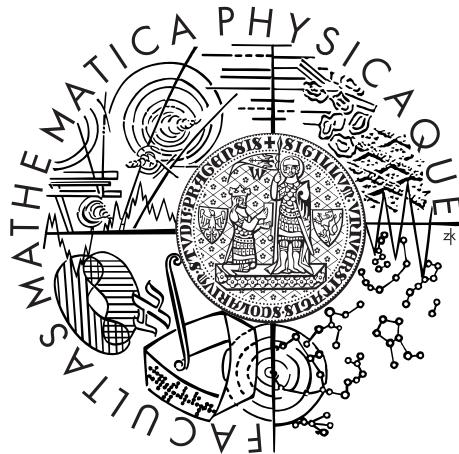


Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Dáša Krasnayová

O prúdovej šifre, ktorá využíva reťazové zlomky

Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2014

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

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

V dne

Podpis autora

Název práce: O proudové šifře, která využívá řetězové zlomky

Autor: Dáša Krasnayová

Katedra: Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Práce se zabývá teorií řetězových zlomků, na níž je založen návrh proudové šifry z článku [1]. Jelikož fakta o rozdělení pravděpodobnosti výskytu jednotlivých čísel jako částečných podílů v zobecněných řetězových zlomcích potřebné k prokázání bezpečnosti navrhované šifry nebyla dosud dokázána, v práci jsou shrnutы dosavadní poznatky, které by mohly vést k jejich prokázání. Jde zejména o základní vlastnosti klasických a zobecněných řetězových zlomků a důkaz Kuzminovy věty, jejímž důsledkem je rozdělení pravděpodobnosti výskytu jednotlivých přirozených čísel jako částečných podílů klasických řetězových zlomků. V práci je také návrh šifry z článku [1] stručně představen.

Klíčová slova: řetězové zlomky, proudová šifra, Kuzminova věta

Title: A stream cipher based on continued fractions

Author: Dáša Krasnayová

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: This bachelor thesis deals with the theory of continued fractions which is design of a stream cipher in [1] based on. Since results about probability for a positive integer number to be a partial quotient of a generalised continued fraction which are necessary for proving the cipher secure, has not been proved yet, there are summarized previous results which could lead to proving them. In particular, basic properties of classical and generalised continued fractions and proof of Kuzmin theorem are presented here. Distribution of probability for a positive integer number to be a partial quotient of a classical continued fraction follows from Kuzmin theorem. The design of the stream cipher from [1] is briefly introduced at the end of the thesis.

Keywords: continued fractions, stream cipher, Kuzmin theorem

Názov práce: O prúdovej šifre, ktorá využíva reťazové zlomky

Autor: Dáša Krasnayová

Katedra: Katedra algebry

Vedúci bakalárskej práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Práca sa zaobrá teóriou reťazových zlomkov, na ktorej je založený návrh prúdovej šifry z článku [1]. Keďže fakty o rozdelení pravdepodobnosti výskytu jednotlivých čísel ako čiastočných podielov v zovšeobecnených reťazových zlomkoch potrebné k dokázaniu bezpečnosti navrhovanej šifry neboli dosiaľ dokázané, v práci sú zhrnuté doterajšie poznatky, ktoré by mohli viest' k ich dokázaniu. Ide najmä o základné vlastnosti klasických a zovšeobecnených reťazových zlomkov a dôkaz Kuzminovej vety, ktorej dôsledkom je rozdelenie pravdepodobnosti výskytu jednotlivých prirodzených čísel ako čiastočných podielov klasických reťazových zlomkov. V práci je tiež návrh šifry z článku [1] stručne predstavený.

Kľúčové slová: reťazové zlomky, prúdová šifra, Kuzminova veta

Obsah

Úvod	1
1 Klasické reťazové zlomky a niektoré ich vlastnosti	2
2 Gaussov problém a Kuzminova veta	6
3 Vlastnosti zovšeobecnených reťazových zlomkov	32
4 Návrh prúdovej šifry	36
Záver	39
Zoznam použitej literatúry	40

Úvod

Pôvodnou myšlienkou práce bolo analyzovať šifru popísanú v článku [1]. Pri bližšom zoznámení sa s článkom sa však ukázalo, že popis šifry je málo jasný a navyše predpokladá isté matematické fakty, ktoré nie sú dokázané, ale uvedené iba ako hypotéza. Ide presnejšie o Hypotézu 4.1, ktorá sa týka frekvencií výskytu jednotlivých čísel ako čiastočných podielov v zovšeobecnených reťazových zlomkoch.

Ked'že akýkoľvek dôkaz tejto hypotézy pravdepodobne bude vychádzať zo známej teórie pre klasické reťazové zlomky a túto teóriu bude d'alej rozvíjať, bolo prirodzené sa s touto teóriou podrobnejšie zoznámiť. Ukázalo sa, že to samo o sebe je úloha, ktorá vyžaduje značné úsilie, pretože klasický text Chinčina [2], ktorý pochádza z polovice štyridsiatych rokov, nie je na niektorých miestach formulovaný úplne presne a na viacerých miestach je dosť neprehľadný.

Výsledkom je teda štruktúra práce taká, že v prvej kapitole sa pripomínajú základné pojmy súvisiace s klasickými reťazovými zlomkami vrátane dôkazu tvrdenia o tom, kedy je zlomok periodický (to je v určitom vzťahu k doporučenej voľbe parametrov šifry).

V druhej kapitole sa dokazuje Kuzminova veta, na ktorej základe možno frekvenciu výskytu čiastočných podielov relatívne jednoducho odvodiť. V tretej kapitole sa uvádzajú niektoré základné vlastnosti zovšeobecnených reťazových zlomkov. Samotná šifra je potom v štvrtnej kapitole iba stručne popísaná. V tejto kapitole je tiež naznačnené, čím je nutné sa d'alej zaoberať, ak má byť šifra dotiahnutá do rigorózneho podania.

Ťažisko práce je teda v jej finálnej podobe v druhej kapitole.

Kapitola 1

Klasické reťazové zlomky a niektoré ich vlastnosti

Definícia 1.1 (reťazový zlomok). Nech $(a)_{n=0}^{\infty} = a_0, a_1, \dots$, $(b)_{n=1}^{\infty} = b_1, b_2, \dots$ sú postupnosti reálnych (prípadne komplexných) čísel. Ak sú obe postupnosti konečné alebo má postupnosť (a) o jeden člen viac ako postupnosť (b) , potom zápis týchto postupností v tvare

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{\ddots}}}}$$

sa nazýva (zovšeobecnený) reťazový zlomok. V prípade, že sú postupnosti konečné, hovoríme o konečnom reťazovom zlomku, inak je to nekonečný reťazový zlomok. Čísla a_0, a_1, \dots nazývame čiastočné podielmy a čísla b_1, b_2, \dots čiastočné čitatele.

V prípade, že $b_1 = b_2 = b_3 = \dots = 1$, $a_0 \in \mathbb{Z}$ a $a_1, a_2, \dots \in \mathbb{N}$ zápis nazývame klasický reťazový zlomok.

Poznámka. Ak je reťazový zlomok konečný, vieme mu priradiť hodnotu

$$x = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{\ddots + \cfrac{b_n}{a_n}}}}}.$$

Zápisom $[a_0; a_1, a_2, \dots, a_n]$ rozumieme hodnotu reťazového zlomku s čiastočnými podielmi a_0, a_1, \dots, a_n a čiastočnými čitateľmi rovnými 1. V prípade, že je $a_0 = 0$, používa sa pre túto hodnotu značenie $[a_1, a_2, \dots, a_n]$.

Poznámka (Výpočet klasického reťazového zlomku). Vezmieme $x \in \mathbb{R}$

- Do a_0 priradíme dolnú celú časť x , do x priradíme $x - a_0$.
- Ak je $x = 0$, potom už máme všetky koeficienty. Ak nie, do x priradíme $\frac{1}{x}$ a opakujeme postup v predošлом bode pre a_1 . Opakujeme, kým nie je $x = 0$.

Postup sa zastaví práve vtedy, ak x bolo racionálne číslo. Inak dostaneme nekonečný reťazový zlomok. Čiastočné podiely v nekonečnom reťazovom zlomku sú určené jednoznačne. Pri konečnom nastáva nejednoznačnosť pri poslednom člene, pretože

$$\frac{1}{k} = \frac{1}{(k-1) + \frac{1}{1}}$$

pre každé $k \in \mathbb{N}$.

Definícia 1.2 (kvadratické iracionálne číslo). *Prirodzené číslo sa nazýva bezštvorcové, ak je rôzne od 1 a nie je deliteľné druhou mocninou prvočísla. Iracionálne číslo nazveme kvadratické iracionálne číslo (iracionálne stupňa 2), ak je koreňom polynómu stupňa 2 s racionálnymi koeficientami. (Teda ak ho môžeme zapísat v tvare $a + b\sqrt{d}$, kde $a, b, d \in \mathbb{Q}$, $b \neq 0$, $d > 0$ a d je bezštvorcové.)*

Tvrdenie 1.1. Nech α je iracionálne číslo, $[a_0; a_1, a_2, \dots]$ reťazový zlomok α . Rekurentne definujeme postupnosti p a q ako $p_{r+1} = p_r a_{r+1} + p_{r-1}$ a $q_{r+1} = q_r a_{r+1} + q_{r-1}$, kde $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$. Označíme α_r také číslo, že

$$\alpha = [a_0; a_1, a_2, \dots, a_r + \alpha_r] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_r + \alpha_r}}}.$$

Potom platí:

1. Čísla p_r a q_r sú nesúdelitel'né,
2. $\frac{p_r}{q_r} = [a_0; a_1, a_2, \dots, a_r]$,
3. $\alpha = \frac{p_r + \alpha_r p_{r-1}}{q_r + \alpha_r q_{r-1}}$,
4. $p_r q_{r+1} - p_{r+1} q_r = (-1)^{r+1}$,
5. $q_r \geq 2^{\frac{r-1}{2}}$,
6. Postupnosť $\left(\frac{p_r}{q_r}\right)_{r=0}^{\infty}$ konverguje k α .

Dôkaz. Body 1.-4. a 6. sú známe výsledky z prednášky Teorie čísel a RSA [3], bod 5. plynie z nerovnosti

$$q_r = a_r q_{r-1} + q_{r-2} \geq q_{r-1} + q_{r-2} \geq 2q_{r-2}.$$

□

Poznámka. Analogicky môžeme postupnosti p a q definovať aj pre α racionálne. Vtedy má reťazový zlomok α n členov pre nejaké $n \in \mathbb{N}$, teda tieto postupnosti definujeme iba pre $r = 0, 1, \dots, n$. Budú platiť vzťahy 1. - 5. rovnako ako pre nekonečné zlomky a 6. v zmysle, že rozdiel medzi p_i/q_i a α sa zmenšuje, keď i rastie od 0 do n .

Definícia 1.3. Číslo $\frac{p_r}{q_r}$ z predošlého Tvrdenia nazývame r -tý konvergent α .

Veta 1.2. Majme nakoniec periodický klasický reťazový zlomok

$$u_0 + [\mathbf{u}, \bar{\mathbf{v}}] = u_0 + [\mathbf{u}, \mathbf{v}, \mathbf{v}, \dots] = [u_0; u_1, u_2, \dots, u_s, v_1, \dots, v_t, v_1, \dots, v_t, \dots].$$

Potom príslušné reálne číslo $\alpha = u_0 + [\mathbf{u}, \bar{\mathbf{v}}]$ je kvadratické iracionálne číslo. Naošak platí, že klasický reťazový zlomok kvadratického racionálneho čísla je nakoniec periodický.

Dôkaz. (Podľa [4]) Ak $\alpha = u_0 + [\mathbf{u}, \bar{\mathbf{v}}]$, potom α určite nie je racionálne číslo, lebo zlomok by bol konečný. Teda vieme napísat $\alpha = u_0 + [\mathbf{u} + \beta]$, kde $\beta = [\mathbf{v} + \beta]$.

Podľa Tvrdenia 1.1 platí $\beta = \frac{p_t + \beta p_{t-1}}{q_t + \beta q_{t-1}}$, kde $\frac{p_t}{q_t}$ je t -ty konvergent β . Po úprave

$$q_{t-1}\beta^2 + (q_t - p_{t-1})\beta - p_t = 0,$$

z čoho plynie, že β je kvadratické iracionálne číslo, teda α ním bude tiež.

Pre dôkaz opačným smerom, predpokladajme, že α je kvadratické iracionálne číslo v tvare $a + b\sqrt{d}$, kde $a, b \in \mathbb{Q}$, $b \neq 0$ a $d \in \mathbb{N}$ bezštvorcové. Bez ujmy na všeobecnosti môžeme predpokladať, že $0 < \alpha < 1$, teda $a_0 = 0$. α môžeme prepísat do tvaru $(\theta \pm \sqrt{\phi})/\psi$, kde $\theta, \phi, \psi \in \mathbb{Z}$ a $\phi, \psi \neq 0$. Z tohto tvaru to môžeme prepísat do tvaru $\alpha = (s \pm \sqrt{t})/r$, kde $s, t, r \in \mathbb{Z}$, $t, r > 0$ a $r \mid (t - s^2)$ rozšírením pôvodného zlomku menovateľom ψ , teda $s = \psi\theta$, $t = \psi^2\phi$ a $r = \psi^2$.

Najprv uvážime prípad kedy $x = (s + \sqrt{t})/r$, kde $r > 0$, $r \mid (t - s^2)$, $t > s^2$ a $0 < x < 1$. Urobíme jeden krok algoritmu na výpočet reťazového zlomku. Dostaneme $x^* = 1/x - \lfloor 1/x \rfloor = 1/x - k$ pre nejaké $k \in \mathbb{N}$. Toto k je príslušným čiastočným podielom x . Ak označíme $r^* = (t - s^2)/r > 0$ a $s^* = -s - kr^*$, potom

$$x^* = \frac{r}{\sqrt{t} + s} - k = \frac{r(\sqrt{t} - s)}{t - s^2} - k = \frac{\sqrt{t} - s}{r^*} - k = \frac{\sqrt{t} + (-s - kr^*)}{r^*} = \frac{\sqrt{t} + s^*}{r^*}.$$

Vieme, že $0 < x^* < 1$ z toho, ako sme získali x^* . Keďže $r^* > 0$, platí $\sqrt{t} + s^* > 0$ a teda $-s^* < \sqrt{t}$. Z predpokladu platí $|s| < \sqrt{t}$ a navyše $k, r^* > 0$, teda

$$s^* = -s - kr^* < -s < \sqrt{t},$$

čiže dokopy $|s^*| < \sqrt{t}$, respektíve $(s^*)^2 < t$. Navyše platí

$$t - (s^*)^2 = t - s^2 - skr^* - (kr^*)^2 = r^*(r - sk - k^2r^*),$$

teda $r^* \mid (t - (s^*)^2)$.

