Kombinatorické počítání

Martin Klazar

Výběrová přednáška

Tento text je rozšířenou verzí poznámek k výběrové přednášce, kterou jsem poprvé konal v letním semestru v r. 1996. Stihl jsem tehdy kapitoly 1–11, jejich písemná podoba zaznamenává dosti věrně, co bylo přednášeno. Zbývající kapitoly byly plánovány, ale z časových důvodů nebylo možné je přednést, jsou tedy doplněny dodatečně. První část přednášky je věnována kombinatorické teorii čísel. Druhá část ukazuje použití generujících funkcí v kombinatorické enumeraci a důraz je kladen na příklady ilustrující tuto techniku. Na rozdíl od tradičního stylu věta–důkaz v první části jsem proto ve druhé zvolil styl výpočet–výsledek, který je konkrétním příkladům přiměřenější. Pro lepší čtenářův přehled je ve druhé části vždy hlavní výsledek umístěn v rámečku.

Jde pouze o přičísnuté poznámky k přednášce, proto určitá lakoničnost a nesystematičnost, za něž se čtenáři omlouvám. Nahlíženo z pozitivní stránky: tím více příležitostí k vlastnímu domýšlení věcí do konce. Podoba výběrové přednášky není konečná, považuji tento text za odrazový můstek. V budoucnu plánuji celou přednášku věnovat technikám kombinatorické enumerace a přepracovat ji.

Martin Klazar

5. Dokažte Větu 32 z 10. kapitoly.

6. Věta 40 z 13. kapitoly jistě neplatí, má-li uvažovaný polynom všechny kořeny reálné, nicméně s různými znaménky. Kde jsme přesně v důkazu použili stejnost znamének?

7. Nalezněte ve 14.1 bijektivní korespondenci mezi oběma druhy číselných rozkladů.

8. Nalezněte počet pěstovaných stromů na n vrcholech, v nichž každý vrchol má buď tři syny nebo žádného syna.

18 Literatura ke druhé části

Důkaz Jacobiho formule pro počet reprezentací n ve tvaru součtu čtyř čtverců se nalézá např. v [3]. S teorií stojící za identitami obsahujícími funkci $\sigma_k(n)$ se lze seznámit v [4]. Výsledky 9.1, 9.2 a 9.3 jsou klasické, 9.1 jsem zpracoval podle knihy [8]. Rekurenci v 10.1 nalezl Klarner (1968), příklad je zpracován podle [6]. Příklad 10.2 je klasický, v jiné formulaci se jím zabýval již Schröder v r. 1870. P-rekurzivitou se zabývá přehledový článek [7]. Příklad 11.1 jsem převzal z [6]. Asymptotická enumerace je zmíněna v [8], základní monografií je [6]. Kapitola 13 je zpracována podle [8]. Příklad 14.1 je klasický, stejně jako výsledky v kapitole 15. Pro důkaz Lagrangeovy inversní formule odkazuji do [8] nebo do [1]. Důkaz asymptotiky pro Bellova čísla lze nalézt v [5] nebo v [6]. Příklad 16.1 jsem převzal z [8].

1. I. Gessel, R. P. Stanley, Algebraic Enumeration, 21. kapitola v [2].
2. R. L. Graham, M. Grötschel a L. Lovász (editors), *Handbook of Combinatorics*, North-Holland, Amsterdam, 1995.
3. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, Berlin, 1982. Ruský překlad: K. Ajerlend, M. Rouzen, *Klassičeskoe vvedenie v sovremennuju teoriju čisel*, Mir, Moskva, 1987.
4. N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer, New York etc., 1984.
5. L. Lovász, *Combinatorial problems and exercises*, Akadémiai Kiadó, Budapest 1979.
6. A. M. Odlyzko, Asymptotic Enumeration Methods, 22. kapitola v [2].
7. R. P. Stanley, Differentiably finite power series, *Eur. J. Comb.* **1** (1980), 175–188.
8. H. Wilf, *Generatingfunctionology*, Academic Press, Boston MA, 1994.

a vidíme, že

$$R(y)^{<-1>} = y(1-y^2).$$

Podle Lagrangeovy inverzní formule v 15.4 dostáváme

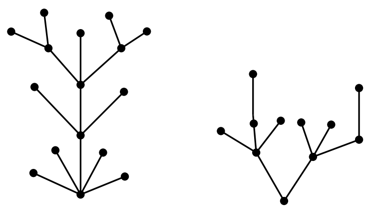
$$[x^n]R(x) = \frac{1}{n}[x^{n-1}]\left(\frac{x}{R(x)^{<-1>}}\right)^n = \frac{1}{n}[x^{n-1}](1-x^2)^{-n} = \begin{cases} \frac{1}{n}\binom{3(n-1)/2}{n-1} & \text{pro } n \text{ liché} \\ 0 & n \text{ sudé.} \end{cases}$$

Celkově dostáváme modulo 2

$$\boxed{s(n) \equiv \begin{cases} 0 & \text{pro } n \text{ liché} \\ \frac{1}{n+1}\binom{3n/2}{n} & \text{pro } n \text{ sudé.} \end{cases}}$$

17 Příklady ke druhé části

1. Pojem pěstovaného stromu je vysvětlen v 9.2. *Symetrickým pěstovaným stromem* budeme rozumět pěstovaný strom, jehož znázornění v rovině se nemění při zrcadlení podle svislé osy. Např. strom vlevo je symetrický, strom vpravo nikoli:



Nalezněte, třeba pomocí GF, formuli pro počet symetrických pěstovaných stromů na n vrcholech.

2. Pro která n je Catalanovo číslo c_n liché?

3. Narayanova čísla $n(a,b)$ jsou definována v 9.3. Nalezněte explicitní formuli pro OGF o dvou proměnných pro tato čísla a pokuste se odtud odvodit explicitní formuli pro čísla sama.

4. Dokažte přímo z kombinatorické definice, bez použití explicitního vzorce, že $n(a,b) = n(a,a-b)$.

Obsah

Kombinatorická teorie čísel

1 Odhadování sum

Začneme dvěma lemmaty, která vyjadřují součty pomocí integrálů. Symboly $\mathbf{N}, \mathbf{Z}, \mathbf{R}$ a $\mathbf{C}$ označují množinu přirozených čísel $\{1, 2, \ldots\}$, množinu celých čísel, množinu reálných čísel a množinu komplexních čísel. Pro $x \in \mathbf{R}$ je $\lfloor x \rfloor \in \mathbf{Z}$ největší celé číslo nepřesahující x (*celá část* čísla x). Symbol $\{x\}$ značí *zlomkovou část* čísla x, tj. $\{x\} = x - \lfloor x \rfloor$.

Lemma 1 (Abelova transformace) *Nechť $f \in C[1, \infty)$ (tj. f je reálná funkce, hladká v uvedeném intervalu), $h:\ \mathbf{N} \to \mathbf{C}$ (tj. h je posloupnost komplexních čísel), $x \in \mathbf{R}$ je reálné číslo a $g(x) = \sum h(n)$, kde sčítáme přes čísla $n = 1, 2, \ldots, \lfloor x \rfloor$. Potom*

$$\sum_{n \le x} h(n)f(n) = g(x)f(x) - \int_1^x g(t)f'(t)dt.$$

Důkaz.

$$\begin{aligned}
\sum_{n \le x} h(n)f(n) &= g(x)f(\lfloor x \rfloor + 1) + \sum_{n \le x} g(n)(f(n) - f(n+1)) \\
&= \circ - \sum_{n \le x} g(n) \int_n^{n+1} f'(t)dt = \circ - \int_1^{\lfloor x \rfloor + 1} g(t)f'(t)dt \\
&= \circ - \int_1^x g(t)f'(t) - \int_x^{\lfloor x \rfloor + 1} g(t)f'(t)dt \\
&= \circ - \int_1^x g(t)f'(t) - g(\lfloor x \rfloor) \int_x^{\lfloor x \rfloor + 1} f'(t)dt \\
&= \circ - \int_1^x g(t)f'(t)dt - \circ + g(x)f(x) = g(x)f(x) - \int_1^x g(t)f'(t)dt.
\end{aligned}$$

□

Lemma 2 (Eulerova sumační formule) *Nechť $a \in \mathbf{N}$, $x \in \mathbf{R}$ a $f \in C[a, \infty)$. Pak*

$$\sum_{a \le n \le x} f(n) = \int_a^x f(t)dt + R,\ \textit{kde}\ R = \int_a^x \{t\}f'(t)dt + f(a) - \{x\}f(x).$$

Důkaz. Plyne z předchozího lemmatu. Položíme $h(m) = 0$ pro $m = 1, 2, \ldots, a-1$ a $h(m) = 1$ pro $m \ge a$. Dostaneme

$$\begin{aligned}
\sum_{a \le n \le x} f(n) &= (\lfloor x \rfloor - a + 1)f(x) - \int_a^x (\lfloor t \rfloor - a + 1)f'(t)dt \\
&= \lfloor x \rfloor f(x) - (a-1)f(a) - \int_a^x \lfloor t \rfloor f'(t)dt.
\end{aligned}$$

$1, 2, \ldots, k$ — se musely křížit s A. Proto při vhodném očíslování $a_1 < a_2 < \cdots < a_k < b_k < \cdots < b_2 < b_1$. Rozlišíme dva případy.

Nechť $k > 0$. Závorky U' různé od A_i se rozpadají do $k+1$ množin S_i, $i = 0, 1, \ldots, k$, kde v S_i se nacházejí závorky ležící uvnitř A_i a vně A_{i+1}. Každá S_i je opět špatným uzávorkováním, lze je volit libovolně a nezávisle na sobě. Označíme-li $|S_i|$ počet závorek S_i, je počet možných poloh A_{i+1} v S_i roven $2|S_i| + 1$. Obdobně pro počet poloh čísla a v mezerách S_k. Tyto koeficienty získáme pomocí derivování. Příspěvek k počtu všech špatných uzávorkování s n závorkami tedy je

$$[x^n](x(2xS' + S))^{k+1}.$$

Nechť $k = 0$. U' je samo o sobě špatným uzávorkováním. Je třeba pouze rozvážit, kolik je možností pro umístění a v jeho mezerách. Zakázány jsou ty polohy, kdy A nekříží žádnou závorku z U'. Tehdy se U' rozpadá na část nalevo od a a na část napravo od a, obě jsou špatnými uzávorkováními a lze je volit libovolně a vzájemně nezávisle. Obdržíme příspěvek

$$[x^n](x(2xS' + S) - xS^2).$$

Celkem dostáváme pro $S(x)$ rovnici

$$S(x) = \sum_{k \ge 0} (x(2xS(x)' + S(x)))^k - xS(x)^2.$$

Pomocí vztahu pro součet geometrické řady a s trochou úprav to lze přepsat jako

$$S(x) \cdot (1 + xS(x)) \cdot (1 - xS(x) - 2x^2 S(x)') = 1.$$

Odtud lze pro čísla $s(n)$ odvodit explicitní rekurentní formuli, tento směr však nebudeme sledovat. Setkáváme se zde s novou situací. Není těžké vidět přímo z definice, že čísla $s(n)$ rostou superexponenciálně, zhruba jako faktoriál. Proto OGF $S(x)$ má nulový poloměr konvergence a neurčuje žádnou analytickou funkci. Diferenciální rovnice, kterou jsme odvodili, je čistě formální a nemá smysl se ji snažit řešit.

Zajímá-li nás však pouze parita $s(n)$, můžeme předešlou rovnici redukovat modulo 2 a dostaneme algebraickou rovnici

$$x^2 T(x)^3 - T(x) + 1 = 0$$

($T(x)$ je redukce formální mocninné řady $S(x)$ modulo 2). Tento vztah již určuje analytickou funkci, bylo by však chybou se snažit aplikovat postupy pro řešení kubických rovnic. Substituce $R(x) = xT(x)$ vede na rovnici

$$R(x)^3 - R(x) + x = 0$$

$$c(k,n) \equiv \binom{\lfloor n/2 \rfloor}{k - \lceil n/2 \rceil}.$$

Speciálně pro $k < \lceil n/2 \rceil$ je binomický koeficient roven nule a Stirlingovo číslo je tehdy sudé.

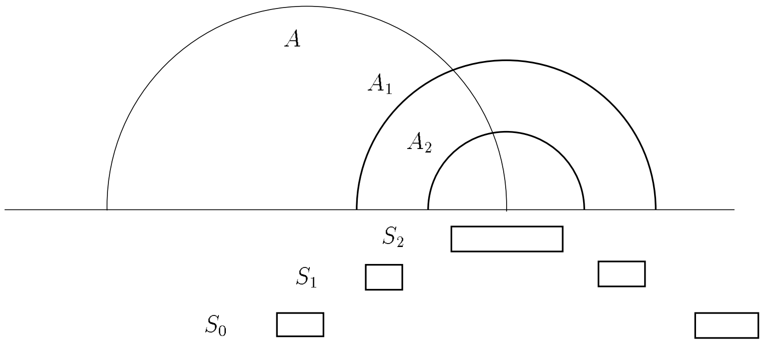
16.2 Špatná uzávorkování. *Uzávorkováním* s n *závorkami* budeme rozumět rozklad $\{1, 2, \ldots, 2n\}$ na n dvouprvkových množin. Budeme nuceni přecházet k poduzávorkováním a proto jako bázickou množinu připouštíme u uzávorkování i libovolnou podmnožinu $\mathbf{N}$ se sudým počtem prvků. Dvě závorky $A = \{a, b\}$ a $B = \{c, d\}$ se *kříží*, pokud $a < c < b < d$ nebo $c < a < d < b$. *Dobré* uzávorkování je uzávorkování bez křížení. Naopak *špatné* uzávorkování je takové, v němž se každá závorka kříží s nějakou jinou závorkou.

Není těžké nalézt počet dobrých uzávorkování s n závorkami. Učinili jsme to vlastně v 9.2. Tento počet se totiž rovná počtu pěstovaných stromů s $n-1$ vrcholy a je tedy dán Catalanovým číslem c_{n-1}. Pro počet špatných uzávorkování s největší pravděpodobností žádný jednoduchý vzorec neexistuje, odvodíme však jednoduchý vztah pro jejich paritu.

Nechť $s(n)$ je počet špatných uzávorkování s n závorkami a nechť

$$S = S(x) = \sum_{n \geq 0} s(n) x^n = 1 + x^2 + 4x^3 + \cdots$$

je odpovídající OGF. Uvažme nějaké špatné uzávorkování U a jeho první závorku $A = \{1, a\}$. Viz následující obrázek:



Po vyhození A dostaneme uzávorkování U', které nemusí být špatné. Je jasné, že všechny závorky U', které nekříží jinou závorku — buďte to $A_i = \{a_i, b_i\}, a_i < b_i, i =$

Přičtením formule integrace per partes

$$0 = \int_a^x f(t)dt - xf(x) + af(a) + \int_a^x tf'(t)dt$$

získáváme Eulerovu sumační formuli. □

Je-li f nezáporná a neklesající, popř. nerostoucí, pak zřejmě $R = O(f(x))$, popř. $R = O(f(a))$.

Použitím Eulerovy sumační formule snadno spočítáme, že

$$\sum_{n=1}^{N} \frac{1}{n} = \log N + \gamma + O(1/N), \text{ kde číslo}$$

$$\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2} dt = \lim_{N \to \infty} \left(\sum_{n=1}^{N} \frac{1}{n} - \log N \right) = 0.57721\ldots$$

se nazývá *Eulerova-Mascheroniova konstanta*.

S pomocí tohoto odhadu nalezneme průměrnou hodnotu počtu dělitelů $\tau(n)$ přirozeného čísla n. Máme

$$\begin{aligned}
\frac{1}{N}\sum_{n=1}^{N} \tau(n) &= \frac{1}{N}\Big(2 \sum_{n \leq \sqrt{N}} \sum_{m \leq N/n} 1 - \left\lfloor \sqrt{N} \right\rfloor^2\Big) = \frac{2}{N} \sum_{n \leq \sqrt{N}} \left\lfloor \frac{N}{n} \right\rfloor - \frac{1}{N} \left\lfloor \sqrt{N} \right\rfloor^2 \\
&= 2 \sum_{n \leq \sqrt{N}} \frac{1}{n} - \frac{2}{N} \sum_{n \leq \sqrt{N}} \left\{ \frac{N}{n} \right\} - 1 + \frac{2}{\sqrt{N}} \left\{ \sqrt{N} \right\} - \frac{1}{N} \left\{ \sqrt{N} \right\}^2 \\
&= 2 \log \left\lfloor \sqrt{N} \right\rfloor + 2\gamma - 1 + O(N^{-1/2}).
\end{aligned}$$

Podle věty o střední hodnotě můžeme $\log \left\lfloor \sqrt{N} \right\rfloor$ nahradit $\log \sqrt{N}$ za cenu chyby $O(N^{-1/2})$. Dokázali jsme následující výsledek.

Věta 3 (Dirichlet)

$$\frac{1}{N} \sum_{n=1}^{N} \tau(n) = \log N + 2\gamma - 1 + O(1/\sqrt{N}).$$

Není těžké spočítat, že pro veličinu $r(n) = \#\{(x, y) \in \mathbf{Z}^2 : \ x^2 + y^2 = n\}$ platí

Věta 4 (Gauss)

$$\frac{1}{N} \sum_{n=1}^{N} r(n) = \pi + O(1/\sqrt{N}).$$

Geometrická interpretace druhého tvrzení je očividná: $\sum r(n)$ je prostě počet mřížových bodů v kruhu o poloměru $\sqrt{N}$. Tento výklad také vede ke snadnému důkazu Gaussovy věty. První suma $\sum \tau(n)$ je počet mřížových bodů v rovinné oblasti omezené kladnými poloosami os x a y a hyperbolou $xy = N$. Další dvě zajímavé asymptotiky sum jsou čtenáři předloženy k důkazu v Příkladech 6 a 7.

Problém zlepšení odhadu zbytku ve Větách 3 a 4 se nazývá *Dirichletovým problémem dělitelů* a *Gaussovým kruhovým problémem*. Hledáme infimum θ_0 množiny kladných reálných čísel θ, pro něž $O(N^\theta/N)$ je platným odhadem zbytku ve Větě 3 a 4. Viděli jsme, že elementární úvahy dávají v obou případech $\theta_0 \leq 1/2$. Následující meze jsou platné rovněž pro obě úlohy. Hardy a Landau (1916) dokázali, že $\theta_0 \geq 1/4$. Iwaniec a Mozzochi (1988) dokázali, že $\theta_0 \leq 7/22$.

