Přednáška 5, 27. března 2014 (část)

Rademacherova domněnka a její vyvrácení. K rozkladu na parciální zlomky použitému v odvození Schurovy asymptotiky koefientů $p_A(n)$ rozvoje

$$\frac{1}{(1-x^{a_1})(1-x^{a_2})\dots(1-x^{a_k})} = \sum_{n\geq 0} p_A(n)x^n$$

se váže zajímavý problém, jenž byl nedávno po více než 30 letech vyřešen. Vezmeme tento rozklad pro části $a_i = i$, $i = 1, 2, \dots, n$:

$$\frac{1}{(1-x)(1-x^2)\dots(1-x^n)} = \sum_{d=1}^{n} \sum_{0\leq e<d,\,(e,d)=1} \sum_{j=1}^{\lfloor n/d \rfloor} \frac{\beta(d,e,j,n)}{(1-\exp(2\pi i\cdot e/d)x)^j}\ .$$

V posmrtně publikované knize [2] H. Rademacher vyslovil domněnku, že koeficienty $\beta(\dots)$ se pro $n\to\infty$ blíží jistým limitním hodnotám (které explicitně uvádí, my tyto vzorce zde pomineme), tedy že pro každou pevnou trojici parametrů d, e, j existuje vlastní limita

$$\lim_{n\to\infty} \beta(d,e,j,n)\ .$$

Jak však nedávno dokázali M. Drmota a S. Gerhold v [1], tyto limity obecně neexistují a domněnka je vyvrácena.

Budeme se zabývat racionálními generujícími funkcemi (mocninnými řadami), což jsou podíly polynomů. Začneme tedy obecnými algebraickými vlastnostmi moc. řad a hlavně tím, jak se jimi dělí.

Jako $\mathbb{C}[[x]]$ označíme množinu všech formálních mocninných řad (dále fmř) s koeficienty v $\mathbb{C}$:

$$\mathbb{C}[[x]] = \{(a_0, a_1, a_2, \dots) = a_0 + a_1x + a_2x^2 + \dots = \textstyle\sum_{n\geq 0} a_nx^n \mid a_n \in \mathbb{C}\}$$

(první reprezentaci ve tvaru nekonečných posloupností nebudeme používat). Na $\mathbb{C}[[x]]$ máme známé operace sčítání a (Cauchyova) násobení:

$$\begin{aligned} \sum_{n\geq 0} a_nx^n + \sum_{n\geq 0} b_nx^n &:= \sum_{n\geq 0}(a_n+b_n)x^n \quad \text{a} \\ \sum_{n\geq 0} a_nx^n \cdot \sum_{n\geq 0} b_nx^n &:= \sum_{n\geq 0} \Big(\sum_{k=0}^{n} a_kb_{n-k}\Big)x^n\ . \end{aligned}$$

Není těžké ověřit, že $(\mathbb{C}[[x]], +, \cdot)$ je komutativní okruh s 1. Pro $f = f(x) = a_0 + a_1x + \cdots \in \mathbb{C}[[x]]$ definujeme $[x^n]f := a_n$ (koeficient u x^n). Pro $0 \neq f \in \mathbb{C}[[x]]$ definujeme $\mathrm{ord}(f)$, *řád* f, jako nejmenší $n \in \mathbb{N}_0$, že $[x^n]f \neq 0$; pro $f = 0$ definujeme $\mathrm{ord}(f) = +\infty$. Pak pro každé dvě fmř f, g máme identitu

$$\mathrm{ord}(fg) = \mathrm{ord}(f) + \mathrm{ord}(g)\ ,$$

která už v sobě zahrnuje, že pro nenulové fmř f, g je i jejich součin fg nenulový. Okruh $\mathbb{C}[[x]]$ je tedy obor integrity. Zjistíme, jaké jsou v něm jednotky, to jest které fmř mají multiplikativní inverz.

Tvrzení (jednotky v $\mathbb{C}[[x]]$). *Fmř $f(x) = a_0 + a_1x + a_2x^2 + \ldots$ je jednotka, právě když $[x^0]f = f(0) = a_0 \neq 0$, tj. právě když $\mathrm{ord}(f) = 0$.*

Důkaz. Pokud $a_0 = 0$, pak f není jednotka, protože fg má nulový konstantní člen pro každou fmř g a nikdy tedy nemáme $fg = 1$. Nechť $a_0 \neq 0$. Ukážeme, že existuje jediná $g(x) = b_0 + b_1 + b_2x^2 + \ldots$, že $fg = 1$. Poslední rovnost je ekvivalentní nekonečné soustavě rovnic (s neznámými b_n)

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ &\vdots \\ \textstyle\sum_{k=0}^{n} a_kb_{n-k} &= 0 \\ &\vdots\ . \end{aligned}$$