Nový zlomok $x^* = (s^* + \sqrt{t})/r^*$ teda spĺňa rovnaké predpoklady ako pôvodné x . Po každom takomto kroku algoritmu teda dostaneme dvojicu (s, r) , ktorá spĺňa

$s^2 < t$ a $r \mid (t-s^2)$. Ked'že t je prirodzené číslo, vhodných celých čísel s vieme nájsť iba konečne veľa. Ak zvolíme s pevne, potom pre r musí platiť $r \mid (t - s^2)$, teda pre každé s je iba konečne veľa vhodných čísel r . Preto je aj rôznych dvojíc (s,r) konečne veľa. Dvojica (s,r) jednoznačne určuje x , ktoré určuje k , teda čiastočný podiel v reťazovom zlomku a tiež všetky nasledujúce x^* a (s^*,t^*) . Ked'že dvojíc je iba konečne veľa, po niekoľkých iteráciách dostaneme dvojicu, ktorú sme už dostali predtým a postupnosť dvojíc, ktoré dostávame bude od istého člena periodická. Preto bude periodická aj postupnosť x , ktoré dostávame a príslušných čiastočných podielov k . Zlomok teda bude nakoniec periodický.

Všimnime si, že prípad $x = (s - \sqrt{t})/r$, kde $r > 0$, $r \mid (t - s^2)$ a $t > s^2$ nikdy nenastáva, lebo x je z celom priebehu algoritmu v intervale $(0,1)$.

Nakoniec uvažujme ostatné prípady, kedy $x = (s \pm \sqrt{t})/r$, kde $r > 0$, $r \mid (t - s^2)$, $t < s^2$ a $0 < x < 1$. Môžeme si všimnúť, že určite platí $s > 0$, inak by bolo x menšie ako 0. Ďalej postupujeme analogicky ako v prvom prípade, ale tentokrát $r^* = (s^2 - t)/r > 0$ a $s^* = s - kr^*$, kde $k = \lfloor 1/x \rfloor$. Zjavne opäť platí podobný vzťah $x^* = (s^* \pm \sqrt{t})/r^*$. Ked'že $s^* < s$, po každej iterácii sa s v zlomku zmenší až kým po konečne veľa iteráciách nenastane $t > s^2$, čím sa dostávame opäť k prvemu prípadu. □

Kapitola 2

Gaussov problém a Kuzminova veta

Z kryptografického hľadiska nás môže zaujímať pravdepodobnosť výskytu jednotlivých prirodzených čísel v reťazových zlomkoch reálnych čísel. Keďže pre všetky čísla, až na racionálne, ku ktorým sa vrátim neskôr, sú čiastočné podiely jednoznačne určené a je ich nekonečne veľa, môžeme sa na čiastočný podiel a_n dívať ako na funkciu $a_n(\alpha)$, kde $\alpha \in \mathbb{R}$. Nultý čiastočný podiel a_0 je rovný $\lfloor \alpha \rfloor$, teda pravdepodobnosť, že $a_0 = k$, kde $k \in \mathbb{N}$ je rovná pravdepodobnosti, že $\alpha \in [k, k+1)$. Nasledujúce čiastočné podiely od nultého nezávisia, teda ďalej predpokladajme, že $a_0(\alpha) = 0$ a $\alpha \neq 0$, čiže $\alpha \in (0,1)$.

Funkcia $a_1(\alpha) = \lfloor 1/\alpha \rfloor$ môže nadobúdať všetky rôzne hodnoty $k \in \mathbb{N}$. Z predpisu funkcie plynie, že $a_1(\alpha) = k$ práve vtedy, ak $k \leq 1/\alpha < k+1$, čo odpovedá

$$\frac{1}{k+1} < \alpha \leq \frac{1}{k}.$$

V prípade, že nastáva rovnosť, platí $\alpha = 1/k$. Vtedy nastáva nejednoznačnosť v zápise α v tvare reťazového zlomku, pretože

$$\alpha = \frac{1}{k} = \cfrac{1}{k-1 + \cfrac{1}{1}}.$$

Pre tieto α teda nebude funkcia a_1 definovaná. Vidíme, že funkcia a_1 je konštantná na všetkých intervaloch $(1/(k+1), 1/k)$. Tieto intervaly nazývame *intervaly prvého rádu*. Môžeme si všimnúť, že interval $(0,1)$ je až na množinu $\{1/k | k = 2, 3, \dots\}$ spočítateľným zjednotením intervalov prvého rádu.

Zvolíme si pevne interval $(1/(k+1), 1/k)$ a pozrieme sa, ako sa správa funkcia $a_2(\alpha)$ na tomto intervale. Keďže sa nachádzame na intervale $(1/(k+1), 1/k)$,

$$\alpha = \cfrac{1}{k + \cfrac{1}{r}},$$

kde $r \in \mathbb{R}$ a $r > 1$. Potom $a_2(\alpha) = \lfloor r \rfloor$, teda $a_2(\alpha) = \ell$ práve vtedy, keď $\ell \leq r < \ell + 1$, čiže

$$\frac{1}{k + \frac{1}{\ell}} \leq \alpha < \frac{1}{k + \frac{1}{\ell+1}}.$$

Ak nastáva rovnosť, opäť dochádza k nejednoznačnosti zápisu, takže funkciu a_2 nedefinujeme pre hodnoty, na ktorých nie je definovaná funkcia a_1 a navyše hodnoty $\{1/(k+1/\ell) | k, \ell = 1, 2, 3, \dots\}$. Funkcia a_2 je teda opäť konštantná na intervaloch tvaru

$$\left(\frac{\frac{1}{k} + \frac{1}{\ell}}{k + \frac{1}{\ell}}, \frac{\frac{1}{k+1} + \frac{1}{\ell+1}}{k + \frac{1}{\ell+1}} \right),$$

ktoré nazývame *intervaly druhého rádu*. Môžeme si všimnúť, že zjednotením týchto intervalov pre $\ell = 1, 2, \dots$ dostávame interval $(1/(k+1), 1/k)$, bez niektorých racionálnych čísel. Ak teraz zjednotíme všetky tieto zjednotené intervale $(1/(k+1), 1/k)$, dostávame až na niektoré racionálne čísla interval $(0, 1)$.

Ak si to teda zhrnieme, množina čísel α , pre ktoré $a_1(\alpha) = k$, odpovedá práve jednému konkrétnemu intervalu prvého rádu a množina čísel α , pre ktoré $a_2(\alpha) = \ell$, odpovedá spočítateľnému zjednoteniu intervalov druhého rádu (z každého intervalu prvého rádu sa vyberie práve jeden). Každý interval prvého rádu je jednoznačne určený číslom $k \in \mathbb{N}$ a každý interval druhého rádu dvojicou (k, ℓ) , kde $k, \ell \in \mathbb{N}$. Ak neberieme do úvahy krajné body, každý interval prvého rádu sa pri vyšetrovaní priebehu a_2 rozdelí na spočítateľne veľa intervalov druhého rádu. Intervalov druhého rádu bude teda opäť spočítateľne veľa a ich zjednotením dostaneme interval $(0, 1)$.

Podobným postupom a vyšetrovaním funkcií $a_1(\alpha), a_2(\alpha), a_3(\alpha), \dots$ vieme postupne konštruovať intervale vyšších rádov.

Definícia 2.1 (Interval n -tého rádu). *Nech $n \in \mathbb{N}$, k_1, k_2, \dots, k_n je n -ticia prirodzených čísel. Potom interval*

$$J = \{\alpha | \alpha \in (0, 1), a_i(\alpha) = k_i \text{ pre všetky } i = 1, \dots, n, \alpha \neq [k_1, \dots, k_n]\}$$

nazveme intervalom n -tého rádu. Množinu všetkých intervalov rádu n označujeme \mathcal{J}_n .

Tvrdenie 2.1. *Nech $J \in \mathcal{J}_n$ určený n -ticou k_1, k_2, \dots, k_n . Potom jeho krajné body sú*

$$\frac{p_n}{q_n} \text{ a } \frac{p_n + p_{n-1}}{q_n + q_{n-1}},$$

kde p_n/q_n je spoločný n -tý konvergent čísel z J .

Dôkaz. Každé číslo $\alpha \in J$ môžeme zapisať v tvare $\alpha = [k_1, k_2, \dots, k_n + \alpha_n]$, pričom $\alpha_n \in (0, 1)$, teda si môžeme hned' všimnúť, že všetky čísla z J majú rovnaké všetky konvergenty $p_1/q_1, \dots, p_n/q_n$, pretože tieto sú určené číslami k_1, \dots, k_n . Naopak, ak volíme rôzne $\alpha_n \in (0, 1)$, dostaneme jednoznačne určené α z intervalu J . Funkcia g definovaná ako $g(\gamma) = [k_1, \dots, k_n + \gamma]$ je teda bijekcia medzi intervalom $(0, 1)$ a intervalom J . S využitím vzťahov z Tvrdenia 1.1 platí, že

$$\begin{aligned} g(\gamma) - \frac{p_n}{q_n} &= \frac{p_n + \gamma p_{n-1}}{q_n + \gamma q_{n-1}} - \frac{p_n}{q_n} = \frac{p_n q_n + \gamma p_{n-1} q_n - p_n q_n - \gamma p_n q_{n-1}}{q_n (q_n + \gamma q_{n-1})} \\ &= \frac{(-1)^{n-1} \gamma}{q_n (q_n + \gamma q_{n-1})} = \frac{(-1)^{n-1}}{q_n \left(q_n \frac{1}{\gamma} + q_{n-1} \right)}. \end{aligned}$$

Z toho výplýva, že g je monotónou funkciou na intervale $(0,1)$. Z limit

$$\lim_{\gamma \rightarrow 0^+} g(\gamma) = \lim_{\gamma \rightarrow 0^+} \frac{p_n + \gamma p_{n-1}}{q_n + \gamma q_{n-1}} = \frac{p_n}{q_n}$$

$$\lim_{\gamma \rightarrow 1^-} g(\gamma) = \lim_{\gamma \rightarrow 1^-} \frac{p_n + \gamma p_{n-1}}{q_n + \gamma q_{n-1}} = \frac{p_n + p_{n-1}}{q_n + q_{n-1}}$$

teda plynie, že $\frac{p_n}{q_n}$ a $\frac{p_n + p_{n-1}}{q_n + q_{n-1}}$ sú krajné body intervalu J .

□

Poznámka. Intervaly n -tého rádu odpovedajú n -ticiam prirodzených čísel k_1, \dots, k_n a pre každý interval n -tého rádu vieme pomocou tejto n -tice definovať konvergenty $p_1/q_1, \dots, p_n/q_n$. Zápisom

$$\sum^{(n)}$$

označujeme skrátený zápis pre sumu

$$\sum_{(k_1, \dots, k_n), k_i \in \mathbb{N}},$$

teda sumu cez všetky n -tice prirodzených čísel. Ak sa v tejto sume vyskytujú $p_1, \dots, p_n, q_1, \dots, q_n$, potom odpovedajú čitateľom alebo menovateľom konvergentov určených n -ticami, cez ktoré suma prebieha.

Zjednotením všetkých intervalov rádu n bude interval $(0,1)$ bez racionálnych čísel, ktoré sú krajnými bodmi intervalov n -tého rádu.

Definícia 2.2. Ak je $A \subseteq (0,1)$, zápisom $\mathfrak{M}A$ označujeme Lebesgueovu mieru množiny A .

Ked'že krajné body intervalu J sú $\frac{p_n}{q_n}$ a $\frac{p_n + p_{n-1}}{q_n + q_{n-1}}$, platí

$$\begin{aligned} \mathfrak{M}J &= \left| \frac{p_n}{q_n} - \frac{p_n + p_{n-1}}{q_n + q_{n-1}} \right| = \left| \frac{p_n q_n + p_n q_{n-1} - p_n q_n - p_{n-1} q_n}{q_n (q_n + q_{n-1})} \right| \\ &= \left| \frac{(-1)^n}{q_n (q_n + q_{n-1})} \right| = \frac{1}{q_n (q_n + q_{n-1})}. \end{aligned}$$

Zjednotením všetkých intervalov n -tého rádu je interval $(0,1)$ až na niektoré racionálne čísla. Miera množiny všetkých racionálnych čísel je nulová a zjednotenie intervalov n -tého rádu je spočítateľné, preto platí

$$\sum_{J \in \mathcal{J}_n} \mathfrak{M}J = 1.$$

Definícia 2.3. Nech $n_1, n_2, \dots, n_s, k_1, k_2, \dots, k_s \in \mathbb{N}$, potom zápisom

$$E \begin{pmatrix} n_1, & n_2, & \dots, & n_s \\ k_1, & k_2, & \dots, & k_s \end{pmatrix}$$

rozumieme množinu všetkých $\alpha \in (0,1)$, pre ktoré $a_{n_i}(\alpha)$ je definované a $a_{n_i}(\alpha) = k_i$ pre všetky $i = 1, 2, \dots, s$.

Pomocou tohto zápisu môžeme vyjadriť aj konkrétny interval J rádu n určeného hodnotami $a_i = k_i$, $i \in \{1, \dots, n\}$. Platí

$$J = E \begin{pmatrix} 1, & 2, & \dots, & n \\ k_1, & k_2, & \dots, & k_n \end{pmatrix}.$$

Ďalej pre všetky $\ell = 1, \dots, s$ platí vzťah

$$\bigcup_{k_\ell=1}^{\infty} E \begin{pmatrix} n_1, & \dots, & n_{\ell-1}, & n_\ell, & n_{\ell+1}, & \dots, & n_s \\ k_1, & \dots, & k_{\ell-1}, & k_\ell, & k_{\ell+1}, & \dots, & k_s \end{pmatrix} = E \begin{pmatrix} n_1, & \dots, & n_{\ell-1}, & n_{\ell+1}, & \dots, & n_s \\ k_1, & \dots, & k_{\ell-1}, & k_{\ell+1}, & \dots, & k_s \end{pmatrix},$$

ked'že a_{n_ℓ} je pre každé α rovné nejakému prirodzenému číslu. Z toho potom dostávame, že platí rovnosť

$$\bigcup_{J \in \mathcal{J}_{n+1}, a_{n+1}=k} J = E \begin{pmatrix} n+1 \\ k \end{pmatrix},$$

kde ľavá strana rovnice je rovná zjednoteniu všetkých intervalov $(n+1)$ -ého rádu určených hodnotami $a_i = k_i$ pre $i \in \{1, \dots, n\}$ a $a_{n+1} = k$. Pre miery týchto množín potom platí

$$\sum_{J \in \mathcal{J}_{n+1}, a_{n+1}=k} \mathfrak{M}_J = \mathfrak{M}_E \begin{pmatrix} n+1 \\ k \end{pmatrix},$$

protože zjednotenie $J \in \mathcal{J}_{n+1}$ bolo spočítateľné.