Byla nalezena zesílení Lemmatu 2. Uvedeme si bez důkazu jedno z nich, používá *Bernoulliovy polynomy* $B_n(x)$ definované rozvojem

$$\frac{ze^{xz}}{e^z - 1} = \sum_{n=0}^{\infty} B_n(x)\frac{z^n}{n!}$$

a *Bernoulliova čísla* $B_n = B_n(0)$. Tedy

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

Díky záměně z za $-z$ vidíme, že $B_n = 0$ pro všechna lichá $n > 1$. Pár hodnot: $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, $B_8 = -1/30$, $B_{10} = 5/66$, $B_{12} = -691/2730$, $B_{14} = 7/6, \ldots$

Lemma 5 (obecná Eulerova sumační formule) *Nechť $a, b \in \mathbf{N}$ a $f \in C^{2m}[a, b]$ (tj. f je v uvedeném intervalu $2m$ krát spojitě diferencovatelná). Potom*

$$\sum_{n=a}^{b} f(n) = \int_a^b f(t)dt + \frac{f(a) + f(b)}{2} + \sum_{r=1}^{m} \frac{B_{2r}}{(2r)!}\left(f^{(2r-1)}(b) - f^{(2r-1)}(a)\right) + R_m, \ \textit{kde}$$

$$R_m = -\int_a^b f^{(2m)}(t)\frac{B_{2m}(\{t\})}{(2m)!}dt.$$

Je známo, že $|B_{2m}(\{t\})| \leq |B_{2m}|$. Proto můžeme R_m odhadnout jako

$$|R_m| \leq \frac{|B_{2m}|}{(2m)!}\int_a^b |f^{(2m)}(t)|dt.$$

Připomínáme notaci $f(x) \sim g(x)$, která je zkratkou pro

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Uvažme EGF

$$Z(x) = \sum_{n\geq 1} \frac{z(n)x^n}{n!}$$

a $\mathcal{S}$-strukturu všech označených zakořeněných stromů na $\{1, 2, \ldots, n\}$. Nechť T je takový strom s kořenem i a sousedy kořene $i_1, i_2, \ldots, i_m$. Vyhozením i se T rozpadá na m zakořeněných označených stromů s kořeny $i_1, i_2, \ldots, i_m$. Jejich vrcholové množiny tvoří rozklad $\{1, 2, \ldots, n\}\backslash\{i\}$ na m bloků. Obecnou $\mathcal{S}$-strukturu obdržíme tedy tak, že $\{1, 2, \ldots, n\}$ rozložíme uspořádaně na (A, B), množinu A vybavíme strukturou "být jednoprvkovou množinou" — pro ni je EGF patrně rovna x — a B rozložíme na množinu neprázdných disjunktních bloků, z nichž každý vybavíme $\mathcal{S}$-strukturou. Množinu bloků vybavíme triviální strukturou "být množinou", její EGF je e^x. Podle Součinové a Kompoziční formule dostáváme rovnici

$$Z(x) = xe^{Z(x)}.$$

Vidíme, že

$$Z(y)^{<-1>} = \frac{y}{e^y}.$$

Podle Lagrangeovy inverzní formule

$$\frac{z(n)}{n!} = [x^n]Z(x) = \frac{1}{n}[x^{n-1}]\left(\frac{x}{Z(x)^{<-1>}}\right)^n = \frac{1}{n}[x^{n-1}]e^{nx} = \frac{n^{n-1}}{n!}.$$

Cayleyova formule je dokázána.

16 GF dokazují kongruence

16.1 Stirlingova čísla prvního druhu. V 13.1 jsme ve Větě 39 nalezli GF pro čísla $c(k, n)$, která počítají počty permutací $\{1, 2, \ldots, n\}$ s k cykly. Z explicitního vzorce

$$\sum_{k\geq 1} c(k, n)x^k = x(x + 1)\cdots(x + n - 1)$$

odvodíme vztah pro paritu $c(k, n)$. Všechny následující kongruence jsou modulo 2.

$$\sum_k c(k, n)x^k \equiv x(x + 1)x(x + 1)\cdots = x^{\lceil n/2\rceil}(1 + x)^{\lfloor n/2\rfloor}.$$

Tedy

$$c(k, n) \equiv [x^k]x^{\lceil n/2\rceil}(1 + x)^{\lfloor n/2\rfloor} = \left[x^{k-\lceil n/2\rceil}\right](1 + x)^{\lfloor n/2\rfloor} = \binom{\lfloor n/2\rfloor}{k - \lceil n/2\rceil}.$$

Celkem

Metodami komplexní analýzy lze odtud odvodit asymptotiku pro b_n:

$$b_n \sim \frac{1}{\sqrt{n}} \lambda(n)^{n+1/2} e^{\lambda(n)-n-1},$$

kde $\lambda(n)$ je řešením rovnice $\lambda(n)\log\lambda(n) = n$. V prvním přiblížení je $\lambda(n)$ zhruba $n/\log n$.

Při použití Kompoziční formule je třeba mít vždy na mysli, že formální složenina mocninných řad $F(G(x))$ je dobře definována jen za podmínky $G(0) = 0$. Proto ta -1 v exponentu.

15.4 Lagrangeova inverzní formule. Občas se stane, že pro OGF či EGF popisující náš problém — buď to funkce $F(x)$ — odvodíme rovnici, z níž neumíme vyjádřit explicitně $F(x)$ pomocí x, avšak umíme vyjádřit naopak x pomocí $F(x)$. Jinými slovy: víme, jak vypadá inverzní funkce $F(x)^{<-1>}$. Potom lze použít následují výsledek, který popisuje koeficient u x^n v $F(x)$ pomocí koeficientů inverzní mocninné řady. Připomínáme, že $[x^n]F(x)$ je symbolické označení pro tento koeficient.

Věta 42 (Lagrangeova inverzní formule) *$F(x)$ buď mocninná řada, pro niž platí*

$$[x^0]F(x) = 0 \text{ a } [x^1]F(x) \neq 0.$$

Potom

$$[x^n]F(x)^{<-1>} = \frac{1}{n}[x^{n-1}]\left(\frac{x}{F(x)}\right)^n.$$

V poslední kapitole uvedeme odkazy na literaturu, v níž lze nalézt jak kombinatorické tak analytické důkazy tohoto užitečného tvrzení.

15.5 Cayleyova formule. Cayleyova formule patří k perlám kombinatoriky. Tvrdí, že pro počet $t(n)$ označených stromů na množině vrcholů $\{1, 2, \ldots, n\}$ platí

$$\boxed{t(n) = n^{n-2}.}$$

Důkaz, který teď uvedeme, kombinuje obraty 15.1, 15.2 a 15.4. Jako $z(n)$ označíme počet zakořeněných označených stromů s vrcholovou množinou $\{1, 2, \ldots, n\}$. Cayleyova formule je zřejmým způsobem ekvivalentní s

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

Například,

$$1 \cdot 2 \cdot 3 \cdots n = n! \sim C\sqrt{n}\left(\frac{n}{e}\right)^n,$$

kde $e = 2.71828\ldots$ je Eulerovo číslo a $C > 0$ jistá konstanta (jemnějšími metodami lze ukázat, že $C = \sqrt{2\pi}$). Tento odhad plyne z Lemmatu 5 při volbě $f(t) = \log t$, $a = 1$, $b = n$ a $m = 1$.

Je překvapující, že Bernoulliova čísla propojují technické lemma o náhradě sum integrály s hlubokým Kummerovým výsledkem o Fermatově hypotéze. Ta tvrdí, že rovnice $x^n + y^n = z^n$ nemá pro exponent $n > 2$ žádné celočíselné řešení s $z \neq 0$.

Věta 6 (Kummer, 1850) *Fermatova hypotéza platí pro každý exponent $n = p > 2$, který je regulárním prvočíslem (definice regularity je komplikovaná a vyžaduje aparát algebraické teorie čísel). Prvočíslo $p > 2$ je regulární právě když p nedělí žádného čitatele Bernoulliových čísel $B_2, B_4, \ldots, B_{p-3}$.*

Mezi lichými prvočísly nepřesahujícími 100 pouze 3 nejsou regulární a předchozí věta tudíž pro ně není použitelná, jsou to 37, 59 a 67. V r. 1993 A. Wiles oznámil důkaz Fermatovy hypotézy, který je v současnosti světovou matematickou komunitou všeobecně uznáván jako správné řešení rébusu starého 300 let.

2 Odhady počtu prvočísel

Hezkým příkladem kombinatorického počítání jsou odhady funkce $\pi(x)$, která je definována jako

$$\pi(x) = \sum_{p \leq x} 1,$$

tj. rovná se počtu prvočísel nepřesahujících (reálné) číslo x. V dalším budeme často používat písmena p a q pro označení prvočísel. *Mangoldtova funkce* $\Lambda(n)$ je definována jako $\log p$, je-li n mocninou prvočísla p, a jako 0 jinak.

Lemma 7

$$\begin{aligned} \sum_{n\leq x} \Lambda(n)\left\lfloor\frac{x}{n}\right\rfloor &= x\log x - x + O(\log x) \\ \sum_{n\leq x} \Lambda(n)\left(\left\lfloor\frac{x}{n}\right\rfloor - 2\left\lfloor\frac{x}{2n}\right\rfloor\right) &= x\log 2 + O(\log x). \end{aligned}$$

Důkaz. Nejprve dokážeme první vztah.

$$\sum_{n\le x}\Lambda(n)\left\lfloor\frac{x}{n}\right\rfloor=\sum_{n\le x}\Lambda(n)\sum_{m\le x,\ n|m}1=\sum_{m\le x}\sum_{n|m}\Lambda(n)=\sum_{m\le x}\log m=x\log x-x+O(\log x).$$

V posledním kroku jsme použili Eulerovu sumační formuli. Druhý vztah snadno plyne z prvního. Označíme-li první sumu jako $M(x)$, máme

$$\sum_{n\le x}\Lambda(n)\left(\left\lfloor\frac{x}{n}\right\rfloor-2\left\lfloor\frac{x}{2n}\right\rfloor\right)=M(x)-2M(x/2)=x\log 2+O(\log x).$$

□

Lemma užijeme k důkazu základního výsledku o míře růstu prvočíselné funkce $\pi(x)$.

Věta 8 (Čebyšev, 1850) *Existují absolutní konstanty $0<c_1<c_2$, že pro každé číslo $x\ge 1$ platí*

$$\frac{c_1x}{\log x}<\pi(x)<\frac{c_2x}{\log x}.$$

Důkaz. Snadno se vidí, že pro každé reálné číslo a platí $\lfloor a\rfloor-2\lfloor a/2\rfloor\le 1$. Proto z druhého vztahu Lemmatu 7 dostáváme

$$x\log 2+O(\log x)\le\sum_{n\le x}\Lambda(n)=\sum_{p\le x}\left\lfloor\frac{\log x}{\log p}\right\rfloor\log p\le\log x\sum_{p\le x}1=\pi(x)\log x.$$

Dokázali jsme dolní odhad.

Pro důkaz horního odhadu použijeme, že vždy $\lfloor a\rfloor-2\lfloor a/2\rfloor\ge 0$ a že tato veličina je 1 pro $1\le a<2$. Pomocí druhé formule Lemmatu 7 máme

$$\begin{aligned}\pi(x)\log x-\pi(x/2)\log x/2 &= \sum_{x/2<p\le x}\log p+O(x)\\ &\le \sum_{x/2<n\le x}\Lambda(n)(\lfloor x/n\rfloor-2\lfloor x/2n\rfloor)+O(x)\\ &\le \sum_{n\le x}\Lambda(n)(\lfloor x/n\rfloor-2\lfloor x/2n\rfloor)+O(x)\\ &= O(x).\end{aligned}$$

Ukázali jsme tedy, že $\pi(x/2^k)\log x/2^k-\pi(x/2^{k+1})\log x/2^{k+1}=O(x/2^k)$, kde konstanta v O nezávisí na k (a samozřejmě ani na x). Sečteme-li tyto odhady pro $k=0,1,\ldots,K$, kde K je určeno z $2^K\le x<2^{K+1}$, dostaneme kýžený horní odhad

Důkaz je opět lehký. Z jedné strany

$$h_n=\sum_{k=1}^{\infty}\frac{f_k}{k!}\sum_{\dots}\binom{n}{m_1\ m_2\ \ldots\ m_k}g_{m_1}g_{m_2}\cdots g_{m_k},$$

kde sčítáme přes všechny uspořádané k-tice přirozených čísel $m_1,m_2,\ldots,m_k$, pro něž $m_1+m_2+\cdots+m_k=n$. Multinomický koeficient vyjadřuje počet všech *uspořádaných* rozkladů $\{1,2,\ldots,n\}$ na k bloků s mohutnostmi $m_1,m_2,\ldots,m_k$. Tento počet musíme vydělit $k!$, protože v definici $\mathcal{H}$-struktury vystupují *neuspořádané* rozklady. Členy $g_{m_1}g_{m_2}\cdots g_{m_k}$ a f_k vyjadřují počty možných voleb $\mathcal{G}$-struktur a $\mathcal{F}$-struktur. Mírně upraveno,

$$\frac{h_n}{n!}=\sum_{k=1}^{\infty}\frac{f_k}{k!}\sum_{\dots}\frac{g_{m_1}}{m_1!}\cdot\frac{g_{m_2}}{m_2!}\cdots\frac{g_{m_k}}{m_k!}.$$

Z druhé strany se lehce nahlédne, že tento výraz je přesně koeficient u x^n ve složenině mocninných řad $F(G(x))$.

15.3 Bellova čísla. Kolik je všech rozkladů množiny $\{1,2,\ldots,n\}$ na neprázdné bloky? Např. pro $n=3$ dostáváme 5 rozkladů:

$$\{\{1,2,3\}\},\ \{\{1,2\},\{3\}\},\ \{\{1,3\},\{2\}\},\ \{\{2,3\},\{1\}\},\ \{\{1\},\{2\},\{3\}\}.$$

Označme si obecný počet jako b_n a uvažme EGF

$$B(x)=\sum_{n\ge 1}\frac{b_nx^n}{n!}.$$

Známe-li Kompoziční formuli, je nalezení explicitního vzorce pro $B(x)$ téměř trivialitou. $\mathcal{G}$-strukturou je struktura "být neprázdnou množinou", pro niž $g_n=1$ pro $n\ge 1$ a $g_0=0$. Jako $\mathcal{F}$-strukturu bychom mohli vzít tutéž strukturu, vezměme však strukturu "být množinou", pro niž $f_n=1$ pro $n\ge 0$; vyjde hezčí vzoreček. Tedy

$$F(x)=e^x \text{ a } G(x)=e^x-1$$

a podle Kompoziční formule

$$\boxed{B(x)=F(G(x))=e^{e^x-1}.}$$

$\mathcal{H}$-*struktury* vypadají tak, že v každém *uspořádaném* rozkladu $\{1, 2, \ldots, n\}$ na dvě neprázdné množiny (A, B) množinu A strukturujeme $\mathcal{F}$-strukturou a množinu B strukturujeme $\mathcal{G}$-strukturou. Obě volby jsou vzájemně nezávislé. Nechť

$$H(x) = \sum_{n \geq 1} \frac{h_n x^n}{n!}$$

je EGF pro počet h_n všech $\mathcal{H}$-struktur na $\{1, 2, \ldots, n\}$. Platí

Součinová formule: $H(x) = F(x)G(x)$.

Důkaz je lehký. Počet uspořádaných rozkladů (A, B) s $|A| = k$ je dán příslušným binomickým koeficientem. Tedy

$$h_n = \sum_{k=1}^{n-1} \binom{n}{k} f_k g_{n-k}.$$

Po úpravě

$$\frac{h_n}{n!} = \sum_{k=1}^{n} \frac{f_k}{k!} \cdot \frac{g_{n-k}}{(n-k)!},$$

což je právě koeficient u x^n v součinu $F(x)G(x)$.

15.2 Kompoziční formule. Mějme tutéž situaci a totéž označení jako v 15.1. $\mathcal{H}$-*struktury* budeme definovat pomocí jiné standardní konstrukce. Bázickou množinu $\{1, 2, \ldots, n\}$ rozložíme na *množinu* neprázdných bloků, na každém z nich zvolíme vzájemně nezávisle $\mathcal{G}$-strukturu, a množinu bloků strukturujeme $\mathcal{F}$-strukturou (nezávisle na zvolených $\mathcal{G}$-strukturách). EGF pro počty $\mathcal{H}$-struktur buď opět

$$H(x) = \sum_{n \geq 1} \frac{h_n x^n}{n!}.$$

Platí

Kompoziční formule: $H(x) = F(G(x))$.

$$\pi(x) \log x = O\left(\sum_{k=0}^{K} x/2^k \right) = O(x).$$

□

Jiným zajímavým tvrzením o prvočíslech je Mertensova věta, která podává asymptotiky tří výrazů definovaných pomocí prvočísel.

Věta 9 (Mertens, 1874)

$$\begin{aligned}
\sum_{p \leq x} \frac{\log p}{p} &= \log x + O(1). \\
\sum_{p \leq x} \frac{1}{p} &= \log\log x + c + O(1/\log x). \\
\prod_{p \leq x} \left(1 - \frac{1}{p}\right) &= \frac{c'}{\log x}\,(1 + O(1/\log x)).
\end{aligned}$$

Důkaz. Podle první formule Lemmatu 7 máme

$$\begin{aligned}
x \log x - x + O(\log x) &= \sum_{n \leq x} \Lambda(n) \left\lfloor \frac{x}{n} \right\rfloor \\
&= \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor \log p + \sum_{p^v \leq x,\, v \geq 2} \left\lfloor \frac{x}{p^v} \right\rfloor \log p \\
&= x \sum_{p \leq x} \frac{\log p}{p} + O(x) + \\
&\quad + O\left(x \left(\sum_{n=1}^{\infty} \frac{\log n}{n^2} + \sum_{n=1}^{\infty} \frac{\log n}{n^3} + \cdots \right) \right) \\
&= x \sum_{p \leq x} \frac{\log p}{p} + O(x).
\end{aligned}$$

Dokázali jsme prvou Mertensovu formuli, v důkazu jsme použili horní odhad z Čebyševovy věty (kde?).

Druhá Mertensova formule plyne z první pomocí Abelovy transformace.

$$\begin{aligned}
\sum_{p \leq x} \frac{1}{p} &= \sum_{p \leq x} \frac{\log p}{p} \cdot \frac{1}{\log p} = \frac{1}{\log x} \sum_{p \leq x} \frac{\log p}{p} + \int_2^x \sum_{p \leq t} \frac{\log p}{p} \cdot \frac{dt}{t \log^2 t} \\
&= 1 + O(1/\log x) + \int_2^x \frac{dt}{t \log t} + \int_2^x \left(\sum_{p \leq t} \frac{\log p}{p} - \log t \right) \frac{dt}{t \log^2 t} \\
&= \log\log x + 1 - \log\log 2 + \int_2^{\infty} \frac{w(t) dt}{t \log^2 t} + O\left(\frac{1}{\log x} + \int_x^{\infty} \frac{|w(t)| dt}{t \log^2 t} \right).
\end{aligned}$$

Symbolem $w(t)$ jsme označili omezenou funkci $\sum_{p\le t}\log p/p-\log t$. První integrál konverguje, druhý je $O(1/\log x)$, druhá formule je dokázána.

