KALEIDOSKOP TEORIE ČÍSEL (1. 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 1. kapitoly 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 a 1999/00. V KAM Seriích budou postupně vydány další kapitoly: kapitola 2 (diofantické aproximace), kapitola 3 (diofantické rovnice), kapitola 4 (kongruence), kapitola 5 (prvočísla), kapitola 6 (geometrie čísel), kapitola 7 (číselné rozklady), kapitola 8 (medailony matematiků) a kapitola 9 (návody k řešením úloh). Obtížnost úloh je bodována 0 (nejlehčí) až 5 (nejtěžší).

leden 2000 — Martin Klazar

Obsah

Kapitola 1

Základní pojmy a obraty

Do první přípravné kapitoly jsme zařadili výsledky, které se budou hodit později. Mnohé z nich jsou zajímavé a důležité i samy o sobě.

V oddílu 1.1 připomeneme značení a pojmy týkající se základních číselných oborů $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}$ a $\mathbf{C}$ (přirozená čísla, celá čísla, zlomky, reálná čísla a komplexní čísla). V 1.2 dokážeme základní větu aritmetiky, čínskou větu o zbytku, Möbiovu inverzní formuli a další aritmetické výsledky. V 1.3 odvodíme, že celá algebraická čísla tvoří podokruh a algebraická čísla podtěleso tělesa $\mathbf{C}$. Oddíl 1.4 je věnován jednoduchým analytickým technikám odhadů sum. Mimo jiné dokážeme Eulerovu–MacLaurinovu sumační formuli pro druhou derivaci.

Dvě zahřívací úlohy. Má těleso reálných čísel neidentický automorfismus? To jest, existuje bijekce $f : \mathbf{R} \to \mathbf{R}$ různá od identity a taková, že pro každá dvě čísla $x, y \in \mathbf{R}$ platí vztahy $f(x+y) = f(x) + f(y)$ a $f(xy) = f(x)f(y)$?

V tělese komplexních čísel je takový automorfismus nasnadě: komplexní konjugace. Má však těleso $\mathbf{C}$ ještě jiný automorfismus kromě identity a konjugace? (Úlohy 4, 5 a 6.)

1.1 Číselné obory

Přirozenými čísly rozumíme množinu $\mathbf{N} = \{1, 2, 3, \ldots\}$. Pomocí symbolu $\mathbf{N}_0$ značíme množinu $\mathbf{N} \cup \{0\}$. Pomocí $\mathbf{Z}$ označujeme *celá čísla* $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Pro relaci *dělitelnosti* na $\mathbf{Z} \times \mathbf{Z}$ vyhrazujeme binární relační symbol $\backslash$ — $a \backslash b$ právě když $b = ac$ pro nějaké $c \in \mathbf{Z}$. Číslo

a je pak *dělitelem* b a b je *násobkem* a. V dalším se většinou omezujeme jen na dělitele ležící v $\mathbf{N}$. *Kongruence* a a b modulo c, symbolicky $a \equiv b$ mod c, znamená, že $c \backslash (a-b)$. *Největší společný dělitel* a a b, symbolicky (a,b), je největší přirozené číslo dělící a a b. Například $(-5,8)=1$, $(-16,-12)=4$ a $(0,0)$ není definován. Pokud $(a,b)=1$, řekneme, že a a b jsou *nesoudělná*, a píšeme též $a \perp b$. Nesoudělnost tedy znamená, že a a b dělí současně pouze 1 a -1. *Nejmenší společný násobek* čísel $a,b \in \mathbf{Z}$ značíme $[a,b]$ a je to nejmenší $c \in \mathbf{N}$, které je dělitelné a i b. Obdobně se definuje největší společný dělitel $(a_1,\ldots,a_k)$ a nejmenší společný násobek $[a_1,\ldots,a_k]$ pro více čísel.

Zlomky neboli *racionálními čísly* rozumíme množinu $\mathbf{Q} = \{a/b :\ a \in \mathbf{Z}\ \&\ b \in \mathbf{N}\}$. Symbol a/b chápeme zde jako uspořádanou dvojici, často ovšem bude znamenat podíl čísel a a b. Jak známo, zlomky a/b a c/d jsou stejné, pokud $ad = bc$. Relace stejnosti je ekvivalence. Každá třída stejných zlomků obsahuje právě jeden zlomek a/b takový, že $a \perp b$. Zlomek a/b pak je v *základním tvaru.*

Důležitá jsou *reálná čísla* $\mathbf{R}$. Představujeme si je jako přímku:

$$\mathbf{R}$$
$$\ldots \ \text{———————————————————————} \ \ldots$$

Doufáme, že si čtenářka alespoň mlhavě vzpomíná na některou z klasických metod budování reálných čísel ze zlomků, na Dedekindovu metodu řezů nebo na Cantorovy fundamentální (cauchyovské) posloupnosti, a že zná základní vlastnosti $\mathbf{R}$. Klíčovou roli hraje úplnost $\mathbf{R}$ vzhledem k metrice dané absolutní hodnotou. To jest, každá cauchyovská posloupnost reálných čísel má limitu. Uvědomme si podstatný rozdíl mezi přirozenými, celými a racionálními čísly na straně jedné a reálnými čísly na straně druhé. Jednotlivé prvky oborů $\mathbf{N}, \mathbf{Z}$ a $\mathbf{Q}$ jsou konečné objekty, ale „typické“ reálné číslo sestává z nekonečného množství *nepopsatelně* chaotické informace. Jako konečné bytosti nás tak od skoro všech reálných čísel odděluje nepřekonatelná propast. Ani pan Š. se zázračnou pamětí, hrdina Lurijovy knihy zmíněné v mottu, by si za celý život nedokázal zapamatovat jedno jediné typické reálné číslo.

Číslo $\alpha \in \mathbf{R}$ se nazývá *iracionální*, pokud není racionální. (Úlohy na iracionalitu: 1, 2 a 3.) Pythagorejcům vděčíme za příklad iracionálního čísla

$$\sqrt{2} = 1.41421356237309504880168887\ldots$$

Jedním z nejmladších příkladů je číslo

$$\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3} = 1.2020569031595942853997381\ldots,$$

jehož iracionalita byla dokázána v r. 1978 (viz oddíl 2.4). Jde o hodnotu *Eulerovy–Riemannovy funkce* ζ, která je pro reálné $s > 1$ dána součtem $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.

Kvadratické iracionality jsou komplexní čísla α splňující vztah

$$a\alpha^2 + b\alpha + c = 0,$$

kde $a, b, c \in \mathbf{Z}$ nejsou všechna nulová. Nejslavnější kvadratická iracionalita je jistě *zlatý řez*

$$\phi = 1.6180339887498948482045868\ldots,$$

kořen rovnice $x^2 - x - 1 = 0$. Obecnější třídu komplexních čísel tvoří *algebraická čísla*, kořeny algebraických rovnic

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

kde $a_i \in \mathbf{Z}$ a $a_n \neq 0$. Nealgebraická komplexní čísla se nazývají *transcendentní*. Nejznámější transcendentní čísla jsou Ludolfovo číslo

$$\pi = 3.1415926535897932384626433\ldots$$

a základ přirozených logaritmů (Eulerovo číslo)

$$\mathrm{e} = 2.7182818284590452353602874\ldots$$

(viz oddíl 2.5). Setkáme se i s *Eulerovou–Mascheroniovou konstantou*

$$\gamma = \lim_{n\to\infty} \left(\sum_{m=1}^{n} \frac{1}{m} - \log n \right) = 0.5772156649015328606065120\ldots$$

O té ovšem není ani známo, zda je iracionální.

Horní celá část $\lceil\alpha\rceil \in \mathbf{Z}$ čísla $\alpha \in \mathbf{R}$ se definuje vztahem

$$\lceil\alpha\rceil - 1 < \alpha \leq \lceil\alpha\rceil$$

a *(dolní) celá část* $\lfloor\alpha\rfloor \in \mathbf{Z}$ vztahem

$$\lfloor\alpha\rfloor \leq \alpha < \lfloor\alpha\rfloor + 1.$$

Zlomková část $\{\alpha\} \in [0,1)$ se rovná rozdílu

$$\{\alpha\} = \alpha - \lfloor\alpha\rfloor.$$

Používá se i symbol $\|\alpha\|$ označující vzdálenost α od nejbližšího celého čísla. Tedy $\|\alpha\| = \min(\{\alpha\}, 1 - \{\alpha\})$.