Pravdepodobnosť výskytu čísla $k \in \mathbb{N}$ ako n -tého čiastočného podielu odpovedá miere množiny $E \begin{pmatrix} n \\ k \end{pmatrix}$, takže nasledujúce úvahy a veta povedú k jej určeniu.

Tento výsledok nás bude zaujímať pre n dostatočne veľké, chceme sa teda dopracovať k

$$\lim_{n \rightarrow \infty} \mathfrak{M}_E \begin{pmatrix} n \\ k \end{pmatrix}.$$

Gaussov problém Pre $x \in [0,1]$ definujme funkciu $m_n(x)$ ako mieru množiny čísel $\alpha \in (0,1)$, pre ktoré je α_n definované a $\alpha_n < x$. Bez ujmy na všeobecnosti môžeme predpokladať, že všetky čísla α sú iracionálne, pretože $m_n(x)$ je miera a racionálne čísla mieru množiny nezmenia. Pre α iracionálne platí, že α_n je definované pre všetky n a je z intervalu $(0,1)$.

Gauss v jednom zo svojich listov dokázal vetu, z ktorej plynie, že

$$\lim_{n \rightarrow \infty} m_n(x) = \frac{\ln(1+x)}{\ln 2},$$

kde x je z intervalu $[0,1]$. V tomto liste ďalej naznačil, že by bolo užitočné dobre approximovať rozdiel

$$m_n(x) - \lim_{n \rightarrow \infty} m_n(x)$$

pre $x \in [0,1]$ a n dostatočne veľké. To dokázal až Kuzmin a dôkaz bude nižšie reprodukovany.

Lema 2.2. Postupnosť funkcií m_0, m_1, \dots definovaných vyššie splňa funkcionálnu rovnosť

$$m_{n+1}(x) = \sum_{k=1}^{\infty} \left\{ m_n \left(\frac{1}{k} \right) - m_n \left(\frac{1}{k+x} \right) \right\}$$

pre každé $x \in [0,1]$ a $n = 0, 1, \dots$

Dôkaz. Nech $x \in [0,1]$. Označme $M = \{\alpha \in (0,1) | \alpha \text{ iracionálne}, \alpha_{n+1} < x\}$. Ak zvolíme ľubovoľné iracionálne $\alpha \in (0,1)$, platí vzťah

$$\alpha_n = \frac{1}{a_{n+1} + \alpha_{n+1}}.$$

Položme $k = a_{n+1}$. Potom nerovnosť $\alpha_{n+1} < x$ je ekvivalentná s nerovnosťou

$$\frac{1}{k+x} < \alpha_n < \frac{1}{k}. \quad (2.1)$$

Z tejto nerovnosti plynie, že

$$M = \bigcup_{k \geq 1} \left(M \cap E \left(\binom{n+1}{k} \right) \right).$$

Z nerovnosti (2.1) ďalej plynie, že miera množiny $M \cap E \left(\binom{n+1}{k} \right)$ je rovná

$$m_n \left(\frac{1}{k} \right) - m_n \left(\frac{1}{k+x} \right).$$

Z aditivity miery teda dostávame

$$m_{n+1}(x) = \mathfrak{M}M = \sum_{k=1}^{\infty} \left\{ m_n \left(\frac{1}{k} \right) - m_n \left(\frac{1}{k+x} \right) \right\}.$$

□

Poznámka. Môžeme si všimnúť, že funkcia $\varphi(x) = C \ln(1+x)$ splňa analogickú rovnicu

$$\varphi(x) = \sum_{k=1}^{\infty} \left\{ \varphi \left(\frac{1}{k} \right) - \varphi \left(\frac{1}{k+x} \right) \right\}.$$

Tento vzťah overíme priamo dosadením.

$$\begin{aligned} \sum_{k=1}^{\infty} \left\{ \varphi \left(\frac{1}{k} \right) - \varphi \left(\frac{1}{k+x} \right) \right\} &= C \sum_{k=1}^{\infty} \left\{ \ln \left(1 + \frac{1}{k} \right) - \ln \left(1 + \frac{1}{k+x} \right) \right\} \\ &= C \sum_{k=1}^{\infty} \left\{ \ln \left(\frac{k+1}{k} \right) - \ln \left(\frac{k+x+1}{k+x} \right) \right\} \\ &= C \sum_{k=1}^{\infty} \{ \ln(k+1) - \ln(k) - \ln(k+x+1) + \ln(k+x) \}. \end{aligned}$$

Definujeme postupnosť čiastočných súčtov

$$\begin{aligned}
s_n &= C \sum_{k=1}^n \{\ln(k+1) - \ln(k) - \ln(k+x+1) + \ln(k+x)\} \\
&= C\{(\ln(2) - \ln(1) - \ln(2+x) + \ln(1+x)) + (\ln(3) - \ln(2) - \ln(3+x) + \ln(2+x)) + \\
&\quad + \dots + (\ln(n+1) - \ln(n) - \ln(n+1+x) + \ln(n+x))\} \\
&= C(\ln(1+x) - \ln(1) + \ln(n+1) - \ln(n+1+x)) = C \left(\ln(1+x) + \ln \left(\frac{n+1}{n+1+x} \right) \right)
\end{aligned}$$

pre $n \in \mathbb{N}$. Platí

$$\begin{aligned}
\sum_{k=1}^{\infty} \left\{ \varphi \left(\frac{1}{k} \right) - \varphi \left(\frac{1}{k+x} \right) \right\} &= \lim_{n \rightarrow \infty} s_n = C \lim_{n \rightarrow \infty} \ln(1+x) + \ln \left(\frac{n+1}{n+1+x} \right) \\
&= C \ln(1+x) = \varphi(x).
\end{aligned}$$

Formulujme niekoľko užitočných viet z matematickej analýzy a teórie miery a integrálu.

Veta 2.3 (Weiestrassova veta,[5],7.10). *Nech $\{f_n\}$ je postupnosť reálnych funkcií definovaných na množine E a existuje postupnosť reálnych čísel M_1, M_2, \dots taká, že*

$$|f_n(x)| \leq M_n$$

pre všetky $x \in E$ a $n = 1, 2, \dots$, potom ak rad $\sum_{n=1}^{\infty} M_n$ konverguje, potom rad $\sum_{n=1}^{\infty} f_n(x)$ konverguje rovnomerne na množine E .

Veta 2.4 (Derivovanie radu člen po člene). *Nech $\{f_n\}$ je postupnosť reálnych funkcií spojitej na intervale $[a,b]$. Nech sú tieto funkcie navýše diferencovateľné na intervale (a,b) a rad $\sum_{n=1}^{\infty} f_n(x)$ konverguje aspoň v jednom bode intervalu (a,b) .*

Potom ak $\sum_{n=1}^{\infty} f'_n(x)$ konverguje rovnomerne na intervale (a,b) , aj rad $\sum_{n=1}^{\infty} f_n(x)$ konverguje rovnomerne na celom intervale (a,b) a platí

$$\left(\sum_{n=1}^{\infty} f_n(x) \right)' = \sum_{n=1}^{\infty} f'_n(x).$$

Dôkaz. Táto veta je dosledkom vety 7.17, [5]. □

Nasledujúcu vetu som v tomto znení nenašla v štandardných učebniciach, preto uvádzam verziu z anglickej Wikipedie [6] s dôkazom.

Veta 2.5 (Prvá veta o strednej hodnote pre integráciu). *Nech $a < b$ sú reálne čísla, $G(x)$ je reálna funkcia spojitá na intervale $[a,b]$ a $\varphi(x)$ je reálna funkcia, ktorá je integrovateľná na (a,b) a na tomto intervale nemení znamienko. Potom existuje $\xi \in (a,b)$ také, že*

$$\int_a^b G(t)\varphi(t)dt = G(\xi) \int_a^b \varphi(t)dt.$$

Dôkaz. Bez ujmy na všeobecnosti predpokladajme, že $\varphi(x) \geq 0$ pre všetky $x \in [a,b]$. Ak $\varphi(x) \leq 0$ na intervale $[a,b]$, dôkaz prejde rovnako, zmení sa len smer nerovnosti. Keďže G je spojitá na uzavretom intervale $[a,b]$, podľa Vety o nadobúdaní maxima a minima (tiež Veta 4.16, [5]) nadobúda v nejakých bodoch $p,q \in [a,b]$ konečné maximum $G(p) = M$ a konečné minimum $G(q) = m$. Máme teda nerovnosť $m \leq G(x) \leq M$ pre všetky $x \in [a,b]$. Z tejto nerovnosti, vzťahu $\varphi(x) \geq 0$ na intervale $[a,b]$ a monotónnosti integrálu dostávame

$$mI = \int_a^b m\varphi(t)dt \leq \int_a^b G(t)\varphi(t)dt \leq \int_a^b M\varphi(t)dt = MI,$$

kde

$$I = \int_a^b \varphi(t)dt.$$

Ak $I = 0$, potom dostávame

$$0m \leq \int_a^b G(t)\varphi(t)dt \leq MI,$$

teda

$$\int_a^b G(t)\varphi(t)dt = 0 = 0.G(x)$$

pre všetky $x \in [a,b]$, teda veta platí. Prepočítajme teda, že $I > 0$. Potom platí

$$G(p) = m \leq \frac{1}{I} \int_a^b G(t)\varphi(t)dt \leq M = G(q).$$

Keďže G je spojitá, z Vety o nadobúdaní medzhodôt (Veta 4.23, [5]) dostávame existenciu ξ z otvoreného intervalu s krajinými bodmi p a q pre ktoré

$$G(\xi) = \frac{1}{I} \int_a^b G(t)\varphi(t)dt,$$

teda dostávame

$$IG(\xi) = G(\xi) \int_a^b \varphi(t)dt = \int_a^b G(t)\varphi(t)dt.$$

□

Veta 2.6 (O zámene limity a integrálu, [5], 7.16). *Nech $a < b$ sú reálne čísla, f_1, f_2, \dots je postupnosť reálnych funkcií integrovateľných na intervale $[a,b]$. Ak táto postupnosť rovnomerne konverguje k funkcií f na intervale $[a,b]$, potom aj f je integrovateľná na tomto intervale a platí*

$$\int_a^b f(x)dx = \lim_{n \rightarrow \infty} \int_a^b f_n(x)dx.$$

Veta 2.7 (O zámene sumy a integrálu, [5], Dôsledok Vety 7.16). *Nech f_1, f_2, \dots je postupnosť funkcií integrovateľných na intervale $[a,b]$ a $f(x) = \sum_{n=1}^{\infty} f_n(x)$ konverguje rovnomerne na intervale $[a,b]$, potom platí*

$$\int_a^b f(x) dx = \sum_{n=1}^{\infty} \int_a^b f_n(x) dx.$$

Veta 2.8 (O strednej hodnote, [5], 5.10). *Nech $a < b$ sú reálne čísla. Ak je f reálna funkcia, ktorá je spojité na intervale $[a,b]$ a diferencovateľná na intervale (a,b) , potom existuje $\xi \in (a,b)$ pre ktoré*

$$f'(\xi) = \frac{f(a) - f(b)}{a - b}.$$

Veta 2.9 ([5], 6.13). *Ak f je reálna funkcia integrovateľná na intervale $[a,b]$, potom funkcia $|f|$ je na tomto intervale tiež integrovateľná a platí*

$$\left| \int_a^b f(x) dx \right| \leq \int_a^b |f(x)| dx.$$

Našim hlavným cieľom teraz bude dokázať Kuzminovu vetu 2.19. K tomu slúži ako pomocná nasledujúca definícia.

Definícia 2.4 (Vlastnosti (σ) a (ε)). *Hovoríme, že postupnosť kladných reálnych funkcií $f_0(x), f_1(x), \dots$ má vlastnosť (σ) , ak pre všetky $x \in [0,1]$ a $n \geq 0$ platí*

$$f_{n+1}(x) = \sum_{k=1}^{\infty} \left\{ \frac{1}{(k+x)^2} f_n \left(\frac{1}{k+x} \right) \right\}.$$

Reálna funkcia f má vlastnosť (ε) s parametrami $\mu, M > 0$, teda skrátene má vlastnosť $(\varepsilon : \mu, M)$, ak má deriváciu na intervale $(0,1)$, deriváciu sprava v bode 0, deriváciu zľava v bode 1 a pre všetky $x \in [0,1]$ platí

$$\begin{aligned} 0 &< f(x) < M \\ |f'(x)| &< \mu. \end{aligned}$$

Kuzminova veta ukazuje, že ak má postupnosť f_0, f_1, \dots vlastnosť (σ) a f_0 má vlastnosť $(\varepsilon : \mu, M)$, potom

$$\lim_{n \rightarrow \infty} f_n = \frac{a}{1+x},$$

kde

$$a = \frac{1}{\ln 2} \int_0^1 f_0(z) dz.$$

Zároveň odhaduje rýchlosť tejto konvergencie. Dôkaz sa opiera o niekoľko prípravných lemov, kde Lema 2.10 ukazuje súvislosť s reťazovými zlomkami. Ďalšie lemy sa dokazujú štandardnými prostriedkami. Ukážeme, že f_n má vlastnosť

$$\left(\varepsilon : \frac{\mu}{2^{n-3}} + 4M, 2M \right),$$

že hodnota $S = \int_0^1 f_n(x)dx$ nezávisí na voľbe n . Klúčová je Lema 2.16, v ktorej sa ukazuje, že $f_n(x)$ možno zdola odhadnúť hodnotou $S/2 - \mu/2^n$. Táto Lema potom nie je použitá priamo pre f_n , ale pre funkcie

$$f_n(x) - \frac{t}{1+x} \text{ a } \frac{T}{1+x} - f_n(x),$$

kde t a T sú zvolené najprv tak, že

$$\frac{t}{1+x} < f_0(x) < \frac{T}{1+x}.$$

Použitie Lemy 2.16 na tieto funkcie vedie k zlepšeniu pôvodného odhadu. Tento postup je vhodným spôsobom iterovaný tak, že v limite dostaneme požadovaný odhad konvergencie.

Lema 2.10. *Nech postupnosť kladných reálnych funkcií $f_0(x), f_1(x), \dots$ má vlastnosť (σ) . Potom pre všetky $n \geq 0$ a $x \in [0,1]$ platí*

$$f_n(x) = \sum_{k=1}^{(n)} f_0 \left(\frac{p_n + xp_{n-1}}{q_n + xq_{n-1}} \right) \frac{1}{(q_n + xq_{n-1})^2}, \quad (2.2)$$

kde suma prebieha cez všetky n -tice prirodzených čísel $k_1, k_2, \dots, k_n, p_n/q_n$ a $(p_n + p_{n-1})/(q_n + q_{n-1})$ sú krajiné body intervalu n -tého rádu určeného hodnotami k_1, \dots, k_n . (Mohli sme teda tiež povedať, že suma prebieha cez všetky intervale n -tého rádu.)

