KALEIDOSKOP TEORIE ČÍSEL

(7. kapitola)

Martin Klazar

Vím, že čísla jsou krásná. A jestliže krásná nejsou, pak není krásné nic.

(Paul Erdős, *Sunday Times Magazine,* 27. listopadu 1988.)

Analogicky prožíval pan Š. číslice.
“Pro mne 2, 4, 6, 5 nejsou pouhá čísla. Mají tvar ...
1 — to je ostré číslo, nezávisle na jeho grafickém vyjádření,
je to něco ukončeného, tvrdého.
2 — to je plošší, čtverhranné, bělavé, bývá trochu našedlé ...
3 — to je zaostřený úlomek a točí se.
4 — to je opět čtvercové, tupé, podobné 2, ale mohutnější, tlusté ...
5 — plné zakončení v podobě kužele, věže, masívní.
6 — to následuje první za “5”, je bělavé.
8 — to je nevinné, modravě mléčné, podobné vápnu.”

(A. R. Lurija, *Malá Knížka o Velké Paměti.*)

Toto je předběžný text 7. kapitoly o číselných rozkladech ze skript k mé přednášce *Úvod do teorie čísel*, kterou jsem konal na MFF UK v Praze v zimních semestrech školních roků 1996/97, 1998/99, 1999/00, 2000/01 a 2001/02. Zatím v preprintové řadě KAM-DIMATIA Series vyšly kapitoly 1 (základní pojmy a obraty), 2 (diofantické aproximace), 3 (diofantické rovnice), 4 (kongruence) a 5 (prvočísla) a budou v ní postupně vydány zbylé kapitoly 6 (geometrie čísel), 8 (medailony matematiků) a 9 (návody k řešením úloh). Obtížnost úloh je bodována 0 (nejlehčí) až 5 (nejtěžší).

říjen 2002 Martin Klazar

Obsah

Kapitola 7

Číselné rozklady

Kolika způsoby lze dané přirozené číslo rozložit na součet přirozených čísel, nezáleží-li na pořadí sčítanců? G. W. Leibniz se na to zeptal J. Bernoulliho v dopisu v r. 1674. Zkusmo zjistil, že zpočátku jsou počty rozkladů prvočíselné: 3 má tři rozklady (3, $2+1$ a $1+1+1$), 4 pět, 5 sedm a 6 jedenáct. Vše kazí 7 s patnácti rozklady. Existuje nekonečně mnoho přirozených čísel s prvočíselným počtem rozkladů? Andrews uvádí, že tento problém naznačený Leibnizovými úvahami je stále otevřený. Z výsledků o kongruencích partitní funkce, které dokážeme v této kapitole, plyne, že naopak pro nekonečně mnoho n je počet rozkladů složené číslo.

Kapitolu 7 věnujeme číselným rozkladům a příbuzným otázkám. Jejich teorie je součástí aditivní teorie čísel, která zkoumá aritmetické vlastnosti operace sčítání. První etapa rozvoje aditivní teorie čísel proběhla po polovině 18. století, kdy L. Euler zkoumal číselné rozklady a partitní funkci a kdy byly zformulovány její nejznámější problémy, které patří současně k nejslavnějším matematickým problémům: Goldbachův (každé sudé přirozené číslo větší než 2 je součtem dvou prvočísel) a Waringův (každé přirozené číslo je součtem omezeně mnoha čtverců, omezeně mnoha třetích mocnin, omezeně mnoha čtvrtých mocnin, atd.). Zatímco Goldbachův problém zůstává stále otevřený, Waringův byl ve své původní formulaci úplně vyřešen, ale jeho některé aspekty stále matematiky zaměstnávají.

V předchozích kapitolách jsme se už s řadou výsledků aditivní teorie čísel setkali. Patří k nim Eulerova věta 20 o dvou čtvercích (kapitola 2), Lagrangeova věta 55 o čtyřech čtvercích (kapitola 3), Erdős–Ginzburg–Zivova věta 97 a výsledky o Sidonových množinách (kapitola 4), samozřejmě Šnirelmanova věta 150 (kapitola 5), výsledky o funkci $r_2(n)$ (tj. fakticky celý kruhový problém) a zejména Erdős–Fuchsova věta 209 (kapitola 6).

V oddílu 7.1 zavedeme klasické číselné rozklady a pomocí Ferrersových diagramů dokážeme dvě pozoruhodné identity: Eulerovu pentagonální identitu (věta 215) a Jacobiho třísoučinovou identitu (věta 216). Z Jacobiho identity odvodíme řadu důsledků, které použijeme dále. Dokážeme Ramanujanovu větu 224 o kongruencích partitní funkce $p(n)$ modulo 5, 7 a 11. V oddílu 7.2 odvodíme dvě známé Jacobiho formule pro počty vyjádření přirozených čísel součtem dvou a čtyř celočíselných čtverců. Oddíl 7.3 obsahuje jeden klasický a dva neklasické výsledky o rozkladových identitách: Rogers–Ramanujanovy identity (věta 227), identitu pro divácké rozklady (věta 228) a kombinatorickou metaidentitu založenou na principu inkluze a exkluze (věta 232). V oddílu 7.4 odvodíme ve větě 237 asymptotiku partitní funkce. Oddíl 7.5 je věnován Linnikovu elementárnímu řešení Waringova problému — ukážeme, že pro každé přirozené číslo k existuje počet $g = g(k)$ tak, že každé přirozené čislo je součtem nejvýše g k-tých mocnin přirozených čísel.

7.1 Klasické číselné rozklady

Uspořádaným k-ticím přirozených čísel $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ budeme říkat *kompozice*. Pokud $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k \geq 1$, říkáme jim *rozklady*. Sumu $\lambda_1 + \lambda_2 + \cdots + \lambda_k$ značíme jako $|\lambda|$. Pokud $|\lambda| = n$, řekneme, že λ je *kompozicí*, popřípadě *rozkladem, čísla n*. Číslům λ_i říkáme *části* kompozice či rozkladu. Části jsou obvykle kladné, ale někdy (třeba v diváckých rozkladech v oddílu 7.3) povolujeme i nulové části. Budeme se zabývat enumerací rozkladů. Enumeraci kompozic, která je většinou snazší a více záležitostí kombinatoriky, věnujeme pouze úlohu 1. Například číslo 6 má 11 rozkladů, jak věděl už Leibniz:

$$\begin{gathered}6,\ 5+1,\ 4+2,\ 4+1+1,\ 3+3,\ 3+2+1,\ 3+1+1+1,\\ 2+2+2,\ 2+2+1+1,\ 2+1+1+1+1\ \text{ a }\ 1+1+1+1+1+1\ .\end{gathered}$$

Skutečnost, že $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ je rozkladem n se zapisuje značením

$$\lambda \vdash n\ .$$

Opakování částí se zachycuje pomocí exponentů. Závorky a oddělující čárky se pro stručnost vynechávají (pokud části nepřesahují 9, nemůže dojít k nedorozumění). Rozklady čísla 6 v tomto zápisu jsou:

$$6,\ 51,\ 42,\ 41^2,\ 3^2,\ 321,\ 31^3,\ 2^3,\ 2^21^2,\ 21^4\ \text{ a }\ 1^6\ .$$

Počet všech rozkladů čísla n se označuje $p(n)$ a funkce $p(n)$ se nazývá *partitní funkcí*. Předchozí příklad ukazuje, že $p(6) = 11$. První hodnoty partitní funkce jsou:

n	1	2	3	4	5	6	7	8	9	10	11	12
$p(n)$	1	2	3	5	7	11	15	22	30	42	56	77

Roznásobením nekonečně mnoha závorek $(1 + x^1 + x^2 + x^3 + x^4 + \cdots)(1 + x^2 + x^4 + x^6 + x^8 + \cdots)(1 + x^3 + x^6 + x^9 + x^{12} + \cdots)\ldots$ dostaneme mocninnou řadu, v níž koeficient u x^n je roven počtu nezáporných celočíselných řešení rovnice

$$n = x_1 + 2x_2 + 3x_3 + \cdots\ .$$

Tato řešení odpovídají vzájemně jednoznačně rozkladům čísla n, protože x_i je počet částí i v rozkladu n. Koeficient u x^n se tedy rovná $p(n)$. Protože $1 + x^i + x^{2i} + x^{3i} + \cdots = 1/(1 - x^i)$, dostáváme *součinový tvar* (klademe $p(0) = 1$)

$$\sum_{n\ge 0} p(n)x^n = \prod_{n=1}^{\infty} \frac{1}{1 - x^n}\ .$$

Názorným prostředkem pro práci s rozklady jsou *Ferrersovy diagramy*. Ferrersův diagram rozkladu $(\lambda_1, \lambda_2, \ldots, \lambda_p) \vdash n$ je maticové schéma s p řádky a λ_1 sloupci, v němž i-tý řádek (počítáno shora) obsahuje λ_i teček a tečky v řádcích jsou zarovnány vlevo. Například rozklady $2^21^2 \vdash 6$, $321 \vdash 6$ a $5^32 \vdash 17$ se Ferrersovými diagramy zaznamenají jako

$$\begin{array}{ll} \bullet & \bullet \\ \bullet & \bullet \\ \bullet & \\ \bullet & \end{array} \qquad\qquad \begin{array}{lll} \bullet & \bullet & \bullet \\ \bullet & \bullet & \\ \bullet & & \end{array} \qquad\qquad \begin{array}{lllll} \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & & & \end{array}$$

Následující věta je snad první známou rozkladovou identitou. V oddílu 7.3 ji dvěma netriviálními způsoby rozvineme.

Věta 213 (Euler, 1748). *Každé $n \in \mathbf{N}$ má tolik rozkladů na vzájemně různé části jako rozkladů na liché části.*

Důkaz. Uvádíme dva důkazy. První používá generující funkce. Jako $p_r(n)$ a $p_l(n)$ označíme počty rozkladů čísla n na různé části a na liché části. Podobně jako jsme odvodili vyjádření generující funkce hodnot $p(n)$ nekonečným součinem, máme i

$$\sum_{n\geq 0} p_r(n)x^n = \prod_{n=1}^{\infty}(1+x^n) \quad \text{a} \quad \sum_{n\geq 0} p_l(n)x^n = \prod_{n=1}^{\infty} \frac{1}{1-x^{2n-1}} \ ,$$

kde opět $p_r(0) = p_l(0) = 1$. Protože

$$1 + x^n = \frac{1-x^{2n}}{1-x^n},$$

dostáváme zkrácením faktorů $1 - x^{2n}$, že se oba nekonečné součiny rovnají:

$$\prod_{n=1}^{\infty}(1+x^n) = \prod_{n=1}^{\infty} \frac{1-x^{2n}}{1-x^n} = \prod_{n=1}^{\infty} \frac{1}{1-x^{2n-1}} \ .$$

V druhém důkazu sestrojíme bijekci mezi rozklady obou druhů. Nechť $a_1 > a_2 > \cdots > a_k \geq 1$ je rozklad n na různé části. Číslo a_i má jednoznačné vyjádření $a_i = 2^{b_i}c_i$, kde $b_i \in \mathbf{N}_0$ a $c_i \in \mathbf{N}$ je liché. Každou část a_i nahradíme 2^{b_i} částmi c_i a vše uspořádáme sestupně podle velikosti. Výsledný rozklad je rozkladem n na liché části. Naopak, mějme rozklad n na liché části. Jako $d_m \in \mathbf{N}$, $m \in \mathbf{N}$ liché, označíme počet částí m. Každé číslo $v \in \mathbf{N}$ má jednoznačný rozklad na součet různých mocnin čísla 2 (daný binárním rozvojem v). Označme množinu těchto mocnin 2 jako $S(v)$. Nyní d_m částí m v rozkladu n nahradíme částmi xm, kde x probíhá $S(d_m)$. Vznikne rozklad n na různé části. Obě transformace jsou vzájemně inverzní a tvoří hledanou bijekci. Například, pro $n = 185$ si v ní odpovídají rozklady

$$(80, 40, 32, 12, 10, 5, 3, 2, 1) \ \text{ a } \ (5^{27}, 3^5, 1^{35}).$$

$\diamondsuit$

Nechť $p(n;k)$ je počet rozkladů čísla n na části nepřesahující k. Stejně snadno, jako jsme nahlédli součinové formule pro $\sum_{n\geq 0} p(n)x^n$, $\sum_{n\geq 0} p_l(n)x^n$ a $\sum_{n\geq 0} p_r(n)x^n$, vidíme, že i

$$\sum_{n\geq 0} p(n;k)x^n = \frac{1}{(1-x)(1-x^2)\dots(1-x^k)} \ .$$

Operace *konjugace* Ferrersova diagramu rozkladu znamená jeho transponování podle úhlopříčky; prostě záměníme řádky a sloupce. Rozklady, které se konjugací nemění, jako třeba $521^3 \vdash 10$, se nazývají *samokonjugované* (viz úloha 4b). Konjugace je bijekce (dokonce involuce) množiny všech rozkladů n na sebe a převádí počet částí na velikost největší části a naopak. Počet rozkladů n na nejvýše k částí se tedy také rovná $p(n;k)$. Obě podmínky současně definují počet $p(n;k,l)$ rozkladů n na nejvýše l částí, které nepřesahují k. Názorně, $p(n;k,l)$ je počet rozkladů čísla n, jejichž Ferrersovy diagramy se vejdou do obdélníku $k \times l$ (vzhledem ke konjugaci je jedno, co je délka a co šířka). Je pozoruhodné, že i generující polynom čísel $p(n;k,l)$ má jednoduchý součinový tvar, uvedeme ho následujícím tvrzení. Jedná se o polynom, protože $p(n;k,l) = 0$, jakmile $n > kl$.

Pro $a, b \in \mathbf{N}_0$, $a \geq b$, definujeme *q-binomický koeficient* (nebo též *Gaussův koeficient*) jako racionální funkci

$$\binom{a}{b}_q = \frac{(1-q^{a-b+1})(1-q^{a-b+2})\dots(1-q^a)}{(1-q)(1-q^2)\dots(1-q^b)} \ .$$

Je jasné, že i

$$\binom{a}{b}_q = \frac{(q)_a}{(q)_b(q)_{a-b}} \ ,$$

kde pro $n \in \mathbf{N}$ značíme $(q)_n = (1-q)(1-q^2)\dots(1-q^n)$ a $(q)_0 = 1$. Odtud je zřejmé, že $\binom{a}{a-b}_q = \binom{a}{b}_q$. Z třetí ekvivalentní formy

$$\binom{a}{b}_q = \frac{\prod_{i=1}^{a}(1+q+q^2+\dots+q^{i-1})}{\prod_{i=1}^{b}(1+q+q^2+\dots+q^{i-1})\prod_{i=1}^{a-b}(1+q+q^2+\dots+q^{i-1})} \ ,$$

kterou dostaneme z druhé zkrácením faktoru $(1-q)^a$, plyne, že $\binom{a}{b}_{q=1} = \binom{a}{b}$. Z rekurence odvozené v důkazu následujícího tvrzení plyne, že $\binom{a}{b}_q$ je vlastně polynom stupně $b(a-b)$, jehož koeficienty jsou kladná celá čísla. Tato čísla jsou právě počty $p(n;k,l)$.

Tvrzení 214 (význam q-binomického koeficientu). *Nechť $p(n;k,l)$ je počet rozkladů čísla n na nejvýše l částí nepřesahujících k. Pak*

$$\sum_{n=0}^{kl} p(n;k,l)q^n = \binom{k+l}{k}_q \ .$$

DŮKAZ. Označme $b(k,l) = \binom{k+l}{k}_q$. Podle definic $b(k,0) = 1$ a $b(0,l) = 1$ pro všechna $k, l \in \mathbf{N}_0$ a

$$\begin{aligned} b(k,l) - b(k,l-1) &= \frac{(q)_{k+l-1}}{(q)_k (q)_l} \cdot ((1-q^{k+l}) - (1-q^l)) \\ &= q^l (1-q^k) \cdot \frac{(q)_{k+l-1}}{(q)_k (q)_l} = q^l \cdot \frac{(q)_{k+l-1}}{(q)_{k-1} (q)_l} \\ &= q^l \cdot b(k-1,l) \ . \end{aligned}$$

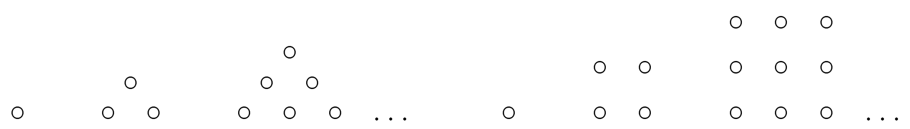
Rekurence $b(k,l) - b(k,l-1) = q^l \cdot b(k-1,l)$ určuje $b(k,l)$ jednoznačně pro všechna $k, l \in \mathbf{N}_0$ a ukazuje, že $b(k,l)$ jsou polynomy. Generující polynom čísel $p(n;k,l)$ si označíme $c(k,l)$. Stačí ukázat, že $c(k,l)$ splňuje tutéž rekurenci jako $b(k,l)$. Okrajové podmínky $c(k,0) = c(0,l) = 1$ jsou jasné z definice. Rozdíl $c(k,l) - c(k,l-1)$ je generující polynom počtů rozkladů na *právě* l částí nepřesahujících k. Stačí nalézt bijekci mezi těmito rozklady čísla n a rozklady čísla $n-l$ na nejvýše l částí nepřesahujících $k-1$. Tato bijekce je dána vypuštěním částí rovných jedné a zmenšením ostatních částí o jednu. Takže $c(k,l) - c(k,l-1) = q^l \cdot c(k-1,l)$ a tvrzení je dokázáno. $\diamondsuit$

Pro další kombinatorickou interpretaci $\binom{a}{b}_q$ a další q-zobecnění viz úlohy 5 a 6.

Číslo $n \in \mathbf{N}$ se nazývá *pentagonální* (či *pětiúhelníkové*), pokud $n = (3m^2 - m)/2$ pro vhodné $m \in \mathbf{Z} \backslash \{0\}$. Trochu jinak řečeno, jsou to čísla $(3m^2 \pm m)/2$, kde $m \in \mathbf{N}$. Posloupnost pentagonálních čísel začíná

$$1,\ 2,\ 5,\ 7,\ 12,\ 15,\ 22,\ 26,\ 35,\ 40,\ \ldots$$

Terminologie má geometrický původ. *Trojúhelníková čísla* $1,\ 3 = 1+2,\ 6 = 1+2+3, \ldots$ a *čtvercová čísla* $1,\ 4 = 1+3,\ 9 = 1+3+5, \ldots$ vzniknou z trojúhelníkových a čtvercových schémat:



Pětiúhelníková čísla (přesněji, polovina jejich posloupnosti) $1,\ 5 = 1+4,\ 12 = 1+4+7, \ldots$ vzniknou z podobných pětiúhelníkových schémat. Následující věta je známá jako *Eulerova pentagonální identita*.

Věta 215 (Euler, 1748). *Označme $\omega(m) = (3m^2 - m)/2$. Následující tři tvrzení jsou vzájemně ekvivalentní.*

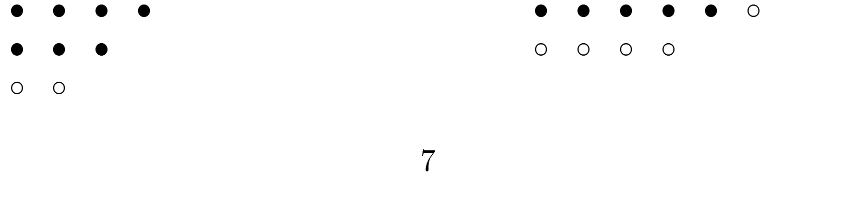
1.
$$\prod_{k=1}^{\infty}(1-x^k) = 1 + \sum_{m=1}^{\infty}(-1)^m(x^{\omega(m)} + x^{\omega(-m)}) = \sum_{m=-\infty}^{\infty}(-1)^m x^{\omega(m)} \ .$$

2. *Pro nepentagonální $n \in \mathbf{N}$ je počet jeho rozkladů na sudý počet různých částí týž jako počet rozkladů na lichý počet různých částí. Pro pentagonální $n = \omega(\pm m)$ přesahuje první počet druhý o $(-1)^m$.*

3. *Pro každé $n \in \mathbf{N}$ platí rekurence*
$$\begin{aligned} p(n) &= \sum_{m\ge 1}(-1)^{m+1}(p(n-\omega(m)) + p(n-\omega(-m))) \\ &= p(n-1) + p(n-2) - p(n-5) - p(n-7) \\ &\quad + p(n-12) + p(n-15) - \dots \ , \end{aligned}$$
kde klademe $p(0) = 1$ a $p(k) = 0$ pro $k < 0$.

Důkaz. **(Franklin, 1881).** Nejprve ukážeme, že všechny tři formulace říkají totéž, a pak dokážeme druhou z nich. Že 1 $\Leftrightarrow$ 2 je jasné z rozvoje nekonečného součinu v mocninnou řadu: koeficient u x^n je právě rozdíl počtů rozkladů popsaných v druhé formulaci. Že 1 $\Leftrightarrow$ 3 plyne z porovnání koeficientů u x^n v identitě
$$\Big(\sum_{n\ge 0} p(n)x^n\Big)\prod_{n=1}^{\infty}(1-x^n) = 1 \ ,$$
která je důsledkem součinové formule pro $\sum_{n\ge 0} p(n)x^n$.

Nechť $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k) \vdash n$, $\lambda_1 > \lambda_2 > \dots > \lambda_k$, je rozklad n na různé části. *Základnou* Ferrersova diagramu λ rozumíme poslední řádek a jeho *sklonem* rozumíme nejdelší souvislý úsek teček jdoucí jihozápadním směrem a začínající v poslední tečce prvního řádku. Označíme-li velikosti základny a sklonu z a s, máme $z = \lambda_k$ a $s = \max j$, že $\lambda_1, \lambda_1 - 1, \lambda_1 - 2, \dots, \lambda_1 - j + 1$ jsou části λ. V následujících diagramech jsme vyznačili sklon a základnu pro rozklady $(7, 6, 4, 3, 2) \vdash 22$ a $(8, 7, 6, 4) \vdash 25$:



Z rozkladu $\lambda \vdash n$ vytvoříme nový rozklad $\mu \vdash n$ tak, že v případě $z \leq s$ základnu přesuneme na místo nového sklonu a v případě $z > s$ přesuneme sklon na místo nové základny. Například z $\lambda = (7, 6, 4, 3, 2)$ vznikne $\mu = (8, 7, 4, 3)$ a z $\lambda = (8, 7, 6, 4)$ vznikne $\mu = (7, 6, 5, 4, 3)$:

• • • • • • ○ ○	• • • • • • •
• • • • • ○ ○	• • • • • •
• • • •	• • • • •
• • •	○ ○ ○ ○
	○ ○ ○

Podívejme se na situace, kdy transformace $\lambda \mapsto \mu$ nefunguje. První případ nefunguje (nevznikne Ferrersův diagram), právě když $z = s = k$ a základna a sklon se protínají:

• • • • ○
• • • ○
○ ○ ○

Pak $n = k + (k+1) + \cdots + (2k-1) = \omega(k)$. Druhý případ nefunguje (vznikne Ferrersův diagram, ale ne s různými částmi), právě když $s = k$, $z = k+1$ a základna a sklon se protínají:

• • • ○
○ ○ ○

Pak $n = (k+1) + (k+2) + \cdots + 2k = \omega(-k)$.

Transformace $\lambda \mapsto \mu$ je involucí na množině rozkladů n na různé části. Mění počet částí o 1, pro nepentagonální n je definována pro každé λ a pro $n = \omega(\pm k)$ není definována pro jediný rozklad. Tato involuce vždy páruje rozklad se sudým počtem různých částí s rozkladem s lichým počtem různých částí. Parita počtu částí jediného nespárovaného rozkladu pentagonálního n je rovna paritě k. Druhé tvrzení je dokázáno. $\diamondsuit$

Následující identita je známa jako *Jacobiho třísoučinová identita* (Jacobi triple product identity), dále stručně JTI.

Věta 216 (Jacobi, 1829).