Formule pro součin vyplývá následovně.

$$\begin{aligned}
\log\prod_{p\le x}(1-1/p) &= \sum_{p\le x}\log(1-1/p) = -\sum_{p\le x}\sum_{n=1}^{\infty}\frac{(1/p)^n}{n}\\
&= -\sum_{p\le x}\frac{1}{p}-\sum_{n\ge 2}\frac{1}{n}\sum_{p\le x}\frac{1}{p^n}\\
&= -\sum_{p\le x}\frac{1}{p}-\sum_{n\ge 2}\frac{1}{n}\sum_{p}\frac{1}{p^n}+O\left(\sum_{n\ge 2}\frac{1}{n}\sum_{p>x}\frac{1}{p^n}\right)\\
&= -\sum_{p\le x}\frac{1}{p}+c''+O\left(\sum_{n\ge 2}\frac{1}{n}\sum_{m>x}\frac{1}{m^n}\right)\\
&= -\sum_{p\le x}\frac{1}{p}+c''+O\left(\sum_{n\ge 2}\frac{1}{n}\cdot\frac{1}{(n-1)x^{n-1}}\right)\\
&= -\log\log x-c+O(1/\log x)+c''+O(1/x).
\end{aligned}$$

V závěru jsme sumu $\sum_{m>x}1/m^n$ odhadli Eulerovou sumační formulí a užili jsme druhou Mertensovu formuli. Odlogaritmováním dostaneme třetí Mertensovu formuli. □

Přesnějším počítáním ve třetí formuli lze ukázat, že

$$c'=e^{-\gamma}.$$

Slavným výsledkem o prvočíslech je tzv. Prvočíselná věta. Tvrdí, že $\pi(x)\log x/x\to 1$ pro $x\to\infty$.

Věta 10 (Hadamard, de la Vallé Poussin, 1896)

$$\pi(x)\sim\frac{x}{\log x}.$$

Pro důsledek viz Příklad 1. Původní důkaz i jeho pozdější zjednodušení využívají metod komplexní analýzy. V letech 1947–48 nalezli Selberg a Erdös důkaz, v kterém se pracuje pouze s elementárními počítacími technikami a reálnou analýzou (ukázky těchto metod jsme si již předvedli a ještě si předvedeme), důkaz sám je ale poměrně komplikovaný.

Lépe než funkcí $x/\log x$ je $\pi(x)$ aproximována funkcí integrállogaritmus

$$li(x)=\int_0^x\frac{dt}{\log t}=\lim_{\varepsilon\to 0}\left(\int_0^{1-\varepsilon}+\int_{1+\varepsilon}^{x}\right)\frac{dt}{\log t}$$

kde používáme zkratku

$$x_k=1+x+x^2+\cdots+x^k=(x^{k+1}-1)/(x-1).$$

Dostáváme tak kvadratickou rovnici

$$xP_k^2-x_kP_k+x_k=0,$$

jejímž řešením je

$$P_k(x)=\frac{x_k-\sqrt{x_k^2-4xx_k}}{2x}.$$

Odvození pro druhou OGF je velmi podobné, jediný rozdíl spočívá v tom, že v druhém případě, kdy se v u vyskytuje 1 právě dvakrát, rozložíme u jako $u=1v1w$. Proto součet obou délek bude $l-2$. Nyní w již může být prázdná. Pro $Q_k(x)$ tak dostaneme vztah

$$Q_k(x)=1+xQ_k(x)+x^2(Q_k(x)-x_{k-1})Q_k(x).$$

Z něj odvodíme kvadratickou rovnici

$$x(xQ_k)^2-(x^2x_{k-1}-x+1)(xQ_k)+x=0.$$

Koeficient u xQ_k lze přepsat, podle definice x_k, jako $x_{k+1}-2x$. Místo k píšeme $k-1$ a řešíme rovnici:

$$xQ_{k-1}(x)=\frac{x_k-2x-\sqrt{(x_k-2x)^2-4x^2}}{2x}.$$

Vidíme, že opravdu platí

$$xQ_{k-1}(x)=P_k(x)-1.$$

□

15 Kompoziční formule a Lagrangeova inverzní formule

Popíšeme dvě důležité techniky, které lze často při práci s GF použít. Každou z nich ilustrujeme jedním příkladem. Dosud jsme se setkali pouze s OGF, nyní budeme pracovat s EGF.

15.1 Součinová formule. Mějme dva typy struktur definované na základní množině $\{1,2,\ldots,n\}$, říkejme jim $\mathcal{F}$-struktury a $\mathcal{G}$-struktury. Symboly f_n a g_n označují počty $\mathcal{F}$-struktur a $\mathcal{G}$-struktur na $\{1,2,\ldots n\}$. Zavedeme si pro ně EGF:

$$F(x)=\sum_{n\ge 1}\frac{f_nx^n}{n!}\ \text{a}\ G(x)=\sum_{n\ge 1}\frac{g_nx^n}{n!}.$$

$X = \{1, 2, \ldots, l\}$, jejichž sjednocením je celá množina X. K číslu l budeme poukazovat jako k *délce* rozkladu. Řekneme, že rozklad je *abab-prostý*, pokud neexistují čtyři čísla $1 \leq x < y < z < t \leq l$ a dva různé bloky B_i, B_j, že by platilo $x, z \in B_i$ a $y, t \in B_j$. Řekneme, že rozklad je *k-pravidelný*, pokud neexistuje blok B_i a dvě čísla $x, y \in B_i$, že $0 < y - x < k$.

Je pohodlnější místo množinového zápisu používat pro rozklady zápis ve tvaru posloupností, popř. *normálních posloupností*. Rozklad P délky l s n bloky se snadno zapíše posloupností nějakých symbolů $u = a_1a_2 \ldots a_l$ tak, že i a j padnou do stejného bloku právě když $a_i = a_j$. Řekneme, že *u určuje P*. Takových u je mnoho, požadujeme-li však, aby navíc $\{a_1, a_2, \ldots, a_l\} = \{1, 2, \ldots, n\}$ a aby pro každé $1 \leq i < j \leq n$ předcházel v u první výskyt i první výskyt j, je u již určena jednoznačně. Takovým u budeme říkat *normální posloupnosti.* Jako příklad si uvedeme všechny 2-pravidelné *abab*-prosté rozklady délky 5 zapsané jako normální posloupnosti:

$$\{12345, 12343, 12342, 12341, 12324, 12321, 12314, 12134, 12131\}.$$

Rozklad nazveme *chudým*, má-li každý blok nejvýše dva prvky. Uvedeme si všechny chudé *abab*-prosté rozklady délky 4:

$$\{1234, 1233, 1232, 1231, 1223, 1221, 1213, 1123, 1122\}.$$

Není náhodné, že nám pokaždé vyšel stejný počet rozkladů.

Věta 41 *Počet k-pravidelných abab-prostých rozkladů délky l je roven počtu $(k-1)$-pravidelných chudých abab-prostých rozkladů délky $l-1$.*

Důkaz. Počet rozkladů prvního typu označíme jako $p(l, k)$ a počet rozkladů druhého typu jako $q(l, k)$. Zavedeme pro obě struktury OGF

$$P_k(x) = \sum_{l \geq 0} p(l, k)x^l \quad \text{a} \quad Q_k(x) = \sum_{l \geq 0} q(l, k)x^l.$$

Nalezneme explicitní vyjádření pro obě OGF a uvidíme, že jsou přesně v tom vztahu, v jakém mají podle identity být.

Uvažme k-pravidelný *abab*-prostý rozklad délky $l \geq 1$ zapsaný normální posloupností u. Pokud se číslo 1 vyskytuje v u jen jednou, rozložíme u jako $u = 1v$. Posloupnost v určuje k-pravidelný *abab*-prostý rozklad o délce $l-1$, který může být zcela libovolný.

Vyskytuje-li se 1 v u vícekrát, rozložíme u podle druhého výskytu 1 jako $u = 1vw$, kde w začíná onou druhou jedničkou. Žádné číslo se nevyskytuje v obou posloupnostech současně. Je zřejmé, že v a w určují nezávisle na sobě dva k-pravidelné *abab*-prosté rozklady. Jediné omezující podmínky jsou, že první rozklad má délku alespoň $k-1$, druhý alespoň 1 a součet jejich délek je $l-1$. První OGF proto splňuje

$$P_k(x) = 1 + xP_k(x) + x(P_k(x) - x_{k-1})(P_k(x) - 1),$$

(viz Příklad 2). Zbytek $R(x)$ ve vyjádření $\pi(x) = li(x) + R(x)$ byl v původním Hadamardově a de la Vallé Poussinově důkazu odhadnut jako

$$R(x) = O\left(xe^{-\delta(\log x)^{1/2}}\right)$$

pro jistou absolutní konstantu $\delta > 0$. Korobov v r. 1958 zesílil tento odhad na

$$R(x) = O\left(xe^{-\delta(\log x)^{3/5}(\log\log x)^{-1/5}}\right).$$

Gauss se domníval, že vždy platí $\pi(x) < li(x)$. To bylo vyvráceno Littlewoodem, podíl

$$\frac{(\pi(x) - li(x))\log x}{\sqrt{x}\log\log x}$$

má pro $x \to \infty$ záporný limes inferior a kladný limes superior. Konkrétní protipříklad ke Gaussově domněnce však není znám, Riele odhadl, že nejmenší z nich nepřesahuje $6.69 \cdot 10^{370}$.

3 Brunovo síto

Poté, co byla Wilesem dokázána Fermatova domněnka, kandidují na pozici nejznámějších nerozhodnutých matematických problémů dvě následující hypotézy.

Hypotéza prvočíselných dvojčat je tvrzení, že existuje nekonečně mnoho prvočísel p, že i $p+2$ je prvočíslo.

Goldbachova hypotéza z r. 1742 tvrdí, že každé sudé číslo $n > 2$ lze zapsat ve tvaru součtu dvou prvočísel.

Matematik V. Brun atakoval v období 1915–24 oba problémy metodou založenou na principu inkluze a exkluze, která byla po něm nazvána Brunovým sítem. Později byla vynalezena další síta: Selbergovo, Linnikovo, Rényiho, … Pro technickou komplikovanost musíme pominout důkazy výsledků dosažených těmito metodami a předvedeme si pouze důkaz používající slabou formu Brunova síta.

Věta 11 (Brun) *Nechť $N = N(x, z)$ je počet přirozených čísel n nepřesahujících $x-2$ a takových, že n ani $n+2$ nemají prvočinitele nepřesahujícího z. Předpokládejme, že $z \leq x^{1/(20\log\log x)}$ a $x, z \to \infty$. Pak*

$$N \sim e^{-2\gamma}\alpha\,\frac{x}{\log^2 z}, \quad \text{kde } \alpha = 2\prod_{p>2}(1 - (p-1)^{-2}) = 1.3202\ldots$$

Připomínáme, že γ je Eulerova-Mascheroniova konstanta. Označme si jako

$$\mathcal{D} = \{3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 43, \ldots\}$$

množinu všech prvočíselných dvojčat.

Důsledek 12 (Brun) *Počet prvočíselných dvojčat $\leq x$ je $O(x(\log\log x)^2/\log^2 x)$. Tudíž suma reciprokých hodnot dvojčat*

$$\sum_{p\in\mathcal{D}} \frac{1}{p}$$

konverguje (nebo je konečná).

Důkaz. Důsledek plyne z Věty 11 snadno Abelovou transformací. Označíme-li počet dvojčat nepřesahujících x jako $D(x)$, máme

$$\sum_{p\in\mathcal{D},\, p\leq x} \frac{1}{p} = \frac{D(x)}{x} + \int_2^x \frac{D(t)}{t^2}dt$$

a zbytek je rutinní a snadné odhadování. $\Box$

Důkaz. (Věty 11) Uvažme konečné množiny $A_1, A_2, \ldots, A_n$ obsažené v jiné konečné množině A. Princip inkluze a exkluze říká, že

$$|\,\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_n}\,| = \sum_{i=0}^{n} (-1)^i P_i, \text{ kde}$$

$\overline{A_i}$ je doplněk A_i v A, $P_0 = |A|$ a

$$P_i = \sum_{|I|=i} |\bigcap_{j\in I} A_j|.$$

Jenoduché lemma, známe jako "Bonferoniho nerovnosti", říká, že suma $\sum_{i=0}^{m}(-1)^i P_i$ podhodnocuje kardinalitu průniku na levé straně pro liché m a nadhodnocuje ji pro m sudé. Položíme

$$\mathcal{A} = \{n(n+2) :\ n \in \mathbf{N}, n \leq x-2\},\ \mathcal{P} = \{\text{prvočísla } \leq z\},$$

$$\mathcal{A}(d) = \{a \in \mathcal{A} :\ d|a\} \text{ a } \omega(d) = |\{n :\ 0 \leq n < d,\ n(n+2) \equiv 0 \pmod d\}|.$$

Jako $\nu(n)$ označíme počet prvočinitelů čísla n. Pro čtvercuprosté d platí

$$\left||\mathcal{A}(d)| - \omega(d)\,\frac{x}{d}\right| \leq \omega(d) \leq 2^{\nu(d)},$$

několika přirozených sčítanců. Dva rozklady lišící se pouze pořadím sčítanců nepovažujeme za různé. Sčítance se mohou opakovat. Uveďme si všechny různé rozklady čísla 6.

$$\begin{array}{rll} 6 = & 6 & 1+2+3 \\ & 1+5 & 2+2+2 \\ & 2+4 & 1+1+1+3 \\ & 3+3 & 1+1+2+2 \\ & 1+1+4 & 1+1+1+1+2 \\ & & 1+1+1+1+1+1. \end{array}$$

Z jedenácti rozkladů mají čtyři všechny sčítance různé a rovněž přesně čtyři rozklady obsahují pouze liché sčítance. Dokážeme si pomocí GF, že se tyto dva počty rovnají bez ohledu na to, jaké číslo rozkládáme.

> **Euler:** Počet rozkladů čísla n na různé sčítance se rovná počtu rozkladů na liché sčítance.

První počet si označíme jako $r(n)$ a druhý jako $l(n)$. Není obtížné najít explicitní vyjádření pro OGF posloupností $\{r(n)\}_{n\geq 0}$ a $\{l(n)\}_{n\geq 0}$:

$$\sum_{n\geq 0} r(n)x^n = (1+x)(1+x^2)(1+x^3)(1+x^4)\cdots$$

a

$$\sum_{n\geq 0} l(n)x^n = \frac{1}{(1-x)(1-x^3)(1-x^5)(1-x^7)\cdots}.$$

Ukážeme, že výrazy na pravé straně určují tutéž mocninnou řadu. Uvědomíme-li si, že

$$1+x = \frac{1-x^2}{1-x},\ 1+x^2 = \frac{1-x^4}{1-x^2},\ 1+x^3 = \frac{1-x^6}{1+x^3}, \ldots$$

můžeme první pravou stranu přepsat ve tvaru

$$\frac{(1-x^2)(1-x^4)(1-x^6)(1-x^8)(1-x^{10})\cdots}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)\cdots}.$$

Členy se sudými exponenty ve jmenovateli se zkrátí oproti všem členům v čitateli a co zůstane, je přesně druhá pravá strana.

14.2 Dva druhy množinových rozkladů. Zde budeme slovem *rozklad* rozumět soubor neprázdných a disjunktních podmnožin (zvaných *bloky*) $\{B_1, \ldots, B_n\}$ množiny

Podle právě vysvětleného tvrzení má tento kvadratický polynom jen reálné kořeny (dokonce se stejným znaménkem) a proto jeho diskriminant je nezáporný:

$$c_{n-m-1}^2 - \frac{c_{n-m-2}(m+2)}{n-m-1} \cdot \frac{c_{n-m}(n-m)}{m+1} \geq 0.$$

Odtud se hned vidí, že

$$c_{n-m-1}^2 > c_{n-m-2}c_{n-m}.$$

Unimodalita je dokázána. □

Protože kořeny polynomu

$$\sum_{k=1}^{n} c(k,n)t^{k-1}$$

jsou podle Věty 39 čísla $-1, -2, \ldots, -n+1$, dostáváme výsledek

> Posloupnost Stirlingových čísel prvního druhu $\{c(k,n)\}_{k=1}^n$ je unimodální.

Stirlingova čísla druhého druhu $d(k,n)$ jsou definována jako počet rozkladů n-prvkové množiny na k neprázdných disjunktních podmnožin. Jejich unimodalitu lze dokázat obdobným způsobem.

14 Důkazy identit

Identitou se v kombinatorice rozumí překvapivá rovnost mezi dvěma zdánlivě zcela odlišnými výrazy. Výrazy bývají často ve tvaru sum členů zahrnujících binomické koeficienty. Často se ale také identitou rozumí rovnost počtů kombinatorických struktur dvou zdánlivě odlišných druhů. Identity se dokazují dvěma základními způsoby. V *bijektivním důkazu* se nalezne bijekce mezi oběma druhy struktur. Je třeba prohlédnout onu zdánlivost a ukázat, jakým způsobem proměnit jednu strukturu v druhou. V *důkazu pomocí GF* se určí OGF či EGF pro počty obou struktur a ukáže se, že jde o jednu a tutéž funkci. V této kapitole si předvedeme dva příklady ilustrující druhý přístup.

14.1 Rozklady čísel na liché sčítance a na různé sčítance. Tato pěkná identita pochází od Eulera. *Rozkladem* přirozeného čísla n rozumíme jeho vyjádření jako součtu

protože funkce $\omega(d)$ je podle Čínské věty o zbytku multiplikativní a $\omega(p) = 2$. Dále položíme

$$P(z) = \prod_{p \in \mathcal{P}} p \quad \text{a} \quad N = |\{a \in \mathcal{A}: \ \text{žádné } p \in \mathcal{P} \text{ nedělí } a\}|.$$

Připomeňme nyní Möbiovu funkci $\mu(n)$ definovanou jako 1 pro $n = 1$, jako 0 pro n dělitelné čtvercem větším než 1, a jako $(-1)^k$ pro n rovno součinu k různých prvočísel. Podle principu inkluze a exkluze a Bonferoniho nerovností platí — parametr t určíme později —

$$\begin{aligned} N &= \sum_{\substack{d|P(z) \\ \nu(d) \leq 2t}} \mu(d)\,|\mathcal{A}(d)| + O\Big(\sum_{\substack{d|P(z) \\ \nu(d) = 2t}} |\mathcal{A}(d)|\Big) \\ &= x \sum_{d|P(z)} \mu(d)\,\frac{\omega(d)}{d} + O\Big(x \sum_{\substack{d|P(z) \\ \nu(d) \geq 2t}} \frac{\omega(d)}{d}\Big) + O\Big(x \sum_{\substack{d|P(z) \\ \nu(d) \leq 2t}} 2^{\nu(d)}\Big) \\ &= x \sum_{d|P(z)} \mu(d)\,\frac{\omega(d)}{d} + O(E_1) + O(E_2). \end{aligned}$$

Suma se rovná

$$\sum_{d|P(z)} \mu(d)\,\frac{\omega(d)}{d} = \prod_{p \leq z}\Big(1 - \frac{\omega(p)}{p}\Big) \ \sim \ e^{-2\gamma}\alpha/\log^2 z.$$

Při úpravě jsme využili třetí formuli Mertensovy věty, rovností $\omega(2) = 1$ a $\omega(p) = 2$, a multiplikativity ω.