Komplexní čísla $\mathbf{C}$ získáme z tělesa $\mathbf{R}$ adjunkcí kořene i rovnice $x^2+1=0$, takže $\mathbf{C} = \{a+bi:\ a,b \in \mathbf{R}\}$. Někdy budeme místo i psát $\sqrt{-1}$. Reálnou část a čísla $z = a+bi$ značíme $\mathrm{Re}(z)$ a imaginární část b $\mathrm{Im}(z)$. Číslo *komplexně sdružené (konjugované)* k $z = a+bi$ je číslo $\overline{z} = a - bi$. Podle základní věty algebry má v $\mathbf{C}$ každá algebraická rovnice s komplexními koeficienty kořen. $\mathbf{C}$ je vzhledem k metrice odvozené z normy $|z| = \sqrt{z\overline{z}}$ úplným metrickým prostorem. (Rozdíly mezi $\mathbf{R}$ a $\mathbf{C}$ se zabývají úlohy 4, 5, 6, 7 a 8).

1.2 Trocha aritmetiky

Každá neprázdná podmnožina $X \subset \mathbf{N}$ má nejmenší prvek. Ekvivalentní formulací je známý princip indukce: Má-li 1 vlastnost V a platí-li pro každé číslo $n \in \mathbf{N}$ implikace „každé $m \in \mathbf{N}, m \leq n$, má vlastnost V $\Rightarrow n+1$ má vlastnost V“, pak každé číslo $n \in \mathbf{N}$ má vlastnost V. Princip indukce platí samozřejmě i pro $\mathbf{N}_0$.

Tvrzení 1 (dělení se zbytkem). *Pro každá dvě čísla $m \in \mathbf{Z}$ a $n \in \mathbf{N}$ existují čísla $a, b \in \mathbf{Z}$ taková, že*

$$m = an + b \ \&\ 0 \leq b < n.$$

DŮKAZ. Nechť $X = \{m - c:\ c \in \mathbf{Z}\ \&\ n \backslash c\ \&\ c \leq m\}$. X je neprázdná podmnožina $\mathbf{N}_0$. Její nejmenší prvek buď b. Zřejmě $0 \leq b < n$ a $m = c + b = an + b$. $\diamondsuit$

Číslo $n \in \mathbf{N}$ je *prvočíslo*, pokud je větší než 1 a jeho (přirození) dělitelé jsou pouze 1 a n. Řada prvočísel začíná

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ldots$$

Prvočíselná funkce $\pi(x)$, kde $x \in \mathbf{R}$, udává počet prvočísel nepřesahujících číslo x. Například $\pi(17) = \pi(18.6) = 7$. Prvočísly a funkcí π se podrobně zabýváme v páté kapitole. Jejich fundamentální význam pro teorii čísel popisuje následující věta.

Věta 2 (základní věta aritmetiky). *Každé přirozené číslo n má rozklad na součin (ne nutně různých) prvočísel $n = p_1 p_2 \dots p_r$. Rozklad je jednoznačný, kromě pořadí činitelů.*

Důkaz. Nejprve indukcí dokážeme, že každé přirozené číslo n je součinem prvočísel. Pro $n = 1$ to je pravda (prázdný součin). Pro $n > 1$ je množina dělitelů n větších než 1 neprázdná, nejmenší z nich buď m. Číslo m je zřejmě prvočíslo. Podle indukčního předpokladu je n/m součinem prvočísel, tedy i $n = m \cdot (n/m)$ je součinem prvočísel.

Nyní jednoznačnost. Nejprve dokážeme implikaci

$$p \backslash ab \;\Rightarrow\; p \backslash a \text{ nebo } p \backslash b,$$

v níž a a b jsou celá čísla a p je prvočíslo. Postupujeme indukcí podle p. Pro $p = 2$ implikace platí, protože součin dvou lichých čísel je opět liché číslo. Předpokládáme, že $p > 2$ a pro prvočísla q menší než p implikace platí. Nechť $ab = pc$. Podle předešlého tvrzení můžeme a a b vyjádřit jako $a = pa_1 + a_0$ a $b = pb_1 + b_0$, kde $a_i, b_i \in \mathbf{Z}$ a $0 \leq a_0, b_0 < p$. Takže p dělí $a_0 b_0$, $a_0 b_0 = pc'$. Pokud $a_0 > 0$ a $b_0 > 0$, odvodíme spor. Napíšeme si a_0 a b_0 jako součiny prvočísel, $a_0 = p_1 \dots p_r$ a $b_0 = q_1 \dots q_s$, a uvážíme rovnost $p_1 \dots p_r q_1 \dots q_s = pc'$. Protože $p_i \leq a_0 < p$ a $q_i \leq b_0 < p$, podle indukčního předpokladu pro každé p_i a q_i již dokazovaná implikace platí. Žádné z těchto prvočísel ale nedělí p. Každé z nich tedy můžeme zkrátit proti c' (či přesněji proti číslu, které z c' zbývá) a nakonec dostaneme nemožnou rovnost $1 = pd$, kde $d \in \mathbf{N}$. Takže $a_0 = 0$ nebo $b_0 = 0$ a implikace platí i pro p.

Z implikace plyne hned, že rovné součiny prvočísel $p_1 p_2 \dots p_a = q_1 q_2 \dots q_b$ mají stejnou délku $a = b$ a liší se jen pořadím činitelů. ♢

V prvočíselném rozkladu n shrneme stejná prvočísla do jedné mocniny a píšeme $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$, kde p_i jsou různá prvočísla a $a_i \in \mathbf{N}$. Prvočíslům dělícím n se říká *prvočinitelé* n. Složitost rozkladu měříme funkcemi *počet prvočinitelů* $\omega(n) = s$ a *počet prvočinitelů s násobnostmi* $\Omega(n) = a_1 + \dots + a_s$.

Číslo $n \in \mathbf{Z}$ buď celé a nenulové. Exponent prvočísla p, s nímž vystupuje v rozkladu čísla $|n| \in \mathbf{N}$, označíme jako $\mathrm{ord}_p(n)$; když p není prvočinitel $|n|$, $\mathrm{ord}_p(n) = 0$. Položíme $\mathrm{ord}_p(0) = \infty$ pro každé p. Nechť $a, b \in \mathbf{Z}$ jsou dvě celá čísla. Z věty 2 plyne, že $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$ pro každé p. Dále,

$$(a, b) = \prod_p p^{\min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))} \text{ a } [a, b] = \prod_p p^{\max(\mathrm{ord}_p(a), \mathrm{ord}_p(b))}.$$

(Analogicky pro největší společný dělitel a nejmenší společný násobek více čísel.) Vidíme, že $(a,b)[a,b] = ab$. Je rovněž jasné, že z $d\backslash a$ & $d\backslash b$ plyne $d\backslash(a,b)$ a že $[a,b]$ dělí každý společný násobek a a b. Podobně pro společné dělitele a násobky více čísel.

Čtenář jistě ví, že pro nalezení největšího společného dělitele přirozených čísel $a < b$ není třeba znát jejich prvočíselné rozklady. Získá se pomocí *Euklidova algoritmu* — nejprve dělíme b číslem a se zbytkem r_0, pak dělíme a číslem r_0 se zbytkem r_1 a tak dále až dostaneme nulový zbytek $r_i = 0$. Pak $(a,b) = r_{i-1}$.

Přirozené číslo n je *čtvercuprosté*, pokud $m^2\backslash n$ pouze pro $m^2 = 1$. Jinak řečeno, $\mathrm{ord}_p(n) = 1$ pro každý prvočinitel n. Každé $n \in \mathbf{N}$ má jednoznačný rozklad $n = k^2 l$, kde l je čtvercuprosté: Za k^2 vezmeme největší čtverec dělící n. Z jiné strany: l je součin těch prvočinitelů n, které mají lichý exponent.

Tvrzení 3 (vynucení čtverce). *Nechť $a, b, c \in \mathbf{N}$ jsou tři čísla, přičemž $ab = c^2$ a $a \perp b$. Pak a i b jsou čtverce.*

Důkaz. Protože $2\cdot\mathrm{ord}_p(c) = \mathrm{ord}_p(c^2) = \mathrm{ord}_p(a)+\mathrm{ord}_p(b)$ pro každé prvočíslo p (podle věty 2), přičemž vpravo je vždy alespoň jeden ze sčítanců nulový, jsou sčítance $\mathrm{ord}_p(a)$ a $\mathrm{ord}_p(b)$ vždy sudé. Proto (podle věty 2) jsou a i b čtverce. $\diamondsuit$

Podobně se dokážou i různé varianty tvrzení 3, které mají místo čtverců jinou mocninu a místo 1 jinou hodnotu čísla (a,b). V algebraických strukturách, v nichž neplatí věta 2 (úlohy 9 a 10), selhává i tvrzení 3. Několikrát ho využijeme v oddílu 3.1.

Tvrzení 4 (o ideálech). *Nechť celá čísla $a_1, \ldots, a_k$ nejsou současně nulová a $c = (a_1, \ldots, a_k)$. Pak*

$$L := \{a_1x_1 + \cdots + a_kx_k : \ x_i \in \mathbf{Z}\} = \{cx : \ x \in \mathbf{Z}\} =: P.$$

Důkaz. Je jasné, že $L \subset P$. Je rovněž jasné, že množina L je uzavřená na součty a rozdíly a s každým svým prvkem obsahuje i jeho libovolný celočíselný násobek. Nechť d je nejmenší kladný prvek L a $e \in L$ je libovolný prvek. Po vydělení e číslem d vyjde nulový zbytek, jinak bychom měli spor s definicí d. Každý prvek L je celočíselný násobek d. Tudíž L sestává ze všech celočíselných násobků d. Nerovnost $d < c$ je nemožná, protože $L \subset P$. Ovšem $d\backslash a_i$ pro každé i, takže $d\backslash c$ a $d \le c$. Nutně $d = c$ a $L = P$. $\diamondsuit$

Algebraicky řečeno, v okruhu $\mathbf{Z}$ je ideál generovaný čísly $a_1, \dots, a_k$ rovný (hlavnímu) ideálu generovanému jejich největším společným dělitelem.

Tvrzení 5 (čínská věta o zbytku). *Čísla $m_1, \dots, m_k \in \mathbf{N}$ buďte po dvou nesoudělná a $m = m_1 m_2 \cdots m_k$. Pro každou k-tici celých čísel $b_1, \dots, b_k$ má systém kongruencí*

$$x \equiv b_1 \bmod m_1, \dots, x \equiv b_k \bmod m_k$$

řešení a každá dvě řešení se liší o násobek m.

Důkaz. Položíme $n_i = m/m_i$. Snadno se vidí, že $(m_i, n_i) = 1$. Podle předchozího tvrzení existují čísla $r_i, s_i \in \mathbf{Z}$ taková, že $r_i m_i + s_i n_i = 1$. Položíme

$$x_0 = \sum_{i=1}^{k} b_i s_i n_i.$$

Protože $s_i n_i \equiv 1 \bmod m_i$ a $s_i n_i \equiv 0 \bmod m_j, j \neq i$, je x_0 řešením systému. Je-li x_1 jiné řešení, je $x_1 - x_0$ dělitelné každým m_i a tedy i jejich nejmenším společným násobkem, což je m. $\diamondsuit$

Předchozí tvrzení se dá přeformulovat následujícím způsobem. Uvažme zobrazení $F : \{1, 2, \dots, m\} \to \{1, 2, \dots, m_1\} \times \{1, 2, \dots, m_2\} \times \cdots \times \{1, 2, \dots, m_k\}$, které číslu x přiřazuje k-tici $(x_1, x_2, \dots, x_k)$ určenou kongruencemi $x_i \equiv x \bmod m_i$. Podle čínské věty o zbytku jde o bijekci.

Aritmetickou funkcí rozumíme funkci $f : \mathbf{N} \to \mathbf{C}$. Je *multiplikativní*, pokud $f(1) = 1$ a $f(mn) = f(m)f(n)$ jakmile $m \perp n$. Platí-li $f(mn) = f(m)f(n)$ pro každá dvě přirozená čísla m a n, je f *úplně multiplikativní*. Důležitým příkladem úplně multiplikativní funkce je *Möbiova funkce* $\mu : \mathbf{N} \to \{-1, 0, 1\}$,

$$\mu(n) = \mu(p_1 p_2 \dots p_r) = (-1)^r \text{ pro čtvercuprosté } n \text{ a } \mu(n) = 0 \text{ jinak.}$$

Pro $n = 1$ máme $\mu(1) = 1$ podle definice, v souladu s konvencí o prázdném součinu.

Tvrzení 6 (identita pro μ). *Nechť $n \in \mathbf{N}$. Pak*

$$\sum_{d \backslash n} \mu(d) = \begin{cases} 0 & \text{pro } n > 1 \\ 1 & \text{pro } n = 1. \end{cases}$$

Důkaz. Část tvrzení pro $n = 1$ je jasná. Pro $n > 1$ se součet nezmění, nahradíme-li n součinem všech jeho prvočinitelů m, $m = p_1p_2\dots p_r, r > 0$. Podle binomické věty,

$$\sum_{d\backslash n}\mu(d) = \sum_{d\backslash m}\mu(d) = \sum_{i=0}^{r}\binom{r}{i}(-1)^i = (1-1)^r = 0.$$

$\diamondsuit$

Tvrzení 7 (Möbiova inverzní formule). *Nechť f, g jsou dvě aritmetické funkce. Platí ekvivalence*

$$f(n) = \sum_{d\backslash n} g(d) \quad \textit{pro každé } n \quad \Longleftrightarrow \quad g(n) = \sum_{d\backslash n} f(d)\mu(n/d) \quad \textit{pro každé } n.$$

Důkaz. Dokážeme jen implikaci $\Rightarrow$, opačná implikace se dokazuje podobně.

$$\begin{aligned}
\sum_{d\backslash n} f(d)\mu(n/d) &= \sum_{d\backslash n}\Big(\sum_{e\backslash d} g(e)\Big)\mu(n/d) \quad \text{(předpoklad)}\\
&= \sum_{e\backslash n} g(e) \sum_{e\backslash d\backslash n}\mu(n/d)\\
&= \sum_{e\backslash n} g(e) \sum_{h\backslash (n/e)}\mu(h)\\
&= g(n) \quad \text{(podle tvrzení 6).}
\end{aligned}$$

$\diamondsuit$

(Viz též úlohu 11.)

Další příklady multiplikativních funkcí představují funkce $d, \sigma : \mathbf{N} \to \mathbf{N}$, které počítají počet a součet dělitelů argumentu:

$$d(n) = \sum_{d\backslash n} 1 \quad \text{a} \quad \sigma(n) = \sum_{d\backslash n} d.$$

Nejsou úplně multiplikativní. Multiplikativita plyne ze snadno dokazatelných formulí (úloha 12), $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$,

$$d(n) = (a_1+1)(a_2+1)\cdots(a_r+1) \quad \text{a} \quad \sigma(n) = \frac{(p_1^{a_1}-1)(p_2^{a_2}-1)\cdots(p_r^{a_r}-1)}{(p_1-1)(p_2-1)\cdots(p_r-1)}.$$

Dá se ukázat, že i funkce

$$r_2(n) = |\{(x,y) \in \mathbf{Z}^2 : \; x^2 + y^2 = n\}|$$

počítající vyjádření n součtem dvou celočíselných čtverců je multiplikativní. Není úplně multiplikativní.

Funkce $\omega(n)$ je multiplikativní a není úplně multiplikativní. Funkce $\Omega(n)$ je úplně multiplikativní.

