(F_{n+2} + F_{n+3}) + 2F_{n+4} \\ &= 4F_{n+4}\end{aligned} \tag{4.2.2}$$

□

Podobným způsobem bychom mohli odvodit i následující tvrzení:

Věta 4.2.4. ([8, str. 9]) *Součet deseti po sobě jdoucích Fibonacciho čísel je vždy dělitelný* 11. *Navíc pro pevně zvolené* $n \in \mathbb{N}_0$ *platí:*

$$\sum_{r=0}^{9} F_{n+r} = 11F_{n+6} \tag{4.2.3}$$

Poznamenejme ještě, že věty 4.2.3 a 4.2.4 platí nejen pro Fibonacciho posloupnost, ale také pro každou posloupnost čísel $\{a_n\}_{n=0}^{\infty}$, která splňuje rekurentní vztah $a_n = a_{n-1} + a_{n-2}$ pro $n \geq 2$, což je patrné z důkazu věty 4.2.3.

4.3 Dláždění

V této sekci kombinatoricky odvodíme některé užitečné vlastnosti Fibonacciho čísel související s dělitelností. Úlohy, které nás k těmto zajímavým výsledkům dovedou, se týkají určování počtu způsobů, jak lze vydláždit obdélník o daných rozměrech dlaždicemi určitého typu.

Příklad 4.3.1. ([8, str. 33]) Začněme s obdélníkem o rozměrech $2 \times n$ pro $n \geq 1$. Chceme takový obdélník pokrýt dlaždicemi o rozměrech 1×2 (horizontálními), které však můžeme rovněž použít jako dlaždice o rozměrech 2×1 (vertikální). Dlaždice se navzájem nesmějí překrývat.

Pro $n \geq 1$ označme q_n počet možností, kterými lze pokrýt obdélník o rozměrech $2 \times n$ dlaždicemi o rozměrech 1×2 nebo 2×1. Zřejmě $q_1 = 1$, na pokrytí obdélníka 2×1 potřebujeme dlaždici 2×1. Pokrytí obdélníka 2×2 lze provést dvěma způsoby, a to buď použitím dvou dlaždic 1×2 (horizontálních), nebo použitím dvou dlaždic 2×1 (vertikálních). Obě možnosti jsou znázorněny na obrázku 4.1(a). Tedy $q_2 = 2$. Pro $n \geq 3$ se zamysleme nad možnostmi pokrytí prvního sloupce obdélníka $2 \times n$. Snadno zjistíme, že existují dvě možnosti:

(i) Pokryjeme tento sloupec dlaždicí 2×1 (vertikální). Potom zbývající část obdélníka o rozměrech $2 \times (n-1)$ může být pokryta q_{n-1} způsoby, viz obrázek 4.1(b).

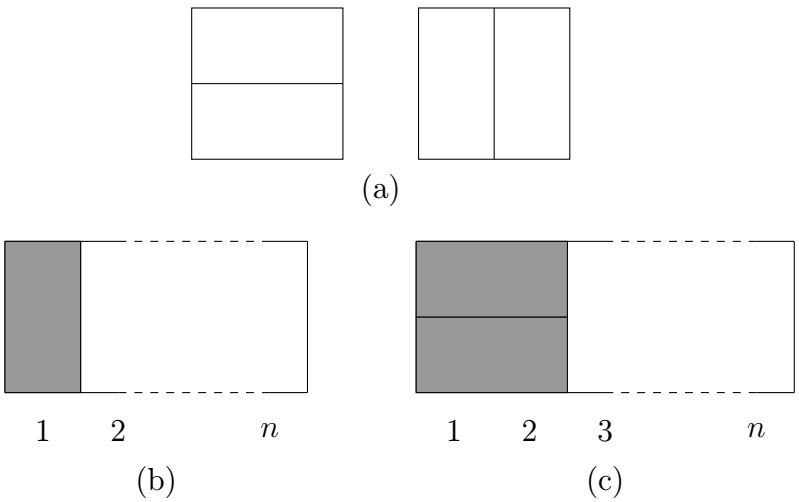
(ii) Pokryjeme tento sloupec levými polovinami dvou dlaždic 1×2 (horizontálních) umístěných nad sebou. Tyto dlaždice současně pokryjí i druhý sloupec obdélníka zleva, zbývá tedy pokrýt ještě obdélník o rozměrech $2 \times (n-2)$, což lze provést q_{n-2} způsoby, viz obrázek 4.1(c).

Jiné možnosti než ty popsané v (i) a (ii) neexistují a žádné pokrytí nemůže být zároveň zahrnuto v případu (i) i v případu (ii), proto platí:

$$q_n = q_{n-1} + q_{n-2} \quad \text{pro} \quad n \geq 3,\ q_1 = 1,\ q_2 = 2. \tag{4.3.1}$$

Protože $q_1 = F_2$, $q_2 = F_3$ a každý další člen posloupnosti $\{q_n\}$ je součtem předchozích dvou členů, musí platit

$$q_n = F_{n+1},\ n \geq 1. \tag{4.3.2}$$



Obrázek 4.1: Znázornění možností dláždění v příkladu 4.3.1

Uveďme ještě jeden jednoduchý, v podstatě analogický, leč méně tradiční příklad.

Příklad 4.3.2. ([8, str. 34]) Nechť je dán obdélník o rozměrech $1 \times n$, který chceme vydláždit použitím dlaždic dvou typů, a to čtvercovými o rozměrech 1×1 a obdélníkovými o rozměrech 1×2. Označme l_n počet možností, jak vydláždit obdélník o rozměrech $1 \times n$. Zřejmě $l_1 = 1$, $l_2 = 2$.

Abychom odvodili rekurentní vzorec pro l_n, uvažme, jakými způsoby může být pokryto první pole obdélníka pro $n \geq 3$:

(i) První pole bude pokryto čtvercovou dlaždicí, viz obr. 4.2(a). Potom zbývá pokrýt obdélník $1 \times (n-1)$, což lze provést l_{n-1} způsoby.

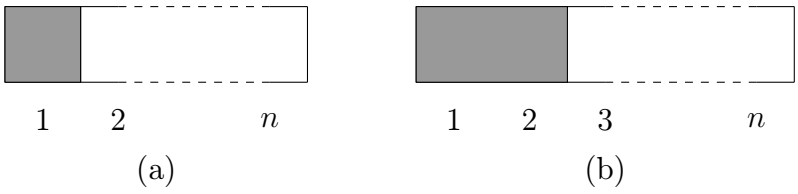
(ii) První pole bude pokryto obdélníkovou dlaždicí, která současně pokryje i druhé pole, viz obr. 4.2(b). Potom zbývá pokrýt obdélník $1 \times (n-2)$, což lze provést l_{n-2} způsoby.

Jiné možnosti než ty popsané v (i) a (ii) neexistují a žádné pokrytí nemůže být zároveň zahrnuto v případu (i) i v případu (ii), proto platí:

$$l_n = l_{n-1} + l_{n-2} \quad \text{pro} \quad n \geq 3, \quad l_1 = 1,\ l_2 = 2, \tag{4.3.3}$$

tedy

$$l_n = F_{n+1},\ n \geq 1. \tag{4.3.4}$$



Obrázek 4.2: Znázornění možností dláždění v příkladu 4.3.2

Poznamenejme, že existuje jednoduchá souvislost mezi dlážděními v příkladech 4.3.1 a 4.3.2. Dláždění z příkladu 4.3.2 získáme rozdělením velkého obdélníku $2 \times n$ (viz obr. 4.1(b,c)) na dvě stejné části podle vodorovné osy.

Nyní zformulujeme další tvrzení o Fibonacciho číslech, které dokážeme kombinatoricky s využitím znalostí nabytých při řešení příkladu 4.3.2.

Věta 4.3.3. ([8, str. 36]) *Pro $m \geq 1$ a $n \geq 0$ platí:*

$$F_{n+m} = F_m F_{n+1} + F_{m-1} F_n. \tag{4.3.5}$$

Důkaz. Pro $n = 0$ je $F_n = F_0 = 0$ a $F_{n+1} = F_1 = 1$, v takovém případě zřejmě platí (4.3.5) pro každé $m \geq 1$. Pokud je $m = 1$, potom $F_m = F_1 = 1$ a $F_{m-1} = F_0 = 0$, v takovém případě platí (4.3.5) pro každé $n \geq 1$. Nadále tedy předpokládejme, že $m \geq 2$ a $n \geq 1$.