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1}z)(1+x^{2n-1}z^{-1}) = \sum_{n=-\infty}^{\infty} x^{n^2} z^n \ .$$

DŮKAZ. **(Wright, 1965).** Podáme kombinatorický důkaz pomocí Ferrersových diagramů. Faktor $1 - x^{2n}$ převedeme na druhou stranu a substitucí $u = xz$ a $v = x/z$ zavedeme nové proměnné u a v. Dostaneme ekvivalentní tvar JTI:

$$\prod_{n=1}^{\infty}(1+u^n v^{n-1})(1+u^{n-1}v^n) = \sum_{r=-\infty}^{\infty} u^{r(r+1)/2}v^{r(r-1)/2}\prod_{k=1}^{\infty}\frac{1}{1-u^k v^k} \ .$$

Vlevo po roznásobení dostaneme mocninnou řadu o dvou proměnných

$$\sum_{n,m\geq 0} a(n,m)u^n v^m \ ,$$

kde koeficient $a(n,m)$ je roven počtu rozkladů čísla $n + m\sqrt{-1}$ na vzájemně různé části tvaru

$$a + (a-1)\sqrt{-1} \ \text{ a } \ (b-1) + b\sqrt{-1}$$

($a, b \in \mathbf{N}$). Vpravo nekonečný součin nahradíme $\sum_{k\geq 0} p(k)x^k$. Vidíme, že potřebujeme dokázat rovnost

$$a(n,m) = p(k) \ , \quad \text{kde} \ \ n = k + r(r+1)/2 \ \text{ a } \ m = k + r(r-1)/2 \ .$$

Čísla $k \in \mathbf{N}_0$ a $r \in \mathbf{Z}$ jsou čísly $n, m \in \mathbf{N}$ jednoznačně určena. Bez újmy na obecnosti lze vzít $n \geq m$ (to je ekvivalentní s $r \geq 0$). Bijekci mezi rozklady $n+m\sqrt{-1}$ na různé části tvaru $a+(a-1)\sqrt{-1}$ a $(b-1)+b\sqrt{-1}$ a obyčejnými rozklady k popíšeme na konkrétním příkladu $n = 43$ a $m = 39$. Pak $k = 33$ a $r = 4$. Vezmeme rozklad

$$\kappa = (10, 7, 5, 4, 3^2, 1) \vdash 33 \ .$$

Na Ferrersův diagram rozkladu $\lambda \vdash n$ přiložíme na první řádek pravoúhlé trojúhelníkové schéma složené z r nových řádků s $1, 2, \ldots, r$ novými tečkami. Celkem dostaneme n teček. Posloupnost r teček začínající v první (a jediné) tečce v novém prvním řádku a jdoucí jihovýchodně prodloužíme na maximální délku starými tečkami. Vzniklou posloupnost teček nazveme *hranicí*. Pro náš konkrétní rozklad $\kappa \vdash 33$ dostaneme (na obrázku jsou nové tečky označeny kroužky a hranice je označena asterixy):

$$
\begin{array}{llllllllll}
* \\
\circ & * \\
\circ & \circ & * \\
\circ & \circ & \circ & * \\
\bullet & \bullet & \bullet & \bullet & * & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & * & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet \\
\bullet
\end{array}
$$

Část diagramu ležící nad hranicí a čtená po řádcích dává hodnoty čísel $b-1$ (může být i $b-1=0$). V našem příkladu $b-1=5,1$. Část diagramu ležící na hranici a pod ní a čtená po sloupcích dává hodnoty a. V našem příkladu $a=11,9,8,5,3,1$. Obě posloupnosti jsou klesající. Je evidentní, že součet všech hodnot a a $b-1$ je n. Protože hodnot a je o r více než hodnot b, je součet všech hodnot $a-1$ a b roven $n-r=m$. Sčítance $a+(a-1)\sqrt{-1}$ a $(b-1)+b\sqrt{-1}$ tvoří rozklad $n+m\sqrt{-1}$ na různé části. V našem příkladu

$$
\begin{aligned}
43+39\sqrt{-1} &= (11+10\sqrt{-1})+(9+8\sqrt{-1})+(8+7\sqrt{-1})+(5+4\sqrt{-1}) \\
&\quad +(3+2\sqrt{-1})+1+(5+6\sqrt{-1})+(1+2\sqrt{-1})\ .
\end{aligned}
$$

Popsaná korespondence je hledanou bijekcí. $\diamondsuit$

Jiný důkaz JTI je popsán v úloze 7.

Následující identity, zejména vyjádření součinů $\prod_{n\geq 1}(1-x^n)^r$ pro $r=3,6$ a 10 sumami (pro $r=1$ viz 1 věty 215), budeme potřebovat k důkazům Ramanujanových kongruencí pro hodnoty partitní funkce, k důkazům Jacobiho čtvercových identit v následujícím oddílu a konečně k důkazu Rogers–Ramanujanových identit v oddílu 7.3.

Tvrzení 217 (důsledek JTI).

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

Důkaz. Součin vlevo mírně upravíme na

$$\begin{aligned}\prod_{n=1}^{\infty}\frac{(1-x^{2n-1})(1-x^{2n})}{1+x^n} &= \prod_{n=1}^{\infty}(1-x^{2n-1})(1-x^n)\\ &= \prod_{n=1}^{\infty}(1-x^{2n-1})(1-x^{2n-1})(1-x^{2n})\end{aligned}$$

a použijeme JTI se $z=-1$. ♢

Tvrzení 218 (důsledek JTI).

$$\begin{aligned}\prod_{n=1}^{\infty}(1-x^{5n})(1-x^{5n-2})(1-x^{5n-3}) &= \sum_{n=-\infty}^{\infty}(-1)^n x^{n(5n+1)/2}\\ \prod_{n=1}^{\infty}(1-x^{5n})(1-x^{5n-1})(1-x^{5n-4}) &= \sum_{n=-\infty}^{\infty}(-1)^n x^{n(5n+3)/2}\ .\end{aligned}$$

Důkaz. V JTI provedeme substituci $x\mapsto x^k$ a $z\mapsto -x^l$ a dostaneme

$$\prod_{n=1}^{\infty}(1-x^{2kn})(1-x^{2kn-k-l})(1-x^{2kn-k+l})=\sum_{n=-\infty}^{\infty}(-1)^n x^{kn^2+ln}\ .$$

Dokazované identity jsou speciálními případy této obecnější identity pro volbu $k=5/2, l=1/2$ a $k=5/2, l=3/2$. ♢

Lemma 219.

$$(z-z^{-1})\prod_{n=1}^{\infty}(1-x^n)(1-x^n z^2)(1-x^n z^{-2})=\sum_{n=-\infty}^{\infty}(-1)^n x^{n(n+1)/2}z^{2n+1}\ .$$

Důkaz. Tato identita plyne z JTI (věta 216) postupnými substitucemi $z\mapsto -xz^2$ a $x^2\mapsto x$ a vynásobením z. ♢

Tvrzení 220 (třetí mocnina).

$$\prod_{n=1}^{\infty}(1-x^n)^3=\sum_{n=0}^{\infty}(-1)^n(2n+1)x^{n(n+1)/2}\ .$$

Důkaz. Identitu v předchozím lemmatu zderivujeme podle z, položíme $z = 1$ a výsledek vydělíme dvěma. Derivaci nekonečného součinu nemusíme počítat, protože má výsledně beztak nulový koeficient. $\diamondsuit$

Tvrzení 221 (šestá mocnina).

$$\prod_{n=1}^{\infty}(1-x^n)^6 \;=\; \frac{1}{2}\sum_{r,s=-\infty}^{\infty}((2r+1)^2-(2s)^2)x^{r^2+s^2+r} \;.$$

Důkaz. Identitu tvrzení 220 přepíšeme pro sumaci přes $\mathbf{Z}$ a umocníme na druhou. Dostaneme

$$\prod_{n=1}^{\infty}(1-x^n)^6 = \frac{1}{4}\sum_{m,n=-\infty}^{\infty}(-1)^{m+n}(2m+1)(2n+1)x^{(m^2+n^2+m+n)/2} \;.$$

Sumu vpravo rozdělíme na dvě podle parity $m+n$. Pro sudé $m+n$ položíme $r=(m+n)/2$ a $s=(m-n)/2$ a pro liché $m+n$ položíme $r=(m-n-1)/2$ a $s=(m+n+1)/2$. Snadno se ověří, že v prvním případě $(2m+1)(2n+1) = (2r+1)^2-(2s)^2$ a $m^2+n^2+m+n = 2(r^2+s^2+r)$ a v druhém $-(2m+1)(2n+1) = (2r+1)^2-(2s)^2$ a $m^2+n^2+m+n = 2(r^2+s^2+r)$. Sudá a lichá suma po přechodu k r a s splynou, čímž dostáváme dokazovanou identitu. $\diamondsuit$

Tvrzení 222 (desátá mocnina podle Winquista).

$$\prod_{n=1}^{\infty}(1-x^n)^{10}$$
$$= \sum_{i=0}^{\infty}\sum_{j=-\infty}^{\infty}(-1)^{i+j}(2i+1)(6j+1)\frac{(3i+1)(3i+2)-3j(3j+1)}{2}\cdot x^k \;,$$

kde $k = k(i,j) = 3i(i+1)/2 + j(3j+1)/2$.

Důkaz. Dokazovaná identita je specializací obecnější veleidentity

$$\prod_{n=1}^{\infty}(1-ax^{n-1})(1-a^{-1}x^n)(1-bx^{n-1})(1-b^{-1}x^n)(1-ab^{-1}x^{n-1})$$
$$(1-a^{-1}bx^n)(1-abx^{n-1})(1-a^{-1}b^{-1}x^n)(1-x^n)^2$$
$$= \sum_{j=-\infty}^{\infty}\sum_{i=0}^{\infty}(-1)^{j+i}\Big((b^{-3j}-b^{3j+1})(a^{-3i}-a^{3i+3})$$
$$+ (b^{3i+2}-b^{-3i-1})(a^{-3j+1}-a^{3j+2})\Big)x^{j(3j+1)/2+i(3i+1)/2} \;.$$

Dokažme ji. Desetičlenný součin vlevo si označíme $F(a,b,x)$. Snadno se ověří, že

$$F(ax,b,x) = -F(a,b,x)\cdot a^{-3} \quad \text{a} \quad F(a^{-1},b,x) = -F(a,b,x)\cdot a^{-3}\ .$$

Nechť $[a^r]F$ pro $r \in \mathbf{Z}$ označuje koeficient u a^r v roznásobeném součinu F. Podle první rovnice máme pro každé $k \in \mathbf{N}_0$

$$[a^{r+3k}]F = (-1)^k x^{(r+3k-3)+(r+3k-6)+\cdots+r}[a^r]F = (-1)^k x^{kr+3k(k-1)/2}[a^r]F\ .$$

Podle druhé máme $[a^{3-r}]F = -[a^r]F$. Položíme-li $r=0$ a $r=2$ a označíme-li $[a^0]F = A_0(b,x)$ a $[a^1]F = A_1(b,x)$, dostáváme

$$\begin{aligned} F(a,b,x) &= A_0(b,x)\sum_{i=0}^{\infty}(-1)^i(a^{-3i}-a^{3i+3})x^{3i(i+1)/2} \\ &\quad + A_1(b,x)\sum_{j=-\infty}^{\infty}(-1)^j(a^{-3j+1}-a^{3j+2})x^{j(3j+1)/2}\ . \end{aligned}$$

Pro důkaz veleidentity stačí nalézt A_0 a A_1.

Substituce $x \mapsto x^3$ a $a \mapsto x$ dává na levé straně poslední rovnosti

$$\begin{aligned} F(x,b,x^3) &= \prod_{n=1}^{\infty}(1-x^{3n})\cdot\prod_{n=1}^{\infty}(1-x^n)(1-bx^{n-1})(1-b^{-1}x^n) \\ &= \prod_{n=1}^{\infty}(1-x^{3n})\sum_{i=0}^{\infty}(-1)^i(b^{-i}-b^{i+1})x^{i(i+1)/2}\ , \end{aligned}$$

přičemž poslední úprava, podobná lemmatu 219, plyne z JTI (substitucí $x \mapsto x^2$ a $b \mapsto -bx$). Vpravo dostaneme

$$\begin{aligned} &A_0(b,x^3)\sum_{i=0}^{\infty}(-1)^i(x^{3i(3i+1)/2}-x^{(3i+2)(3i+3)/2}) \\ &+ xA_1(b,x^3)\sum_{j=-\infty}^{\infty}(-1)^j(x^{3j(3j-1)/2}-x^{(3j+2)(3j+1)/2})\ . \end{aligned}$$

Není těžké se přesvědčit, že obě sumy se rovnají sumě

$$1+\sum_{i=1}^{\infty}(-1)^i(x^{3i(3i-1)/2}+x^{3i(3i+1)/2}) = \sum_{j=-\infty}^{\infty}(-1)^j x^{3j(3j-1)/2}\ ,$$

která se ovšem podle 1 věty 215 rovná $\prod_{n\ge1}(1-x^{3n})$. Zkrácením tohoto společného faktoru dostaneme rovnost

$$\sum_{i=0}^{\infty}(-1)^i(b^{-i}-b^{i+1})x^{i(i+1)/2}=A_0(b,x^3)+xA_1(b,x^3)\ .$$

Nyní už porovnání koeficientů u mocnin x na obou stranách dává

$$\begin{aligned}A_0(b,x) &= \sum_{j=-\infty}^{\infty}(-1)^j(b^{-3j}-b^{3j+1})x^{j(3j+1)/2}\\ A_1(b,x) &= \sum_{i=0}^{\infty}(-1)^i(b^{3i+2}-b^{-3i-1})x^{3i(i+1)/2}\ ,\end{aligned}$$

čímž je veleidentita dokázána.

V $F(a,b,x)$ máme faktor $1-b$ a $b=1$ je jednoduchou nulou obou stran. Veleidentitu zderivujeme podle b a položíme $b=1$. Dostaneme

$$\begin{aligned}&\prod_{n=1}^{\infty}(1-ax^{n-1})^3(1-a^{-1}x^n)^3(1-x^n)^4\\ &=\sum_{j=-\infty}^{\infty}(-1)^j(6j+1)x^{j(3j+1)/2}\sum_{i=0}^{\infty}(-1)^i(a^{-3i}-a^{3i+3})x^{3i(i+1)/2}\\ &\quad-3\sum_{i=0}^{\infty}(-1)^i(2i+1)x^{3i(i+1)/2}\sum_{j=-\infty}^{\infty}(-1)^j(a^{-3j+1}-a^{3j+2})x^{j(3j+1)/2}\ .\end{aligned}$$

Nyní je $a=1$ trojnásobnou nulou obou stran. Poslední identitu třikrát zderivujeme podle a a položíme $a=1$. Dostaneme dokazovanou identitu. $\diamondsuit$

Připomínáme, že pro mocninnou řadu f označuje $[x^n]f$ koeficient u x^n. Pro dvě mocninné řady $f,g\in\mathbf{Z}[[x]]$ a $m\in\mathbf{N}$ značení $f\equiv g \bmod m$ znamená, že $[x^n]f\equiv[x^n]g \bmod m$ pro každé $n\in\mathbf{N}_0$.

Lemma 223. *Pro každé prvočíslo p platí kongruence mezi mocninnými řadami*

$$\frac{1}{(1-x)^p}\equiv\frac{1}{1-x^p}\bmod p\ .$$

DŮKAZ. Podle binomické věty $(1-x)^p=1-x^p-h(x)$, kde $h(x)$ má všechny koeficienty dělitelné p. Tedy $1/(1-x)^p=1+(x^p+h(x))+(x^p+h(x))^2+\cdots\equiv 1+x^p+x^{2p}+\cdots \bmod p$. $\diamondsuit$

Věta 224 (Ramanujan, 1919). *Pro každé $m \in \mathbf{N}_0$ platí kongruence*

$$\begin{aligned} p(5m+4) &\equiv 0 \bmod 5 \\ p(7m+5) &\equiv 0 \bmod 7 \\ p(11m+6) &\equiv 0 \bmod 11 \ . \end{aligned}$$

Důkaz. 1. Dokážeme kongruenci $p(5m+4) \equiv 0 \bmod 5$. Podle 1 věty 215 a tvrzení 220 máme

$$x \prod_{n=1}^{\infty} (1-x^n)^4 = x \prod_{n=1}^{\infty} (1-x^n) \cdot \prod_{n=1}^{\infty} (1-x^n)^3 = \sum_{r=-\infty}^{\infty} \sum_{s=0}^{\infty} (-1)^{r+s}(2s+1)x^k \ ,$$

kde $k = k(r,s) = 1 + r(3r+1)/2 + s(s+1)/2$. Protože

$$8k \equiv 8k - 10r^2 - 5 = 2(r+1)^2 + (2s+1)^2 \bmod 5 \ ,$$

z $k \equiv 0 \bmod 5$ plyne $2(r+1)^2 + (2s+1)^2 \equiv 0 \bmod 5$. Čtverce modulo 5 jsou 0 a ± 1, a tak $k \equiv 0 \bmod 5$ implikuje $2s+1 \equiv 0 \bmod 5$. Tedy

$$[x^{5m}] \ x \prod_{n=1}^{\infty} (1-x^n)^4 \equiv 0 \bmod 5$$

pro každé $m \in \mathbf{N}_0$. Podle lemmatu 223

$$\frac{1-x^{5n}}{(1-x^n)^5} \equiv 1 + 0x + 0x^2 + \cdots = 1 \bmod 5$$

pro každé $n \in \mathbf{N}_0$, a tak

$$[x^{5m}] \ x \prod_{n=1}^{\infty} \frac{1-x^{5n}}{1-x^n} = [x^{5m}] \ x \prod_{n=1}^{\infty} (1-x^n)^4 \cdot \prod_{n=1}^{\infty} \frac{1-x^{5n}}{(1-x^n)^5} \equiv 0 \bmod 5$$

pro každé $m \in \mathbf{N}_0$. Tudíž

$$\begin{aligned} p(5m+4) &= [x^{5m+5}] \ \frac{x}{(1-x)(1-x^2)(1-x^3)\ldots} \\ &= [x^{5m+5}] \ x \prod_{n=1}^{\infty} \frac{1-x^{5n}}{1-x^n} \cdot \prod_{n=1}^{\infty} (1 + x^{5n} + x^{10n} + \cdots) \\ &\equiv 0 \bmod 5 \ . \end{aligned}$$

2. Dokážeme kongruenci $p(7m+5) \equiv 0 \bmod 7$. Umocněním identity tvrzení 220 na druhou máme

$$x^2 \prod_{n=1}^{\infty} (1-x^n)^6 = \sum_{r,s=0}^{\infty} (-1)^{r+s} (2r+1)(2s+1) x^k \ ,$$

kde $k = k(r,s) = 2 + r(r+1)/2 + s(s+1)/2$. Protože

$$k = 2 + r(r+1)/2 + s(s+1)/2 \equiv (2r+1)^2 + (2s+1)^2 \bmod 7 \ ,$$

$k \equiv 0 \bmod 7$ implikuje $(2r+1)^2 + (2s+1)^2 \equiv 0 \bmod 7$. To implikuje $2r+1$ i $2s+1$ dělitelné 7, protože čtverce modulo 7 jsou $0, 1, 2$ a -3. Tedy

$$[x^{7m}] \ x^2 \prod_{n=1}^{\infty} (1-x^n)^6 \equiv 0 \bmod 7$$

pro každé $m \in \mathbf{N}_0$. Dále důkaz postupuje analogicky modulu 5.

3. **(Winquist, 1969).** Dokážeme kongruenci $p(11m+6) \equiv 0 \bmod 11$. Podle tvrzení 222

$$\begin{aligned} & x^5 \prod_{n=1}^{\infty} (1-x^n)^{10} \\ & = \sum_{r=0}^{\infty} \sum_{s=-\infty}^{\infty} (-1)^{r+s} (2r+1)(6s+1) \frac{(3r+1)(3r+2) - 3s(3s+1)}{2} \cdot x^k \ , \end{aligned}$$

kde $k = k(r,s) = 3r(r+1)/2 + s(3s+1)/2 + 5$. Protože

$$k = 3r(r+1)/2 + s(3s+1)/2 + 5 \equiv 2(5(2r+1)^2 + 3(6s+1)^2) \bmod 11 \ ,$$

$k \equiv 0 \bmod 11$ implikuje $5(2r+1)^2 + 3(6s+1)^2 \equiv 0 \bmod 11$. Zbytky $5x^2$ i $3x^2$ modulo 11 jsou $0, 1, -2, 3, 4$ a 5, a tak $k \equiv 0 \bmod 11$ implikuje $2r+1$ i $6s+1$ dělitelné 11. Tedy

$$[x^{11m}] \ x^5 \prod_{n=1}^{\infty} (1-x^n)^{10} \equiv 0 \bmod 11$$

pro každé $m \in \mathbf{N}_0$. Dále důkaz postupuje analogicky modulu 5. $\diamondsuit$

7.2 Součty dvou a čtyř čtverců

Pro $g \in \mathbf{N}$ a $n \in \mathbf{N}_0$ definujeme $r_g(n)$ jako počet celočíselných řešení $x_i \in \mathbf{Z}$ rovnice

$$x_1^2 + x_2^2 + \cdots + x_g^2 = n \ .$$

Aritmetická funkce $r_g : \mathbf{N}_0 \to \mathbf{N}_0$ tedy udává počet vyjádření čísla n jako součtu g čtverců, přičemž vyjádření lišící se znaménky nebo pořadím bereme jako různá. Ve větách 225 a 226 odvodíme přesné formule pro hodnoty $r_2(n)$ a $r_4(n)$.

Věta 225 (Gauss, 1801; Jacobi, 1829). *Nechť $d_i(n)$ je počet těch dělitelů d čísla $n \in \mathbf{N}$, že $d \equiv i \bmod 4$. Pak pro každé $n \in \mathbf{N}$ platí*

$$r_2(n) = 4(d_1(n) - d_3(n)) \ .$$

DŮKAZ. **(Hirschhorn, 1985).** Pravou stranu identity lemmatu 219 rozdělíme podle parity n na dvě sumy a ty nahradíme součiny podle JTI ($x \mapsto x^2$ a $z \mapsto x^{\pm 1} z^4$):

$$\sum_{n=-\infty}^{\infty} x^{(2n^2+n)} z^{4n+1} - \sum_{n=-\infty}^{\infty} x^{(2n^2-n)} z^{4n-1} = z \prod_{n=1}^{\infty} P_n(1,3) - z^{-1} \prod_{n=1}^{\infty} P_n(3,1) \ ,$$

kde $P_n(a,b) = (1 - x^{4n})(1 + x^{4n-a} z^4)(1 + x^{4n-b} z^{-4})$. Poslední rozdíl zderivujeme podle z, položíme $z = 1$, výsledek vydělíme dvěma a po úpravách dostaneme

$$\prod_{n=1}^{\infty} Q_n \cdot \left(1 - 4 \sum_{n \ge 1} \left(\frac{x^{4n-3}}{1 + x^{4n-3}} - \frac{x^{4n-1}}{1 + x^{4n-1}}\right)\right) \ ,$$

kde $Q_n = (1 - x^{4n})(1 + x^{4n-3})(1 + x^{4n-1})$; nekonečné součiny jsme zderivovali podle pravidla $(\prod_{n \ge 1} u_n)' = (\prod_{n \ge 1} u_n) \cdot \sum_{n \ge 1} \frac{u_n'}{u_n}$. Na levé straně identity lemmatu 219 dostaneme (jak už víme z tvrzení 220) $\prod_{n \ge 1}(1 - x^n)^3$. Celkem máme rovnost

$$\prod_{n=1}^{\infty} (1 - x^n)^3 = \prod_{n=1}^{\infty} Q_n \cdot \left(1 - 4 \sum_{n \ge 1} \left(\frac{x^{4n-3}}{1 + x^{4n-3}} - \frac{x^{4n-1}}{1 + x^{4n-1}}\right)\right) \ .$$

Tu vydělíme identitou

$$\begin{aligned}
\prod_{n=1}^{\infty}(1+x^n)^2(1-x^n) &= \prod_{n=1}^{\infty}(1+x^n)(1-x^{2n}) \\
&= \prod_{n=1}^{\infty}(1+x^{2n-1})(1+x^{2n})(1-x^{2n}) \\
&= \prod_{n=1}^{\infty}(1+x^{2n-1})(1-x^{4n}) \\
&= \prod_{n=1}^{\infty} Q_n
\end{aligned}$$

a dostaneme

$$\prod_{n=1}^{\infty}\left(\frac{1-x^n}{1+x^n}\right)^2 = 1-4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right).$$

Podle tvrzení 217 máme

$$\left(\sum_{n=-\infty}^{\infty}(-1)^n x^{n^2}\right)^2 = 1-4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right).$$

Substituce $x \mapsto -x$ dává

$$\left(\sum_{n=-\infty}^{\infty} x^{n^2}\right)^2 = 1+4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1-x^{4n-3}}-\frac{x^{4n-1}}{1-x^{4n-1}}\right).$$

Pro $r \in \mathbf{N}_0$ je koeficient u x^r vlevo $r_2(r)$. Koeficient u x^r, $r \geq 1$, vpravo je $4(d_1(r)-d_3(r))$, protože koeficient u x^r v

$$\sum_{n\geq 1}\frac{x^{an+b}}{1-x^{an+b}} = \sum_{n,m\geq 1} x^{m(an+b)}$$

je počet dělitelů d čísla r tvaru $d = an+b$, $n \in \mathbf{N}$. Tím je identita $r_2(n) = 4(d_1(n)-d_3(n))$ dokázána. $\diamondsuit$

Bezprostředním důsledkem předchozí věty je, že pro každé prvočíslo $p \equiv 1 \bmod 4$ máme $r_2(p) = 4(d_1(p)-d_3(p)) = 8 > 0$. Jiným způsobem jsme tak dokázali větu 20 z 2. kapitoly. Navíc vidíme, že při ignorování znamének a pořadí je vyjádření prvočísla p součtem dvou čtverců jednoznačné.