Nyní odhadneme zbytek E_1.

$$E_1 \leq x \sum_{l \geq 2t} 2^l \sum_{\substack{d|P(z) \\ \nu(d) = l}} \frac{1}{d} \leq x \sum_{l \geq 2t} \frac{2^l}{l!}\Big(\sum_{p \leq z} \frac{1}{p}\Big)^l \leq x \sum_{l \geq 2t} \frac{1}{l!}(2\log\log z + 2c)^l.$$

To lze majorizovat prvním členem, volíme totiž $t = \lfloor 5 \log\log z \rfloor$. Tedy

$$E_1 = O\Big(\frac{x}{(2t)!}(2\log\log z + 2c)^{2t}\Big) = O\left(x(e/5)^{10\log\log z}\right) = O(x/\log^6 z).$$

Nyní odhadneme zbytek E_2.

$$E_2 \leq 2^{2t} \sum_{\substack{d|P(z) \\ \nu(d) \leq 2t}} 1 \leq 2^{2t}\pi(z)^{2t}.$$

Proto $E_2 \le z^{2t} = O(x^{1/2})$. Celkově

$$N \sim xe^{-2\gamma}\alpha \log^{-2} z + O(x \log^{-6} z).$$

$\square$

Nechť pro $n \in \mathbf{N}$ s prvočíselným rozkladem $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ označuje $s(n)$ jeho složitost, tj. $s(n) = \alpha_1 + \ldots + \alpha_k$. Brun se v předchozí větě dokázal zbavit faktoru $\log\log x$.

Věta 13 (Brun, 1919) *Existuje nekonečně mnoho čísel n, pro něž $s(n), s(n+2) \le 7$ (Brun ukázal, že počet takových $n \le x$ se chová zhruba jako $x/\log^2 x$).*

Obdobný výsledek obdržel Brun pro Goldbachův problém.

Metodami síta byla dokázána následující věta. Její důkaz je komplikovaný a proto ho neuvádíme, větu samu však v budoucnu několikrát použijeme.

Věta 14 *Nechť $a_i, b_i \in \mathbf{N}_0$ je k dvojic nesoudělných čísel, která splňují*

$$E = \prod a_i \prod (a_r b_s - a_s b_r) \ne 0.$$

Nechť $0 < \varepsilon < 1$ a x, y jsou reálná čísla. Položme

$$\mathcal{A} = \{\prod (a_i n + b_i) : \ n \in \mathbf{N}, \ x - y < n \le x\}$$

a

$$\omega(p) = |\{0 \le n < p : \ \prod (a_i n + b_i) \equiv 0 \pmod p\}|.$$

Nechť dále $z = y^\varepsilon$. Potom

$$|\{n \in \mathcal{A} : \ n \text{ nemá prvočinitele} \le z\}| \le c \cdot \prod_{p|E,\ p \le y} (1 - 1/p)^{\omega(p)-k} \cdot \frac{y}{\log^k y},$$

kde konstanta c závisí jen na k a ε.

Důsledek 15

$$\exists \quad c > 0, \text{ že } |\{q : \ q \text{ a } q+2 \text{ jsou prvočísla}, \ q \le x - 2\}| \le \frac{cx}{\log^2 x}$$

$$\exists \quad c > 0, \text{ že } |\{p : \ p \text{ a } n - p \text{ jsou prvočísla}\}| \le c \prod_{p|n} (1 - 1/p)^{-1} \cdot \frac{n}{\log^2 n}$$

$$\exists \quad c > 0, \text{ že } \pi(x) - \pi(x - y) \le cy/\log y.$$

Nyní již jsme schopni dokázat unimodalitu čísel $c(k, n)$. Dokážeme dokonce, že se vyznačují jistou silnější vlastností. Posloupnost $(c_1, c_2, \ldots, c_n)$ reálných čísel se nazývá *log-konkávní*, platí-li pro každé $j = 1, 2, \ldots, n-1$ nerovnost $c_{j-1} c_{j+1} \le c_j^2$. Nastává-li ostrá nerovnost, mluvíme o *ostré log-konkavitě*. Povšimněme si, že v případě kladných čísel log-konkavita implikuje unimodalitu.

Věta 40 *$p(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ buď polynom, jehož všechny kořeny jsou záporná reálná čísla (nebo jsou všechny kladná reálná čísla). Pak $\{c_k\}_{k=0}^n$ je ostře log-konkávní.*

Důkaz. Nejprve si uvědomíme, že i všechny derivace polynomu p mají všechny kořeny záporné (nebo všechny kladné). Skutečně, má-li p celkem m různých záporných kořenů, přispějí počtem $n - m$ k počtu kořenů derivace p' (protože zderivováním se násobnost kořene snižuje o 1). V každé z $m - 1$ mezer mezi kořeny však podle Rolleovy věty musí vzniknout další kořen p'. Máme již, počítáno s násobnostmi, alespoň $n - m + m - 1 = n - 1$ záporných reálných čísel, která jsou kořeny p'. Vyčerpali jsme nevyhnutelně všechny kořeny.

Odtud vyplývá, že homogení polynom ve dvou proměnných

$$f(x, y) = c_0 x^n + c_1 x^{n-1} y + c_2 x^{n-2} y^2 \cdots + c_n y^n$$

má po libovolné kombinaci derivování podle x a podle y všechny kořeny záporné (nebo všechny kladné).

Toto tvrzení je asi nutné blíže vysvětlit. Polynom $f(x, y)$ píšeme jako $f(x, y) = x^n p(y/x) = y^n q(x/y)$ a jeho kořeny rozumíme kořeny polynomů jedné proměnné $p(z)$ a $q(z)$. Připomínáme, že p má všechny kořeny záporné (nebo všechny kladné) a tudíž má všechny koeficienty nenulové. Zřejmě $q(z) = p(1/z)$ a proto i q má všechny kořeny záporné (nebo všechny kladné). Parciálním zderivováním f podle y dostaneme opět homogení polynom (stupně $n - 1$) a navíc

$$\frac{\partial f}{\partial y} = x^{n-1} p'(y/x).$$

Podobně pro $\partial f/\partial x$. Proto dostáváme po zderivování vždy všechny kořeny reálné a s týmž znaménkem.

Po m-násobném zderivování podle x a $n - m - 2$-násobném zderivování podle y a vydělení koeficientem

$$\frac{(m+1)!(n-m-1)!}{2}$$

dostaneme

$$\frac{c_{n-m-2}(m+2)}{n-m-1} x^2 + 2c_{n-m-1} xy + \frac{c_{n-m}(n-m)}{m+1} y^2.$$

Nechť $s = a_1 a_2 \dots a_n \in S_n$ je permutace zapsaná ve tvaru posloupnosti. Řekneme, že i je jejím *levopravým minimem*, pokud $a_j > a_i$ pro všechna $j < i$. Např. levopravými minimy permutace 35214 jsou 1, 3 a 4.

Lemma 37 *$c(k,n)$ je rovno počtu permutací v S_n s k levopravými miminimy.*

Důkaz. Danou $\pi \in S_n$ s k cykly zapíšeme v posloupnostním tvaru následujícím kanonickým způsobem. Každý cyklus napíšeme jako posloupnost, přičemž začneme jeho nejmenším prvkem. Tyto posloupnosti seřadíme klesavě podle nejmenších prvků a shrneme je takto do jediné posloupnosti. Ta představuje hledaný posloupnostní tvar π. Např.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 6 & 3 \end{pmatrix}$$

se zakóduje jako

$$356214.$$

Dostaneme posloupnost s k levopravými minimy, úseky určené minimy odpovídají přesně cyklům. Nyní je jistě jasné, jak naopak z posloupnosti čísel $1, 2, \dots, n$ s k levopravými minimy vyrobit permutaci s k cykly. Tato bijekce dokazuje tvrzení lemmatu. $\square$

Pro permutaci $s = a_1 a_2 \dots a_n \in S_n$ budeme *tabulkou inverzí* rozumět posloupnost $b_1 b_2 \dots b_n$, kde

$$b_j = |\{i:\ i < j, a_i > a_j\}|.$$

Např. 35214 má tabulku inverzí 00231.

Lemma 38 *Existuje bijekce mezi S_n a množinou tabulek inverzí*

$$T_n = \{0\} \times \{0,1\} \times \dots \times \{0, 1, \dots, n-1\}.$$

Důkaz. Zřejmý. $\square$

Je jasné, že pro permutaci $s = a_1 a_2 \dots a_n \in S_n$ s tabulkou inverzí $b_1 b_2 \dots b_n$ je j levopravým minimem právě když $b_j = j - 1$. V T_n, v j-té souřadnici, přidělme číslu $j-1$ váhu t a ostatním váhu 1. Generující polynom pro permutace $\pi \in S_n$ podle počtů levopravých minim pak je

$$t(t+1)(t+1+1)\cdots(t+1+1+\dots+1) = t(t+1)(t+2)\cdots(t+n-1).$$

Tato úvaha a obě předchozí lemmata dohromady dávají následující tvrzení.

Věta 39

$$\sum_{k=1}^{n} c(k,n)t^k = t(t+1)(t+2)\cdots(t+n-1).$$

Důkaz. Pro první dvě tvrzení položíme v předchozí větě $k = 2, a_1 = 1, b_1 = 0, x = y, \varepsilon = 1/2$. Pro první tvrzení položíme dále $a_2 = 1, b_2 = 2$, pro druhé $a_2 = -1, b_2 = n$. Třetí odhad dostaneme z volby $k = 1, a_1 = 1, b_1 = 0, \varepsilon = 1/2$. $\square$

Věta 16 (Chen, cca 1970) *Existuje nekonečně mnoho dvojic $n, n+2$, v nichž je jeden člen prvočíslem a druhý je součinem nejvýše dvou prvočísel.*

Chen dokázal analogický výsledek v Goldbachově problému pro dostatečně velké sudá čísla.

Pišme $d_n = p_n - p_{n-1}$ pro mezeru mezi po sobě jdoucími prvočísly. Z prvočíselné věty plyne, že

$$\liminf_{n\to\infty} \frac{d_n}{\log n} \le 1.$$

Věta 17 (Erdös, 1940)

$$\liminf_{n\to\infty} \frac{d_n}{\log n} \le c < 1.$$

Důkaz. Plyne z Věty 14 a jednoho elementárního odhadu. Nechť $\varepsilon > 0$ je pevné. Předpokládejme, že $\liminf_{n\to\infty} d_n/\log n > 1 - \varepsilon/2$. Tudíž pro $x \ge x_0$ nerovnost $n > \pi(x/\log x)$ implikuje $d_n > (1-\varepsilon)\log x$.

Položíme L rovno $\pi(x) - \pi(x/\log x)$ a definujeme $\delta = \delta(x,\varepsilon) > 0$ pomocí

$$\delta L = |\{n:\ \pi(x/\log x) < n \le \pi(x),\ (1-\varepsilon)\log x < d_n < (1+\varepsilon)\log x\}|.$$

Protože $x \ge x_0$, dostáváme

$$\delta L(1-\varepsilon)\log x + (1-\delta)L(1+\varepsilon)\log x \le \sum_{n \le \pi(x)} d_n \le x.$$

Tudíž

$$\varepsilon(1-2\delta) \le \frac{x}{L\log x} - 1.$$

Protože $L\log x \sim x$, máme pro $x \ge x_1(\varepsilon)$ nerovnost $\delta > 1/3$ (δ můžeme dostat k $1/2$ tak blízko, jak chceme).

Tento odhad nyní pomocí Věty 14 přivedeme ke sporu — ukážeme, že $\delta = O(\varepsilon)$. Definujeme si $D(t,x)$ jako počet prvočísel $p \le x$, pro něž $p + t$ je rovněž prvočíslo. Zřejmě platí

$$\delta L \le \sum_{(1-\varepsilon)\log x < t < (1+\varepsilon)\log x} D(t,x).$$

Věta 14 dává ($k = 2,\ a_1 = 1,\ b_1 = 0,\ a_2 = 1,\ b_2 = t,\ x = y,\ \varepsilon = 1/2$)

$$D(t, x) \le c' \cdot \prod_{p|t,\ p\le x} \left(1 - \frac{1}{p}\right)^{-1} \cdot \frac{x}{\log^2 x}.$$

Elementárními odhady, které neuvádíme, lze spočítat, že pro $u \to \infty$

$$\sum_{t\le u} \prod_{p|t} \left(1 - \frac{1}{p}\right)^{-1} \sim c''u.$$

Tudíž

$$\sum_{(1-\varepsilon)\log x<t<(1+\varepsilon)\log x} D(t, x) \le c'(c'' + o(1))2\varepsilon \log x \cdot x/\log^2 x.$$

Odhadli jsme tedy, že $\delta \le 3c'c''\varepsilon$, kde x je dostatečně velké (v závislosti na ε) a c', c'' jsou absolutní konstanty. Pro $\varepsilon \to 0$ dostáváme spor. □

Věta 18 (Maier, 1988) *Předešlá věta platí s konstantou $c < 1/4$.*

4 Báze a podstatné komponenty

Goldbachova hypotéza je úlohou aditivní teorie čísel, což je disciplína zabývající se vyjádřeními přirozených čísel jako součtů sčítanců z předem dané množiny. K slavným úlohám tohoto typu patří

Waringova hypotéza z r. 1770. Tvrdí, že pro každé $n \in \mathbf{N}$ existuje $g = g(n) \in \mathbf{N}$, že pro každé $x \in \mathbf{N}$ má rovnice

$$x = y_1^n + y_2^n + \ldots + y_g^n$$

řešení v $\mathbf{N_0}$.

Česky řečeno, každé přirozené číslo lze napsat jako součet omezeně mnoha n-tých mocnin přirozených čísel. V roce 1770 Lagrange dokázal, že $g(2) = 4$ (uvážíme-li čísla tvaru $8n+7$ vidíme, že $g(2) = 3$ neplatí) a v roce 1909 Hilbert Waringovu hypotézu dokázal, nyní to již tedy je věta. V této kapitole ukážeme překvapivě elementární kombinatorickou techniku, kterou byly pro aditivní úlohy dosaženy netriviální výsledky.

Řekneme, že $\mathcal{A} \subset \mathbf{N}$ je *báze řádu k*, pokud každé $x \in \mathbf{N}$ je součtem nejvýše k sčítanců z $\mathcal{A}$. Řekneme, že $\mathcal{A} \subset \mathbf{N}$ je *asymptotická báze řádu k*, pokud to platí pro

Věta 36 (Pringsheim) *Nechť*

$$F(z) = \sum_{n\ge 0} a_n z^n$$

je mocninná řada s nezápornými reálnými koeficienty a poloměrem konvergence $R, 0 < R < \infty$. Pak R je nutně singularitou F.

V orámečkovaném principu jsou tedy znaky absolutních hodnot zbytečné, protože vždy můžeme vzít $\alpha = R$ jako kladné reálné číslo. Na konvergenční kružnici se ovšem mohou nacházet i další singularity, které už jsou obecně komplexní a ty je třeba při hledání přesné asymptotiky již brát v úvahu.

13 Unimodalita posloupností

Posloupnost nezáporných reálných čísel $a_1, a_2, \ldots, a_n$ se nazývá *unimodální*, existuje-li index k tak, že

$$a_1 \le a_2 \le \cdots \le a_k \ge a_{k+1} \ge \cdots \ge a_n.$$

Unimodální posloupnost tedy monotóně stoupá ke svému vrcholu a potom zase monotóně klesá. Takové posloupnosti se v kombinatorice vyskytují často. Příkladem je posloupnost binomických koeficientů

$$\left\{\binom{n}{k}\right\}_{k=0}^{n}.$$

Ta je mimoto symetrická, tj. $\binom{n}{k} = \binom{n}{n-k}$, a její unimodalitu je lehké dokázat, máme totiž k dispozici explicitní formuli pro obecný člen. Stává se však, že je k dispozici pouze kombinatorická definice posloupnosti a pak může důkaz unimodality představovat nelehký problém. Ukážeme si na jednom příkladu, jak za takových okolností mohou GF pomoci.

13.1 Stirlingova čísla prvního druhu. Symbolem S_n zde rozumíme množinu všech permutací na $\{1, 2, \ldots, n\}$. Stirlingova čísla prvního druhu $c(k, n)$ jsou definována jako počet permutací z S_n, které mají právě k cyklů. Posloupnost

$$\{c(k, n)\}_{k=1}^{k=n}$$

je unimodální. Abychom to dokázali, musíme nejprve odvodit formuli pro generující polynom

$$\sum_{k=1}^{n} c(k, n)t^k.$$

Proto α bude kořen kvadratického polynomu $1 - 6x + x^2$ nejbližší počátku. Zřejmě $\alpha = 3 - 2\sqrt{2}$ a odtud vyplývá, že počet rozřezání n-úhelníku — Schröderovo číslo — roste jako $(1/\alpha)^n = (3+2\sqrt{2})^n$.

Pokud nás v příkladu 11.1 zajímá asymptotika počtů $f_A(n)$ nebo $g_A(n)$, stačí nalézt kořen polynomu

$$z^k + (1-2z)C_A(z)$$

ležící nejblíže počátku.

V příkladu 11.2 pracujeme s OGF

$$\frac{x(1+3\sqrt{1-4x})}{4(1-9x/2)}.$$

Odtud plyne, že celkový počet řetězců v pěstovaných stromech s n vrcholy roste jako $(9/2)^n$. Průměrný počet $\overline{r}(n)$ tudíž roste jako $(9/8)^n$. Asymptotiku $r(n)$ určíme přesně. Budeme potřebovat následující větu. Důkaz je snadný, ale z důvodu stručnosti ho pomineme.