Dôkaz. Postupujeme indukciou podľa n . Pre $n = 0$ rovnosť (2.2) platí triviálne, pretože $\mathcal{J}_0 = \{(0,1)\}$, $p_0 = 0$, $q_0 = 1$, $p_{-1} = 1$ a $q_{-1} = 0$. Na pravej strane dostávame

$$f_0 \left(\frac{0+x}{1+0 \cdot x} \right) \frac{1}{1+0 \cdot x} = f_0(x),$$

čo sme chceli.

Predpokladajme, že rovnosť (2.2) platí pre nejaké $n \in \mathbb{N}$. Z vlastnosti (σ) a s využitím indukčného predpokladu platí

$$\begin{aligned} f_{n+1}(x) &= \sum_{k=1}^{\infty} \left\{ \frac{1}{(k+x)^2} f_n \left(\frac{1}{k+x} \right) \right\} \\ &= \sum_{k=1}^{\infty} \frac{1}{(k+x)^2} \sum_{l=1}^{(n)} f_0 \left(\frac{p_n + \frac{1}{k+x} p_{n-1}}{q_n + \frac{1}{k+x} q_{n-1}} \right) \frac{1}{\left(q_n + \frac{1}{k+x} q_{n-1} \right)^2} \\ &= \sum_{k=1}^{\infty} \frac{1}{(k+x)^2} \sum_{l=1}^{(n)} f_0 \left(\frac{p_n k + p_{n-1} + p_n x}{q_n k + q_{n-1} + q_n x} \right) \frac{(k+x)^2}{(q_n k + q_{n-1} + q_n x)^2} \\ &= \sum_{k=1}^{\infty} \sum_{l=1}^{(n)} f_0 \left(\frac{p_n k + p_{n-1} + p_n x}{q_n k + q_{n-1} + q_n x} \right) \frac{1}{(q_n k + q_{n-1} + q_n x)^2}. \end{aligned}$$

Tieto dve sumy môžeme vymeniť, lebo hodnoty, ktoré sčítame sú kladné. Suma cez všetky n -tice prirodzených čísel a následne cez všetky prirodzené čísla k potom odpovedá sume cez všetky $(n+1)$ -tice, kde posledný člen odpovedá k . Inak povedané, ak si zafixujeme n -ticu a_1, \dots, a_n a postupne volíme $k = 1, 2, \dots$, prechádzame všetky intervaly $(n+1)$ -ého rádu v intervale n -tého rádu určenom n -ticou a_1, a_2, \dots . Výraz $p_{nk} + p_{n-1}$ odpovedá podľa Tvrdenia 1.1 menovateľu $(n+1)$ -ého konvergentu ľubovoľného čísla α z intervalu $(n+1)$ -ého rádu určeného touto $(n+1)$ -ticou. Podobne $q_{nk} + q_{n-1}$ odpovedá q_{n+1} . Dokopy teda dostávame

$$f_{n+1}(x) = \sum^{(n+1)} f_0 \left(\frac{p_{n+1} + p_n x}{q_{n+1} + q_n x} \right) \frac{1}{(q_{n+1} + q_n x)^2}.$$

□

Lema 2.11. Nech $n \in \mathbb{N}$ a a_1, \dots, a_n je n -tica prirodzených čísel. Nech q_n je menovateľ čiastočného podielu určeného touto n -ticou. Potom platí

$$\frac{1}{(q_n + xq_{n-1})^2} < \frac{2}{q_n(q_n - q_{n-1})}$$

pre všetky $x \in [0,1]$.

Dôkaz. Platí

$$\begin{aligned} 2(q_n + xq_{n-1})^2 - q_n(q_n + q_{n-1}) &= q_n^2 + (4x - 1)q_n q_{n-1} + 2xq_{n-1}^2 \\ &\geq q_n^2 - q_n q_{n-1} > 0, \end{aligned}$$

protože x berieme z intervalu $[0,1]$ a $q_n > q_{n-1}$ pre všetky $n \in \mathbb{N}$. Z toho už priamo plynie, že

$$\frac{1}{(q_n + xq_{n-1})^2} < \frac{2}{q_n(q_n + q_{n-1})}.$$

□

Poznámka. Môžeme si všimnúť, že pomocou vlastnosti (σ) z obmedzenej funkcie $f_0(x)$ môžno jednoznačne definovať postupnosť $f_0(x), f_1(x), \dots$, ktorá bude mať túto vlastnosť.

Dôkaz. Nech $|f_0(x)| < M$ pre všetky $x \in [0,1]$. Potom podľa Lemy 2.11 platí

$$\left| \sum^{(n)} f_0 \left(\frac{p_n + xp_{n-1}}{q_n + xq_{n-1}} \right) \frac{1}{(q_n + xq_{n-1})^2} \right| < M \sum^{(n)} \frac{1}{(q_n + xq_{n-1})^2} < 2M$$

konverguje rovnomerne pre ľubovoľné n , teda podľa Lemy 2.10

$$f_n = \sum^{(n)} f_0 \left(\frac{p_n + xp_{n-1}}{q_n + xq_{n-1}} \right) \frac{1}{(q_n + xq_{n-1})^2}$$

je dobre definovaná funkcia na $[0,1]$.

□

Lema 2.12. Nech f_0, f_1, \dots je postupnosť kladných reálnych funkcií, ktoré majú vlastnosť (σ) . Ďalej prepokladajme, že f_0 má vlastnosť $(\varepsilon : \mu, M)$ pre nejaké kladné reálne čísla μ a M . Potom pre ľubovoľné $n = 0, 1, \dots$ platí, že postupnosť f_n, f_{n+1}, \dots má vlastnosť (σ) a navyše f_n má vlastnosť

$$\left(\varepsilon : \frac{\mu}{2^{n-3}} + 4M, 2M \right).$$

Okrem toho existuje také $n_0 \in \mathbb{N}$, že pre všetky $n \geq n_0$ má funkcia f_n vlastnosť $(\varepsilon : 5M, 2M)$.

Dôkaz. To, že postupnosť funkcií f_n, f_{n+1}, \dots má vlastnosť (σ) plynie priamo z toho, že postupnosť f_0, f_1, \dots má túto vlastnosť, pretože je časťou tejto postupnosti.

Podľa Lemy 2.10 platí pre $f_n(x)$ rovnosť (2.2). Na základe odhadu z predošej Lemy 2.11 a vlastnosti $(\varepsilon : \mu, M)$, ktorú má f_0 , môžeme odhadnúť pravú stranu tejto rovnosti

$$\sum_{n=0}^{\infty} f_0 \left(\frac{p_n + xp_{n-1}}{q_n + xq_{n-1}} \right) \frac{1}{(q_n + xq_{n-1})^2} < \sum_{n=0}^{\infty} M \frac{2}{q_n(q_n + q_{n-1})} = 2M \sum_{J \in \mathcal{J}_n} \mathfrak{M} J = 2M.$$

Pre f_n teda platí

$$0 \leq f_n(x) \leq 2M.$$

Daný rad navyše konverguje rovnomerne podľa Vety 2.3 na intervale $[0,1]$, teda určite konverguje v jednom bode. S využitím Vety 2.4 dokážeme, že f_n má deriváciu na tomto intervale. Nech $\kappa = (k_1, \dots, k_n)$ je n -tica prirodzených čísel. Potom funkcia

$$\varphi_\kappa = f_0 \left(\frac{p_n + xp_{n-1}}{q_n + xq_{n-1}} \right) \frac{1}{(q_n + xq_{n-1})^2}$$

má zjavne deriváciu pre každú n -ticu κ (resp. dvojicu p_n, q_n) na celom intervale $[0,1]$, v krajných bodoch ide o jednostranné derivácie. Ak túto funkciu derivujeme, dostávame

$$\begin{aligned} \varphi'_\kappa(x) &= f'_0(u) \frac{p_{n-1}(q_n + xq_{n-1}) - q_{n-1}(p_n + xp_{n-1})}{(q_n + xq_{n-1})^2} \frac{1}{(q_n + xq_{n-1})^2} \\ &\quad + f_0(u) \cdot (-2) \cdot \frac{1}{(q_n + xq_{n-1})^3} q_{n-1} \\ &= f'_0(u) \frac{(-1)^{n-1}}{(q_n + xq_{n-1})^4} - 2f_0(u) \frac{q_{n-1}}{(q_n + xq_{n-1})^3}, \end{aligned}$$

kde

$$u = \frac{p_n + xp_{n-1}}{q_n + xq_{n-1}}.$$

S využitím Tvrdenia 1.1 platí

$$q_n(q_n + q_{n-1}) > q_n^2 > 2^{n-1}$$

a f_0 má vlastnosť $(\varepsilon : \mu, M)$. Ak navyše použijeme odhad z Lemy 2.11, môžeme odhadnúť $\varphi'_\kappa(x)$ nasledovne

$$\begin{aligned} |\varphi'_\kappa(x)| &< \left| f'_0(u) \left(\frac{2}{q_n(q_n + q_{n-1})} \right)^2 + 2f_0(u) \frac{q_{n-1}}{q_n + xq_{n-1}} \frac{2}{q_n(q_n + q_{n-1})} \right| \\ &< \frac{1}{q_n(q_n + q_{n-1})} \left(\mu \frac{4}{q_n(q_n + q_{n-1})} + 4M \frac{q_{n-1}}{q_n + xq_{n-1}} \right) \\ &< \frac{1}{q_n(q_n + q_{n-1})} \left(\frac{4\mu}{2^{n-1}} + 4M \right) = \frac{1}{q_n(q_n + q_{n-1})} \left(\frac{\mu}{2^{n-3}} + 4M \right). \end{aligned}$$

Všimnime si, že tento odhad nezávisí od x . Ked'že platí

$$\sum_{n=1}^{\infty} \frac{1}{q_n(q_n + q_{n-1})} = \sum_{n=1}^{\infty} \mathfrak{M} J_n = 1,$$

dostávame

$$\sum_{n=1}^{\infty} \frac{1}{q_n(q_n + q_{n-1})} \left(\frac{\mu}{2^{n-3}} + 4M \right) = \frac{\mu}{2^{n-3}} + 4M,$$

z čoho plynie, že rad

$$\sum_{\kappa=(k_1, \dots, k_n), k_i \in \mathbb{N}} \varphi'_\kappa(x)$$

rovnomerne konverguje podľa Vety 2.3. Predpoklady Vety 2.4 sú teda splnené a dostávame, že funkcia

$$f_n(x) = \sum_{\kappa=(k_1, \dots, k_n), k_i \in \mathbb{N}} \varphi_\kappa(x) = \sum_{n=1}^{\infty} f_0 \left(\frac{p_n + xp_{n-1}}{q_n + xq_{n-1}} \right) \frac{1}{(q_n + xq_{n-1})^2}$$

má deriváciu na intervale $[0,1]$ a navyše

$$|f'_n(x)| = \left| \sum_{\kappa=(k_1, \dots, k_n), k_i \in \mathbb{N}} \varphi_\kappa(x) \right| < \sum_{n=1}^{\infty} \frac{1}{q_n(q_n + q_{n-1})} \left(\frac{\mu}{2^{n-3}} + 4M \right) = \frac{\mu}{2^{n-3}} + 4M.$$

Dokopy teda dostávame, že f_n má vlastnosť $(\varepsilon : \frac{\mu}{2^{n-3}} + 4M, 2M)$. Ked'že platí

$$\lim_{n \rightarrow \infty} \frac{\mu}{2^{n-3}} = 0,$$

určite existuje $n_0 \in \mathbb{N}$, také, že pre všetky $n \geq n_0$ platí

$$\frac{\mu}{2^{n-3}} < M,$$

teda tiež platí

$$|f'_n(x)| < 5M.$$

□

Lema 2.13. Postupnosť funkcií

$$F_0(x) = F_1(x) = \dots = \frac{C}{1+x},$$

kde $x \in [0,1]$ a C je reálna konšanta, má vlastnosť (σ) .

Dôkaz. Vlastnosť overíme priamo dosadením.

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{1}{(k+x)^2} F_n \left(\frac{1}{k+x} \right) &= \sum_{k=1}^{\infty} \frac{1}{(k+x)^2} \frac{C}{1+\frac{1}{k+x}} = C \sum_{k=1}^{\infty} \frac{1}{(k+x)^2} \frac{k+x}{k+x+1} \\ &= C \sum_{k=1}^{\infty} \frac{1}{k+x} \frac{1}{k+x+1}. \end{aligned}$$

Platí

$$\frac{1}{k+x} - \frac{1}{k+x+1} = \frac{k+x+1-k-x}{(k+x)(k+x+1)} = \frac{1}{(k+x)(k+x+1)},$$

teda dostávame

$$\sum_{k=1}^{\infty} \frac{1}{(k+x)^2} F_n \left(\frac{1}{k+x} \right) = C \sum_{k=1}^{\infty} \frac{1}{k+x} - \frac{1}{k+x+1}.$$

Definujme čiastočné súčty

$$\begin{aligned} s_n &= C \sum_{k=1}^n \frac{1}{k+x} - \frac{1}{k+x+1} \\ &= C \left(\frac{1}{1+x} - \frac{1}{2+x} + \frac{1}{2+x} - \frac{1}{3+x} + \dots + \frac{1}{n+x} - \frac{1}{n+1+x} \right) \\ &= C \left(\frac{1}{1+x} - \frac{1}{n+1+x} \right). \end{aligned}$$

Platí

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{1}{(k+x)^2} F_n \left(\frac{1}{k+x} \right) &= \lim_{n \rightarrow \infty} s_n = \lim_{n \rightarrow \infty} C \left(\frac{1}{1+x} - \frac{1}{n+1+x} \right) = \frac{C}{1+x} \\ &= F_{n+1}(x). \end{aligned}$$

□

Lema 2.14. Nech f_0, f_1, \dots je postupnosť reálnych funkcií definovaných na intervale $[0,1]$, $0 < t < T$ sú reálne konštanty a platí

$$\frac{t}{1+x} < f_0(x) < \frac{T}{1+x}$$

pre všetky $x \in [0,1]$. Potom platí

$$\frac{t}{1+x} < f_n(x) < \frac{T}{1+x}$$

pre všetky $x \in [0,1]$ a $n \geq 0$.