Věta 226 (Jacobi, 1829). *Pro každé $n \in \mathbf{N}$ platí*

$$r_4(n) = 8 \sum_{d \backslash n}{}' \; d \;,$$

kde čárka označuje vynechání dělitelů, které jsou násobky čtyř.

DŮKAZ. **(Hirschhorn, 1987).** Sumu na pravé straně identity tvrzení 221 rozdělíme na

$$\begin{aligned}
&\frac{1}{2}\Bigg(\sum_{s=-\infty}^{\infty} x^{s^2} \sum_{r=-\infty}^{\infty} (2r+1)^2 x^{r^2+r} - \sum_{r=-\infty}^{\infty} x^{r^2+r} \sum_{s=-\infty}^{\infty} (2s)^2 x^{s^2} \Bigg) \\
&= \frac{1}{2}\Bigg(\sum_{s=-\infty}^{\infty} x^{s^2} \cdot \left(1 + 4x\frac{d}{dx}\right) \sum_{r=-\infty}^{\infty} x^{r^2+r} - \sum_{r=-\infty}^{\infty} x^{r^2+r} \cdot 4x\frac{d}{dx} \sum_{s=-\infty}^{\infty} x^{s^2} \Bigg)
\end{aligned}$$

a všechny čtyři sumy nahradíme součiny podle JTI ($z \mapsto 1$ a $z \mapsto x$):

$$\begin{aligned}
&\frac{1}{2}\Bigg(\prod_{n=1}^{\infty} (1+x^{2n-1})^2(1-x^{2n}) \cdot \left(1 + 4x\frac{d}{dx}\right) 2 \prod_{n=1}^{\infty} (1+x^{2n})^2(1-x^{2n}) \\
&\qquad - 2 \prod_{n=1}^{\infty} (1+x^{2n})^2(1-x^{2n}) \cdot 4x\frac{d}{dx} \prod_{n=1}^{\infty} (1+x^{2n-1})^2(1-x^{2n}) \Bigg) .
\end{aligned}$$

Nekonečné součiny zderivujeme podle pravidla $(\prod_{n\geq 1} u_n)' = (\prod_{n\geq 1} u_n) \cdot \sum_{n\geq 1} \frac{u_n'}{u_n}$ a po úpravách obdržíme identitu

$$\prod_{n=1}^{\infty} (1-x^n)^6 \;=\; \prod_{n=1}^{\infty} Q_n \cdot \left(1 - 8 \sum_{n\geq 1} \left(\frac{(2n-1)x^{2n-1}}{1+x^{2n-1}} - \frac{2nx^{2n}}{1+x^{2n}} \right) \right) ,$$

kde $Q_n = (1+x^{2n-1})^2(1+x^{2n})^2(1-x^{2n})^2$. Obě strany vydělíme identitou

$$\begin{aligned}
\prod_{n=1}^{\infty} (1+x^n)^4(1-x^n)^2 \;&=\; \prod_{n=1}^{\infty} (1+x^n)^2(1-x^{2n})^2 \\
&=\; \prod_{n=1}^{\infty} Q_n
\end{aligned}$$

a dostaneme

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

Podle tvrzení 217 máme

$$\Big(\sum_{n=-\infty}^{\infty}(-1)^n x^{n^2}\Big)^4 = 1 - 8\sum_{n\geq 1}\Big(\frac{(2n-1)x^{2n-1}}{1+x^{2n-1}} - \frac{2nx^{2n}}{1+x^{2n}}\Big)\ .$$

Substitucí $x \mapsto -x$ se zbavíme faktoru $(-1)^n$ vlevo a pravá strana přejde na

$$\begin{aligned}
&1 + 8\sum_{n\geq 1}\Big(\frac{(2n-1)x^{2n-1}}{1-x^{2n-1}} + \frac{2nx^{2n}}{1+x^{2n}}\Big)\\
&= 1 + 8\sum_{n\geq 1}\Big(\frac{(2n-1)x^{2n-1}}{1-x^{2n-1}} + \frac{2nx^{2n}}{1-x^{2n}}\Big) - 8\sum_{n\geq 1}\Big(\frac{2nx^{2n}}{1-x^{2n}} - \frac{2nx^{2n}}{1+x^{2n}}\Big)\\
&= 1 + 8\sum_{n\geq 1}\frac{nx^n}{1-x^n} - 8\sum_{n\geq 1}\frac{4nx^{4n}}{1-x^{4n}}\ .
\end{aligned}$$

Takže

$$\Big(\sum_{n=-\infty}^{\infty} x^{n^2}\Big)^4 = 1 + 8{\sum_{n\geq 1}}'\ \frac{nx^n}{1-x^n}\ ,$$

kde čárka označuje vynechání n dělitelných čtyřmi. Pro $r \in \mathbf{N}_0$ je koeficient u x^r vlevo $r_4(r)$. Koeficient u x^r, $r \geq 1$, vpravo je $8\sum'_{d\backslash r} d$, protože

$${\sum_{n\geq 1}}'\ \frac{nx^n}{1-x^n} = {\sum_{n,m\geq 1}}'\ nx^{nm}\ .$$

Tím je věta dokázána. $\diamondsuit$

Každé $n \in \mathbf{N}$ má alespoň jednoho dělitele, který není násobkem čtyř, totiž číslo 1. Poslední věta tak dává $r_4(n) \geq 8 > 0$ pro každé $n \in \mathbf{N}$. Dostáváme třetí důkaz věty 55 z 3. kapitoly.

7.3 Další rozkladové identity

Věta 227 (Rogers, 1894; Ramanujan, 1916; Schur, 1917). *Platí následující identity.*

$$\begin{aligned}
\prod_{n=1}^{\infty}\frac{1}{(1-x^{5n-1})(1-x^{5n-4})} &= \sum_{m\geq 0}\frac{x^{m^2}}{(1-x)(1-x^2)\dots(1-x^m)}\\
\prod_{n=1}^{\infty}\frac{1}{(1-x^{5n-2})(1-x^{5n-3})} &= \sum_{m\geq 0}\frac{x^{m(m+1)}}{(1-x)(1-x^2)\dots(1-x^m)}\ .
\end{aligned}$$

První identita praví, že počet rozkladů čísla n na části kongruentní 1 nebo 4 modulo 5 je týž jako počet rozkladů na části lišící se vzájemně alespoň o 2. Druhá identita praví, že počet rozkladů čísla n na části kongruentní 2 nebo 3 modulo 5 je týž jako počet rozkladů na části větší než 1 a lišící se vzájemně alespoň o 2.

Koeficient u x^n na levé straně první identity je zjevně roven počtu rozkladů n na části $\equiv 1, 4 \bmod 5$. Koeficient u x^n na pravé straně je roven počtu celočíselných řešení rovnice

$$m^2 + x_1 + 2x_2 + \cdots + mx_m = n \quad m, x_i \geq 0 \ ,$$

která je ekvivalentní rovnici

$$(1 + x_m) + (3 + x_{m-1} + x_m) + \cdots + ((2m-1) + x_1 + x_2 + \cdots + x_m) = n \ .$$

Sčítance vlevo dávají přesně všechny rozklady n na části s rozdíly alespoň 2. Podobně odvodíme rozkladové vyjádření druhé identity pomocí rozvoje $m(m+1) = 2 + 4 + \cdots + 2m$. Zbývá však obě identity dokázat.

Důkaz věty 227. Položíme $P_0 = 1$ a pro $r \in \mathbf{N}$

$$P_r = \prod_{s=1}^{r} \frac{1}{1 - x^s} \quad \text{a} \quad Q_r = Q_r(a) = \prod_{s=r}^{\infty} \frac{1}{1 - ax^s} \ .$$

Dále nechť $\lambda(r) = r(5r+1)/2$. Pro $m = 0, 1, 2$ položíme

$$H_m = H_m(a) = \sum_{r=0}^{\infty} (-1)^r a^{2r} x^{\lambda(r) - mr} (1 - a^m x^{2mr}) P_r Q_r \ .$$

Naším cílem je rozvinout H_1 a H_2 do mocninné řady v a. Protože

$$(1 - ax^r) Q_r = Q_{r+1} \ , \ (1 - x^r) P_r = P_{r-1}$$

a

$$H_m - H_{m-1} = \sum_{r=0}^{\infty} (-1)^r a^{2r} x^{\lambda(r)} C_{mr} P_r Q_r \ ,$$

kde

$$C_{mr} = a^{m-1} x^{r(m-1)} (1 - ax^r) + x^{-mr} (1 - x^r) \ ,$$

máme

$$H_m - H_{m-1} = \sum_{r=0}^{\infty}(-1)^r a^{2r+m-1} x^{\lambda(r)+r(m-1)} P_r Q_{r+1} + \sum_{r=1}^{\infty}(-1)^r a^{2r} x^{\lambda(r)-mr} P_{r-1} Q_r \ .$$

Ve druhé sumě r nahradíme $r+1$ a dostaneme

$$H_m - H_{m-1} = \sum_{r=0}^{\infty}(-1)^r D_{mr} P_r Q_{r+1} \ ,$$

kde

$$D_{mr} = a^{2r+m-1} x^{\lambda(r)+r(m-1)} (1 - a^{3-m} x^{(2r+1)(3-m)}) \ .$$

S použitím operátoru $\eta f(a) = f(ax)$ máme $\eta Q_r = Q_{r+1}$ a

$$D_{mr} = a^{m-1} \eta \Big(a^{2r} x^{\lambda(r)-r(3-m)} (1 - a^{3-m} x^{2r(3-m)}) \Big) \ ,$$

a tak

$$H_m - H_{m-1} = a^{m-1} \eta H_{3-m} \ .$$

Položíme-li v poslední identitě $m = 1, 2$ a využijeme-li $H_0 = 0$, máme $H_1 = \eta H_2$ a

$$H_2 = H_1 + a\eta H_1 = \eta H_2 + a\eta^2 H_2 \ .$$

Pro hledaný rozvoj $H_2 = \sum_{s \geq 0} c_s a^s$ $(c_0 = 1)$ poslední transformace dává rovnici

$$\sum_{s \geq 0} c_s a^s = \sum_{s \geq 0} c_s x^s a^s + \sum_{s \geq 0} c_s x^{2s} a^{s+1} \ .$$

Porovnáním koeficientů u a^s dostáváme

$$c_1 = \frac{1}{1-x} \quad \text{a} \quad c_s = \frac{x^{2s-2} c_{s-1}}{1-x^s} = \frac{x^{2+4+\cdots+2(s-1)}}{(1-x)(1-x^2)\ldots(1-x^s)} = x^{s(s-1)} P_s \ .$$

Dostali jsme rozvoj

$$H_2(a) = \sum_{s \geq 0} a^s x^{s(s-1)} P_s \ .$$

Takže $H_2(x)$ je suma na pravé straně první dokazované identity. Z druhé strany, v definici $H_2(a)$ položíme $a = x$ a dostaneme ($P_\infty = P_r \cdot Q_r(x)$)

$$\begin{aligned} H_2(x) &= P_\infty \cdot \sum_{r\geq 0} (-1)^r x^{\lambda(r)} (1 - x^{2(2r+1)}) \\ &= P_\infty \cdot \Big(\sum_{r\geq 0} (-1)^r x^{\lambda(r)} + \sum_{r\geq 1} (-1)^r x^{\lambda(r-1)+2(2r-1)}) \Big) \\ &= P_\infty \cdot \Big(1 + \sum_{r\geq 1} (-1)^r (x^{r(5r+1)/2} + x^{r(5r-1)/2}) \Big) \ . \end{aligned}$$

Pomocí tvrzení 218 dostáváme

$$\begin{aligned} H_2(x) &= P_\infty \cdot \prod_{n=1}^{\infty} (1 - x^{5n-2})(1 - x^{5n-3})(1 - x^{5n}) \\ &= \prod_{n=1}^{\infty} \frac{1}{(1 - x^{5n-1})(1 - x^{5n-4})} \ . \end{aligned}$$

Tím je první identita dokázána.

$H_1(x)$ je suma na pravé strané druhé dokazované identity, protože (podle transformace η a hořejšího rozvoje $H_2(a)$)

$$H_1(a) = \eta H_2(a) = H_2(ax) = \sum_{s\geq 0} a^s x^{s^2} P_s \ .$$

V definici $H_1(a)$ nyní položíme $a = x$ a důkaz dokončíme pomocí tvrzení 218 stejným způsobem. $\diamondsuit$

Ve zbytku tohoto oddílu dvěma způsoby rozvineme "pramáti" rozkladových identit z věty 213. Nejprve uvedeme jedno její pozoruhodné zjemnění. *Divácký rozklad* (lecture hall partition) délky $k \in \mathbf{N}$ je rozklad $(\lambda_1, \lambda_2, \ldots, \lambda_k)$, jehož části se mohou rovnat i nule a splňují nerovnosti

$$\frac{\lambda_1}{k} \geq \frac{\lambda_2}{k-1} \geq \frac{\lambda_3}{k-2} \geq \ldots \geq \frac{\lambda_k}{1} \geq 0 \ .$$

Proč zrovna "divácký"? Mají-li sedačky na stupních amfiteátru postaveného v prvním kvadrantu roviny souřadnice $(1, \lambda_k), (2, \lambda_{k-1}), \ldots, (k, \lambda_1)$, $\lambda_i \in \mathbf{N}_0$, je z každé z nich vidět do počátku, právě když $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ tvoří divácký rozklad.

Věta 228 (Bousquet-Mélou a Eriksson, 1997). *Nechť $k \in \mathbf{N}$. Každé $n \in \mathbf{N}$ má tolik diváckých rozkladů délky k jako rozkladů na liché části menší než $2k$. Řečeno generujícími funkcemi, označuje-li L_k množinu diváckých rozkladů délky k,*

$$\sum_{\lambda \in L_k} x^{|\lambda|} = \frac{1}{(1-x)(1-x^3)(1-x^5)\dots(1-x^{2k-1})} \; .$$

Například číslo 10 má sedm diváckých rozkladů délky 3,

$$(10,0,0),\ (9,1,0),\ (8,2,0),\ (7,3,0),\ (6,4,0),\ (7,2,1)\ \text{ a }\ (6,3,1),$$

a rovněž sedm rozkladů na liché části menší než 6,

$$5^2,\ 531^2,\ 51^5,\ 3^31,\ 3^21^4,\ 31^7\ \text{ a }\ 1^{10}\; .$$

Pro každý rozklad $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ s různými částmi existuje k, $k \geq r$, tak, že $(\lambda_1, \lambda_2, \dots, \lambda_r, 0, 0, \dots, 0)$ (na konci je $k-r$ nul) je divácký rozklad délky k. Pro pevné n tak z věty 228 sumací přes všechna k plyne, že n má tolik rozkladů na různé části jako rozkladů na liché části. Věta 228 představuje zjemnění (či snad "zkonečnění") věty 213.

Namísto věty 228 dokážeme o něco obecnější a jemnější výsledek. Pro číslo $m \in \mathbf{N}$, $m \geq 2$, definujeme posloupnost $a(m) = (a_0, a_1, a_2, \dots)$ jako $a_0 = 0$, $a_1 = 1$ a pro $i \geq 2$ rekurencí

$$a_i = m a_{i-1} - a_{i-2}\; .$$

Například $a(2) = (0, 1, 2, 3, 4, \dots)$.

Lemma 229. *Nechť $m \in \mathbf{N}$ a $a(m) = (a_0, a_1, a_2, \dots)$. Pak pro každé $i \geq 1$ a $v \in \mathbf{N}_0$ platí*

$$\left\lfloor \frac{a_{i-1}v}{a_i} \right\rfloor + \left\lceil \frac{a_{i+1}v}{a_i} \right\rceil = mv\; .$$

DŮKAZ. Pro $i = 1$ to platí a pro $i \geq 2$ podle definice posloupnosti $a(m)$ máme $\lfloor a_{i-1}v/a_i \rfloor + \lceil a_{i+1}v/a_i \rceil = \lfloor a_{i-1}v/a_i \rfloor + \lceil mv - a_{i-1}v/a_i \rceil = \lfloor a_{i-1}v/a_i \rfloor + mv + \lceil -a_{i-1}v/a_i \rceil = mv$. $\diamondsuit$

Pro rozklad $\lambda = (\lambda_1, \lambda_2, \dots)$ (nulové části jsou povoleny) položíme $\lambda^l = (\lambda_1, \lambda_3, \lambda_5, \dots)$ a $\lambda^s = (\lambda_2, \lambda_4, \lambda_6, \dots)$. Pro $m \geq 2$ jako L_k^m označíme množinu všech rozkladů s k nezápornými částmi λ_i, které pro $1 \leq i < k$ splňují

$$\lambda_i \geq \frac{a_{k-i+1}}{a_{k-i}} \lambda_{i-1}\; ,$$

přičemž a_i jsou členy posloupnosti $a(m)$. Patrně $L_k^2 = L_k$, kde L_k je množina diváckých rozkladů délky k. Věta 228 je speciálním případem $m = 2$ a $x = y$ následujícího tvrzení. (Pro jeho další použití viz úloha 12.)

Tvrzení 230 (zobecnění a zjemnění věty 228). *Nechť $m \geq 2$ a $k \geq 1$ jsou celá čísla a $a(m) = (a_0, a_1, a_2, \ldots)$. Pak*

$$\sum_{\lambda \in L_k^m} x^{|\lambda^l|} y^{|\lambda^s|} = \prod_{i=1}^{k} \frac{1}{1 - x^{a_i} y^{a_{i-1}}} \ .$$

Důkaz. Pro $k \in \mathbf{N}$ označíme

$$G_k^m(x, y) = \sum_{\lambda \in L_k^m} x^{|\lambda^l|} y^{|\lambda^s|} \ .$$

Patrně $G_1^m(x, y) = 1/(1 - x)$. Pro $k \geq 1$ dokážememe rekurenci

$$G_{k+1}^m(x, y) = \frac{G_k^m(x^m y, x^{-1})}{1 - x} \ .$$

Odtud a z definice čísel a_i už indukcí podle k plyne dokazovaný součinový tvar.

Pro $i \in \mathbf{N}_0$ definujeme

$$L_{k,i}^m = \{\lambda \in L_k^m : \ \lambda_1 - \lceil a_k \lambda_2 / a_{k-1} \rceil = i\} \ .$$

Patrně $\bigcup_{i \geq 0} L_{k,i}^m = L_k^m$. Zmenšení první části o i dává bijekci mezi $L_{k,i}^m$ a $L_{k,0}^m$, která zmenšuje $|\lambda^l|$ o i a nemění $|\lambda^s|$. Pro důkaz rekurence proto stačí sestrojit takovou bijekci $\phi : L_k^m \to L_{k+1,0}^m$, $\lambda \mapsto \gamma$, že vždy platí $|\gamma^s| = |\lambda^l|$ a $|\gamma^l| = m|\lambda^l| - |\lambda^s|$. Zobrazení ϕ definujeme předpisem $(1 \leq i \leq k + 1)$

$$\gamma_i = \begin{cases} \lceil a_{k+1} \lambda_1 / a_k \rceil & \text{pokud } i = 1 \\ \lambda_{i-1} & \text{pokud } i \text{ je sudé} \\ \lceil a_{k-2j+1} \lambda_{2j+1} / a_{k-2j} \rceil & \\ +\lfloor a_{k+1-2j} \lambda_{2j-1} / a_{k+2-2j} \rfloor - \lambda_{2j} & \text{pokud } i = 2j + 1 \geq 3 \ . \end{cases}$$

Z definice a přechozího lemmatu plyne, že $|\gamma^s|$ a $|\gamma^l|$ závisí na $|\lambda^s|$ a $|\lambda^l|$ tak, jak je požadováno. Ukážeme, že $\gamma \in L_{k+1,0}^m$. Nerovnost $\gamma_i \geq \lceil \frac{a_{k+2-i} \gamma_{i+1}}{a_{k+1-i}} \rceil$ je pro $i = 1$ podle definice splněna s rovností. Protože $\lambda_{2j} \geq \frac{a_{k+1-2j}}{a_{k-2j}} \lambda_{2j+1}$, máme $\lceil \frac{a_{k+1-2j} \lambda_{2j+1}}{a_{k-2j}} \rceil - \lambda_{2j} \leq 0$ a podle definice γ_{2j+1}

$$\gamma_{2j+1} \leq a_{k-2j+1} \lambda_{2j-1} / a_{k+2-2j} = a_{k-2j+1} \gamma_{2j} / a_{k+2-2j} \ ,$$

z čehož plyne požadovaná nerovnost pro $i = 2j$. Protože $\lambda_{2j-1} \geq \frac{a_{k+2-2j}\lambda_{2j}}{a_{k+1-2j}}$, máme $\lfloor \frac{a_{k+1-2j}\lambda_{2j-1}}{a_{k+2-2j}} \rfloor - \lambda_{2j} \geq 0$ a podle definice γ_{2j+1}

$$\gamma_{2j+1} \geq a_{k-2j+1}\lambda_{2j+1}/a_{k-2j} = a_{k-2j+1}\gamma_{2j+2}/a_{k-2j}\ ,$$

což je požadovaná nerovnost pro $i = 2j + 1$. Tedy $\phi(\lambda) \in L^m_{k+1,0}$. Inverzní zobrazení $\psi : L^m_{k+1,0} \to L^m_k$, $\gamma \mapsto \lambda$, definujeme předpisem $(1 \leq i \leq k)$

$$\lambda_i = \begin{cases} \gamma_{i+1} & \text{pokud } i \text{ je liché} \\ \lceil a_{k-2j+1}\gamma_{2j+2}/a_{k-2j} \rceil & \\ +\lfloor a_{k+1-2j}\gamma_{2j}/a_{k+2-2j} \rfloor - \gamma_{2j+1} & \text{pokud } i = 2j\ . \end{cases}$$

Podobným způsobem jako před chvílí ověříme, že $\psi(\gamma) \in L^m_k$. Nechť $\lambda \in L^m_k$, $\phi(\lambda) = \gamma$ a $\psi(\gamma) = \mu$. Podle definice ϕ a ψ máme $\mu_{2j+1} = \gamma_{2j+2} = \lambda_{2j+1}$ a $\mu_{2j} = \lceil \frac{a_{k-2j+1}\gamma_{2j+2}}{a_{k-2j}} \rceil + \lfloor \frac{a_{k+1-2j}\gamma_{2j}}{a_{k+2-2j}} \rfloor - \gamma_{2j+1} = \lceil \frac{a_{k-2j+1}\lambda_{2j+1}}{a_{k-2j}} \rceil + \lfloor \frac{a_{k+1-2j}\lambda_{2j-1}}{a_{k+2-2j}} \rfloor - \gamma_{2j+1} = \lambda_{2j}$. Zobrazení $\psi \circ \phi$ je identické. Podobně se ukáže identičnost $\phi \circ \psi$. Takže ϕ je bijekce. $\diamondsuit$

Druhé zobecnění věty 213 predstavuje věta 232, která ji obsahuje jako jeden z mnoha speciálních případů. Nejprve dokážeme princip involuce. Nechť $A = A^+ \cup A^-$ je rozklad množiny A. Řekneme, že zobrazení $\alpha : A \to A$ *mění znaménko*, když pro $a \in A$, $a \neq \alpha(a)$, máme $a \in A^+ \iff \alpha(a) \in A^-$ a pro $a \in A$, $a = \alpha(a)$, máme $a \in A^+$. Nechť $f : A \to B$ a $B = B^+ \cup B^-$ je též rozklad. Řekneme, že zobrazení f *zachovává znaménko*, když $f(A^+) \subset B^+$ a $f(A^-) \subset B^-$. Pro $\alpha : A \to A$ symbolem F_α označíme množinu pevných bodů α:

$$F_\alpha = \{a \in A :\ \alpha(a) = a\}\ .$$

Tvrzení 231 (princip involuce). *Nechť A a B jsou konečné množiny, $A = A^+ \cup A^-$ a $B = B^+ \cup B^-$ jsou rozklady, $\alpha : A \to A$ a $\beta : B \to B$ jsou znaménko měnící bijekce a $f : A \to B$ je znaménko zachovávající bijekce. Potom $|F_\alpha| = |F_\beta|$.*

DŮKAZ. Z vlastností α a β plyne, že $|A^-| + |F_\alpha| = |A^+|$ a $|B^-| + |F_\beta| = |B^+|$. Z vlastností f plyne, že $|A^-| = |B^-|$ a $|A^+| = |B^+|$. Tedy $|F_\alpha| = |F_\beta|$. $\diamondsuit$

Zobrazení α a β jsou podle předpokladů takové permutace množin A a B, které kromě pevných bodů nemají žádné cykly liché délky. Tvrzení svůj název dostalo proto, že v konkrétních aplikacích jsou α a β obvykle involuce —

permutace s cykly délek pouze 1 a 2. Rozklad $A = A^+ \cup A^-$ se často definuje zřejmým způsobem pomocí *znaménkové funkce* $s : A \to \{+1, -1\}$. Bijekci mezi F_α a F_β lze konkrétně definovat z bijekcí α, β a f, viz úloha 13.