Ta má jednoznačné řešení: $b_0 = 1/a_0$, $b_1 = -a_1b_0/a_0 = -a_1/a_0^2$ a tak dále. Důvodem je, že v n-té rovnici je levá strana lineární funkce v b_n tvaru $a_0b_n + f_n(a_1, \ldots, a_n, b_0, \ldots, b_{n-1})$ a $a_0 \neq 0$, takže pro už vypočítané $b_0, b_1, \ldots, b_{n-1}$ je i b_n určeno jednoznačně. $\square$

Než ukážeme jiné vyjádření inverzu $1/f$, podíváme se na *podílově těleso okruhu* $\mathbb{C}[[x]]$. Je to nejmenší rozšíření $\mathbb{C}[[x]]$ na těleso, abychom mohli dělit každou nenulovou formální mocninnou řadou. Není těžké ukázat, že jím je těleso *(formálních) Laurentových řad*

$$\mathbb{C}((x)) = \{a_kx^k + a_{k+1}x^{k+1} + \cdots = \textstyle\sum_{n\geq k} a_nx^n \mid k \in \mathbb{Z},\ a_n \in \mathbb{C}\}\ ,$$

v němž operace $+$ a $\cdot$ jsou jako v $\mathbb{C}[[x]]$ (sčítání po složkách a Cauchyův součin). Jsou to tedy trochu obecnější fmř, s povolenými konečně mnoha mocninami x se záporným exponentem. Řečí inteligenčních testů: $\mathbb{C}((x))$ se má k $\mathbb{C}[[x]]$ jako se má $\mathbb{Q}$ k $\mathbb{Z}$.

Formální konvergence. Okruh fmř $\mathbb{C}[[x]]$ vybavíme strukturou formální konvergence. Řekneme, že posloupnost $(f_k)_{k\geq 1} = (f_1, f_2, \dots)$, kde $f_k = f_k(x) \in \mathbb{C}[[x]]$, *formálně konverguje*, když je pro každé $n \in \mathbb{N}_0$ posloupnost $([x^n]f_k)_{k\geq 1} \subset \mathbb{C}$ eventuálně konstantní, s hodnotou a_n. *Formální limitu* pak definujeme samozřejmě jako

$$\lim_{k\to\infty} f_k(x) = a_0 + a_1 x + a_2 x^2 + \dots \ .$$

Pomocí formální konvergence dokážeme za příhodných okolností sečíst nebo i vynásobit nekonečně mnoho fmř. Jsou-li $f_k = f_k(x) \in \mathbb{C}[[x]]$, pak nekonečná řada

$$\sum_{k=1}^{\infty} f_k$$

formálně konverguje, když formálně konverguje posloupnost částečných součtů $(f_1 + f_2 + \dots + f_k)_{k\geq 1}$. Limita této posloupnosti pak je *součtem dané nekonečné řady*. Podobně definujeme hodnotu nekonečného součinu

$$\prod_{k=1}^{\infty}(1 + f_k)$$

jako formální limitu posloupnosti částečných součinů. Na rozdíl od klasické (tj. archimedovské) analýzy máme v případě formální konvergence v $\mathbb{C}[[x]]$ (kterou lze zachytit jistou nearchimedovskou metrikou popř. normou, již nebudeme zavádět) jednoznačné kritérium konvergence nekonečných řad:

Tvrzení (kritérium konvergence). *Nekonečná řada fmř*

$$\sum_{k=1}^{\infty} f_k,\ \ f_k \in \mathbb{C}[[x]]\ ,$$

formálně konverguje, právě když pro $k \to \infty$ i $\mathrm{ord}(f_k) \to \infty$.

Důkaz. DOM. CV. □

Příkladem použití nekonečných řad fmř je vyjádření multiplikativního inverzu, jehož existenci jsme dokázali v předminulém tvrzení.

Tvrzení ($1/f$ jako součet geometrické řady). *Nechť* $f = f(x) = a_0 + a_1x + a_2x^2 + \cdots \in \mathbb{C}[[x]]$ *a* $a_0 \neq 0$. *Pak*

$$\frac{1}{f} = \frac{1}{a_0}\sum_{n=0}^{\infty}\Big(-\frac{a_1}{a_0}x - \frac{a_2}{a_0}x^2 - \dots\Big)^n \,.$$

Důkaz. Fmř v závorce označíme jako $g = g(x)$. Daná nekonečná řada formálně konverguje podle posledního tvrzení, protože $\mathrm{ord}(g^n) \geq n$. Tedy $fa_0^{-1} = 1 - g$ a (protože formální limita a součin komutují)

$$fa_0^{-1}\sum_{n\geq 0} g^n = (1-g)\lim_{N\to\infty}(1 + g + g^2 + \cdots + g^N) = \lim_{N\to\infty}(1 - g^{N+1}) = 1 \,.$$

$\square$

Reference

[1] M. Drmota and S. Gerhold, Disproof of a conjecture by Rademacher on partial fractions, `http://arxiv.org/abs/1312.4289` .

[2] H. Rademacher, *Topics in Analytic Number Theory*, Springer, New York, 1973 (edited by E. Grosswald, J. Lehner and M. Newman).