Uvažme obdélník o rozměrech $1 \times (n + m - 1)$, viz obrázek 4.3(a). Podle výsledku z příkladu 4.3.2 lze takový obdélník pokrýt $F_{(n+m-1)+1} = F_{n+m}$ způsoby s použitím dvou typů dlaždic, a to o rozměrech 1×1 a 1×2. Nyní určíme počet možných pokrytí takového obdélníka jiným způsobem – budeme sledovat, jaké jsou možnosti pokrytí n-tého pole obdélníka (počítáno zleva).

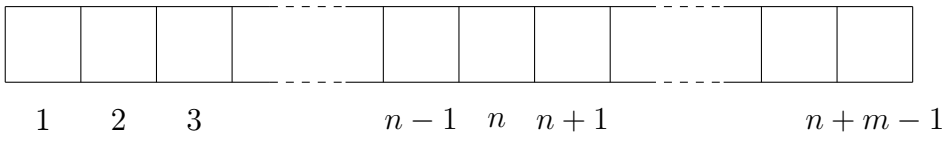
(i) Přepokládejme, že n-té pole obdélníka je pokryto obdélníkovou dlaždicí, která současně pokrývá i pole $n+1$, viz obrázek 4.3(b). Existuje $F_{(n-1)+1} = F_n$ možností, jak pokrýt část obdélníka nalevo od sledovaného n-tého pole (tj. pole 1 až $n-1$). Dále existuje $F_{((n+m-1)-(n+1))+1} = F_{m-1}$ možností, jak pokrýt část obdélníka napravo od pole $n+1$ (tj. pole $n+2$ až $n+m-1$, kterých je $(n+m-1)-(n+1) = m-2$). Celkem je tedy $F_{m-1}F_n$ možností, jak pokrýt pole vlevo a vpravo.

(ii) Při jakémkoli jiném pokrytí jsou pole n a $n+1$ „oddělená“, přesněji řečeno každé je pokryto jinou dlaždicí, viz obrázek 4.3(c). Počet možných pokrytí levé části obdélníka, tedy včetně n-tého pole, je F_{n+1}. Počet možností, jak pokrýt pravou část, tedy od pole $n+1$ až do $n+m-1$, je $F_{((n+m-1)-n)+1} = F_m$. Celkem tedy existuje $F_m F_{n+1}$ možností, jak pokrýt celý obdélník za předpokladu, že jsou pole n a $n+1$ pokryta různými dlaždicemi.

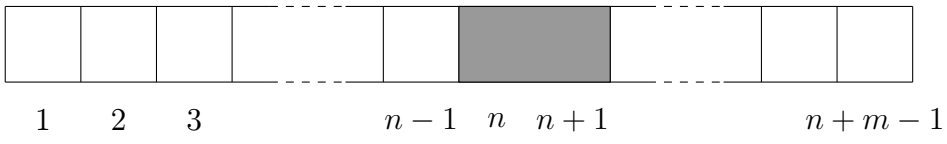
Zvážením případů (i) a (ii) jsme zahrnuli všechna možná pokrytí, přičemž žádné pokrytí nemůže být zároveň zahrnuto v případu (i) i v případu (ii). Proto počet všech možností, jak pokrýt obdélník o rozměrech $1 \times (n + m - 1)$, je $F_m F_{n+1} + F_{m-1} F_n$. Odtud dostáváme rovnost (4.3.5).

□

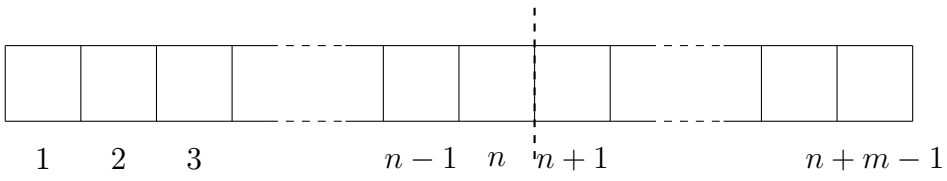
Jako důsledky věty 4.3.3 dostáváme následující tvrzení.



(a)



(b)



(c)

Obrázek 4.3: Znázornění možností dláždění obdélníka $1 \times (n + m - 1)$

(i) Pokud $n = m \geq 1$, platí

$$\begin{aligned} F_{2n} = F_{n+n} &= F_n F_{n+1} + F_{n-1} F_n \\ &= F_n (F_{n+1} + F_{n-1}), \end{aligned} \tag{4.3.6}$$

tedy F_n dělí F_{2n} pro $n \geq 1$.

(ii) Jelikož

$$F_{3n} = F_{n+2n} = F_{2n} F_{n+1} + F_{2n-1} F_n \tag{4.3.7}$$

a F_n dělí F_{2n}, platí také, že F_n dělí F_{3n}.

(iii) Obecně pro $n \geq 1$, $k \geq 1$ platí

$$F_{(k+1)n} = F_{n+kn} = F_{kn} F_{n+1} + F_{kn-1} F_n. \tag{4.3.8}$$

Tedy pokud F_n dělí F_{kn}, pak dělí i $F_{(k+1)n}$.

(iv) Indukcí podle k pro pevné $n \geq 1$ z (i) a (iii) plyne, že F_n dělí F_{kn} pro $k \geq 2$, přičemž tento výsledek zřejmě platí i pro $k = 1$.

Výsledek z (iv) zformulujeme jako větu.

Věta 4.3.4. ([8, str. 38]) *Pro $n \geq 1$, $m \geq 1$*

$$F_m \text{ dělí } F_{mn}. \tag{4.3.9}$$

4.4 Největší společný dělitel Fibonacciho čísel

V této sekci zformulujeme stěžejní větu kapitoly o Fibonacciho číslech a jejich dělitelnosti. Než tak učiníme, předvedeme dva motivační příklady.

(i)

$$\begin{aligned} \mathrm{NSD}(F_8, F_{12}) &= \mathrm{NSD}(21, 144) = \mathrm{NSD}(3 \cdot 7, 2^4 \cdot 3^2) \\ &= 3 = F_4 = F_{\mathrm{NSD}(8,12)} \end{aligned} \tag{4.4.1}$$

(ii)

$$\begin{aligned} \mathrm{NSD}(F_{12}, F_{18}) &= \mathrm{NSD}(144, 2\,584) = \mathrm{NSD}(2^4 \cdot 3^2, 2^3 \cdot 17 \cdot 19) \\ &= 2^3 = 8 = F_6 = F_{\mathrm{NSD}(12,18)} \end{aligned} \tag{4.4.2}$$

Rovnosti (4.4.1) a (4.4.2) napovídají, že platí:

Věta 4.4.1. ([8, str. 121]) *Pro* $m \geq n \geq 1$

$$\mathrm{NSD}(F_m, F_n) = F_{\mathrm{NSD}(m,n)}. \tag{4.4.3}$$

Důkazu věty 4.4.1 předešleme tři lemmata a využijeme některá tvrzení odvozená v předchozích sekcích této kapitoly. V sekci 4.3 jsme odvodili větu 4.3.4, která říká, že F_m dělí F_{mn} pro $m \geq 1, n \geq 1$. Toto tvrzení využijeme při dokazování následujícího lemmatu.

Lemma 4.4.2. ([8, str. 122]) *Pro* $q \geq 1, n \geq 1$ *platí* $\mathrm{NSD}(F_{qn-1}, F_n) = 1$.

Důkaz. Buď $d = \mathrm{NSD}(F_{qn-1}, F_n)$. Potom d dělí F_{qn-1} a F_n. Podle věty 4.3.4 také d dělí F_{qn}. Tedy d je dělitelem obou po sobě jdoucích Fibonacciho čísel F_{qn-1} a F_{qn}. Podle věty 4.2.1 je největším společným dělitelem dvou po sobě jdoucích Fibonacciho čísel 1. Proto $\mathrm{NSD}(F_{qn-1}, F_n) = d = 1$.

□

Následující lemma demonstruje vlastnost týkající se největšího společného dělitele dvou čísel obecně.