Multimnožina je dvojice $A = (A', \nu) = (A', \nu_A)$, kde A' je množina a $\nu : A' \to \mathbf{N}_0$ je zobrazení určující násobnosti prvků A'. A si můžeme představovat jako seznam, v němž nezáleží na pořadí a opakování prvků je dovoleno. Potřebujeme-li hodnotu $\nu_A(x)$ pro nějaký prvek $x \notin A'$, dodefinujeme ji jako 0. A je *konečná*, je-li A' konečná. Pro konečnou multipodmnožinu $\mathbf{N}$, to jest pro $A = (A', \nu)$ s konečnou $A' \subset \mathbf{N}$, definujeme $\|A\| = \sum_{a \in A'} \nu(a)a$. A je pak rozkladem čísla $\|A\|$. $A = (A', \nu_A)$ a $B = (B', \nu_B)$ buďte dvě multimnožiny. Relace $A \subset B$ znamená, že $\nu_A(a) \le \nu_B(a)$ pro všechny $a \in A'$. (Nemusí platit, že $A' \subset B'$, ovšem nutně $\nu_A(x) = 0$ pro všechny $x \in A' \backslash B'$.) Sjednocení A a B definujeme jako $A \cup B = (A' \cup B', \nu)$, kde $\nu(x) = \max(\nu_A(x), \nu_B(x))$. Podobně definujeme sjednocení konečně mnoha multimnožin. Rozdíl A a B definujeme jako $A - B = (\{x \in A' : \ \nu_A(x) \ge \nu_B(x)\}, \nu)$, kde $\nu(x) = \nu_A(x) - \nu_B(x)$. Součet A a B definujeme jako $A + B = (A' \cup B', \nu)$, kde $\nu(x) = \nu_A(x) + \nu_B(x)$.

Číselný rozklad $\lambda = (l^{a_l}, \ldots, 2^{a_2}, 1^{a_1}) \vdash n$ chápeme jako multimnožinu $(\{1, 2, \ldots, l\}, \nu)$ s $\nu(i) = a_i$. Patrně $\|\lambda\| = |\lambda| = n$. Nechť $\mathcal{A} = (A_i)_{i \ge 1} = ((A_i', \nu_{A_i}))_{i \ge 1}$ je posloupnost konečných multipodmnožin $\mathbf{N}$ a n je přirozené číslo. Definujeme

$$P_n(\mathcal{A}) = \{\lambda \vdash n : \ A_i \not\subset \lambda \ \text{ pro } \ \forall i\} \ \text{ a } \ p(n, \mathcal{A}) = |P_n(\mathcal{A})| \ .$$

Můžeme předpokládat, že $\mathcal{A}$ je prostá posloupnost, protože opakování jejích členů nemá na $P_n(\mathcal{A})$ vliv.

Věta 232 (Cohen, 1981; Remmel, 1982). *$\mathcal{A} = (A_i)_{i \ge 1}$ a $\mathcal{B} = (B_i)_{i \ge 1}$ buďte takové dvě prosté posloupnosti konečných multipodmnožin $\mathbf{N}$, že pro každou konečnou podmnožinu $S \subset \mathbf{N}$ platí*

$$\Big\| \bigcup_{i \in S} A_i \Big\| = \Big\| \bigcup_{i \in S} B_i \Big\| \ .$$

Potom pro každé číslo $n \in \mathbf{N}$ platí $p(n, \mathcal{A}) = p(n, \mathcal{B})$.

Důkaz. Pro rozklad λ položíme $S_{\mathcal{A}}(\lambda) = \{i \in \mathbf{N} : \ A_i \subset \lambda\}$ a $S_{\mathcal{B}}(\lambda) = \{i \in \mathbf{N} : \ B_i \subset \lambda\}$. Obě množiny jsou konečné. Pro pevné $n \in \mathbf{N}$ uvážíme konečné množiny

$$A = \{(\lambda, S) : \ \lambda \vdash n \ \& \ S \subset S_{\mathcal{A}}(\lambda)\} \ \text{ a } \ B = \{(\lambda, S) : \ \lambda \vdash n \ \& \ S \subset S_{\mathcal{B}}(\lambda)\} \ .$$

A a B rozložíme na dvě části znaménkovou funkcí $(\lambda, S) \mapsto (-1)^{|S|}$. Zobrazení $\alpha : A \to A$ definujeme jako $(\lambda, \emptyset) \mapsto (\lambda, \emptyset)$ pro $S_{\mathcal{A}}(\lambda) = \emptyset$ a jako

$$(\lambda, S) \mapsto \left\{ \begin{array}{lll} (\lambda, S \backslash \{a_\lambda\}) & \ldots & a_\lambda \in S \\ (\lambda, S \cup \{a_\lambda\}) & \ldots & a_\lambda \notin S \end{array} \right.$$

pro $S_{\mathcal{A}}(\lambda) \neq \emptyset$, kde $a_\lambda = \max S_{\mathcal{A}}(\lambda)$. Zobrazení $\beta : B \to B$ definujeme zcela analogicky. Zobrazení α a β jsou zřejmě involuce na A, respektive na B, a jejich množiny pevných bodů jsou

$$F_\alpha = \{(\lambda, \emptyset) : \ S_{\mathcal{A}}(\lambda) = \emptyset\} \ \text{ a } \ F_\beta = \{(\lambda, \emptyset) : \ S_{\mathcal{B}}(\lambda) = \emptyset\} \ .$$

Je zřejmé, že α a β mění znaménko. Všimněme si, že $|F_\alpha| = p(n, \mathcal{A})$ a $|F_\beta| = p(n, \mathcal{B})$.

Zobrazení $f : A \to B$ definujeme předpisem

$$(\lambda, S) \mapsto ((\lambda - \textstyle\bigcup_{i \in S} A_i) + \bigcup_{i \in S} B_i, S) \ .$$

Podle definic množin A a B a operací s multimnožinami a podle předpokladu o $\mathcal{A}$ a $\mathcal{B}$ je pro $\lambda \vdash n$ i $(\lambda - \bigcup_{i \in S} A_i) + \bigcup_{i \in S} B_i \vdash n$ a jedná se vskutku o zobrazení z A do B. Navíc to je bijekce, protože $(\lambda, S) \mapsto ((\lambda - \bigcup_{i \in S} B_i) + \bigcup_{i \in S} A_i, S)$ je inverzní zobrazení. Z definice f plyne, že f zachovává znaménko. Podle předchozího tvrzení máme $|F_\alpha| = |F_\beta|$ a věta je dokázána. $\diamondsuit$

Předpoklad předchozí věty o $\mathcal{A}$ a $\mathcal{B}$ je zřejmě splněn, pokud obě posloupnosti jsou disjunktní ($A'_i \cap A'_j = \emptyset$ a $B'_i \cap B'_j = \emptyset$ pro každé $i \neq j$) a $\|A_i\| = \|B_i\|$ pro každé $i \in \mathbf{N}$. Pak řekneme, že předpoklad věty je *disjunktně splněn.*

Z nepřeberného množství identit, které se z věty dají odvodit, vybíráme čtyři příklady.

Tvrzení 233 (zakázané čtverce). *Každé $n \in \mathbf{N}$ má tolik rozkladů na části, mezi nimiž není čtverec, jako rozkladů, v nichž je každá část $k \in \mathbf{N}$ použita méně než k krát.*

DŮKAZ. Speciální případ věty 232 pro posloupnosti

$$\mathcal{A} = (\{1\}, \{4\}, \{9\}, \ldots) \ \text{ a } \ \mathcal{B} = (\{1\}, \{2, 2\}, \{3, 3, 3\}, \ldots) \ .$$

Předpoklad věty je zřejmě disjunktně splněn. $\diamondsuit$

Tvrzení 234 (Glaisherova identita). *Nechť $d \in \mathbf{N}$. Pro každé $n \in \mathbf{N}$ se počet rozkladů n na části nedělitelné číslem d rovná počtu rozkladů na části s násobnostmi nepřesahujícími $d-1$.*

DŮKAZ. Speciální případ věty 232 pro posloupnosti

$$\begin{aligned}\mathcal{A} &= (\{d\},\{2d\},\{3d\},\ldots)\\ \mathcal{B} &= (\{1,1,\ldots,1\},\{2,2,\ldots,2\},\{3,3,\ldots,3\},\ldots)\ ,\end{aligned}$$

kde v každé $B_i = \{i,i,\ldots,i\}$ máme d opakování. Předpoklad věty je zřejmě disjunktně splněn. $\diamondsuit$

Věta 213 je speciální případ poslední identity pro $d = 2$.

Tvrzení 235 (Schurova identita). *Každé $n \in \mathbf{N}$ má tolik rozkladů n na části $\equiv \pm 1 \bmod 6$ jako rozkladů na vzájemně různé části $\equiv \pm 1 \bmod 3$.*

DŮKAZ. Speciální případ věty 232 pro posloupnosti

$$\begin{aligned}\mathcal{A} &= (\{2\},\{3\},\{4\},\{6\},\{8\},\{9\},\{10\},\{12\},\{14\},\ldots)\\ \mathcal{B} &= (\{1,1\},\{3\},\{2,2\},\{6\},\{4,4\},\{9\},\{5,5\},\{12\},\{7,7\},\ldots)\ .\end{aligned}$$

Předpoklad věty je zřejmě disjunktně splněn. $\diamondsuit$

Tvrzení 236 (ještě jedna identita). *Pro každé $n \in \mathbf{N}$ se počet rozkladů na části, které se opakují nejvýše třikrát a pro dvě po sobě jdoucí části se vždy alespoň jedna z nich neopakuje, rovná počtu rozkladů, v nichž se sudé části vždy liší alespoň o 4 (a neopakují se, liché části nejsou nijak omezeny).*

DŮKAZ. Speciální případ věty 232 pro posloupnosti

$$\begin{aligned}\mathcal{A} &= (\{1,1,1,1\},\{1,1,2,2\},\{2,2,2,2\},\{2,2,3,3\},\{3,3,3,3\},\ldots)\\ \mathcal{B} &= (\{2,2\},\{2,4\},\{4,4\},\{4,6\},\{6,6\},\ldots)\ .\end{aligned}$$

Předpoklad věty je splněn, ale ne disjunktně. $\diamondsuit$

7.4 Asymptotika partitní funkce

V tomto oddílu odvodíme asymptotiku funkce $p(n)$ pro $n \to \infty$.

Věta 237 (Hardy a Ramanujan, 1918; Uspensky, 1920). *Partitní funkce $p(n)$ počítající rozklady čísla $n \in \mathbf{N}$ má pro $n \to \infty$ asymptotiku*

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

K důkazu věty budeme potřebovat dvě tvrzení a pět lemmat. Pro $z \in \mathbf{C}$, $|z| < 1$, položíme

$$\Phi(z) = \left(\frac{1-z}{2\pi}\right)^{1/2} \cdot \exp\left(\frac{\pi^2}{12} \cdot \frac{1+z}{1-z}\right) .$$

Nalezneme asymptotiku koeficientů $q(n)$ rozvoje funkce $\Phi(z)$ do mocninné řady a ukážeme, že dobře aproximují hodnoty $p(n)$.

Tvrzení 238 (růst koeficientů q(n)). *Nechť $\Phi(z) = \sum_{n \geq 0} q(n) z^n$. Pro $n \to \infty$ platí*

$$q(n) \sim \frac{1}{4n\sqrt{3}} \cdot \mathrm{e}^{\pi(2n/3)^{1/2}} .$$

Důkaz. Vyjdeme ze známé identity $\int_{-\infty}^{\infty} \mathrm{e}^{-t^2}\, dt = \sqrt{\pi}$. Lineární substituce $t \mapsto at - b$ dává $\int_{-\infty}^{\infty} \mathrm{e}^{-(at-b)^2}\, dt = \sqrt{\pi}/a$, a tak

$$\int_{-\infty}^{\infty} \mathrm{e}^{-a^2 t^2} \mathrm{e}^{2abt}\, dt = \frac{\sqrt{\pi}}{a} \cdot \mathrm{e}^{b^2} .$$

Položíme $a^2 = 1 - z$, $b^2 = \frac{\pi^2}{6(1-z)}$ (nyní je z reálná konstanta) a dostaneme

$$\int_{-\infty}^{\infty} \exp(zt^2) \cdot \exp\left(\pi t \sqrt{2/3} - t^2\right) dt = \left(\frac{\pi}{1-z}\right)^{1/2} \cdot \exp\left(\frac{\pi^2}{6(1-z)}\right) .$$

Odtud

$$\Phi(z) = \frac{\mathrm{e}^{-\pi^2/12}}{\pi\sqrt{2}} (1-z) \int_{-\infty}^{\infty} \exp(zt^2) \cdot \exp\left(\pi t \sqrt{2/3} - t^2\right) dt .$$

Porovnání koeficientů u z^n vede k integrální reprezentaci

$$q(n) = \frac{\mathrm{e}^{-\pi^2/12}}{\pi\sqrt{2}} \int_{-\infty}^{\infty} \left(\frac{t^{2n}}{n!} - \frac{t^{2n-2}}{(n-1)!}\right) \exp\left(\pi t\sqrt{2/3} - t^2\right)\, dt\ ,$$

která substitucí $t = s + \sqrt{n}$ a úpravami přechází v

$$q(n) = C_n \int_{-\infty}^{\infty} K_n(s) \cdot 2s \cdot \mathrm{e}^{-2(s-\pi/2\sqrt{6})^2}\, ds\ ,$$

kde

$$C_n = \frac{\mathrm{e}^{\pi(2n/3)^{1/2}}}{\pi n\sqrt{2}} \cdot \frac{n^{n+1/2}}{\mathrm{e}^n n!} \sim \frac{1}{2\pi^{3/2}} \cdot \frac{\mathrm{e}^{\pi(2n/3)^{1/2}}}{n}$$

pro $n \to \infty$ díky Stirlingově formuli $n! \sim (2\pi n)^{1/2}(n/\mathrm{e})^n$ a

$$K_n(s) = \frac{1 + \frac{s}{2\sqrt{n}}}{\left(1 + \frac{s}{\sqrt{n}}\right)^2} \left(\left(1 + \frac{s}{\sqrt{n}}\right) \cdot \exp\left(\frac{-s}{\sqrt{n}} + \frac{s^2}{2n}\right)\right)^{2n}\ .$$

Vzhledem k rozvoji $1 + \frac{s}{\sqrt{n}} = \exp(\log(1 + \frac{s}{\sqrt{n}})) = \exp(sn^{-1/2} - s^2 n^{-1}/2 + O_s(n^{-3/2}))$ máme $\lim_{n\to\infty} K_n(s) = 1$ pro každé $s \in \mathbf{R}$. Pro zdůvodnění záměny pořadí limity a integrace ukážeme, že integrand v posledním vyjádření $q(n)$ má integrabilní majorantu.

Funkce $x\mathrm{e}^{-x}$ nabývá v $x \geq 0$ maxima pro $x = 1$. Pro $s \geq 0$ tedy platí $(1 + \frac{s}{\sqrt{n}}) \cdot \mathrm{e}^{-s/\sqrt{n}} \leq 1$ (položili jsme $x = 1 + \frac{s}{\sqrt{n}}$) a pro $x < 0$ platí $|1 + \frac{s}{\sqrt{n}}| \cdot \mathrm{e}^{-s/\sqrt{n}} \leq \mathrm{e}^{s^2/2n}$ (položili jsme $x = (1 + \frac{s}{\sqrt{n}})^2$). Takže

$$|K_n(s)| \leq \mathrm{e}^{s^2} \quad \text{pro} \quad s \geq 0$$

a pro $s < 0$

$$\begin{aligned} |K_n(s)| &\leq (1-s) \cdot \mathrm{e}^{s^2 - 2s/\sqrt{n}} \left(\left|1 + \frac{s}{\sqrt{n}}\right| \cdot \mathrm{e}^{-s/\sqrt{n}}\right)^{2n-2} \\ &\leq (1-s) \cdot \mathrm{e}^{s^2 - 2s/\sqrt{n}} \cdot \mathrm{e}^{(n-1)s^2/n} \\ &= (1-s) \cdot \mathrm{e}^{2s^2 + 1 - (1 - s/\sqrt{n})^2} \\ &\leq (1-s) \cdot \mathrm{e}^{2s^2+1}\ . \end{aligned}$$

Integrand ve vyjádření $q(n)$ je tedy v absolutní hodnotě shora omezen

$$2s \cdot \mathrm{e}^{s^2 - 2(s-\pi/2\sqrt{6})^2} \quad \text{pro} \quad s \geq 0 \quad \text{a} \quad 2s \cdot (1-s) \cdot \mathrm{e}^{2s^2 - 2(s-\pi/2\sqrt{6})^2 + 1} \quad \text{pro} \quad s < 0\ .$$

Tato majoranta má na $(-\infty, \infty)$ konečný integrál.

Pro $n \to \infty$ tak ve vyjádření $q(n)$ můžeme $K_n(s)$ nahradit konstantou 1. Pomocí substituce $s = \frac{u}{\sqrt{2}} + \frac{\pi}{2\sqrt{6}}$ dostáváme

$$\begin{aligned} q(n) &\sim C_n \int_{-\infty}^{\infty} 2s \cdot \mathrm{e}^{-2(s-\pi/2\sqrt{6})^2}\, ds \\ &= C_n \int_{-\infty}^{\infty} \left(u + \frac{\pi}{2\sqrt{3}}\right) \mathrm{e}^{-u^2}\, du = C_n \frac{\pi}{2\sqrt{3}} \int_{-\infty}^{\infty} \mathrm{e}^{-u^2}\, du \\ &\sim \frac{\mathrm{e}^{\pi(2n/3)^{1/2}}}{4\sqrt{3}n} \ . \end{aligned}$$

Na druhém řádku jsme využili lichost funkce ue^{-u^2} a na třetím znovu identitu $\int_{-\infty}^{\infty} \mathrm{e}^{-u^2}\, du = \sqrt{\pi}$. $\diamondsuit$

Nechť $I \subset \mathbf{C}$ je orientovaná úsečka, polopřímka či přímka a $f : I \to \mathbf{C}$ je funkce. *Totální variací* f na I rozumíme supremum

$$\sup \sum_{i=1}^{n-1} |f(a_{i+1}) - f(a_i)|$$

brané přes všechny konečné posloupnosti $a_1 < a_2 < \ldots < a_n$ bodů na I, kde $<$ je uspořádání dané orientací I.

Lemma 239. *Nechť $L \subset \mathbf{C}$ je polopřímka vycházející z počátku, $w \in L$, $w \neq 0$ a funkce $g : L \to \mathbf{C}$ je na L integrovatelná a má na ní totální variaci V. Potom*

$$\left| w \sum_{n \geq 1} g(nw) - \int_L g(u)\, du \right| \leq |w| V \ .$$

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že $L = [0, \infty)$. Nechť $w > 0$ je reálné číslo a $N \in \mathbf{N}$. Pak $\left| w \sum_{n=1}^{N} g(nw) - \int_0^{Nw} g(u)\, du \right|$ se rovná

$$\begin{aligned} & w \left| \int_0^1 \left(\sum_{n=0}^{N-1} g(nw + w) - g(nw + uw) \right) du \right| \\ & \leq w \int_0^1 \left(\sum_{n=0}^{N-1} |g(nw + w) - g(nw + uw)| \right) du \\ & \leq w \int_0^1 V\, du = wV \ . \end{aligned}$$

Limitním přechodem $N \to \infty$ dostáváme dokazovanou nerovnost. $\diamondsuit$

Lemma 240. *Nechť*

$$g(x) = \frac{1}{x(\mathrm{e}^x - 1)} - \frac{1}{x^2} + \frac{\mathrm{e}^{-x}}{2x}$$

a $L \subset \{z \in \mathbf{C} : \ \mathrm{Re}(z) > 0\} \cup \{0\}$ *je libovolná polopřímka vycházející z počátku. Pak*

$$\int_L g(x)\ dx = \int_0^\infty g(x)\ dx = -\frac{1}{2}\log 2\pi\ .$$

DŮKAZ. První rovnost plyne z Cauchyho věty. Podle věty o konvergenci s majorantou máme $\int_0^\infty g(x)\ dx = \lim_{N\to\infty} \int_0^\infty (1-\mathrm{e}^{-Nx}) g(x)\ dx$. Poslední integrál se rovná

$$\begin{aligned}
&\int_0^\infty (1-\mathrm{e}^{-Nx})\Big(\frac{1}{\mathrm{e}^x - 1} - \frac{1}{x}\Big)\frac{dx}{x} + \int_0^\infty (1-\mathrm{e}^{-Nx})\frac{\mathrm{e}^{-x}}{2x}\ dx \\
&= \sum_{k=1}^N \int_0^\infty \mathrm{e}^{-kx}\cdot\frac{1+x-\mathrm{e}^x}{x^2}\ dx + \frac{1}{2}\int_0^\infty \frac{\mathrm{e}^{-x}-\mathrm{e}^{-(N+1)x}}{x}\ dx \\
&= -\sum_{k=1}^N \int_0^\infty \mathrm{e}^{-kx}\int_0^1 t\mathrm{e}^{(1-t)x}\ dt\ dx + \frac{1}{2}\int_0^\infty\int_1^{N+1} \mathrm{e}^{-sx}\ ds\ dx \\
&= -\sum_{k=1}^N \int_0^1\int_0^\infty t\mathrm{e}^{(1-t-k)x}\ dx\ dt + \frac{1}{2}\int_1^{N+1}\int_0^\infty \mathrm{e}^{-sx}\ dx\ ds \\
&= -\sum_{k=1}^N \int_0^1 \frac{t\ dt}{k+t-1} + \frac{1}{2}\int_1^{N+1}\frac{ds}{s} \\
&= \sum_{k=1}^N \Big((k-1)\log\Big(\frac{k}{k-1}\Big) - 1\Big) + \frac{\log(N+1)}{2} \\
&= N\log N - \sum_{k=1}^N \log k - N + \frac{\log(N+1)}{2} \\
&= N\log N - \log N! - N + \frac{\log(N+1)}{2}\ .
\end{aligned}$$

Podle Stirlingovy formule $N! \sim (2\pi N)^{1/2}(N/\mathrm{e})^N$ poslední výraz pro $N\to\infty$ konverguje k $\log(1/\sqrt{2\pi})$. $\diamondsuit$

Lemma 241. *Nechť* $g(x)$ *a* L *jsou jako v předchozím lemmatu, přičemž pro* $z \in L\backslash\{0\}$ *platí* $|\arg(z)| < K < \pi/2$. *Pak totální variace funkce* $g(x)$ *na* L *splňuje odhad* $V_L \ll_K 1$.

Důkaz. Z definice totální variace plyne, že ji spočteme z formule

$$V_L = \int_L |g(z)'| \cdot |dz| \ .$$

Pro $z \in L$, $|z| > 1$, máme odhad

$$|g(z)'| \ll_K |z|^{-3} \ .$$

Funkce $g(z)$ je holomorfní v kruhu $|z| < 2\pi$, a tak $|g(z)'| \ll 1$ pro $|z| \leq 1$. Předchozí integrál tedy konverguje a V_L omezena konstantou závisející jen na K. $\diamondsuit$

Pro $z \in \mathbf{C}$, $|z| < 1$, položíme

$$F(z) = \sum_{n\geq 0} p(n) z^n = \prod_{n=1}^{\infty} \frac{1}{1-z^n} \ .$$

Logaritmováním dostaneme identitu

$$\log F(z) = \sum_{n,m\geq 1} \frac{z^{nm}}{m} = \sum_{m\geq 1} \frac{z^m}{m(1-z^m)} \ .$$

Lemma 242. *Pro všechna $z \in \mathbf{C}$, $|z| < 1$, platí*

$$|F(z)| < \exp\left(\frac{1}{1-|z|} + \frac{1}{|1-z|}\right) \ .$$

Důkaz. Podle hořejší identity pro $\log F(z)$ máme

$$\begin{aligned}
|\log F(z)| &\leq \frac{|z|}{|1-z|} + \sum_{m\geq 2} \frac{|z|^m}{m(1-|z|^m)} \\
&< \frac{1}{|1-z|} + \frac{1}{1-|z|} \sum_{m\geq 2} \frac{1}{m^2} \cdot \frac{m}{|z|^{-1} + |z|^{-2} + \cdots + |z|^{-m}} \\
&< \frac{1}{|1-z|} + \frac{1}{1-|z|} \sum_{m\geq 2} \frac{1}{m^2} < \frac{1}{|1-z|} + \frac{1}{1-|z|}
\end{aligned}$$

a lemma je dokázáno. $\diamondsuit$

Lemma 243. *Pro všechna $z \in \mathbf{C}$ splňující $|z| < 1$ a $|1-z| \le 2(1-|z|)$ platí*

$$F(z) = \Phi(z) \cdot (1 + O(1-z)) \quad (z \to 1)\ .$$

DŮKAZ. Položíme $z = \mathrm{e}^{-w}$, kde $|\mathrm{Im}(w)| \le \pi$. Podle předpokladů o z máme $|\arg(w)| < K < \pi/2$ pro nějakou konstantu K. Hořejší vyjádření $\log F(z)$ pak přejde v

$$\log F(z) = \sum_{m \ge 1} \frac{1}{m(\mathrm{e}^{mw} - 1)}\ .$$

S použitím rozvojů $\pi^2/6 = \sum_{n\ge1} n^{-2}$ a $\log(1-x) = -\sum_{n\ge1} x^n/n$ tuto rovnost přepíšeme jako

$$\begin{aligned}\log F(z) &= \frac{\pi^2}{6w} + \frac{1}{2}\log(1-\mathrm{e}^{-w}) + w\sum_{m\ge1}\left(\frac{1}{mw(\mathrm{e}^{mw}-1)} - \frac{1}{m^2w^2} + \frac{\mathrm{e}^{-mw}}{2mw}\right)\\ &= \frac{\pi^2}{6w} + \frac{1}{2}\log(1-\mathrm{e}^{-w}) + w\sum_{m\ge1} g(mw)\ ,\end{aligned}$$

kde $g(x)$ je funkce z lematu 240. Vezmeme polopřímku L vycházející z počátku a jdoucí ve směru $\arg(w)$. Podle lemmat 239, 240 a 241 máme pro $|\mathrm{Im}(w)| \le \pi$ a $|\arg(w)| < K < \pi/2$ odhad

$$w\sum_{m\ge1} g(mw) = -\frac{1}{2}\log 2\pi + O(|w|)\ .$$

Tudíž, s využitím $w^{-1} = (-\log z)^{-1} = (\log\frac{1}{1-(1-z)})^{-1} = (1-z)^{-1}(1 + (1-z)/2 + O((1-z)^2))^{-1} = (1-z)^{-1} - 1/2 + O(1-z)$,

$$\begin{aligned}\log F(z) &= \frac{\pi^2}{6w} + \frac{1}{2}\log\frac{1-\mathrm{e}^{-w}}{2\pi} + O(w)\\ &= \frac{\pi^2}{6(1-z)} - \frac{\pi^2}{12} + \frac{1}{2}\log\frac{1-z}{2\pi} + O(1-z)\\ &= \log\Phi(z) + O(1-z)\ .\end{aligned}$$

Tím je lemma dokázáno. ♢

Tvrzení 244 ($\mathbf{p(n) \sim q(n)}$). *Koeficienty rozvojů $\Phi(z) = \sum_{n\ge0} q(n)z^n$ a $F(z) = \sum_{n\ge0} p(n)z^n$ pro $n \to \infty$ splňují*

$$p(n) = q(n) + O\Big(n^{-5/4}\exp(\pi(2n/3)^{1/2})\Big)\ .$$

DŮKAZ. Podle Cauchyho věty

$$p(n) - q(n) = \frac{1}{2\pi i} \int_C \frac{F(z) - \Phi(z)}{z^{n+1}}\, dz \ ,$$

kde C je kružnice $|z| = 1 - \pi/\sqrt{6n}$. C rozdělíme na dva oblouky

$$A = \{z \in C :\ |1 - z| < \pi(2/(3n))^{1/2}\} \ \text{ a } \ B = C\backslash A \ .$$

Pro $z \in C$ máme $|z|^{-n} = \mathrm{e}^{-n \log(1-(1-|z|))} = \mathrm{e}^{\pi(n/6)^{1/2}+O(1)}$ a $|z|^{-1} < 2$. Podle definice $\Phi(z)$, lemmatu 242 a trojúhelníkové nerovnosti platí

$$\begin{aligned}
\int_B \frac{F(z) - \Phi(z)}{z^{n+1}}\, dz &\ll \int_B |z|^{-n} \Big(\mathrm{e}^{|1-z|^{-1}+(1-|z|)^{-1}} + \mathrm{e}^{\pi^2/(6|1-z|)}\Big)\, |dz| \\
&\ll \mathrm{e}^{\pi(n/6)^{1/2}} \Big(\mathrm{e}^{((3n/2)^{1/2}+(6n)^{1/2})/\pi} + \mathrm{e}^{(\pi/6)(3n/2)^{1/2}}\Big) \\
&= \mathrm{e}^{n^{1/2}(\pi/6^{1/2}+((3/2)^{1/2}+6^{1/2})/\pi)} + \mathrm{e}^{\pi n^{1/2}(3/8)^{1/2}} \\
&\ll \mathrm{e}^{\pi n^{1/2} a} \ ,
\end{aligned}$$

kde $0 < a < (2/3)^{1/2}$ (to se vidí z odhadu $1/\pi < \pi/9$). Podle definice $\Phi(z)$, lemmatu 243 (jehož předpoklad je pro naši volbu oblouku A splněn) a odhadu $|A| \ll n^{-1/2}$ platí

$$\begin{aligned}
\int_A \frac{F(z) - \Phi(z)}{z^{n+1}}\, dz &\ll \int_A |z|^{-n} \cdot |1 - z|^{3/2} \cdot \mathrm{e}^{\pi^2/(6|1-z|)}\, |dz| \\
&\ll \mathrm{e}^{\pi(n/6)^{1/2}} \cdot n^{-3/4} \cdot \mathrm{e}^{\pi(n/6)^{1/2}} \cdot n^{-1/2} \\
&= n^{-5/4} \cdot \mathrm{e}^{\pi(2n/3)^{1/2}} \ .
\end{aligned}$$

Spojení obou odhadů dává dokazovanou asymptotiku $p(n) - q(n)$. $\diamondsuit$

DŮKAZ VĚTY 237. **(Newman, 1962).** Asymptotika partitní funkce $p(n)$ bezprostředně plyne z tvrzení 238 a 244. $\diamondsuit$

7.5 Linnikovo řešení Waringova problému

Řešením rovnic v tomto oddílu rozumíme celočíselná řešení. Pro čísla $n \in \mathbf{N}_0$ a $g, d \in \mathbf{N}$ označíme $W(n, g, d)$ počet řešení rovnice

$$x_1^d + x_2^d + \cdots + x_g^d = n \quad x_i \geq 0 \ .$$

Waringův problém požaduje dokázat, že pro každé $d \in \mathbf{N}$ existuje $g \in \mathbf{N}$ tak, že $W(n,g,d) \geq 1$ pro všechna $n \in \mathbf{N}_0$. Jinak řečeno, pro každé pevné $d \geq 1$ lze každé přirozené číslo vyjádřit jako součet nejvýše g d-tých mocnin přirozených čísel. Nejmenší takové g se označuje $g(d)$. Jako $G(d)$ označíme nejmenší takové g, že existuje $n_0 \in \mathbf{N}$ tak, že každé $n > n_0$ je součtem nejvýše g d-tých mocnin přirozených čísel. Patrně $G(d) \leq g(d)$. Na druhou stranu z $G(d) < \infty$ plyne, že i $g(d) < \infty$. Věta 246, kterou dokážeme, říká, že $g(d) < \infty$ pro každé $d \in \mathbf{N}$. Věta 55 a skutečnost, že čísla tvaru $8n + 7$ nejsou součtem tří čverců, ukazují, že $g(2) = G(2) = 4$. Jednoduché důkazy odhadů $G(3) \leq 13$ a $g(4) \leq 53$ obsahuje úloha 20.

Podívejme se nyní na horní odhady pro $W(n,g,d)$. Je jasné, že

$$W(n,g,d) \leq (n^{1/d}+1)^{g-1} < 2n^{(g-1)/d} \quad (n \geq n_0) ,$$

protože pro každou složku řešení máme nejvýše $1 + n^{1/d}$ hodnot a při zvolených $x_1, \ldots, x_{g-1}$ už pro x_g máme nejvýše jednu hodnotu. Klíčem k řešení Waringova problému pomocí šnirelmanovského obratu je skutečnost, že tento triviální horní odhad lze zesílit na $W(n,g,d) \ll_d n^{g/d-1}$. Poznamenejme, že obtížný je případ $d \geq 2$, $W(n,g,1)$ lze snadno spočítat přesně (úloha 1b).

Tvrzení 245 (netriviální odhad $W(n,g,d)$). *Pro každé $d \in \mathbf{N}$ existuje $g_0 = g_0(d) \in \mathbf{N}$ tak, že pro každé pevné $g \geq g_0$ a n probíhající $\mathbf{N}$ platí*

$$W(n,g,d) \ll_d n^{g/d-1} .$$

Tento odhad stačí dokázat pro jediné g_0 a pro $g \geq g_0$ už plyne triviálně. Pro každé pevné $g \geq g_0$ totiž

$$\begin{aligned} W(n,g,d) &= \sum_{x_1,\ldots,x_{g-g_0} \geq 0} W(n - x_1^d - \cdots - x_{g-g_0}^d, g_0, d) \\ &\leq (1+n^{1/d})^{g-g_0} \cdot \max_{0 \leq m \leq n} W(m, g_0, d) \\ &< 2n^{(g-g_0)/d} \cdot W(M, g_0, d) , \end{aligned}$$

kde $n \geq n_0$ a $0 \leq M \leq n$. Ovšem $W(M,g_0,d) \ll_d M^{g_0/d-1} \leq n^{g_0/d-1}$, a tak $W(n,g,d) \ll_d n^{g/d-1}$ s konstantou nezávisející na g. Důkaz tvrzení na chvíli odsuneme a přejdeme hned k řešení Waringova problému.

Věta 246 (Hilbert, 1909). *Pro každé $d \in \mathbf{N}$ existuje $g = g(d) \in \mathbf{N}$ tak, že rovnice*

$$x_1^d + x_2^d + \cdots + x_g^d = n \quad x_i \geq 0$$

má pro každé $n \in \mathbf{N}_0$ alespoň jedno řešení. Jinak řečeno, každé přirozené číslo je součtem nejvýše g d-tých mocnin přirozených čísel.

DŮKAZ. **(Linnik, 1943).** Nechť $d \in \mathbf{N}$ je pevné. Pro každé $g \in \mathbf{N}$ a $x > 0$ součet d-tých mocnin libovolných g čísel vybraných z $\{1, 2, \ldots, \lfloor (x/g)^{1/d} \rfloor\}$ nepřesahuje x. Odtud máme pro $x > 1$ triviální odhad

$$\sum_{n \leq x} W(n, g, d) \geq (\lfloor (x/g)^{1/d} \rfloor)^g \gg_g x^{g/d} .$$

Na druhou stranu existuje $g_0 \in \mathbf{N}$ tak, že $W(n, g_0, d)$ máme shora odhadnuto tvrzením 245. Z obou odhadů plyne existence konstanty $c > 0$ závisející jen na d takové, že

$$\frac{1}{x} \cdot \#\{n \leq x : \; W(n, g_0, d) \geq 1\} > c$$

pro všechna $x > 1$. Množina X těch přirozených čísel, která jsou součtem nejvýše g_0 d-tých mocnin, má proto kladnou Šnirelmanovu hustotu (patrně $1 \in X$). Podle Šnirelmanovy věty 152 z 5. kapitoly je X aditivní bází $\mathbf{N}$. Každé $n \in \mathbf{N}$ je součtem omezeně mnoha sčítanců z X a tudíž i omezeně mnoha d-tých mocnin přirozených čísel. $\diamondsuit$

Zbývá ovšem dokázat tvrzení 245. Následující elementární důkaz náleží Linnikovi. Sestává z pěti lemmat a dvou tvrzení.

Lemma 247. *Nechť $a_1, a_2, \ldots, a_l \in \mathbf{Z}$, $l \geq 2$, jsou vesměs nesoudělná čísla, $m \in \mathbf{Z}$, $A > 0$ je reálné číslo a $\max_{1 \leq i \leq l} |a_i| = H \leq A$. Pak rovnice*

$$a_1 x_1 + a_2 x_2 + \cdots + a_l x_l = m \quad |x_i| \leq A$$

má $\ll_l A^{l-1}/H$ řešení.

DŮKAZ. Nejprve ukážeme, že pro $l = 2$ odhad platí s konstantou 3. Můžeme předpokládat, že $|a_1| \geq |a_2|$. Jsou-li (x_1, x_2) a (x_1', x_2') dvě různá řešení, odečtením dostaneme $a_1(x_1 - x_1') = a_2(x_2' - x_2)$. Tedy a_1 dělí $x_2 - x_2'$. Složky x_2 řešení jsou obsaženy v jisté aritmetické posloupnosti X s diferencí $|a_1|$, přičemž celá X leží v intervalu délky $2A$. Proto

$$|X| \leq \frac{2A}{|a_1|} + 1 \leq \frac{3A}{|a_1|} = \frac{3A}{H} .$$

Složka x_2 jednoznačně určuje x_1, a tak $3A/H$ odhaduje i počet řešení.

Pro $l > 2$ budeme postupovat indukcí podle l. Můžeme předpokládat, že $|a_l| = H \geq 1$. Pokud $a_1 = a_2 = \cdots = a_{l-1} = 0$, máme $|a_l| = H = 1$. Složky $x_1, \ldots, x_{l-1}$ pak mohou být libovolné a pro x_l máme nejvýše jednu hodnotu. Máme nejvýše

$$(3A)^{l-1} \ll_l \frac{A^{l-1}}{H}$$

řešení. Můžeme tedy předpokládat, že alespoň jedno a_i, $1 \leq i \leq l-1$, je nenulové. Původní rovnice pak je ekvivalentní soustavě dvou rovnic

$$\frac{a_1}{d}x_1 + \frac{a_2}{d}x_2 + \cdots + \frac{a_{l-1}}{d}x_{l-1} = m' \quad \text{a} \quad dm' + a_l x_l = m \ ,$$

kde $d = (a_1, a_2, \ldots, a_{l-1})$. Podle indukčního předpokladu má pro pevné m' první rovnice $\ll_l A^{l-2}/H'$ řešení v oboru $|x_i| \leq A$, kde $H' = \max_{1 \leq i \leq l-1} |a_i|/d \geq 1$. Koeficienty d a a_l v druhé rovnici jsou nesoudělná čísla a $d \leq |a_l|$. Dále $|a_i| \leq A$ implikuje $|m'| < lH'A$. Počet řešení (m', x_l) druhé rovnice v oboru $|m'|, |x_l| \leq lH'A$ podle případu $l = 2$ nepřesahuje $3lH'A/|a_l|$. Celkem má soustava nejvýše

$$\ll_l \frac{A^{l-2}}{H'} \cdot \frac{3lH'A}{|a_l|} \ll_l \frac{A^{l-1}}{H}$$

řešení. $\diamondsuit$

Lemma 248. *Nechť $l \in \mathbf{N}$, $l \geq 3$ a $m \in \mathbf{Z}$. Nechť $A > 0$ a $B = B(l) > 0$ jsou reálná čísla, přičemž $A \leq B \ll_l A^{l-1}$. Rovnice*

$$y_1 x_1 + y_2 x_2 + \cdots + y_l x_l = m \quad |y_i| \leq A, |x_i| \leq B$$

má $\ll_l (AB)^{l-1}$ řešení.

Důkaz. Řešení rozdělíme do tří skupin podle y-ové složky a ukážeme, že v každé skupině je $\ll_l (AB)^{l-1}$ řešení.

1. $y_1 = y_2 = \cdots = y_l = 0$. Těchto řešení je

$$\leq (2B+1)^l \ll_l B^l = BB^{l-1} \ll_l (AB)^{l-1} \ .$$

2. Alespoň jedno $y_i \neq 0$ a čísla y_i jsou vesměs nesoudělná. Fixujeme jednu takovou l-tici $\overline{y} = (y_1, y_2, \ldots, y_l)$ a položíme $\max_{1 \leq i \leq l} |y_i| = H$, patrně $H \leq A$. Vezmeme jednoznačné $r \in \mathbf{N}_0$ určené z

$$\frac{A}{2^{r+1}} < H \leq \frac{A}{2^r} \ .$$

Podle předchozího lemmatu počet l-tic $(x_1, x_2, \ldots, x_l)$ odpovídajících $\overline{y}$ nepřesahuje

$$\ll_l \frac{B^{l-1}}{H} \le \frac{B^{l-1}2^{r+1}}{A} \ll \frac{B^{l-1}2^r}{A} .$$

Počet l-tic $\overline{y}$, pro něž $H \le A/2^r$, je $\le (2A/2^r + 1)^l \ll_l A^l 2^{-rl}$. Celkem máme ve skupině 2

$$\ll_l \sum_{r \ge 0} \frac{B^{l-1}2^r}{A} \cdot A^l 2^{-rl} = (AB)^{l-1} \sum_{r \ge 0} 2^{-r(l-1)} \ll_l (AB)^{l-1}$$

řešení.

3. Alespoň jedno $y_i \ne 0$ a $(y_1, y_2, \ldots, y_l) = d > 1$. Fixujeme d, původní rovnici nahradíme rovnicí

$$y'_1 x_1 + y'_2 x_2 + \cdots + y'_l x_l = 0 \quad |y'_i| \le A/d, |x_i| \le B ,$$

kde $y'_i = y_i/d$, a postupujeme podle 2. A jsme nahradili číslem A/d, čímž se podmínka $B \ll_l A^{l-1}$ mohla porušit. Ovšem tu jsme v případu 2, který nyní aplikujeme, nepoužili (použili jsme ji jen v případu 1). Ve skupině 3 tedy máme celkem ($l \ge 3$)

$$\ll_l \sum_{d > 1} (AB/d)^{l-1} = (AB)^{l-1} \sum_{d > 1} \frac{1}{d^{l-1}} \ll_l (AB)^{l-1}$$

řešení. $\diamondsuit$

Multimnožiny jsme uvažovali již v 7.3. Připomínáme, že multimnožina celých čísel je dvojice $U = (U, \kappa)$, kde $U \subset \mathbf{Z}$ a $\kappa : U \to \mathbf{N}_0$. Multimnožinu vykládáme jako množinu s opakujícími se prvky: $\kappa(a)$ je násobnost prvku $a \in U$ ($\kappa(a) = 0$ pro všechny $a \in \mathbf{Z} \backslash U$). Při počítání řešení rovnic nad multimnožinami bereme v úvahu násobnosti: Počet řešení nějaké rovnice či soustavy s m neznámými $x_1, \ldots, x_m$ v oboru $x_i \in U_i$, kde $(U_1, \kappa_1), \ldots, (U_m, \kappa_m)$ jsou dané multimnožiny celých čísel, je roven $\sum \kappa_1(a_1)\kappa_2(a_2) \ldots \kappa_m(a_m)$, kde sčítáme přes všechna celočíselná řešení $a_1, \ldots, a_m$ dané rovnice či soustavy. Pro k konečných multimnožin celých čísel $U_1, \ldots, U_k$ a libovolnou funkci $f : \mathbf{Z}^k \to \mathbf{Z}$ značením

$$U \stackrel{m}{=} \{f(x_1, x_2, \ldots, x_k) : \ x_i \in U_i\}$$

rozumíme multimnožinu, v níž násobnost prvku y je rovna počtu řešení rovnice $y = f(x_1, x_2, \ldots, x_k)$, $x_i \in U_i$.

Lemma 249. *U a V buďte dvě konečné multimnožiny celých čísel a $c \in \mathbf{Z}$. Jako P, P_U a P_V označíme postupně počty řešení rovnic*

$$\begin{aligned} x+y &= c \quad x \in U, y \in V \\ x-y &= 0 \quad x, y \in U \\ x-y &= 0 \quad x, y \in V\ . \end{aligned}$$

Potom

$$P \leq (P_U + P_V)/2\ .$$

Speciálně, pokud $U = V$ (včetně násobností), potom $P \leq P_U = P_V$.

Důkaz. Nechť $\kappa : U \to \mathbf{N}_0$ a $\lambda : V \to \mathbf{N}_0$ jsou násobnosti prvků v U a V. Pro každé $x \in U$ existuje nejvýše jedno $y_x \in V$, že $x + y_x = c$. Počet řešení rovnice $x + y = c$ s $x \in U$ a $y \in V$ je roven $\sum_{x \in U} \kappa(x)\lambda(y_x)$ (pro neexistující y_x klademe $\lambda(y_x) = 0$). Patrně $x \neq x' \Rightarrow y_x \neq y_{x'}$. Máme

$$\sum_{x \in U} \kappa(x)\lambda(y_x) \leq \frac{1}{2} \cdot \sum_{x \in U} (\kappa(x)^2 + \lambda(y_x)^2) \leq \frac{1}{2} \cdot \left(\sum_{x \in U} \kappa(x)^2 + \sum_{y \in V} \lambda(y)^2 \right)\ .$$

Poslední dvě sumy jsou přesně počty řešení rovnice $x - y = 0$ pro $x, y \in U$ a pro $x, y \in V$. Dodatek je zřejmý. $\diamondsuit$

Lemma 250. *Nechť $l = k2^s$, kde $k, s \in \mathbf{N}$, $c \in \mathbf{Z}$ a $U_1, U_2, \ldots, U_l$ jsou konečné multimnožiny celých čísel. Nechť P je počet řešení rovnice (s l neznámými)*

$$x_1 + x_2 + \cdots + x_l = c, \quad x_i \in U_i$$

a pro každé m, $0 \leq m \leq 2^s - 1$, je P_m počet řešení rovnice (také s l neznámými)

$$\sum_{i=1}^{k} (y_{i,1} + \cdots + y_{i,2^{s-1}} - y_{i,2^{s-1}+1} - \cdots - y_{i,2^s}) = 0, \quad y_{i,j} \in U_{mk+i}\ .$$

Potom

$$P \leq (P_0 + P_1 + \cdots + P_{2^s - 1})/2^s\ .$$

DŮKAZ. Pro k libovolné a $s=1$ tvrzení plyne z lemmatu 249, když položíme $U \stackrel{m}{=} \{x_1+\cdots+x_{l/2}:\ x_i\in U_i\}$ a $V \stackrel{m}{=} \{x_{l/2+1}+\cdots+x_l:\ x_i\in U_i\}$. Nechť tvrzení platí pro $l=k2^s$, $P_m=P_m(k,s)$ jsou příslušné počty řešení, a k je sudé. Ukážeme, že tvrzení platí i pro rozklad $l=k'2^{s'}=(k/2)2^{s+1}$. Tím bude indukcí dokázána platnost tvrzení pro všechna k a s. Pro každé m, $0\le m\le 2^s-1$, položíme

$$\begin{aligned} U_m &\stackrel{m}{=} \left\{\textstyle\sum_{i=1}^{k/2}\left(\sum_{j=1}^{2^{s-1}} y_{i,j}-\sum_{j=2^{s-1}+1}^{2^s} y_{j,i}\right):\ y_{i,j}\in U_{mk+i}\right\}\\ V_m &\stackrel{m}{=} \left\{\textstyle\sum_{i=k/2+1}^{k}\left(\sum_{j=1}^{2^{s-1}} y_{i,j}-\sum_{j=2^{s-1}+1}^{2^s} y_{j,i}\right):\ y_{i,j}\in U_{mk+i}\right\}\ . \end{aligned}$$

Podle lemmatu 249 (nyní $c=0$) máme $P_m\le\frac{1}{2}(P'_m+P''_m)$, kde P'_m a P''_m jsou počty řešení rovnice $x-y=0$ pro $x,y\in U_m$ a pro $x,y\in V_m$. Tedy

$$P\le\frac{1}{2^s}\sum_{i=0}^{2^s-1}P_i\le\frac{1}{2^{s+1}}\cdot(P'_0+P''_0+\cdots+P'_{2^s-1}+P''_{2^s-1})\ .$$

Počty P'_m a P''_m nejsou nic jiného než počty $P_m=P_m(k/2,s+1)$. $\diamondsuit$

Pro celočíselný polynom $f(x)=a_0x^d+\cdots+a_{d-1}x+a_d$ stupně $d\ge 1$ je jeho *přidružený polynom* $\varphi(h,x)$ definován vztahem $f(x+h)-f(x)=h\cdot\varphi(h,x)$. Jedná se o celočíselný polynom

$$\varphi(h,x)=\sum_{i=1}^{d}b_i(h)x^{d-i}=\sum_{i=1}^{d-1}\left(\sum_{j=0}^{i-1}a_j\binom{d-j}{i-j}h^{i-j-1}\right)x^{d-i}\ .$$

Pro každé nenulové $h_0\in\mathbf{Z}$ má $\varphi(h_0,x)$ stupeň $d-1$.

Lemma 251. *Nechť $f(x)=a_0x^d+\cdots+a_{d-1}x+a_d$ je celočíselný polynom stupně $d\ge 1$, jehož koeficienty splňují odhady $a_i\ll_d n^{i/d}$, čísla $h_0,x_0\in\mathbf{Z}$ splňují $h_0,x_0\ll_d n^{1/d}$ a $\varphi(h,x)=b_1(h)x^{d-1}+\cdots+b_{d-1}x+b_d(h)$ je přidružený polynom f. Pak, pro $1\le i\le d$,*

$$b_i(h_0)\ll_d n^{(i-1)/d}\quad a\quad \varphi(h_0,x_0)\ll_d n^{(d-1)/d}\ .$$

DŮKAZ. Podle předpokladů $a_jh_0^{i-j-1}\ll_d n^{(i-1)/d}$ a $x_0^{d-i}\ll_d n^{(d-i)/d}$. Tudíž

$$b_i(h_0)\ll_d n^{(i-1)/d}\sum_{j=0}^{i-1}\binom{d-j}{i-j}\ll_d n^{(i-1)/d}$$

a také

$$|\varphi(h_0, x_0)| \leq \sum_{i=1}^{d} |b_i(h_0) x_0^{d-i}| \ll_d n^{(d-1)/d} .$$

$\diamondsuit$

Tvrzení 252 (indukční krok). *Nechť $k, s \in \mathbf{N}$, $l = k2^{s+1}$, $m \in \mathbf{Z}$, $A > 0$ je reálné číslo, $f(x)$ je celočíselný polynom stupně $d \geq 1$ a $\varphi(h, x)$ je jeho přidružený polynom. Nechť P a Q jsou postupně počty řešení dvou rovnic (s l, resp. $k + l/2$ neznámými)*

$$\begin{aligned} f(x_1) + f(x_2) + \cdots + f(x_l) &= m \quad |x_i| \leq A \\ \sum_{i=1}^{k} h_i \sum_{j=1}^{2^{s-1}} (\varphi(h_i, y_{i,j}) - \varphi(h_i, y_{i,j+2^{s-1}})) &= 0 \quad |h_i|, |y_{i,j}| \leq 2A . \end{aligned}$$

Potom

$$P \leq (1 + 4A)^{l/2-k} Q .$$

Důkaz. Podle dodatku lemmatu 249 platí $P \leq Q_1$, kde Q_1 je počet řešení rovnice

$$\sum_{i=1}^{l/2} (f(x_i) - f(y_i)) = 0 \quad |x_i|, |y_i| \leq A$$

(lemma aplikujeme na multimnožinu $U \stackrel{m}{=} \{f(x_1) + \cdots + f(x_{l/2}) : \ |x_i| \leq A\}$). Položíme $x_i = y_i + h_i$. Nerovnosti $|x_i|, |y_i| \leq A$ implikují $|h_i| \leq 2A$. Takže $Q_1 \leq Q_2$, kde Q_2 je počet řešení rovnice

$$z_1 + z_2 + \cdots + z_{l/2} = 0, \quad z_i \in U \stackrel{m}{=} \{h \cdot \varphi(h, y) : \ |h|, |y| \leq 2A\} .$$

Pro každou $l/2$-tici $\overline{h} = (h_1, h_2, \ldots, h_{l/2})$, $|h_i| \leq 2A$, označíme $U_i^{\overline{h}} \stackrel{m}{=} \{h_i \cdot \varphi(h_i, y) : \ |y| \leq 2A\}$. $Q_{2,\overline{h}}$ je počet řešení rovnice

$$z_1 + z_2 + \cdots + z_{l/2} = 0, \quad z_i \in U_i^{\overline{h}} .$$

Patrně

$$Q_2 = \sum_{\overline{h}} Q_{2,\overline{h}} .$$

Podle lemmatu 250 máme $Q_{2,\overline{h}} \leq (Q_{\overline{h},0} + Q_{\overline{h},1} + \cdots + Q_{\overline{h},2^s-1})/2^s$, kde $Q_{\overline{h},m}$ je počet řešení rovnice (s $l/2$ neznámými)

$$\sum_{i=1}^{k}(z_{i,1} + \cdots + z_{i,2^{s-1}} - z_{i,2^{s-1}+1} - \cdots - z_{i,2^s}) = 0, \quad z_{i,j} \in U^{\overline{h}}_{mk+i} .$$

Pro každé pevné m, $0 \leq m < 2^s$, platí

$$\sum_{\overline{h}} Q_{\overline{h},m} \leq (1+4A)^{l/2-k} Q .$$

Vektory $\overline{h}$ délky $l/2$ totiž můžeme rozložit na třídy tak, že vektory v jedné třídě se mohou lišit pouze v souřadnicích $mk+1, mk+2, \ldots, mk+k$ a v ostatních $l/2-k$ souřadnicích se musejí shodovat. Součet hodnot $Q_{\overline{h},m}$ v jedné třídě je přesně Q a tříd je nejvýše $(1+4A)^{l/2-k}$. Celkem

$$\begin{aligned} P \leq Q_2 = \sum_{\overline{h}} Q_{2,\overline{h}} &\leq \sum_{\overline{h}} (Q_{\overline{h},0} + Q_{\overline{h},1} + \cdots + Q_{\overline{h},2^s-1})/2^s \\ &= \sum_{m=0}^{2^s-1} \frac{1}{2^s} \sum_{\overline{h}} Q_{\overline{h},m} \leq \sum_{m=0}^{2^s-1} \frac{1}{2^s}(1+4A)^{l/2-k} Q \\ &= (1+4A)^{l/2-k} Q . \end{aligned}$$

◊

Přistoupíme k důkazu klíčového tvrzení 245. Budeme postupovat indukcí podle exponentu d. Indukce nás nutí dokázat obecnější tvrzení — místo x^d budeme muset pracovat se systémy celočíselných polynomů. Pro celočíselný polynom f stupně d a čísla $n, g \in \mathbf{N}$ a $N \in \mathbf{Z}$ označíme $w(n, N, g, f)$ počet řešení rovnice

$$f(x_1) + f(x_2) + \cdots + f(x_g) = N \quad |x_i| \leq n^{1/d} .$$

Následující tvrzení kvůli jasnosti formulujeme explicitně pomocí konstant c_i a c závisejících jen na parametru d. V důkazu používáme kompaktnější (v tomto případě ovšem méně jasné) značení $\ll_d$.

Tvrzení 253 (induktivní zobecnění tvrzení 245). *Pro každé číslo $d \in \mathbf{N}$ existuje $g_0(d) \in \mathbf{N}$ tak, že platí následující. Nechť je dáno $d \in \mathbf{N}$ a $d+1$ libovolných konstant $c_i > 0$, $0 \leq i \leq d$. Pak existuje konstanta $c > 0$ tak, že* *pro každé $n \in \mathbf{N}$, $N \in \mathbf{Z}$ a každý celočíselný polynom $f = f(x) = a_0x^d + \cdots + a_{d-1}x + a_d$ stupně d, jehož koeficienty splňují nerovnosti $|a_i| < c_i n^{i/d}$, pro $g = g_0(d)$ platí*

$$w(n, N, g, f) < cn^{g/d-1} .$$

DŮKAZ. **(Linnik, 1943).** Postupujeme indukcí podle stupně d. Pro $d = 1$ tvrzení platí s $g = g_0(1) = 1$: $f(x_1) = a_0x_1 + a_1 = N$ má pro $|x_1| \le n$ nejvýše jedno řešení. Nechť $d > 1$ a tvrzení platí pro stupeň $d - 1$. Položíme

$$g = g_0(d) = 2d2^{s+1}, \quad \text{kde} \quad s = \lceil \log_2 g_0(d-1) \rceil + 2 .$$

Buď dán celočíselný polynom $f(x) = a_0x^d + \cdots + a_{d-1}x + a_d$ stupně d, jehož koeficienty splňují $a_i \ll_d n^{i/d}$. Číslo $n \in \mathbf{N}$ buď libovolné pevné. Podle předchozího tvrzení, použitého s $l = g$, $k = 2d$ a $A = n^{1/d}$, máme $w(n, N, g, f) \le (1 + 4A)^{g/2-2d} Q \ll_d n^{g/2d-2} Q$, kde Q je počet řešení rovnice

$$\sum_{i=1}^{2d} h_i z_i = 0 \quad |h_i|, |y_{i,j}| \le 2n^{1/d} ,$$

přičemž

$$z_i = \sum_{j=1}^{2^{s-1}} (\varphi(h_i, y_{i,j}) - \varphi(h_i, y_{i,j+2^{s-1}}))$$

a φ je polynom přidružený k f.

Pro fixované hodnoty neznámých $h_1, \ldots, h_{2d}$ a libovolné pevné i, $1 \le i \le 2d$, nyní shora odhadneme násobnost čísla $z = z_i \in \mathbf{Z}$. Je rovna počtu řešení rovnice

$$\sum_{j=1}^{2^{s-1}} (\varphi(h_i, y_{i,j}) - \varphi(h_i, y_{i,j+2^{s-1}})) = z \quad |y_{i,j}| \le 2n^{1/d} .$$

Položíme $t = g_0(d-1)$ — patrně $t < 2^{s-1}$ — a rovnici přepíšeme ve tvaru soustavy dvou rovnic

$$\sum_{j=1}^{t} \varphi(h_i, y_{i,j}) = m \text{ , kde } m = z - \sum_{j=t+1}^{2^{s-1}} \varphi(h_i, y_{i,j}) + \sum_{j=1}^{2^{s-1}} \varphi(h_i, y_{i,j+2^{s-1}}) .$$

Počet řešení první rovnice odhadneme z indukčního předpokladu a počet řešení druhé triviálně. Hodnoty neznámých $y_{i,j}$, $t < j \le 2^s$, lze zafixovat nejvýše $(2n^{1/d} + 1)^{2^s - t} \ll_d n^{(2^s-t)/d}$ způsoby. Tím je určeno m. Polynomy

$\varphi(h_i, y)$ stupně $d-1$, kde h_i je parametr, splňují předpoklady tvrzení pro $d-1$, ovšem s n nahrazeným číslem $\lceil n^{(d-1)/d} \rceil$: Pro $|h_i| \le 2n^{1/d}$ pro koeficienty v $\varphi(h_i, y) = b_1(h_i)y^{d-1} + \cdots + b_{d-1}(h_i)y + b_d(h_i)$ podle lemmatu 251 platí $b_k(h_i) \ll_d n^{(k-1)/d} = (n^{(d-1)/d})^{(k-1)/(d-1)}$. Díky indukčnímu předpokladu má proto rovnice

$$\sum_{j=1}^{t} \varphi(h_i, y_{i,j}) = m \quad |y_{i,j}| \le 2n^{1/d} = 2\Big(n^{(d-1)/d}\Big)^{1/(d-1)}$$

nejvýše $\ll_d (n^{(d-1)/d})^{t/(d-1)-1} = n^{(t-d+1)/d}$ řešení. Násobnost čísla $z = z_i$ proto při fixovaných i a $h_1, \ldots, h_{2d}$ nepřesahuje

$$\ll_d n^{(t-d+1)/d} \cdot n^{(2^s-t)/d} = n^{(2^s-d+1)/d} \ .$$

Lemma 251 též vzhledem k $|h_i|, |y_{i,j}| \le 2n^{1/d}$ implikuje, že vždy $z_i \ll_d n^{(d-1)/d}$ $(1 \le i \le 2d)$.

Rekapitulujme: Pro uvedenou volbu $g = g_0(d)$ máme $w(n, N, g, f) \ll_d n^{g/2d-2}R$, kde R je počet řešení rovnice

$$\sum_{i=1}^{2d} h_i z_i = 0 \quad |h_i| \le 2n^{1/d}, |z_i| \ll_d n^{(d-1)/d} \ ,$$

v níž se při pevných $h_1, \ldots, h_{2d}$ každé z_i vybírá s jistou násobností nepřesahující $\ll_d n^{(2^s-d+1)/d}$. Jako S označíme počet řešení této rovnice pro z_i bez násobností. S odhadneme pomocí lemmatu 248, použitého pro $l = 2d$, $A = 2n^{1/d}$ a $B \ll_d n^{(d-1)/d}$ (horní mez pro $|z_i|$). Celkem dostáváme

$$\begin{aligned} w(n, N, g, f) &\ll_d n^{g/2d-2}R \ll_d n^{g/2d-2}\Big(n^{(2^s-d+1)/d}\Big)^{2d} S \\ &\ll_d n^{2^{s+1}-2} \cdot n^{2^{s+1}-2d+2} \cdot (n^{1/d} n^{(d-1)/d})^{2d-1} \\ &= n^{2^{s+2}-1} = n^{g/d-1} \ . \end{aligned}$$

Tvrzení 253 je dokázáno. ◊

Uvažme polynom x^d. Podle definic veličin $W(n, g, d)$ a $w(n, N, g, f)$ a podle předchozího tvrzení, pro $g = g_0(d)$ máme

$$W(n, g, d) \le w(n, n, g, x^d) \ll_d n^{g/d-1} \ .$$

Tím jsou tvrzení 245 a věta 246 dokázány.

7.6 Poznámky

7.1. Klasické číselné rozklady. Literatura: Hardy a Wright [47], Andrews [4], van Lint a Wilson [62] a Winquist [96].

O výsledcích a problémech aditivní teorie čísel podávají dobrý přehled Nathansonovy monografie [66, 67, 68] a Halberstam a Roth [42]. Různé aspekty analytické kruhové metody probírá Vaughan [91]. Základní literaturou o číselných rozkladech je Andrewsova monografie [4], jejíž autor sám věnoval teorii rozkladů více než 200 článků.

Mistrem kombinatoriky a číselných rozkladů byl na přelomu 19. a 20. století major britské armády P. MacMahon. Andrews se spoluautory rehabilitují v rozsáhlé sérii článků [5]–[13] MacMahonovy pozoruhodné avšak pozapomenuté výsledky. MacMahon v [63] mimo jiné zkoumal *r-rozměrné rozklady*. To jsou zobrazení $f : \mathbf{N}^r \to \mathbf{N}_0$, která mají jen konečně mnoho nenulových hodnot a splňují $f(i_1, \ldots, i_r) \geq f(j_1, \ldots, j_r)$ vždy, když $i_1 \leq j_1, \ldots, i_r \leq j_r$. Pokud $\sum_{x \in \mathbf{N}^r} f(x) = n$, řekneme, že f je r-rozměrný rozklad n. Nejdůležitější případy jsou $r = 1$, kdy dostáváme klasické číselné rozklady, a $r = 2$, kdy dostáváme *rovinné rozklady* (plane partitions). Rovinný rozklad n si můžeme představovat jako "třírozměrný Ferrersův diagram", což je takové umístění n jednotkových kostek v oktantu $K = \{(x, y, z) \in \mathbf{R}^3 :\ x \geq 0, y \leq 0, z \geq 0\}$ ($z = 0$ je vodorovná rovina), že hrany kostek jsou rovnoběžné s osami a každá kostka se celou levou, spodní a zadní stěnou dotýká hranice K nebo jiné kostky. Například, číslo 3 má šest rovinných rozkladů, které popíšeme počty kostek v jednotlivých sloupcích stojících na rovině $z = 0$:

$$
3, \quad 21, \quad \begin{matrix}2,\\1\end{matrix} \quad 111, \quad \begin{matrix}11\\1\end{matrix} \ \text{a} \ \begin{matrix}1\\1\\1\end{matrix}\,.
$$

Nechť $pp(n)$ je počet rovinných rozkladů čísla n. MacMahon dokázal, že

$$
\sum_{n \geq 0} pp(n) x^n = \prod_{n=1}^{\infty} \frac{1}{(1 - x^n)^n}\ .
$$

Na rozdíl od 1-rozměrných rozkladů není vůbec jednoduché tento součinový tvar odvodit a pro $r > 2$ obdobné formule selhávají. Kombinatorický důkaz podali Knuth a Bender [56]. Další informace o rovinných rozkladech lze nalézt v [4, kap. 11] a Stanleym [85, 86]. Pro další kombinatorické souvislosti rovinných rozkladů viz Bressoud [25].

S kombinačními čísly sdílejí koeficienty polynomu $\binom{a+b}{b}_q$ symetrii $p(n;a,b) = p(ab-n;a,b)$, která se lehce vidí, a unimodalitu $p(0;a,b) \leq p(1;a,b) \leq \ldots \leq p(\lfloor ab/2 \rfloor;a,b) \geq p(\lfloor ab/2 \rfloor + 1;a,b) \geq \ldots \geq p(ab;a,b)$, která se dlouho uměla dokázat jen algebraicky, např. pomocí teorie invariantů (Sylvester, 1878). Čistě kombinatorický důkaz podal O'Hara [73].

V oddílu 7.1 jsme pro $r = 1, 3, 6$ a 10 nalezli součtové vyjádření součinu $\prod_{n\geq 1}(1-x^n)^r$. Nejslavnější hodnotou r v tomto kontextu však je 24. Tehdy se dostane *Ramanujanova tau funkce* $\tau(n)$:

$$x\prod_{n=1}^{\infty}(1-x^n)^{24} = \sum_{n\geq 1}\tau(n)x^n = x - 24x^2 + 255x^3 - 1472x^4 + 4830x^5 + \cdots .$$

Ramanujan se domníval, že $\tau(n)$ je multiplikativní, a Mordell to v r. 1917 dokázal. Jinou Ramanujanovu domněnku, že vždy $|\tau(n)| < n^{11/2}d(n)$, kde $d(n)$ je počet dělitelů n, dokázal v r. 1974 Deligne [31] jako důsledek svého řešení Weilovy hypotézy. Viz Apostol [14], Katz [54], Koblitz [57] a Serre [82]. Lehmerova domněnka z r. 1947, že $\tau(n)$ není nikdy nulová, je stále otevřená.

Ramanujan původně vyslovil tuto hypotézu o kongruenčních vlastnostech $p(n)$: Je-li m tvaru $5^a7^b11^c$ a $24k \equiv 1 \bmod m$, potom $p(mn+k) \equiv 0 \bmod m$ pro každé $n \in \mathbf{N}_0$. Věta 224 je speciálním případem pro $m = 5, 7$ a 11. Ve třicátých letech 20. století však Chowla nalezl protipříklad: $24 \cdot 243 \equiv 1 \bmod 7^3$, ale $p(243) = 133978259344888 \not\equiv 0 \bmod 7^3$. V r. 1967 Atkin [16] dokázal správnou verzi Ramanujanovy domněnky: Pokud $m = 5^a7^b11^c$ $(a,b,c \in \mathbf{N}_0)$ a $24k \equiv 1 \bmod m$ $(k \in \mathbf{N})$, pak $p(mn+k) \equiv 0 \bmod 5^a7^{\lfloor b/2 \rfloor+1}11^c$ pro každé $n \in \mathbf{N}_0$. Atkin [17] též dokázal, že $p(206839n + 2623) \equiv 0 \bmod 17$.

Významné nové výsledky v teorii kongruenčních vlastností $p(n)$ získal Ono [74]. V [1] spolu s Ahlgrenem oznamují následující rozsáhlou třídu kongruencí. Pro prvočíslo $l \geq 5$ označme $\delta_l = (l^2-1)/24$ a S_l buď množina těch $k, 0 \leq k < l$, že $k + \delta_l \equiv 0 \bmod l$ nebo $\left(\frac{k+\delta_l}{l}\right) = -\left(\frac{-6}{l}\right)$ (užíváme Legendreův symbol). Potom pro každé prvočíslo $l \geq 5$, $m \in \mathbf{N}$ a $k \in S_l$ má kladná frakce prvočísel $q \equiv -1 \bmod 24l$ tu vlastnost, že

$$p((q^3n+1)/24) \equiv 0 \bmod l^m$$

pro všechna $n \in \mathbf{N}$ taková, že $n \perp q$ a $n \equiv 1 - 24k \bmod 24l$.

7.2. Součty dvou a čtyř čtverců. Literatura: Hirschhorn [49, 50].

V úloze 10 reprodukujeme Zagierův důkaz [101] toho, že každé prvočíslo $p = 4n+1$ je součtem dvou čtverců. Veličiny $r_g(n)$ vzhledem k započítávání všech pořadí a znamének zahrnují velikou redundanci. Například $r_4(30) = 8(1+2+3+5+6+10+15+30) = 576$, i když 30 má jen dva rozklady na čtyři nezáporné čtvercové části: $30 = 4^2+3^2+2^2+1^2$ a $30 = 5^2+2^2+1^2+0^2$. Hirschhorn [51] odvodil formule pro $p_{2\square}(n)$, $p_{3\square}(n)$ a $p_{4\square}(n)$, počty rozkladů n na dvě, tři a čtyři nezáporné čtvercové části. Například

$$p_{2\square}(n) = \frac{1}{2}\Big(d_1(n) - d_3(n) + \delta(n) + \delta(n/2)\Big) \ ,$$

kde $d_i(n)$ jsou jako ve větě 225 a $\delta(n) = 1$ pokud je n čtverec a 0 jinak.

Formule pro $r_2(n)$ a $r_4(n)$ odvodil Jacobi ve spisu *Fundamenta Nova Theoriae Functionum Ellipticarum* (1829) pomocí eliptických funkcí. První z nich se implicitně nachází už v Gaussových *Disquisitiones Arithmeticae* (1801). Formule

$$r_6(n) = 16\sum_{d\backslash n}\chi(n/d)d^2 - 4\sum_{d\backslash n}\chi(d)d^2 \quad \text{a} \quad r_8(n) = 16\sum_{d\backslash n}(-1)^{n+d}d^3 \ ,$$

kde $\chi(d) = (-1)^{(d-1)/2}$ pro liché d a $\chi(d) = 0$ pro sudé d, byly odvozeny rovněž v Jacobiho spisu. Pro sudé $g \geq 10$ platí komplikovanější formule, například

$$r_{10}(n) = \frac{4}{5}\Big(\sum_{d\backslash n}\chi(d)d^4 + 16\sum_{d\backslash n}\chi(n/d)d^4 + 4\sum_{a^2+b^2=n}(a^4 - 3a^2b^2)\Big) \ .$$

Pro liché g je problém určit $r_g(n)$ obtížnější. (Formule pro $r_5(n)$ sehrála důležitou úlohu v kariére H. Minkowskiho, viz kapitola 8.) Pro další informace o reprezentacích čísel čtverci viz Grosswald [41]. Významné nové výsledky o $r_g(n)$ získal nedávno v rozsáhlém memoáru Milne [65]. Jacobiho klasické identity pro $r_g(n)$ s $g = 4$ a 8 rozšířil na nekonečné rodiny identit pro $g = 4l^2$ a $g = 4l(l+1)$, $l \in \mathbf{N}$. Například pro $g = 24$ Milneho identita praví, že

$$\begin{aligned} r_{24}(n) &= (-1)^n\frac{16}{9}\Big(17\sigma_3^\dagger(n) + 8\sigma_5^\dagger(n) + 2\sigma_7^\dagger(n)\Big) \\ &\quad + (-1)^n\frac{512}{9}\sum_{m=1}^{n-1}\Big(\sigma_3^\dagger(m)\sigma_7^\dagger(n-m) - \sigma_5^\dagger(m)\sigma_5^\dagger(n-m)\Big) \ , \end{aligned}$$

kde

$$\sigma_k^\dagger(n) = \sum_{d\backslash n}(-1)^d d^k \ .$$

"Podivnou a mocnou" ([68]) elementární metodu, kterou v sérii osmnácti článků vyvinul v letech 1858–65 Liouville a kterou odvozoval formule pro $r_g(n)$ (g sudé), vysvětluje Nathanson [68, kap. 13 a 14] na hodnotách $g = 2, 4, 6, 8$ a 10. Metoda spočívá zhruba řečeno v ověření, že dokazovaná formule a $r_g(n)$ splňují tutéž rekurenci (uvedenou v úloze 11).

Reprezentace prvků součtem čtverců se zkoumají i v jiných okruzích než $\mathbf{Z}$. Například Landau v r. 1906 dokázal, že každý nezáporný *racionální* polynom $P \in \mathbf{Q}[x]$ (tj. $P(x) \geq 0$ pro všechna $x \in \mathbf{R}$) je v $\mathbf{Q}[x]$ součtem osmi čtverců. Kdy je nezáporný polynom $P \in \mathbf{R}[x_1, x_2, \ldots, x_n]$ součtem (nějakého počtu) čtverců v $\mathbf{R}[x_1, x_2, \ldots, x_n]$? (Stupeň $\deg(P) = d$ je nutně sudý.) Hilbert v r. 1888 dokázal, že odpověď zní "ano" pouze v případech $(n, d) \in \{(1, 2e) :\ e \in \mathbf{N}\} \cup \{(n, 2) :\ n \in \mathbf{N}\} \cup \{(2, 4)\}$. Pro ostatní dvojice (n, d), d sudé, existuje reálný polynom stupně d v n proměnných, který je vždy nezáporný, ale není součtem žádného počtu čtverců. Viz úloha 9 a Rudin [81]. Analogická otázka v tělese racionálních funkcí $\mathbf{R}(x_1, x_2, \ldots, x_n)$ představuje Hilbertův 17. problém. Ten v r. 1927 vyřešil Artin [15], když dokázal, že každá nezáporná racionální funkce $P \in \mathbf{R}(x_1, x_2, \ldots, x_n)$ je v tomto tělese součtem čtverců, a že totéz platí i v $\mathbf{Q}(x_1, x_2, \ldots, x_n)$. Viz Rajwade [76] a Taussky [89].

7.3. Další rozkladové identity. Literatura: Hardy a Wright [47], Corteel a Savage [29], Bousquet-Mélou a Eriksson [23] a Remmel [77].

Identity ve větě 227, nyní nazývané Rogers–Ramanujanovými, objevil a dokázal jako první Rogers [80]. Hardy o nich a o něm v knize [43] napsal:

> They were found first in 1894 by Rogers, a mathematician of great talent but comparatively little reputation, now remembered mainly from Ramanujan's rediscovery of his work. Rogers was a fine analyst, whose gifts were, on a smaller scale, not unlike Ramanujan's; but no one paid much attention to anything he did, and the particular paper in which he proved the formulae was quite neglected.

Ramanujan, který naopak patří k nejlegendárnějším a nejromantičtějším postavám příběhu matematiky, identity objevil nezávisle v Indii někdy před r. 1913. Neuměl je však dokázat a neuměl to ani Hardy, kterému je poslal, ani Littlewood, MacMahon a Perron, které Hardy konzultoval. Byly uvedeny bez důkazu v druhém dílu MacMahonova spisu [63]. V r. 1917 sám Ramanujan, pobývající nyní už v Cambridge a intenzivně spolupracující s Hardym, náhodou narazil na Rogersův článek. V následné korespondenci Rogers zjednodušil svůj přes 20 let starý důkaz. Zhruba ve stejné době identity nezávisle znovu objevil Schur [83], izolovaný v Německu válkou.

Rogers–Ramanujanovy identity inspirovaly mnohá zobecnění a mnohé příbuzné identity. Uvádíme tři příklady. Gordon [40] dokázal, že pro pevné $a, k \in \mathbf{N}$, $a \leq k$, má každé $n \in \mathbf{N}$ tolik rozkladů na části $\not\equiv 0, \pm a \bmod 2k+1$ jako rozkladů na části $b_1 \geq b_2 \geq \ldots \geq b_j \geq 1$ splňující $b_i - b_{i+1} \geq 1$, $b_i - b_{i+k-1} \geq 2$ a $b_{j-a+1} \geq 2$. Pro důkaz a další zobecnění viz [4, kap. 7]. Andrews [3] dokázal, že každé $n \in \mathbf{N}$ má tolik rozkladů na části $\equiv 1, 9, 11 \bmod 14$ jako rozkladů $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ splňujících $\lambda_i - \lambda_{i+1} \geq 7$ pro $\lambda_{i+1} \equiv 1, 2, 4 \bmod 7$, $\lambda_i - \lambda_{i+1} \geq 10$ pro $\lambda_{i+1} \equiv 5, 6 \bmod 7$, $\lambda_i - \lambda_{i+1} \geq 12$ pro $\lambda_{i+1} \equiv 3 \bmod 7$ a $\lambda_i - \lambda_{i+1} \geq 15$ pro $\lambda_{i+1} \equiv 0 \bmod 7$. Andrews [2] dokázal i toto "zkonečnění" Rogers–Ramanujanových identit: Pro každé $m \in \mathbf{N}$ a $a = 0, 1$ platí

$$\sum_{n=0}^{\infty} q^{n(n+a)} \binom{m-n-a}{n}_q = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(5n+2a+1)/2} \binom{m}{\lfloor (m-5n-a)/2 \rfloor}_q .$$

(Rogers–Ramanujanovy identity odtud plynou limitním přechodem $m \to \infty$ a pomocí JTI.) Rogers–Ramanujanovy a jim příbuzné identity mají důležité místo při studiu modelů statistické fyziky, hlavně v tzv. "hard hexagon model", viz Baxter [19, 20]. O těchto použitích číselných rozkladů ve fyzice viz např. Berkoich a McCoy [21].

Identitu pro divácké rozklady objevili a dokázali Bousquet-Mélou a Eriksson [22] (v [23] je dokázána obecnější verze tvrzení 230). Jiný důkaz podal brzy Andrews [5]. Zde sledujeme podání Corteelové a Savageové [29]. Viz též Bousquet-Mélou a Eriksson [24].

Větu 232 dokázal Remmel v [77], její disjunktní forma se v jiné formulaci objevuje už u Cohena [28] a celá věta je implicitně obsažena v Cohenově přístupu. Princip involuce použili Garsia a Milne [37] ke kombinatorickému důkazu Rogers–Ramanujanových identit. Mnohem kratší kombinatorický důkaz podali Bressoud a Zeilberger [26]. Glaisherova identita je z r. 1883 ([39]) a Schurova z r. 1926 ([84]).

7.4. Asymptotika partitní funkce. Literatura: Newman [71, 72].

Po Hardym a Ramanujanovi [46] asymptotiku $p(n)$ nalezl nezávisle Uspensky [90]. Hardy a Ramanujan však v [46] dokonce nalezli asymptotický rozvoj $p(n)$, který Rademacher [75] vylepšil na konvergentní řadu:

$$p(n)=\frac{1}{\pi\sqrt{2}}\sum_{k=1}^{\infty}A_k(n)k^{1/2}\left[\frac{d}{dx}\frac{\sinh\left(\frac{\pi}{k}(\frac{2}{3}(x-\frac{1}{24}))^{1/2}\right)}{(x-\frac{1}{24})^{1/2}}\right]_{x=n},$$

kde

$$A_k(n)=\sum_{h \bmod k,\ h\perp k}\mathrm{e}^{-2\pi i\cdot nh/k+\pi i\cdot s(h,k)},$$

přičemž

$$s(h,k)=\sum_{\mu=1}^{k-1}\left(\frac{\mu}{k}-\left\lfloor\frac{\mu}{k}\right\rfloor-\frac{1}{2}\right)\left(\frac{h\mu}{k}-\left\lfloor\frac{h\mu}{k}\right\rfloor-\frac{1}{2}\right).$$

Toto je slavná Hardy–Ramanujan-Rademacherova formule (HRR formule) pro $p(n)$. Rademacher v [75] též ukázal, že po ukončení nekonečné řady po $k=r$ členech se součet liší od $p(n)$ nejvýše o

$$\frac{2\pi^2}{9\sqrt{3}}\exp((2n/3)^{1/2}\pi/(r+1))\cdot r^{-1/2}.$$

Asymptotika věty 237 se dostane hned z prvního členu $k=1$ řady. Důkaz HRR formule, přesněji jeho druhou polovinu, lze nalézt v [4, kap. 5]. První polovinu důkazu představuje skutečnost, že po změně proměnné $z=\mathrm{e}^{2\pi iy}$, $|z|<1$ a (ekvivalentně) $\mathrm{Im}(y)>0$, se ze součinu $\prod_{n\ge1}(1-z^n)$ dostane modulární forma

$$\eta(y)=z^{1/24}\prod_{n=1}^{\infty}(1-z^n),$$

tzv. *Dedekindova eta funkce*. Její modularita se projevuje funkcionálními rovnicemi $\eta(y+1)=\mathrm{e}^{\pi i/12}\eta(y)$ a $\eta(-1/y)=\sqrt{-iy}\cdot\eta(y)$ (bere se $\sqrt{\ }$ s nezápornou reálnou částí). O modulárních funkcích a formách viz [14, 57, 82].

Erdős [35] skoro celou asymptotiku $p(n)$ odvodil elementárně. Jeho postup vychází z rekurence uvedené v úloze 3. Dokázal, že pro $n\to\infty$

$$p(n)\sim\frac{c}{n}\cdot\mathrm{e}^{\pi(2n/3)^{1/2}}$$

s neznámou konstantou $c>0$. Newman [69] ji elementárně dopočítal jako $c=1/4\sqrt{3}$. Erdős a Lehner [36] dokázali, že pro hodnotu $k=c\sqrt{n}\cdot\log n+x\sqrt{n}$ ($c,x>0$ jsou konstanty) počet rozkladů čísla n na nejvýše k částí splňuje

$$\lim_{n\to\infty}\frac{p(n;k)}{p(n)}=\exp\left(-2c\cdot\mathrm{e}^{-x/(2c)}\right).$$

Téměř všechny rozklady n tedy mají zhruba $c\sqrt{n} \cdot \log n$ částí.

Szekeres [87, 88] rozšířil Hardyho–Ramanujanovu asymptotiku na asymptotiku počtů $p^*(n;k)$ rozkladů n na přesně k částí, přičemž $k, n \to \infty$ a $k \geq n^{1/6}$. Canfield [27] podal elementární důkaz Szekeresovy asymptotiky bez použití komplexní analýzy. Szekeresova asymptotika je jediný známý způsob, jak pro dostatečně velké n dokázat unimodalitu posloupnosti $(p^*(n;k))_{k=1}^n$: $p^*(n;1) \leq p^*(n;2) \leq \ldots \leq p^*(n;m) \geq p^*(n;m+1) \geq \ldots \geq p^*(n;n)$.

Wright [100] zkombinoval asymptotiku $p(n)$ s Waringovým problémem a nalezl asymptotiku počtu rozkladů $p_k(n)$ čísla n na k-té mocniny přirozených čísel (počet částí není omezen, $k \geq 1$ je pevné, $p_1(n) = p(n)$):

$$p_k(n) \sim \frac{\Delta}{(2\pi)^{(k+1)/2}} \cdot \frac{k^{1/2}}{(k+1)^{3/2}} \cdot n^{\frac{1}{k+1} - \frac{3}{2}} \cdot \mathrm{e}^{\Delta n^{1/(k+1)}} ,$$

kde

$$\Delta = (k+1) \cdot \Big((1/k) \cdot \Gamma(1 + 1/k) \cdot \zeta(1 + 1/k)\Big)^{1-1/(k+1)}$$

($\Gamma(z) = \int_0^\infty \mathrm{e}^{-t} t^{z-1}\, dt$ je gama funkce a $\zeta(z) = \sum_{n \geq 1} n^{-z}$ je zeta funkce). Wright pro $p_k(n)$ dokonce odvodil asymptotický rozvoj, zbytek řady však pro $k > 1$ (na rozdíl od HRR formule pro $k = 1$) nekonverguje k nule.

7.5. Linnikovo řešení Waringova problému. Literatura: Gelfond a Linnik [38].

Waringův problém se těšil a těší velkému zájmu matematiků. Kvantitativně to znamená, že třeba bibliografie knihy [91] čítá přes 700 položek. Zajímavý přehledový článek sepsal Ellison [34]. Původní Waringova formulace v [93, str. 203–204] zní:

> Omnis integer numerus vel est cubus; vel e duobus, tribus, 4, 5, 6, 7, 8, vel novem cubus compositus: est etiam quadratoquadratus; vel e duobus, tribus &c. usque at novemdecim compositus &sic deinceps.

Waringovu domněnku dokázal jako první Hilbert [48] v r. 1909. Zjednodušené verze jeho důkazu založeného na algebraických identitách lze nalézt v [34] a [66]. Rieger [78] ukázal, že Hilbertova metoda vede na odhad $g(d) \leq (2d+1)^{260(d+3)^{3d+8}}$. Linnikův elementární důkaz [60] založený na Šnirelmanově metodě jsme vyložili (nikoli doslovně) podle [38, kap. 2], viz též Chinčin [53]. Obecnější verzi lze nalézt v Nathansonovi [68]. Rieger [79] z Linnikovy metody získal odhad $g(d) \leq 2^{2 \cdot 16^d (d+1)!}$. Newman se pokusil o technicky co nejjednodušší důkaz Waringovy domněnky za pomoci kombinace Šnirelmanovy metody s exponenciálními sumami (odhad v tvrzení 245 dokazuje pomocí jednoduché verze tzv. Weylovy nerovnosti). Bohužel jak důkaz v [70] tak i jeho prezentace v [72, kap. 5] obsahují mezery.

Ve dvacátých letech 20. století Hardy a Littlewood, navazujíc na [46], v sérii článků (viz např. [44, 45]) vyvinuli mocnou analytickou metodu, která poskytuje silné horní odhady $G(d)$ a kterou lze nasadit v mnoha dalších aditivních úlohách. "Kruhovou" neboli Hardy–Littlewoodovu metodu jsme už v jednoduché podobě použili v 6.4 k důkazu věty 209 a v 7.4 k důkazu věty 237. Hardy a Littlewood vyjádřili $W(n,g,d)$ pomocí Cauchyho věty jako

$$W(n,g,d) = \frac{1}{2\pi i}\int_C F(z)^g z^{-n-1}\,dz\ ,$$

kde $F(z) = \sum_{m\ge 0} z^{m^d}$ a C je kružnice $\rho e^{2\pi i\alpha}$, v níž α probíhá $[0,1)$ a poloměr ρ splňuje $0 < \rho < 1$. Další postup je v kostce ten, že se vhodně položí $\rho \to 1^-$ (např. $\rho = 1 - 1/n$) a interval $[0,1)$ se vhodně rozdělí na úsečky dvou druhů: na tzv. hlavní úsečky (major arcs), v nichž je α dobře aproximováno zlomkem s relativně malým (v závislosti na n) jmenovatelem, a na zbylé tzv. vedlejší úsečky (minor arcs). Příspěvek integrálu přes hlavní úsečky vytvoří hlavní člen asymtotické formule pro $W(n,g,d)$. Příspěvek přes vedlejší úsečky se shora odhadne Weylovou nerovností pro exponenciální sumy, což vytvoří zbytkový člen. Hardy a Littlewood takto za předpokladu $g \ge 2^d + 1$ odvodili asymptotiku

$$W(n,g,d) = \frac{\Gamma(1+1/d)^g}{\Gamma(g/d)} \cdot S(n) \cdot n^{g/d-1} + O(n^{g/d-1-\delta})\ ,$$

kde $\delta > 0$ a $S(n)$ je jistá aritmetická funkce splňující $c_1 > S(n) > c_2 > 0$ (konstanty c_i závisí jen na g a d). Speciálně, $G(d) \le 2^d + 1$. Viz [66] nebo [91].

Vinogradov v r. 1928 zavedl řadu zlepšení kruhové metody, z nichž jedno spočívá v nové reprezentaci

$$W(n,g,d) = \int_0^1 f(\alpha)^g e(-\alpha n)\,d\alpha\ ,$$

kde $e(x) = e^{2\pi i x}$, $f(\alpha) = \sum_{m=0}^{N} e(\alpha m^d)$ a $N = \lfloor n^{1/d} \rfloor$ (tato identita plyne z ortogonality $\int_0^1 e(\alpha h)\ d\alpha = 0$ pro $h \ne 0$ a $= 1$ pro $h = 0$). Dokázal, že hořejší asymptotika $W(n,g,d)$ platí už pro $g > cd^2 \log d$. Vinogradovův odhad $G(d) \leq (2+o(1))d\log d$ z [92] byl nepřekonán po více než 30 roků. V r. 1992 rekord putoval díky Wooleymu [97] do Michiganu a současný nejlepší odhad $G(d) \leq d(\log d + \log\log d + 2 + O(\log\log d/\log d))$ náleží též Wooleymu [98]. Zasvěcený přehled o klasickém i moderním rozvoji kruhové metody (s důrazem na Waringův problém) podává Vaughan [91], viz též Wooley [99].

Silné horní odhady $G(d)$ spolu s obtížným vyšetřením "malých" n vedly k téměř přesnému určení funkce $g(d)$. Je lehké dokázat, že $g(d) \geq 2^d + \lfloor (3/2)^d \rfloor - 2$ (úloha 19). V sérii prací Dicksona, Pillaie, Rubugundaye a Nivena publikovaných v letech 1928–44 bylo dokázáno, že pro $d \geq 6$ platí

$$g(d) = \begin{cases} 2^d + \lfloor (3/2)^d \rfloor - 2 & \dots \text{ pokud } \alpha \leq 2^d \\ 2^d + \lfloor (3/2)^d \rfloor + \lfloor (4/3)^d \rfloor - 2 & \dots \text{ pokud } \alpha > 2^d \text{ a } \beta = 2^d \\ 2^d + \lfloor (3/2)^d \rfloor + \lfloor (4/3)^d \rfloor - 3 & \dots \text{ pokud } \alpha > 2^d \text{ a } \beta > 2^d \end{cases},$$

kde

$$\alpha = 2^d\{(3/2)^d\} + \lfloor (3/2)^d \rfloor \ \text{ a } \ \beta = \lfloor (4/3)^d \rfloor \lfloor (3/2)^d \rfloor + \lfloor (4/3)^d \rfloor + \lfloor (3/2)^d \rfloor .$$

(Snadno se nahlédne, že vždy $\beta \geq 2^d$.) Kubina a Wunderlich [58] pomocí počítače dokázali, že pro každé $6 \leq d \leq 4.716 \cdot 10^8$ nastává první možnost. Mahler [64] dokázal, že druhá a třetí možnost nastávají jen pro konečně mnoho d. Podívejme se na zbývající tři hodnoty $g(3), g(4)$ a $g(5)$ ($g(2) = 4$ podle Lagrange). Výše citovaný Waringův text ve stručné parafrázi praví, že $g(3) \leq 9$, $g(4) \leq 19$ "a tak dál". Wieferich [95] v r. 1909 dokázal, že $g(3) = 9$. Chybu v jeho důkazu opravil Kempner [55]. Chen [52] v r. 1964 ukázal, že $g(5) = 37$. Nejdéle odolávající bikvadráty se nakonec poddaly v r. 1992, kdy společným úsilím Balasubramaniana [18] a Deshouillerse a Dresse [32] bylo dokázáno, že skutečně $g(4) = 19$. Formule $g(d) = 2^d + \lfloor (3/2)^d \rfloor - 2$ tedy platí i pro $d < 6$.

V kontrastu s $g(d)$ jsou známy pouze dvě přesné hodnoty $G(d)$: $G(2) = 4$ (Lagrange, 1770) a, poněkud paradoxně, $G(4) = 16$ (Davenport [30], 1939). Landau [59] dokázal, že $G(3) \leq 8$. Dickson [33] ukázal, že 23 a 239 jsou jediná přirozená čísla, která nejsou součtem osmi (nezáporných) třetích mocnin. Linnik [61] dokázal, že $G(3) \leq 7$. Watson [94] podal jednodušší důkaz Linnikova výsledku. Watsonův důkaz a další výsledky o třetích mocninách lze nalézt v [66, kap. 2]. Lehce se vidí, že $G(3) \geq 4$ (úloha 20c). Přes veškeré úsilí se o $G(3)$ stále ví jen to, že $4 \leq G(3) \leq 7$. Podle [99], kde lze nalézt příslušné reference, jsou nejlepší v současnosti známé horní odhady $G(d)$ pro $d \leq 20$ tyto: $G(5) \leq 17, G(6) \leq 24, G(7) \leq 33, G(8) \leq 42, G(9) \leq 50, G(10) \leq$

$59, G(11) \leq 67, G(12) \leq 76, G(13) \leq 84, G(14) \leq 92, G(15) \leq 100, G(16) \leq 109, G(17) \leq 117, G(18) \leq 125, G(19) \leq 134$ a $G(20) \leq 142$.

7.7 Úlohy

1. Nechť $n \in \mathbf{N}$.

   (a) (**2**) Dokažte, že n má 2^{n-1} kompozic.

   (b) (**2**) Nalezněte počet kompozic n na g kladných částí, resp. na g nezáporných částí. (Druhý počet je právě hodnota funkce $W(n, g, 1)$ z oddílu 7.5.)

   (c) (**2**) Nalezněte počet kompozic n, které nepoužívají část 1.

   (d) (**2**) Nalezněte rozdíl mezi počtem kompozic n na sudý počet částí a počtem kompozic na lichý počet částí.

2. Množinové rozklady — vyjádření dané množiny ve tvaru sjednocení vzájemně disjunktních neprázdných množin — mají v kombinatorice důležité místo. Uvedeme proto na ně jednu úlohu. *Párování* M na množině $[2n] = \{1, 2, \ldots, 2n\}$ je její rozklad na n dvouprvkových množin, kterým říkáme *hrany*. Dvě různé hrany $B_1 = \{a, b\}$, $a < b$, a $B_2 = \{c, d\}$, $c < d$, párování M se *kříží*, pokud $a < c < b < d$ nebo $c < a < d < b$. *Počet křížení* $c(M)$ je počet dvojic $\{B_1, B_2\}$ křížících se hran v M. Množinu všech párování na $[2n]$ označíme $M(n)$.