Věta 35 (Bender)

$$a(z) = \sum_{n\geq 0} a_n z^n \ \text{ a } \ b(z) = \sum_{n\geq 0} b_n z^n$$

buďte mocninné řady s poloměry konvergence $\alpha > \beta \geq 0$. Nechť $b_{n-1}/b_n \to \beta$ pro $n \to \infty$ a nechť $a(\beta) \neq 0$. Pak pro

$$a(z)b(z) = \sum_{n\geq 0} c_n z^n$$

máme

$$c_n \sim a(\beta)b_n.$$

V příkladu 11.2 položíme

$$a(x) = \frac{x(1+3\sqrt{1-4x})}{4} \text{ a } b(x) = \frac{1}{1-9x/2}.$$

Dále $\alpha = 1/4$, $\beta = 2/9$ a $b_n = (9/2)^n$. Větu lze použít a pro počet řetězců $r(n)$ dostáváme asymptotiku

$$r(n) \sim a(2/9)\left(\frac{9}{2}\right)^n = \frac{1}{9}\left(\frac{9}{2}\right)^n.$$

Ve všech našich použitích orámečkovaného principu vyšla singularita ležící nejblíže počátku dokonce jako kladné reálné číslo. To nebyla náhoda.

dostatečně velká x. Řekneme-li krátce, že $\mathcal{A}$ je *(asymptotickou) bazí*, znamená to, že $\mathcal{A}$ je (asymptotickou) bazí nějakého řádu. V dalším $\mathcal{P} = \{2, 3, 5, 7, \ldots\}$ označuje množinu všech prvočísel. Z Goldbachovy hypotézy triviálně plyne, že $\mathcal{P} \cup \{1\}$ je bazí řádu 3 (a tu 1 potřebujeme jen pro vyjádření 1). To je zřejmě nejnižší možný řád. Hardy a Littlewood v r. 1922 dokázali, za předpokladu Riemannovy hypotézy, že každé dostatečně velké liché číslo je součtem tří prvočísel. Vinogradov v r. 1937 dokázal tento výsledek absolutně, tj. bez použití jakékoli nedokázané hypotézy. Tudíž $\mathcal{P}$ je asymptotická báze řádu 4. Vinogradov použil analytických metod, prvním průlomem v této oblasti byl však Šnirelmannův výsledek, který je založen na kombinatorické metodě.

Věta 19 (Šnirelmann, 1930) *$\mathcal{P} \cup \{1\}$ je bazí.*

Čísla 1 se ale umíme snadno zbavit. Tedy: každé $n > 1$ je součtem omezeně mnoha prvočísel. Šnirelmannovu větu si nyní téměř dokážeme ("téměř" proto, že v jistém kroku se potřebuje výsledek o síle Věty 14). Budeme sledovat původní Šnirelmannův postup.

Šnirelmannova hustota $\sigma(\mathcal{A})$ množiny $\mathcal{A} \subset \mathbf{N}$ je definována jako

$$\sigma(\mathcal{A}) = \inf_{n\in\mathbf{N}} \frac{|\mathcal{A} \cap \{1, 2, \ldots, n\}|}{n}.$$

Všimněme si, že podle této definice má $\mathcal{A}$ neobsahující 1 nulovou Š. hustotu. Symbol $\mathcal{A} + \mathcal{B}$ označuje množinu

$$\{a + b : \ a \in \mathcal{A}, \ b \in \mathcal{B}\}.$$

Symbolem $k\mathcal{A}$ označíme k-násobný součet

$$\mathcal{A} + \mathcal{A} + \cdots + \mathcal{A}.$$

Lemma 20 *Nechť $\mathcal{A}, \mathcal{B} \subset \mathbf{N}_0$ a $0 \in \mathcal{A} \cap \mathcal{B}$. Potom*

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B}).$$

Důkaz. Búno $\sigma(\mathcal{A}) > 0$, tedy $1 \in \mathcal{A}$. $1 = a_1 < a_2 < \cdots < a_k$ buďte prvky množiny $\mathcal{A} \cap \{1, 2, \ldots, n\}$. Patrně $a_i \in \mathcal{A} + \mathcal{B}$. Platí

$$\begin{aligned} |\{c \in \mathcal{A} + \mathcal{B} : \ a_i < c < a_{i+1}\}| &\geq (a_{i+1} - a_i - 1)\sigma(\mathcal{B}) \text{ a} \\ |\{c \in \mathcal{A} + \mathcal{B} : \ a_k < c \leq n\}| &\geq (n - a_k)\sigma(\mathcal{B}). \end{aligned}$$

Celkem

$$
\begin{aligned}
|(\mathcal{A}+\mathcal{B})\cap\{1,2,\dots,n\}| &\geq k+(n-a_k)\sigma(\mathcal{B})+\sum_{i=1}^{k-1}(a_{i+1}-a_i-1)\sigma(\mathcal{B}) \\
&= k+(n-a_1-k+1)\sigma(\mathcal{B}) \\
&= k+(n-k)\sigma(\mathcal{B}) = (1-\sigma(\mathcal{B}))k+n\sigma(\mathcal{B}) \\
&\geq (1-\sigma(\mathcal{B}))n\sigma(\mathcal{A})+n\sigma(\mathcal{B}).
\end{aligned}
$$

Čili $\sigma(\mathcal{A}+\mathcal{B}) \geq \sigma(\mathcal{A})+\sigma(\mathcal{B})-\sigma(\mathcal{A})\sigma(\mathcal{B})$. □

Lemma 21 *Nechť $\mathcal{A},\mathcal{B}\subset \mathbf{N}_0$, $0\in\mathcal{A}\cap\mathcal{B}$ a $\sigma(\mathcal{A})+\sigma(\mathcal{B})\geq 1$. Potom*

$$\mathcal{A}+\mathcal{B}=\mathbf{N}_0.$$

Důkaz. Zavedeme si zkratku $A^*(n) = |\mathcal{A}\cap\{1,2,\dots,n\}|$. Potřebujeme ukázat, že $n=a+b$ má pro každé přirozené n řešení $a\in\mathcal{A}$, $b\in\mathcal{B}$. Můžeme předpokládat, že $n>1$ a $n\notin\mathcal{A}\cup\mathcal{B}$. Potom $n\leq A^*(n)+B^*(n)=A^*(n-1)+B^*(n-1)$. Množiny $\{a\in\mathcal{A}:\ 0<a<n\}$ a $\{n-b:\ b\in\mathcal{B}, 0<b<n\}$ mají tedy dohromady více než $n-1$ prvků a proto nutně nastane $a=n-b$. Tím jsme hotovi. □

Věta 22 (Šnirelmann) *Každá $\mathcal{A}\subset\mathbf{N}$ s kladnou Šnirelmannovou hustotou je nutně bazí.*

Důkaz. K $\mathcal{A}$ přidáme nulu. Pomocí Lemmatu 20 se snadno indukcí dokáže, že $\sigma(k\mathcal{A})\geq 1-(1-\sigma(\mathcal{A}))^k$. Pro dostatečně velké k tedy platí $\sigma(k\mathcal{A})\geq 1/2$. Podle předchozího lemmatu $2k\mathcal{A}=\mathbf{N}_0$ a tedy $\mathcal{A}$ je bazí řádu $2k$. □

Tento pozoruhodný výsledek nemůžeme bezprostředně použít na množinu prvočísel, protože ta má nulovou Š. hustotu. Avšak:

Věta 23 (Šnirelmann) *Označme si $\mathcal{P}_1=\mathcal{P}\cup\{0,1\}$. Pak $\sigma(2\mathcal{P}_1)>0$.*

Důkaz. Potřebujeme ukázat, že

$$\liminf_{n\to\infty}\frac{|\{m:\ 1\leq m\leq n,\ m=p+q\}|}{n}>0.$$

Odvodíme to jako důsledek (v tomto textu nedokázané) Věty 14 (všimněme si, že tato věta podává horní odhad, my však nyní potřebujeme odhad dolní). Pro přirozené n

Nechť OGF posloupnosti $\{a_n\}_{n\geq 0}$

$$\sum_{n\geq 0} a_n z^n$$

určuje funkci $F(z)$ holomorfní v nějakém okolí počátku, ne však v celém $\mathbf{C}$. Nechť $\alpha\in\mathbf{C}$ je singularita $F(z)$ nejbližší k počátku. Potom ze všech exponenciálních funkcí c^n, $c>0$, aproximuje růst čísel a_n nejlépe funkce $(1/|\alpha|)^n$, tj.

$$|a_n| < \left(\frac{1}{|\alpha|-\varepsilon}\right)^n$$

pro každé $\varepsilon>0$ pro $n>n(\varepsilon)$, ale

$$|a_n| > \left(\frac{1}{|\alpha|+\varepsilon}\right)^n$$

pro každé $\varepsilon>0$ pro nekonečně mnoho n.

Budeme to zkracovat rčením "a_n roste jako $(1/|\alpha|)^n$". Je to samozřejmě mnohem slabší výsledek než asymptotika typu $\sim$, kterou bychom chtěli odvodit; pro ni bychom potřebovali některé další (ale celkem jednoduché) poznatky z komplexní analýzy. Přesto i tato slabá asymptotika ukazuje zjevně sílu GF. Podívejme se na naše předchozí příklady.

V příkladu 9.2 se OGF rovná

$$\frac{1-\sqrt{1-4x}}{2}.$$

Jediná singularita je $\alpha=1/4$ a proto Catalanova čísla c_n rostou jako 4^n. Stirlingova formule však dává přesnou asymptotiku typu $\sim$. Totéž v příkladu 9.4.

V příkladu 10.1 je OGF rovna

$$\frac{y(1-y)^3}{1-5y+7y^2-4y^3}.$$

Proto je důležitý kořen kubického polynomu ve jmenovateli ležící nejblíže počátku. Označme jej jako α, není těžké jej nalézt numericky. Počty vodorovně konvexních polymin a_n rostou tudíž jako $(1/\alpha)^n=(3.2055\dots)^n$.

V příkladu 10.2 je OGF rovna

$$\frac{x(1-3x-\sqrt{1-6x+x^2})}{4}.$$

časté jsou i ty případy, kdy známe explicitně pouze rovnici, kterou naše GF splňuje. Nicméně skoro vždy je tato informace dostatečná k určení přesné asymptotiky obecného členu posloupnosti. Tento postup je většinou nejelegantnější a často i jedinou možností, jak asymptotiku nalézt. Zde fungují GF jako most mezi diskrétním a spojitým nejlépe a zde se nalézají nejhlubší výsledky metody GF.

Diskrétní stranou mostu jsou kombinatorické rekurence a závislosti, které vyvodíme pro danou strukturu kombinatorickými úvahami a které se zrcadlí v GF odpovídajícími funkcionálními závislostmi. Spojitou, přesněji řečeno *analytickou*, stranou mostu je GF sama a na ni použitelná teorie funkce komplexní proměnné. Nechceme po čtenáři vyžadovat rozsáhlejší znalosti komplexní analýzy. Spokojíme se tedy s tím, že uvedeme bez důkazu několik základních tvrzení a ukážeme, jak z nich plynou výsledky o asymptotice.

Věta 33 *Nechť*

$$S = \sum_{n \geq 0} a_n z^n$$

je mocninná řada s komplexními koeficienty. Pak existuje právě jedno $0 \leq R \leq \infty$, *že* S *konverguje pro všechna* z *z kruhu* $\{z : |z| < R\} \cup \{0\}$ *a diverguje pro všechna* $\{z : |z| > R\}$. *Číslo* R *se nazývá poloměrem konvergence a je dáno formulí*

$$\frac{1}{R} = \limsup_{n \to \infty} |a_n|^{1/n}.$$

Věta 34 *Nechť* $0 < R < \infty$ *je poloměr konvergence mocninné řady* $\sum_{n \geq 0} a_n z^n$. *Součet této řady* $F(z)$ *je komplexní funkce, která je holomorfní v kruhu* $\{z : |z| < R\}$ *a má na hraniční kružnici* $\{z : |z| = R\}$ *singularitu.*

Co znamená přesně "holomorfní" a "singularita" se lze dozvědět v kurzu komplexní analýzy. Zjednodušeně můžeme říci, že "holomorfní" je totéž co diferencovatelná a "singularita" totéž co nula ve jmenovateli nebo pod odmocninou. Z obou vět plyne následující závěr.

klademe $P(n)$ rovno počtu vyjádření $n = p + q$. Jako n' si označíme ta n, že $P(n) > 0$. Pak, podle Schwarzovy nerovnosti,

$$\sum_{n' \leq x} 1 \geq \frac{\left(\sum_{n \leq x} P(n)\right)^2}{\sum_{n \leq x} P(n)^2}.$$

Čitatel je $\geq (\pi^2(x/2))^2 \geq c_0 x^4 / \log^4 x$ pro jistou absolutní konstantu c_0. Podle Důsledku 15 platí

$$P(n) \leq c_1 \prod_{p|n} \left(1 + \frac{1}{p}\right) \frac{n}{\log^2 n}$$

pro nějakou absolutní konstantu c_1. Proto můžeme **jmenovatele** odhadnout shora pomocí

$$c_1 \frac{x^2}{\log^4 x} \sum_{n \leq x} \prod_{p|n} \left(1 + \frac{1}{p}\right)^2.$$

Suma v tomto výrazu je nejvýše rovna (symbol (d_1, d_2) označuje NSD čísel d_1 a d_2)

$$\begin{aligned}
\sum_{n \leq x} \Big(\sum_{d|n} \frac{1}{d}\Big)^2 &= \sum_{d_1 d_2 \leq x} \frac{1}{d_1 d_2} \sum_{\substack{\frac{d_1 d_2}{(d_1, d_2)} | n \\ n \leq x}} 1 \\
&\leq x \sum_{\substack{d_1 d_2 \leq x \\ k = (d_1, d_2)}} \frac{k}{(d_1 d_2)^2} + \sum_{d_1 d_2 \leq x} \frac{1}{d_1 d_2} \\
&\leq x \sum_{k \leq x} \frac{1}{k^3} \sum_{\substack{l_1 l_2 \leq x \\ (l_1, l_2) = 1}} \frac{1}{l_1^2 l_2^2} + \sum_{n \leq x} \frac{\tau(n)}{n} \\
&\leq x \left(\sum_{k \leq x} \frac{1}{k^3}\right) \left(\sum_{l \leq x} \frac{1}{l^2}\right)^2 + c_3 \log^2 x \\
&\leq c_4 x.
\end{aligned}$$

Čili **jmenovatel** je shora odhadnut výrazem $c_1 c_4 x^3 / \log^4 x$ a celkově máme

$$\sum_{n' \leq x} 1 \geq \alpha x$$

pro nějakou absolutní konstantu $\alpha > 0$. □

Důkaz Věty 19 je hotov. Každé přirozené číslo n lze napsat jako součet omezeně mnoha jedniček a prvočísel. Jedniček se snadno zbavíme rozkladem $n = 2 + (n - 2) = 2 + \cdots$ a nahrazením dvou a více jedniček dvojkami a trojkami.

Lemma 20 byla zesílena na

Věta 24 (Mann, 1942) *Nechť $\mathcal{A}, \mathcal{B} \subset \mathbf{N}_0$ a $0 \in \mathcal{A} \cap \mathcal{B}$. Potom*

$$\sigma(\mathcal{A}+\mathcal{B}) \geq \min(1, \sigma(\mathcal{A})+\sigma(\mathcal{B})).$$

Množina $\mathcal{B} \subset \mathbf{N}_0$ se nazývá *podstatnou komponentou*, pokud pro každou $\mathcal{A} \subset \mathbf{N}_0$, $0 < \sigma(\mathcal{A}) < 1$ platí $\sigma(\mathcal{A}+\mathcal{B}) > \sigma(\mathcal{A})$. Z hořejších nerovností plyne, že každá množina s kladnou Š. hustotou je podstatnou komponentou. V roce 1933 Chinčin dokázal, že množina všech čtverců je podstatnou komponentou. Tento výsledek překrásně zobecnil Erdös.

Věta 25 (Erdös, 1936) *Je-li $0 \in \mathcal{B} \subset \mathbf{N}_0$ báze řádu h a $\mathcal{A} \subset \mathbf{N}_0$ je libovolná, pak*

$$\sigma(\mathcal{A}+\mathcal{B}) \geq \sigma(\mathcal{A}) + \frac{1}{2h}(1-\sigma(\mathcal{A}))\sigma(\mathcal{A}).$$

Landau si však povšiml, že se důkaz téměř nezmění, zaměníme-li h veličinou h^* definovanou pomocí

$$h^* = \sup_n \frac{1}{n} \sum_{m=1}^{n} h(m),$$

kde $h(m)$ je nejmenší počet prvků $\mathcal{B}$, které nasčítají m. Např. pro množinu všech čtverců je $h = 4$, ale $h^* = 19/6$. V tomto tvaru si Erdösovu větu dokážeme.

Věta 26 (Erdös a Landau, 1937) *Za předpokladů předchozí věty platí*

$$\sigma(\mathcal{A}+\mathcal{B}) \geq \sigma(\mathcal{A}) + \frac{1}{2h^*}(1-\sigma(\mathcal{A}))\sigma(\mathcal{A}).$$

Důkaz. Definujeme si $\mathcal{C} = \mathcal{A}+\mathcal{B}$. Dále pro $1 \leq m \leq n$ klademe $\overline{D}_n(m)$ rovno počtu těch $a \in \mathcal{A}$, že $a+m \leq n$, ale $a+m \notin \mathcal{A}$. Pomocí $A(n)$ si označíme $\mathcal{A} \cap \{1, 2, \ldots, n\}$, obdobně $C(n)$. Zjevně platí, pro každé $b \in \mathcal{B}$,

$$\overline{D}_n(b) \leq C(n) - A(n).$$

Snadno se rovněž nahlédne platnost (trojúhelníkové) nerovnosti

$$\overline{D}_n(m+m') \leq \overline{D}_n(m) + \overline{D}_n(m').$$

Rozepsáním m jako součtu $h(m)$ sčítanců z $\mathcal{B}$ dostaneme pomocí těchto nerovností, že

$$\overline{D}_n(m) \leq h(m)(C(n)-A(n)) \quad (1 \leq m \leq n).$$

Sumací přes m vyplyne

$$\overline{D}_n^* := \frac{1}{n} \sum_{m=1}^{n} \overline{D}_n(m) \leq h^*(C(n)-A(n)).$$

$$\begin{aligned} &= \frac{x}{C} \sum_{m \geq 1} \left(\frac{xC^2}{x^2} \cdot \frac{x}{x-C^2} \right)^m \\ &= \frac{x}{C} \sum_{m \geq 1} \left(\frac{C^2}{x-C^2} \right)^m \\ &= \frac{xC(x)}{x-2C(x)^2}. \end{aligned}$$

Povšimněme si, že jsme pro $F(x)$ dostali dvě zdánlivě odlišné formule. Ovšem po dalších úpravách a dosazení výrazu pro $C(x)$, který jsme odvodili v 9.2, dostaneme z jakéhokoliv z obou vyjádření $F(x)$ pomocí $C(x)$ následující výsledek.

$$\boxed{F(x) = \frac{x(1+3\sqrt{1-4x})}{4(1-9x/2)}.}$$

V následující kapitole odvodíme z tohoto explicitního vzorce informaci o asymptotickém chování čísel $r(n)$.