Lemma 4.4.3. ([8, str. 123]) *Nechť jsou* a, b, c *přirozená čísla a nechť* $\mathrm{NSD}(a, c) = 1$. *Pak* $\mathrm{NSD}(ab, c) = \mathrm{NSD}(b, c)$.

Důkaz. Nechť je $d_1 = \mathrm{NSD}(b, c)$ a $d_2 = \mathrm{NSD}(ab, c)$. Číslo d_1 je dělitelem b, tedy je i dělitelem ab. Současně je také d_1 dělitelem c. Tedy d_1 dělí d_2.

Nyní chceme ještě dokázat, že d_2 dělí d_1. Zvažme dva případy:

(i) d_2 dělí a: Číslo d_2 dělí c, takže vzhledem k nesoudělnosti a a c je $d_2 = 1$.

(ii) d_2 nedělí a: Číslo d_2 dělí c, tedy nemůže dělit $|a-c|$. Je ale dělitelem bc i ab, tedy i $b\,|c-a|$. Vzhledem k nesoudělnosti a a $|c-a|$ musí být d_2 dělitelem b. Tedy d_2 dělí d_1.

Jelikož d_1 dělí d_2 a d_2 dělí d_1 a obě čísla jsou přirozená, musí platit $d_1 = d_2$, tedy $\mathrm{NSD}(ab, c) = \mathrm{NSD}(b, c)$.

□

Lemma 4.4.4. ([8, str. 123]) *Nechť jsou m, n přirozená čísla splňující $m = qn+r$, kde q je přirozené číslo a $r \in \{0, \ldots, n-1\}$. Potom*

$$\mathrm{NSD}(F_m, F_n) = \mathrm{NSD}(F_n, F_r). \tag{4.4.4}$$

Důkaz. Podle věty 4.3.3 je

$$\mathrm{NSD}(F_m, F_n) = \mathrm{NSD}(F_{qn+r}, F_n) = \mathrm{NSD}(F_{qn}F_{r+1} + F_{qn-1}F_r, F_n). \tag{4.4.5}$$

Nechť jsou $h = \mathrm{NSD}(F_{qn}F_{r+1} + F_{qn-1}F_r, F_n)$ a $k = \mathrm{NSD}(F_{qn-1}F_r, F_n)$. Potom h dělí $F_{qn}F_{r+1} + F_{qn-1}F_r$ a současně F_n. Podle věty 4.3.4 dělí i F_{qn}, tudíž dělí i $F_{qn}F_{r+1}$. Jelikož h je dělitelem čísla $F_{qn}F_{r+1}$ i čísla $F_{qn}F_{r+1} + F_{qn-1}F_r$, musí být h rovněž dělitelem $F_{qn-1}F_r$. Tudíž h dělí k.

Podobně, k dělí $F_{qn-1}F_r$ a současně F_n. Podle věty 4.3.4 dělí i F_{qn}, tudíž dělí i $F_{qn}F_{r+1}$. Jelikož k je dělitelem čísla $F_{qn-1}F_r$ i čísla $F_{qn}F_{r+1}$, musí být k rovněž dělitelem čísla $F_{qn}F_{r+1} + F_{qn-1}F_r$. Tudíž k dělí h. Čísla h, k jsou přirozená, proto $h = k$.

Víme tedy, že platí

$$\mathrm{NSD}(F_m, F_n) = \mathrm{NSD}(F_{qn}F_{r+1} + F_{qn-1}F_r, F_n) = \mathrm{NSD}(F_{qn-1}F_r, F_n). \tag{4.4.6}$$

Podle lemmatu 4.4.2 je $\mathrm{NSD}(F_{qn-1}, F_n) = 1$. Z lemmatu 4.4.3 proto vyplývá, že $\mathrm{NSD}(F_{qn-1}F_r, F_n) = \mathrm{NSD}(F_r, F_n) = \mathrm{NSD}(F_n, F_r)$. Odtud a z (4.4.6) dostáváme (4.4.4).

□

Nyní jsme připraveni dokázat větu 4.4.1. Poznamenejme ještě, že lemmata 4.4.2, 4.4.3 a 4.4.4 neslouží jen k dokázání věty 4.4.1, nýbrž se jedná o obecné výsledky, se kterými se můžeme seznámit při studiu teorie čísel a abstraktní algebry [8, str. 123].

Nechť jsou m, n přirozená čísla a $m \geq n$. Budeme-li hledat jejich největšího společného dělitele pomocí Eukleidova algoritmu, dostaneme rovnosti

$$\begin{aligned}
m &= q_1 n + r_1, && 0 \leq r_1 < n \\
n &= q_2 r_1 + r_2, && 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, && 0 \leq r_3 < r_2 \\
&\vdots \\
r_{k-2} &= q_k r_{k-1} + r_k, && 0 \leq r_k < r_{k-1} \\
r_{k-1} &= q_{k+1} r_k,
\end{aligned} \tag{4.4.7}$$

přičemž $\mathrm{NSD}(m,n) = \mathrm{NSD}(n,r_1) = \mathrm{NSD}(r_1,r_2) = \cdots = \mathrm{NSD}(r_{k-1},r_k) = r_k$.

Z lemmatu 4.4.4 odvozujeme

$$\begin{aligned}
\mathrm{NSD}(F_m, F_n) &= \mathrm{NSD}(F_{q_1 n + r_1}, F_n) \\
&= \mathrm{NSD}(F_n, F_{r_1}) \\
&= \mathrm{NSD}(F_{q_2 r_1 + r_2}, F_{r_1}) \\
&= \mathrm{NSD}(F_{r_1}, F_{r_2}) \\
&= \mathrm{NSD}(F_{q_3 r_2 + r_3}, F_{r_2}) \\
&= \mathrm{NSD}(F_{r_2}, F_{r_3}) \\
&\quad \vdots \\
&= \mathrm{NSD}(F_{q_k r_{k-1} + r_k}, F_{r_{k-1}}) \\
&= \mathrm{NSD}(F_{r_{k-1}}, F_{r_k}).
\end{aligned} \tag{4.4.8}$$

Jelikož r_k dělí r_{k-1}, podle věty 4.3.4 také F_{r_k} dělí $F_{r_{k-1}}$. Tedy platí

$$\mathrm{NSD}(F_m, F_n) = \mathrm{NSD}(F_{r_{k-1}}, F_{r_k}) = F_{r_k} = F_{\mathrm{NSD}(m,n)}, \tag{4.4.9}$$

čímž je věta 4.4.1 dokázána.

Na závěr této sekce ukážeme, jak věta 4.4.1 zjednoduší hledání největšího společného dělitele dvou Fibonacciho čísel.

Příklad 4.4.5. ([8, str. 124]) Nalezněme největšího společného dělitele Fibonacciho čísel F_{30} a F_{70}, nejdříve s pomocí rozkladu na součin prvočísel. Dá trochu zabrat, než zjistíme, že

$$\begin{aligned}
F_{30} &= 832\,040 = 2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61, \\
F_{70} &= 190\,392\,490\,709\,135 = 5 \cdot 11 \cdot 13 \cdot 29 \cdot 71 \cdot 911 \cdot 141\,961.
\end{aligned} \tag{4.4.10}$$

Z prvočíselných rozkladů v (4.4.10) je vidět, že

$$\mathrm{NSD}(F_{30}, F_{70}) = 5 \cdot 11 = 55. \tag{4.4.11}$$

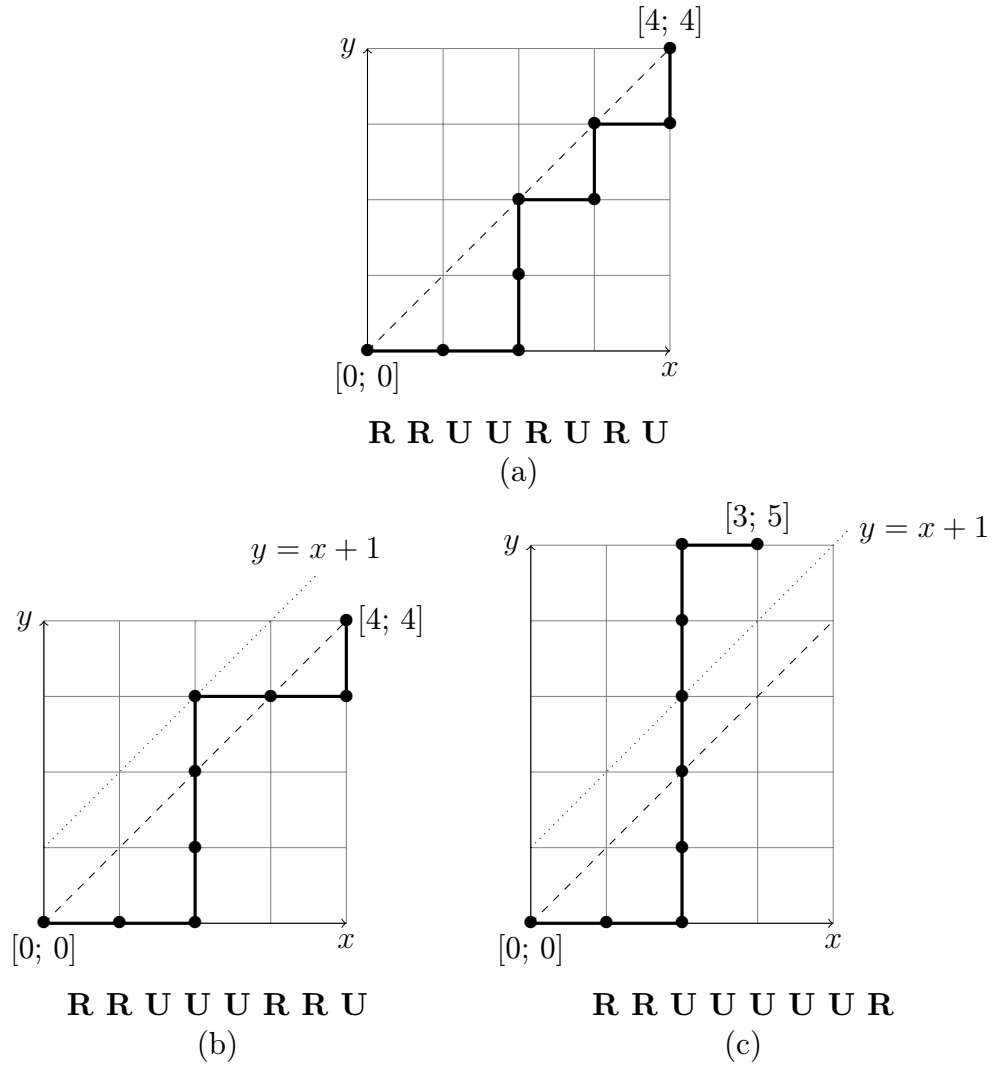
S využitím věty 4.4.1 můžeme faktorizaci zadaných Fibonacciho čísel, ba dokonce hledání jejich přesných hodnot, přeskočit, jelikož víme, že platí

$$\mathrm{NSD}(F_{30}, F_{70}) = F_{\mathrm{NSD}(30,70)} = F_{10} = 55. \tag{4.4.12}$$

5. Catalanova čísla

5.1 Úvodní příklad

Mezi významné kombinatorické posloupnosti patří tzv. Catalanova čísla, která vyplynou na povrch při řešení mnoha populárních kombinatorických úloh. Uveďme na úvod pěkné kombinatorické řešení jedné z nich.



Obrázek 5.1: Zobrazení cest z příkladu 5.1.1

Příklad 5.1.1. ([8, str. 150]) Nechť je dána jednotková mřížka v kartézské soustavě souřadnic. Nacházíme se v bodě o souřadnicích $[0; 0]$ a chceme určit, kolika způsoby se můžeme dostat do bodu o souřadnicích $[4; 4]$, jestliže se pohyb v mřížce řídí následujícími pravidly:

(i) V každém kroku se můžeme pohybovat dvěma způsoby – buď o jednotku v kladném směru osy x (tedy „doprava“), nebo o jednotku v kladném směru osy y (tedy „nahoru“).

(ii) Nikdy se nesmíme dostat „nad“ přímku s rovnicí $y = x$, tj. v žádném kroku se nemůžeme nacházet v bodě $[x; y]$, pro který je $y > x$. Tedy v momentě, kdy se nacházíme v některém z bodů $[0; 0], [1; 1], [2; 2], [3; 3]$, je povolen pohyb pouze ve směru osy x.

Příklad povolené cesty vidíme na obrázku 5.1(a). Pro zápis cesty z $[0; 0]$ do $[4; 4]$ definujme symboly:

R pro pohyb ve směru osy x, tj. **R**: $[x; y] \to [x + 1; y]$,

U pro pohyb ve směru osy y, tj. **U**: $[x; y] \to [x; y + 1]$.

Cestu na obrázku 5.1(a) zapíšeme jako sekvenci kroků **R R U U R U R U**.

V zápisu libovolné cesty z bodu $[0; 0]$ do bodu $[4; 4]$ (podle stanovených pravidel), se zřejmě vždy objeví čtyřikrát symbol **R** a čtyřikrát symbol **U**. Celkový počet způsobů, jak uspořádat řetězec čtyř **R** a čtyř **U**, je

$$\frac{8!}{4! \cdot 4!} = \binom{8}{4} = 70, \tag{5.1.1}$$

což odpovídá počtu způsobů, jak se dostat z bodu $[0; 0]$ do bodu $[4; 4]$, pokud ignorujeme pravidlo (ii) o nepřekročení přímky $y = x$. Pokud nalezneme počet všech cest, které právě pravidlo (ii) porušují, odečtením získáme řešení úlohy.

Definujme nyní transformaci, která se týká cest z bodu $[0; 0]$ do bodu $[4; 4]$, které porušují právě pravidlo (ii). Každou takovou cestu transformujeme tak, že od okamžiku, kdy překročí přímku $y = x$, ji začneme zrcadlit podél přímky $y = x+1$. Například transformací cesty z obrázku 5.1(b) dostáváme cestu vyobrazenou na 5.1(c). Výsledkem transformace je vždy cesta z bodu $[0; 0]$ do bodu $[3; 5]$. Sledujme, co se při transformaci cesty z obrázku 5.1(b) na cestu v 5.1(c) stalo s jejím symbolickým zápisem:

$$\mathbf{R\ R\ U\ U\ U} \mid \mathbf{R\ R\ U} \leftrightarrow \mathbf{R\ R\ U\ U\ U} \mid \mathbf{U\ U\ R}. \tag{5.1.2}$$

Po přečtení pátého symbolu zleva, který zaznamenává překročení přímky $x = y$, jsme zaměnili všechny následující symboly **R** za **U** a naopak (transformovaná část řetězce je oddělená svislou čarou). Jelikož je výsledkem transformace cesta z bodu $[0; 0]$ do bodu $[3; 5]$, symbolický zápis výsledné cesty musí obsahovat 5 symbolů **U** a 3 symboly **R**.

Ukázali jsme, jak lze každou cestu z bodu $[0; 0]$ do bodu $[4; 4]$, která porušuje právě pravidlo (ii), jednoznačně „přetransformovat“ na některou cestu z bodu $[0; 0]$ do bodu $[3; 5]$ dodržující pravidlo (i). Nyní ještě ukážeme, že každá cesta z bodu $[0; 0]$ do bodu $[3; 5]$, která respektuje pravidlo (i), může být jednoznačně „přetransformována“ na některou z cest z bodu $[0; 0]$ do bodu $[4; 4]$, která porušuje pravidlo (ii).

Uvažme libovolnou cestu z bodu $[0; 0]$ do bodu $[3; 5]$, která respektuje pravidlo (i). Jelikož se bod $[3; 5]$ nachází nad přímkou $y = x$, musí existovat krok, při kterém cesta poprvé vystoupí nad přímku $y = x$. Po tomto kroku budeme zbytek cesty zrcadlit podle přímky $y = x + 1$, tedy provádíme transformaci, jejímž výsledkem je cesta z $[0; 0]$ do $[4; 4]$. Navíc jsme zachovali krok, ve kterém cesta poprvé vystoupila nad přímku $y = x$, tudíž výsledná cesta splňuje (i), ale porušuje (ii).