Jako poslední příklad multiplikativní (ale ne úplně multiplikativní) funkce uvádíme *Eulerovu funkci* $\varphi : \mathbf{N} \to \mathbf{N}$, jež počítá přirozená čísla $m \leq n$ nesoudělná s n:

$$\varphi(n) = \#\{m \in \mathbf{N} : \; m \leq n \;\&\; m \perp n\}.$$

Její multiplikativita vyplývá z tvrzení 5. Pro nesoudělná čísla $m_1, m_2 \in \mathbf{N}$ vezmeme zobrazení F popsané za čínskou větou o zbytku. Protože $x, 1 \leq x \leq m_1 m_2$, je nesoudělné s $m_1 m_2$, právě když x_i, kde $F(x) = (x_1, x_2)$, je nesoudělné s m_i (a F je bijekce), máme $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.

Hodnota Eulerovy funkce na mocnině prvočísla je $\varphi(p^n) = p^n - p^n/p = p^{n-1}(p-1)$. S použitím multiplikativity dostáváme

Tvrzení 8 (vzorec pro φ). *Je-li $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ prvočíselný rozklad n, platí formule*

$$\begin{aligned} \varphi(n) &= p_1^{a_1-1} p_2^{a_2-1} \cdots p_k^{a_k-1}(p_1-1)(p_2-1)\cdots(p_k-1) \\ &= n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\cdots(1-\tfrac{1}{p_k}). \end{aligned}$$

Tvrzení 9 (identita pro φ). *Pro každé číslo $n \in \mathbf{N}$ platí identita*

$$\sum_{m \backslash n} \varphi(m) = n.$$

DůKAZ. Každé číslo $p, 1 \leq p \leq n$, má jednoznačný rozklad $p = mk$, kde m je dělitel n a $k \perp n/m$. Vidíme, že $\{p \in \mathbf{N} : \; 1 \leq p \leq n\}$ je v bijekci s $\{(m,k) \in \mathbf{N}^2 : \; m\backslash n \;\&\; k \perp n/m \;\&\; k \leq n/m\}$. Pro pevné m máme $\varphi(n/m)$ dvojic. Identita je očividná. $\diamondsuit$

(Pro jiný pohled na funkce μ a φ viz úlohy 13, 14, 15 a 16.)

Malá Fermatova věta je kongruence

$$a^{p-1} \equiv 1 \bmod p,$$

kde p je prvočíslo a $a \in \mathbf{Z}$ není dělitelné p. Přepíšeme ji do ekvivalentní podoby $a^p \equiv a \bmod p$, již dokážeme indukcí podle $a \in \mathbf{N}_0$. Pro $a = 0$ je platná. Z binomické věty a indukčního předpokladu máme pro $a > 0$

$$a^p = (1+(a-1))^p = \sum_{i=0}^{p} \binom{p}{i}(a-1)^i \equiv 1+(a-1)^p \equiv 1+(a-1) \equiv a \bmod p.$$

Tvrzení 10 (Eulerovo zobecnění malé Fermatovy věty). *Pokud $m, n \in \mathbf{N}$ a $(m,n) = 1$, platí kongruence*

$$m^{\varphi(n)} \equiv 1 \bmod n.$$

Důkaz. Vzhledem k tvrzení 5 a multiplikativitě φ stačí kongruenci dokázat jen pro případ $n = p^k$, $k \in \mathbf{N}$. Je-li totiž $n = p_1^{a_1} \cdots p_k^{a_k}$ prvočíselný rozklad n a máme-li $m^{\varphi(p_i^{a_i})} \equiv 1 \bmod p_i^{a_i}$ pro každé i, máme i

$$m^{\varphi(n)} = \left(m^{\varphi(p_i^{a_i})}\right)^{\varphi(n/p_i^{a_i})} \equiv 1 \bmod p_i^{a_i},$$

a $m^{\varphi(n)} \equiv 1 \bmod n$ podle tvrzení 5.

Pro modul $n = p^k$ dokážeme kongruenci indukcí podle k. Pro $k = 1$ platí. Pro $k > 1$ máme $m^{\varphi(p^{k-1})} = 1 + rp^{k-1}$ podle indukce a binomická věta znovu dává

$$m^{\varphi(p^k)} = (1+rp^{k-1})^p = \sum_{i=0}^{p} \binom{p}{i}(rp^{k-1})^i \equiv 1 \bmod p^k.$$

$\diamond$

Elegantnější algebraický argument dokazuje poslední tvrzení následovně. Zbytky modulo n nesoudělné s n tvoří multiplikativní grupu řádu $\varphi(n)$. Teorie grup nám říká, že každý prvek grupy umocněný na její řád dává jednotkový prvek.

1.3 Algebraická čísla

Okruh polynomů v proměnných $x_1, \ldots, x_k$ s komplexními koeficienty značíme $\mathbf{C}[x_1, \ldots, x_k]$; obdobně pro jiné obory koeficientů. Pro polynom f pomocí $\deg(f)$ značíme jeho stupeň. Polynom $f \in \mathbf{C}[x]$ je *monický*, má-li u nejvyšší mocniny x koeficient 1.

Připomínáme, že komplexní číslo $\alpha \in \mathbf{C}$ je algebraické, je-li kořenem polynomu $f \in \mathbf{Z}[x]$. Ekvivalentně řečeno, $g(\alpha) = 0$ pro monický polynom $g \in \mathbf{Q}[x]$. Množinu algebraických čísel označíme jako $\mathbf{C}^{\,\mathrm{alg}}$. *Minimální polynom* α je monický racionální polynom nejmenšího stupně s kořenem α. Je určen jednoznačně a dělí každý racionální polynom, který se na α anuluje. Jeho stupni se říká také *stupeň* čísla α. Není těžké ukázat, že minimální polynom každého α je ireducibilní (v $\mathbf{Q}[x]$) a má pouze jednoduché kořeny.

Následující výsledek zobecňuje implikaci z důkazu věty 2.

Tvrzení 11 (Gaussovo lemma). *Pokud prvočíslo p dělí všechny koeficienty součinu celočíselných polynomů gh, dělí p všechny koeficienty g nebo všechny koeficienty h.*

DŮKAZ. Nechť $g(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbf{Z}[x]$, $h(x) = b_0 + b_1x + \cdots + b_mx^m \in \mathbf{Z}[x]$ a p nedělí ani všechna a_k ani všechna b_k. Čísla i a j buďte minimální taková, že p nedělí ani a_i ani b_j. Koeficient c u x^{i+j} v gh je součet součinů a_kb_l, přičemž $k + l = i + j$. Kromě jediného sčítance a_ib_j jsou ostatní dělitelné p, protože v nich je $k < i$ nebo $l < j$. Tedy p nedělí c. $\diamondsuit$

Tvrzení 12 (o faktorizaci celočíselných polynomů). *Nechť $f = gh$, kde $f \in \mathbf{Z}[x]$ je celočíselný a $g, h \in \mathbf{Q}[x]$ racionální polynomy. Pak existují zlomky $a, b \in \mathbf{Q}$ a celočíselné polynomy $g_1, h_1 \in \mathbf{Z}[x]$ takové, že $f = g_1h_1$, $g_1 = ag$ a $h_1 = bh$ (tudíž $ab = 1$).*

DŮKAZ. Nechť $c \in \mathbf{N}$ je nějaký společný násobek jmenovatelů koeficientů polynomu g a číslo $d \in \mathbf{N}$ je stejně definováno pro polynom h. Pak $cdf = (cg) \cdot (dh)$ a $cdf, cg, dh \in \mathbf{Z}[x]$. Podle Gaussova lemmatu zkrátíme každý prvočinitel čísla cd proti všem koeficientům polynomu cg nebo všem koeficientům polynomu dh. Dostaneme tak faktorizaci f v $\mathbf{Z}[x]$, přičemž faktory g_1 a h_1 jsou skalární racionální násobky polynomů g a h. $\diamondsuit$

Speciálně, polynom je ireducibilní v $\mathbf{Z}[x]$, právě když je ireducibilní v $\mathbf{Q}[x]$. (Pro třídu ireducibilních polynomů viz úlohy 17 a 18.)

Podtřídu algebraických čísel tvoří *celá algebraická čísla*, což jsou kořeny celočíselných *monických* polynomů. Jejich množinu označíme jako $\mathbf{C}^{\,\mathrm{calg}}$. Například zlatý řez $(1+\sqrt{5})/2$ je celé algebraické číslo, ale $\sqrt{2}/2$ nikoli. Ukážeme, že každé celé algebraické číslo α má celočíselný minimální polynom. Nechť $f \in \mathbf{Z}[x]$ je monický polynom nejmenšího stupně, který se anuluje na α. Je jasné, že f je ireducibilní v $\mathbf{Z}[x]$. Kdyby se minimální polynom α lišil od f, musel by dělit f a f by se rozkládal v $\mathbf{Q}[x]$, což je spor.

Užitečné pozorování. Je-li α kořenem polynomu $b_nx^n + b_{n-1}x^{n-1} + \cdots + b_0 \in \mathbf{Z}[x]$, je $b_n\alpha$ celé algebraické číslo. Vynásobením b_n^{n-1} totiž obdržíme $(b_n\alpha)^n + b_{n-1}(b_n\alpha)^{n-1} + \cdots + b_0b_n^{n-1} = 0$.

Polynom $f \in \mathbf{Z}[x_1, \ldots, x_k]$ je *symetrický*, když se nemění při žádné permutaci proměnných x_i. Například, pro $k = 2$, $7x_1^2x_2 + 7x_1x_2^2 - x_1x_2 + 5$ je symetrický. Polynom $x_1x_2^2 - 1$ symetrický není. Symetrické polynomy v k proměnných $x_1, \ldots, x_k$

$$e_1 = \sum_i x_i,\ e_2 = \sum_{i<j} x_ix_j,\ e_3 = \sum_{i<j<l} x_ix_jx_l,\ \ldots,\ e_k = x_1x_2\cdots x_k$$

se nazývají *elementární symetrické polynomy*. S algebraickými čísly souvisejí prostřednictvím identity (x a α_i jsou proměnné)

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k) = x^k + \sum_{i=1}^{k}(-1)^i e_i(\alpha_1, \ldots, \alpha_k)x^{k-i}.$$

Pro každý monický polynom $x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$ tak platí *Viètovy vztahy* $a_{k-i} = (-1)^i e_i(\alpha_1, \ldots, \alpha_k)$, kde $\alpha_1, \ldots, \alpha_k$ jsou kořeny polynomu.

Rozkladem p čísla $n \in \mathbf{N}$ (nezaměňovat s prvočíselným rozkladem) rozumíme vyjádření $n = n_1 + n_2 + \cdots + n_k$, kde $n_i \in \mathbf{N}$. Liší-li se dva rozklady n pouze pořadím sčítanců, nepovažujeme je za různé. V zápisu $p = (n_1, n_2, \ldots, n_k)$ tak můžeme a budeme předpokládat, že $1 \le n_1 \le n_2 \le \cdots \le n_k$. Fakt, že neklesající seznam přirozených čísel p je rozkladem n se zapisuje symbolicky jako $p \vdash n$. Opakování členu p se vyznačuje exponentem. Například, $(1^3, 2, 3, 6^2) \vdash 20$, protože $20 = 1+1+1+2+3+6+6$. *Výškou* $v(p)$ rozkladu p rozumíme největší člen p (tj. n_k) a *šířkou* $s(p)$ délku koncového konstantního úseku (tj. maximální i takové, že $n_k = n_{k-1} = \cdots = n_{k-i+1}$).

Typem monomu $ax_1^{n_1}x_2^{n_2}\ldots x_k^{n_k}$ stupně n je rozklad $n = n_1+n_2+\cdots+n_k$. *Jednoduchým symetrickým polynomem* rozumíme nekonstantní symetrický polynom f, jehož všechny monomy mají stejný typ a koeficient $a = 1$. *Typ* f je pak tento jediný typ monomu f. Například typ e_i je (1^i) (i jedniček) a typ $x^2z + z^2x \in \mathbf{Z}[x, z]$ je $(1, 2)$. Výška $v(f)$ a šířka $s(f)$ polynomu f jsou pak definovány zřejmým způsobem. Takže $v(e_i) = 1$ a $s(e_i) = i$.

Tvrzení 13 (základní věta o symetrických polynomech). *Každý symetrický polynom $f \in \mathbf{Z}[x_1, \ldots, x_k]$ se dá vyjádřit jako*

$$f = F(e_1, e_2,\ \ldots, e_k),$$

kde $F \in \mathbf{Z}[x_1, \dots, x_k]$. *Má-li* f *stupeň* d *v každé z proměnných* x_i*, má* F *celkový stupeň* d*. Má-li* f *celkový stupeň* d*, platí pro každý (nenulový) monom* $ax_1^{i_1} \dots x_k^{i_k}$ *polynomu* F *rovnost* $i_1 + 2i_2 + \cdots + ki_k = d$*.*

Důkaz. Každý symetrický polynom je celočíselnou lineární kombinací jednoduchých symetrických polynomů a konstanty 1. Tvrzení stačí proto dokázat pouze pro ně. Případ $f = 1$ je jasný. Nechť $f \in \mathbf{Z}[x_1, \dots, x_k]$ je jednoduchý symetrický polynom. Postupujeme indukcí podle $v(f)$, pro danou výšku pak indukcí podle $s(f)$. Pokud $v(f) = 1$, $f = e_i$ pro nějaké i a $F = x_i$. Pro $v(f) > 1$ a p typ f buď q rozklad, který vznikne z p odečtením 1 od každého z posledních $s(p)$ členů p. Nechť $g \in \mathbf{Z}[x_1, \dots, x_k]$ je jednoduchý symetrický polynom typu q. Patrně $v(g) = v(f) - 1$. Polynom

$$h = f - e_{s(f)} \cdot g$$

je symetrický (obecně ne jednoduchý) a pro každý typ r jeho monomu platí $v(r) < v(f)$ nebo $v(r) = v(f)$ & $s(r) < s(f)$. Podle indukčního předpokladu mají g i h hledané vyjádření. Má je tedy i $f = h + e_{s(f)} \cdot g$. Dodatek o stupních je zřejmý. $\diamondsuit$

Rozklady čísel se podrobně zabýváme v sedmé kapitole.

Tvrzení 14 (podtěleso a podokruh). *Množina* $\mathbf{C}^{\mathrm{alg}}$ *je uzavřená na součet, součin a podíl. Množina* $\mathbf{C}^{\mathrm{calg}}$ *je uzavřená na součet a součin. Algebraicky řečeno,* $\mathbf{C}^{\mathrm{alg}}$ *je podtěleso a* $\mathbf{C}^{\mathrm{calg}}$ *podokruh tělesa* $\mathbf{C}$*.*

Důkaz. Dokážeme, že $\alpha, \beta \in \mathbf{C}^{\mathrm{alg}}$ implikuje $\alpha + \beta \in \mathbf{C}^{\mathrm{alg}}$. Vezmeme monický polynom $f \in \mathbf{Q}[x]$ stupně n (například součin minimálních polynomů čísel α a β) takový, že $f(\alpha) = f(\beta) = 0$. $S = (\gamma_1, \dots, \gamma_n)$ buď seznam všech kořenů f s příslušnými násobnostmi. Uvážíme seznam $m = n^2$ součtů $T = (t_1, \dots, t_m) = (\gamma_i + \gamma_j :\ \gamma_i, \gamma_j \in S)$. Stačí dokázat, že každý $e_i \in \mathbf{Z}[x_1, \dots, x_m]$ má na T racionální hodnotu. Číslo $\alpha + \beta$ se totiž vyskytuje mezi kořeny monického polynomu

$$P(x) = \prod_{t \in T} (x - t),$$

jehož koeficienty jsou racionální podle Viètových vztahů, a tak $\alpha + \beta \in \mathbf{C}^{\mathrm{alg}}$.

Chápejme na chvíli $\gamma_1, \dots, \gamma_n$ jako proměnné. Jakákoli permutace S pouze permutuje seznam T, takže polynom $r_i \in \mathbf{Z}[\gamma_1, \dots, \gamma_n]$ definovaný jako

$r_i = e_i(t_1, \ldots, t_m)$, kde $e_i \in \mathbf{Z}[x_1, \ldots, x_m]$, je symetrický. Podle předchozího tvrzení máme reprezentaci $r_i = F(e_1, \ldots, e_n)$, kde $F \in \mathbf{Z}[x_1, \ldots, x_n]$ a $e_j \in \mathbf{Z}[\gamma_1, \ldots, \gamma_n]$. Nyní se vrátíme k číslům $\gamma_1, \ldots, \gamma_n \in \mathbf{C}^{\text{alg}}$. Číslo $e_i(t_1, \ldots, t_m) = r_i(\gamma_1, \ldots, \gamma_n)$ je vyjádřeno z racionálních čísel $e_j(\gamma_1, \ldots, \gamma_n)$ (to jsou, až na znaménko, koeficienty f) celočíselným polynomem F a je tedy rovněž racionální.

Pokud $\alpha, \beta \in \mathbf{C}^{\text{calg}}$, můžeme v předchozí úvaze vzít f ze $\mathbf{Z}[x]$ a máme $e_j(\gamma_1, \ldots, \gamma_n) \in \mathbf{Z}$. Hodnoty elementárních symetrických polynomů na T jsou nyní celočíselné a hořejší monický polynom $P(x)$ je celočíselný. Takže $\alpha + \beta \in \mathbf{C}^{\text{calg}}$.

Pro součin $\alpha\beta$ se postupuje zcela obdobně, celistvá algebraičnost se zachovává ze stejného důvodu. Algebraičnost podílu plyne pomocí součinu a reciproké hodnoty. Je-li $\beta \in \mathbf{C}^{\text{alg}}$ nenulové číslo, máme $a_k\beta^k + \cdots + a_1\beta + a_0 = 0$ pro nějaká čísla $a_i \in \mathbf{Z}, a_k \neq 0$. Pak $a_k + a_{k-1}(1/\beta) + \cdots + a_0(1/\beta)^k = 0$ a algebraické je i $1/\beta$. Takže z $\alpha, \beta \in \mathbf{C}^{\text{alg}}, \beta \neq 0$ plyne hned $\alpha/\beta \in \mathbf{C}^{\text{alg}}$. Nyní se ovšem celistvá algebraičnost nezachovává. $\diamondsuit$

($\mathbf{C}^{\text{alg}}$ je ještě „uzavřenější" — viz úlohy 19 a 20.)

1.4 Asymptotika a sumy

Nejprve připomeneme asymptotické značení, které se hojně užívá v teorii čísel, diskrétní matematice i jinde. Nechť f a g jsou aritmetické funkce. Fakt, že nerovnost $|f(n)| \leq c|g(n)|$ platí pro vhodnou konstantu $c > 0$ pro všechna $n \in \mathbf{N}$ (případně kromě konečně mnoha n) se zkráceně zapisuje jako

$$f(n) = O(g(n)) \quad \text{nebo} \quad f(n) \ll g(n).$$

Indexy jako $O_k(f)$ nebo $\ll_{\alpha,m}$ znamenají, že implicitní konstanta není absolutní, nicméně závisí jen na zmíněných parametrech. Pokud $f(n)/g(n) \to 0$ pro $n \to \infty$, píšeme

$$f(n) = o(g(n)).$$

Symbolika

$$f(n) \sim g(n)$$

znamená, že $f(n)/g(n) \to 1$ pro $n \to \infty$. Obdobně se symboly $O, \ll, o$ a $\sim$ užívají i pro jiné definiční obory než $\mathbf{N}$ a jiné limitní body než ∞.

Mohutnost množiny X, v konečném případě tedy počet jejích prvků, značíme $|X|$ nebo $\#X$. Například $\#\{2,*,0\}=3$, $|\mathbf{Q}|=\aleph_0$ a $|\mathbf{R}|\ge\aleph_1$.

Manipulaci se sumami zpřehledňuje *charakteristická funkce výroku* $\langle\cdots\rangle$. Je-li $\phi(x,y,\ldots)$ výrok, jehož parametry $x,y,\ldots$ probíhají $\mathbf{N}$, položíme

$$\langle\phi(x,y,\ldots)\rangle=\begin{cases}1 & \text{pokud } \phi(x,y,\ldots) \text{ platí a}\\ 0 & \text{pokud } \phi(x,y,\ldots) \text{ neplatí.}\end{cases}$$

Místo, například,

$$\sum_{d\le x,\, d\backslash(a,b)} h(d)$$

tak můžeme psát

$$\sum_d \langle d\le x \,\&\, d\backslash(a,b)\rangle\cdot h(d) \quad \text{nebo} \quad \sum_{d\le x}\langle d\backslash(a,b)\rangle\cdot h(d).$$

Oborem parametrů je $\mathbf{N}$, není-li uvedeno jinak.

Odhadneme dvě sumy a pak uvedeme dvě užitečné proměny sum v integrály.

Tvrzení 15 (harmonická čísla). *Pro $n\in\mathbf{N}$ platí asymptotika*

$$\sum_{m=1}^{n}\frac{1}{m}=\log n+\gamma+O(n^{-1}),$$

kde $\gamma=0.57221\ldots$ je Eulerova-Mascheroniova konstanta.

Důkaz. Rutiním výpočtem se zjistí, že

$$\int_m^{m+1}\frac{dx}{x}=\log(1+m^{-1})=\frac{1}{m}+z(m),$$

kde $z(m)=O(m^{-2})$. Proto

$$\begin{aligned}\sum_{m=1}^{n}\frac{1}{m} &= \int_1^{n+1}\frac{dx}{x}-\sum_{m=1}^{n}z(m)\\ &= \log(n+1)-\sum_{m=1}^{\infty}z(m)+\sum_{m=n+1}^{\infty}z(m).\end{aligned}$$

První člen v poslední rovnosti lze psát jako $\log n+O(n^{-1})$ (Taylorův rozvoj). Druhý člen je součtem konvergentní řady, označíme jej γ. Konečně třetí člen je zbytkem této řady. Protože $z(m)=O(m^{-2})$, dostaneme jednoduchým integrálním odhadem, že třetí člen je $O(n^{-1})$. $\diamondsuit$

Tvrzení 16 (logaritmus faktoriálu). *Pro $n \in \mathbf{N}$ platí asymptotika*

$$\sum_{m=1}^{n} \log m = n \log n - n + \tfrac{1}{2} \log n + c + O(n^{-1}),$$

kde $c \in \mathbf{R}$ je absolutní konstanta.

Důkaz. Pro $m \geq 2$ platí

$$\log m = \int_{m-1/2}^{m+1/2} \log x \cdot dx + O(m^{-2}).$$

Opravdu, s použitím Taylorova rozvoje pro logaritmus dostáváme

$$\begin{aligned}
(x \log x - x)|_{m-1/2}^{m+1/2} &= m \log \frac{m+1/2}{m-1/2} + \frac{\log(m^2 - 1/4)}{2} - 1 \\
&= m \log \left(1 + \frac{1}{m-1/2}\right) + \frac{\log(1 - 1/(4m^2))}{2} + \log m - 1 \\
&= \frac{m}{m-1/2} - \frac{m}{2(m-1/2)^2} - 1 + O(m^{-2}) + \log m \\
&= \frac{-1}{4(m-1/2)^2} + O(m^{-2}) + \log m \\
&= \log m + O(m^{-2}).
\end{aligned}$$

Proto, opět s použitím Taylorova rozvoje pro logaritmus,

$$\begin{aligned}
\sum_{m=2}^{n} \log m &= \sum_{m=2}^{n} \left(\int_{m-1/2}^{m+1/2} \log x \cdot dx + O(m^{-2}) \right) \\
&= c_1 + O(n^{-1}) + \int_{3/2}^{n+1/2} \log x \cdot dx \\
&= (n+1/2) \log(n+1/2) - (n+1/2) + c_2 + O(n^{-1}) \\
&= n \log n - n + \tfrac{1}{2} \log n + c + O(n^{-1}).
\end{aligned}$$

$\diamondsuit$

V kapitole 5, kde tento výsledek potřebujeme, by stačila již asymptotika

$$\sum_{m=1}^{n} \log m = n \log n - n + O(\log n).$$

Není však o mnoho těžší odvodit její silnější verzi, což jsme učinili. Po odlogaritmování popisuje rychlost růstu faktoriálu $n! = 1 \cdot 2 \cdot \ldots \cdot n$:

$$n! = (1 + O(n^{-1}))\mathrm{e}^c\sqrt{n}\left(\frac{n}{\mathrm{e}}\right)^n.$$

Lze ukázat (úloha 21), že $\mathrm{e}^c = \sqrt{2\pi}$. Takže, pro $n \in \mathbf{N}$,

$$n! = (1 + O(n^{-1}))\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n.$$

Tato asymptotika je známa jako *Stirlingova formule.* S pomocí vynalézavějších sumačních postupů, jejichž představitelem je následující identita, se Stirlingova formule dá dále zjemňovat (úloha 24).

Tvrzení 17 (speciální případ Eulerovy–MacLaurinovy formule). *Nechť má reálná funkce f na intervalu (a, b) spojitou druhou derivaci, reálná čísla a, b nejsou celá a funkce $\rho(x)$ a $\sigma(x)$ jsou definovány vztahy*

$$\rho(x) = 1/2 - \{x\} \quad a \quad \sigma(x) = \int_0^x \rho(u)du.$$

Potom platí identita

$$\sum_{a<i<b} f(i) = \int_a^b f(x)dx + \rho(x)f(x)|_a^b - \sigma(x)f'(x)|_a^b + \int_a^b \sigma(x)f''(x)dx.$$

DŮKAZ. Interval (a, b) rozdělíme celými čísly na intervaly $(a, \lceil a \rceil)$, $(\lceil a \rceil, \lceil a \rceil + 1), \ldots, (\lfloor b \rfloor, b)$. Poslední integrál vpravo rozložíme na součet integrálů přes tyto intervaly:

$$\int_a^b \sigma(x)f''(x)dx = \int_a^{\lceil a \rceil} + \sum_{n=\lceil a \rceil}^{\lfloor b \rfloor - 1} \int_n^{n+1} + \int_{\lfloor b \rfloor}^b.$$

Na každém z intervalů jsou $\rho(x)$ a $\sigma(x)$ spojitě diferencovatelné a $\sigma'(x) = \rho(x)$. Pro $m \in \mathbf{Z}$ máme rovnost $\sigma(m) = 0$ a jednostranné limity $\rho(m^-) = -1/2$ a $\rho(m^+) = 1/2$ ($\rho(x)$ je v celých číslech nespojitá; $\sigma(x)$ je všude spojitá). Dvakrát integrujeme per partes:

$$\begin{aligned}
\int_n^{n+1} \sigma(x)f''(x)dx &= \sigma(x)f'(x)|_n^{n+1} - \int_n^{n+1} \rho(x)f'(x)dx \\
&= 0 - \rho(x)f(x)|_{n^+}^{(n+1)^-} + \int_n^{n+1} \rho'(x)f(x)dx \\
&= \tfrac{1}{2}(f(n) + f(n+1)) - \int_n^{n+1} f(x)dx.
\end{aligned}$$

Podobně dostaneme

$$\begin{aligned}
\int_a^{\lceil a\rceil} \sigma(x)f''(x)dx &= -\sigma(a)f'(a)+\rho(a)f(a)+\tfrac{1}{2}f(\lceil a\rceil)-\int_a^{\lceil a\rceil} f(x)dx \\
\int_{\lfloor b\rfloor}^{b} \sigma(x)f''(x)dx &= \sigma(b)f'(b)-\rho(b)f(b)+\tfrac{1}{2}f(\lfloor b\rfloor)-\int_{\lfloor b\rfloor}^{b} f(x)dx.
\end{aligned}$$

Po dosazení do hořejší rovnosti získáme dokazovanou identitu. ♢

(Obecná Eulerova–MacLaurinova sumační formule je popsána v úlohách 22 a 23).

Podobným obratem je i *parciální* (též *Abelova*) *sumace*.

Tvrzení 18 (Abelova sumace). *Reálná funkce $f(x)$ měj pro $x \geq 1$ spojitou derivaci, $(h_n)_{n\in\mathbf{N}}$ buď posloupnost reálných čísel a $h(x)$ buď pro reálné $x \geq 1$ definována jako*

$$h(x) = \sum_{i\leq x} h_i.$$

Pak platí identita

$$\sum_{i\leq x} h_i f(i) = h(x)f(x) - \int_1^x h(t)f'(t)dt.$$

Důkaz. Pišme $m = \lfloor x\rfloor$. Počítejme:

$$\begin{aligned}
\sum_{i=1}^{m} h_i f(i) &= \sum_{i=1}^{m}(h(i)-h(i-1))f(i) \\
&= \sum_{i=1}^{m-1} h(i)(f(i)-f(i+1)) + h(m)(f(m)-f(x)) + h(m)f(x) \\
&= -\sum_{i=1}^{m-1} h(i)\int_i^{i+1} f'(t)dt - h(m)\int_m^x f'(t)dt + h(m)f(x) \\
&= -\int_1^x h(t)f'(t)dt + h(x)f(x).
\end{aligned}$$

♢

1.5 Poznámky

Sovětský psychiatr A. R. Lurija (1912–1971) byl zakladatelem a průkopníkem neuropsychiatrie. V knize [10] popsal, jaký osud připravila zázračná paměť bez hranic v objemu i v trvání svému nositeli. O P. Erdősovi se píše v osmé kapitole.

1.1 Číselné obory. Knihou o rozmanitých druzích čísel je Ebbinghaus [3]. Fascinujícím číselným světem jsou p-adická čísla, o nichž se zmiňujeme alespoň nyní. Viz například Ebbinghaus [3], Gouvêa [4], Koblitz [6].

1.2 Trocha aritmetiky. Euklidovým algoritmem začíná Knuthův gesamtkunstwerk [5], zajímavý i z hlediska teorie čísel. Koncepty a pojmy tohoto oddílu (rozklad na prvočísla, dělení se zbytkem, čínská věta o zbytku aj.) se zkoumají v dalekosáhlých zobecněních v komutativní algebře (Atiyah a Macdonald [1], Lang [8]) a algebraické teorii čísel (Borevič a Šafarevič [2], Lang [7]). Möbiova funkce byla kombinatoricky zobecněna (G.-C. Rota) na částečně uspořádané množiny, viz Lovász [9] nebo Stanley [11].

1.3 Algebraická čísla. Dotkli jsme se teorie symetrických funkcí. R. P. Stanley v úvodu k [12] píše: "Although the theory of symmetric functions and its connections with combinatorics is in my opinion one of the most beautiful topics in all of mathematics, it is a difficult subject for beginners to learn." Nyní se už můžeme naštěstí začíst do kapitoly 7 jeho knihy.

1.4 Asymptotika a sumy. Pro přímé náhrady sum integrály je místo Riemannova integrálu vhodnější integrál Stieltjesův (který „má $dF(x)$ místo dx“), viz **!doplnit!**.

1.6 Úlohy

1. (**0**) Dokažte, že čísla $\log_{10} 3$ a ϕ (zlatý řez) jsou iracionální.

2. (**1**) Dokažte, že číslo e je iracionální.

3. (**2**) Dokažte, že pro každá dvě čísla $m, n \in \mathbf{N}, m + n > 2$, je číslo $2^{1/m} + 3^{1/n}$ iracionální.

4. (**1**) Dokažte, že těleso $\mathbf{R}$ má jen triviální automorfismus $f(x) = x$.

5. (**0**) Jak vypadají automorfismy tělesa $\mathbf{C}$, které zobrazují reálná čísla zase na reálná čísla?

6. (**3**) Dokažte, že těleso $\mathbf{C}$ má alespoň $\aleph_2$ automorfismů.

7. (**0**) Dokažte, že na $\mathbf{C}$ se nedá definovat unární relace $x \succ 0$ („kladnost“), která by měla tyto vlastnosti: (i) pro každé $x \in \mathbf{C}$ nastává právě jedna z možností $x \succ 0, x = 0, -x \succ 0$ a (ii) z $x, y \succ 0$ plyne vždy $x + y \succ 0$ a $xy \succ 0$.

8. (**1**) Dokažte, že topologické prostory $\mathbf{R}$ a $\mathbf{C}$ (topologie jsou dány standardními metrikami) nejsou homeomorfní. Jinými slovy: Neexistuje v obou směrech spojitá bijekce mezi $\mathbf{R}$ a $\mathbf{C}$.

9. (**1**) Uvažte okruh $\mathbf{Z}[x, x^{1/2}, x^{1/4}, x^{1/8}, \ldots]$. Dokažte, že jde o obor integrity s jednotkami ± 1, v němž x není součinem konečně mnoha ireducibilních prvků.

10. (**1**) Uvažte okruh $\mathbf{Z}[\sqrt{-3}]$. Dokažte, že v něm každý prvek je součinem ireducibilních prvků, ale neplatí jednoznačnost rozkladu.

11. (**1**) Dokažte druhou Möbiovu inverzní formuli: Jsou-li f a g reálné funkce definované na $[1, \infty)$, platí ekvivalence
$$f(x) = \sum_{n \le x} g(x/n) \quad \text{pro všechna } x \ge 1 \iff$$
$$g(x) = \sum_{n \le x} f(x/n)\mu(n) \quad \text{pro všechna } x \ge 1.$$

12. (**1**) Dokažte explicitní vzorce pro funkce $d(n)$ a $\sigma(n)$ z oddílu 1.2.

13. (**1**) Nechť fa g jsou dvě aritmetické funkce a $f * g$ je nová aritmetická funkce: $(f*g)(n) = \sum_{d \backslash n} f(d)g(n/d)$. Operace $*$ se nazývá *Dirichletova konvoluce*. Ukažte, že vzhledem k $+$ (sčítání po složkách) a $*$ tvoří aritmetické funkce komutativní okruh s jedničkou, který nemá dělitele nuly (když $f, g \not\equiv 0$, tak i $f * g \not\equiv 0$), a jehož jednotkami (tj. prvky invertibilními vzhledem k $*$) jsou právě ty f, že $f(1) \neq 0$. Tento okruh označíme $\mathcal{A}$.

14. (**1**) Jak se dají definovat Möbiova funkce μ a Eulerova funkce φ pomocí operace $*$?

15. (**2**) Jsou-li f a g multiplikativní, jsou multiplikativní i $f*g$ a $*$-inverz f. To jest, multiplikativní funkce tvoří podgrupu grupy jednotek okruhu $\mathcal{A}$.

16. (**4**) Dokažte, že $\mathcal{A}$ je okruh s jednoznačným rozkladem. (Platí v něm obdoba základní věty aritmetiky.)

17. (**1**) Dokažte Eisensteinovo kritérium ireducibility: Pokud $a_n x^n + \cdots + a_1 x + a_0$ je celočíselný polynom takový, že $a_n \not\equiv 0 \bmod p$ a přitom $a_{n-1} \equiv a_{n-2} \equiv \cdots \equiv a_0 \equiv 0 \bmod p$, ale $a_0 \not\equiv 0 \bmod p^2$ pro nějaké prvočíslo p, je tento polynom ireducibilní (v $\mathbf{Q}[x]$).

18. (**1**) Odvoďte, že pro každé prvočíslo p je polynom $x^{p-1}+x^{p-2}+\cdots+x+1$ ireducibilní.

19. (**2**) Dokažte, že těleso $\mathbf{C}^{\,\mathrm{alg}}$ je algebraicky uzavřené. (Kořeny polynomu s algebraickými koeficienty jsou opět algebraická čísla.)

20. (**1**) Nechť $z \in \mathbf{C}^{\,\mathrm{alg}}$. Pak i $|z| \in \mathbf{C}^{\,\mathrm{alg}}$.

21. (**2**) Víme, že $n! \sim \sqrt{cn}(\frac{n}{\mathrm{e}})^n$, kde $c > 0$ je neznámá konstanta. Podle následujícího návodu spočítejte, že $c = 2\pi$.

    (a) Nechť $w_n = \int_0^{\pi/2} (\cos t)^n dt$. (To je tzv. *Wallisův integrál*.) Integrací per partes odvoďte rekurenci $nw_n = (n-1)w_{n-2}$ $(n \geq 2)$.

    (b) Pomocí této rekurence a předpokladu o $n!$ odvoďte, že $w_{2n} \sim \pi/\sqrt{2cn}$ a $w_{2n+1} \sim \sqrt{c/8n}$.

    (c) Dokažte, že $w_n \sim w_{n-1}$ a dopočtěte odtud c.

22. (**2**) *Bernoulliovy polynomy* $B_n(x) \in \mathbf{Q}[x]$ a *Bernoulliova čísla* $B_n \in \mathbf{Q}$ jsou definovány rozvoji:

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

Takže $B_n(0) = B_n$.

(a) Spočtěte, že $B_{2n+1} = 0$, kromě $B_1 = -1/2$, a

$$B_0 = 1,\ B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30},\ B_{10} = \frac{5}{66},$$

$$B_{12} = -\frac{691}{2730},\ B_{14} = \frac{7}{6},\ B_{16} = -\frac{3617}{510},\ B_{18} = \frac{43867}{798}, \ldots$$

(b) Odvoďte, že $B_n(x)$ splňují rekurenci

$$B_0(x) = 1,\ B_n(x) = n \cdot \int B_{n-1}(x)dx.$$

Ta vzhledem k $B_n(0) = B_n$ určuje $B_n(x)$ jednoznačně. Takže

$$B_1(x) = x - \tfrac{1}{2},\ B_2(x) = x^2 - x + \tfrac{1}{6},\ B_3(x) = x^3 - \tfrac{3}{2}x^2 + \tfrac{1}{2}x, \ldots$$

(c) Jako $\overline{B}_n(x)$ označíme zperiodičnění $\overline{B}_n(x) = B_n(x - \lfloor x \rfloor)$. Dokažte nerovnost $|\overline{B}_{2n}(x)| \leq B_{2n}$.

23. (**2**) Dokažte *obecnou Eulerovu–MacLaurinovu sumační formuli*: Pro funkci f s n spojitými derivacemi na intervalu $[a, b]$ platí identita

$$\begin{aligned}\sum_{k=a}^{b} f(k) = f(b) \quad &+ \quad \int_a^b f(x)dx \\ &+ \quad \sum_{i=1}^{n} \frac{B_i}{i!} f^{(i-1)}(x)|_a^b + \frac{(-1)^{n-1}}{n!} \int_a^b \overline{B}_n(x) f^{(n)}(x)dx.\end{aligned}$$

Poslední integrál se odhadne lehce díky nerovnosti v úloze 22 c.

24. (**2**) Jaké zpřesnění Stirlingovy formule dostaneme, použijeme-li předchozí výsledek pro $n = 4$?

Literatura

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra,* Addison-Wesley, Reading, Mass. 1969.

[2] Z. I. Borevič a I. R. Šafarevič, *Těorija čisel,* Mir, Moskva 1985. [Anglický překlad: Z. I. Borevich and I. R. Shafarevich, *Number theory,* Academic Press, New York 1966.]

[3] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel and R. Remmer, *Numbers,* Springer-Verlag, New York 1991. [Překlad německého vydání.]

[4] F. Q. Gouvêa, *p-adic numbers,* Springer-Verlag, Berlin 1997.

[5] D. E. Knuth, *The art of computer programming, Volumes 1–3,* Addison-Wesley, Reading, Mass. 1997 (Vol. 1) and 1998 (Vol. 2 and 3). [Jde o třetí (sv. 1 a 2) a druhé (sv. 3) vydání.]

[6] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions,* Springer-Verlag, Berlin 1984.

[7] S. Lang, *Algebraic number theory,* Springer-Verlag, Berlin 1994. [Druhé vydání, první v r. 1970 v Addison-Wesley.]

[8] S. Lang, *Algebra,* Addison-Wesley, Reading, Mass. 1965. [Třetí vydání v r. 1993.]

[9] L. Lovász, *Combinatorial problems and exercises,* Akadémiai Kiadó, Budapest 1993. [První vydání v r. 1979.]

[10] A. R. Lurija, *Malá knížka o velké paměti,* SPN, Praha 1973. [Překlad ruského vydání.]

[11] R. P. Stanley, *Enumerative combinatorics, Volume I,* Wadsworth & Brooks/Cole, Monterey, CA 1986. [Druhé vydání v r. 1997 v Cambridge University Press.]

[12] R. P. Stanley, *Enumerative combinatorics, Volume II,* Cambridge University Press, Cambridge, UK 1999.