12 Asymptotika

Jednou z nejznámějších asymptotických formulí je Stirlingova formule

$$1 \cdot 2 \cdots n = n! \sim \sqrt{2\pi n} \left(\frac{n}{e} \right)^n.$$

Nebo ještě přesněji,

$$\log(n!(2\pi n)^{-1/2} n^{-n} e^n) \sim \frac{1}{12n} - \frac{1}{360n^3} + \cdots$$

Setkali jsme se s ní už v první části textu, kde jsme odvodili její mírně slabší podobu s neznámou multiplikativní konstantou. S pomocí Stirlingovy formule snadno odhadneme rychlost růstu Catalanových čísel z příkladu 9.2:

$$\binom{2n}{n} \sim \frac{\sqrt{4\pi n}(2n/e)^{2n}}{(\sqrt{2\pi n}(n/e)^n)^2} = \frac{2^{2n}}{\sqrt{\pi n}} \text{ a tedy } c_{n+1} = \frac{1}{n+1}\binom{2n}{n} \sim \frac{4^n}{n\sqrt{\pi n}}.$$

Případy, kdy GF posloupnosti poskytne pro obecný člen explicitní vzorec však nejsou příliš časté. Většinou se musíme spokojit s explicitním vzorcem pouze pro GF samu a

Předvedeme dva postupy pro určení $F(x)$.

První postup je založen na rekurenci pro $r(T)$. Pěstovaný strom T je jednoznačně určen svými podstromy zakořeněnými v synech kořene. Buďte to, zleva doprava, $T_1, T_2, \dots, T_k$. Lehce se nahlédne, že

$$r(T) = 1 + 2\sum_{i=1}^{k} r(T_i).$$

Zavedeme-li si GF

$$G(x,y) = \sum_{T\in\mathcal{T}} x^{r(T)} y^{|V(T)|}$$

($\mathcal{T}$ označuje všechny pěstované stromy), vyjádří se rekurence pro $r(T)$ jako

$$G(x,y) = xy\sum_{k\geq 0} G(x^2,y)^k = \frac{xy}{1-G(x^2,y)}.$$

Nás ovšem zajímá OGF

$$F(y) = \left.\frac{\partial G}{\partial x}\right|_{x=1}.$$

Je zřejmé, že $G(1,y) = C(y)$, kde $C(y)$ je OGF pro Catalanova čísla určená v 9.2. Zderivujeme rovnici pro $G(x,y)$ parciálně podle x a položíme $x = 1$. Dostaneme

$$F(y) = y\,\frac{1-C(y)+2F(y)}{(1-C(y))^2}.$$

Tedy

$$F(y) = y\,\frac{1-C(y)}{(1-C(y))^2-2y}.$$

Druhý postup využívá myšlenku, kterou jsme předvedli v 9.4. Patrně

$$r(n) = \sum_{m=1}^{n} k(m),$$

kde $k(m)$ je počet způsobů, jak pěstovaný strom P tvaru cesty o m vrcholech rozšířit na pěstovaný strom s n vrcholy. P rozšiřujeme přivěšením stromu nad horní vrchol P a přivěšením ke každému z ostatních vrcholů P jednoho stromu vpravo a jednoho stromu vlevo. Dále podrozdělíme některé hrany P několika vrcholy (to provedeme i s hranou přidanou pod kořen P) a opět napravo a nalevo od nových vrcholů přivěsíme stromy. Tedy, podobně jako v 9.4,

$$F(x) \;=\; \sum_{m\geq 1} x^m \left(\frac{C(x)}{x}\right)^{2m-1} \left(\frac{x}{x-C(x)^2}\right)^m$$

Definujeme si analogicky $D_n(m)$ jako počet těch $a \in \mathcal{A}$, že $a + m \leq n$, a $a + m \in \mathcal{A}$. Jistě $\overline{D}_n(m) + D_n(m) = A(n-m) \geq (n-m)\sigma(\mathcal{A})$. Sumací přes m dostáváme

$$n\overline{D}_n^* \geq \frac{(n-1)n}{2}\sigma(\mathcal{A}) - \sum_{m=1}^{n} D_n(m) = \frac{(n-1)n}{2}\sigma(\mathcal{A}) - \frac{1}{2}(A(n)-1)A(n).$$

Tedy

$$\overline{D}_n^* \geq \frac{1}{2}(n-1)\sigma(\mathcal{A}) - \frac{1}{2}(A(n)-1)\frac{A(n)}{n} \geq \frac{n}{2}(\sigma(\mathcal{A}) - (A(n)/n)^2).$$

Zkombinujeme tento dolní odhad $\overline{D}_n^*$ s hořejším horním odhadem a vyjádříme si $C(n)/n$:

$$\frac{C(n)}{n} \geq \frac{A(n)}{n} - \frac{1}{2h^*}\left(\frac{A(n)}{n}\right)^2 + \frac{1}{2h^*}\sigma(\mathcal{A}).$$

Zbývá nahradit $A(n)/n$ veličinou $\sigma(\mathcal{A})$. To je přípustné, protože $\sigma(\mathcal{A}) \leq A(n)/n$ a funkce $x - x^2/(2h^*)$ je v intervalu $[0,1]$ rostoucí. □

Každá báze tedy je podstatnou komponentou.

Existuje podstatná komponenta, která není bazí? V r. 1942 Linnik dokázal existenci podstatné komponenty $\mathcal{B} \subset \mathbf{N}_0$, pro niž platí

$$B(x) \leq \exp((\log x)^{9/10+\varepsilon}).$$

Taková množina samozřejmě nemůže být bazí žádného řádu (proč?). Definitivní odpověď na otázku, jak útlá může být podstatná komponenta, nalezl Ruzsa.

Věta 27 (Ruzsa, 1987) *Pro každé $\varepsilon > 0$ existuje podstatná komponenta $\mathcal{B}$ s $B(x) = O((\log x)^{1+\varepsilon})$. Naopak, pro každou podstatnou komponentu $\mathcal{B}$ existuje $c > 0$, že $B(x) > (\log x)^{1+c}$ pro všechna dostatečně velká x.*

5 Dva klasické výsledky o čtvercích

Nyní si dokážeme klasický Lagrangeův výsledek o tom, že každé přirozené číslo je součtem čtyř čtverců.

Věta 28 (Lagrange, 1770) $\mathcal{L} = \{n^2 :\ n \in \mathbf{N}\}$ *je bazí řádu čtyři.*

Důkaz. **Lemma** Pro každé prvočíslo $p > 2$ existují nezáporná celá čísla x, y, m, $0 < m < p$, že $1 + x^2 + y^2 = mp$.

Důkaz je jednoduchý. Čísla $\{x^2 : \ 0 \le x \le (p-1)/2\}$ stejně jako čísla $\{-1 - y^2 : 0 \le y \le (p-1)/2\}$ jsou vzájemně nekongruentní mod p. Dohromady ale jich je $p+1$, takže $x^2 \equiv -1 - y^2 \pmod p$ pro nějaká x a y. Dokonce $1 + x^2 + y^2 = mp$, $0 < m < p$.

Eulerova identita. $x_i, y_i, i = 1 \dots 4$ buďte proměnné. Pak

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2, \text{ kde}$$

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4,$$

$$z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3,$$

$$z_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4,$$

$$z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2.$$

Identita ukazuje, že stačí vyjádřit ve tvaru součtu čtyř čtverců všechna prvočísla. V dalším se omezíme na lichá prvočísla $p > 2$, protože $2 = 1^2 + 1^2 + 0^2 + 0^2$. Podle hořejšího lemmatu máme $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ pro $0 < m < p$, $x_i \in \mathbf{N}_0$. Nechť m_0 je nejmenší m, pro které to platí. Ukážeme, že $m_0 = 1$. Buď $m_0 > 1$.

Ukážeme, že m_0 nemůže být sudé. Kdyby ano, tak lze čísla x_i rozdělit do dvou dvojic, řekněme x_1, x_2 a x_3, x_4, že členy v jedné dvojici mají shodnou paritu. Pak ale

$$\frac{m_0p}{2} = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

a to je spor s minimalitou m_0. Tedy $m_0 > 2$ je liché.

Proto můžeme x_i vyjádřit jako $x_i = m_0b_i + y_i$, kde $b_i \in \mathbf{N}_0$, $y_i \in \mathbf{Z}$ a $|y_i| < m_0/2$. Ne všechna x_i jsou dělitelná m_0 a proto $y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0$. Tedy $0 < \sum y_i^2 < m_0^2$. Zřejmě m_0 dělí $\sum y_i^2$. Máme situaci

$$\sum x_i^2 = m_0p \ \text{ a } \ \sum y_i^2 = m_1m_0,$$

kde $0 < m_1 < m_0 < p$. Podle Eulerovy identity

$$m_0^2m_1p = \sum z_i^2$$

pro nějaká nezáporná celá čísla z_i. Z vyjádření z_1 v Eulerově identitě však vidíme, že $z_1 = \sum x_iy_i \equiv \sum x_i^2 \equiv 0 \pmod{m_0}$. Obdobně pro ostatní z_i. Tedy $z_i = m_0t_i$ a dostáváme kýžený spor

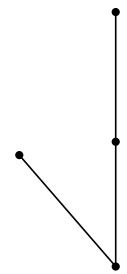
$$m_1p = \sum t_i^2.$$

Na začátku tedy muselo být $m_0 = 1$. □

Položením $r = 1$ dostáváme jiné odvození zarámečkované formule. Zkusme ještě položit $r = 2$, vyjde druhý moment doby, než se A objeví:

$$\begin{aligned}\sum_{n\ge1} n^2 g_A(n)2^{-n} &= 2^{2k+1}C_A(1/2)^2 - (2k-1)2^kC_A(1/2) + 2^kC_A'(1/2)\\ &= 2^{2k}C_A(1/2)^2 + O(k2^k).\end{aligned}$$

11.2 Průměrný počet řetězců v pěstovaném stromu. Pro definici a příklady pěstovaných stromů odkazujeme do 9.2. Každý takový strom můžeme přirozeně pojímat jako částečně uspořádanou množinu: vrchol u je níže než vrchol v v T, pokud u leží na cestě spojující kořen T s vrcholem v. *Řetězcem* rozumíme neprázdnou lineárně uspořádanou podmnožinu. Např. strom



obsahuje 9 řetězců. Označme si jako $r(T)$ počet řetězců ve stromu T. Je snadné určit extrémní hodnoty této funkce, pokud T probíhá množinu pěstovaných stromů s n vrcholy. Maximální hodnotu nabývá, když T je cesta, pak je rovna $2^n - 1$, a minimální je pro koště, pak se rovná $2n - 1$. Jaká ale je průměrná hodnota $r(T)$? Zajímá nás podíl

$$\overline{r}(n) = \frac{r(n)}{|\mathcal{T}(n)|},$$

kde $\mathcal{T}(n)$ označuje množinu pěstovaných stromů s n vrcholy a

$$r(n) = \sum_{T\in\mathcal{T}(n)} r(T).$$

V 9.2 jsme zjistili, že jmenovatel se rovná Catalanovu číslu. Hodnoty $r(n)$ budeme zkoumat pomocí OGF

$$F(x) = \sum_{n\ge1} r(n)x^n.$$

Např. $C_{A_0}(z) = 1 + z^5 + z^7$. K odvození formule pro $F_A(z)$ se nám bude hodit veličina

$$g_A(n) = \#\{v \in \{0,1\}^n : \quad A \text{ je na začátku } v\text{, ale nikde jinde}\}$$

a její OGF

$$G_A(z) = \sum_{n\geq 0} g_A(n) z^n.$$

Nalezneme dva vztahy svazující obě OGF. Pokud $b \in \{0,1\}^n$ neobsahuje A jako podslovo, dostáváme uvážením slov tvaru $0b$ a $1b$ rovnici $2f_A(n) = f_A(n+1) + g_A(n+1)$. V řeči OGF

$$2F_A(z) = \frac{F_A(z) - 1}{z} + \frac{G_A(z)}{z}.$$

Slova tvaru Ab vedou na rovnici $f_A(n) = \sum g_A(n+j)$, kde sčítáme přes j od 1 do k, pro něž $c_A(k-j) = 1$. Tedy

$$F_A(z) = z^{-k} C_A(z) G_A(z).$$

Vyřešením soustavy získáváme

$$F_A(z) = \frac{C_A(z)}{z^k + (1-2z)C_A(z)} \quad \text{a} \quad G_A(z) = \frac{z^k}{z^k + (1-2z)C_A(z)}.$$

Jednoduchou pravděpodobnostní úvahou (přenechanou čtenáři) plyne, že střední doba čekání na objevení se A je rovna součtu pravděpodobností, že se A neobjeví v prvních $n = 1, 2, \ldots$ hodech. Proto

$$\boxed{\text{Střední doba čekání na } A \text{ je } \sum_{n\geq 1} f_A(n)(1/2)^n = F_A(1/2) = 2^k C_A(1/2).}$$

Pro naše konkrétní A_0 to je

$$2^8 (1 + \left(\frac{1}{2}\right)^5 + \left(\frac{1}{2}\right)^7) = 2^8 \left(1 + \frac{5}{128}\right).$$

Hodnota r-tého momentu doby, kdy se A prvně objeví, je rovna

$$\sum_{n\geq 1} n^r g_A(n) 2^{-n} = \left(z \frac{d}{dz}\right)^r G_A(z)\bigg|_{z=1/2}.$$

Z toho, že množina čtverců je bazí plyne, že i množina čtvrtých mocnin je bazí. Ukážeme, že

$$n = x_1^4 + x_2^4 + \cdots + x_{53}^4$$

má pro každé $n \in \mathbf{N}_0$ celočíselné řešení. Snadno se ověří platnost identity

$$6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2 = \sum_{1\leq i<j\leq 4} (x_i + x_j)^4 + (x_i - x_j)^4.$$

Nyní si dané n vyjádříme jako $n = 6k + j$, $0 \leq j \leq 5$. Podle Lagrangeovy věty tedy můžeme psát $n = 6(a^2 + b^2 + c^2 + d^2) + j$ pro vhodná a, b, c, d. Číslo j je součtem nejvýše pěti čtvrtých mocnin. Použijeme znovu Lagrangeovu větu pro každé z čísel a, b, c, d a pomocí identity vyjádříme n jako součet nejvýše $4 \cdot 12 + 5 = 53$ čtvrtých mocnin.

Následující tvrzení, kterým zakončíme první část přednášky, je klasickým výsledkem. Poprvé jej dokázal Fermat, existuje mnoho jednoduchých i méně jednoduchých číselně-teoretických důkazů. My si předvedeme geometrický a kombinatorický důkaz. Oba tyto důkazy nepatří k těm nejjednodušším, demonstrují ale názorně techniky (Minkowského větu a princip involuce), které mají řadu dalších použití.

Věta 29 (Fermat, 17. st.) *Každé prvočíslo p tvaru $4n + 1$ lze psát jako součet dvou čtverců (dokonce jednoznačně, ale to nedokážeme).*

V geometrickém důkazu budeme pracovat v $\mathbf{R}^d$, $z_1, z_2, \ldots, z_d$ buďte lineárně nezávislé vektory. *Mřížka* generovaná těmito vektory je množina

$$\Lambda(z_1, \ldots, z_d) = \{\sum a_i z_i : \; a_i \in \mathbf{Z}\}.$$

Symbol Vol bude označovat d-rozměrnou Lebesgueovu míru, tj. objem těles. $Vol(\Lambda)$ je objem základního rovnoběžnostěnu mřížky. Mřížky s $Vol(\Lambda) = 1$ se nazývají jednotkové.

Věta 30 (Minkowski) *Nechť $C \subset \mathbf{R}^d$ je konvexní množina, která je měřitelná a středově souměrná podle počátku. Nechť Λ je jednotková mřížka a nechť $Vol(C) > 2^d$. Pak $\Lambda \cap C$ obsahuje kromě počátku ještě další bod mřížky.*

Důkaz. Ukážeme si dva důkazy.

1 Množina $\{\frac{1}{2}C + v : \; v \in \Lambda\}$ se nemůže skládat ze vzájemně disjunktních kopií tělesa $\frac{1}{2}C$. Předpokládejme pro spor, že se skládá. T buď nějaký základní rovnoběžník mřížky, potom

$$Vol(\tfrac{1}{2}C) = \sum_{z\in\Lambda} Vol(\tfrac{1}{2}C \cap (T - z)) = \sum_{z\in\Lambda} Vol((\tfrac{1}{2}C + z) \cap T) \leq 1$$

a to je spor. Proto $\frac{1}{2}x' + v_1 = \frac{1}{2}x'' + v_2$, kde $x', x'' \in C$, a $v_1 \neq v_2$ jsou dva prvky mřížky. Tedy $0 \neq v_2 - v_1 = (x' - x'')/2 \in C$ a jsme hotovi.

2 Tento důkaz pochází od Mordella. Nechť $\Lambda = \mathbf{Z}^d$, úvaha se snadno modifikuje pro libovolnou jednotkovou mřížku. Jako R_m označíme počet racionálních mřížových bodů

$$\{(a_1/m, a_2/m, \ldots, a_d/m) : \ a_i \in \mathbf{Z}\},$$

které padnou do C. Pro m jdoucí do nekonečna máme zřejmě

$$R_m \to Vol(C)m^d$$

a proto pro velké m platí $R_m > (2m)^d$. Existují proto dva různé vektory

$$x = (a_1/m, \ldots, a_d/m), y = (b_1/m, \ldots, b_d/m) \in R_m \cap C, a_i, b_i \in \mathbf{Z},$$

že $a_i \equiv b_i \pmod{2m}$. Nenulový celočíselný mřížový bod $\frac{1}{2}(x-y)$ padne do C. $\square$

Než přikročíme k důkazu Věty 29 poznamenejme, že pro obecnou nejednotkovou mřížku se podmínka $Vol(C) > 2^d$ nahradí podmínkou $Vol(C) > 2^d Vol(\Lambda)$.

První důkaz Věty 29. Nejprve si ukážeme, že pro $p = 4n+1$ má kongruence

$$x^2 \equiv -1 \pmod p$$

vždy řešení. Hned se vidí ($(\mathbf{Z}_p, \cdot)$ je grupa), že $p-3$ čísel $2, 3, \ldots, p-2$ lze spárovat do $(p-3)/2$ dvojic $(i,j), i \neq j$, pro něž $ij \equiv 1 \pmod p$. Proto

$$(p-1)! \equiv -1 \pmod p.$$

Obdobné párování můžeme udělat pro čísla $1, 2 \ldots, p-1$ s podmínkou $ij \equiv -1 \pmod p$. Nyní ale nemůže vždy platit $i \neq j$, protože to bychom dostali

$$(p-1)! \equiv (-1)^{(p-1)/2} \equiv 1 \pmod p.$$

Vskutku někdy $i^2 \equiv -1$.

Minkowského větu použijeme pro mřížku $\Lambda = \{(i, qi+pj) : \ i,j \in \mathbf{Z}\}$, kde q je řešení $x^2 \equiv -1 \pmod p$, a pro těleso C rovno kruhu o poloměru $r = \sqrt{2p}$. Patrně $Vol(\Lambda) = p$, předpoklady jsou splněny. Věta nám garantuje existenci mřížového bodu $(0,0) \neq (a,b) \in \Lambda$, že $a^2+b^2 < 2p$. Snadno se spočte, že $a^2+b^2 \equiv 0 \pmod p$ a proto nutně $a^2+b^2 = p$.