Dôkaz. Prepokladajme, že Lema platí až do nejakého $n \in \mathbb{N}_0$. Ak označíme $h(x) = 1/(1+x)$ a $H(x) = T/(1+x)$, zjavne platí

$$h\left(\frac{1}{k+x}\right) = \frac{t}{1 + \frac{1}{k+x}} < f_n\left(\frac{1}{k+x}\right) < \frac{T}{1 + \frac{1}{k+x}} = H\left(\frac{1}{k+x}\right)$$

pre všetky $x \in [0,1]$ a $k = 1, 2, \dots$, pretože $1/(k+x) \in [0,1]$. Z vlastnosti (σ) plynie

$$\sum_{k=1}^{\infty} h\left(\frac{1}{k+x}\right) \frac{1}{(k+x)^2} < f_{n+1}(x) < \sum_{k=1}^{\infty} H\left(\frac{1}{k+x}\right) \frac{1}{(k+x)^2}.$$

Podľa Lemy 2.13 platí

$$\sum_{k=1}^{\infty} h\left(\frac{1}{k+x}\right) \frac{1}{(k+x)^2} = h(x)$$

a

$$\sum_{k=1}^{\infty} H\left(\frac{1}{k+x}\right) \frac{1}{(k+x)^2} = H(x)$$

pre všetky $x \in [0,1]$, teda platí

$$\frac{t}{1+x} = h(x) < f_{n+1}(x) < H(x) = \frac{T}{1+x}.$$

Dôkaz teda plynie z indukcie. □

Lema 2.15. Nech f_0, f_1, \dots je postupnosť reálnych funkcií, ktorá má vlastnosť (σ) . Nech navyše f_0 má vlastnosť $(\varepsilon : \mu, M)$. Potom platí

$$\int_0^1 f_0(z) dz = \int_0^1 f_n(z) dz$$

pre všetky $n \geq 0$.

Dôkaz. Z vlastnosti (σ) plynie

$$\int_0^1 f_n(z) dz = \int_0^1 \sum_{k=1}^{\infty} f_{n-1}\left(\frac{1}{k+z}\right) \frac{dz}{(k+z)^2}.$$

Ked'že f_0 má vlastnosť $(\varepsilon : \mu, M)$, z Lemou 2.12 plynie, že $0 \leq f_{n-1}(x) \leq 2M$. Teda platí

$$\sum_{k=1}^{\infty} f_{n-1}\left(\frac{1}{k+z}\right) \frac{1}{(k+z)^2} < 2M \sum_{k=1}^{\infty} \frac{1}{(k+z)^2} \leq 2M \sum_{k=1}^{\infty} \frac{1}{k^2}$$

pre všetky $z \in [0,1]$, teda podľa Vety 2.3 tento rad konverguje rovnomerne na intervale $[0,1]$. Podľa Vety 2.7 môžeme vymeniť sumu a integrál. Dostávame teda

$$\int_0^1 f_n(z) dz = \sum_{k=1}^{\infty} \int_0^1 f_{n-1} \left(\frac{1}{k+z} \right) \frac{dz}{(k+z)^2}.$$

Použijeme substitúciu $1/(k+z) = u$, teda $-dz/(k+z)^2 = du$. Pre $z = 0$ je $u = 1/k$ a pre $z = 1$ je $u = 1/(k+1)$. Medze sú teda $1/(k+1)$ (horná) a $1/k$ (spodná). Dostávame teda

$$\sum_{k=1}^{\infty} - \int_{\frac{1}{k}}^{\frac{1}{k+1}} f_{n-1}(u) du = \sum_{k=1}^{\infty} \int_{\frac{1}{k+1}}^{\frac{1}{k}} f_{n-1}(u) du = \int_0^1 f_{n-1}(u) du.$$

Dôkaz teda už plynie z indukcie. □

Lema 2.16. Nech f_0, f_1, \dots je postupnosť reálnych funkcií, ktorá má vlastnosť (σ) a nech f_0 má navyše vlastnosť $(\varepsilon : \mu, M)$, potom pre každé $n \geq 0$ a $x \in [0,1]$ platí

$$f_n(x) > -\frac{\mu}{2^n} + \frac{1}{2} S,$$

kde

$$S = \int_0^1 f_0(z) dz.$$

Dôkaz. Nech $n \geq 0$ a $x \in [0,1]$. Vyjdeme z Lemy 2.10, ktorá hovorí, že

$$f_n(x) = \sum_{u=0}^{(n)} f_0(u) \frac{1}{(q_n + xq_{n-1})^2},$$

kde

$$u = \frac{p_n + xp_{n-1}}{q_n + xq_{n-1}}.$$

Ked'že platia nerovnosti $q_n + xq_{n-1} \leq q_n + q_{n-1} < 2q_n$ a $f_0(x) > 0$ pre všetky $x \in [0,1]$, dostávame

$$f_n(x) > \frac{1}{2} \sum_{u=0}^{(n)} f_0(u) \frac{1}{q_n(q_n + q_{n-1})}. \quad (2.3)$$

Postupnosť f_0, f_1, \dots splňa tiež predpoklady Lemy 2.15, teda platí

$$\int_0^1 f_0(x) dx = \int_0^1 f_n(x) dx = \int_0^1 \sum_{u=0}^{(n)} f_0(u) \frac{1}{(q_n + xq_{n-1})^2} dx,$$

kde $u = (p_n + xp_{n-1})/(q_n + xq_{n-1})$.

Každá z funkcií

$$f_0(u) \frac{1}{(q_n + xq_{n-1})^2}$$

je integrovateľná na $[0,1]$. Keďže $0 < f_0(x) < M$ je obmedzená funkcia a

$$\sum_{n=1}^{\infty} \frac{1}{(q_n + xq_{n-1})^2} < \sum_{n=1}^{\infty} \frac{2}{q_n(q_n + q_{n-1})} = 2,$$

suma na pravej strane rovnomerne konverguje, teda podľa Vety 2.7 môžeme prehodiť sumu a integrál. Funkcia φ_0 je navýše spojitá na intervale $[0,1]$ a funkcia $1/q_n(q_n + q_{n-1})$ je integrovateľná na intervale $[0,1]$, z Vety 2.5 o strednej hodnote pre integráciu teda vyplýva, že pre každý interval $J \in \mathcal{J}_n$ existuje taký body u'_J , že

$$\int_0^1 f_0(u) \frac{1}{(q_n + xq_{n-1})^2} dx = f(u'_J) \int_0^1 \frac{1}{(q_n + xq_{n-1})^2} dx,$$

kde u'_J je z intervalu J rádu n . Pripomeňme, že krajné body J sú $(p_n + p_{n-1})/(q_n + q_{n-1})$ a p_n/q_n . Nakoniec ešte vypočítame

$$\begin{aligned} \int_0^1 \frac{1}{(q_n + xq_{n-1})^2} dx &= \frac{1}{q_n} \int_{q_n}^{q_n + q_{n-1}} \frac{1}{y^2} dy = \frac{1}{q_n} \left[-\frac{1}{y} \right]_{q_n}^{q_n + q_{n-1}} = \frac{1}{q_n} \left(-\frac{1}{q_n + q_{n-1}} + \frac{1}{q_n} \right) \\ &= \frac{1}{q_n(q_n + q_{n-1})}. \end{aligned}$$

Z toho plynie, že platí rovnosť

$$\frac{1}{2} \int_0^1 f_0(z) dz = \frac{1}{2} \sum_{n=1}^{\infty} f_0(u'_J) \frac{1}{q_n(q_n + q_{n-1})}. \quad (2.4)$$

Zo vzťahov (2.3) a (2.4) dostávame

$$f_n(x) - \frac{1}{2} \int_0^1 f_0(z) dz > \frac{1}{2} \sum_{n=1}^{\infty} (f_0(u) - f_0(u'_J)) \frac{1}{q_n(q_n + q_{n-1})}. \quad (2.5)$$

Funkcia f_0 je spojitá na intervale s krajnými bodmi u a u'_J a má na tomto intervale deriváciu. Z Vety 2.8 o strednej hodnote potom existuje c_J z tohto intervalu také, že

$$f'_0(c_J) = \frac{f_0(u) - f_0(u')}{u - u'}.$$

Ak použijeme odhad z vlastnosti (ε)

$$|f'_0(c_J)| < \mu,$$

ktorý platí pre všetky $c_J \in (0,1)$, dostávame

$$|f_0(u) - f_0(u')| < (\mu) |u - u'| < \frac{\mu}{q_n(q_n + q_{n-1})} < \frac{\mu}{q_n^2} < \frac{\mu}{2^{n-1}},$$

teda

$$f_0(u) - f_0(u') > -\frac{\mu}{2^{n-1}}.$$

Z nerovnosti (2.5) potom dostávame

$$f_n(x) > \frac{1}{2} \int_0^1 f_0(z) dz - \frac{\mu}{2^n} = -\frac{\mu + g}{2^n} + S,$$

kde

$$S = \frac{1}{2} \int_0^1 f_0(z) dz.$$

□

Lema 2.17. Nech f_0, f_1, \dots je postupnosť reálnych funkcií definovaných na intervale $[0,1]$, $0 < t < T$ sú reálne konštanty a nech pre všetky $x \in [0,1]$ platí

$$\frac{t}{1+x} < f_0(x) < \frac{T}{1+x}.$$

Potom platí

1. ak má postupnosť f_0, f_1, \dots vlastnosť (σ) , potom aj postupnosť funkcií $f_0(x) - t/(1+x), f_1(x) - t/(1+x), \dots$ má vlastnosť (σ) ,
2. ak funkcia f_0 má vlastnosť $(\varepsilon : \mu, M)$, potom funkcia $f_0 - t/(1+x)$ má vlastnosť $(\varepsilon : \mu + t, M)$,
3. ak má postupnosť f_0, f_1, \dots vlastnosť (σ) , potom aj postupnosť funkcií $T/(1+x) - f_0(x), T/(1+x) - f_1(x), \dots$ má vlastnosť (σ) ,
4. ak funkcia f_0 má vlastnosť $(\varepsilon : \mu, M)$, potom funkcia $T/(1+x) - f_0(x)$ má vlastnosť $(\varepsilon : \mu + T, T)$.

Dôkaz. Označme $\varphi_n(x) = f_n(x) - t/(1+x)$ a $\psi_n(x) = T/(1+x) - f_n(x)$ pre $n = 0, 1, \dots$

1. Platí

$$\begin{aligned} & \sum_{k=1}^{\infty} \left\{ \frac{1}{(k+x)^2} \varphi_n \left(\frac{1}{k+x} \right) \right\} \\ &= \sum_{k=1}^{\infty} \left\{ \frac{1}{(k+x)^2} f_n \left(\frac{1}{k+x} \right) \right\} - \sum_{k=1}^{\infty} \left\{ \frac{1}{(k+x)^2} \frac{t}{1+\frac{1}{k+1}} \right\}. \end{aligned}$$

Ked'že postupnosť f_0, f_1, \dots má vlastnosť (σ) a postupnosť rovnakých funkcií $t/(1+x)$ má podľa Lemy 2.13 tiež vlastnosť (σ) , platí

$$\sum_{k=1}^{\infty} \left\{ \frac{1}{(k+x)^2} \varphi_n \left(\frac{1}{k+x} \right) \right\} = f_{n+1}(x) - \frac{t}{1+x} = \varphi_{n+1}(x).$$

Postupnosť funkcií $\varphi_0, \varphi_1, \dots$ má teda vlastnosť (σ) .

2. Ked'že $t/(1+x) < f_0(x)$, platí $\varphi_0(x) > 0$ pre všetky $x \in [0,1]$. f_0 má vlastnosť $(\varepsilon : \mu, M)$ a $t/(1+x) > 0$, teda platí

$$\varphi_0(x) = f_0(x) - \frac{t}{1+x} < M$$

pre všetky $x \in [0,1]$. Ďalej platí, že

$$\varphi'_0(x) = f'_0(x) + \frac{t}{(1+x)^2},$$

teda

$$|\varphi'_0(x)| = |f'_0(x)| + \frac{t}{(1+x)^2} < \mu + t.$$

Dokopy teda φ_0 má vlastnosť $(\varepsilon : \mu + t, M)$.

3.

$$\begin{aligned} & \sum_{k=1}^{\infty} \left\{ \psi_n \left(\frac{1}{k+x} \right) \frac{1}{(k+x)^2} \right\} \\ &= \sum_{k=1}^{\infty} \left\{ \frac{T}{1 + \frac{1}{k+x}} \frac{1}{(k+x)^2} \right\} - \sum_{k=1}^{\infty} \left\{ f_n \left(\frac{1}{k+x} \right) \frac{1}{(k+x)^2} \right\}. \end{aligned}$$

Opäť postupnosť f_0, f_1, \dots má vlastnosť (σ) a ak využijeme Lemu 2.13 pre $T/(1+x)$, dostávame

$$\sum_{k=1}^{\infty} \left\{ \psi_n \left(\frac{1}{k+x} \right) \frac{1}{(k+x)^2} \right\} = \frac{T}{1+x} - f_{n+1}(x) = \psi_{n+1}(x).$$

4. Ked'že $f_0(x) < T/(1+x)$, máme nerovnosť $\psi_0(x) > 0$ pre všetky $x \in [0,1]$. Ďalej ked'že $f_0(x)$ je kladná funkcia a x berieme z intervalu, platí

$$\psi_0(x) = \frac{T}{1+x} - f_0(x) < T.$$

Pre $\psi'_0(x)$ máme

$$|\psi'_0(x)| = \left| -\frac{T}{(1+x)^2} - f'_0(x) \right| < \frac{T}{(1+x)^2} + \mu < T + \mu,$$

teda ψ_0 má vlastnosť $(\varepsilon : \mu + T, T)$.

□

Lema 2.18. Nech f_0, f_1, \dots je postupnosť reálnych funkcií definovaných na $[0,1]$, $0 < t < T$ reálne čísla a nech platí

$$\frac{t}{1+x} < f_0(x) < \frac{T}{1+x}$$

pre všetky $x \in [0,1]$. Ak má postupnosť f_0, f_1, \dots vlastnosť (σ) a f_0 má vlastnosť $(\varepsilon : \mu, M)$, potom pre ľubovoľné $n \in \mathbb{N}$ a $x \in [0,1]$ platí

$$\frac{g_n}{1+x} < f_n(x) < \frac{G_n}{1+x},$$

kde

$$g_n = \max \left\{ t, t\delta + \frac{1}{2}S - \frac{\mu+t}{2^{n-1}} \right\},$$

$$G_n = \min \left\{ T, T\delta + \frac{1}{2}S + \frac{\mu+T}{2^{n-1}} \right\},$$

$$\delta = 1 - \ln 2/2 \text{ a}$$

$$S = \int_0^1 f_0(z) dz.$$

Pritom platí

$$G_n - g_n < (T-t)\delta + \frac{\mu+T}{2^{n-2}}.$$

Dôkaz. Označme $\varphi_n(x) = f_n(x) - t/(1+x)$ a $\psi_n(x) = T/(1+x) - f_n(x)$, pre $n = 0, 1, \dots$. Podľa Lemy 2.17 má postupnosť funkcií $\varphi_0, \varphi_1, \dots$ vlastnosť (σ) a φ_0 vlastnosť $(\varepsilon : \mu+t, M)$. Môžeme teda použiť Lemu 2.16, podľa ktorej potom

$$\begin{aligned} \varphi_n(x) &> -\frac{\mu+t}{2^n} + \frac{1}{2} \int_0^1 \varphi_0(z) dz = -\frac{\mu+t}{2^n} + \frac{1}{2} \int_0^1 f_0(z) dz - \frac{1}{2} \int_0^1 \frac{t}{1+x} dz \\ &= -\frac{\mu+t}{2^n} + \frac{1}{2}S - \frac{t}{2} [\ln(1+x)]_0^1 = -\frac{\mu+t}{2^n} + \frac{1}{2}S - \frac{t \ln 2}{2}, \end{aligned}$$

kde

$$S = \int_0^1 f_0(z) dz.$$

Pre f_n teda dostávame

$$\begin{aligned} f_n(x) &= \varphi_n + \frac{t}{1+x} > \frac{t}{1+x} - \frac{\mu+t}{2^n} + \frac{1}{2}S - \frac{t \ln 2}{2} \\ &= \frac{1}{1+x} \left(t - \frac{(\mu+t)(1+x)}{2^n} + \left(\frac{1}{2}S - \frac{t \ln 2}{2} \right) (1+x) \right). \end{aligned}$$

Ked'že x volíme z $[0,1]$ a z monotónnosti integrálu plynie, že $(S - t \ln 2)/2 > 0$, platí

$$\begin{aligned} f_n(x) &> \frac{1}{1+x} \left(t - \frac{(\mu+t)2}{2^n} + \frac{1}{2}S - \frac{t \ln 2}{2} \right) = \frac{1}{1+x} \left(t \left(1 - \frac{\ln 2}{2} \right) - \frac{\mu+t}{2^{n-1}} + \frac{1}{2}S \right) \\ &= \frac{t\delta + \frac{1}{2}S - \frac{\mu+t}{2^{n-1}}}{1+x}, \end{aligned}$$

kde $\delta = 1 - \ln 2/2$. Označme

$$g_n = \max \left\{ t, t\delta + \frac{1}{2}S - \frac{\mu + t}{2^{n-1}} \right\}$$

a dostávame

$$f_n(x) > \frac{g_n}{1+x}.$$

V prípade, že $g_n = t$ totiž nerovnosť plynie z Lemy 2.14. Druhú nerovnosť získame rovnakým postupom pre postupnosť ψ_0, ψ_1, \dots . Tá má podobne podľa Lemy 2.17 vlastnosť (σ) a ψ_0 má vlastnosť $(\varepsilon : \mu + T, T)$. Použijeme Lemu 2.16 a dostávame

$$\begin{aligned} \psi_n(x) &> -\frac{\mu + T}{2^n} + \frac{1}{2} \int_0^1 \psi_0(z) dz = -\frac{\mu + T}{2^n} - \frac{1}{2} \int_0^1 f_0(z) dz + \frac{T}{2} \int_0^1 \frac{dz}{1+z} \\ &= -\frac{\mu + T}{2^n} - \frac{1}{2}S + \frac{T \ln 2}{2}. \end{aligned}$$

Pre f_n teda dostávame

$$\begin{aligned} f_n(x) &= \frac{T}{1+x} - \psi_n(x) < \frac{T}{1+x} + \frac{\mu + T}{2^n} + \frac{1}{2}S - \frac{T \ln 2}{2} \\ &= \frac{1}{1+x} \left(T + \frac{(\mu + T)(1+x)}{2^n} + \left(\frac{1}{2}S - \frac{T \ln 2}{2} \right) (1+x) \right), \end{aligned}$$

kde opäť

$$S = \int_0^1 f_0(z) dz.$$

Ked'že $0 \leq x \leq 1$ a $(S - T \ln 2)/2 < 0$ kvôli monotónnosti integrálu, platí

$$\begin{aligned} f_n(x) &< \frac{1}{1+x} \left(T + \frac{(\mu + T)2}{2^n} + \frac{1}{2}S - \frac{T \ln 2}{2} \right) = \frac{1}{1+x} \left(T \left(1 - \frac{\ln 2}{2} \right) + \frac{1}{2}S + \frac{\mu + T}{2^{n-1}} \right) \\ &= \frac{T\delta + \frac{1}{2}S + \frac{\mu + T}{2^{n-1}}}{1+x}, \end{aligned}$$

kde $\delta = 1 - \ln 2/2$. Označme

$$G_n = \min \left\{ T, T\delta + \frac{1}{2}S + \frac{\mu + T}{2^{n-1}} \right\}$$

a dostávame druhú nerovnosť

$$f_n(x) < \frac{G_n}{1+x},$$

pretože v prípade, že $G_n = T$ nerovnosť opäť plynie z Lemy 2.14. Dostávame teda odhad

$$\frac{g_n}{1+x} < f_n(x) < \frac{G_n}{1+x},$$

pre všetky $n \geq 1$ a $x \in [0,1]$. Navyše ak vieme, že $t < T$, z voľby g_n a G_n plynie

$$\begin{aligned} G_n - g_n &\leq T\delta + \frac{1}{2}S + \frac{\mu+T}{2^{n-1}} - t\delta - \frac{1}{2}S + \frac{\mu+t}{2^{n-1}} = (T-t)\delta + \frac{\mu+T}{2^{n-1}} + \frac{\mu+t}{2^{n-1}} \\ &< (T-t)\delta + \frac{2(\mu+T)}{2^{n-1}} = (T-t)\delta + \frac{\mu+T}{2^{n-2}}. \end{aligned}$$

□

Veta 2.19 (Kuzminova veta). *Nech $f_0(x), f_1(x), f_2(x), \dots, f_n(x), \dots$ je postupnosť reálnych funkcií definovaných na intervale $[0,1]$, ktorá má vlastnosť (σ) . Ak f_0 má vlastnosť $(\varepsilon : \mu, M)$ pre nejaké $M, \mu \in \mathbb{R}$, potom pre n dostatočne veľké*

$$\left| f_n(x) - \frac{a}{1+x} \right| < Ae^{-\lambda\sqrt{n}},$$

kde

$$a = \frac{1}{\ln 2} \int_0^1 f_0(z) dz,$$

$$\lambda = -\ln \left(1 - \frac{\ln 2}{2} \right)$$

a A je kladná konštantá, ktorá závisí iba od M a μ .

Dôkaz. Ked'že f_0 má vlastnosť $(\varepsilon : \mu, M)$, je to nezáporná funkcia na uzavretom intervale $[0,1]$ a teda na tomto intervale nadobúda minimum, ktoré označíme m . Teda platí $m \leq f_0(x) < M$ pre všetky $x \in [0,1]$. Z toho plynie, že pre všetky $x \in [0,1]$ platí nerovnosť

$$\frac{g}{1+x} = \frac{m}{2(1+x)} < \frac{m}{1+x} \leq f_0(x) < \frac{2M}{1+x} = \frac{G}{1+x},$$

kde $g = m/2$ a $G = 2M$. Pre f_0 s takýmto odhadom a postupnosť f_0, f_1, \dots s vlastnosťou (σ) môžeme použiť Lemu 2.18. Pre každé $n \geq 1$ dostávame čísla $g_{1,n}, G_{1,n}$, pre ktoré platí

$$\frac{g_{1,n}}{1+x} < f_n(x) < \frac{G_{1,n}}{1+x},$$

pričom

$$G_{1,n} - g_{1,n} < (G-g)\delta + \frac{\mu+G}{2^{n-2}} = (G-g)\delta + \frac{\mu+2M}{2^{n-2}}.$$

Postupnosť f_n má podľa Lemy 2.12 vlastnosť $(\varepsilon : \frac{\mu}{2^{n-3}} + 4M, 2M)$, navyše ak volíme $n \geq n_0$ z Lemy 2.12, potom f_n má vlastnosť $(\varepsilon : 5M, 2M)$. Postupnosť f_n, f_{n+1}, \dots má navyše zjavne vlastnosť (σ) , teda opäť použijeme Lemu 2.18, tentoraz pre f_n a pre všetky $m > n \geq n_0$, dostávame

$$\frac{g_m}{1+x} < f_m(x) < \frac{G_m}{1+x},$$

kde

$$g_m = \max \left\{ g_{1,n}, g_{1,n}\delta + \frac{1}{2}S - \frac{5M + g_{1,n}}{2^{m-n-1}} \right\},$$

$$G_m = \min \left\{ G_{1,n}, G_{1,n}\delta + \frac{1}{2}S + \frac{5M + G_{1,n}}{2^{m-n-1}} \right\}$$

a

$$G_m - g_m < (G_{1,n} - g_{1,n})\delta + \frac{5M + G_{1,n}}{2^{m-n-2}} \leq (G_{1,n} - g_{1,n})\delta + \frac{7M}{2^{m-n-2}}.$$

Vol'me $m = 2n$, $n \geq n_0$ a pre takúto voľbu označme $g_m = g_{2,n}$ a $G_m = G_{2,n}$. Pre f_{2n} máme nerovnosti

$$\frac{g_{2,n}}{1+x} < f_{2n}(x) < \frac{G_{2,n}}{1+x},$$

$$G_{2,n} - g_{2,n} < (G_{1,n} - g_{1,n})\delta + \frac{7M}{2^{n-2}}.$$

Ked'že $2n > n$, podľa Lemy 2.12 má tátó funkcia vlastnosť ($\varepsilon : 5M, 2M$). Postupnosť f_{2n}, f_{2n+1}, \dots má vlastnosť (σ), teda opäť môžeme použiť Lemu 2.18. Špeciálne dostávame

$$\frac{g_{3,n}}{1+x} < f_{3n}(x) < \frac{G_{3,n}}{1+x},$$

kde

$$g_{3,n} = \max \left\{ g_{2,n}, g_{2,n}\delta + \frac{1}{2}S - \frac{5M + g_{2,n}}{2^{n-1}} \right\},$$

$$G_{3,n} = \min \left\{ G_{2,n}, G_{2,n}\delta + \frac{1}{2}S + \frac{5M + G_{2,n}}{2^{n-1}} \right\}.$$

Ak analogicky postupujeme d'alej, pre ľubovoľné $k \geq 2$ takto definujeme $g_{k,n}$ a $G_{k,n}$, pre ktoré platí

$$\frac{g_{k,n}}{1+x} < f_{kn}(x) < \frac{G_{k,n}}{1+x},$$

$$G_{k,n} - g_{k,n} < (G_{(k-1),n} - g_{(k-1),n})\delta + \frac{7M}{2^{n-2}}.$$

Pre $k = n$ teda dostávame

$$G_{n,n} - g_{n,n} < (G_{(n-1),n} - g_{(n-1),n})\delta + \frac{7M}{2^{n-2}}$$

$$< \left((G_{(n-2),n} - g_{(n-2),n})\delta + \frac{7M}{2^{n-2}} \right) \delta + \frac{7M}{2^{n-2}}$$

$$< (G_{(n-2),n} - g_{(n-2),n})\delta^2 + \frac{1}{2^{n-2}}(7M\delta + 7M)$$

$$< (G_{(n-3),n} - g_{(n-3),n})\delta^3 + \frac{1}{2^{n-2}}(7M\delta^2 + 7M\delta + 7M) < \dots$$

$$< (G_{1,n} - g_{1,n})\delta^{n-1} + \frac{1}{2^{n-2}}(7M\delta^{n-2} + 7M\delta^{n-3} + \dots + 7M\delta + 7M)$$

$$< (G - g)\delta^n + \frac{1}{2^{n-2}}((\mu + 2M)\delta^{n-1} + 7M\delta^{n-2} + \dots + 7M\delta + 7M).$$

Dosadíme $G = 2M$ a označme $D = \max\{\mu + 2M, 7M\}$. Dostávame

$$G_{n,n} - g_{n,n} < 2M\delta^n + \frac{D}{2^{n-2}}(\delta^{n-1} + \delta^{n-2} + \dots + \delta + 1) = 2M\delta^n + \frac{D\delta^n}{2^{n-2}} \sum_{i=1}^n \frac{1}{\delta^i}.$$

Upravme teraz sumu z tejto nerovnosti. Suma je zjavne rovná

$$\sum_{i=0}^n \left(\frac{1}{\delta}\right)^i - 1 = \frac{\frac{1}{\delta^{n+1}} - 1}{\frac{1}{\delta} - 1} - 1 = \frac{\frac{1 - \delta^{n+1}}{\delta^{n+1}}}{\frac{1 - \delta}{\delta}} - 1 = \frac{1 - \delta^{n+1}}{\delta^n(1 - \delta)} - 1 = \frac{1 - \delta^n}{\delta^n(1 - \delta)}.$$

Dosad'me $\delta = (2 - \ln 2)/2$.

$$\frac{1 - \frac{(2 - \ln 2)^n}{2^n}}{\frac{(2 - \ln 2)^n}{2^n} \frac{2 - 2 + \ln 2}{2}} = \frac{2}{\ln 2} \frac{2^n - (2 - \ln 2)^n}{(2 - \ln 2)^n} < \frac{2}{\ln 2} \frac{2^n}{(2 - \ln 2)^n} < \frac{2^{n+1}}{\ln 2},$$

ked'že $(2 - \ln 2) > 1$. Z pôvodnej nerovnosti teda dostávame

$$G_{n,n} - g_{n,n} < 2M\delta^n + \frac{D\delta^n}{2^{n-2}} \frac{2^{n+1}}{\ln 2} = 2M\delta^n + \frac{D\delta^n}{8\ln 2} = \delta^n \left(2M + \frac{D}{8\ln 2}\right).$$

Označme

$$K = \max \left\{ 2e, 2M + \frac{D}{8\ln 2} \right\}.$$

Potom

$$G_{n,n} - g_{n,n} < \delta^n K = e^{\ln K} e^{n \ln \delta} = Be^{-\lambda n},$$

kde B je kladná konšanta, ktorá závisí iba od μ a M , pretože D a K závisia iba od týchto parametrov a

$$\lambda = -\ln \delta = -\ln \left(1 - \frac{\ln 2}{2}\right).$$

Z tohto odhadu plynie, že existuje $b \in \mathbb{R}$ také, že

$$\lim_{n \rightarrow \infty} G_{n,n} = \lim_{n \rightarrow \infty} g_{n,n} = b.$$

Navyše z nerovnosti

$$\frac{g_{n,n}}{1+x} < f_{n^2}(x) < \frac{G_{n,n}}{1+x}$$

dostávame

$$\left| f_{n^2}(x) - \frac{b}{1+x} \right| < Be^{-\lambda n} \quad (2.6)$$

pre všetky x z $[0,1]$ a teda $f_{n^2}(x)$ konverguje rovnomerne k funkcií $b/(1+x)$ na $[0,1]$. Funkcia f_{n^2} je integrovateľná pre všetky n , teda podľa Vety 2.6 môžeme vymeniť limitu a integrál a dostávame

$$\lim_{n \rightarrow \infty} \int_0^1 f_{n^2}(x) dx = \int_0^1 \frac{b}{1+x} dx = b \ln 2.$$

Podľa Lemy 2.15 platí

$$\int_0^1 f_{n^2}(x)dx = \int_0^1 f_0(x)dx,$$

teda

$$b = a = \frac{1}{\ln 2} \int_0^1 f_0(x)dx.$$

Ak si zvolíme $N \in \mathbb{N}$, $N \geq n_0^2$, potom platí, že existuje $n \geq n_0$, pre ktoré $n^2 \leq N < (n+1)^2$. Z nerovnosti 2.6 plynie

$$\frac{a - 2Be^{-\lambda n}}{1+x} < f_{n^2}(x) < \frac{a + 2Be^{-\lambda n}}{1+x}$$

a z Lemy 2.14 potom

$$\frac{a - 2Be^{-\lambda n}}{1+x} < f_N(x) < \frac{a + 2Be^{-\lambda n}}{1+x},$$

teda

$$\left| f_n(x) - \frac{a}{1+x} \right| < 2Be^{-\lambda n} = 2Be^\lambda e^{-\lambda(n+1)} < Ae^{-\lambda\sqrt{N}},$$

kde $A = 2Be^\lambda$ je kladná reálna konšstanta závislá od M a μ . Táto nerovnosť platí pre N dostatočne veľké, teda ak zvolíme dostatočne veľké A , bude platiť pre ľubovoľné $N \geq 0$.

□

Teraz sa vrátimy k pôvodnej postupnosti funkcií m_0, m_1, \dots a dokážeme odhad, ktorý plynie z Kuzminovej vety.

Veta 2.20. *Pre postupnosť funkcií m_0, m_1, \dots , ktorá je definovaná vyššie, platí*

$$\left| m_n(x) - \frac{\ln(1+x)}{\ln 2} \right| < Ae^{-\lambda\sqrt{n}},$$

kde A je kladná konšstanta a

$$\lambda = -\ln \left(1 - \frac{\ln 2}{2} \right) \doteq 0,4255.$$

Dôkaz. Indukciou dokážeme, že funkcia $m_n(x)$ má deriváciu na intervale $[0,1]$ pre každé $n \in \mathbb{N}_0$.

Ked'že $\alpha_0(\alpha) = \alpha$, platí

$$m_0(x) = \mathfrak{M}\{\alpha \in (0,1) | \alpha < x\} = x$$

pre všetky $x \in [0,1]$. Vidíme teda, že funkcia $m_0(x)$ má deriváciu na $[0,1]$ a platí $m'_0(x) = 1$ na celom intervale $[0,1]$. Táto derivácia je spojitá a obmezdená. Podľa Lemy 2.2 platí

$$m_{n+1}(x) = \sum_{k=1}^{\infty} \left\{ m_n \left(\frac{1}{k} \right) - m_n \left(\frac{1}{k+x} \right) \right\}.$$

Prepodkladajme, že $m_n(x)$ má spojitú a obmedzenú deriváciu na intervale $[0,1]$, teda existuje $B \in \mathbb{R}$, pre ktoré $|m'_n(x)| < B$ pre všetky $x \in [0,1]$. Potom sčítance

$$m_n\left(\frac{1}{k}\right) - m_n\left(\frac{1}{k+x}\right)$$

majú deriváciu na $[0,1]$ a platí

$$-m'_n\left(\frac{1}{k+x}\right)\left(\frac{-1}{(k+x)^2}\right) = m'_n\left(\frac{1}{k+x}\right)\frac{1}{(k+x)^2} < B\frac{1}{k^2}.$$

Suma

$$\sum_{k=1}^{\infty} m'_n\left(\frac{1}{k+x}\right)\frac{1}{(k+x)^2}$$

teda rovnomerne konverguje podľa Vety 2.3, pretože $\sum_{k=1}^{\infty} 1/k^2$ konverguje. Podľa Vety 2.4 má potom m_{n+1} deriváciu. Táto je opäť spojité a obmedzená pomocou

$$B\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{B\pi^2}{6}.$$

Indukciou teda dostávame, že m_n má deriváciu pre každé $n = 0, 1, \dots$ a pre postupnosť m'_0, m'_1, \dots platí

$$m'_{n+1} = \sum_{k=1}^{\infty} \frac{1}{(k+x)^2} m'_n\left(\frac{1}{k+x}\right),$$

teda má vlastnosť (σ) . Navyše $m'_0(x) \equiv 1$, a teda má vlastnosť $(\varepsilon : 2,2)$. Pre túto postupnosť teda môžeme použiť Vetu 2.19 a dostávame

$$\left| m'_n(x) - \frac{1}{(1+x)\ln 2} \right| < Ae^{-\lambda\sqrt{n}}, \quad (2.7)$$

kde A je kladná reálna konšstanta nezávislá od n a

$$\lambda = -\ln\left(1 - \frac{\ln 2}{2}\right).$$

Platí, že $m_n(x) = \int_0^x m'_n(y)dy$ a

$$\int_0^x \frac{dy}{(1+y)\ln 2} = \frac{1}{\ln 2} [\ln(1+y)]_0^x = \frac{\ln(x+1)}{\ln 2}.$$

Podľa Vety 2.9 teda integráciou nerovnosti (2.7), ktorú sme dostali z Vety 2.19 dostávame

$$\left| \int_0^x m'_n(y)dy - \int_0^x \frac{dy}{(1+y)\ln 2} \right| \leq \int_0^x \left| m'_n(x) - \frac{1}{(1+x)\ln 2} \right| < \int_0^x Ae^{-\lambda\sqrt{n}} dy.$$

Dohromady

$$\left| m_n(x) - \frac{\ln(1+x)}{\ln 2} \right| < Ae^{-\lambda\sqrt{n}} \cdot x \leq Ae^{-\lambda\sqrt{n}},$$

čím sme dokázali nielen Gaussov výsledok, ale aj dobrý odhad rýchlosťi konvergencie. □

Veta 2.21. *Nech k je prirodzené číslo, potom*

$$\lim_{n \rightarrow \infty} \mathfrak{M}E\left(\frac{n}{k}\right) = \frac{1}{\ln 2} \ln \left(1 + \frac{1}{k(k+2)}\right).$$

Dôkaz. Môžeme si všimnúť, že $a_n(\alpha) = k$ práve vtedy, ak

$$\left\lfloor \frac{1}{\alpha_{n-1}(\alpha)} \right\rfloor = k,$$

čo je ekvivalentné s nerovnosťami

$$k \leq \frac{1}{\alpha_{n-1}(\alpha)} < k+1,$$

a

$$\frac{1}{k+1} < \alpha_{n-1}(\alpha) \leq \frac{1}{k}.$$

Z toho vyplýva, že platí

$$\mathfrak{M}E\left(\frac{n}{k}\right) = m_{n-1}\left(\frac{1}{k}\right) - m_{n-1}\left(\frac{1}{k+1}\right) = \int_{\frac{1}{k+1}}^{\frac{1}{k}} m'_{n-1}(x) dx.$$

Ak teda integrujeme nerovnosť (2.7) pre $n-1$, vďaka monotónnosti integrálu dostávame

$$\begin{aligned} & \left| m_{n-1}\left(\frac{1}{k}\right) - m_{n-1}\left(\frac{1}{k+1}\right) - \int_{\frac{1}{k+1}}^{\frac{1}{k}} \frac{dx}{(x+1)\ln 2} \right| = \left| E\left(\frac{n}{k}\right) - \left[\frac{\ln(1+x)}{\ln 2} \right]_{\frac{1}{k+1}}^{\frac{1}{k}} \right| \\ &= \left| E\left(\frac{n}{k}\right) - \frac{\ln(1+\frac{1}{k})}{\ln 2} + \frac{\ln(1+\frac{1}{k+1})}{\ln 2} \right| = \left| E\left(\frac{n}{k}\right) - \frac{\ln\left(\frac{k+1}{k+2}\right)}{\ln 2} \right| \\ &= \left| E\left(\frac{n}{k}\right) - \frac{\ln\left(1+\frac{1}{k(k+2)}\right)}{\ln 2} \right| < \int_{\frac{1}{k+1}}^{\frac{1}{k}} Ae^{-\lambda\sqrt{n-1}} dx = Ae^{-\lambda\sqrt{n-1}} \left(\frac{1}{k} - \frac{1}{k+1} \right) \\ &= Ae^{-\lambda\sqrt{n-1}} \frac{1}{k(k+1)}. \end{aligned}$$

Z toho dostávame limitu, ktorú sme chceli

$$\lim_{n \rightarrow \infty} \mathfrak{M}E\left(\frac{n}{k}\right) = \frac{1}{\ln 2} \ln \left(1 + \frac{1}{k(k+2)}\right).$$



Kapitola 3

Vlastnosti zovšeobecnených reťazových zlomkov

Nech postupnosť čiastočných čitateľov $\mathbf{b} = (b_1, b_2, \dots)$ je postupnosť nenulových reálnych čísel a α je reálne číslo. Potom zovšeobecnený reťazovový zlomok α s čiastočnými čitateľmi b_1, b_2, \dots vypočítame nasledovne: Definujeme $\alpha_0 = \alpha$.

- Začneme s $i = 0$.
- Priradíme $a_i = \lfloor \alpha_i \rfloor$.
- Ak $\alpha_i - \lfloor \alpha_i \rfloor = 0$, výpočet končí, inak priradíme

$$\alpha_{i+1} = \frac{b_{i+1}}{\alpha_i - \lfloor \alpha_i \rfloor}$$

a opakujeme posledné dva kroky pre $i + 1$.

Môžeme si všimnúť, že akonáhle by platilo $b_i = 0$ pre nejaké $i \in \mathbb{N}$, potom by platilo $\alpha_i = 0$, postup by sa zastavil a $a_i = 0$, teda zlomok by nemal zmysel. Preto predpoklad, že sú všetky členy postupnosti \mathbf{b} nenulové, bol odôvodnený.

Pozorovanie. Ak je výraz $\alpha_i - \lfloor \alpha_i \rfloor \neq 0$, potom je menší ako 1, teda platí

$$\frac{1}{\alpha_i - \lfloor \alpha_i \rfloor} > 1.$$

Z toho dostávame, že

$$a_{i+1} = \lfloor \alpha_{i+1} \rfloor = \left\lfloor \frac{b_{i+1}}{\alpha_i - \lfloor \alpha_i \rfloor} \right\rfloor \geq \lfloor b_{i+1} \rfloor,$$

čiže ak budú b_i veľké čísla, a_i budú tiež veľké.

Tvrdenie 3.1. *Ak sú všetky členy postupnosti \mathbf{b} z predošej poznámky racionalné, potom sa algoritmus sa zastaví po konečnom počte krokov práve vtedy, ak α je racionalne číslo. V takomto prípade je navyše hodnota takto vytvoreného zlomku*

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{\ddots + \cfrac{b_n}{a_n}}}$$

rovná α .

Dôkaz. Indukciou podľa k ukážeme, že

$$\alpha = a_0 + \frac{b_1}{a_1 + \frac{b_2}{\ddots + \frac{b_k}{a_k}}}$$

pre všetky k také, že α_k je definované. Pre $k = 1$ dostávame

$$a_0 + \frac{b_1}{\alpha_1} = a_0 + \frac{b_1}{\frac{b_1}{\alpha_0 - [\alpha_0]}} = a_0 + \alpha_0 - a_0 = \alpha.$$

V indukčnom kroku si stačí uvedomiť, že

$$\alpha_k = \frac{b_k}{\alpha_{k-1} - [\alpha_{k-1}]} = \frac{b_k}{\alpha_{k-1} - a_{k-1}}$$

a preto

$$a_{k-1} + \frac{b_k}{\alpha_k} = a_{k-1} + \alpha_{k-1} - a_{k-1} = \alpha_{k-1}.$$

Z toho dostávame, že

$$a_0 + \frac{b_1}{a_1 + \frac{b_2}{\ddots + \frac{b_{k-1}}{a_{k-1} + \frac{b_k}{\alpha_k}}}} = a_0 + \frac{b_1}{a_1 + \frac{b_2}{\ddots + \frac{b_{k-1}}{\alpha_{k-1}}}} = \alpha,$$

pričom posledná rovnosť platí z indukčného predpokladu.

Ked'že sa algoritmus zastavil a žiadne b_i nie je rovné 0, nutne platí $\alpha_n = [\alpha_n]$, teda $\alpha_n = a_n$ a

$$\alpha = a_0 + \frac{b_1}{a_1 + \frac{b_2}{\ddots + \frac{b_n}{a_n}}}.$$

Naopak predpokladajme, že α je racionálne číslo. Ulkážeme, že postup sa zastaví. Nech $\alpha_i = p/q$ je racionálne číslo, $p \in \mathbb{Z}$, $q \in \mathbb{N}$ nesúdeliteľné čísla. Potom

$$\alpha_{i+1} = \frac{b_{i+1}}{\alpha_i - [\alpha_i]}$$

je zjavne opäť racionálne číslo, pretože

$$\alpha_i - [\alpha_i] = \frac{p \bmod q}{q}.$$

Potom teda

$$\alpha_i = \frac{q \cdot b_i}{p \bmod q}.$$

Ked'že $(p \bmod q) < q$, menovateľ sa zmenšíl. Ked'že $\alpha_0 = \alpha$ je racionálne číslo, teda je rovné p_0/q_0 pre nejaké $p_0 \in \mathbb{Z}$, $q_0 \in \mathbb{N}$ nesúdeliteľné čísla a po každom kroku sa menovateľ zmenší, najneskôr po q_0 krokoch bude α_i celé číslo (menovateľ bude rovný 1) a algoritmus sa zastaví.



Definícia 3.1 (Konvergenty zovšeobecneného reťazového zlomku). *Podobne ako pre klasické reťazové zlomky, môžeme pre nekonečné zovšeobecnené reťazové zlomky definovať postupnosti $\mathbf{P} = P_0, P_1, \dots$ a $\mathbf{Q} = Q_0, Q_1, \dots$ ako $P_{-1} = 1, Q_{-1} = 0, P_0 = a_0, Q_0 = 1$ a d'alej rekurentnými vzťahmi*

$$P_n = a_n P_{n-1} + b_n P_{n-2} \text{ a } Q_n = a_n Q_{n-1} + b_n Q_{n-2}.$$

Číslo $x_n = P_n/Q_n$ nazveme n -tý kovergent. Hovoríme, že reťazový zlomok konverguje, ak konverguje jeho postupnosť konvergentov.

Poznámka. Pre konvergenty navyše platí, že

$$x_n = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{\ddots + \cfrac{b_n}{a_n}}}.$$

V prípade zovšeobecnených reťazových zlomkov nemusí každý zlomok konvergoval.

Definícia 3.2 (Nakoniec periodický zovšeobecnený zlomok). *Nekonečný zovšeobecnený zlomok s čiastočnými podielmi a_0, a_1, \dots a čiastočnými čitateľmi b_1, b_2, \dots nazveme nakoniec periodický, ak existujú čísla $n_0, k \in \mathbb{N}$, také, že $a_n = a_{n+k}$ a $b_{n+1} = b_{n+k+1}$ pre všetky $n \geq n_0$. Číslo k nazývame dĺžka periódy a n_0 dĺžka predperiódy.*

Tvrdenie 3.2. *Ak je postupnosť čiastočných čitateľov \mathbf{b} postupnosťou celých čísel a pri výpočte zovšeobecneného reťazového zlomku reálneho čísla α dostaneme nakoniec periodický zovšeobecnený reťazový zlomok, potom α je kvadratické iracionálne číslo.*

Dôkaz. Nech k je dĺžka periódy a n_0 dĺžka predperiódy. Ak si označíme

$$a_{n_0} + \cfrac{b_{n_0+1}}{a_{n_0+1} + \cfrac{b_{n_0+2}}{\ddots + \cfrac{b_{n_0+k-1}}{a_{n_0+k-1} + \cfrac{b_{n_0+k}}{a_{n_0} + \cfrac{b_{n_0+1}}{\ddots}}}} = \beta,$$

Potom platí

$$\beta = a_{n_0} + \cfrac{b_{n_0+1}}{a_{n_0+1} + \cfrac{b_{n_0+2}}{\ddots + \cfrac{b_{n_0+k-1}}{a_{n_0+k-1} + \cfrac{b_{n_0+k}}{\beta}}}},$$

čo vedie na kvadratickú rovnicu pre β s racionálnymi koeficientami. β je teda kvadratické iracionálne číslo (β nie je racionálne číslo, pretože by zlomok neboli

nekonečný). Pre pôvodné α platí

$$\alpha = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{\ddots + \cfrac{b_{n_0}}{\alpha_{n_0}}}},$$

pričom $\alpha_{n_0} = \beta$. α je teda zjavne tiež kvadratické iracionálne číslo.



Kapitola 4

Návrh prúdovej šifry

Kane [1] navrhol schému, ako vytvoriť prúdovú šifru pomocou reťazových zlomkov. Schéma predpokladá výmenu kľúčov štandardným spôsobom, ktorá predchádza vlastnej prúdovej šifre. V konkrétnom príklade použitia tejto schémy je použité RSA. Schéma je koncipovaná veľmi všeobecne a pracuje s celočíselnými funkciami g a h_z , ktoré nie sú nijak špecifikované, až na uvedený najjednoduchší príklad použitia schémy, v ktorom sa predpokladá, že $g = \ln$ a $h_z(t) = z$ pre všetky t a z .

Schéma predpokladá, že prebieha viacero kôl a pre každé je inak volený kľúč z_i a inicializačný parameter t_i .

Okrem funkcií g , h_{z_i} , kľúča z_i a parametra t_i sa v popise vyskytuje ešte číslo a , ktoré sa v príklade použitia schémy volí rovnaké ako verejný exponent e jednej z komunikujúcich strán z inštancie RSA použitej pri výmene kľúčov pred šifrovaním.

Šifra predpokladá, že sa pracuje so zovšeobecneným reťazovým zlomkom, ktorý sa počíta z vopred zadaných čiastočných čitateľov b_1, b_2, \dots . Podľa autora článku by sa mohli posieláť zašifrovane pred začiatkom komunikácie, ale nenašiel sa útok ani na verziu tejto schémy, pri ktorej by boli b_1, b_2, \dots verejne prístupné. Jedinou informáciou o ich volbe, ktorá sa dá v článku nájsť, je doporučenie autora, aby šlo o veľké iracionálne čísla, ktorých celá časť je väčšia ako $10^{5000} \doteq 2^{16610}$.

Nie je ani úplne zrejmé, koľko čiastočných menovateľov potrebujeme v jednom kole. Celkovo sa to dá z článku pochopiť troma spôsobmi. Prvá možnosť je, že sa v každom kole pri výpočte reťazového zlomku opakovane používa iba jeden čiastočný čitateľ. Táto predstava najlepšie odpovedá značeniu a algoritmu na konci článku. Druhý spôsob, ako sa dá text pochopiť je, že pri počítaní každého nasledujúceho čiastočného podielu a_j sa použije nasledujúci člen postupnosti b_1, \dots . V nasledujúcom kole sa použije postupnosť b_i znova. Tretia možnosť je, že výpočet bude prebiehať ako pri druhej možnosti, ale v ďalšom kole sa už znova nepoužijú tie isté čitatele. Táto možnosť mi však príde nepravdepodobná, pretože celková dĺžka postupnosti b_i ako binárneho reťazca by bola väčšia ako dĺžka reťazca vyprodukovaného algoritmom, ktorý sa použije na zašifrovanie správy. Posledné dve verzie lepšie odpovedajú úvahám o bezpečnosti tejto schémy.

Spôsob voľby čiastočných menovateľov teda ostáva aj po opakovacom a dôslednom čítaní článku nejasným. Na niektorých miestach sa hovorí, že sú volené náhodne, ale nie je úplne jasné, k čomu sa táto náhodnosť vzťahuje. Ak sú však hodnoty b_i určené, potom nasleduje výpočet zovšeobecneného reťazového zlomku

čísla $X_i = \sqrt[n]{g(h_{z_i}(t_i))}$. Z neho sa použijú čiastočné podiely $a_{\ell+1}, \dots, a_m$, kde ℓ a m sú vopred určené. Čísla $a_{\ell+1}, \dots, a_m$ sa následne zostavia za sebou ako binárne reťazce a výsledný reťazec je výsledkom práce i -teho kola.

Celá schéma podľa [1] teda vyzerá takto:

- V i -tom kroku:
 - Obe strany vypočítajú $X_i = \sqrt[n]{g(h_{z_i}(t_i))}$.
 - Obe strany vypočítajú zovšeobecnený reťazový zlomok iracionálneho čísla X_i .
 - Obe strany vyberú prvých m čiastočných podielov reťazového zlomku nasledujúcich po ℓ -tom.
 - Tieto čiastočné podiely sa zreťazia a prevedú do binárneho zápisu, ten bude časťou prúdu kľúča (keystream).
 - Ak je vyprodukovaný keystream kratší ako správa, ktorú treba zašifrovať, prechádzajú obe strany do kroku $i + 1$ a postup opakujú.
- Po získaní prúdu kľúča k dostatočnej dĺžky, Alice zašifruje správu p tak, že vypočíta $c = p \oplus k$. Šifrový text c potom pošle Bobovi.
- Bob dešifruje správu p ako $p = c \oplus k$.

Konkrétny príklad použitia tohto algoritmu uvedený v článku odpovedá tejto schéme, kde $X_i = \sqrt[e]{\ln(z_i)}$.

Čo sa týka hodnôt X_i , autor uvádza, že je potrebné sa vyhnúť racionálnym a kvadratickým iracionálnym číslam a to treba zohľadniť aj pri výbere funkcií g a h_{z_i} a voľbe parametrov t_i a a . Toto doporučenie je založené na výsledkoch z prvej a tretej kapitoly.

V príklade použitá voľba $X_i = \sqrt[e]{\ln(z_i)}$ dokonca vedie na čísla transcendentné, ako plynie z nasledujúcej vety.

Veta 4.1. *Ak je $n \geq 3$ prirodzené číslo a x je reálne algebraické číslo väčšie ako 1, potom*

$$\sqrt[n]{\ln x}$$

je transcendentné číslo.

Dôkaz. Veta je dôsledkom Dôsledku 3.16 z [7]

□

Nie je však zrejmé, či pri voľbe iracionálnych čiastočných čitateľov je vôbec voľbu X_i nutné obmedzovať. Aj to stojí za ďalšie podrobnejšie skúmanie, ktoré by presahovalo rozsah tejto práce.

Autor šifry odkazuje na výsledok o frekvencii jednotlivých čiastočných podielov v klasických reťazových zlomkoch, ktorý je uvedený a dokázaný v druhej kapitole. Navyše uvádza hypotézu, že pre zovšeobecnené reťazové zlomky bude rozdelenie frekvencií rovnomerné. Hypotéza nie je celkom presne formulovaná, píše sa v nej, že postupnosť b_1, b_2, \dots je tvorená náhodne volenými veľkými iracionálnymi číslami.

Táto hypotéza určite stojí za podrobnejšie skúmanie. Pochybnosti o jej platnosti viedli k záujmu o dôkaz popisu rozloženia frekvencií čiastočných podielov

v klasických iracionálnych zlomkoch a následne o Kuzminovu vetu 2.19. Overenie tejto hypotézy by mohlo nadväzovať na túto prácu, je totiž dosť možné, že sa pri tom opäť využije Kuzminova veta. Bohužiaľ nedostatok času a neprehľadná prezentácia dôkazu Kuzminovej vety zapríčinili, že táto úloha ostala za horizontom tejto práce. Presné znenie hypotézy z článku [1] preložené do slovenčiny vyzerá nasledovne.

Hypotéza 4.1. Ak je čiastočný čitateľ veľké iracionálne číslo zvolené náhodne a čiastočné podiely sú počítané z náhodne vybraného reálneho čísla x , ktoré nie je racionálne, ani kvadratické iracionálne číslo, potom:

1. Existuje veľký interval $[S,P]$, ktorý obsahuje väčšinu čiastočných podielov a nie je možné vyskúšať všetky čísla z tohto intervalu v polynomiálnom čase.
2. Pravdepodobnosť, že v polynomiálnom čase nastane kolízia v rozvoji zovšeobecneného reťazového zlomku je blízka nule, čo prispieva k dobrej distribúcii čiastočných podielov v intervale $[S,P]$.
3. Pravdepodobnosť, že sa prvok intervalu $[S,P]$ vyskytne ako čiastočný podiel, je pre všetky prvky intervalu $[S,P]$ takmer rovnaká (blíži sa k nule).

Záver

Cieľom tejto práce bolo na začiatku analyzovať prúdovú šifru predstavenú v článku [1]. Autor v článku formuluje Hypotézu 4.1 o rozdelení pravdepodobnosti, s ktorou sa jednotlivé čísla vyskytujú ako čiastočné podiely zovšeobecnených reťazových zlomkov, na ktorej stojí a padá bezpečnosť predstavenej šifry. Prirodzeným cieľom teda bolo pokúsiť sa zistiť niečo o platnosti tejto hypotézy. Poznatky z tejto oblasti však nie sú na takej úrovni, aby sa dala táto hypotéza potvrdiť alebo vyvrátiť. Predpokladám však, že akékoľvek poznatky, ktoré budú viest k overeniu alebo vyvráteniu hypotézy budú vychádzať s obdobných výsledkov pre klasické reťazové zlomky, ktoré už k dispozícii sú.

Ďalším predmetom môjho záujmu sa teda stalo tvrdenie o rozdelení pravdepodobnosti, s ktorou sa jednotlivé čísla vyskytujú ako čiastočné podiely klasických reťazových zlomkov, v literatúre tiež nazývané ako Gauss-Kuzminovo rozdelenie. Ako zdroj bol použitý klasický text o reťazových zlomkoch [2]. Nezdá sa, že by sa tento text dal nahradíť nejakým novším spracovaním. Existuje aj český preklad [8], ktorý je ale zjavne preložený z takmer totožnej verzie ako text použitý v tejto práci.

Tento text sa však ukázal byť dosť neprehľadný a na niektorých miestach, najmä v dôkaze Kuzminovej vety, dokonca nepresný. Konkrétnie napríklad narozdiel od Lemy 2.18, v originálnom teste boli čísla g_n a G_n definované priamo ako

$$g_n = t\delta + \frac{1}{2}S - \frac{\mu + t}{2^{n-1}},$$
$$G_n = T\delta + \frac{1}{2}S + \frac{\mu + T}{2^{n-1}},$$

pričom bola uvedená iba poznámka, že n sa volí dostatočne veľké, aby platila nerovnosť

$$G_n - g_n < (T - t)\delta + \frac{\mu + T}{2^{n-2}}.$$

To sa určite dá, ale neumožňuje to taký jednoduchý prechod ku g_{kn} a G_{kn} , pre $k = 2, 3, \dots$, aký je v originálnom teste uvedený. V každom prípade v dôkaze, ktorý bol prezentovaný v druhej kapitole, sú tieto nedostatky napravené. Okrem drobných nepresností je tiež prerobená celková štruktúra dôkazu pre lepšiu prehľadnosť.

Pôvodný cieľ sa teda bohužiaľ nepodarilo dosiahnuť - ostal do budúcnosti ako výzva. Prínos tejto práce vidím v spracovaní základných pojmov o reťazových zlomkoch a prepracovaní dôkazu Kuzminovej vety tak, aby bol prístupný dnešnému čitateľovi. Vďaka tomu by mohla byť táto bakalárská práca dobrým začiatkom pre štúdium obdoby Gauss-Kuzminovho rozdelenia pre zovšeobecnené ratzové zlomky, čo by viedlo k overeniu alebo vyvráteniu Hypotézy 4.1 uvedenej v článku [1].

Zoznam použitej literatúry

- [1] A. M. Kane. On the use of continued fractions for stream ciphers. 2013.
<http://eprint.iacr.org/2013/319.pdf>.
- [2] A.Y. Khinchin. *Continued fractions*. Courier Dover Publications, 1997.
- [3] Š. Holub. Text k prednáške Teorie čísel a RSA.
<http://www.karlin.mff.cuni.cz/~holub/soubory/Retez.pdf>.
- [4] D. Hensley. *Continued fractions*. World Scientific Publishing Co., 2006. ISBN 981-256-477-2.
- [5] W. Rudin. *Principles of mathematical analysis*. Third edition. McGraw-Hill, Inc., 1976. ISBN 0-07-054235-X.
- [6] Text na wikipédii o vetách o strednej hodnote.
http://en.wikipedia.org/wiki/Mean_value_theorem.
- [7] E.B. Burger and R. Tubbs. *Making transcendence transparent: An intuitive approach to classical number theory*. Springer-Verlag, 2004. ISBN 978-1-4419-1948-9.
- [8] A.J. Chinčin. *Řetězové zlomky*. Přírodovědecké vydavatelství, 1952. Preložil Karel Rychlík.