Dokázali jsme existenci vzájemně jednoznačného vztahu mezi cestami z $[0;0]$ do $[4;4]$, které porušují právě pravidlo (ii), a cestami z $[0;0]$ do $[3;5]$, které dodržují pravidlo (i). Jejich počty se tedy rovnají. Počet cest z $[0;0]$ do $[3;5]$, které dodržují pravidlo (i), určíme jako počet způsobů, jak lze uspořádat pět symbolů **U** a tři symboly **R**. Hledaný počet všech cest z $[0;0]$ do $[4;4]$, které splňují pravidla (i) a (ii), je tedy

$$\binom{8}{4} - \binom{8}{3} = 70 - 56 = 14. \tag{5.1.3}$$

Pokud zobecníme příklad 5.1.1 na hledání počtu cest z bodu $[0;0]$ do bodu $[n;n]$ pro $n \geq 0$, řešením je n-té Catalanovo číslo ([8, str. 152]), tedy číslo

$$C_n = \binom{2n}{n} - \binom{2n}{n-1} \quad \text{pro} \quad n \geq 1, \quad C_0 = 1. \tag{5.1.4}$$

Předpis pro n-té Catalanovo číslo ještě upravíme:

$$\begin{aligned} \binom{2n}{n} - \binom{2n}{n-1} &= \binom{2n}{n} - \frac{(2n)!}{(n-1)! \cdot (n+1)!} \\ &= \binom{2n}{n} - \frac{(2n)! \cdot n}{n! \cdot n! \cdot (n+1)} \\ &= \binom{2n}{n} \cdot \left(1 - \frac{n}{n+1}\right) = \frac{1}{n+1}\binom{2n}{n}. \end{aligned} \tag{5.1.5}$$

Další z možných definic posloupnosti Catalanových čísel je tedy

$$C_n = \frac{1}{n+1}\binom{2n}{n} \quad \text{pro} \quad n \geq 0. \tag{5.1.6}$$

n	0	1	2	3	4	5	6	7
C_n	1	1	2	5	14	42	132	429
n	8	9	10	11	12	13	14	15
C_n	1 430	4 862	16 796	58 786	208 012	742 900	2 674 440	9 694 845

Tabulka 5.1: Tabulka Catalanových čísel pro malá n

Hodnoty pro prvních 16 Catalanových čísel najdeme v tabulce 5.1.

Mezi další klasické úlohy vedoucí na Catalanova čísla patří nalezení počtu různých triangulací konvexního mnohoúhelníka. Leonhard Euler roku 1751 ukázal, že pro $n \in \mathbb{N}$ je C_n počet způsobů, jak rozdělit konvexní $(n+2)$-úhelník na trojúhelníky neprotínajícími se úhlopříčkami. Elegantní kombinatorický důkaz správnosti tohoto řešení podal v roce 1838 Gabriel Lamé, jehož úvahy dále rozvedl Eugène Charles Catalan ve svých článcích z let 1838 a 1839 ([8, str. 52]).

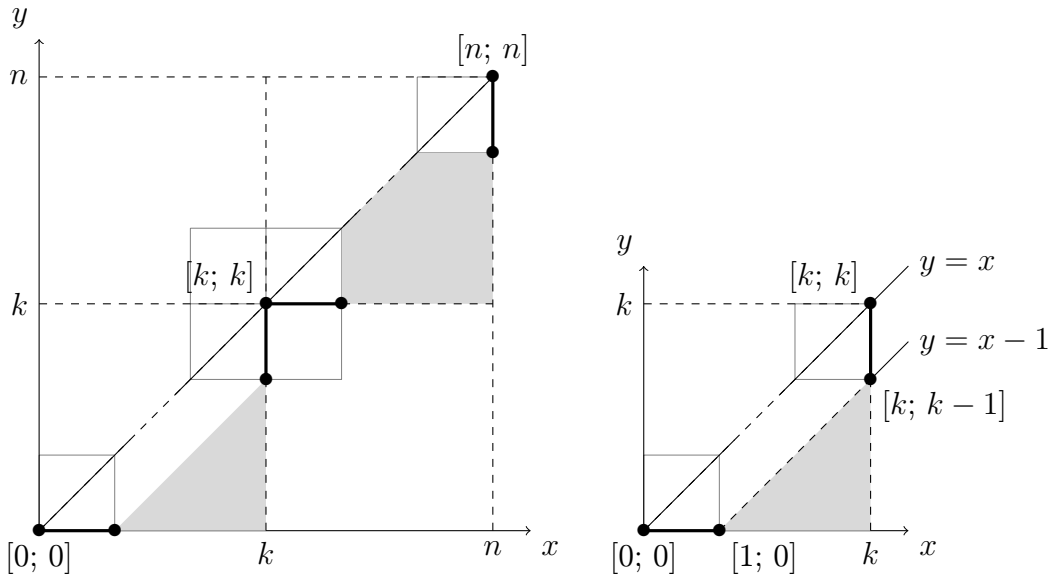
Další úlohy vedoucí na Catalanova čísla lze najít v [8].

5.2 Rekurentní vzorec

V předchozí sekci jsme definovali n-té Catalanovo číslo C_n pomocí vzorce (5.1.6), ke kterému jsme dospěli při řešení kombinatorické úlohy. V této sekci se

vrátíme k úloze o cestách v mřížové síti a odvodíme rekurentní vzorec pro C_n, který využijeme v následující sekci při odvozování některých poznatků o dělitelnosti Catalanových čísel.

Opět budeme uvažovat cesty z bodu $[0;0]$ do $[n;n]$, $n \in \mathbb{N}_0$, které se skládají pouze z kroků **R**: $[x;y] \to [x+1;y]$, **U**: $[x;y] \to [x;y+1]$, a nikdy nevystoupí nad přímku $y = x$, tj. splňují pravidla (i), (ii) popsaná v příkladu 5.1.1 ([8, str. 231]).



Šedá pole naznačují oblasti, ve kterých se mohou neznámé části cesty nacházet.

Obrázek 5.2: Rozdělení cesty z $[0;0]$ do $[n;n]$ podle $[k;k]$

Víme, že C_n udává počet cest, které vedou z $[0;0]$ do $[n;n]$ a splňují pravidla (i), (ii). Zvolme libovolnou takovou cestu a zaměřme se na bod, ve kterém se tato cesta poprvé po opuštění bodu $[0;0]$ dotkne přímky $y = x$. Tento bod, jehož souřadnice označíme $[k;k]$, rozdělí cestu z $[0;0]$ do $[n;n]$ na dvě části (viz obrázek 5.2(a)):

- cesta z $[0;0]$ do $[k;k]$:

  Určíme, jaký je počet možností, jak se dostat z $[0;0]$ do $[k;k]$, jestliže se uvažovaná cesta nesmí dotknout přímky $y = x$ (vyjma bodů $[0;0]$ a $[k;k]$). První krok uvažované cesty musí být **R** a poslední **U**. Musí platit, že v žádném kroku cesta nevystoupá nad přímku $y = x - 1$ (jinak by se dotkla přímky $y = x$, viz obrázek 5.2(b)). Každá cesta z $[1;0]$ do $[k;k-1]$, která nevystoupá nad přímku $y = x - 1$, odpovídá cestě z $[0;0]$ do $[k-1;k-1]$, která nevystoupá nad přímku $y = x$, tedy splňuje pravidlo (ii) (stačí celou cestu z $[1;0]$ do $[k;k-1]$ posunout o jednotkovou vzdálenost doleva, tj. snížit všechny x-ové souřadnice o 1). Počet všech cest z $[0;0]$ do $[k-1;k-1]$ splňujících pravidlo (ii) je C_{k-1}. Tedy počet cest z $[0;0]$ do $[k;k]$, které se po opuštění $[0;0]$ dotknou přímky $y = x$ až v bodě $[k;k]$, je taktéž C_{k-1}.

- cesta z $[k;k]$ do $[n;n]$:

Podobným způsobem jako v předchozím případě zjistíme, že počet všech cest z $[k;k]$ do $[n;n]$ splňujících (ii) je roven počtu cest z $[0;0]$ do $[n-k;n-k]$ splňujících (ii), tedy C_{n-k}.

Analýzou obou částí cesty zjišťujeme, že počet cest z $[0;0]$ do $[n;n]$, které se poprvé po opuštění bodu $[0;0]$ dotknou přímky $y=x$ v bodě $[k;k]$ a splňují (ii), je $C_{k-1}\cdot C_{n-k}$. Jelikož k může nabývat hodnot $1,\ldots,n$, počet všech cest z $[0;0]$ do $[n;n]$ splňujících pravidla (i),(ii) je

$$\begin{aligned} C_n &= C_0C_{n-1}+C_1C_{n-2}+\cdots+C_{n-2}C_1+C_{n-1}C_0 \\ &= \sum_{k=1}^{n} C_{k-1}C_{n-k} \quad \text{pro} \quad n\geq 1, \quad C_0=1. \end{aligned} \tag{5.2.1}$$

5.3 Parita a prvočíselnost Catalanových čísel

V této sekci odvodíme, pro která n je C_n liché a pro která n je C_n prvočíslo. Začneme s vyšetřováním parity Catalanových čísel. Podíváme-li se na tabulku 5.1, zjistíme, že mezi prvními 16 Catalanovými čísly jsou lichá C_n pouze pro $n=0$, $n=1$, $n=3$, $n=7$, $n=15$, tedy pro n tvaru 2^k-1 pro $k\geq 0$. Toto pozorování nabádá k formulaci věty, kterou vzápětí dokážeme:

Věta 5.3.1. ([17, str. 52]) *Pro $n\in\mathbb{N}_0$ platí: C_n je liché právě tehdy, když $n=2^k-1$ pro nějaké $k\in\mathbb{N}_0$.*

Důkaz. Zřejmě pro $n=0$ věta platí, neboť $C_0=1$ a $0=2^0-1$. K vyšetření parity C_n pro $n\geq 1$ využijeme rekurentní vzorec (5.2.1). Z něj plyne, že

$$\begin{aligned} &C_n = 2(C_0C_{n-1}+C_1C_{n-2}+\cdots+C_{(n/2)-1}C_{n/2}) \quad \text{pro} \quad n \quad \text{sudé}, \\ &C_n = 2(C_0C_{n-1}+C_1C_{n-2}+\cdots+C_{(n-3)/2}C_{(n+1)/2})+(C_{(n-1)/2})^2 \quad \text{pro} \quad n \quad \text{liché}. \end{aligned} \tag{5.3.1}$$

Ihned vidíme, že pokud je n sudé, pak i C_n je sudé. Dále vidíme z druhého řádku (5.3.1), že pro n liché je C_n liché, právě když $C_{(n-1)/2}$ je liché. Paritu čísla $C_{(n-1)/2}$ můžeme opět zkoumat pomocí vzorce (5.3.1) atd.; celý proces se dá dobře představit, pokud zapíšeme n ve dvojkové soustavě.

Nechť tedy $n=b_k\cdots b_1b_0$ je dvojkový zápis čísla $n\geq 1$. Pokud $b_0=0$, pak n je sudé a C_n je sudé. Jinak testování lichosti/sudosti C_n převedeme na testování lichosti/sudosti Catalanova čísla s indexem $(n-1)/2=b_k\cdots b_1$ a opakujeme stejný postup. Tento proces může skončit dvěma způsoby:

1) V některém okamžiku se na konci binárního zápisu testovaného čísla poprvé objeví nulová cifra b_i. Pak Catalanovo číslo s indexem $b_k\cdots b_i$ je sudé, a tedy C_n je sudé.

2) Všechny cifry $b_k,\ldots,b_0$ jsou jedničky; to nastane právě tehdy, když $n=2^{k+1}-1$. Pak výše popsaný proces skončí po k krocích, kdy testujeme lichost/sudost Catalanova čísla b_k; to je liché, takže i C_n je liché.

Tedy pro $n \geq 1$ je C_n liché, právě když n je tvaru $n = 2^{k+1} - 1$ pro $k \geq 0$.

□

Poznámka 5.3.2. Čísla tvaru $2^m - 1$ pro $m \geq 0$ jsou známa jako Mersennova čísla. Věta 5.3.1 tedy říká, že pro $n \geq 0$ je C_n liché, právě když je n Mersennovo číslo.

Podíváme-li se pozorněji na tabulku 5.1, zjistíme, že pouze dvě z vypsaných Catalanových čísel jsou prvočísla, a to pro $n = 2$ a $n = 3$. Dokažme, že žádná jiná Catalanova prvočísla neexistují:

Věta 5.3.3. ([17, str. 53]) *Jediná Catalanova prvočísla jsou $C_2 = 2$ a $C_3 = 5$.*

Důkaz. Ze vztahu (5.1.6) odvozujeme

$$\begin{aligned} C_{n+1} &= \frac{1}{n+2}\binom{2n+2}{n+1} = \frac{1}{n+2} \cdot \frac{(2n+2)!}{(n+1)!(n+1)!} \\ &= \frac{1}{n+2} \cdot \frac{(2n)!(2n+1)(2n+2)}{(n!)^2(n+1)(n+1)} \\ &= \frac{1}{n+2} \cdot \frac{(2n)!(2n+1)\cdot 2}{(n!)^2(n+1)} = \frac{1}{n+2}\binom{2n}{n}\frac{4n+2}{n+1} \\ &= \frac{1}{n+2} \cdot C_n \cdot (4n+2), \end{aligned} \tag{5.3.2}$$

tedy

$$(n+2)C_{n+1} = (4n+2)C_n. \tag{5.3.3}$$

Předpokládejme, že C_n je prvočíslo pro nějaké n. Potom ze vztahu (5.3.3) plyne, že C_n je buď dělitelem $(n+2)$, nebo C_{n+1}.

Zjevně pro $n > 3$ je $C_n > n + 2$ (např. ze vztahu (5.2.1)), tedy v takovém případě musí být C_n dělitelem C_{n+1}. Tedy existuje přirozené číslo k tak, že $C_{n+1} = kC_n$. Tedy podle (5.3.3) platí $4n + 2 = k(n + 2)$. Tato rovnost může být splněna jen za předpokladu, že $k \leq 3$ (pro $k \geq 4$ je pravá strana větší, neboť $kn \geq 4n$ a $2k > 2$). Vyřešíme tedy tři případy:

$k = 1$: Pak $n = 0$. To je v rozporu s předpokladem $n > 3$.

$k = 2$: Pak $n = 1$. To je rovněž v rozporu s předpokladem $n > 3$.

$k = 3$: Pak $n = 4$. Již víme, že $C_4 = 14$ není prvočíslo.

Dokázali jsme, že pro $n > 3$ je C_n složené číslo, jediná dvě prvočísla jsou tedy $C_2 = 2$ a $C_3 = 5$.

□

5.4 Dělitelé Catalanových čísel

V předchozí sekci jsme ukázali, pro která n je číslo C_n liché a pro která n je sudé. Zjistili jsme, že

$$2 \nmid C_n \Leftrightarrow C_n \text{ je liché} \Leftrightarrow n = 2^k - 1 \text{ pro nějaké } k \in \mathbb{N}_0. \tag{5.4.1}$$

Tedy Catalanova čísla dělitelná dvěma jsou ta, která nelze psát ve tvaru $n = 2^k - 1$ pro $k \in \mathbb{N}_0$. Tato čísla tvoří v posloupnosti všech Catalanových čísel jakési „bloky“, tj. skupiny po sobě jdoucích Catalanových čísel s danou vlastností. Blok sudých Catalanových čísel je vždy následován lichým číslem, viz tabulku 5.2.

n	0	1	2	3	4	5	6	7
C_n	1	1	2	5	14	42	132	429
mod 2	1	1	0	1	0	0	0	1
n	8	9	10	11	12	13	14	15
C_n	1 430	4 862	16 796	58 786	208 012	742 900	2 674 440	9 694 845
mod 2	0	0	0	0	0	0	0	1

Tabulka 5.2: Bloky sudých Catalanových čísel

Pro $k \in \mathbb{N}$ má blok $B_{2,k}$ Catalanových čísel dělitelných dvěma tvar

$$B_{2,k} = [C_{2^k}, C_{2^k+1}, \ldots, C_{2^{k+1}-2}], \tag{5.4.2}$$

délka tohoto (k-tého) bloku je $L_{2,k} = 2^{k+1} - 2 - 2^k + 1 = 2^k - 1$. V tabulce 5.2 jsou šedou barvou vyznačeny bloky $B_{2,1}, B_{2,2}, B_{2,3}$.

V posloupnosti Catalanových čísel se střídají bloky lichých čísel $\overline{B_{2,k}}$ s bloky sudých čísel $B_{2,k}$, přičemž délka bloku $\overline{B_{2,k}}$ pro $k > 1$ je $\overline{L_{2,k}} = 1$.

Podobné výsledky platí i pro dělitelnost Catalanových čísel prvočísly $p \geq 3$. Obecně pro dané prvočíslo p je v posloupnosti Catalanových čísel blok $\overline{B_{p,k}}$ čísel nedělitelných p následován blokem $B_{p,k}$ čísel dělitelných p (viz tabulku 5.5, bloky čísel dělitelných daným p jsou opět vyznačeny šedou barvou). V článku [2] nalezneme odvození délek těchto bloků $\overline{L_{p,k}}$, resp. $L_{p,k}$, pro $p \geq 3$. Výsledek shrneme do věty, kterou uvádíme bez důkazu.

Věta 5.4.1. ([2]) *Pro prvočíslo $p \geq 3$ platí:*

1)

$$p \nmid C_{p^k-1} \tag{5.4.3}$$

2) *Pro $k \in \mathbb{N}$ má blok $\overline{B_{p,k}}$ Catalanových čísel nedělitelných p délku $\overline{L_{p,k}}$, kde*

$$\overline{L_{3,1}} = 5, \ \forall k \geq 2 \ \overline{L_{3,k}} = 6 \tag{5.4.4}$$

a pro $p > 3$

$$\overline{L_{p,1}} = \frac{p+3}{2} - 1, \ \forall k \geq 2 \ \overline{L_{p,k}} = \frac{p+3}{2}. \tag{5.4.5}$$

3) *Pro $k \in \mathbb{N}$ má blok $B_{p,k}$ Catalanových čísel dělitelných p délku $L_{p,k}$, kde*

$$L_{3,k} = \frac{3^{m+2}-3}{2}, \ \forall p > 3 \ L_{p,k} = \frac{p^{m+1}-3}{2}, \tag{5.4.6}$$

přičemž $m \in \mathbb{N}_0$ je největší číslo takové, že

$$\left(\frac{p+1}{2}\right)^m \mid k, \ \ tj. \ m = \epsilon_{(p+1)/2}(k). \tag{5.4.7}$$

Délky bloků $\overline{L_{p,k}}$, resp. $L_{p,k}$, pro malá p, k udávají tabulky 5.3, resp. 5.4. V tabulce 5.5 najdeme zbytky po dělení C_n malými prvočísly pro malá n. Bloky zbytků reprezentujících dělitelnost daného C_n daným p (tj. zbytek 0) jsou zde zvýrazněny šedě.

Poznámka 5.4.2. V článku [2] se mírně liší definice posloupnosti Catalanových čísel, konkrétně autoři uvažují posunutou posloupnost $a_n = C_{n-1}$ pro $n \in \mathbb{N}$.

$\overline{L_{p,k}}$	$p=2$	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
$k=1$	2	5	3	4	6	7
$k \geq 2$	1	6	4	5	7	8

Tabulka 5.3: Délky bloků Catalanových čísel nedělitelných prvočísly 2, 3, 5, 7, 11, 13

	$p=2$	$p=3$	$p=5$	$p=7$	$p=11$	$p=13$
$k=1$		$\epsilon_2(1)=0$	$\epsilon_3(1)=0$	$\epsilon_4(1)=0$	$\epsilon_6(1)=0$	$\epsilon_7(1)=0$
	$L_{2,1}$=1	$L_{3,1}$=3	$L_{5,1}$=1	$L_{7,1}$=2	$L_{11,1}$=4	$L_{13,1}$=5
$k=2$		$\epsilon_2(2)=1$	$\epsilon_3(2)=0$	$\epsilon_4(2)=0$	$\epsilon_6(2)=0$	$\epsilon_7(2)=0$
	$L_{2,2}$=3	$L_{3,2}$=12	$L_{5,2}$=1	$L_{7,2}$=2	$L_{11,2}$=4	$L_{13,2}$=5
$k=3$		$\epsilon_2(3)=0$	$\epsilon_3(3)=1$	$\epsilon_4(3)=0$	$\epsilon_6(3)=0$	$\epsilon_7(3)=0$
	$L_{2,3}$=7	$L_{3,3}$=3	$L_{5,3}$=11	$L_{7,3}$=2	$L_{11,3}$=4	$L_{13,3}$=5
$k=4$		$\epsilon_2(4)=2$	$\epsilon_3(4)=0$	$\epsilon_4(4)=1$	$\epsilon_6(4)=0$	$\epsilon_7(4)=0$
	$L_{2,4}$=15	$L_{3,4}$=39	$L_{5,4}$=1	$L_{7,4}$=23	$L_{11,4}$=4	$L_{13,4}$=5

Tabulka 5.4: Délky bloků Catalanových čísel dělitelných prvočísly 2, 3, 5, 7, 11, 13

Dále můžeme zkoumat, jakou největší mocninou daného prvočísla p je dělitelné dané číslo C_n. V případě $p = 2$ dává odpověď na tuto otázku následující věta.

Věta 5.4.3. ([4, str. 193]) *Pro $n \in \mathbb{N}$ platí:*

$$\epsilon_2(C_n) = \nu_2(n+1) - 1. \tag{5.4.8}$$

n	C_n	mod 2	mod 3	mod 5	mod 7	mod 11	mod 13
0	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
2	2	0	2	2	2	2	2
3	5	1	2	0	5	5	5
4	14	0	2	4	0	3	1
5	42	0	0	2	0	9	3
6	132	0	0	2	6	0	2
7	429	1	0	4	2	0	0
8	1430	0	2	0	2	0	0
9	4862	0	2	2	4	0	0
10	16 796	0	2	1	3	10	0
11	58 786	0	1	1	0	2	0
12	208 012	0	1	2	0	2	12
13	742 900	0	1	0	4	4	2
14	2 674 440	0	0	0	6	10	2
15	9 694 845	1	0	0	6	6	4
16	35 357 670	0	0	0	5	7	10
17	129 644 790	0	0	0	2	0	2
18	477 638 700	0	0	0	0	0	6
19	1 767 263 190	0	0	0	0	0	4
20	6 564 120 420	0	0	0	4	0	0

Tabulka 5.5: Dělitelnost Catalanových čísel prvočísly 2, 3, 5, 7, 11, 13

Důkaz. S využitím (5.1.6) a (3.6.1) dostáváme

$$\epsilon_2(C_n) = \epsilon_2\left(\binom{2n}{n}\right) - \epsilon_2(n+1). \tag{5.4.9}$$

Platí $\nu_2(2n) = \nu_2(n)$, tedy podle (3.6.2) je

$$\epsilon_2\left(\binom{2n}{n}\right) = 2\nu_2(n) - \nu_2(2n) = \nu_2(n), \tag{5.4.10}$$

tedy

$$\epsilon_2(C_n) = \nu_2(n) - \epsilon_2(n+1). \tag{5.4.11}$$

Zvažme dva případy:

- n je sudé: Potom $\epsilon_2(n+1) = 0$ a $\nu_2(n) = \nu_2(n+1) - 1$, dosazením do (5.4.11) dostáváme (5.4.8).
- n je liché: Dvojkový zápis čísla n končí nenulovým počtem jedniček, označme tento počet z. Číslo n má tedy buď právě z-ciferný dvojkový zápis, nebo je na pozici $z+1$ zprava číslice 0. Z toho vyplývá, že číslo $n+1$ končí právě z nulami, tedy $\epsilon_2(n+1) = z$. Navíc platí $\nu_2(n) = \nu_2(n+1) + z - 1$. Dosazením těchto vztahů do (5.4.11) dostáváme

$$\epsilon_2(C_n) = \nu_2(n+1) + z - 1 - z = \nu_2(n+1) - 1. \tag{5.4.12}$$

Tím je tvrzení dokázáno.

□

Kapitolu uzavřeme větou, která je vylepšením výsledku 5.4.1 pro $p = 3$. Zatímco věta 5.4.1 říká pouze, pro která n je C_n dělitelné třemi, věta 5.4.4 podává úplnou informaci o zbytcích C_n při dělení třemi.

Věta 5.4.4. ([4, str. 205]) *Nechť je T množina všech čísel $n \in \mathbb{N}$, která mají v trojkové soustavě na všech pozicích kromě poslední (tj. kromě řádu jednotek) pouze číslice 0, 1 (na poslední pozici může být libovolná číslice). Dále nechť $\nu_3^*(n)$ značí celkový počet jedniček na všech pozicích trojkového zápisu čísla n kromě poslední. Potom pro Catalanova čísla platí*

$$\begin{aligned} &C_n \equiv (-1)^{\nu_3^*(n+1)} \pmod 3, \text{ pokud } n+1 \in T, \\ &C_n \equiv 0 \pmod 3 \text{ jinak.} \end{aligned} \tag{5.4.13}$$

Důkaz. Pro $n = 0$ a $n = 1$ je tvrzení zřejmé, dále předpokládejme $n \geq 2$. Pro Catalanova čísla platí

$$C_n = \frac{4n-2}{n+1} C_{n-1}. \tag{5.4.14}$$

Pokud je $n \equiv 0$ nebo $n \equiv 1 \pmod 3$, pak je $n+1$ invertibilní modulo 3 a $(4n-2)/(n+1) \equiv 1 \pmod 3$. Tedy pro $k \geq 1$ je

$$C_{3k-1} \equiv C_{3k} \equiv C_{3k+1} (\text{mod } 3). \tag{5.4.15}$$

Podívejme se zvlášť na tyto tři případy.

- $n = 3k$:

  Pro n dělitelné třemi je $C_n \equiv \binom{2n}{n} \pmod 3$ (plyne z (5.1.6)) a můžeme tedy využít výsledek z příkladu 3.6.11. Tedy

  $$\begin{aligned} C_n \equiv & (-1)^{\nu_3(n)} \pmod 3, \\ & \text{pokud se v trojkovém zápisu čísla } n \text{ vyskytují pouze číslice 0, 1,} \\ C_n \equiv & 0 \pmod 3 \quad \text{jinak.} \end{aligned} \tag{5.4.16}$$

  Číslo n končí nulou, tedy v trojkovém zápisu čísla n se vyskytují pouze číslice 0, 1 právě tehdy, když $n + 1 \in T$. Přitom $\nu_3^*(n + 1) = \nu_3(n)$ – tedy pro n dělitelné třemi jsou vzorce (5.4.16) a (5.4.13) ekvivalentní.

- $n = 3k + 1$:

  Platí $3k + 2 \in T$, právě když $3k + 1 \in T$. Dále je zřejmé, že $\nu_3^*(3k + 2) = \nu_3^*(3k + 1)$. Vzorec (5.4.13) tedy dává pro $n = 3k + 1$ stejný výsledek jako pro $n - 1 = 3k$. To je v souladu s tím, že podle vztahu (5.4.15) má platit $C_n = C_{3k+1} \equiv C_{3k} = C_{n-1} \pmod 3$.

- $n = 3k - 1$:

  Platí $3k \in T$, právě když $3k+1 \in T$. Dále je zřejmé, že $\nu_3^*(3k) = \nu_3^*(3k+1)$. Vzorec (5.4.13) tedy dává pro $n = 3k-1$ stejný výsledek jako pro $n+1 = 3k$. To je v souladu s tím, že podle vztahu (5.4.15) má platit $C_n = C_{3k-1} \equiv C_{3k} = C_{n+1} \pmod 3$.

Rozborem těchto tří případů jsme dokázali, že věta platí pro $n \geq 2$.

□

Seznam obrázků

3.1 Barevně odlišená parita čísel v Pascalově trojúhelníku 17

4.1 Znázornění možností dláždění v příkladu 4.3.1 28
4.2 Znázornění možností dláždění v příkladu 4.3.2 29
4.3 Znázornění možností dláždění obdélníka $1 \times (n + m - 1)$ 30

5.1 Zobrazení cest z příkladu 5.1.1 34
5.2 Rozdělení cesty z $[0; 0]$ do $[n; n]$ podle $[k; k]$ 37

Seznam tabulek

2.1 Tabulka faktoriálů pro malá n 3
2.2 Výpočet $\epsilon_2(10!)$ po sloupcích 4
2.3 Výpočet $\epsilon_2(10!)$ po řádcích 4
2.4 Význam binárního zápisu pro dolní součty 5

3.1 Prvních 7 řádků Pascalova trojúhelníku 9
3.2 Rozmístění lichých čísel v Pascalově trojúhelníku 17

4.1 Řešení úlohy s králíky 25
4.2 Prvních 25 Fibonacciho čísel 26

5.1 Tabulka Catalanových čísel pro malá n 36
5.2 Bloky sudých Catalanových čísel 40
5.3 Délky bloků Catalanových čísel nedělitelných prvočísly 2, 3, 5, 7, 11, 13 41
5.4 Délky bloků Catalanových čísel dělitelných prvočísly 2, 3, 5, 7, 11, 13 41
5.5 Dělitelnost Catalanových čísel prvočísly 2, 3, 5, 7, 11, 13 42

Literatura

[1] Aigner, M., Ziegler, G. M.: *Proofs from The Book.* Fourth Edition, Springer-Verlag Berlin Heidelberg, 2010.

[2] Alter, A., Kubota, K. K.: *Prime and Prime Power Divisibility of Catalan Numbers.* Journal of Combinatorial Theory 15 (1973), 243–256.

[3] Benjamin, A. T., Quinn, J. J.: *Proofs that really count.* Mathematical Association of America, Washington, DC, 2003.

[4] Deutsch, E., Sagan, B. E.: *Congruences for Catalan and Motzkin numbers and related sequences.* Journal of Number Theory 117 (2006), 191–215.

[5] Fine, N. J.: *Binomial Coefficients Modulo a Prime.* The American Mathematical Monthly 54 (1947), 589–592.

[6] Gardner, M.: *Mathematical carnival.* Mathematical Association of America, Washington, DC, 1989.

[7] Graham, R. L., Knuth, D. E., Patashnik, O.: *Concrete Mathematics.* Addison-Wesley, New York, 1994.

[8] Grimaldi, R. P.: *Fibonacci and Catalan numbers. An introduction.* John Wiley & Sons, Inc., Hoboken, NJ, 2012.

[9] Hering, F.: *Beziehung zwischen Binomialkoeffizienten und Primzahlpotenzen.* Archiv der Mathematik 19 (1968), 411–412.

[10] Heye, T.: *PlanetMath: Kummer's Theorem.*
http://planetmath.org/sites/default/files/texpdf/33909.pdf.
Citováno 7. 8. 2017.

[11] Joris, H., Oestreicher, C., Steinig, J.: *The greatest common divisor of certain sets of binomial coefficients.* Journal of Number Theory 21 (1985), 101–119 .

[12] Kummer, E.: *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen.* Journal für die reine und angewandte Mathematik 44 (1852), 93–146.

[13] Legendre, A.-M.: *Essai sur la Théorie des Nombres.* Second ed. Courcier, Paris, 1808, http://gallica.bnf.fr/ark:/12148/bpt6k62826k/f37.

[14] Lucas, É.:*Théorie des Fonctions Numériques Simplement Périodiques.* American Journal of Mathematics 1 (1878), 197–240.

[15] *Mathematical Behavior of Pascal's Triangle (mod 2)*
http://ecademy.agnesscott.edu/~lriddle/ifs/siertri/Pascalmath.htm.
Citováno 1.2.2017.

[16] Mihet, D.: *Legendre's and Kummer's Theorems Again.* Resonance 15 (2010), 1111–1121.

[17] *Parity and Primality of Catalan Numbers.* The College Mathematics Journal 37 (2006), 52–53.

[18] Scheid, H.: *Die Anzahl der Primfaktoren in* $\binom{n}{k}$. Archiv der Mathematik 20 (1969), 581–582.

[19] Stahl, W.: *Bermerkung zu einer Arbeit von Hering.* Archiv der Mathematik 20 (1969), 580.

[20] Sury, B.: *Revisiting Kummer's and Legendre's Formulae.* Resonance 10 (2005), 62–71.

[21] *Wikipedia: Kummer's Theorem.* https://en.wikipedia.org/wiki/Kummer's_theorem. Citováno 7. 8. 2017.

[22] *Wikipedia: Legendre's formula.* https://en.wikipedia.org/wiki/Legendre's_formula. Citováno 24. 10. 2016.