Druhý důkaz Věty 29 pochází od Zagiera. Podle tvrzení autora jde o důkaz jedinou gramatickou větou, přeložme ji tedy do češtiny:

P-rekurzivní posloupnosti zobecňují třídu posloupností definovaných lineárními homogeními diferenčními rovnicemi s konstantními koeficienty. Takovou posloupností je např. posloupnost Fibonacciových čísel nebo posloupnost polyminových čísel z úlohy 10.1. V případě konstantních koeficientů lze vybudovat elegantní obecnou teorii, která podává explicitní vzorec pro n-tý člen příslušné posloupnosti. Lze se s ní setkat např. v kurzu numerické matematiky. Pro polynomiální koeficienty taková teorie není známa.

Zamyslíme-li se nad odvozením rekurence pro Schröderova čísla, vidíme, že klíčovou byla skutečnost, že $F(x)$ je řešením kvadratické rovnice s polynomiálními koeficienty. Obecně vyplývá P-rekurzivita pro rovnici libovolného stupně.

Věta 32 *$F(x) = \sum_{n\geq 0} a_n x^n \in \mathbf{C}[[x]]$ buď algebraická mocninná řada, tj.*

$$P(x, F(x)) = 0$$

pro nějaký polynom $P \in \mathbf{C}[x,y]$. Potom $\{a_n\}_{n\geq 0}$ je P-rekurzivní.

11 Hledání průměrů

11.1 Čekání na podslovo. Jsme vybaveni mincí a binárním slovem

$$A = a_1 a_2 \ldots a_k \in \{0,1\}^k.$$

Nechť pro konkrétnost např. $A_0 = 10101101$. Házením mincí generujeme náhodnou posloupnost nul a jedniček z $\{0,1\}^\omega$. Jaká je střední doba čekání, než se A objeví jako podslovo v této posloupnosti? Podslovem rozumíme souvislý úsek. Pomocí GF nalezneme odpověď.

Definujeme

$$f_A(n) = \#\{v \in \{0,1\}^n : \ A \not\subset v\}$$

a OGF

$$F_A(z) = \sum_{n\geq 0} f_A(n) z^n.$$

Užitečný bude korelační polynom

$$C_A(z) = \sum_{j=0}^{k-1} c_A(j) z^j,$$

kde $c_A(0) = 1$ a pro $1 \leq j \leq k-1$ klademe

$$c_A(j) = \begin{cases} 1 & \text{pokud } a_1 a_2 \ldots a_{k-j} = a_{j+1} a_{j+2} \ldots a_k \\ 0 & \text{jinak.} \end{cases}$$

Tedy
$$F(x) = \frac{x(1-3x-\sqrt{1-6x+x^2})}{4}.$$
A kde je slíbená rekurence? Označme si
$$H(x) = \frac{F(x)}{x} = \frac{1}{4}(1-3x-\sqrt{1-6x-x^2}) = \sum_{n\geq 3} a_n x^{n-1}.$$
Zřejmě
$$\begin{aligned}(x-3)H(x) &= \frac{1}{4}(-3+10x-3x^2-(x-3)\sqrt{\ldots}) \text{ a}\\ (1-6x+x^2)H(x)' &= \frac{1}{4}(-3+18x-3x^2-(x-3)\sqrt{\ldots}).\end{aligned}$$
Vidíme, že $H(x)$ splňuje diferenciální rovnici
$$(1-6x+x^2)H' - (x-3)H = 2x.$$
Porovnání koeficientů u x^n vede pro $n>1$ k rovnici
$$(n+1)a_{n+2} - (6n-3)a_{n+1} + (n-2)a_n = 0.$$
Pro $n>1$ máme
$$\boxed{a_{n+2} = \frac{(6n-3)a_{n+1} - (n-2)a_n}{n+1}.}$$
Tato relace určuje posloupnost tzv. *Schröderových čísel*
$$\{a_n\}_{n\geq 3} = \{1, 3, 11, 45, 197, 913, \ldots\}.$$

10.3 P-rekurzivita. Posloupnost Schröderových čísel je příkladem P-rekurzivní posloupnosti. Posloupnost $\{a_n\}_{n\geq 0} \subset \mathbf{C}$ se nazývá *P-rekurzivní* (zkratka od *polynomiálně rekurzivní*), existují-li polynomy $P_0(x), P_1(x), \ldots, P_m(x) \in \mathbf{C}[x]$, že pro každé $n \in \mathbf{N_0}$ platí
$$P_0(n)a_n + P_1(n)a_{n+1} + \cdots + P_m(n)a_{n+m} = 0.$$
P-rekurzivní posloupnosti s $m=1$ se nazývají *hypergeometrické*. S hypergeometrickou posloupností jsme se již setkali, je jí posloupnost Catalanových čísel (proč?).

“ Involuce na konečné množině $S = \{(x,y,z) \in \mathbf{N}^3 :\ x^2+4yz = p\}$ definovaná jako
$$(x,y,z) \to \begin{cases} (x+2z, z, y-x-z) & \text{pokud } x < y-z\\ (2y-x, y, x-y+z) & \text{pokud } y-z < x < 2y\\ (x-2y, x-y+z, y) & \text{pokud } x > 2y\end{cases}$$
má právě jeden pevný bod, proto má S lichý počet prvků a jiná involuce definovaná předpisem $(x,y,z) \to (x,z,y)$ má rovněž pevný bod.”

Involuce na konečné množině je permutace π této množiny taková, že $\pi \circ \pi = \pi$. Graf involuce se skládá z pevných bodů a dvojcyklů. Že první involuce je definována korektně, že to je opravdu involuce a že má právě jeden pevný bod ponecháváme k ověření jako cvičení. Pevný bod druhé involuce, který musí v důsledku lichosti $|S|$ existovat, poskytuje hledanou reprezentaci p jako součtu dvou čtverců.

6 Příklady k první části

Nejprve značení. p je prvočíslo, p_n je n-té prvočíslo, $\pi(x)$ je počet prvočísel nepřesahujících x. $\mu(n)$ je Möbiova funkce, která je 1 pro $n=1$, 0 pro n dělitelné čtvercem větším než 1 a $(-1)^k$ pro n rovno součinu k různých prvočísel. $\varphi(n)$ je Eulerova funkce — počet čísel $1 \leq m \leq n$ nesoudělných s n.

1. Ukažte, že z prvočíselné věty plyne, pro $n \to \infty$,
$$\frac{p_n}{n \log n} \to 1.$$

2. Ukažte, že odhad
$$\pi(x) = \frac{x}{\log x} + O(x/\log^3 x)$$
neplatí.

Návod: přiveďte ke sporu s Mertensovou větou.

3. Nechť, pro $n \geq 1$,
$$P(n) = \prod_{p\geq \log n,\ p|n} (1 - \frac{1}{p}).$$
Pak $\lim_{n\to\infty} P(n) = 1$.

4. $\mathcal{A} \subset \mathbf{N}$ se nazývá Sidonova, pokud $n = a_1 + a_2$, $a_1 \leq a_2$, $a_i \in \mathcal{A}$, má pro každé n nejvýše jedno řešení. Dokažte, že v $\{1, 2, \ldots, n\}$ existuje Sidonova podmnožina velikosti alespoň $\lfloor n^{1/3} \rfloor$.

Návod: postupujte hladově.

5. Dokažte identity:

$$(a)\ \sum_{d|n}\varphi(d)=n,\ (b)\ \varphi(n)=\sum_{d|n}\frac{n}{d}\,\mu(d),\ (c)\ \sum_{d|n}\mu(d)=0 \text{ (pro } n>1).$$

6. Nalezněte asymptotiku pro $\sum_{m=1}^{n}\varphi(m)$.
Návod: použijte (b). Vyjde hlavní člen obsahující $\sum\mu(m)/m^2$. Pak se použije

$$(\sum 1/k^s).(\sum\mu(m)/m^s)=1,$$

což plyne z (c). Dále se užije $\sum 1/m^2=\pi^2/6$.

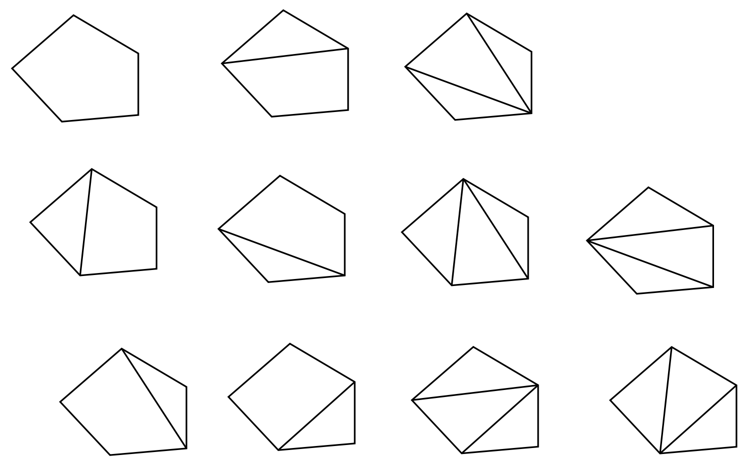
7. Nalezněte asymptotiku pro $\sum_{m=1}^{n}\varphi(m)/m$.

7 Literatura k první části

Z knihy [6] je převzat úsek od Lemmatu 1 k Větě 4. Obecnou Eulerovu sumační formuli jsme převzali z encyklopedie [4], z 22. kapitoly Asymptotic Enumeration Methods napsané A.M. Odlyzkem. O roli Bernoulliových čísel ve Fermatově hypotéze se lze poučit v [1] nebo v [7], v [7] jim je věnována celá kapitola. Důkazy Čebyševovy věty a Mertensovy věty, tj. úsek od Lemmatu 7 po Větu 9, jsme převzali z [6]. V této knize je uveden relativně jednoduchý důkaz Prvočíselné věty pomocí metod teorie funkcí komplexní proměnné. Přehledový článek o elementárních důkazech Prvočíselné věty je [8]. Ve skriptech [9] lze nalézt kompletní elementární důkaz. Celý třetí oddíl a první část čtvrtého oddílu (Věta 11 až Věta 22) jsou zpracovány podle 20. kapitoly encyklopedie [4] Combinatorial Number Theory napsané C. Pommerancem a A. Sárközym. Důkaz Věty 23 je převzat z [3]. Tam lze nalézt i důkaz Věty 24 (viz též [9]). Důkaz Věty 26 je převzat z [5]. Větu 28 dokazujeme podle [2]. Důkaz faktu, že $\{n^4:\ n\in\mathbf{N}\}$ je bazí referoval na přednášce student P. Kraemer a pochází od francouzského matematika I. Liouvillea. Geometrický důkaz Věty 29 je převzat z výběrové přednášky J. Matouška Kombinatorická geometrie. Oba důkazy Minkowského věty jsou zpracovány podle [10]. Kombinatorický důkaz Věty 29 byl publikován v [11].

1. Z. I. Borevič a I. R. Šafarevič, *Těorija čisel*, Nauka, Moskva, 1985.

2. K. Chandrasekharan, *Introduction to analytic number theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1968.



Chceme odvodit rekurentní vztah pro počet a_n všech možných rozřezání P. To se nám zdaří s pomocí jiné veličiny b_n, která je definována jako počet těch rozřezání P, v nichž z vrcholu 1 nevede žádná uhlopříčka. Zavedeme si OGF

$$F(x)=\sum_{n\geq 0}a_nx^n=x^3+3x^4+11x^5+\cdots\quad\text{a}\quad G(x)=\sum_{n\geq 0}b_nx^n=x^3+2x^4+6x^5+\cdots$$

Uvažme rozřezání P, v němž z 1 vede alespoň jedna uhlopříčka. P se rozříznutím podle nejlevější uhlopříčky vedoucí z 1 rozpadne na dvě rozřezání dvou mnohoúhelníků, které mají dohromady $n+2$ vrcholů. Jejich vrcholy očíslujeme tak, že oba vrcholy vzniklé z 1 budou opět označeny 1. V prvním rozřezání z 1 nevychází žádná uhlopříčka a druhé je obecné. Naopak, z každé takové dvojice rozřezání se jednoznačně složí rozřezání P. Proto

$$F(x)=G(x)+\frac{F(x)G(x)}{x^2}.$$

Nyní uvažme rozřezání P, v nichž z 1 nevede žádná uhlopříčka. Rozpadají se na dvě třídy podle toho, zda 2 a n jsou či nejsou spojeny uhlopříčkou. Každá z obou tříd je však v jednoznačné korespondenci s rozřezáními $n-1$ úhelníka a obsahuje a_{n-1} prvků. Tato úvaha ale funguje až pro $n>3$. Proto

$$G(x)=2xF(x)+x^3.$$

Eliminací $G(x)$ z obou rovnic získáváme

$$2F(x)^2+(3x^2-x)F(x)+x^4=0.$$

Při úpravách jsme užili vztah pro součet geometrické řady, který je speciálním případem formule

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

(která je sama speciálním případem binomické věty) a z té jsme v poslední úpravě použili instanci $k = 2$. Odvodili jsme vztah

$$A(x,y) = \frac{xy}{1-xy} + \frac{x^2y^2}{(1-xy)^2}A(1,y) + \frac{xy}{1-xy}G(y),$$

kde

$$G(y) = \frac{\partial}{\partial x}A(x,y)\Big|_{x=1}.$$

Substituce $x = 1$ vede k první rovnici

$$A(1,y) = \frac{y}{1-y} + \frac{y^2}{(1-y)^2}A(1,y) + \frac{y}{1-y}G(y).$$

Parciální derivování podle x a substituce $x = 1$ vede ke druhé rovnici

$$G(y) = \frac{y}{(1-y)^2} + \frac{2y^2}{(1-y)^3}A(1,y) + \frac{y}{(1-y)^2}G(y).$$

Eliminováním $G(y)$ z obou rovnic získáváme

$$A(1,y) = \frac{y(1-y)^3}{1-5y+7y^2-4y^3}.$$

Ovšem

$$A(1,y) = \sum_{n\geq 1} a_n x^n$$

je přesně ta OGF, která nás zajímá. Rovnice $A(1,y)(1-5y+7y^2-4y^3) = y(1-y)^3$ ústí ve hledanou rekurenci ($n \geq 2$)

$$\boxed{a_{n+3} = 5a_{n+2} - 7a_{n+1} + 4a_n.}$$

Tedy $a_4 = 19$, $a_5 = 61$, $a_6 = 196$, ...

10.2 Rozřezání mnohoúhelníku. Uvažujme pevný konvexní n-úhelník P s vrcholy očíslovanými proti směru hodinových ručiček čísly $1, 2, \ldots, n$. Jeho *rozřezáním* budeme rozumět jakoukoli množinu nekřížících se uhlopříček. Např. pro $n = 5$ máme 11 následujících rozřezání (pro jednoduchost pomíjíme označení vrcholů čísly $1 \ldots 5$)

3. A. O. Gelfond a Ju. V. Linnik, *Elementarnye metody v analytičeskoj těorii čisel*, Fizmatgiz, Moskva, 1962.

4. R. L. Graham, M. Grötschel a L. Lovász (editors), *Handbook of Combinatorics*, North-Holland, Amsterdam, 1995.

5. H. Halberstam, K. F. Roth, *Sequences*, Oxford University Press, 1966.

6. E. Hlawka, J. Schoissengaier and R. Taschner, *Geometric and Analytic Number Theory*, Springer, Berlin, 1986.

7. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, Berlin, 1982. Ruský překlad: K. Ajerlend, M. Rouzen, *Klassičeskoe vvedenie v sovremennuju teoriju čisel*, Mir, Moskva, 1987.

8. B. Novák, O elementárním důkazu prvočíselné věty, *Časopis pro pěstování matematiky* **100** (1975), 71–84.

9. B. Novák, *Vybrané partie z teorie čísel*, skriptum MFF UK, SPN Praha, 1972.

10. W. M. Schmidt, *Diophantine Approximations*, Lecture Notes in Mathematics 785, Springer, 1980. Ruský překlad: V. Šmidt, *Diofantovy približenija*, Mir, Moskva, 1983.

11. D. Zagier, A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares, *American Mathematical Monthly* **97** (1990), 144.

Generující funkce

8 Úvod

Generující (nebo též vytvořující) funkce, krátce GF, jsou mocnou a fascinující technikou kombinatorické enumerace. Nalézají však použití i v jiných matematických disciplínách, např. právě v teorii čísel.

Kombinatorická enumerace se zabývá nalezením (pokud možno přesného) počtu kombinatorických struktur závisejících na jednom či více parametrech. Konkrétněji, $\mathcal{M} = \{\mathcal{M}_n\}_{n\geq 0}$ buď posloupnost množin kombinatorických struktur, struktury $M \in \mathcal{M}_n$ mají bázickou množinu $\{1, 2, \ldots, n\}$ a $a_n = |\mathcal{M}_n|$ je jejich počet. *Obyčejná generující funce* (OGF) pro struktury $\mathcal{M}$ je definována předpisem

$$f(x) = \sum_{n\geq 0} a_n x^n.$$

Exponenciální generující funkce (EGF) pro struktury $\mathcal{M}$ je definována předpisem

$$g(x) = \sum_{n\geq 0} \frac{a_n x^n}{n!}.$$

V kombinatorice se jiné typy GF téměř nevyskytují. Samozřejmě, často se uvažují GF více proměnných, např.

$$f(x, y) = \sum_{k\geq 0} \sum_{n\geq 0} a_{k,n} x^k y^n$$

nebo

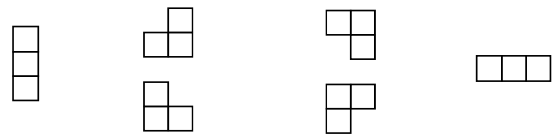
$$g(x, y) = \sum_{k\geq 0} \sum_{n\geq 0} \frac{a_{k,n} x^k y^n}{n!}$$

apod. Parametr k může být určitá “váha” struktury $M \in \mathcal{M}_n$ a $a_{k,n}$ pak je počet struktur na $\{1, 2, \ldots, n\}$ s vahou k. Překvapivě často lze kombinatorické závislosti a rekurence platné pro strukturu $\mathcal{M}$ přeložit do řeči GF jako algebraické, diferenciální či funkcionální rovnice platné pro příslušnou OGF či EGF. Brzy si uvedeme řadu konkrétních příkladů. Nejprve se však v posledním ohlédnutí za první částí přednášky krátce a zběžně zmíníme o použití GF v teorii čísel.