   (a) (**1**) Nalezněte kardinalitu množiny $M(n)$.

   (b) (**3**) Nalezněte počet těch $M \in M(n)$, že $c(M)$ je liché.

   (c) (**3**) Nalezněte počet těch $M \in M(n)$, že $c(M) = 0$.

   (d) (**1**) Nalezněte počet těch $M \in M(n)$, že $c(M)$ je maximální možné.

   (e) (**4**) Dokažte, že

   $$\sum_{M \in M(n)} q^{c(M)} = \frac{1}{(1-q)^n} \sum_{k=-n}^{n} \binom{2n}{n-k} (-1)^k q^{k(k-1)/2} .$$

3. (**2**) Dokažte, že partitní funkce splňuje rekurenci

   $$np(n) = \sum_{i=1}^{n} p(n-i)\sigma(i) ,$$

kde $\sigma(i)$ je součet dělitelů čísla i.

4. Tři úlohy na Ferrersovy diagramy.

   (a) (**2**) Nechť a, b, c jsou přirozená čísla, přičemž $b, c < a$. Dokažte, že číslo $a - c$ má tolik rozkladů na $b - 1$ částí nepřesahujících c, jako má číslo $a - b$ rozkladů na $c - 1$ částí nepřesahujících b.

   (b) (**2**) Dokažte, že každé $n \in \mathbf{N}$ má tolik samokonjugovaných rozkladů jako rozkladů na různé liché části.

   (c) (**2**) Dokažte identitu

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

5. (a) (**2**) Nechť p^r, $r \in \mathbf{N}$, je mocnina prvočísla, $n \in \mathbf{N}$ a V je n-rozměrný vektorový prostor nad konečným tělesem $\mathrm{GF}(p^r)$. Spočtěte, že V má právě

$$\binom{n}{k}_{q=p^r}$$

   k-rozměrných podprostorů.

   (b) (**3**) Dokažte předchozí výsledek převedením na kombinatorickou interpretaci $\binom{n}{k}_q$ v tvrzení 214.

6. (**2**) Dokažte q-binomickou větu

$$(1+x)(1+xq)(1+xq^2)\ldots(1+xq^{n-1}) = \sum_{i=0}^{n} x^i q^{\binom{i}{2}} \binom{n}{i}_q .$$

7. (**3**) Dokažte Jacobiho třísoučinovou identitu (věta 216) algebraicky podle následujícího návodu. Označíme-li nekonečný součin vlevo jako $P(x, z)$, platí $P(x, z) = P(x, z^{-1})$ a $P(x, x^2 z) = (xz)^{-1} P(x, z)$. Odtud plyne, že $P(x, z) = a(x) \sum_{-\infty}^{\infty} x^{n^2} z^n$ pro neznámou mocninnou řadu $a(x)$. Ovšem $a(0) = 1$ a specializace $z = i$ ukazuje, že $a(x^4) = a(x)$. Proto $a(x) = 1$. Proveďte tento důkaz podrobně bez analytické konvergence jen za pomoci formální algebraické konvergence mocninných řad.

8. (**2**) Odvoďte identitu 1 věty 215 z Jacobiho třísoučinové identity.

9. (**3**) Dokažte, že každý reálný polynom, který na reálných číslech nabývá jen nezáporných hodnot (a je tak nutně sudého stupně), je součtem dvou čtverců reálných polynomů.

10. (**2**) Vyznejte se v následujícím textu, který jednou gramatickou větou popisuje důkaz toho, že každé prvočíslo $p \equiv 1 \bmod 4$ je součtem dvou čtverců.

    The involution on the finite set $S = \{(x,y,z) \in \mathbf{N}^3:\ x^2 + 4yz = p\}$ defined by

    $$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) & \text{if } x < y-z \\ (2y-x, y, x-y+z) & \text{if } y-z < x < 2y \\ (x-2y, x-y+z, y) & \text{if } x > 2y \end{cases}$$

    has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x,y,z) \mapsto (x,z,y)$ also has a fixed point. $\square$

11. (**3**) Nechť $g, n \in \mathbf{N}$. Dokažte identitu

    $$\sum_{|m| \le \sqrt{n}} (n-(g+1)m^2) \cdot r_g(n-m^2) = 0\ .$$

12. (**2**) Nechť $(F_n)_{n\ge1} = (1,2,3,5,8,13,21,\ldots)$ je posloupnost Fibonacciových čísel a $(G_n)_{n\ge0} = (F_{2n-1}+F_{2n+1})_{n\ge0} = (1,4,11,29,76,\ldots)$, kde $F_{-1}=0$. Dokažte, že každé $n \in \mathbf{N}$ má tolik rozkladů na různé části $\lambda_1 > \lambda_2 > \ldots > \lambda_k \ge 1$ splňující $\lambda_i/\lambda_{i+1} > (3+\sqrt{5})/2$ jako rozkladů na části ležící v posloupnosti $(G_n)_{n\ge0}$.

13. (**2**) Nechť α, β a f jsou jako v tvrzení 231. Definujte pomocí nich bijekci mezi množinami pevných bodů F_α a F_β.

14. Dvě úlohy na větu 232.

    (a) (**3**) Dokažte její obrácení v disjunktním případě: Jsou-li $\mathcal{A} = (A_i)_{i\ge1}$ a $\mathcal{B} = (B_i)_{i\ge1}$ dvě prosté posloupnosti *disjuntních* konečných multipodmnožin $\mathbf{N}$ a pro každé $n \in \mathbf{N}$ platí $p(n,\mathcal{A}) = p(n,\mathcal{B})$, potom se posloupnosti $(\|A_i\|)_{i\ge1}$ a $(\|B_i\|)_{i\ge1}$ liší jen přerovnáním.

(b) (**1**) Ukažte, že každé $n \in \mathbf{N}$ má jednoznačný rozklad na různá a nesousední Fibonacciova čísla $(F_n)_{n\geq 0} = (1, 1, 2, 3, 5, 8, 13, 21, \ldots)$; například $12 = 8 + 3 + 1$ nebo $29 = 21 + 5 + 2 + 1$.

15. Dokažte Glaisherovu identitu (tvrzení 234) bez použití věty 232

    (a) (**2**) bijekcí

    (b) (**2**) pomocí generujících funkcí.

16. (**3**) Připomínáme, že $p^*(n; k)$ je počet rozkladů n na právě k částí. Pro pevné k a $n \to \infty$ dokažte asymptotiku

$$p^*(n; k) \sim \frac{n^{k-1}}{k!(k-1)!} \ .$$

17. Připomínáme, že $p(n; k)$ je počet rozkladů n na nejvýše k částí. Odvoďte následující formule.

    (a) (**1**) $p(n; 1) = 1$ a $p(n; 2) = 1 + \lfloor n/2 \rfloor$.

    (b) (**2**) $p(n; 3) = \|(n + 3)^2/12\|$ ($\| \cdot \|$ označuje nejbližší celé číslo).

    (c) (**3**) $p(n; 4) = \|(n + 5)(n^2 + n + 22 + 18\lfloor n/2 \rfloor)/144\|$.

    (d) (**3**) $p(n; 5) = \|(n + 8)(n^3 + 22n^2 + 44n + 248 + 180\lfloor n/2 \rfloor)/2880\|$.

18. Pro reálné číslo $t, 0 < t < 1$, označíme $f(t) = \log\left(\sum_{n\geq 0} p(n)t^n\right)$.

    (a) (**2**) Dokažte, že $f(t) < \frac{\pi^2}{6} \cdot \frac{t}{t-1}$.

    (b) (**3**) Odvoďte z předchozí nerovnosti, že pro $n > 2$

$$p(n) < \frac{\pi}{(6n - 6)^{1/2}} \cdot \mathrm{e}^{\pi(2n/3)^{1/2}} \ .$$

19. (**1**) Dokažte, že pro každé $d \in \mathbf{N}$ platí

$$g(d) \geq 2^d + \left\lfloor \left(\frac{3}{2}\right)^d \right\rfloor - 2 \ .$$

20. (a) (**2**) Nechť $n, z \in \mathbf{N}$, $z \equiv 1 \bmod 6$, a celá čísla r, s jsou definována vztahy $n \equiv 6r \bmod z^3, 1 \leq r \leq z^3$, a $n \equiv s + 4 \bmod 6, 0 \leq s \leq 5$. Dokažte, že $(r+1)^3+(r-1)^3+2(z^3-r)^3+(sz)^3 \equiv n-8z^9 \bmod 6z^3$.

(b) (**3**) Pomocí předchozí kongruence a identity

$$8x^9 + 6x^3(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \sum_{i=1}^{4} (x^3 + y_i)^3 + (x^3 - y_i)^3$$

odvoďte, že $G(3) \leq 13$.

(c) (**3**) Ukažte, že $G(3) \geq 4$.

(d) (**2**) Pomocí identity

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

odvoďte, že $g(4) \leq 53$.

Literatura

[1] S. Ahlgren and K. Ono, Congruence properties of the partition function, *Proc. Natl. Acad. Sci. USA,* **98** (2001), 12882–12884.

[2] G. E. Andrews, A polynomial identity which implies the Rogers–Ramanujan identities, *Scripta Math.,* **28** (1970), 297–305.

[3] G. E. Andrews, Partition identities, *Advances in Math.,* **9** (1972), 10–51.

[4] G. E. Andrews, *The Theory of Partitions,* Addison-Wesley, Reading, MA 1976.

[5] G. E. Andrews, MacMahon's partition analysis. I: The lecture hall partition theorem, 1–22. In: B. E. Sagan et al. (ed.), *Mathematical Essays in Honor of Gian-Carlo Rota's 65th Birthday (Cambridge, MA, 1996)*, Birkhäuser, Boston, MA, 1998.

[6] G. E. Andrews, MacMahon's partition analysis. II: Fundamental theorems, *Ann. Comb.,* **4** (2000), 327–338.

[7] G. E. Andrews, P. Paule and A. Riese, MacMahon's partition analysis III: The Omega package, *European J. Combin.,* **22** (2001), 887–904.

[8] G. E. Andrews and P. Paule, MacMahon's partition analysis. IV. Hypergeometric multisums, *Sém. Lothar. Combin.,* **42** (1999), 24 pages.

[9] G. E. Andrews, P. Paule, A. Riese and V. Strehl, MacMahon's partition analysis. V: Bijections, recursions and magic squares, 1–31. In: A. Beten et al. (ed.), *Algebraic Combinatorics and Applications (Gößweinstein, 1999)*, Springer, Berlin 2001.

[10] G. E. ANDREWS, P. PAULE AND A. RIESE, MacMahon's partition analysis. VI: A new reduction theorem, *Ann. Comb.,* **5** (2002), 251–270.

[11] G. E. ANDREWS, P. PAULE AND A. RIESE, MacMahon's partition analysis. VII: Constrained compositions, 11–27. In: B. Berndt et al. (ed.), *q-series with Applications to Combinatorics, Number Theory, and Physics*, American Math. Society, Providence, RI 2001.

[12] G. E. ANDREWS, P. PAULE AND A. RIESE, MacMahon's partition analysis. VIII: Plane partitions diamonds, *Adv. Appl. Math.,* **27** (2001), 231–242.

[13] G. E. ANDREWS, P. PAULE AND A. RIESE, MacMahon's partition analysis IX: k-gon partitions, *Bull. Austral. Math. Soc.,* **64** (2001), 321–329.

[14] T. M. APOSTOL, *Modular Functions and Dirichlet Series in Number Theory,* Springer-Verlag, New York 1997.

[15] E. ARTIN, Über die Zerlegung definiter Funktionen in Quadrate, *Hamb. Abh.,* **5** (1927), 100–115.

[16] A. O. L. ATKIN, Proof of a conjecture of Ramanujan, *Glasgow Math. J.,* **8** (1967), 14–32.

[17] A. O. L. ATKIN, Congruence Hecke operators, *Proc. Symp. Pure Math.,* **12** (1969), 33–40.

[18] R. BALASUBRAMANIAN, On Waring's problem: $g(4) \leq 20$, *Hardy–Ramanujan J.,* **8** (1985), 1–40.

[19] R. J. BAXTER, Hard hexagons: exact solution, *J. Phys. A,* **13** (1980), L61–L80.

[20] R. J. BAXTER, Rogers–Ramanujan identities in the hard hexagon model, *J. Stat. Phys.,* **26** (1981), 427–452.

[21] A. BERKOICH AND B. M. MCCOY, Rogers–Ramanujan identities: a century of progress from mathematics to physics, 163–172. In: A. K. Louis, U. Rehmann and P. Schneider (ed.), *Proceedings of the 1998 ICM, Vol. 3*, Documenta Mathematica, Berlin 1998.

[22] M. Bousquet-Mélou and K. Eriksson, Lecture hall partitions, *The Ramanujan J.,* **1** (1997), 101–111.

[23] M. Bousquet-Mélou and K. Eriksson, Lecture hall partitions 2, *The Ramanujan J.,* **1** (1997), 165–185.

[24] M. Bousquet-Mélou and K. Eriksson, A refinement of the lecture hall theorem, *J. Combinatorial Th., Ser. A,* **86** (1999), 63–84.

[25] D. M. Bressoud, *Proofs and Confirmations: The Story of the Alternating Sign Matrix Conjecture,* Cambridge University Press, Cambridge, UK 1999.

[26] D. M. Bressoud and D. Zeilberger, A short Rogers–Ramanujan bijection, *Discrete Math.,* **38** (1982), 313–315.

[27] E. R. Canfield, From recursion to asymptotics: On Szekeres' formula on the number of partitions, *Electr. J. Combin.,* **4** (1997), R6, 16 stran.

[28] D. I. A. Cohen, PIE-sums: a combinatorial tool for partition theory, *J. Combinatorial Th., Ser. A,* **31** (1981), 223–236.

[29] S. Corteel and C. D. Savage, Partitions and compositions defined by (in)equalities, Proceedings of FPSAC'02, 2002.

[30] H. Davenport, On Waring's problem for fourth powers, *Ann. Math.,* **40** (1939), 731–747.

[31] P. Deligne, La conjecture de Weil, *Inst. Hautes Etudes Sci. Publ. Math.,* **43** (1974), 273–307.

[32] J.-M. Deshouillers and F. Dress, Sums of 19 biquadrates: On the representation of large integers, *Annali Scuola Normale Super. Pisa,* **19** (1992), 113–153.

[33] L. E. Dickson, All integers except 23 and 239 are sums of eight cubes, *Bull. Am. Math. Soc.,* **45** (1939), 588–591.

[34] W. J. Ellison, Waring's problem, *Amer. Math. Monthly,* **78** (1971), 10–36.

[35] P. Erdős, On an elementary proof of some asymptotic formulas in the theory of partitions, *Ann. Math.,* **43** (1942), 437–450.

[36] P. Erdős and I. Lehner, The distribution of the number of summands in the partitions of a positive integer, *Duke. Math. J.,* **8** (1941), 335–345.

[37] A. M. Garsia and S. C. Milne, A Rogers–Ramanujan bijection, *J. Combinatorial Th., Ser. A,* **31** (1981), 289–339.

[38] A. O. Gelfond i Ju. V. Linnik, *Elementarnyje Metody v Analytičeskoj Tĕorii Čisel,* Fizmatgiz, Moskva 1962.

[39] J. W. L. Glaisher, A theorem in partitions, *Messenger of Math.,* **12** (1883), 158–170.

[40] B. Gordon, A combinatorial generalization of the Rogers-Ramanujan identities, *Amer. J Math.,* **83** (1961), 393–399.

[41] E. Grosswald, *Representations of Integers as Sums of Squares,* Springer-Verlag, New York 1985.

[42] H. Halberstam and K. F. Roth, *Sequences,* Oxford University Press, Oxford 1966. [Reprint v r. 1983 v Springer-Verlag.]

[43] G. H. Hardy, *Ramanujan: Twelve Lectures on Subjects Suggested by his Life and Work,* Cambridge University Press, London and New York 1940.

[44] G. H. Hardy and J. E. Littlewood, Some problems of "Partitio numerorum". I A new solution of Waring's problem, *Göttingen Nachrichten,* (1920), 33–54.

[45] G. H. Hardy and J. E. Littlewood, Some problems of "Partitio numerorum". II Proof that every large number is a sum of at most 21 biquadrates, *Math. Z.,* **9** (1921), 14–27.

[46] G. H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc (2),* **17** (1918), 75–115.

[47] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* Oxford University Press, Oxford 1945. [Tato klasická učebnice se dočkala od r. 1938 celkem 5 vydání, posledního v roce 1979.]

[48] D. Hilbert, Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem), *Math. Annalen,* **67** (1909), 281–300. [Viz též: *Gesammelte Abhandlungen. Erster Band. Zahlentheorie,* Springer, Berlin 1932.]

[49] M. D. Hirschhorn, A simple proof of Jacobi's two-square theorem, *Amer. Math. Monthly,* **92** (1985), 579–580.

[50] M. D. Hirschhorn, A simple proof of Jacobi's four-square theorem, *Proc. Amer. Math. Soc.,* **101** (1987), 436–438.

[51] M. D. Hirschhorn, Some formulae for partitions into squares, *Discrete Math.,* **211** (2000), 225–228.

[52] J. Chen, Waring's problem for $g(5)$, *Sci. Sinica,* **13** (1964), 1547–1568.

[53] A. Ja. Chinčin, *Tri Žemčužiny Tĕorii Čisel,* Fizmatgiz, Moskva 1948.

[54] N. Katz, An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields, *Amer. Math. Soc. Symp. Pure Math.,* **28** (1976), 275–305.

[55] A. Kempner, Bemerkungen zum Waringschen Problem, *Mat. Annalen,* **72** (1912), 387–399.

[56] D. E. Knuth and E. A. Bender, Enumeration of plane partitions, *J. Combinat. Th.,* **13** (1972), 40–54.

[57] N. Koblitz, *Introduction to Eliptic Curves and Modular Forms,* Springer-Verlag, Berlin 1993.

[58] J. F. Kubina and M. C. Wunderlich, Extending Waring's conjecture to 471,600,000, *Math. Comp.,* **55** (1990), 815–820.

[59] E. LANDAU, Über eine Anwendung der Primzahltheorie auf das Waringsche Problem in der elementaren Zahlentheorie, *Mat. Annalen,* **66** (1909), 102–106.

[60] JU. V. LINNIK, Elementarnoje rešenije problemy Varinga po metodu Šnirelmana, *Matem. Sb.,* **12** (1943), 225–230.

[61] JU. V. LINNIK, O predstavlenii bolšich čisel summoju semi kubov, *Matem. Sb.,* **12** (1943), 220–224.

[62] J. H. VAN LINT AND R. M. WILSON, *A Course in Combinatorics,* Cambridge University Press, Cambridge, UK 1992.

[63] P. A. MACMAHON, *Combinatory Analysis, Volume 1 and 2,* Cambridge University Press, Cambridge, UK 1916.

[64] K. MAHLER, On the fractional parts of the powers of a rational number II., *Mathematika,* **4** (1957), 122–124.

[65] S. MILNE, Infinite families of exact sums of squares formulas, Jacobi elliptic functions, and Schur functions, *Ramanujan J.,* **6** (2002), 7–149.

[66] M. NATHANSON, *Additive Number Theory. The Classical Bases,* Springer, Berlin 1996.

[67] M. NATHANSON, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets,* Springer, Berlin 1996.

[68] M. NATHANSON, *Elementary Methods in Number Theory,* Springer, Berlin 2000.

[69] D. J. NEWMAN, The evaluation of the constant in the formula for the number of partitions of n, *Amer. J. Math.,* **73** (1951), 599-601.

[70] D. J. NEWMAN, A simplified proof of Waring's conjecture, *Michigan Math. J.,* **7** (1960), 291–295.

[71] D. J. NEWMAN, A simplified proof of the partition formula, *Michigan Math. J.,* **9** (1962), 283–287.

[72] D. J. NEWMAN, *Analytic Number Theory,* Springer, Berlin 1998.

[73] K. O'Hara, Unimodality of the Gaussian coefficients: a constructive proof, *J. Combin. Th., Ser. A,* **53** (1990), 29–52.

[74] K. Ono, Distribution of the partition function modulo m, *Ann. of Math.,* **151** (2000), 293–307.

[75] H. Rademacher, On the partition function $p(n)$, *Proc. London. Math. Soc (2),* **43** (1937), 241–254.

[76] A. R. Rajwade, *Squares,* Cambridge University Press, Cambridge, UK 1993.

[77] J. B. Remmel, Bijective proofs of some classical partition identities, *J. Combinatorial Th., Ser. A,* **33** (1982), 273–286.

[78] G. J. Rieger, Zur Hilbertschen Lösung des Waringschen Problems: Abschätzung von $g(n)$, *Arch. der Math.,* **4** (1953), 275–281.

[79] G. J. Rieger, Zur Linniks Lösung des Waringschen Problems: Abschätzung von $g(n)$, *Math. Z.,* **60** (1954), 213–234.

[80] L. J. Rogers, Second memoir on the expansion of certain infinite products, *Proc. London Math. Soc.,* **25** (1894), 318–343.

[81] W. Rudin, Sums of squares of polynomials, *Amer. Math. Monthly,* **107** (2000), 813–821.

[82] J.-P. Serre, *A Course in Arithmetics,* Springer, Berlin 1996. [První vydání v r. 1973.]

[83] I. Schur, Ein Beitrag zur additiven Zahlentheorie und zur Theorie der Kettenbrüche, *Sitzungsber. Preuss. Akad. Wiss. Phys.-Math. Kl.,* (1917), 302–321.

[84] I. Schur, Zur additiven Zahlentheorie, *Sitzungsber. Preuss. Akad. Wiss. Phys.-Math. Kl.,* (1926), 488–495.

[85] R. P. Stanley, Symmetries of plane partitions, *J. Combin. Th., Ser. A,* **43** (1986), 103–113. [erratum ibid. **44** (1987), 310.]

[86] R. P. Stanley, A Baker's dozen of conjectures concerning plane partitions, 285–293. In: G. Labelle and P. Leroux (ed.), *Combinatoire Énumérative*, Springer-Verlag, Berlin 1986.

[87] G. Szekeres, An asymptotic formula in the theory of partitions, *Quart. J. of Math. (Oxford) (2),* **2** (1951), 85–108.

[88] G. Szekeres, Some asymptotic formulae in the theory of partitions (II), *Quart. J. of Math. (Oxford) (2),* **4** (1953), 96–111.

[89] O. Taussky, Sums of squares, *Amer. Math. Monthly,* **77** (1970), 805–830.

[90] J. V. Uspensky, Asymptotic expressions of numerical functions occurring in problems concerning the partition of numbers into summands, *Bull. Acad. Sci. de Russie,* **14** (1920), 199–218.

[91] R. C. Vaughan, *The Hardy–Littlewood Method,* Cambridge University Press, Cambridge, UK 1997.

[92] I. M. Vinogradov, On an upper bound on $G(n)$, *Izv. Akad. Nauk SSSR Ser. Mat.,* **23** (1959), 637–642.

[93] E. Waring, *Meditationes Algebraicae,* Cambridge University Press, Cambridge 1770.

[94] G. L. Watson, A proof of the seven cube theorem, *J. London Math. Soc.,* **26** (1951), 153–156.

[95] A. Wieferich, Beweis des Satzes, daß sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen läßt, *Mat. Annalen,* **66** (1909), 95–101.

[96] L. Winquist, An elementary proof of $p(11m+6) \equiv 0 \pmod{11}$, *J. Combinatorial Th.,* **6** (1969), 56–59.

[97] T. D. Wooley, Large improvements in Waring's problem, *Ann. of Math. (2),* **135** (1992), 131–164.

[98] T. D. Wooley, New estimates for smooth Weyl sums, *J. London Math. Soc. (2),* **51** (1995), 1–13.

[99] T. D. Wooley, Diophantine methods for exponential sums, and exponential sums for diophantine problems, 207–217. In: LI Tatsien (ed.), *Proceedings of the ICM 2002, Vol. II*, Higher Education Press, Beijing 2002.

[100] E. M. Wright, Asymptotic partition formulae, III. Partitions into k-th powers, *Acta Math.,* **63** (1934), 143–191.

[101] D. Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, *Amer. Math. Monthly,* **97** (1990), 144.