Zde jsou velmi důležité *Dirichletovy řady*. Dirichletova řada přiřazená posloupnosti

$$\{a(n)\}_{n\geq 0} \subset \mathbf{C}$$

Počet různých (tj. neztotožnitelných posunutím) vodorovně konvexní polymin s n čtverečky si označíme jako a_n. Např. $a_0 = 0$, $a_1 = 1$, $a_2 = 2$, $a_3 = 6$. Toto jsou vodorovně konvexní polymina se třemi čtverečky:



Naším cílem je odvodit rekurentní vztah pro snadný výpočet čísel a_n. Zavedeme si jemnější veličinu $a_{r,n}$, $1 \leq r \leq n$, rovnou počtu vodorovně konvexních polymin s n čtverečky, z toho r v nejdolejší řadě. Zřejmě $a_{n,n} = 1$, klademe $a_{r,n} = 0$ jakmile $r \leq 0$, $r > n$ nebo $n \leq 0$. Dále

$$\sum_{r=1}^{n} a_{r,n} = a_n.$$

Vyjdeme ze zřejmé rekurence

$$a_{r,n} = \sum_{i\geq 1} (r + i - 1) a_{i,n-r},$$

která plyne uvážením možných poloh zbytku polymina na nejdolejší řadě. Nesmíme však přehlédnout, že pro $r = n$ neplatí. Pro OGF

$$A(x, y) = \sum_{r\geq 1} \sum_{n\geq 1} a_{r,n} x^r y^n$$

nám dává

$$\begin{aligned}
A(x, y) &= \sum_{n\geq 1} x^n y^n + \sum_{r\geq 1} \sum_{n\geq 1} \sum_{i\geq 1} (r + i - 1) a_{i,n-r} x^r y^n \\
&= \frac{xy}{1 - xy} + \sum_{r\geq 1} \sum_{n\geq 1} \sum_{i\geq 1} ((r - 1) a_{i,n-r} + i a_{i,n-r}) (xy)^r y^{n-r} \\
&= \frac{xy}{1 - xy} + \sum_{r\geq 1} \sum_{n\geq 1} (r - 1) a_{n-r} y^{n-r} (xy)^r + \sum_{r\geq 1} \sum_{n\geq 1} \sum_{i\geq 1} i a_{i,n-r} y^{n-r} (xy)^r \\
&= \frac{xy}{1 - xy} + \sum_{r\geq 1} (r - 1)(xy)^r \sum_{m\geq 0} a_m y^m + \sum_{r\geq 1} (xy)^r \sum_{m\geq 0} \sum_{i\geq 1} i a_{i,m} y^m \\
&= \frac{xy}{1 - xy} + \frac{x^2 y^2}{(1 - xy)^2} A(1, y) + \frac{xy}{1 - xy} \left. \frac{\partial A(x, y)}{\partial x} \right|_{x=1}.
\end{aligned}$$

pomocí vztahu $C(x)^2 - C(x) + x = 0$.

$$\begin{aligned} K(x) &= \frac{x}{x - C^2(x)} \sum_{k\geq 1} x^k \left(\frac{C(x)}{x}\right)^{2k-1} = \frac{x^2}{C\cdot(x-C^2)} \cdot \frac{C^2/x}{1 - C^2/x} \\ &= \frac{x^2 C}{(x - C^2)^2} \\ &= \frac{x^2 C}{(2x - C)^2} = \frac{1}{1-4x} \cdot \frac{x^2 C}{C - x} = \frac{x}{1-4x}\cdot\frac{x}{C} \\ &= \frac{x}{1-4x} \cdot \frac{1+\sqrt{1-4x}}{2} \\ &= \frac{x}{2(1-4x)} + \frac{x}{2\sqrt{1-4x}}. \end{aligned}$$

Užitím binomické formule dostáváme pro koeficient $k(n)$ u x^n

$$\boxed{k(n) = \frac{4^{n-1} + \binom{2n-2}{n-1}}{2}.}$$

10 Nalezení rekurence

GF nyní využijeme neobvyklým způsobem. Pro posloupnost čísel $\{a_n\}_{n\geq 1}$, kde a_n počítá nějaké kombinatorické struktury, nalezneme s pomocí GF rekurentní relace. To na první pohled vypadá podivně, protože veškerou informaci o OGF či EGF dané posloupnosti čerpáme z rekurencí platných pro tuto posloupnost. Jak bychom tedy mohli odvodit rekurentní vztah, který jsme předtím neznali? Uvidíme!

10.1 Vodorovně konvexní polymina. V tomto příkladu budeme pracovat s konečnými množinami uzavřených čtverečků z nekonečné rovinné čtverečkované sítě S. Taková množina P se nazývá *vodorovně konvexní polymino*, pokud

1. P je souvislá.
2. Každý vodorovný řez $R \cap P$, kde R je nekonečná vodorovná řada čtverečků sítě S, je souvislý.
3. Jsou-li $U_1 = R_1 \cap P$ a $U_2 = R_2 \cap P$ dva neprázdné řezy pro dvě sousední řady R_1 a R_2, pak průnik $U_1 \cap U_2$ není pouze jednobodový.

je komplexní funkce

$$f(z) = \sum_{n\geq 1} a(n) n^{-z}.$$

Pro $a(n)$ multiplikativní (tj. $a(mn) = a(m)a(n)$ jakmile m a n jsou nesoudělné) pak máme vyjádření

$$f(z) = \prod_p (1 + a(p)p^{-z} + a(p^2)p^{-2z} + \cdots),$$

které pochází od Eulera. Nejznámější Dirichletovou řadou je *zeta funkce*

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}.$$

Právě na Eulerově identitě

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} = \prod_p \left(1 - \frac{1}{p}\right)^{-z}$$

jsou založeny neelementární důkazy Prvočíselné věty.

Někdy se zkoumaná čísla mohou objevit i v exponentu. Můžeme si definovat

$$f(z) = \sum_{n\geq 0} z^{a_n},$$

kde $0 \leq a_0 < a_1 < a_2 < \cdots$ jsou přirozená čísla. Pak

$$f(z)^2 = \sum_{n\geq 0} P(n) z^n,$$

kde $P(n)$ je počet reprezentací n ve tvaru $n = a_i + a_j$, a každá netriviální informace o $f(z)$ nám okamžitě cosi řekne i o $P(n)$. Uvažme počet $r(n)$ všech vyjádření n ve tvaru součtu čtyř čtverců celých čísel. Za různé pokládáme i reprezentace lišící se jen pořadím sčítanců nebo znaménky. Patrně

$$\left(\sum_{-\infty}^{\infty} x^{n^2}\right)^4 = \sum_{n\geq 0} r(n) x^n.$$

Jacobi odvodil jiné vyjádření pro výraz stojící na levé straně.

Věta 31 (Jacobi)

$$\left(\sum_{-\infty}^{\infty} x^{n^2}\right)^4 = 1 + 8 \sum_{\substack{n\geq 1 \\ 4 \text{ nedělí } n}} \frac{nx^n}{1-x^n}.$$

Vyjádříme-li každého sčítance vpravo pomocí geometrické řady, dostaneme pozoruhodnou Jacobiho identitu.

$r(n)$ je rovno osminásobku součtu dělitelů n nedělitelných čtyřmi.

Každé n má takového dělitele, ihned tedy jako speciální případ dostáváme Lagrangeovu větu tvrdící, že $r(n) > 0$ pro každé $n \in \mathbf{N}$.

Příklad. Každá ze tří podstatně různých reprezentací čísla 28 jako součtu čtyř □

$$28 = 5^2 + 1^2 + 1^2 + 1^2 = 3^2 + 3^2 + 3^2 + 1^2 = 4^2 + 2^2 + 2^2 + 2^2$$

vytváří $4 \cdot 16 = 64$ různých celočíselných reprezentací. Celkem tedy $r(28) = 192$. Z druhé strany, $8 \cdot (1 + 2 + 7 + 14)$ je rovněž 192.

Jiné záhadné číselné identity pracují s funkcí

$$\sigma_k(n) = \sum_{d|n} d^k.$$

Platí následující identita.

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{j=1}^{n-1} \sigma_3(j)\sigma_3(n-j).$$

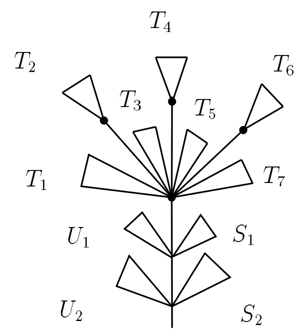
Skutečně např. pro $n = 3$ máme $2188 = 28 + 120 \cdot 18$. Jiná obdobná identita je

$$11\sigma_9(n) = -10\sigma_3(n) + 21\sigma_5(n) + 5040 \sum_{j=1}^{n-1} \sigma_3(j)\sigma_5(n-j).$$

Např. pro $n = 4$ se $11 \cdot 262657 = 2889227$ opravdu rovná $-10 \cdot 73 + 21 \cdot 1057 + 5040 \cdot (244 + 9 \cdot 33 + 28)$. Obě tyto a další identity jsou vedlejšími produkty teorie modulárních forem a jejich důkazy lze s jistým zjednodušení označit za důkazy pomocí GF.

Zpět ke kombinatorice. Wilf ve své knize *Generatingfunctionology* uvádí sedm hlavních oblastí použití GF v kombinatorické enumeraci: (1) nalezení přesné formule, (2) nalezení rekurence, (3) zjištění průměrů a dalších statistických charakteristik, (4) nalezení asymptotiky, (5) důkazy unimodality, (6) důkazy identit a (7) důkazy kongruencí a další aplikace. Pro každou z těchto sedmi oblastí nyní uvedeme konkrétní příklady.

Označme si kořen K jako r a jeho syny zleva doprava jako $r_1, \ldots, r_{k-1}$. T_1 umístíme vlevo od K a jeho kořen ztotožníme s r, T_2 umístíme nad r_1 a jeho kořen ztotožníme s tímto vrcholem, T_3 umístíme mezi hrany rr_1 a rr_2 a jeho kořen ztotožníme s r, atd. až T_{2k-1} umístíme vpravo od K a jeho kořen ztotožníme s r. Z kořene r nakreslíme svislou úsečku kolmo dolů a umístíme na ni (shora dolů) l nových vrcholů $v_1, v_2, \ldots, v_l$. U_i (resp. S_i) umístíme vlevo (resp. vpravo) od v_i a kořeny pěstovaných stromů U_i a S_i ztotožníme s v_i. Vznikne pěstovaný strom T s n vrcholy. Naopak, každé umístění K v nějakém T s n vrcholy je tohoto tvaru. Řečeno obrázkem:



OGF

$$K(x) = \sum_{n \geq 1} k(n)x^n$$

lze proto vyjádřit pomocí funkce $C = C(x)$ odvozené v 9.2 jako

$$K(x) = \frac{x}{x - C(x)^2} \sum_{k \geq 1} x^k \left(\frac{C(x)}{x}\right)^{2k-1}.$$

Člen

$$\frac{x}{x - C(x)^2} = \sum_{l \geq 0} \left(\frac{C(x)^2}{x}\right)^l$$

zachycuje přidávání pěstovaných stromů U_i a S_i a člen

$$\left(\frac{C(x)}{x}\right)^{2k-1}$$

zachycuje přidávání pěstovaných stromů T_i. Nyní už následuje jen přímočarý výpočet, v němž výraz pro $K(x)$ zjednodušujeme pomocí vzorce pro součet geometrické řady a

$$\boxed{n(a,b) = \frac{1}{a-b}\binom{a-1}{b}\binom{a-2}{b-1}.}$$

Její odvození ponecháváme čtenáři jako Příklad 3. Čísla $n(a,b)$ se nazývají *Narayanova čísla* (nebo též *Runyonova čísla*).

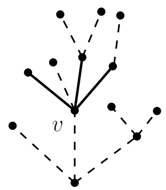
9.4 Počet košťat v pěstovaných stromech. Označme si symbolem $d(T,v)$ stupeň v v T, tj. počet synů vrcholu v v pěstovaném stromu T. Nalezneme explicitní formuli pro výraz

$$k(n) = \sum 2^{d(T,v)},$$

kde sčítáme přes všechny vrcholy všech pěstovaných stromů na n vrcholech. Např. pro 5 stromů na 4 vrcholech dostáváme

$$k(4) = (1+1+1+8)+(1+1+2+4)+(1+1+2+4)+(1+2+2+2)+(1+1+4+2) = 42.$$

Nejprve $k(n)$ interpretujeme kombinatoricky. *Koště* pro nás bude pěstovaný strom, v němž kořen nemá jiné syny než listy. Kolik košťat nalezneme jako podstrom v daném pěstovaném stromu? Košťata v T s centrálním vrcholem shodným s vrcholem $v \in V(T)$ odpovídají jednoznačně podmnožinám množiny synů vrcholu v:



Je jich tedy

$$2^{d(T,v)}.$$

Číslo $k(n)$ je proto celkový počet košťat ve všech pěstovaných stromech na n vrcholech.

Pro nalezení OGF pro čísla $k(n)$ je vhodné zde "počítat druhým způsobem", tj. místo na počet košťat v T se soustředit na počet rozšíření daného koštěte K na pěstovaný strom na n vrcholech. Obecné rozšíření koštěte K s k vrcholy na pěstovaný strom s n vrcholy má následující tvar. Nejprve si zvolíme číslo $l \in \mathbf{N}_0$ a pěstované stromy $U_1, U_2, \ldots, U_l$, $S_1, S_2, \ldots, S_l$ a $T_1, T_2, \ldots, T_{2k-1}$, že

$$\sum_{i=1}^{l} |V(U_i)| + \sum_{i=1}^{l} |V(S_i)| + \sum_{i=1}^{2k-1} |V(T_i)| = n + k + l - 1.$$

9 Explicitní formule

9.1 Fibonacciho čísla. Uvažme posloupnost přirozených čísel $\{F_n\}_{n\geq 0}$ zadanou rekurencí $F_{n+1} = F_n + F_{n-1}$, $F_0 = 0, F_1 = 1$. Tedy

$$\{F_n\}_{n\geq 1} = \{1,1,2,3,5,8,13,21,34,55,89,144,\ldots\}.$$

Jaká je explicitní formule pro F_n? OGF posloupnosti je

$$F = F(x) = \sum_{n\geq 1} F_n x^n.$$

Přeložme rekurenci pro F_n do řeči funkce $F(x)$. Překlad zní

$$\frac{F-x}{x} = F + xF.$$

Teď už je snadné vyjádřit F pomocí x:

$$F(x) = \frac{x}{1-x-x^2}.$$

Označíme-li jako $r_\pm$ čísla $(1\pm\sqrt{5})/2$, dostáváme

$$\begin{aligned} F(x) &= \frac{x}{1-x-x^2} = \frac{x}{(1-xr_+)(1-xr_-)} \\ &= \frac{1}{r_+ - r_-}\left(\frac{1}{1-xr_+} - \frac{1}{1-xr_-}\right) \\ &= \frac{1}{\sqrt{5}}\left(\sum_{j\geq 0} r_+^j x^j - \sum_{j\geq 0} r_-^j x^j\right). \end{aligned}$$

Odtud máme

$$F_n = \frac{r_+^n - r_-^n}{\sqrt{5}} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Protože

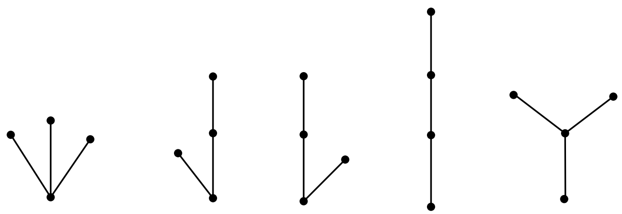
$$\left|\frac{r_-^n}{\sqrt{5}}\right| < \frac{1}{2},$$

platí dokonce, že

$$\boxed{F_n \doteq \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n.}$$

Zaokrouhlujeme na nejbližší celé číslo.

9.2 Pěstované stromy. *Pěstovaný strom* T na n vrcholech je zakořeněný strom s n vrcholy a s hranami orientovanými od kořene, v němž je každá množina synů jednoho vrcholu lineárně uspořádána. V rovině je kreslíme tak, že kořen leží nejníže, hrany jsou úsečky orientované směrem vzhůru a přirozené pravolevé uspořádání synů daného vrcholu se shoduje s předepsaným abstraktním uspořádáním. Jako příklad si uveďme všech pět pěstovaných stromů se čtyřmi vrcholy:



Není obtížné se přesvědčit, že na pěti vrcholech již máme čtrnáct pěstovaných stromů. Označíme-li si počet pěstovaných stromů na n vrcholech jako c_n, je zcela přirozenou otázka, zda pro čísla c_n neexistuje explicitní formule. Tu nyní pomocí GF odvodíme.

Zaveďme pro posloupnost $\{c_n\}_{n\geq 1}$ OGF:

$$C = C(x) = \sum_{n\geq 1} c_n x^n.$$

Každý pěstovaný strom T určuje dvojici (T_1, T_2), kde T_1 je podstrom kořenící v nejlevějším synu kořene T a T_2 je zbytek T. Patrně $|V(T_1)| + |V(T_2)| = |V(T)|$. Naopak, každá taková dvojice určuje jednoznačně T. Tento rozklad nelze provést pouze pro jednovrcholový strom. Tedy $c_1 = 1$ a pro $n > 1$

$$c_n = \sum_{i=1}^{n-1} c_i c_{n-i}.$$

Pomocí OGF se to stručněji vyjádří jako

$$C = C^2 + x.$$

Je-li tento textík vaším prvním setkáním s GF, nelitujte času pro zamyšlení nad předchozí úvahou! Ve složitějších obměnách se při enumeraci kombinatorických struktur stále vrací. Vyřešením kvadratické rovnice dostaneme

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

Záporné znaménko jsme zvolili proto, že koeficient u x^0 v C je nula. Číslo $c_n, n > 0$, je tedy rovno koeficientu u x^n v mocninném rozvoji funkce $(-\sqrt{1-4x})/2$. To se standardním způsobem stručně zapisuje jako

$$c_n = [x^n](-\sqrt{1-4x})/2.$$

Protože podle binomické věty

$$(1-4x)^{1/2} = \sum_{n\geq 0}\binom{1/2}{n}(-4x)^n,$$

dostáváme pro c_n vyjádření

$$c_n = \frac{-1}{2}\binom{1/2}{n}(-4)^n = (-1)^{n+1}4^n\,\frac{(1/2)((1/2)-1)\cdots((1/2)-n+1)}{2(n!)}.$$

Po další sérii snadných úprav, které přenecháváme čtenáři, dospíváme ke konečnému tvaru

$$\boxed{c_n = \frac{1}{n}\binom{2n-2}{n-1}.}$$

Členy posloupnosti

$$\{c_n\}_{n\geq 1} = \{1, 1, 2, 5, 14, 42, 132, 429, \ldots\}$$

se nazývají *Catalanovými čísly*.

9.3 Pěstované stromy podle počtu vrcholů a listů. *List* v pěstovaném stromu je vrchol, který nemá ani jednoho syna. Označme si počet pěstovaných stromů s a vrcholy a b listy jako $n(a,b)$. Např. $n(4,1) = 1, n(4,2) = 3, n(4,3) = 1$. Tato čísla zjemňují Catalanova čísla, neboť očividně

$$\sum_{b=1}^{a-1} n(a,b) = c_a.$$

Je zajímavé, že explicitní formule existuje i pro ně: