p-adski brojevi i p-adska interpolacija Riemannove zeta funkcije

Babok, Vanesa

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Vanesa Babok

P-ADSKI BROJEVI I P-ADSKA INTERPOLACIJA RIEMANNOVE ZETA FUNKCIJE

Diplomski rad

Voditelj rada:
prof.dr.sc. Marcela Hanzer

Zagreb, ožujak, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom ćemo se radu upoznati s p-adskim brojevima i postaviti temelje p-adske analize.

Racionalni su nam brojevi svima dobro poznati, no oni ipak imaju svojih nedostataka. Razlog tome je činjenica da skup svih racionalnih brojeva "sadrži rupe" (možemo naći niz racionalnih brojeva koji teži nekom broju koji nije racionalan). Jedan način rješavanja ovog problema je uobičajeno uvođenje iracionalnih brojeva čime dobivamo potpun sustav realnih brojeva. Međutim, postoji i drugi način - možemo uvesti p-adske brojeve što je prvi napravio njemački matematičar K. Hensel. Time dolazimo do mnoštva alternativnih brojevnih sustava od kojih se svaki zasniva na jednom fiksiranom prostom broju, pa tako imamo 2-adske brojeve, 3-adske brojeve i tako dalje.
p-adski su se brojevi s vremenom pokazali iznimno korisnima u brojnim poljima poput algebre, teorije brojeva, topologije, kriptografije, fizike...

p-adska je analiza široko područje koje obuhvaća mnogo više nego ovaj rad, no mi ćemo se većinom fokusirati na samo uvođenje (definiranje) p-adskih brojeva i na postavljanje temelja za p-adski analogon kompleksnih brojeva. Većina rada bazira se na osnovnoj literaturi **[Koblitz]**. U trećem poglavlju dotaknut ćemo se i kompleksne analize jer ćemo proučavati poznatu gama funkciju i način na koji je ona povezana s p-adskom analizom (tu ćemo pratiti **[Freitag-Busam]**).

U prvom se poglavlju upoznajemo s osnovnim konceptima poput norme, metrike i metričkih prostora, uvodimo novi (p-adski) koncept udaljenosti te dijelimo norme na arhimedske i ne-arhimedske. Zatim konstruiramo polje p-adskih brojeva i proučavamo njegovu aritmetiku. Također dokazujemo neke važne rezultate poput Henselove leme.

U drugom ćemo se poglavlju baviti Riemannovom zeta funkcijom i njenom p-adskom interpolacijom. U tu ćemo svrhu navesti (a onda i dokazati) formulu za $\zeta(2k)$. Nadalje, proučavat ćemo topologiju u $\mathbb{Q}_p$ i uvesti p-adske distribucije, mjere i integraciju. Koristeći

jednu interpretaciju vrijednosti $\zeta(2k)$ u obliku integrala i dobivene rezultate o p-adskim distribucijama, definirat ćemo i p-adske interpolacije Riemannove zeta funkcije.

Treće se poglavlje bavi proučavanjem gama funkcije i njenih osnovnih svojstava. Tom se prilikom prisjećamo nekih pojmova kompleksne analize poput analitičkih funkcija, singulariteta i reziduuma. Potom ćemo gama funkciju iskoristiti da pomoću nje dokažemo razvoj hiperbolnog sinusa u beskonačni produkt, što nam je bio važan tehnički korak u prethodnom dijelu rada.

Poglavlje 1

p-adski brojevi

Započet ćemo s uvođenjem osnovnih pojmova p-adske analize. Definirat ćemo p-adsku normu te p-adske brojeve i osnovne operacije nad njima. Također ćemo se osvrnuti na važnu Henselovu lemu.

1.1 Osnovni koncepti

Na početku moramo promotriti osnovne koncepte - definirat ćemo normu, metriku, metričke prostore, polja. Ti će nam pojmovi biti od velike važnosti jer ćemo uskoro uvesti novo poimanje udaljenosti.

Većina skupova koje ćemo promatrati bit će polja. **Polje** $\mathbb{F}$ definiramo kao skup zajedno s operacijama + i $\cdot$ definiranima na njemu i takvima da vrijede asocijativnost te komutativnost zbrajanja i množenja, distributivnost množenja prema zbrajanju, postojanje neutralnog elementa za zbrajanje, postojanje neutralnog elementa za množenje, postojanje inverznog elementa za zbrajanje, postojanje inverznog elementa za množenje za sve elemente različite od nule. Primjeri polja kojima ćemo se baviti su polje racionalnih brojeva $\mathbb{Q}$ i polje realnih brojeva $\mathbb{R}$.

Neka je X proizvoljan neprazan skup. **Metriku (udaljenost)** na njemu definiramo kao funkciju d koja svakom paru elemenata (x, y) iz X pridružuje neki nenegativni realni broj takvu da $(\forall x, y, z \in X)$ vrijede sljedeća svojstva:

(1) $d(x, y) = 0 \iff x = y$
(2) $d(x, y) = d(y, x)$
(3) $d(x, z) \leq d(x, y) + d(y, z)$

Skup X zajedno s metrikom d definiranom na njemu nazivamo **metrički prostor**. Na is-

tom skupu X može se definirati mnogo različitih metrika te tako dobivamo mnogo različitih metričkih prostora. Metrika kojom ćemo se mi baviti na polju $\mathbb{F}$ bit će inducirana **normom** na polju $\mathbb{F}$, to jest preslikavanjem $||\ ||$ koje svakom elementu polja $\mathbb{F}$ pridružuje neki nenegativni realni broj i koje je takvo da $(\forall x, y \in \mathbb{F})$ vrijede svojstva:

(1) $||x|| = 0 \iff x = 0$
(2) $||x \cdot y|| = ||x|| \cdot ||y||$
(3) $||x + y|| \leq ||x|| + ||y||$

Kažemo da je metrika d **inducirana** normom $||\ ||$ ako je d definirana s: $d(x, y) = ||x - y||$.

Tipičan primjer norme na polju racionalnih brojeva $\mathbb{Q}$ je apsolutna vrijednost koju označavamo s $|x|$ (a nekada i s $|x|_\infty$). Metrika inducirana njome $d(x, y) = |x - y|$ predstavlja uobičajen koncept udaljenosti na brojevnom pravcu.

Za normu $||\ ||$ kažemo da je to **trivijalna norma** ako vrijedi:

$$\begin{cases} ||x|| = 1 & , x \neq 0 \\ ||x|| = 0 & , x = 0 \end{cases}$$

1.2 Metrike na racionalnim brojevima

Sada kada smo uveli osnovne definicije, definirat ćemo novu vrstu udaljenosti koja će zadovoljavati svojstva (1)-(3) iz definicije metrike, ali će se znatno razlikovati od ustaljenih intuitivnih koncepata udaljenosti.

Definicija 1.2.1. *Neka je p proizvoljan prost broj.*
Za proizvoljan cijeli broj a različit od nule definiramo $\underline{ord_p(a)}$ kao najveću potenciju od p koja dijeli a.
Ako je $a = 0$, pišemo: $ord_p(0) = \infty$.

Primijetimo da ord_p ima svojstvo slično logaritmu: $ord_p(a_1 a_2) = ord_p(a_1) + ord_p(a_2)$.
Za proizvoljan racionalan broj $x = \frac{a}{b}$ definiramo $ord_p(x)$ na sljedeći način:
$ord_p(x) = ord_p(a/b) = ord_p(a) - ord_p(b)$. Uočimo da vrijedi: $ord_p(a/b) = ord_p(ac/bc)$.

Navodimo nekoliko primjera: $ord_2(96) = 5$, $ord_2(97) = 0$, $ord_5(35) = 1$.

Lema 1.2.2. *Za sve racionalne brojeve x i y vrijedi:* $ord_p(x+y) \geq min\{ord_p(x), ord_p(y)\}$.

Dokaz.
Neka vrijedi: $x = \frac{a}{b}$, $y = \frac{c}{d}$.
Možemo pisati:

$$x = p^{ord_p(x)} \cdot \frac{a'}{b'} \text{ i } y = p^{ord_p(y)} \cdot \frac{c'}{d'}, \text{ uz: } (p \nmid a'), \ (p \nmid b'), \ (p \nmid c'), \ (p \nmid d').$$

$$\Rightarrow \quad x+y = p^{ord_p(x)} \cdot \frac{a'}{b'} + p^{ord_p(y)} \cdot \frac{c'}{d'}$$

B.S.O.M.P. $ord_p(x) \leq ord_p(y)$.
$\Rightarrow$ $ord_p(y) = ord_p(x) + n$ za neki $(n \in \mathbb{N})$ i $ord_p(x)$=min$\{ord_p(x), ord_p(y)\}$

$$\Rightarrow \quad x + y = p^{ord_p(x)} \cdot \left(\frac{a'}{b'} + p^n \cdot \frac{c'}{d'} \right) = p^{ord_p(x)} \cdot \frac{a'd' + p^n \cdot b'c'}{b'd'}$$

$$\Rightarrow \quad ord_p(x+y) = ord_p \left(p^{ord_p(x)} \cdot \frac{a'd' + p^n \cdot b'c'}{b'd'} \right) \geq ord_p(x) = min\{ord_p(x), ord_p(y)\}$$

□

Naposlijetku dolazimo do već spomenutog novog koncepta udaljenosti.

Definicija 1.2.3. *Na skupu racionalnih brojeva* $\mathbb{Q}$ *definiramo* ***p-adsku normu*** *kao preslikavanje* $|\,|_p$ *definirano s:*

$$|x|_p = \begin{cases} \dfrac{1}{p^{ord_p(x)}}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

Teorem 1.2.4. *Upravo definirano preslikavanje* $|\,|_p$ *je norma na* $\mathbb{Q}$.

Dokaz.
Pokazat ćemo da dano preslikavanje zadovoljava svojstva (1)-(3) iz definicije norme.

Svojstvo (1): $|x|_p$=0 $\iff$ x=0.

Smjer $\Leftarrow$ očito slijedi iz definicije od $|\,|_p$, dok smjer $\Rightarrow$ vrijedi zato što je razlomak oblika $\frac{1}{\text{bilo što}}$ uvijek $\neq 0$.

Svojstvo (2): $|x \cdot y|_p$=$|x|_p \cdot |y|_p$.

Prvi slučaj: $x = 0$ i(li) $y = 0$. $\Rightarrow$ $x \cdot y = 0$ $\Rightarrow$[definicija od $|\ |_p$]$\Rightarrow$ $|x \cdot y|_p = 0$.
Također, budući da je barem jedan od njih jednak nuli, slijedi da je barem jedan od $|x|_p$ i $|y|_p$ jednak nuli. $\Rightarrow$ $|x|_p \cdot |y|_p = 0$ $\Rightarrow$ $|x \cdot y|_p = |x|_p \cdot |y|_p$
Drugi slučaj: $x, y \neq 0$.

$$\Rightarrow \quad |x \cdot y|_p = \frac{1}{p^{ord_p(x \cdot y)}} = \frac{1}{p^{ord_p(x)+ord_p(y)}} = \frac{1}{p^{ord_p(x)} \cdot p^{ord_p(y)}} = \frac{1}{p^{ord_p(x)}} \cdot \frac{1}{p^{ord_p(y)}} = |x|_p \cdot |y|_p$$

Svojstvo (3): $|x + y|_p \leq |x|_p + |y|_p$.
Prvi slučaj: $x = 0$ i(li) $y = 0$.
B.S.O.M.P. $y = 0$.
$\Rightarrow$ $|x + y|_p = |x + 0|_p = |x|_p \leq |x|_p + |y|_p$
Drugi slučaj: $(x, y \neq 0)$, $x + y = 0$.
$\Rightarrow$ $|x + y|_p = 0 \leq |x|_p + |y|_p$ jer je $(|x|_p, |y|_p \geq 0)$
Treći slučaj: inače
Neka vrijedi da su $x = \frac{a}{b}$ i $y = \frac{c}{d}$ maksimalno skraćeni razlomci.

$$\Rightarrow \quad |x + y|_p = \left|\frac{a}{b} + \frac{c}{d}\right|_p = \left|\frac{ad + bc}{bd}\right|_p = \frac{1}{p^{ord_p(\frac{ad+bc}{bd})}} \qquad (*)$$

$$\begin{aligned}
\Rightarrow \quad ord_p\left(\frac{ad + bc}{bd}\right) &= ord_p(ad + bc) - ord_p(bd) = \\
&= ord_p(ad + bc) - ord_p(b) - ord_p(d) = \\
&\geq min\Big\{ord_p(ad), ord_p(bc)\Big\} - ord_p(b) - ord_p(d) \qquad \text{(zbog leme 1.2.2)} \\
&= min\Big\{ord_p(a) + ord_p(d), ord_p(b) + ord_p(c)\Big\} - ord_p(b) - ord_p(d) = \\
&= min\Big\{ord_p(a) + ord_p(d) - ord_p(b) - ord_p(d), \\
&\qquad ord_p(b) + ord_p(c) - ord_p(b) - ord_p(d)\Big\} = \\
&= min\Big\{ord_p(a) - ord_p(b), ord_p(c) - ord_p(d)\Big\} = min\Big\{ord_p(x), ord_p(y)\Big\} \qquad (**)
\end{aligned}$$

$\Rightarrow$ $(*)$ i $(**)$ sada daju:

$$|x + y|_p \leq \frac{1}{p^{min\{ord_p(x),ord_p(y)\}}} = max\Big\{\frac{1}{p^{ord_p(x)}}, \frac{1}{p^{ord_p(y)}}\Big\} = max\Big\{|x|_p, |y|_p\Big\} \leq |x|_p + |y|_p$$

Time je dokaz gotov. □

Došli smo do osnovne definicije p-adske analize.

Definicija 1.2.5. *Za normu* $||\ ||$ *kažemo da je to* ***nearhimedska norma*** *ako uvijek vrijedi:* $||x+y|| \leq max\Big\{||x||, ||y||\Big\}$.
Nearhimedska metrika *je ona metrika* d *za koju vrijedi:* $d(x,z) \leq max\{d(x,y), d(y,z)\}$.
Norma (ili metrika) koja nije nearhimedska naziva se ***arhimedskom*** *normom (metrikom).*

Ako na vektorskom prostoru X imamo nearhimedsku normu d, onda ona inducira nearhimedsku metriku jer tada vrijedi:

$$d(x,z) = ||x-z|| = ||(x-y)+(y-z)|| \leq max\Big\{||x-y||, ||y-z||\Big\} = max\Big\{d(x,y), d(y,z)\Big\}.$$

Primjer arhimedske norme na $\mathbb{Q}$ je uobičajena apsolutna vrijednost.

Lema 1.2.6. *Norma* $|\ |_p$ *je nearhimedska na* $\mathbb{Q}$.

Dokaz.
Neka su $(x, y \in \mathbb{Q})$ proizvoljni. Vrijedi:

$$\begin{aligned} |x+y|_p &= \frac{1}{p^{ord_p(x+y)}} = \\ &\leq \frac{1}{p^{min\left\{ord_p(x), ord_p(y)\right\}}} \quad \text{(zbog leme 1.2.2)} \\ &\leq max\left\{\frac{1}{p^{ord_p(x)}}, \frac{1}{p^{ord_p(y)}}\right\} = max\Big\{|x|_p, |y|_p\Big\} \end{aligned}$$

□

Definicija 1.2.7. *Za proizvoljan niz* $(x_n)_n$ *u proizvoljnom metričkom prostoru* X *kažemo da je to* ***Cauchyjev niz*** *ako* $(\forall \epsilon > 0)\ (\exists N)$ *t.d.* $(\forall m, n > N)$ *vrijedi:* $d(x_m, x_n) < \epsilon$.

Definicija 1.2.8. *Za metrike* d_1 *i* d_2 *na istom skupu* X *kažemo da su to* ***ekvivalentne metrike*** *ako je svaki niz Cauchyjev s obzirom na metriku* $d_1 \iff$ *je on Cauchyjev s obzirom na metriku* d_2.
Kažemo da su ***dvije norme ekvivalentne*** *ako induciraju ekvivalentne metrike.*

Lema 1.2.9. *Za svaku normu* $||\ ||$ *na polju* $\mathbb{F}$ *vrijedi:* $||1|| = 1$.

Dokaz.
Vrijedi: $||-1|| = ||(-1)\cdot(1)|| = ||-1|| \cdot ||1||$.
$\Rightarrow$ $||-1|| = ||-1|| \cdot ||1||$
Znamo da je: $||x|| = 0 \iff x = 0$.
$\Rightarrow$ za $x = -1 \neq 0$ je: $||x|| = ||-1| \neq 0$, pa možemo s tim podijeliti čime dobivamo:
$1 = \frac{||-1||}{||-1||} = \frac{||-1||\cdot||1||}{||-1||} = ||1||$
$\Rightarrow$ $||1|| = 1$ □

Lema 1.2.10. *Za svaku normu* $||\ ||$ *na polju* $\mathbb{F}$ *vrijedi:* $||-1|| = 1$.

Dokaz.
$||1|| = ||(-1)\cdot(-1)|| = ||-1|| \cdot ||-1|| = ||-1||^2$
Prema prethodnoj lemi 1.2.9: $||1|| = 1$.
Zato: $||-1||^2 = ||1|| = 1$.
$\Rightarrow$ $||-1|| = 1$
Time je tvrdnja dokazana. □

Lema 1.2.11. *Za svaku nearhimedsku normu* $||\ ||$ *na polju* $\mathbb{Q}$ *i za svaki cijeli broj* n *vrijedi:* $||n|| \leq 1$.

Dokaz.
1. slučaj: $n = 0$ $\Rightarrow$ $||n|| = ||0|| = 0 \leq 1$

2. slučaj: $n \in \mathbb{N}$ Dokaz ide indukcijom:

BAZA: $n = 2$ $\Rightarrow$ $||2|| = ||1+1|| \leq max\{||1||, ||1||\}$ =[]lema 1.2.9]= $max\{1,1\} = 1$
Pretpostavimo da tvrdnja vrijedi za neki $(n \in \mathbb{N})$.
KORAK: $n+1$ $\Rightarrow$ $||n+1|| = ||1+n|| \leq max\{||1||, ||n||\}$
Ako je $max\{||1||, ||n||\} = ||1||$, onda: $||n+1|| \leq max\{||1||, ||n||\} = ||1|| =$ [*lema* 1.2.9] $= 1$.
Ako $max\{||1||, ||n||\} = ||n||$, onda: $||n+1|| \leq max\{||1||, ||n||\} = ||n|| \leq$ [pretp. induk.] ≤ 1.

3. slučaj: $n = -m$ za neki $(m \in \mathbb{N})$
$||n|| = ||-m|| = ||(-1)\cdot(m)|| = ||-1|| \cdot ||m||$, a to je ≤ 1 zbog prethodne leme 1.2.10 i činjenice da zbog 2. slučaja $(\forall m \in \mathbb{N})$ vrijedi: $||m|| \leq 1$ □

Lema 1.2.12. *Neka su* $\| \|_1$ *i* $\| \|_2$ *dvije norme na istom polju* $\mathbb{F}$. *Tada su one ekvivalentne* $\Leftrightarrow$ $(\exists \alpha \in \mathbb{R})$ $(\alpha > 0)$ *t.d.* $(\forall x \in \mathbb{F})$ *vrijedi:* $\|x\|_1 = \|x\|_2^\alpha$.

Dokaz.
Smjer $\Leftarrow$:
Pretpostavimo da $(\exists \alpha \in \mathbb{R})(\alpha > 0)$ t.d. $(\forall x \in \mathbb{F})$ vrijedi: $\|x\|_1 = \|x\|_2^\alpha$.
$\Rightarrow$ $(\forall x \in \mathbb{F})$ $\|x\|_2 = \|x\|_1^{1/\alpha}$ (1)
Neka je $(a_n)_n$ proizvoljan niz u $\mathbb{F}$ koji je Cauchyjev s obzirom na $\| \|_2$.
$\Rightarrow$ $(\forall \epsilon > 0)$ $(\exists N_2)$ t.d. $(\forall m, n > N_2)$ vrijedi: $\|a_m - a_n\|_2 < \epsilon$
$\Rightarrow$ $(\forall m, n > N_2)$ je $\|a_m - a_n\|_1 = \|a_m - a_n\|_2^\alpha < \epsilon^\alpha =: \delta$ (monotono jer je $\alpha > 0$)
$\Rightarrow$ $(\forall \delta > 0)$ $(\exists N_1(\delta) = N_2(\delta^{1/\alpha}))$ t.d. $(\forall m, n > N_1(\delta) = N_2(\delta^{1/\alpha}))$ vrijedi:
$\|a_m - a_n\|_1 = \|a_m - a_n\|_2^\alpha < (\delta^{1/\alpha})^\alpha = \delta$
$\Rightarrow$ niz $(a_n)_n$ je Cauchyjev s obzirom na $\| \|_1$
Posve analogno se pokaže (uz korištenje tvrdnje (1)) da je svaki niz koji je Cauchyjev s obzirom na $\| \|_1$ također Cauchyjev i s obzirom na $\| \|_2$.
$\Rightarrow$ $\| \|_1$ i $\| \|_2$ su ekvivalentne

Smjer $\Rightarrow$:
Pretpostavimo da su norme $\| \|_1$ i $\| \|_2$ ekvivalentne.

Prvi slučaj: obje norme su trivijalne.
x=0 $\Rightarrow$ $\|x\|_1 = 0 = \|x\|_2^\alpha$ $(\forall \alpha > 0)$
$x \neq 0$ $\Rightarrow$ $\|x\|_1 = 1 = \|x\|_2^\alpha$ $(\forall \alpha > 0)$
$\Rightarrow$ tvrdnja vrijedi

Drugi slučaj: barem jedna norma je netrivijalna; B.S.O.M.P. da je to $\| \|_1$.
Prvo ćemo dokazati pomoćnu tvrdnju koja kaže da $(\forall x \in \mathbb{F})$ $\|x\|_1 < 1 \iff \|x\|_2 < 1$.
Pretpostavimo prvo da je $\|x\|_1 < 1$.
$\Rightarrow$ $\|x\|_1^n \to 0$ kada $n \to \infty$
$\Rightarrow$ $\|x^n\|_1 \to 0$ kada $n \to \infty$
$\Rightarrow$ $(x^n)_n$ je konvergentan niz s obzirom na $\| \|_1$
Budući da je svaki konvergentan niz u metričkom prostoru Cauchyjev, slijedi da je $(x^n)_n$ Cauchyjev niz s obzirom na $\| \|_1$.
$\Rightarrow$ norme $\| \|_1$ i $\| \|_2$ su ekvivalentne, pa je $(x^n)_n$ Cauchyjev niz i s obzirom na $\| \|_2$
$\Rightarrow$ $(x^n)_n$ je ograničen (jer znamo da je svaki Cauchyjev niz ograničen), pa $(\exists M)$ t.d. $(\forall n \in \mathbb{N})$ vrijedi: $\|x^n\|_2 \leq M$, pa je i $\|x\|_2^n \leq M$
Ako je $x = 0$, onda je $\|x\|_2 = \|0\|_2 = 0 \leq 1$.
Ako je $x \neq 0$, onda je $\|x\|_2 > 0$ (zbog $\|x\| = 0 \iff x = 0$ i $\|x\| \geq 0$).

Ako je $(0 < \|x\|_2 < 1)$, onda je svakako $\|x\|_2 \leq 1$; a ako je $\|x\|_2 \geq 1$, onda je specijalno $\|x\|_2 \leq \|x\|_2^2 \leq \|x\|_2^3 \leq ...$, a znamo da je $\|x\|_2^k \leq M$ $(\forall k \in \mathbb{N})$, pa je onda $\|x\|_2 = 1$, što povlači da je (specijalno) $\|x\|_2 \leq 1$.
Dakle, dobili smo da je $\|x\|_2 \leq 1$, a želimo da je $\|x\|_2 < 1$.
Pretpostavimo suprotno, tj. da je $\|x\|_2 = 1$.
Budući da je niz $(x^n)_n$ Cauchyjev s obzirom na $\| \|_2$, vrijedi:

$$(\forall m \in \mathbb{N})\ (\exists N(m))\ \text{t.d.}\ \ (\forall k \in \mathbb{N})\ \text{vrijedi:}\ \ \left\|x^{N(m)+k} - x^{N(m)}\right\|_2 < \frac{1}{m}.$$

$$\Rightarrow\ \ \frac{1}{m} > \left\|x^{N(m)+k} - x^{N(m)}\right\|_2 = \left\|x^{N(m)} \cdot (x^k - 1)\right\|_2 = \left\|x^{N(m)}\right\|_2 \cdot \left\|x^k - 1\right\|_2$$

$$\Rightarrow\ \ \underbrace{\left\|x^{N(m)}\right\|_2}_{= 1^{N(m)} = 1} \cdot \left\|x^k - 1\right\|_2 < \frac{1}{m}$$

$$\Rightarrow\ \ \left\|x^k - 1\right\|_2 < \frac{1}{m},\ \ (\forall k \in \mathbb{N})(\forall m \in \mathbb{N})$$

$$\Rightarrow\ \ \text{specijalno za}\ \ (k = 1):\ \ \|x - 1\|_2 < \frac{1}{m}\ \ (\forall m \in \mathbb{N})$$

$$\Rightarrow\ \ \|x - 1\|_2 = 0\ \ \Rightarrow\ \ x - 1 = 0\ \ \Rightarrow\ \ x = 1$$

$$\Rightarrow\ \ \|x\|_1 = \|1\|_1 = [\text{lema } 1.2.9] = 1,\ \text{što je u kontradikciji s:}\ \ \|x\|_1 < 1$$

$$\Rightarrow\ \ \|x\|_2 < 1$$

Suprotni smjer $(\|x\|_2 < 1\ \ \Rightarrow\ \ \|x\|_1 < 1)$ se dokaže analogno.
Time je pomoćna tvrdnja (koju ćemo označiti kao tvrdnju (2)) dokazana.

Sada imamo:

$$\|x\|_1 > 1\ \Leftrightarrow\ \frac{1}{\| x \|_1} < 1\ \Leftrightarrow\ \left\|\frac{1}{x}\right\|_1 < 1\ \Leftrightarrow[\text{tvrdnja (2)}]\Leftrightarrow\ \left\|\frac{1}{x}\right\|_2 < 1\ \Leftrightarrow\ \|x\|_2 > 1$$

Dobili smo: $(\forall x \in \mathbb{F})$ vrijedi $\|x\|_1 > 1 \iff \|x\|_2 > 1.$ (3)

$\Rightarrow$ sada tvrdnje (2) i (3) daju: $(\forall x \in \mathbb{F})\ \|x\|_1 = 1 \iff \|x\|_2 = 1$ (4)

Neka je $(a \in \mathbb{F})$ t.d. $\|a\|_1 < 1$.
Sada zbog tvrdnje (2) imamo: $\|a\|_2 < 1$.
Označimo:

$$\alpha := \frac{ln(\|a\|_1)}{ln(\|a\|_2)}.$$

Vrijedi: $(\alpha > 0)$ zbog:

$\|a\|_i < 1 \Rightarrow ln(\|a\|_i) < 0 \Rightarrow$ i brojnik i nazivnik su < 0 pa je čitav razlomak > 0.

Neka je $b \in \mathbb{F}$ proizvoljan.
Ako je $\|b\|_1 = 1$, onda zbog tvrdnje (4) vrijedi: $\|b\|_2 = 1$ pa je: $\|b\|_1 = 1 = \|b\|_2^{\alpha}$.
Ako je $\|b\|_1 < 1$, onda zbog tvrdnje (2) vrijedi: $\|b\|_2 < 1$.
Označimo za $(i \in \{1, 2\})$:

$$\beta_i := \frac{ln(\|a\|_i)}{ln(\|b\|_i)}.$$

Znamo da su i brojnik i nazivnik tog razlomka < 0, pa je čitav razlomak > 0.
Dokazujemo da je $\beta_1 = \beta_2$.
Ako je $\beta_2 < \beta_1$, onda $\left(\exists\, \frac{m}{n} \in \mathbb{Q}\right)$ t.d. $\beta_2 < \frac{m}{n} < \beta_1$.

Označimo: $x := \frac{a^n}{b^m} \in \mathbb{F}$. Vrijedi:

$$ln(\|x\|_i) = ln\left(\left\|\frac{a^n}{b^m}\right\|_i\right) = ln\left(\frac{\|a^n\|_i}{\|b^m\|_i}\right) = n \cdot ln(\|a\|_i) - m \cdot ln(\|b\|_i) =$$
$$= n \cdot \frac{ln(\|a\|_i)}{ln(\|b\|_i)} \cdot ln(\|b\|_i) - m \cdot ln(\|b\|_i) = n \cdot \beta_i \cdot ln(\|b\|_i) - m \cdot ln(\|b\|_i) =$$
$$= \underbrace{n \cdot ln(\|b\|_i)}_{< 0 \text{ jer je } \|b\|_i < 1} \cdot \underbrace{\left(\beta_i - \frac{m}{n}\right)}_{> 0 \text{ za i=1 , } < 0 \text{ za i=2}}$$

$\Rightarrow$ za $i = 1$ je: $ln(\|x\|_1) < 0 \Rightarrow \|x\|_1 < 1$ (5)

$\Rightarrow$ za $i = 2$ je: $ln(\|x\|_2) > 0 \Rightarrow \|x\|_2 > 1$ (6)

$\Rightarrow$ (5) i (6) su zajedno u kontradikciji s tvrdnjom (2)

Ako je $\beta_1 < \beta_2$, analogno se dođe do kontradikcije.

$$\Rightarrow \beta_1 = \beta_2 \Rightarrow \frac{ln(\|a\|_1)}{ln(\|b\|_1)} = \frac{ln(\|a\|_2)}{ln(\|b\|_2)} \Rightarrow \frac{ln(\|b\|_1)}{ln(\|b\|_2)} = \frac{ln(\|a\|_1)}{ln(\|a\|_2)} = \alpha$$

$$\Rightarrow ln(\|b\|_1) = \alpha \cdot ln(\|b\|_2) \Rightarrow \|b\|_1 = exp\left\{\alpha \cdot ln(\|b\|_2)\right\} = exp\left\{ln(\|b\|_2^{\alpha})\right\} = \|b\|_2^{\alpha}$$

Ako je $\|b\|_1 > 1$, onda vrijedi: $\left\|\frac{1}{b}\right\|_1 < 1$, što je zbog tvrdnje (2) ekvivalentno s: $\left\|\frac{1}{b}\right\|_2 < 1$.

Uz oznaku: $B := \frac{1}{b}$ vrijedi: $\|B\|_i < 1$, pa je prema prethodnom razmatranju:

$$\|B\|_1 = \|B\|_2^{\alpha} \Rightarrow \frac{1}{\|b\|_1} = \frac{1}{\|b\|_2^{\alpha}} \Rightarrow \|b\|_1 = \|b\|_2^{\alpha}.$$

□

Lema 1.2.13. *Neka su* $(\rho \in \langle 0,1\rangle)$ *i prost broj p fiksirani, te* $(x \in \mathbb{Q})$ *proizvoljan. Definiramo:*

$$f(x) = \begin{cases} \rho^{ord_p(x)} & x \neq 0 \\ 0 & x = 0. \end{cases} \tag{1.1}$$

Tako definirano preslikavanje f *je nearhimedska norma.*

Dokaz.
Treba pokazati da je preslikavanje f norma (tj. da zadovoljava svojstva (1)-(3) iz definicije norme) i da za njega vrijedi: $(\forall x, y \in \mathbb{Q})\ \ f(x+y) \leq max\{f(x), f(y)\}$.

Da je f norma slijedi iz teorema 1.2.4 (dokaz za $\rho \in \langle 0,1\rangle$ umjesto $\frac{1}{p}$ je posve analogan).

Dokaz da za f vrijedi: $(\forall x, y \in \mathbb{Q})\ \ f(x+y) \leq max\{f(x), f(y)\}$:

Prvi slučaj: $(x, y \in \mathbb{Q} - \{0\})$.

$$\begin{aligned} \Rightarrow \quad f(x+y) &= \rho^{ord_p(x+y)} = \\ &\leq \rho^{min\{ord_p(x), ord_p(y)\}} = \\ &= \text{[lema 1.2.2]} = max\left\{\rho^{ord_p(x)}, \rho^{ord_p(y)}\right\} = max\left\{f(x), f(y)\right\} \ \Rightarrow \ \text{tvrdnja vrijedi} \end{aligned}$$

Drugi slučaj: $x = y = 0$.

$$\begin{aligned} &\Rightarrow \quad f(x) = f(y) = 0 \ \text{ i } \ x + y = 0 \ \Rightarrow \ \ f(x+y) = 0 \\ &\Rightarrow \quad f(x+y) \leq max\left\{f(x), f(y)\right\} \ \Rightarrow \ \text{tvrdnja vrijedi} \end{aligned}$$

Treći slučaj: točno jedan od x, y *je jednak nuli* .
B.S.O.M.P. da je $y = 0$.

$$\begin{aligned} &\Rightarrow \quad f(x+y) = f(x) = \rho^{ord_p(x)}, \ \ f(y) = 0 \\ &\Rightarrow \quad f(x+y) \leq max\left\{f(x), f(y)\right\} \ \Rightarrow \ \text{tvrdnja vrijedi} \end{aligned}$$

□

Napomena 1.2.14. *Ako je u prethodnoj lemi* $(\rho = 1)$, *onda je* f *trivijalna norma. Ako je, pak,* $(\rho > 1)$, *onda* f *nije norma. Naime, u tom slučaju možemo uzeti* N *t.d. vrijedi:* $(\rho^N > 2)$, $(x = 1)$, $(y = p^N - 1)$. *Onda imamo:*

$$\begin{aligned} f(x+y) = [x+y \neq 0] &= \rho^{ord_p(1+p^N-1)} = \rho^{ord_p(p^N)} = \rho^N = \\ &> 2 = 1+1 = \rho^{ord_p(1)} + \rho^{ord_p(p^N-1)} = \rho^{ord_p(x)} + \rho^{ord_p(y)} \\ \Rightarrow \quad & f(x+y) > f(x) + f(y) \\ \Rightarrow \quad & f \text{ nije norma jer nije zadovoljeno svojstvo (3) iz definicije norme} \end{aligned}$$

U definiciji p-adske norme mogli smo umjesto $\left(\frac{1}{p}\right)^{ord_p(x)}$ pisati $\rho^{ord_p(x)}$ za proizvoljan $(\rho \in \langle 0, 1\rangle)$. Onda iz prethodne dvije leme slijedi da se tako dobije nearhimedska norma ekvivalentna p-adskoj normi.

Propozicija 1.2.15. *Ako su* p_1 *i* p_2 *različiti prosti brojevi, onda norme* $|x|_{p_1}$ *i* $|x|_{p_2}$ *nisu ekvivalentne.*

Dokaz.
Započet ćemo dokazivanjem pomoćne tvrdnje koja kaže da, ako su norme $|x|_{p_1}$ i $|x|_{p_2}$ ekvivalentne, te ako je $(x_n)_n$ proizvoljni niz koji teži prema 0 u $\mathbb{Q}_{p_1}$, onda $(x_n)_n$ teži prema 0 i u $\mathbb{Q}_{p_2}$.
Neka su norme $|x|_{p_1}$ i $|x|_{p_2}$ ekvivalentne, te $(x_n)_n$ proizvoljni niz koji teži prema 0 u $\mathbb{Q}_{p_1}$.

$\Rightarrow \quad |x_n|_{p_1} \to 0$
$\Rightarrow \quad |x_n|_{p_2} = [\text{lema } 1.2.12] = |x_n|_{p_1}^{\alpha} \to 0$
$\Rightarrow \quad (x_n)_n \to 0$ i u $\mathbb{Q}_{p_2}$
Time je pomoćna tvrdnja dokazana.

$(p_1^n)_n \to 0$ u $\mathbb{Q}_{p_1}$ zbog: $\left|p_1^n\right|_{p_1} = \dfrac{1}{p_1^n} \to 0$, a u $\mathbb{Q}_{p_2}$ teži u $1 \neq 0$ jer $\left|p_1^n\right|_{p_2} = 1 \to 1$,
a to zbog pomoćne tvrdnje znači da norme $|x|_1$ i $|x|_2$ nisu ekvivalentne.

□

Teorem 1.2.16. *Za* $(x \in \mathbb{Q})$ *i* $(\alpha \geq 0)$ *definiramo:* $\|x\| = |x|^{\alpha}$.
Tada vrijedi da je preslikavanje $\| \|$ *norma* $\iff$ $(\alpha \leq 1)$, *te je u tom slučaju ta norma ekvivalentna uobičajenoj apsolutnoj vrijednosti.*

Dokaz.
Počinjemo s dokazivanjem prve tvrdnje:

Smjer $\Leftarrow$:
Pretpostavljamo da je $(\alpha \leq 1)$. Pokazat ćemo da su svojstva (1)-(3) iz definicije norme zadovoljena:

svojstvo (1): $\|x\| = 0 \iff x = 0$ očito vrijedi.

svojstvo (2): $\|x \cdot y\| = \|x\| \cdot \|y\|$
$\|x \cdot y\| = |x \cdot y|^\alpha$ =[apsolutna vrijednost je norma pa za nju to svojstvo vrijedi]= $(|x| \cdot |y|)^\alpha = |x|^\alpha \cdot |y|^\alpha = \|x\| \cdot \|y\|$

svojstvo (3): $\|x + y\| \leq \|x\| + \|y\|$
Apsolutna vrijednost je norma pa za nju to svojstvo vrijedi. $\Rightarrow$ $|x + y| \leq |x| + |y|$
$\Rightarrow$ $|x + y|^\alpha \leq (|x| + |y|)^\alpha$
Ako je $(\alpha = 0)$ ili $(\alpha = 1)$, onda tvrdnja iz svojstva (3) očito vrijedi.
Ako je $(\alpha \in \langle 0, 1\rangle)$, onda je α oblika $\frac{1}{a}$ za neki $(a > 1)$.
$\Rightarrow$ $x^\alpha = x^{\frac{1}{a}} = \sqrt[a]{x}$, a korijen je rastuća funkcija
$\Rightarrow$ $\sqrt[a]{|x + y|} = |x + y|^\alpha \leq (|x| + |y|)^\alpha = \sqrt[a]{|x| + |y|}$
Znamo: $\sqrt[a]{|x| + |y|} \leq \sqrt[a]{x} + \sqrt[a]{y} \iff |x| + |y| \leq (\sqrt[a]{x} + \sqrt[a]{y})^a$.
Također, vrijedi: $(\sqrt[a]{x} + \sqrt[a]{y})^a = (\sqrt[a]{x})^a + (\sqrt[a]{y})^a + (\text{nešto} \geq 0) = |x| + |y| + (\text{nešto} \geq 0)$.
Dakle, $(\sqrt[a]{x} + \sqrt[a]{y})^a \geq |x| + |y|$, pa vrijedi: $\sqrt[a]{|x| + |y|} \leq \sqrt[a]{x} + \sqrt[a]{y}$.
$\Rightarrow \|x + y\| = |x + y|^\alpha \leq \sqrt[a]{|x| + |y|} \leq \sqrt[a]{x} + \sqrt[a]{y} = \|x\| + \|y\|$ $\Rightarrow$ tvrdnja iz svojstva (3) vrijedi

$\Rightarrow$ dakle, $\| \ \|$ je norma

Smjer $\Rightarrow$:

Pretpostavljamo da je $\| \ \|$ norma. Želimo pokazati da je $(\alpha \leq 1)$.
Svojstva (1) i (2) iz definicije norme vrijede $(\forall \alpha > 0)$. Zato promatramo svojstvo (3) koje kaže: $|x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$. Želimo pokazati da svojstvo (3) povlači da je $(\alpha \leq 1)$, to jest da svojstvo (3) ne može vrijediti niti za jedan $(\alpha > 1)$.
Pretpostavimo suprotno, tj. da $(\exists \alpha > 1)$ t.d. $(\forall x, y \in \mathbb{Q})$ vrijedi: $|x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$.
Specijalno, za $(x = y = -1 \in \mathbb{Q})$ imamo: $|x + y|^\alpha = |-2|^\alpha = 2^\alpha$ i
$|x|^\alpha + |y|^\alpha = |-1|^\alpha + |-1|^\alpha = 1^\alpha + 1^\alpha = 1 + 1 = 2$.
$\Rightarrow$ tvrdnja da za te konkretne vrijednosti od x, y vrijedi: $|x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$ (tj. da vrijedi: $2^\alpha \leq 2$) nije istinita niti za jedan $(\alpha > 1)$.

Dakle, našli smo neke $(x, y \in \mathbb{Q})$ za koje naša pretpostavka ne vrijedi $\Rightarrow$ naša pretpostavka je bila pogrešna $\Rightarrow$ svojstvo (3) povlači da je $(\alpha \leq 1)$, a pretpostavili smo da je $\|\ \|$ norma pa za nju sigurno vrijedi svojstvo (3), što znači da je sigurno $(\alpha \leq 1)$.

Sada dokazujemo drugu tvrdnju koja kaže da, ako je $\|x\| = |x|^\alpha$ norma (tj. ako je $\alpha \leq 1$), onda je ta norma ekvivalentna uobičajenoj apsolutnoj vrijednosti.
Zapravo želimo pokazati da je niz Cauchyjev s obzirom na normu $|\ |$ ako i samo ako je Cauchyjev s obzirom na normu $|\ |^\alpha$.

Smjer $\Rightarrow$:
Neka je $(a_n)_n$ proizvoljan niz koji je Cauchyjev s obzirom na normu $|\ |$, tj. za kojeg vrijedi: $(\forall \epsilon > 0)$ $(\exists N_1(\epsilon^{\frac{1}{\alpha}}))$ t.d. $(\forall m, n > N_1(\epsilon^{\frac{1}{\alpha}}))$ vrijedi: $|a_m - a_n| < \epsilon^{\frac{1}{\alpha}}$.
Neka je $(\epsilon > 0)$ proizvoljan. Označimo: $N_2(\epsilon) = N_1(\epsilon^{\frac{1}{\alpha}})$.
$\Rightarrow (\forall m, n > N_2(\epsilon) = N_1(\epsilon^{\frac{1}{\alpha}}))$ vrijedi: $|a_m - a_n| < \epsilon^{\frac{1}{\alpha}}\ /^\alpha$
$\Rightarrow$ $(\forall m, n > N_2(\epsilon) = N_1(\epsilon^{\frac{1}{\alpha}}))$ vrijedi: $|a_m - a_n|^\alpha < \epsilon$
$\Rightarrow$ niz $(a_n)_n$ je Cauchyjev i s obzirom na normu $|\ |^\alpha$

Smjer $\Leftarrow$:
Neka je $(a_n)_n$ proizvoljan niz koji je Cauchyjev s obzirom na normu $|\ |^\alpha$, tj. za kojeg vrijedi: $(\forall \epsilon > 0)$ $(\exists N_2(\epsilon^\alpha))$ t.d. $(\forall m, n > N_2)$ vrijedi: $|a_m - a_n|^\alpha < \epsilon^\alpha$.
Za isti taj $(\epsilon > 0)$ definiramo: $N_1(\epsilon) = N_2(\epsilon^\alpha)$.
$\Rightarrow$ $(\forall m, n > N_1 = N_2)$ vrijedi: $|a_m - a_n|^\alpha < \epsilon^\alpha / ^{\frac{1}{\alpha}}$ što je monotona funkcija
$\Rightarrow$ $(\forall m, n > N_1 = N_2)$ vrijedi: $|a_m - a_n| < \epsilon$
$\Rightarrow$ niz $(a_n)_n$ je Cauchyjev i s obzirom na normu $|\ |$

Iz proizvoljnosti niza $(a_n)_n$ slijedi da su $\|\ \| = |\ |^\alpha$ i $|\ |$ uistinu ekvivalentne norme. □

Iz lema 1.2.12 i 1.2.13 te teorema 1.2.16 slijedi tvrdnja sljedećeg teorema (potpuni dokaz ovog rezultata može se naći na stranicama 3-5 iz literature **[Koblitz]**).

Teorem 1.2.17. ***(Ostrowski)***
Svaka netrivijalna norma $\|\ \|$ na $\mathbb{Q}$ je ekvivalentna normi $|\ |_p$ za neki prost broj p ili za $p = \infty$.

Propozicija 1.2.18. *Neka je x proizvoljan ne-nul racionalan broj. Označimo sa $\mathcal{P}$ skup svih prostih brojeva. Tada vrijedi :*

$$\prod_{p\in\mathcal{P}\cup\{\infty\}} |x|_p = 1. \tag{1.2}$$

Dokaz.
Primijetimo prvo da je za svaki ne-nul racionalan broj x ovaj produkt konačan. Naime, neka je rastav od $|x|$ na proste faktore zadan s: $|x| = p_1^{k_1} \cdot ... \cdot p_n^{k_n}$. Tada vrijedi: $|x|_q = \left| |x| \right|_q = 1 \quad (\forall q \notin \{p_1, ..., p_n\})$, pa je u našem promatranom beskonačnom produktu samo konačno mnogo faktora različito od 1.

Neka je x proizvoljan ne-nul racionalan broj.
To znači da je x razlomak oblika: $x = \frac{B}{N}$ (B.S.O.M.P. da je taj razlomak maksimalno skraćen) uz $x \neq 0$ (što povlači $B \neq 0$).
Sada vrijedi:

$$\begin{aligned}
\prod_{p\in\mathcal{P}\cup\{\infty\}} |x|_p &= \{x \neq 0\} = |x| \cdot \prod_{p\in\mathcal{P}} \frac{1}{p^{ord_p(x)}} = \\
&= \left\{\text{ako } p \nmid x \quad \Rightarrow \quad ord_p(x) = 0 \quad \Rightarrow \quad p^{ord_p(x)} = p^0 = 1\right\} = \\
&= |x| \cdot \prod_{\substack{p\in\mathcal{P}\\ p|x}} \frac{1}{p^{ord_p(x)}} = \\
&= \left\{|x| = p_1^{k_1} \cdot ... \cdot p_n^{k_n}\right\} = \\
&= |x| \cdot \prod_{i=1}^{n} \frac{1}{p_i^{ord_{p_i}(x)}} = \\
&= |x| \cdot \prod_{i=1}^{n} \frac{1}{p_i^{k_i}} = \\
&= |x| \cdot \frac{1}{p_1^{k_1}} \cdot ... \cdot \frac{1}{p_n^{k_n}} = \\
&= \frac{|x|}{p_1^{k_1} \cdot ... \cdot p_n^{k_n}} = \\
&= \frac{|x|}{|x|} = 1
\end{aligned}$$

□

Kod osnovnog svojstva nearhimedske metrike koje kaže da je $\|x \pm y\| \leq max\{\ \|x\|,\ \|y\|\ \}$ jednakost vrijedi ako je $\|x\| \neq \|y\|$.

Sada ćemo proučiti primjer u kojem se očituje jedno svojstvo p-adske norme koje je razlikuje od uobičajene apsolutne vrijednosti, a koje se na prvu može činiti pomalo neobičnim.

Primjer 1.2.19. ***(kod nearhimedske norme svaka točka svake kugle je središte)***
Neka je r pozitivan realan broj te $(a \in \mathbb{F})$. ***Otvorenu kuglu*** *sa središtem u točki a radijusa r definiramo kao:*

$$K(a,r) = \{(x \in \mathbb{F}) : \|x-a\| < r\},$$

a ***zatvorenu kuglu*** *sa središtem u točki a radijusa r kao:*

$$\overline{K}(a,r) = \{(x \in \mathbb{F}) : \|x-a\| \leq r\}.$$

Neka je $\|\ \|$ nearhimedska norma na $\mathbb{F}$ te $(b \in K(a,r))$ proizvoljan. Tada vrijedi:

$$\begin{aligned}(x \in K(a,r)) &\Rightarrow \|x-a\| < r \\ &\Rightarrow \|x-b\| = \|(x-a)+(a-b)\| \leq max\{\ \underbrace{\|x-a\|}_{\substack{<r \text{ jer je} \\ x \in K(a,r)}},\ \underbrace{\|a-b\|}_{\substack{<r \text{ jer je} \\ b \in K(a,r)}}\ \} < r \\ &\Rightarrow x \in K(b,r)\end{aligned}$$

Obratna implikacija se dokaže analogno.
$\Rightarrow$ *K(a,r)=K(b,r)*
$\Rightarrow$ *Svaka točka svake otvorene kugle je središte.*

Analogno se pokaže da ista tvrdnja vrijedi i za svaku zatvorenu kuglu.

$\Rightarrow$ *Kod nearhimedske norme svaka točka svake kugle je središte te kugle.*

1.3 Konstrukcija kompleksnih brojeva

Došli smo do novog (p-adskog) koncepta udaljenosti između dva racionalna broja - uz fiksiran prosti broj p, kažemo da su dva racionalna broja **blizu** ako je njihova razlika

djeljiva s velikom potencijom od p. Da bismo mogli raditi s tom "p-**adskom metrikom**", moramo proširiti polje racionalnih brojeva $\mathbb{Q}$ na način koji je analogan načinu na koji smo kod klasične arhimedske metrike konstruirali prvo realne brojeve $\mathbb{R}$ te potom kompleksne brojeve $\mathbb{C}$. Zato ćemo se prvo prisjetiti kako se to radi.

Počet ćemo sa skupom prirodnih brojeva $\mathbb{N}$. Svaki korak u konstruiranju polja $\mathbb{C}$ iz polja $\mathbb{N}$ zadovoljava jednu od dvije osnovne težnje:

(1) Rješavanje polinomnih jednadžbi.
(2) Pronalaženje limesa Cauchyjevih nizova, to jest "upotpunjenje" brojevnog sustava do onoga "bez rupa" (tako da svaki Cauchyjev niz ima limes u tom novom brojevnom sustavu).

Konstrukcija skupa $\mathbb{Z}$
Cijele brojeve uvodimo kao rješenja jednadžbi oblika: $a + x = b$ za neke $(a, b \in \mathbb{N})$.

Konstrukcija polja $\mathbb{Q}$
Racionalne brojeve uvodimo kao rješenja jednadžbi oblika: $a \cdot x = b$ za neke $(a, b \in \mathbb{Z})$.

Konstrukcija polja $\mathbb{R}$
Realne brojeve uvodimo na način da promatramo skup S svih Cauchyjevih nizova racionalnih brojeva.
Za dva Cauchyjeva niza racionalnih brojeva $(s_1 = \{a_j\}, s_2 = \{b_j\} \in S)$ kažemo da su **ekvivalentni** (pišemo: $s_1 \sim s_2$) ako $|a_j - b_j| \to 0$ kada $j \to \infty$.
Upravo definirana relacija $\sim$ je očito **relacija ekvivalencije**, tj. zadovoljava svojstva:
- **refleksivnost:** $(\forall s \in S)$ je $s \sim s$ (svaki element je u relaciji sa samim sobom)
- **tranzitivnost:** $(\forall s_1, s_2, s_3 \in S)$ vrijedi: $s_1 \sim s_2$ i $s_2 \sim s_3 \Rightarrow s_1 \sim s_3$
- **simetričnost:** $(\forall s_1, s_2 \in S)$ vrijedi: $s_1 \sim s_2 \Rightarrow s_2 \sim s_1$
Sada definiramo $\mathbb{R}$ kao skup **klasa ekvivalencije** Cauchyjevih nizova racionalnih brojeva.

Konstrukcija polja $\mathbb{C}$
U nekom trenutku, matematičari su poželjeti uvesti brojeve uz koje će moći riješiti jednadžbe oblika: $x^2 + 1 = 0$. Uvedena je **imaginarna jedinica** $i := \sqrt{-1}$ te su definirani kompleksni brojevi oblika $a + b \cdot i$ uz $(a, b \in \mathbb{R})$. Ispostavilo se da:

(1) Vrijedi **fundamentalni teorem algebre** koji kaže da sve polinomne jednadžbe stupnja barem 1 s koeficijentima u $\mathbb{C}$ imaju rješenja u $\mathbb{C}$ (tj. kažemo da je polje kompleksnih brojeva **algebarski zatvoreno**).

(2) Polje kompleksnih brojeva $\mathbb{C}$ je **potpuno** s obzirom na jedinstvenu normu: $|a + b \cdot i| = \sqrt{a^2 + b^2}$ koja proširuje normu $||$ na $\mathbb{R}$, tj. vrijedi da svaki Cauchyjev niz kompleksnih brojeva $(a_n + b_n \cdot i)_n$ konvergira prema nekom kompleksnom broju $a + b \cdot i$ (budući da su $(a_n)_n$ i $(b_n)_n$ Cauchyjevi nizovi u $\mathbb{R}$, možemo uzeti: $\lim_{n\to\infty} a_n = a$, te $\lim_{n\to\infty} b_n = b$).

$\Rightarrow$ $\mathbb{C}$ je algebarski zatvoreno polje koje je potpuno s obzirom na arhimedsku metriku.

Da bi se došlo do nearhimedskog analogona polja $\mathbb{C}$ koje se obično označava sa Ω (to jest do polja koje je algebarski zatvoreno i potpuno s obzirom na nearhimedsku metriku), prvo se mora doći do p-adskog proširenja polja $\mathbb{Q}$ koje označavamo sa $\mathbb{Q}_p$. Tada se formira beskonačan niz proširenja polja dodavanjem rješenja jednadžbi višeg stupnja (a ne samo kvadratnih jedndažbi). Tako se dođe do polja $\overline{\mathbb{Q}}_p$ koje je algebarski zatvoreno, ali nije potpuno, pa mu treba još "popuniti rupe" da bi se došlo do Ω-e.

1.4 p-adski brojevi

Od sada pa do kraja ovog poglavlja, uzimamo da nam je unaprijed fiksiran neki prost broj $p \neq \infty$.

Za dva niza racionalnih brojeva $\{a_n\}$ i $\{b_n\}$ koji su Cauchyjevi s obzirom na normu $|\,|_p$ kažemo da su to **ekvivalentni nizovi** ako $|a_n - b_n|_p \to 0$ kada $n \to \infty$. Za proizvoljan $(x \in \mathbb{Q})$, sa $\{x\}$ označavamo "konstantan" Cauchyjev niz (onaj kojemu je svaki član jednak x). Očito je $\{x\} \sim \{x'\} \iff x = x'$. Klasa ekvivalencije od $\{0\}$ se označava sa 0.
Sada definiramo **skup p-adskih brojeva** $\mathbb{Q}_p$ kao skup svih klasa ekvivalencije Cauchyjevih nizova racionalnih brojeva.

Ako je a klasa ekvivalencije čiji je reprezentant $\{a_n\}$, **p-adsku normu klase ekvivalencije** a definiramo na sljedeći način:

$$|a|_p = \lim_{n\to\infty} |a_n|_p.$$

Taj limes postoji zato što:
- ako je $a = 0$, onda je po definiciji: $\lim_{n\to\infty}|a_n|_p = 0$
- ako je $a \neq 0$, onda za neki ϵ i za svaki N $(\exists n_N > N)$ t.d. $\left|a_{n_N}\right|_p > \epsilon$
Ako odaberemo N koji je dovoljno velik da $(\forall n, m > N)$ vrijedi: $|a_n - a_m|_p < \epsilon$ (tu tvrdnju ćemo označiti sa (*), a ona vrijedi zato što je $(a_n)_n$ Cauchyjev niz uz normu $|\ |_p$), dobivamo da $(\forall n > N)$ vrijedi:

$$\begin{aligned}\left|a_n - a_{n_N}\right|_p &= \left|(a_n - a_m) + (a_m - a_{n_N})\right|_p \\ &\leq max\Big\{\underbrace{|a_n - a_m|_p}_{<\epsilon},\ \underbrace{\left|a_m - a_{n_N}\right|_p}_{\substack{<\epsilon \text{ zbog } (*) \text{ jer} \\ \text{su } (m, n_N > N)}}\Big\} \\ &< \epsilon\end{aligned}$$

$\Rightarrow$ $(\forall n > N)$ vrijedi: $\left|a_n - a_{n_N}\right|_p < \epsilon$
Znamo da vrijedi:

$$|a_n|_p = \left|(a_n - a_{n_N}) + (a_{n_N})\right|_p \leq max\Big\{\left|a_n - a_{n_N}\right|_p, \left|a_{n_N}\right|_p\Big\}.$$

A znamo i da je: $\left(\left|a_n - a_{n_N}\right|_p < \epsilon\right)$ i $\left(\left|a_{n_N}\right|_p > \epsilon\right)$, tj. te dvije vrijednosti se razlikuju $\left(\text{preciznije, } \left|a_{n_N}\right|_p > \left|a_n - a_{n_N}\right|_p\right)$. Pa iz toga i iz činjenice da kod svojstva nearhimedske metrike jednakost vrijedi akko su te dvije vrijednosti (one čiji maksimum gledamo) različite, zaključujemo da u našem slučaju kod svojstva nearhimedske metrike jednakost vrijedi.

$\Rightarrow$ $|a_n|_p = max\Big\{\left|a_n - a_{n_N}\right|_p, \left|a_{n_N}\right|_p\Big\} = \left|a_{n_N}\right|_p$

$\Rightarrow$ $(\forall n > N)$ vrijedi: $|a_n|_p = \left|a_{n_N}\right|_p = konst.$

Ta konstanta je tada $\lim_{n\to\infty}|a_n|_p$.

Za dvije dane klase ekvivalencije a i b Cauchyjevih nizova racionalnih brojeva možemo odabrati njihove proizvoljne reprezentante $\Big(\{a_n\} \in a\Big)$ i $\Big(\{b_n\} \in b\Big)$ pa definirati **produkt klasa ekvivalencije** $a \cdot b$ kao onu klasu ekvivalencije koja je reprezentirana Cauchyjevim nizom racionalnih brojeva $\{a_n b_n\}$.

Za dvije dane klase ekvivalencije a i b Cauchyjevih nizova racionalnih brojeva možemo odabrati njihove proizvoljne reprezentante $\left(\{a_n\} \in a\right)$ i $\left(\{b_n\} \in b\right)$ pa definirati **zbroj klasa ekvivalencije** $a + b$ kao onu klasu ekvivalencije koja je reprezentirana Cauchyjevim nizom racionalnih brojeva $\{a_n + b_n\}$.

Aditivni inverz klase ekvivalencije a Cauchyjevih nizova racionalnih brojeva reprezentirane s $\{a_n\}$ je ona klasa ekvivalencije b Cauchyjevih nizova racionalnih brojeva reprezentirana s $\{b_n\} = \{-a_n\}$ (to je Cauchyjev niz).

Kod **multiplikativnog inverza klase ekvivalencije** a Cauchyjevih nizova racionalnih brojeva moramo paziti da ne dobijemo nule kao elemente Cauchyjevog niza $\{a_n\}$ koji reprezntira tu klasu. Ali to nam zapravo neće predstavljati problem jer je svaki Cauchyjev niz ekvivalentan nekom koji ne sadrži nule kao elemente - ako je za neke indekse $(i \in \mathbb{N})$ $a_i = 0$, onda možemo umjesto $\{a_n\}$ promatrati primjerice niz $\{a'_n\}$ definiran s:

$$a'_n = \begin{cases} a_n & , a_n \neq 0 \\ p^n & , a_n = 0 \end{cases}$$

Sada multiplikativni inverz klase ekvivalencije a možemo definirati kao klasu ekvivalencije b Cauchyjevih nizova racionalnih brojeva reprezentiranu s: $\{b_n\} = \left\{\frac{1}{a'_n}\right\}$.

Propozicija 1.4.1. *Skup $\mathbb{Q}_p$ klasa ekvivalencije Cauchyjevih nizova racionalnih brojeva je polje uz zbrajanje, množenje, te aditivne i multiplikativne inverze definirane kao gore.*

Dokaz.
Neka su $(a, b, c \in \mathbb{Q}_p)$ proizvoljni.
$\Rightarrow$ a, b, c su klase ekvivalencije čije reprezentante možemo označiti s $\{a_n\}$, $\{b_n\}$, $\{c_n\}$
Postojanje aditivnog i multiplikativnog inverza smo pokazali već ranije.
Distributivnost: Znamo da je $a(b + c)$ klasa ekvivalencije reprezentirana nizom $\{a_n(b_n + c_n)\}$. Također, $\{a_n(b_n + c_n)\} = \{a_n b_n + a_n c_n\}$. Dakle, $ab + ac$ je također klasa ekvivalencije reprezentirana tim nizom. $\Rightarrow$ $a(b+c) = ab+ac$ $\Rightarrow$ distributivnost vrijedi

Asocijativnost zbrajanja: Znamo da je $a+(b+c)$ klasa ekvivalencije reprezentirana nizom $\{a_n+(b_n+c_n)\}$. Također, $\{a_n+(b_n+c_n)\} = \{a_n+b_n+c_n\} = \{(a_n+b_n)+c_n\}$. Dakle, $(a+b)+c$ je također klasa ekvivalencije reprezentirana tim nizom. $\Rightarrow$ $a + (b + c) = (a + b) + c$ $\Rightarrow$

asocijativnost zbrajanja vrijedi
Asocijativnost množenja se dokaže analogno.
Komutativnost zbrajanja: Znamo da je $a+b$ klasa ekvivalencije reprezentirana nizom $\{a_n+b_n\}$. Također, $\{a_n+b_n\}=\{b_n+a_n\}$. Dakle, $b+a$ je također klasa ekvivalencije reprezentirana tim nizom. $\Rightarrow$ $a+b=b+a$ $\Rightarrow$ komutativnost zbrajanja vrijedi
Komutativnost množenja se dokaže analogno.
Postojanje neutralnog elementa za zbrajanje: Znamo da je $a+0$ klasa ekvivalencije reprezentirana nizom $\{a_n+0\}$. Također, $\{a_n+0\}=\{a_n\}$. Dakle, a je također klasa ekvivalencije reprezentirana tim nizom. $\Rightarrow$ $0+a$ =(komutativnost)= $a+0=a$ $\Rightarrow$ 0=$\{0\}$ je neutralni element za zbrajanje
Postojanje neutralnog elementa za množenje: Znamo da je $a\cdot 1$ klasa ekvivalencije reprezentirana nizom $\{a_n\cdot 1\}$. Također, $\{a_n\cdot 1\}=\{a_n\}$. Dakle, a je također klasa ekvivalencije reprezentirana tim nizom. $\Rightarrow$ $1\cdot a$ =(komutativnost)= $a\cdot 1=a$ $\Rightarrow$ 1=$\{1\}$ je neutralni element za množenje za svaki ne-nul element $(a\in\mathbb{Q}_p)$ □

$\mathbb{Q}$ je podskup od $\mathbb{Q}_p$ sastavljen od klasa ekvivalencije u kojima možemo pronaći reprezentant koji se sastoji od konstantnog Cauchyjevog niza.

Propozicija 1.4.2. *Polje p-adskih brojeva $\mathbb{Q}_p$ je potpuno s obzirom na $|\ |_p$, tj. svaki Cauchyjev niz iz $\mathbb{Q}_p$ konvergira i limes mu je element skupa $\mathbb{Q}_p$.*

Dokaz.
Neka je $\{\overline{x}_k\}_k$ proizvoljan Cauchyjev niz iz $\mathbb{Q}_p$, to jest $\overline{x}_k$-ovi su klase ekvivalencije. Njihove pripadajuće reprezentante možemo označiti s $\{a_{k,n}\}_n$, a za njih znamo da su to Cauchyjevi nizovi racionalnih brojeva, pa vrijedi:

$$(\forall\epsilon>0)\ (\exists M=M(\epsilon)\in\mathbb{N})\ \text{t.d.}\ \ (\forall n',n''\geq M)\ \left|a_{k,n'}-a_{k,n''}\right|_p<\epsilon.$$

$$\Rightarrow\ \text{specijalno, za}\ \ \epsilon=\frac{1}{p^n}\quad (\exists M=M(\epsilon)\in\mathbb{N})\ \text{t.d.}\ \ (\forall n',n''\geq M)\ \left|a_{k,n'}-a_{k,n''}\right|_p<\frac{1}{p^n}$$

Sada možemo uzeti: $x_{k,1}:=a_{k,M}$
$x_{k,2}:=a_{k,M+1}$
$\vdots$

$$\Rightarrow\ (\forall i,j\in\mathbb{N})\ \text{vrijedi:}\ \ \left|x_{k,i}-x_{k,j}\right|_p<\frac{1}{p^n}\tag{1.3}$$

Tvrdimo da je dijagonalni niz $\{x_{n,n}\}_n$ Cauchyjev niz racionalnih brojeva (dakle, $\in\mathbb{Q}_p$), i da je on limes niza $\{\overline{x}_k\}_k$.

$\{x_{n,n}\}_n$ je Cauchyjev niz racionalnih brojeva :

Neka je $(\epsilon' > 0)$ proizvoljan.

Znamo: $\{\overline{x}_k\}_k$ je Cauchyjev niz u $\mathbb{Q}_p$.

$\Rightarrow$ $(\forall \epsilon > 0)$ $(\exists N = N(\epsilon) \in \mathbb{N})$ t.d. $(\forall k, n \geq N)$ $\lim\limits_{i\to\infty} \left|x_{k,i} - x_{n,i}\right|_p = |\overline{x}_k - \overline{x}_n|_p < \epsilon$

Pri tome smo odabrali N t.d. vrijedi: $2 \cdot \dfrac{1}{p^N} + \epsilon < \epsilon'$ (to će nam trebati kasnije). (1.4)

Dakle, za $(k, n, m \geq N)$ vrijedi:

$$\left|x_{k,k} - x_{n,n}\right|_p \leq \underbrace{\left|x_{k,k} - x_{k,m}\right|_p}_{\substack{<1/p^n \text{ zbog } 1.3 \\ \leq 1/p^N}} + \underbrace{\left|x_{k,m} - x_{n,m}\right|_p}_{\text{kad } \overset{<\epsilon}{m\to\infty}} + \underbrace{\left|x_{n,m} - x_{n,n}\right|_p}_{\substack{<1/p^n \text{ zbog } 1.3 \\ \leq 1/p^N}} =$$

$$\leq 2 \cdot \frac{1}{p^N} + \epsilon < \epsilon' \qquad \text{zbog (1.4)} \tag{1.5}$$

$\Rightarrow$ za dani $(\epsilon' > 0)$ smo našli $(N \in \mathbb{N})$ (i to baš onaj N od ranije) t.d. $(\forall k, n \geq N)$ $\left|x_{k,k} - x_{n,n}\right|_p < \epsilon'$

$\Rightarrow$ $\{x_{n,n}\}_n$ je uistinu Cauchyjev niz racionalnih brojeva

$\overline{x} := \{x_{n,n}\}_n$ je limes niza $\{\overline{x}_k\}_k$:

Iz prethodnog dijela znamo da za proizvoljni $(\epsilon > 0)$ postoji neki $(N = N(\epsilon) \in \mathbb{N})$ t.d. vrijedi:

$$(\forall k, n \geq N) \quad \lim_{i\to\infty} \left|x_{k,i} - x_{n,i}\right|_p = |\overline{x}_k - \overline{x}_n|_p < \epsilon.$$

Sada za $(k \geq N)$ imamo:

$$|\overline{x}_k - \overline{x}|_p = \lim_{n\to\infty} \left|x_{k,n} - x_{n,n}\right|_p =$$

$$< sup_{n\geq N} \left|x_{k,n} - x_{n,n}\right|_p =$$

$$\leq \underbrace{sup_{n\geq N} \left|x_{k,n} - x_{k,k}\right|_p}_{<1/p^N} + \underbrace{sup_{n\geq N} \left|x_{k,k} - x_{n,n}\right|_p}_{\leq 2\cdot 1/p^N + \epsilon} < 3 \cdot \frac{1}{p^N} + \epsilon$$

$\Rightarrow$ ovo se može proizvoljno smanjiti povećavanjem N-a $\Rightarrow$ teži u nulu

$\Rightarrow$ $|\overline{x}_k - \overline{x}|_p \xrightarrow{k\to\infty} 0$

$\Rightarrow$ $\overline{x}_k \xrightarrow{k\to\infty} \overline{x}$

□

Lema 1.4.3. *Ako je x proizvoljan racionalan broj za kojeg vrijedi da je $|x|_p \leq 1$, onda $(\forall k)$ postoji cijeli broj α t.d. $|\alpha - x|_p \leq p^{-k}$. Cijeli broj α se može odabrati iz skupa $\{0, 1, 2, 3, ..., p^k - 1\}$.*

Dokaz.
Neka je $x = \frac{a}{b}$ proizvoljan. B.S.O.M.P. da je taj razlomak maksimalno skraćen.
Znamo da vrijedi:

$$|x|_p = \frac{1}{p^{ord_p(x)}} \leq 1.$$

$\Rightarrow \quad p^{ord_p(x)} \geq 1$

$\Rightarrow \quad ord_p(a) - ord_p(b) \geq 0$

$\Rightarrow \quad ord_p(b) \leq ord_p(a)$

Budući da je razlomak $\frac{a}{b}$ maksimalno skraćen, vrijedi da ili p dijeli samo a, ili p dijeli samo b, ili p ne dijeli ni a ni b.

1. slučaj: p dijeli samo a $\Rightarrow$ p ne dijeli b

2. slučaj: p dijeli samo b $\Rightarrow$ $1 \leq ord_p(b) \leq ord_p(a) = 0$ $\Rightarrow$ $1 \leq 0$, što je kontradikcija $\Rightarrow$ p ne dijeli b

3. slučaj: p ne dijeli ni a ni b $\Rightarrow$ specijalno, p ne dijeli b

Dakle, u svakom slučaju dobivamo da p ne dijeli b.
$\Rightarrow$ b i p^k su relativno prosti pa postoje cijeli brojevi n i m takvi da: $n \cdot (p^k) + m \cdot (b) = 1$.
Neka je $\alpha = am$.
Ideja je da se mb p-adski malo razlikuje od 1 (tj. za p-adski malu veličinu), pa je m dobra aproksimacija za $\frac{1}{b}$, pa je am dobra aproksimacija za $x = \frac{a}{b}$. Preciznije, vrijedi:

$$\begin{aligned} |\alpha - x|_p &= \left| am - \frac{a}{b} \right|_p = \\ &= \left| \frac{am}{b} \cdot b - \frac{a}{b} \right|_p = \\ &= \left| \frac{a}{b} \cdot (mb - 1) \right|_p = \\ &= \left| \frac{a}{b} \right|_p \cdot |mb - 1|_p = \end{aligned}$$

$$\leq |mb-1|_p \qquad \text{(jer je } |x|_p = \left|\tfrac{a}{b}\right|_p \leq 1\text{)}$$
$$= \left|n \cdot p^k\right|_p \qquad \text{(jer je } mb + np^k = 1\text{)}$$
$$= |n|_p \cdot \left|p^k\right|_p = |n|_p \cdot \frac{1}{p^k} =$$
$$\leq \frac{1}{p^k} \qquad \text{(jer je } |n|_p \leq 1 \text{ prema lemi 1.2.11)}$$

Naposlijetku, ako dodamo umnožak od p^k cijelom broju α, dobit ćemo cijeli broj između 0 i p^k za kojeg vrijedi: $|\alpha - x|_p \leq p^{-k}$. Time je lema dokazana. □

Teorem 1.4.4. *Svaka klasa ekvivalencije* $(a \in \mathbb{Q}_p)$ *za koju vrijedi* $|a|_p \leq 1$ *ima točno jedan reprezentativni Cauchyjev niz prirodnih brojeva* $\{a_i\}$ *za kojeg vrijedi:*
(1) $0 \leq a_i < p^i$ *za* $(i = 1, 2, 3, ...)$
(2) $a_i \equiv a_{i+1}\ (mod\ p^i)$ *za* $(i = 1, 2, 3, ...)$.

Dokaz.
Jedinstvenost:
Ako je $\{a_i'\}$ neki drugi niz koji zadovoljava (1) i (2), i ako se oni razlikuju recimo za neki indeks i_0 (tj. vrijedi: $a_{i_0} \neq a_{i_0}'$), onda zbog činjenice da su a_{i_0} i a_{i_0}' između 0 i p^{i_0} vrijedi:

$$a_{i_0} - a_{i_0}' < p^{i_0}$$
$$\Rightarrow \quad p^{i_0} \nmid (a_{i_0} - a_{i_0}'), \text{ to jest: } a_{i_0} \not\equiv a_{i_0}' (\text{mod } p^{i_0}).$$

$\Rightarrow$ $(\forall i \geq i_0)$ vrijedi: $a_i \equiv a_{i_0} \not\equiv a_{i_0}' \equiv a_i' (\text{mod } p^{i_0})$, to jest: $a_i \not\equiv a_i' \ (\text{mod } p^{i_0})$
$\Rightarrow$ $p^{i_0} \nmid (a_i - a_i')$
$\Rightarrow$ $ord_p(a_i - a_i') < i_0$
$\Rightarrow$ $p^{ord_p(a_i - a_i')} < p^{i_0}$

$$\Rightarrow \quad \left|a_i - a_i'\right|_p = \frac{1}{p^{ord_p(a_i - a_i')}} > \frac{1}{p^{i_0}}$$

$\Rightarrow$ $(\forall i \geq i_0)$ vrijedi: $\left|a_i - a_i'\right|_p > \frac{1}{p^{i_0}}$
$\Rightarrow$ $\{a_i\} \nsim \{a_i'\}$
$\Rightarrow$ $\{a_i\}$ i $\{a_i'\}$ nisu ekvivalentni nizovi pa ne mogu biti reprezentanti iste klase ekvivalencije
$\Rightarrow$ došli smo do kontradikcije $\Rightarrow$ imamo jedinstvenost

Egzistencija:

Pretpostavimo da je Cauchyjev niz $\{b_i\}$ proizvoljan reprezentant klase ekvivalencije a. Želimo naći njemu ekvivalentan niz $\{a_i\}$ koji zadovoljava (1) i (2).

Budući da je niz $\{b_i\}$ Cauchyjev, znamo da $(\forall j = 1, 2, 3, ...)$ $(\exists N(j) \in \mathbb{N})$ t.d. $(\forall i, i' \geq N(j))$ vrijedi: $|b_i - b_{i'}|_p \leq p^{-j}$. (Možemo uzeti da je niz $N(j)$ strogo rastući, recimo: $N(j) \geq j$.)

Uočimo da $(\forall i, i' \geq N(1))$ vrijedi:

$$\begin{aligned} |b_i|_p &= |b_{i'} + b_i - b_{i'}|_p = \\ &\leq max\{\, |b_{i'}|_p, |b_i - b_{i'}|_p \,\} = \\ &\leq max\left\{ |b_{i'}|_p, \frac{1}{p} \right\} \end{aligned}$$

Znamo: $|a|_p = \lim_{i' \to \infty}(|b_{i'}|_p)$. $\Rightarrow$ $|b_{i'}|_p \to |a|_p \leq 1$ kada $i' \to \infty$

Također, $\frac{1}{p} \leq 1$.

$\Rightarrow$ $(\forall i \geq N(1))$ vrijedi: $|b_i|_p \leq 1$

Sada uz pomoć leme 1.4.3 možemo naći niz cijelih brojeva a_j za koje vrijedi: $0 \leq a_j < p^j$ (tj. za njih vrijedi tvrdnja (1)) i $\left|a_j - b_{N(j)}\right|_p \leq \frac{1}{p^j}$.

Tvrdimo da je $\{a_j\}$ traženi niz.

Preostaje dokazati da za niz $\{a_j\}$ vrijedi tvrdnja (2) koja kaže: $a_{j+1} \equiv a_j \pmod{p^j}$ i da vrijedi: $\{b_i\} \sim \{a_j\}$. Imamo:

$$\begin{aligned} \left|a_{j+1} - a_j\right|_p &= \left|(a_{j+1} - b_{N(j+1)}) + (b_{N(j+1)} - b_{N(j)}) - (a_j - b_{N(j)})\right|_p = \\ &\leq max\left\{ \left|a_{j+1} - b_{N(j+1)}\right|_p, \left|b_{N(j+1)} - b_{N(j)}\right|_p, \left|a_j - b_{N(j)}\right|_p \right\} = \\ &\leq max\Big\{ \underbrace{\frac{1}{p^{j+1}}}_{\text{zbog leme}}, \underbrace{\frac{1}{p^j}}_{\substack{\text{jer je } \{b_i\} \\ \text{Cauchyjev}}}, \underbrace{\frac{1}{p^j}}_{\text{zbog leme}} \Big\} = \frac{1}{p^j} \end{aligned}$$

$$\begin{aligned} &\Rightarrow \quad \left|a_{j+1} - a_j\right|_p = \frac{1}{p^{ord_p(a_{j+1} - a_j)}} \leq \frac{1}{p^j} \\ &\Rightarrow \quad ord_p(a_{j+1} - a_j) \geq j \\ &\Rightarrow \quad p^j \mid (a_{j+1} - a_j) \\ &\Rightarrow \quad a_{j+1} \equiv a_j (\text{mod } p^j) \quad \Rightarrow \quad \text{vrijedi tvrdnja (2)} \end{aligned}$$

Također, uz proizvoljan j, $(\forall i \geq N(j))$ vrijedi:

$$\begin{aligned} |a_i - b_i|_p &= \left|(a_i - a_j) + (a_j - b_{N(j)}) - (b_i - b_{N(j)})\right|_p = \\ &\leq max\Big\{ \left|a_i - a_j\right|_p, \left|a_j - b_{N(j)}\right|_p, \left|b_i - b_{N(j)}\right|_p \Big\} = \\ &\leq max\Big\{ \underbrace{\frac{1}{p^j}}_{\substack{\text{zbog (2)} \\ \text{jer je} \\ i \geq N(j) \geq j}}, \underbrace{\frac{1}{p^j}}_{\substack{\text{zbog načina} \\ \text{na koji smo} \\ \text{odabrali } a_j \\ \text{(zbog leme)}}}, \underbrace{\frac{1}{p^j}}_{\substack{\text{zbog (2)} \\ \text{jer je} \\ i \geq N(j) \geq j}} \Big\} = \frac{1}{p^j} \end{aligned}$$

$\Rightarrow$ $(\forall j)$ $(\forall i \geq N(j))$ vrijedi: $|a_i - b_i|_p \leq \frac{1}{p^j}$
$\Rightarrow$ $|a_i - b_i|_p \to 0$ kada $i \to \infty$
$\Rightarrow$ $\{a_i\} \sim \{b_i\}$ □

No što za ako naš p-adski broj a ne vrijedi: $|a|_p \leq 1$?
U tom slučaju ćemo a pomnožiti s p^m uz $m = -ord_p(a)$ (tj. zapravo a množimo s $|a|_p$) pa onda možemo promatrati tako dobiveni p-adski broj $a' := a \cdot p^m = a \cdot |a|_p$.
Znamo da vrijedi:

$$x := |a|_p = \frac{1}{p^{ord_p(a)}} =: \frac{1}{p^k},$$

pa zato:

$$\Big|\, |a|_p \,\Big|_p = |x|_p = \left|\frac{1}{p^k}\right|_p = \frac{|1|_p}{\left|p^k\right|_p} = \frac{1}{\left|p^k\right|_p} = \frac{1}{\frac{1}{p^k}} = p^k = \frac{1}{x} = \frac{1}{|a|_p}$$

$$\Rightarrow \quad |a'|_p = \Big|\, a \cdot |a|_p \,\Big|_p = |a|_p \cdot \Big|\, |a|_p \,\Big|_p = |a|_p \cdot \frac{1}{|a|_p} = \frac{|a|_p}{|a|_p} = 1 \leq 1$$

Dakle, za dobiveni p-adski broj a' vrijedi: $(|a'|_p \leq 1)$ pa na njega možemo primijeniti prethodni teorem. Time dobivamo da je a' reprezentiran točno jednim nizom $\{a'_i\}$ koji zadovoljava svojstva (1) i (2) iz iskaza teorema. To znači da je $a = a' p^{-m}$ reprezentiran nizom: $\{a_i\} = \{a'_i p^{-m}\}$.
Sada je prikladno sve a'_i-ove zapisati u bazi p: $a'_i = b_0 + b_1 p + b_2 p^2 + ... + b_{i-1} p^{i-1}$, gdje su b_i-ovi "znamenke", tj. cijeli brojevi iz skupa $\{0, 1, ..., p-1\}$.
Svojstvo (2) koje vrijedi za niz $\{a'_i\}$ i koje kaže da je $a'_i \equiv a'_{i+1} \pmod{p^i}$ znači da je i: $a'_{i+1} \equiv a'_i \pmod{p^i}$ pa je a'_{i+1} oblika: $a'_{i+1} = a'_i + b_i \cdot p^i$. Zato možemo pisati:

$$a'_{i+1} = b_0 + b_1 p + b_2 p^2 + ... + b_{i-1} p^{i-1} + b_i p^i,$$

pri čemu su svi b_i-ovi iz skupa $\{0, 1, ..., p-1\}$ te su $b_0, ..., b_{i-1}$ isti kao i kod a'_i.
Dakle, o p-adskom broju a' možemo razmišljati kao o broju zapisanom u bazi p koji se zdesna proteže u beskonačnost (tj. svaki put kad prijeđemo s a'_i na a'_{i+1} moramo dodati novu znamenku).

$$\Rightarrow \ [a = a' p^{-m}] \ \Rightarrow a_i = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + ... + \frac{b_{i-1}}{p^{m-(i-1)}}$$

Vidimo da o svom originalnom p-adskom broju a možemo razmišljati kao o decimalnom broju zapisanom u bazi p koji ima samo konačno mnogo znamenki "desno od decimalne točke" (tj. ima samo konačno mnogo negativnih potencija od p u zapisu kao od malo prije). Radi jednostavnosti, pisat ćemo to kao:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + ... + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + ...,$$

pri čemu je izraz s desne strane jednakosti skraćenica za čitav niz $\{a_i\}$ (naime, znamo da je a reprezentiran s točno jednim nizom $\{a_i\}$ čiji je i-ti element a_i zadan s:

$$a_i = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + ... + \frac{b_{i-1}}{p^{m-(i-1)}},$$

to jest, a_i je zapravo suma prvih i pribrojnika u izrazu s desne strane jednakosti). Na taj način možemo na jednom mjestu imati zapisan čitav niz $\{a_i\}$. Taj ćemo način zapisivanja p-adskog broja a od sad pa nadalje nazivati **p-adska ekspanzija** od a.
Dakle, vidimo da svi p-adski brojevi čija je p-adska norma ≤ 1 imaju p-adsku ekspanziju bez negativnih potencija od p, dok svi p-adski brojevi čija je p-adska norma > 1 imaju p-adsku ekspanziju sa samo konačno negativnih potencija od p.

Označimo sada:

$$\mathbb{Z}_p = \Big\{(a \in \mathbb{Q}_p) : \ |a|_p \leq 1\Big\}.$$

Dakle, sa $\mathbb{Z}_p$ smo označili skup svih p-adskih brojeva čija je p-adska norma ≤ 1, to jest čija p-adska ekspanzija nema negativnih potencija od p. Elemente skupa $\mathbb{Z}_p$ nazivamo **p-adskim cijelim brojevima**. Zato ćemo od sada pa nadalje, da izbjegnemo konfuziju, elemente skupa $\mathbb{Z}_p$ nazivati p-adskim cijelim brojevima, dok ćemo elemente skupa $\mathbb{Z}$ nazivati racionalnim cijelim brojevima.
Zbroj, razlika i produkt dva elementa skupa $\mathbb{Z}_p$ je element skupa $\mathbb{Z}_p$ $\Rightarrow$ $\mathbb{Z}_p$ je potprsten polja $\mathbb{Q}_p$.

Propozicija 1.4.5. *Vrijedi:* $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Dokaz.
Neka je $(n \in \mathbb{Z})$ proizvoljan.

$\Rightarrow \quad ord_p(n) \geq 0$
$\Rightarrow \quad p^{ord_p(n)} \geq 1$
$\Rightarrow \quad |n|_p = \dfrac{1}{p^{ord_p(n)}} \leq 1$
$\Rightarrow \quad (n \in \mathbb{Z}_p)$

Kako je n bio proizvoljan, vrijedi da je svaki element od $\mathbb{Z}$ također i element od $\mathbb{Z}_p$. Dakle, $\mathbb{Z} \subseteq \mathbb{Z}_p$ pa je tvrdnja dokazana. □

Za $(a, b \in \mathbb{Q}_p)$ pišemo: $a \equiv b (\text{mod } p^n)$ ako vrijedi: $|a-b|_p \leq \frac{1}{p^n}$ (tj. ako se prva ne-nul znamenka u p-adskoj ekspanziji od $a-b$ pojavljuje ne ranije od p^n-tog mjesta).

Definiramo:

$$\mathbb{Z}_p^\times = \left\{(x \in \mathbb{Z}_p) : \frac{1}{x} \in \mathbb{Z}_p\right\} = \left\{(x \in \mathbb{Z}_p) : x \not\equiv 0 (\text{mod } p)\right\} = \left\{(x \in \mathbb{Z}_p) : |x|_p = 1\right\}.$$

Elemente skupa $\mathbb{Z}_p^\times$ (tj. p-adske cijele brojeve čija je prva znamenka (ona uz $p^0 = 1$, jer p-adski cijeli brojevi nemaju negativnih potencija od p) različita od 0) nazivamo **p-adskim jedinicama**.

Ako je $\{c_i\}$ proizvoljan niz p-adskih brojeva koji (p-adski) konvergiraju u nulu (tj. za koje vrijedi: $|c_i|_p \to 0$ kada $i \to \infty$), onda niz parcijalnih suma $S_N = c_1 + c_2 + ... + c_N$ konvergira prema limesu kojeg označavamo s: $\sum_{i=1}^{\infty} c_i$. To vrijedi zbog (uz $M \geq N$):

$$|S_M - S_N|_p = |c_{N+1} + c_{N+2} + ... + c_M|_p \leq max\left\{|c_{N+1}|_p, |c_{N+2}|_p, ..., |c_M|_p\right\} \to 0 \text{ kada } N \to \infty.$$

Dakle, lakše je provjeriti konvergira li beskonačan red p-adskih brojeva nego beskonačan red realnih brojeva jer je kod realnih brojeva konvergencija u 0 samo nužan uvjet za konvergenciju beskonačnog reda, dok je kod p-adskih brojeva taj uvjet i dovoljan (red u $\mathbb{Q}_p$ konvergira akko mu članovi teže u nulu). To vrijedi zato što je za $(p \neq \infty)$ (tj. kad je norma $|\,|_p$ nearhimedska): $|\sum_n a_n|_p \leq max\{|a_n|_p\}$, a ne $|\sum_n a_n|_p \leq \sum_n |a_n|_p$.

Vratimo se na p-adske ekspanzije. Sada vidimo da beskonačan red zdesna (izraz s desne strane znaka jednakosti) u definiciji p-adske ekspanzije:

$$\frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + ... + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + ...$$

konvergira prema a, pa se ta jednakost može uzeti u smislu sume beskonačnog reda.
Ako dvije p-adske ekspanzije konvergiraju prema istom p-adskom broju, one su jednake (sve znamenke su im iste).

1.5 Aritmetika u $\mathbb{Q}_p$

Iako kod p-adskih brojeva dopuštamo beskonačno mnogo znamenki, o aritmetici p-adskih brojeva možemo razmišljati na isti način kao i o aritmetici prirodnih brojeva zapisanih u bilo kojoj bazi - primjerice, kod zbrajanja dva prirodna broja zapisana u nekoj bazi, zbrajamo dvije po dvije (odgovarajuće) znamenke i "prenosimo" jedinicu kad god je dobivena suma znamenki jednaka zadanoj bazi ili je premašuje. Taj proces kod prirodnih brojeva u nekom trenutku staje jer oni imaju samo konačno mnogo znamenaka, dok kod p-adskih brojeva taj proces ponavljamo u beskonačnost.

Zbrajanje

Neka su dana dva proizvoljna p-adska broja a i b:

$$a = \frac{a_{-m}}{p^m} + \frac{a_{-m+1}}{p^{m-1}} + ... + \frac{a_{-1}}{p} + a_0 + a_1 p + a_2 p^2 + ...$$

$$b = \frac{b_{-n}}{p^n} + \frac{b_{-n+1}}{p^{n-1}} + ... + \frac{b_{-1}}{p} + b_0 + b_1 p + b_2 p^2 + ...$$

(pri čemu B.S.O.M.P. da je $-m \leq -n$), te neka je njihov zbroj označen sa:

$$c = \frac{c_{-m}}{p^m} + \frac{c_{-m+1}}{p^{m-1}} + ... + \frac{c_{-1}}{p} + c_0 + c_1 p + c_2 p^2 + ...$$

Tada vrijedi:

$$c_{-m} \equiv a_{-m} + b_{-m} \pmod{p}$$
$$c_i \equiv a_i + b_i + \epsilon_{i-1} \pmod{p}, \quad (\forall i > -m)$$

gdje je: $a_{i-1} + b_{i-1} = c_{i-1} + \epsilon_{i-1} \cdot p$,

pri čemu je ϵ_{i-1} znamenka koju "prenosimo" te može biti jednaka ili 0 ili 1.
Navodimo primjer:

$$\begin{array}{rl} & 1\cdot 5^{-1}+1\cdot 5^{0}+2\cdot 5^{1}+1\cdot 5^{2}+4\cdot 5^{3}+3\cdot 5^{4}+\ldots \\ + & 0\cdot 5^{-1}+2\cdot 5^{0}+3\cdot 5^{1}+4\cdot 5^{2}+3\cdot 5^{3}+0\cdot 5^{4}+\ldots \\ \hline & 1\cdot 5^{-1}+3\cdot 5^{0}+0\cdot 5^{1}+1\cdot 5^{2}+3\cdot 5^{3}+4\cdot 5^{4}+\ldots \end{array}$$

Oduzimanje

Neka su a i b kao ranije , te njihova razlika označena s: $c=\sum_{i=-m} c_i\cdot p^i$.
Vrijedi:

$$\begin{aligned} c_{-m} &\equiv a_{-m}-b_{-m} \pmod p \\ c_i &\equiv a_i-b_i-\epsilon_{i-1} \pmod p, \quad (\forall i>-m) \end{aligned}$$

gdje je: $a_{i-1}-b_{i-1}=c_{i-1}-\epsilon_{i-1}\cdot p$

Navodimo primjer:

$$\begin{array}{rl} & 2\cdot 7^{-2}+2\cdot 7^{-1}+0\cdot 7^{0}+3\cdot 7^{1}+\ldots \\ - & 0\cdot 7^{-2}+4\cdot 7^{-1}+6\cdot 7^{0}+5\cdot 7^{1}+\ldots \\ \hline & 2\cdot 7^{-2}+5\cdot 7^{-1}+0\cdot 7^{0}+4\cdot 7^{1}+\ldots \end{array}$$

Množenje

Neka su a i b kao ranije , te njihov produkt označen s: $c=\sum_{i=-m} c_i\cdot p^i$.
Vrijedi:

$$\begin{aligned} c_{-m} &\equiv a_{-m}\cdot b_{-m} \pmod p \\ c_i &\equiv \left\{\sum_{\substack{j,k\le i\\ j+k=i}} a_j\cdot b_k\right\}+\epsilon_{i-1} \pmod p, \quad (\forall i>-m) \end{aligned}$$

gdje je: $\displaystyle\sum_{\substack{j,k\le i-1\\ j+k=i-1}} a_j\cdot b_k=c_{i-1}+\epsilon_{i-1}\cdot p$

Navodimo primjer:

$$\begin{array}{rl} & 3\cdot 7^{-1}+3\cdot 7^{0}+6\cdot 7^{1}+2\cdot 7^{2}+\ldots \\ \times & 1\cdot 7^{-1}+4\cdot 7^{0}+5\cdot 7^{1}+1\cdot 7^{2}+\ldots \\ \hline & 3\cdot 7^{-1}+5\cdot 7^{0}+5\cdot 7^{1}+4\cdot 7^{2}+\ldots \end{array}$$

Dijeljenje
Navodimo primjer:

$$\begin{array}{r|l} 3+5\cdot 7^{1}+1\cdot 7^{2}+\ldots & 5+1\cdot 7^{1}+6\cdot 7^{2}+\ldots \\ \hline & 1+2\cdot 7^{1}+4\cdot 7^{2}+\ldots \\ \hline & 1+6\cdot 7^{1}+1\cdot 7^{2}+\ldots \\ \hline & 3\cdot 7^{1}+2\cdot 7^{2}+\ldots \\ & 3\cdot 7^{1}+5\cdot 7^{2}+\ldots \\ \hline & 4\cdot 7^{2}+\ldots \\ & 4\cdot 7^{2}+\ldots \\ \hline & \\ & \vdots \end{array}$$

Teorem 1.5.1. ***(Henselova lema)***
Neka je $F(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \cdots + c_nx^n$ *polinom čiji su koeficijenti iz* $\mathbb{Z}_p^\times$, $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + n\cdot c_nx^{n-1}$ *njegova derivacija i* $(a_0 \in \mathbb{Z}_p^\times)$ *t.d.* $F(a_0) \equiv 0 \ (mod\ p)$ *i* $F'(a_0) \not\equiv 0 \ (mod\ p)$.
Tada $(\exists! a \in \mathbb{Z}_p^\times)$ *t.d.* $F(a) = 0$ *i* $a \equiv a_0 \ (mod\ p)$.

Dokaz.
Tvrdimo da postoji jedinstveni niz cijelih brojeva $\{a_n\}_{n\in\mathbb{N}}$ t.d. $(\forall n \geq 1)$ vrijedi:
(1) $F(a_n) \equiv 0 \pmod{p^{n+1}}$
(2) $a_n \equiv a_{n-1} \pmod{p^n}$
(3) $0 \leq a_n < p^{n+1}$.
Indukcijom ćemo pokazati da takav niz $\{a_n\}_{n\in\mathbb{N}}$ postoji i jedinstven je.

BAZA INDUKCIJE: n=1
Označimo sa $\tilde{a}_0$ jedinstveni element skupa $\{0, 1, \ldots, p-1\}$ koji je kongruentan a_0 (mod p). To znači da $(\exists y)$ t.d. $\tilde{a}_0 = y\cdot p + a_0$, što povlači da je: $a_0 = \tilde{a}_0 - y\cdot p$.
Ako neki a_1 zadovoljava uvjete (2) i (3), onda vrijedi: $(0 \leq a_1 < p^2)$,

$a_1 \equiv a_0 \pmod p \;\Rightarrow\; (\exists x)$ t.d. $a_1 = x \cdot p + a_0$.
Time dobivamo: $a_1 = x \cdot p + a_0 = x \cdot p + \tilde{a}_0 - y \cdot p = \underbrace{(x-y)}_{=:\, b_1} \cdot p + \tilde{a}_0$.

$\Rightarrow$ svaki a_1 koji zadovoljava (2) i (3) mora biti oblika: $a_1 = b_1 \cdot p + \tilde{a}_0$, uz:
$(0 \le b_1 \le p-1)$
Dakle, za proizvoljni b_1 takav da $(0 \le b_1 \le p-1)$, na sljedeći način možemo zadati neki a_1 za koji će vrijediti svojstva (2) i (3): $a_1 = b_1 \cdot p + \tilde{a}_0$.
Ali mi želimo da za taj a_1 vrijedi i svojstvo (1), tj. $F(a_1) \equiv 0 \pmod{p^2}$.

$$\begin{aligned} F(a_1) = F(\tilde{a}_0 + b_1 \cdot p) &= \sum c_i \cdot (\tilde{a}_0 + b_1 \cdot p)^i = \\ &= \sum c_i \cdot (\tilde{a}_0^i + \tilde{a}_0^{i-1} \cdot i \cdot b_1 \cdot p + \text{sumandi djeljivi s } p^2) = \\ &= \sum (c_i \cdot \tilde{a}_0^i + c_i \cdot \tilde{a}_0^{i-1} \cdot i \cdot b_1 \cdot p + \text{sumandi djeljivi s } p^2) = \end{aligned}$$

$$\begin{aligned} &\equiv \sum c_i \cdot \tilde{a}_0^i + b_1 \cdot p \cdot \sum c_i \cdot \tilde{a}_0^{i-1} \cdot i \pmod{p^2} = \\ &= F(\tilde{a}_0) + F'(\tilde{a}_0) \cdot b_1 \cdot p \end{aligned}$$

Uočimo sličnost s: $F(x+h) = F(x) + F'(x) \cdot h +$ (faktori višeg reda) .
Tako dobivamo: $F(\tilde{a}_0) = F(a_0 + y \cdot p) = \underbrace{F(a_0)}_{\substack{\equiv 0 \pmod p \\ \text{prema pretp.}}} + F'(a_0) \cdot y \cdot p +$ (faktori višeg reda)
$\Rightarrow\; F(\tilde{a}_0) \equiv 0 \pmod p \;\Rightarrow\; (\exists \alpha \in \{0, 1, \ldots, p-1\})$ t.d. $F(\tilde{a}_0) = \alpha \cdot p$
$\Rightarrow\; F(\tilde{a}_0) \equiv \alpha p \pmod{p^2}$
Dobili smo: $F(a_1) \equiv F(\tilde{a}_0) + F'(\tilde{a}_0) \cdot b_1 p \pmod{p^2}$, $F(\tilde{a}_0) \equiv \alpha p \pmod{p^2}$.
$\Rightarrow\; F(a_1) \equiv F(\tilde{a}_0) + F'(\tilde{a}_0) \cdot b_1 p \equiv \alpha p + F'(\tilde{a}_0) \cdot b_1 p \pmod{p^2}$
Dakle, za a_1 će svojstvo (1), tj. $F(a_1) \equiv 0 \pmod{p^2}$, vrijediti ako i samo ako:
$\alpha p + F'(\tilde{a}_0) \cdot b_1 p \equiv 0 \pmod{p^2}$, a znamo da je:

$$\begin{aligned} \alpha p + F'(\tilde{a}_0) \cdot b_1 p \equiv 0 \pmod{p^2} &\Leftrightarrow \alpha + F'(\tilde{a}_0) \cdot b_1 \equiv 0 \pmod p \\ &\Leftrightarrow F'(\tilde{a}_0) \cdot b_1 \equiv -\alpha \pmod p \\ &\Leftrightarrow b_1 \equiv -\frac{\alpha}{F'(\tilde{a}_0)} \pmod p \end{aligned}$$

Ovdje smo mogli dijeliti s $F'(\tilde{a}_0)$ jer je, prema pretpostavci, $F'(a_0) \not\equiv 0 \pmod p$ što onda (zbog $a_0 \equiv \tilde{a}_0 \pmod p$) povlači: $F'(\tilde{a}_0) \not\equiv 0 \pmod p$.
Dakle, za b_1 takav da vrijedi $(0 \le b_1 \le p-1)$ i:

$$b_1 \equiv -\frac{\alpha}{F'(\tilde{a}_0)} \pmod p,$$

na sljedeći način možemo zadati a_1 za koji će vrijediti svojstva (1), (2) i (3):
$a_1 = b_1 \cdot p + \tilde{a}_0$ (očito je b_1 jedinstveno određen s ta dva uvjeta).

PRETPOSTAVKA INDUKCIJE:
Pretpostavimo da za neki $(n \in \mathbb{N})$ postoje jedinstveni $a_1, \ldots, a_{n-1}$ za koje vrijede svojstva (1),(2),(3).

KORAK INDUKCIJE:
Želimo naći jedinstveni a_n za kojeg vrijede svojstva:
(1) $F(a_n) \equiv 0 \pmod{p^{n+1}}$
(2) $a_n \equiv a_{n-1} \pmod{p^n}$
(3) $0 \leq a_n < p^{n+1}$.

Da bi za a_n vrijedila svojstva (2) i (3), morao bi postojati neki $(b_n \in \{0, 1, \ldots, p-1\})$ takav da: $a_n = a_{n-1} + b_n p^n$.
Mi želimo da za a_n vrijedi i svojstvo (1): $F(a_n) \equiv 0 \pmod{p^{n+1}}$.

$$\begin{aligned} F(a_n) = F(a_{n-1} + b_n \cdot p^n) &= \sum c_i \cdot (a_{n-1} + b_n \cdot p^n)^i = \\ &= \sum c_i \cdot \left(a_{n-1}^i + a_{n-1}^{i-1} \cdot i \cdot b_n \cdot p^n + \text{sumandi djeljivi s } p^{n+1}\right) = \\ &= \sum \left(c_i \cdot a_{n-1}^i + c_i \cdot a_{n-1}^{i-1} \cdot i \cdot b_n \cdot p^n + \text{sumandi djeljivi s } p^{n+1}\right) = \\ &\equiv \sum c_i \cdot a_{n-1}^i + b_n \cdot p^n \cdot \sum c_i \cdot a_{n-1}^{i-1} \cdot i \pmod{p^{n+1}} = \\ &= F(a_{n-1}) + F'(a_{n-1}) \cdot b_n \cdot p^n \end{aligned}$$

Budući da je prema pretpostavki indukcije (svojstvo (1) za a_{n-1}) $F(a_{n-1}) \equiv 0 \pmod{p^n}$, $(\exists \alpha')$ t.d. $F(a_{n-1}) = \alpha' p^n \Rightarrow F(a_{n-1}) \equiv \alpha' \cdot p^n \pmod{p^{n+1}}$.
Dakle, $F(a_n) \equiv F(a_{n-1}) + F'(a_{n-1}) \cdot b_n \cdot p^n \equiv \alpha' \cdot p^n + F'(a_{n-1}) \cdot b_n \cdot p^n \pmod{p^{n+1}}$.
Time naše željeno svojstvo (1) postaje:

$$\alpha' \cdot p^n + F'(a_{n-1}) \cdot b_n \cdot p^n \equiv 0 \pmod{p^{n+1}} \quad \Leftrightarrow \quad \alpha' + F'(a_{n-1}) \cdot b_n \equiv 0 \pmod{p}.$$

Iz svojstva (2) koje prema pretpostavci indukcije vrijedi za $a_1, \ldots, a_{n-1}$ slijedi:

$$\begin{aligned} &a_{n-1} \equiv a_{n-2} \pmod{p^{n-1}} \Rightarrow a_{n-1} = a_{n-2} + z_{n-1} \cdot p^{n-1} \\ &a_{n-2} \equiv a_{n-3} \pmod{p^{n-2}} \Rightarrow a_{n-2} = a_{n-3} + z_{n-2} \cdot p^{n-2} \\ &\vdots \\ &a_2 \equiv a_1 \pmod{p^2} \Rightarrow a_2 = a_1 + z_2 \cdot p^2 \\ &a_1 \equiv a_0 \pmod{p} \Rightarrow a_1 = a_0 + z_1 \cdot p \end{aligned}$$

Dakle, imamo:

$$a_{n-1} = \underbrace{z_{n-1} \cdot p^{n-1} + z_{n-2} \cdot p^{n-2} + \cdots + z_2 \cdot p^2 + z_1 \cdot p^1}_{\text{djeljivo s } p} + \underbrace{a_0}_{\text{ostatak}}$$

$\Rightarrow \quad a_{n-1} \equiv a_0 \pmod{\text{p}}$
$\Rightarrow \quad F'(a_{n-1}) \equiv F'(a_0) \pmod{\text{p}}$, a znamo da je prema pretpostavci zadatka:
$F'(a_0) \not\equiv 0 \pmod{\text{p}}$
$\Rightarrow \quad F'(a_{n-1}) \not\equiv 0 \pmod{\text{p}}$, pa možemo s tim podijeliti i tako dobivamo:

$$\frac{\alpha'}{F'(a_{n-1})} + b_n \equiv 0 (\text{mod p}) \quad \Rightarrow \quad b_n \equiv \frac{-\alpha'}{F'(a_{n-1})} (\text{mod p})$$

Dakle, dobili smo jedinstveni b_n koji je jedinstven način određuje a_n koji zadovoljava svojstva (1), (2), (3).

Ovime je završena indukcija, a time i dokaz tvrdnje da postoji jedinstveni niz cijelih brojeva $\{a_n\}_{n\in\mathbb{N}}$ t.d. $(\forall n \geq 1)$ vrijedi:
(1) $F(a_n) \equiv 0 \pmod{p^{n+1}}$
(2) $a_n \equiv a_{n-1} \pmod{p^n}$
(3) $0 \leq a_n < p^{n+1}$.
Tvrdnja teorema odmah slijedi iz netom dokazane tvrdnje - jednostavno uzmemo:
$a = \tilde{a}_0 + b_1 p + b_2 p^2 + \ldots$. Budući da $(\forall n)$ vrijedi: $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$, slijedi da p-adski broj $F(a)$ mora biti jednak nuli.
Obratno, svaki $a = \tilde{a}_0 + b_1 p + b_2 p^2 + \ldots$ daje niz a_n-ova kao u tvrdnji, a jedinstvenost tog niza povlači jedinstvenost od a. A očito je da je $a \equiv \tilde{a}_0 \equiv a_0 \pmod{\text{p}}$. Time je Henselova lema dokazana. □

Lema 1.5.2. *Ako* $(a \in \mathbb{Q}_p)$ *ima p-adsku ekspanziju:* $a = a_{-m}p^{-m} + \cdots + a_0 + a_1 p + a_2 p^2 + \ldots$, *p-adska ekspanzija od* $-a$ *glasi:*
$(p - a_{-m}) \cdot p^{-m} + (p - 1 - a_{-m+1}) \cdot p^{-m+1} + \cdots + (p - 1 - a_0) \cdot p^0 + (p - 1 - a_1) \cdot p^1 + \ldots$.

Dokaz.

$$\begin{array}{rrrrr} & 0 \cdot p^{-m} + & 0 \cdot p^{-m+1} + \ldots + & 0 \cdot p^0 + & 0 \cdot p^1 + \ldots \\ - & a_{-m} \cdot p^{-m} + & a_{-m+1} \cdot p^{-m+1} + \ldots + & a_0 \cdot p^0 + & a_1 \cdot p^1 + \ldots \\ \hline & (p - a_{-m}) \cdot p^{-m} + (p - 1 - a_{-m+1}) \cdot p^{-m+1} + \ldots + (p - 1 - a_0) \cdot p^0 + (p - 1 - a_1) \cdot p^1 + \ldots \end{array}$$

Naime, koeficijent uz p^{-m} je: $0 - a_{-m} = -a_{-m} = p - a_{-m} - p = (p - a_{-m}) - 1 \cdot p$
$\Rightarrow$ to je $p - a_{-m}$ i ostatak -1.

Koeficijent uz p^{-m+1} je: $0-a_{-m+1}-1 = -a_{-m+1}-1 = p-a_{-m+1}-1-p = (p-1-a_{-m+1})-1\cdot p$
$\Rightarrow$ to je $p - 1 - a_{-m+1}$ i ostatak -1.

Koeficijent uz p^{-m+2} je: $0-a_{-m+2}-1 = -a_{-m+2}-1 = p-a_{-m+2}-1-p = (p-1-a_{-m+2})-1\cdot p$
$\Rightarrow$ to je $p - 1 - a_{-m+2}$ i ostatak -1.

I tako nastavimo dalje. □

Lema 1.5.3. *U $\mathbb{Q}_p$ vrijedi:*

$$1 + p + p^2 + p^3 + \cdots \to \frac{1}{1-p}$$
$$1 - p + p^2 - p^3 + \cdots \to \frac{1}{1+p}$$
$$1 + (p-1)p + p^2 + (p-1)p^3 + \cdots \to \frac{p^2 - p + 1}{1 - p^2}.$$

Dokaz.
Znamo da $\sum_{n=0}^{\infty} a_n \to a$ u $\mathbb{Q}_p$ ako i samo ako: $\left|\sum_{n=0}^{\infty} a_n - a\right|_p = \lim_{N\to\infty} |S_N - a|_p = 0$
uz oznaku: $S_N = a_1 + \cdots + a_N$.
Vrijedi:

$$\left|\sum_{n=0}^{\infty} p^n - \frac{1}{1-p}\right|_p = \lim_{N\to\infty}\left|S_N - \frac{1}{1-p}\right|_p = \lim_{N\to\infty}\left|\frac{1}{1-p} - S_N\right|_p =$$
$$= \lim_{N\to\infty}\left|\frac{1}{1-p} - \left(1 + p + p^2 + \cdots + p^N\right)\right|_p =$$
$$= \lim_{N\to\infty}\left|\frac{1}{1-p} - \frac{1-p^{N+1}}{1-p}\right|_p =$$

$$= \lim_{N\to\infty}\left|\frac{1 - 1 + p^{N+1}}{1-p}\right|_p = \lim_{N\to\infty}\left|\frac{p^{N+1}}{1-p}\right|_p =$$
$$= \lim_{N\to\infty} \frac{1}{p^{ord_p(p^{N+1}) - ord_p(1-p)}} =$$
$$= \lim_{N\to\infty} \frac{1}{p^{N+1-0}} = \lim_{N\to\infty} \frac{1}{p^{N+1}} = 0$$

Dakle, uistinu vrijedi: $\sum_{n=0}^{\infty} p^n \to \frac{1}{1-p}$ u $\mathbb{Q}_p$.

$$1-p+p^2-p^3+\cdots = \sum_{n=0}^{\infty}(-p)^n = [\text{prema prethodnom primjeru}] = \frac{1}{1-(-p)} = \frac{1}{1+p}$$

$$\begin{aligned}
&1+(p-1)p+p^2+(p-1)p^3+p^4+(p-1)p^5+\cdots = \\
&= 1+(p^2-p)+p^2+(p^4-p^3)+p^4+(p^6-p^5)+\cdots = \\
&= \left(1-p+p^2-p^3+p^4-p^5+\ldots\right)+\left(p^2+p^4+p^6+\ldots\right) = \\
&= \{\text{prema prethodnom primjeru}\} = \\
&= \frac{1}{1+p}+\left(\sum_{n=0}^{\infty}p^{2n}-1\right) = \frac{1}{1+p}+\left(\sum_{n=0}^{\infty}(p^2)^n-1\right) = \\
&= \{\text{prema prvom primjeru iz ovog dokaza}\} = \\
&= \frac{1}{1+p}+\left(\frac{1}{1-p^2}-1\right) = \frac{1}{1+p}+\left(\frac{1}{(1-p)(1+p)}-1\right) = \\
&= \frac{(1-p)+(1)-(1-p^2)}{1-p^2} = \frac{p^2-p+1}{1-p^2}
\end{aligned}$$

□

Propozicija 1.5.4. *p-adska ekspanzija od* $(x \in \mathbb{Q}_p)$ *ima ponavljajuće znamenke od nekog mjesta na dalje ako i samo ako je* $(x \in \mathbb{Q})$.

Dokaz.
Smjer $\Rightarrow$
Pretpostavljamo da p-adska ekspanzija od $(x \in \mathbb{Q}_p)$ ima ponavljajuće znamenke od mjesta k na dalje, to jest:

$$\begin{aligned}
x &= x_{-m}p^{-m}+\cdots+x_0+x_1p+x_2p^2+\cdots+x_{k-1}p^{k-1}+(a_0\cdot p^k+a_1p^{k+1}+a_2p^{k+2}+ \\
&\quad +\cdots+a_sp^{k+s})+(a_0\cdot p^{k+s+1}+a_1p^{k+s+2}+a_2p^{k+s+3}+\cdots+a_sp^{k+2s+1})+\cdots = \\
&= \underbrace{x_{-m}p^{-m}+\cdots+x_0+x_1p+\cdots+x_{k-1}p^{k-1}}_{=:(*)}+\overline{a_0\cdot p^k+a_1p^{k+1}+\cdots+a_sp^{k+s}}
\end{aligned}$$

$$\Rightarrow \quad x-(*) = \overline{a_0\cdot p^k+a_1p^{k+1}+\cdots+a_sp^{k+s}}$$

$$\begin{aligned}
b &:= \frac{x-(*)}{p^k} = \overline{a_0+a_1p^1+\cdots+a_sp^s} = \\
&= (a_0+a_1p^1+\cdots+a_sp^s)+(a_0p^{s+1}+a_1p^{s+2}+\cdots+a_sp^{2s+1})+ \\
&\quad +(a_0p^{2s+2}+a_1p^{2s+3}+\cdots+a_sp^{3s+2})+\ldots
\end{aligned}$$

$\Rightarrow$ $a := a_0 + a_1 p^1 + \cdots + a_s p^s$ je cijeli broj pa time i racionalan i vrijedi:

$$b = a \cdot (1 + p^{s+1} + p^{2s+2} + \dots) = a \cdot (1 + p^{s+1} + p^{2(s+1)} + \dots) = a \cdot \frac{1}{1 - p^{s+1}}$$

$\Rightarrow$ b je racionalan broj $\Rightarrow$ $\frac{x-(*)}{p^k} = b \in \mathbb{Q}$, a znamo da je i (*) racionalan
$\Rightarrow$ $x = b \cdot p^k + (*) \in \mathbb{Q}$

Smjer $\Leftarrow$

Pretpostavljamo da je $(x \in \mathbb{Q}_p)$ racionalan broj. Možemo uzeti: $x = \frac{B}{N}$ pa B.S.O.M.P. da je taj razlomak maksimalno skraćen.
Dovoljno je pokazati da tvrdnja vrijedi u slučaju da $p \nmid B$ i $p \nmid N$.

Naime, ako $p \nmid N$ ali $p \mid B$, tada možemo pisati: $x = p \cdot \frac{B'}{N}$ za neki $p \nmid B'$, pri čemu znamo da vrijedi:

$$\frac{B'}{N} = a_{-m} p^{-m} + \cdots + a_0 + a_1 p + \cdots + a_{k-1} p^{k-1} + \overline{b_0 \cdot p^k + b_1 p^{k+1} + \cdots + b_s p^{k+s}}.$$

Zato imamo:

$$x = p \cdot \frac{B'}{N} = p \cdot \left(a_{-m} p^{-m} + \cdots + a_0 + a_1 p + \cdots + a_{k-1} p^{k-1} + \overline{b_0 \cdot p^k + b_1 p^{k+1} + \cdots + b_s p^{k+s}} \right) =$$
$$= a_{-m} p^{-m+1} + \cdots + a_0 p + a_1 p^2 + \cdots + a_{k-1} p^k + \overline{b_0 \cdot p^{k+1} + b_1 p^{k+2} + \cdots + b_s p^{k+s+1}},$$

pa vidimo da tvrdnja vrijedi i za x.

Ako $p \nmid B$ ali $p \mid N$, tada možemo pisati: $x = \frac{1}{p} \cdot \frac{B}{N'}$ za neki $p \nmid N'$, pri čemu znamo da vrijedi:

$$\frac{B}{N'} = a_{-m} p^{-m} + \cdots + a_0 + a_1 p + \cdots + a_{k-1} p^{k-1} + \overline{b_0 \cdot p^k + b_1 p^{k+1} + \cdots + b_s p^{k+s}}.$$

Zato imamo:

$$x = \frac{1}{p} \cdot \frac{B}{N'} = \frac{1}{p} \cdot \left(a_{-m} p^{-m} + \cdots + a_0 + a_1 p + \cdots + a_{k-1} p^{k-1} + \overline{b_0 \cdot p^k + b_1 p^{k+1} + \cdots + b_s p^{k+s}} \right) =$$
$$= a_{-m} p^{-m-1} + \cdots + a_0 p^{-1} + a_1 + \cdots + a_{k-1} p^{k-2} + \overline{b_0 \cdot p^{k-1} + b_1 p^k + \cdots + b_s p^{k+s-1}},$$

pa tvrdnja vrijedi i za x.

Dakle, dokazujemo tvrdnju u slučaju da $p \nmid B$ i $p \nmid N$, tj. u slučaju $(x \in \mathbb{Z}_p)$.
Neka je p-adska ekspanzija od x dana s: $x = a_0 + a_1 \cdot p + a_2 \cdot p^2 + ...$

$$\Rightarrow \quad \frac{x - a_0}{p} = a_1 + a_2 \cdot p + a_3 \cdot p^2 + ... \in \mathbb{Q}_p$$

$$\Rightarrow \quad a_1 + a_2 \cdot p + a_3 \cdot p^2 + ... = \frac{x - a_0}{p} = \frac{\frac{B}{N} - a_0}{p} = \frac{B}{p \cdot N} - \frac{a_0}{p} = \frac{B - N \cdot a_0}{p \cdot N} = \frac{\frac{B - N \cdot a_0}{p}}{N}$$

$$\Rightarrow \quad \frac{\frac{\frac{B - N \cdot a_0}{p}}{N} - a_1}{p} = a_2 + a_3 \cdot p + a_4 \cdot p^2 + ... \in \mathbb{Q}_p$$

$$\Rightarrow \quad a_2 + a_3 \cdot p + a_4 \cdot p^2 + ... = \frac{B - N \cdot a_0}{p^2 \cdot N} - \frac{a_1}{p} = \frac{B - N \cdot a_0 - p \cdot N \cdot a_1}{p^2 \cdot N} = \frac{\frac{B - N \cdot a_0 - p \cdot N \cdot a_1}{p^2}}{N}$$

Nastavljajući tako dalje, $(\forall r \geq 0)$ dobivamo da vrijedi:

$$\frac{\frac{B - N \cdot a_0 - N \cdot a_1 \cdot p - N \cdot a_2 \cdot p^2 - ... - N \cdot a_r \cdot p^r}{p^{r+1}}}{N} = a_{r+1} + a_{r+2} \cdot p + a_{r+3} \cdot p^2 + ... \in \mathbb{Q}_p$$

Za proizvoljni $(r \geq 0)$ vrijedi:

$$\left| \frac{B - N \cdot a_0 - N \cdot a_1 \cdot p - N \cdot a_2 \cdot p^2 - ... - N \cdot a_r \cdot p^r}{p^{r+1}} \right| =$$

$$\leq \frac{|B| + |N| \cdot a_0 + |N| \cdot a_1 \cdot p + ... + |N| \cdot a_r \cdot p^r}{p^{r+1}} =$$

$$\leq \left[a_i \leq p - 1 \right] \leq \frac{|B| + |N| \cdot (p-1) + |N| \cdot (p-1) \cdot p + ... + |N| \cdot (p-1) \cdot p^r}{p^{r+1}} =$$

$$\leq \frac{|B| + |N| \cdot (p-1) \cdot \left[1 + p + p^2 + ... + p^r \right]}{p^{r+1}} = \frac{|B| + |N| \cdot (p-1) \cdot \frac{1 - p^{r+1}}{1-p}}{p^{r+1}} =$$

$$= \frac{|B| + |N| \cdot (p-1) \cdot \frac{p^{r+1} - 1}{p-1}}{p^{r+1}} = \frac{|B| + |N| \cdot (p^{r+1} - 1)}{p^{r+1}} = \frac{|B|}{p^{r+1}} + |N| - \frac{|N|}{p^{r+1}} =$$

$$\leq \frac{|B|}{p^{r+1}} + |N| \quad \leq \quad |B| + |N| = konst.$$

Dakle, apsolutne vrijednosti cijelih brojeva:

$$\frac{B - N \cdot a_0}{p}, \frac{B - N \cdot a_0 - N \cdot a_1 \cdot p}{p^2}, ..., \frac{B - N \cdot a_0 - N \cdot a_1 \cdot p - ... - N \cdot a_r \cdot p^r}{p^{r+1}}$$

su ograničene, što znači da su oni elementi konačnog skupa.

$\Rightarrow$ za neke $r_1 \neq r_2$ su vrijednosti pripadajućih cijelih brojeva jednake, tj. u $\mathbb{Q}_p$ vrijedi:

$$a_{r_1+1} + a_{r_1+2} \cdot p + a_{r_1+3} \cdot p^2 + ... = \frac{B - Na_0 - Na_1 p - ... - Na_{r_1} p^{r_1}}{p^{r_1+1}} =$$

$$= \frac{B - Na_0 - Na_1 p - ... - Na_{r_2} p^{r_2}}{p^{r_2+1}} = a_{r_2+1} + a_{r_2+2} \cdot p + a_{r_2+3} \cdot p^2 + ...$$

$\Rightarrow$ $a_{r_1+i} = a_{r_2+i}, \quad (\forall i \geq 1)$

$\Rightarrow$ p-adska ekspanzija od $a_0 + a_1 \cdot p + a_2 \cdot p^2 + ...$ je periodična

□

Lema 1.5.5. *p-adska ekspanzija od $(a \in \mathbb{Q}_p)$ terminira (tj. $(\exists N)$ t.d. je $a_i = 0$ $(\forall i \geq N))$ ako i samo ako je a pozitivan racionalan broj čiji nazivnik je potencija od p.*

Dokaz.

Smjer $\Leftarrow$

Pretpostavimo da je $(a \in \mathbb{Q}_p)$ zadan kao razlomak $a = \frac{B}{p^M}$ uz $B > 0$ (B.S.O.M.P. da je taj razlomak maksimalno skraćen).

$\Rightarrow$ $p \nmid B$

Neka je sada n maksimalan cijeli broj takav da $p^n \leq B$.

$$\Rightarrow \quad B = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n \quad (b_i = 0 \text{ za } i > n)$$

$$\Rightarrow \quad a = \frac{B}{p^M} = b_0 \cdot p^{-M} + b_1 \cdot p^{-M+1} + b_2 \cdot p^{-M+2} + \cdots + b_n \cdot p^{-M+n}$$

Uz oznaku $N := -M + n$ imamo da je $(\forall i > N)$ $a_i = 0$.

Smjer $\Rightarrow$

Pretpostavljamo da je a p-adski broj s p-adskom ekspanzijom:

$$a = a_{-m} p^{-m} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots + a_N \cdot p^N \quad (a_i = 0 \text{ za } i > N).$$

$\Rightarrow$ p-adski broj a ima ponavljajuće znamenke od mjesta $N+1$ na dalje (od tog mjesta na dalje su sve znamenke jednake nuli)
$\Rightarrow$ iz propozicije 1.5.4 slijedi da je a racionalan broj (1)

Znamo da je p prost broj pa samim time i pozitivan, te su svi a_i-ovi također pozitivni brojevi, a znamo da je produkt pozitivnih brojeva pozitivan broj i da je suma pozitivnih brojeva pozitivan broj.
Dakle, a je sigurno pozitivan. (2)

$$a = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots + a_N \cdot p^N =$$
$$= \frac{a_{-m} + a_{-m+1} \cdot p + \cdots + a_0 \cdot p^m + a_1 \cdot p^{m+1} + a_2 \cdot p^{m+2} + \cdots + a_N \cdot p^{m+N}}{p^m}$$

$\Rightarrow$ nazivnik od a je potencija od p (3)

Sada nam tvrdnje (1), (2) i (3) zajedno daju da je a pozitivan racionalan broj čiji je nazivnik potencija od p. Time je dokaz gotov. □

Poglavlje 2

p-adska interpolacija Riemannove zeta funkcije

Riemannova zeta funkcija definira se kao funkcija realnih brojeva većih od 1 zadana formulom:

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

Usporedbom s integralom (uz fiksirani $s > 1$):

$$\begin{aligned}\int_1^{\infty} \frac{1}{x^s}\,dx &= \int_1^{\infty} x^{-s}\,dx = \\ &= \frac{x^{1-s}}{1-s}\Big|_{x=1}^{x=+\infty} = \\ &= \{\text{zbog } \; s > 1 \Rightarrow 1 - s < 0\} = \frac{1}{1-s} \cdot (0-1) = \\ &= \frac{-1}{1-s} = \frac{1}{s-1}\end{aligned}$$

vidi se da ta suma konvergira kada je $(s > 1)$.

Neka je p proizvoljan prost broj. Svrha ovog poglavlja je pokazati da se funkcija $\zeta(2k)$ (za $k = 1, 2, 3, \dots$) može na jedinstven način proširiti sa $\mathbb{Z}$ na $\mathbb{Z}_p^{\times}$ i to tako da je dobivena funkcija neprekidna funkcija p-adske varijable s vrijednostima u $\mathbb{Q}_p$. Kao i u realnom slučaju, kažemo da je funkcija p-adske varijable f neprekidna ako vrijedi da, kad god se niz p-adskih cijelih brojeva $\{x_n\}$ p-adski približava x-u, tada se i niz $\{f(x_n)\}$ p-adski približava *f(x)*-u. Na to mislimo kad govorimo o p-adskoj interpolaciji.

2.1 Formula za $\zeta(2k)$

k-ti Bernoullijev broj B_k definiramo kao $k!$ pomnoženo s k-tim koeficijentom u razvoju u Taylorov red izraza $f(t) := \frac{t}{e^t-1}$:

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty} a_k t^k, \quad B_k = a_k \cdot k! \quad \Rightarrow \quad a_k = \frac{B_k}{k!} \quad \Rightarrow \quad \frac{t}{e^t-1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} \cdot t^k$$

U stvari je: $B_k = f^{(k)}(0)$.
Prvih nekoliko B_k-ova su: $B_0 = 1,\ B_1 = \frac{-1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = \frac{-1}{30},\ B_5 = 0,$ $B_6 = \frac{1}{42}, \ldots$.

Lema 2.1.1. $B_k = 0$ *za svaki neparan broj* $(k > 1)$.

Dokaz.

$$\frac{x}{e^x-1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} \cdot x^k = B_1 \cdot x + \sum_{\substack{k\geq 0 \\ k\neq 1}} \frac{B_k}{k!} \cdot x^k = \left(B_1 = \frac{-1}{2}\right) = \frac{-x}{2} + \sum_{\substack{k\geq 0 \\ k\neq 1}} \frac{B_k}{k!} \cdot x^k$$

$$\Rightarrow \ \frac{x}{e^x-1} + \frac{x}{2} = \sum_{\substack{k\geq 0 \\ k\neq 1}} \frac{B_k}{k!} \cdot x^k \tag{1}$$

Također, vrijedi:

$$f(x) := \frac{x}{e^x-1} + \frac{x}{2} = \frac{2x + x(e^x-1)}{2(e^x-1)} = \frac{2x + xe^x - x}{2(e^x-1)} = \frac{xe^x + x}{2(e^x-1)} =$$

$$= \frac{x(e^x+1)}{2(e^x-1)} = \left(\frac{/ \cdot e^{\frac{-x}{2}}}{/ \cdot e^{\frac{-x}{2}}}\right) = \frac{x}{2} \cdot \frac{e^{\frac{x}{2}} + e^{\frac{-x}{2}}}{e^{\frac{x}{2}} - e^{\frac{-x}{2}}} = \left(\frac{/ \cdot (-1)}{/ \cdot (-1)}\right) = -\frac{x}{2} \cdot \frac{e^{\frac{x}{2}} + e^{\frac{-x}{2}}}{e^{-\frac{x}{2}} - e^{\frac{x}{2}}} = f(-x)$$

$$\Rightarrow \ f(x) = f(-x) \tag{2}$$

Sada nam tvrdnje (1) i (2) daju:

$$\sum_{\substack{k\geq 0 \\ k\neq 1}} \frac{B_k}{k!} \cdot x^k = \sum_{\substack{k\geq 0 \\ k\neq 1}} \frac{B_k \cdot (-1)^k}{k!} \cdot x^k$$

$\Rightarrow$ za $(k \geq 0), (k \neq 1)$ je $B_k = (-1)^k \cdot B_k$
$\Rightarrow$ specijalno, za $(k \geq 0), (k \neq 1)$ pri čemu je k neparan vrijedi: $B_k = -1 \cdot B_k = -B_k$
$\Rightarrow$ za takve k (nenegativne, $\neq 1$, neparne) je $B_k = 0$ $\square$

Propozicija 2.1.2. *Za sve realne brojeve* x *beskonačni produkt:*

$$\pi x \cdot \prod_{n=1}^{\infty} \left(1 + \frac{x^2}{n^2}\right)$$

konvergira i jednak je $sh(\pi x)$.

Dokaz ove propozicije ćemo navesti nešto kasnije (u 3. poglavlju).

Propozicija 2.1.3. *Za svaki* $(k \in \mathbb{N})$ *vrijedi formula:*

$$\zeta(2k) = (-1)^k \pi^{2k} \cdot \frac{2^{2k-1}}{(2k-1)!} \cdot \left(-\frac{B_{2k}}{2k}\right).$$

Dokaz.
Prema propoziciji 2.1.2 znamo da vrijedi:

$$sh(\pi x) = \pi x \cdot \prod_{n=1}^{\infty} \left(1 + \frac{x^2}{n^2}\right)$$

Uzimamo logaritam obje strane tog izraza (za $x > 0$).
S lijeve strane dobivamo:

$$\begin{aligned} ln[sh(\pi x)] &= ln\left(\frac{e^{\pi x} - e^{-\pi x}}{2}\right) = \\ &= ln\left[\frac{e^{\pi x}}{2} \cdot (1 - e^{-2\pi x})\right] = ln\left[\frac{e^{\pi x}}{2}\right] + ln(1 - e^{-2\pi x}) = \\ &= ln(e^{\pi x}) - ln(2) + ln(1 - e^{-2\pi x}) = \\ &= \pi x - ln(2) + ln(1 - e^{-2\pi x}) \end{aligned}$$

S desne strane dobijemo (za $0 < x < 1$):

$$\begin{aligned} ln\left[\pi x \cdot \prod_{n=1}^{\infty} \left(1 + \frac{x^2}{n^2}\right)\right] &= ln(\pi) + ln(x) + \sum_{n=1}^{\infty} ln\left(1 + \frac{x^2}{n^2}\right) = \\ &= \left\{ ln(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} \cdot \frac{x^n}{n} \quad \text{za} \quad |x| < 1 \right\} = \\ &= ln(\pi) + ln(x) + \sum_{n=1}^{\infty} \left(\sum_{k=1}^{\infty} (-1)^{k-1} \cdot \frac{x^{2k}}{k n^{2k}} \right) = \end{aligned}$$

$$= ln(\pi) + ln(x) + \sum_{n=1}^{\infty}\left(\sum_{k=1}^{\infty}(-1)^{k+1}\cdot\frac{x^{2k}}{kn^{2k}}\right)$$

Znamo da dvostruki red $\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}a_{nk}$ apsolutno konvergira ako $(\forall n = 1, 2, ...)$ $\sum_{k=1}^{\infty}|a_{nk}|$ konvergira prema nekom b_n i $\sum_{n=1}^{\infty}b_n$ konvergira. Raspišimo to za naš konkretni dvostruki red:

$$\begin{aligned}
\sum_{k=1}^{\infty}|a_{nk}| &= \sum_{k=1}^{\infty}\left|(-1)^{k+1}\cdot\frac{x^{2k}}{kn^{2k}}\right| = \\
&= \left\{0 < x < 1 \Rightarrow x = \frac{1}{a} \text{ za neki } (a > 1)\right\} = \sum_{k=1}^{\infty}\left|\frac{(-1)^{k+1}}{k\cdot(an)^{2k}}\right| = \\
&= \sum_{k=1}^{\infty}\frac{1}{k\cdot(an)^{2k}} = \\
&\leq \sum_{k=1}^{\infty}\frac{1}{(an)^{2k}} = \\
&= \sum_{k=0}^{\infty}\left(\frac{1}{a^2n^2}\right)^k - 1 = \frac{1}{1-\frac{1}{a^2n^2}} - 1 = \frac{a^2n^2}{a^2n^2-1} - 1 = \\
&= \frac{a^2n^2 - a^2n^2 + 1}{a^2n^2-1} = \frac{1}{a^2n^2-1} =: b_n
\end{aligned}$$

$$\begin{aligned}
\sum_{n=1}^{\infty}b_n &= \sum_{n=1}^{\infty}\frac{1}{a^2n^2-1} = \\
&\leq \sum_{n=1}^{\infty}\frac{1}{a^2n^2-n^2} = \sum_{n=1}^{\infty}\frac{1}{n^2\cdot(a^2-1)} = \frac{1}{a^2-1}\cdot\sum_{n=1}^{\infty}\frac{1}{n^2} = \\
&= \left\{\text{znamo da Dirichletov red } \sum_{n=1}^{\infty}\frac{1}{n^p} \text{ konvergira } \Leftrightarrow p > 1, \right\} < \infty
\end{aligned}$$

Dakle, vidimo da naš dvostruki red apsolutno konvergira za $0 < x < 1$, pa možemo promijeniti poredak sumacije te tako dobivamo (nakon izjednačavanja lijeve i desne strane jednakosti na koje smo prethodno djelovali s logaritmom):

$$\begin{aligned}
\pi x - ln(2) + ln(1 - e^{-2\pi x}) &= ln(\pi) + ln(x) + \sum_{k=1}^{\infty}\left((-1)^{k+1}\cdot\frac{x^{2k}}{k}\cdot\sum_{n=1}^{\infty}\frac{1}{n^{2k}}\right) = \\
&= ln(\pi) + ln(x) + \sum_{k=1}^{\infty}\left((-1)^{k+1}\cdot\frac{x^{2k}}{k}\cdot\zeta(2k)\right)
\end{aligned}$$

Sada ćemo obje strane dobivene jednakosti derivirati po varijabli x.
Desnu stranu možemo derivirati član-po-član jer je dobiveni red uniformno konvergentan u $(0 < x < 1 - \epsilon)$ $(\forall \epsilon > 0)$. Naime, da bismo dokazali tu činjenicu, možemo upotrijebiti Weierstrassov M-test koji kaže:
ako za dani niz funkcija $f_k : X \to \mathbb{R}$ postoji niz konstanti $(M_k)_k$ takvih da vrijede sljedeća dva uvjeta:

$$(1) \quad |f_k(x)| \leq M_k \ \ (\forall x \in X)(\forall k \geq 1)$$

$$(2) \quad \sum_{k=1}^{\infty} M_k < \infty,$$

onda red $\sum_{k=1}^{\infty} f_k(x)$ konvergira apsolutno i uniformno na X.
Uzimamo: $f_k(x) = (-1)^{k+1} \cdot \frac{x^{2k}}{k} \cdot \zeta(2k)$ i želimo naći konstante M_k za koje vrijedi tvrdnja M-testa.
Ocijenimo prvo $\zeta(2k)$. Znamo da je: $\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}}$. Označimo sada: $S_N = \sum_{n=1}^{N} \frac{1}{n^{2k}}$.

$\Rightarrow \ S_N - 1 = \sum_{n=2}^{N} \frac{1}{n^{2k}}$

$\Rightarrow \ S_N - 1$ je donja Darbouxova suma za određeni integral: $\int_1^N \frac{1}{x^{2k}}\, dx$ uz subdiviziju: $[1, N] = [1, 2] \cup [2, 3] \cup \cdots \cup [N-1, N]$ i vrijedi:

$$S_N - 1 < \int_1^N \frac{1}{x^{2k}}\, dx = \int_1^N x^{-2k}\, dx = \frac{x^{1-2k}}{1-2k}\Big|_{x=1}^{x=N} = \frac{N^{1-2k} - 1}{1-2k} = \frac{1}{2k-1} \cdot \left(1 - \frac{1}{N^{2k-1}}\right)$$

$$\Rightarrow \ \lim_{N\to\infty}(S_N - 1) < \frac{1}{2k-1} \cdot \lim_{N\to\infty} 1 - \frac{1}{N^{2k-1}} = \frac{1}{2k-1}$$

$$\Rightarrow \ \zeta(2k) = \lim_{N\to\infty}(S_N) = \lim_{N\to\infty}(S_N - 1) + 1 < 1 + \frac{1}{2k-1}$$

$$\Rightarrow \ \left|(-1)^{k+1} \cdot \frac{x^{2k}}{k} \cdot \zeta(2k)\right| \leq \frac{(1-\epsilon)^{2k}}{k} \cdot \left(1 + \frac{1}{2k-1}\right) =: M_k \qquad (\forall \ x \ \text{t.d.} \ \ 0 < x < 1 - \epsilon)$$

Dakle, prema Weierstrassovom M-testu, dobiveni red je uniformno konvergentan u $(0 < x < 1 - \epsilon)$ $(\forall \epsilon > 0)$ pa desnu stranu možemo derivirati član-po-član.

Nakon deriviranja obje strane i izjednačavanja dobivamo:

$$\frac{2\pi \cdot \mathrm{e}^{-2\pi x}}{1 - \mathrm{e}^{-2\pi x}} + \pi = \frac{1}{x} + \sum_{k=1}^{\infty} (-1)^{k+1} \cdot \frac{(2k) \cdot x^{2k-1}}{k} \cdot \zeta(2k) = \frac{1}{x} + 2 \cdot \sum_{k=1}^{\infty} (-1)^{k+1} \cdot x^{2k-1} \cdot \zeta(2k)$$

Možemo sve pomnožiti s x:

$$\frac{2\pi x \cdot \mathrm{e}^{-2\pi x}}{1 - \mathrm{e}^{-2\pi x}} + \pi x = 1 + 2 \cdot \sum_{k=1}^{\infty} (-1)^{k+1} \cdot x^{2k} \cdot \zeta(2k)$$

Nakon što sada uvrstimo $x = \frac{x}{2}$, dobivamo:

$$\frac{\pi x \cdot \mathrm{e}^{-\pi x}}{1-\mathrm{e}^{-\pi x}} + \frac{\pi x}{2} = 1 + \sum_{k=1}^{\infty} (-1)^{k+1} \cdot \frac{x^{2k}}{2^{2k-1}} \cdot \zeta(2k)$$

$$\Rightarrow \left\{ \frac{\mathrm{e}^{-\pi x}}{1-\mathrm{e}^{-\pi x}} = \frac{1}{\mathrm{e}^{\pi x} \cdot (1-\mathrm{e}^{-\pi x})} = \frac{1}{\mathrm{e}^{\pi x}-1} \right\} \Rightarrow \frac{\pi x}{\mathrm{e}^{\pi x}-1} + \frac{\pi x}{2} = 1 + \sum_{k=1}^{\infty} \frac{(-1)^{k+1} \cdot \zeta(2k)}{2^{2k-1}} \cdot x^{2k}$$

$$\Rightarrow \left\{ \frac{\pi x}{\mathrm{e}^{\pi x}-1} = \sum_{k=0}^{\infty} \frac{B_k \cdot (\pi x)^k}{k!} \right\} \Rightarrow \frac{\pi x}{2} + \sum_{k=0}^{\infty} \frac{B_k \cdot (\pi x)^k}{k!} = 1 + \sum_{k=1}^{\infty} \frac{(-1)^{k+1} \cdot \zeta(2k)}{2^{2k-1}} \cdot x^{2k}$$

Usporedbom koeficijenata uz parne potencije od x dobivamo:

$$\frac{B_{2k} \cdot \pi^{2k}}{(2k)!} = \frac{(-1)^{k+1} \cdot \zeta(2k)}{2^{2k-1}}$$

$$\Rightarrow \quad \zeta(2k) = (-1)^k \pi^{2k} \cdot \frac{2^{2k-1}}{(2k-1)!} \cdot \left(-\frac{B_{2k}}{2k}\right) \qquad \square$$

Zapis formule za $\zeta(2k)$ iz prethodnog teorema je namjeran. Naime, o faktoru $-\frac{B_{2k}}{2k}$ razmišljamo kao o "zanimljivom dijelu" formule, dok nam $(-1)^k \pi^{2k} \cdot \frac{2^{2k-1}}{(2k-1)!}$ nije zanimljiv.

2.2 p-adska interpolacija funkcije $f(s) = a^s$

Ako je a fiksiran pozitivan realan broj, funkcija $f(s) = a^s$ definira se kao neprekidna funkcija realne varijable tako da se prvo definira za racionalan s, a zatim se "interpolira" tj. "proširi po neprekidnosti" na sve realne brojeve tako da se prvo pokaže da, ako su racionalne vrijednosti s_1 i s_2 blizu, onda su vrijednosti $f(s_1) = a^{s_1}$ i $f(s_2) = a^{s_2}$ također blizu, i naposlijetku, za proizvoljan realan s definiramo: $f(s) = \lim_{n\to\infty} f(s_n) = \lim_{n\to\infty} a^{s_n}$ pri čemu je $\{s_n\}$ proizvoljan niz racionalnih brojeva koji konvergira prema s. Primijetimo da, ako je promatrana funkcija f definirana na nekom skupu A koji je gust podskup nekog skupa B (što znači da se svaki element skupa B može prikazati kao limes nekog niza elemenata skupa A), onda se funkcija f može na jedinstven način proširiti do neprekidne funkcije na B.

Pretpostavimo sada da je $a = n$ fiksiran prirodni broj. Razmišljat ćemo o n-u kao o elementu skupa $\mathbb{Q}_p$. Za svaki $(s \in \mathbb{N}_0)$ je integer $n^s \in \mathbb{Z}_p$ (naime,
$n \in \mathbb{N}_0 \Rightarrow |n|_p \leq 1 \Rightarrow |n^s|_p = |n|_p^s \leq 1^s = 1$).

Lema 2.2.1. *Skup $\mathbb{N}_0$ je gust u $\mathbb{Z}_p$.*

Dokaz.
Zapravo želimo dokazati da se svaki element skupa $\mathbb{Z}_p$ može aproksimirati nekim nizom elemenata skupa $\mathbb{N}_0$.
Neka je $(x \in \mathbb{Z}_p)$ proizvoljan. To znači da je x oblika: $x = a_0 + a_1 p + a_2 p^2 + \ldots$.
Za svaki $(n \in \mathbb{N}_0)$ definiramo: $x_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n$. Kako su $(a_i, p \in \mathbb{N}_0)$ $(\forall i = 1, \ldots, n)$, tako je i $(x_n \in \mathbb{N}_0)$ $(\forall n \in \mathbb{N}_0)$.
Također vrijedi:

$$|x - x_n|_p = \left|a_{n+1}p^{n+1} + a_{n+2}p^{n+2} + \ldots\right|_p =$$
$$= \frac{1}{p^{ord_p(a_{n+1}p^{n+1} + a_{n+2}p^{n+2} + \ldots)}} \leq \frac{1}{p^{n+1}} < \frac{1}{p^n}$$

$\Rightarrow$ Kako je $(x \in \mathbb{Z}_p)$ bio proizvoljan, zaključujemo da za svaki element skupa $\mathbb{Z}_p$ na opisani način možemo naći neki niz $\{x_n\}$ iz $\mathbb{N}_0$ koji ga aproksimira, što znači da je $\mathbb{N}_0$ uistinu gust u $\mathbb{Z}_p$. □

Dakle, uz $a{=}n$ fiksiran kao ranije, možemo promatrati funkciju $f : \mathbb{N}_0 \to \mathbb{Z}_p$ zadanu s: $f(s) = a^s = n^s$, pri čemu je $\mathbb{N}_0$ gust u $\mathbb{Z}_p$. Prema razmatranju iz uvodnog odlomka ovog poglavlja, vidimo da, ukoliko uopće funkciju f možemo proširiti do neprekidne funkcije na $\mathbb{Z}_p$, to možemo učiniti na jedinstven način. Za to se moramo zapitati vrijedi li da, ako su $(s, s' \in \mathbb{N}_0)$ (p-adski) blizu, da su onda i $f(s) = n^s$ i $f(s') = n^{s'}$ također (p-adski) blizu. To ne vrijedi uvijek. Navodimo primjer:

$s' = s + p^N \Rightarrow |s - s'|_p = \left|p^N\right|_p = \frac{1}{p^N}$

specijalno, za $n = p, s = 0 \Rightarrow s' = p^N \Rightarrow f(s) = p^0, f(s') = p^{p^N}$

$\Rightarrow |f(s) - f(s')|_p = \left|1 - p^{p^N}\right|_p = \frac{1}{p^{ord_p(1-p^{p^N})}} = \frac{1}{p^0} = 1$ bez obzira na to koliki je N

Ali to nam neće predstavljati veliki problem kao što se iz navedenog primjera čini.

1. SLUČAJ: n je $\in \mathbb{N}_0$ čiji je ostatak pri dijeljenju s p jednak 1

Neka je n t.d. je $n \equiv 1 \pmod{p}$, to jest $n = 1 + mp$ za neki m. Neka je $s' = s + s''p^N$ za neki $(s'' \in \mathbb{Z})$ tako da vrijedi:

$$|s' - s|_p = \left|(s + s''p^N) - s\right|_p = \left|s''p^N\right|_p = \frac{1}{p^{ord_p(s''p^N)}} \leq \frac{1}{p^N} \text{ jer je } ord_p(s''p^N) \geq N$$

B.S.O.M.P. da je $(s' > s)$. Sada vrijedi:

$$\left|n^s - n^{s'}\right|_p = \left\{s' > s \Rightarrow n^s - n^{s'} = n^s \cdot (1 - n^{s'-s})\right\} = |n^s|_p \cdot \left|1 - n^{s'-s}\right|_p =$$

$$= \left|1 - n^{s'-s}\right|_p = \left|1 - (1 + mp)^{s'-s}\right|_p = \left|1 - (1 + mp)^{s''p^N}\right|_p =$$

$$\uparrow$$

zbog: $|n^s|_p = \left|(1 + mp)^s\right|_p = \frac{1}{p^{ord_p((1+mp)^s)}} = \left\{p \nmid (1 + mp) \Rightarrow p \nmid (1 + mp)^s\right\} = \frac{1}{p^0} = 1$

$$= \frac{1}{p^{ord_p\left(1-(1+mp)^{s''p^N}\right)}} \leq \frac{1}{p^{N+1}} \tag{2.1}$$

$$\uparrow$$

zbog: $(1 + mp)^{s''p^N} =$ [binomni TM] =

$$= 1 + (s''p^N)mp + \frac{s''p^N(s''p^N - 1)}{2}(mp)^2 + ... + (mp)^{s''p^N}$$

$\Rightarrow$ svaki pribrojnik u $1 - (1 + mp)^{s''p^N}$ je djeljiv s najmanje p^{N+1}

$\Rightarrow$ $ord_p(1 - (1 + mp)^{s''p^N}) \geq N + 1$

Dobili smo: ako $p^N \mid (s' - s)$, onda $p^{N+1} \mid (n^s - n^{s'})$. To jest (za veliki N), ako su s i s' blizu, onda su i n^s i $n^{s'}$ blizu.
Dakle, ako je $n \equiv 1 \pmod{p}$, možemo definirati $f(s) = n^s$ za proizvoljni $(s \in \mathbb{Z}_p)$ kao: $f(s) = \lim_{i\to\infty} n^{s_i}$ (pri čemu je $\{s_i\}$ proizvoljan niz iz $\mathbb{N}_0$ koji teži prema s). Tako dodefinirana funkcija f je neprekidna na $\mathbb{Z}_p$.

2. SLUČAJ: n je proizvoljan $\in \mathbb{N}_0$ koji nije djeljiv s p

Neka je n proizvoljan nenegativan cijeli broj koji nije djeljiv s p. U ovom ćemo slučaju zahtijevati da s i s' budu ne samo p-adski blizu (tj. kongruentni modulo p^N za veliki N), nego ćemo uzimati i da su oni kongruentni modulo $p - 1$. To jest, fiksirat ćemo neki

$(s_0 \in \{0, 1, ..., p-2\})$ i, umjesto da promatramo n^s za sve nenegativne cijele brojeve s, mi ćemo promatrati n^s za sve nenegativne cijele brojeve s koji su kongruentni našem fiksiranom s_0 modulo $p-1$. Označimo skup svih takvih dopuštenih brojeva s sa S_{s_0} $\left(\text{to jest, } S_{s_0} := \left\{(s \in \mathbb{N}_0) : s \equiv s_0(\text{mod p-1})\right\}\right)$. S_{s_0} je gust podskup od $\mathbb{Z}_p$ (to ćemo dokazati u sljedećoj lemi - lemi 2.2.2).
Neka je $(s \in S_{s_0})$ proizvoljan, tj. $(\exists s_1 \in \mathbb{N}_0)$ t.d. $s = s_0 + (p-1)s_1$.

$$\Rightarrow \quad f(s) = n^s = n^{s_0+(p-1)s_1} = \underbrace{n^{s_0}}_{\text{konstanta}} \cdot \underbrace{\left(n^{p-1}\right)^{s_1}}_{\text{konstanta}}$$

$\Rightarrow$ funkcija $f : S_{s_0} \to \mathbb{Z}_p$ definirana sa: $f(s) = n^s$ je zapravo ista kao i funkcija $F : \mathbb{N}_0 \to \mathbb{Z}_p$ definirana sa: $F(s) = n^{s_0} \cdot \underbrace{\left(n^{p-1}\right)^{s}}_{=:\,\mathrm{N}} = \underbrace{n^{s_0}}_{\text{konstanta}} \cdot N^s$ uz n koji nije djeljiv s p, pa prema malom Fermatovom teoremu vrijedi: $N = n^{p-1} \equiv 1$ (mod p)
$\Rightarrow$ sada smo u situaciji kao iz prvog slučaja uz N umjesto n i uz dodanu konstantu n^{s_0}

$\Rightarrow$ za takvu funkciju f (odnosno F) se na analogan način kao i u prvom slučaju pokaže da, ako su $(s, s' \in S_{s_0})$ blizu, onda su i $f(s)$ i $f(s')$ također blizu
Dakle, funkcija $f : S_{s_0} \to \mathbb{Z}_p$ definirana sa: $f(s) = n^s$ može se na jedinstven način proširiti po neprekidnosti sa S_{s_0} na čitav $\mathbb{Z}_p$. Uočimo: u ovom slučaju promatrana funkcija f ovisi o s_0 i n.

Lema 2.2.2. *Skup* $S_{s_0} = \{(s \in \mathbb{N}_0) : s \equiv s_0(mod p-1)\}$ *je gust podskup od* $\mathbb{Z}_p$.

Dokaz.
Zapravo želimo pokazati da se svaki element skupa $\mathbb{Z}_p$ može aproksimirati nekim nizom elemenata skupa S_{s_0}, to jest da $(\forall x \in \mathbb{Z}_p)$ i $(\forall \epsilon > 0)$ postoji neki $(s \in S_{s_0})$ t.d. $|x - s|_p < \epsilon$.
Iz leme 2.2.1 znamo da je $\mathbb{N}_0$ gust u $\mathbb{Z}_p$, pa za proizvoljne $(x \in \mathbb{Z}_p)$ i $(\epsilon > 0)$ postoji neki $(n_0 \in \mathbb{N}_0)$ t.d. $|x - n_0|_p < \frac{\epsilon}{2}$.
Dakle, dovoljno je naći neki $(s \in S_{s_0})$ t.d. $|n_0 - s|_p < \frac{\epsilon}{2}$ jer onda imamo:

$$|x - s|_p \leq \underbrace{|x - n_0|_p}_{<\frac{\epsilon}{2}} + \underbrace{|n_0 - s|_p}_{<\frac{\epsilon}{2}} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \quad \text{pa tvrdnja vrijedi}$$

1. slučaj: $(n_0 \in S_{s_0})$

onda možemo uzeti $s := n_0$ pa vrijedi: $|x - s|_p = |x - n_0|_p < \frac{\epsilon}{2} < \epsilon$ pa tvrdnja vrijedi

2. slučaj: $(n_0 \notin S_{s_0})$

$\Rightarrow \quad n_0 \not\equiv s_0 \pmod{p\text{-}1}$

$\Rightarrow \quad n_0 = s_1 + (p-1)\cdot\alpha \quad$ za neke $\quad (\alpha \geq 0), (s_0 \neq s_1 \in \{0, 1, ..., p-2\})$

Neka je $(N \in \mathbb{N})$ t.d. $p^{-N} < \frac{\epsilon}{2}$, $(k \in \mathbb{N})$ t.d. $k - \alpha = (s_1 - s_0)\cdot(1 + p + p^2 + ... + p^{N-1})$ (ili $k - \alpha = (s_0 - s_1)\cdot(1 + p + p^2 + ... + p^{N-1})$ ako je $(s_0 > s_1)$) i $(s := s_0 + (p-1)\cdot k \in S_{s_0})$.
Vrijedi:

$$
\begin{aligned}
|s - n_0|_p &= |s_0 + k\cdot(p-1) - s_1 - \alpha\cdot(p-1)|_p = \\
&= |(s_0 - s_1) + (p-1)\cdot(k-\alpha)|_p = \\
&= \left|(s_0 - s_1) + (p-1)\cdot(s_1 - s_0)\cdot(1 + p + p^2 + ... + p^{N-1})\right|_p = \\
&= |s_0 - s_1|_p \cdot \left|1 + (p-1)\cdot(1 + p + p^2 + ... + p^{N-1})\right|_p = \\
&= 1 \cdot \left|1 + (p-1)\cdot\frac{1-p^N}{1-p}\right|_p = \left|1 + (p-1)\cdot\frac{p^N - 1}{p-1}\right|_p = \\
&\uparrow \\
&\text{zbog:} \quad s_0, s_1 \in \{0, 1, ..., p-2\} \quad \Rightarrow \quad s_0 - s_1 \in \left\{-(p-2), ..., -1, 0\right\} \\
&\qquad \Rightarrow \quad |s_0 - s_1|_p = \frac{1}{p^0} = 1 \\
&= \left|1 + (p^N - 1)\right|_p = \left|p^N\right|_p = \frac{1}{p^N} < \frac{\epsilon}{2} \quad \text{prema pretpostavci}
\end{aligned}
$$

$\Rightarrow$ tvrdnja vrijedi $\square$

3. SLUČAJ: n je proizvoljan $\in \mathbb{N}_0$ koji je djeljiv s p $\Rightarrow$ n je oblika: $n = m \cdot p$

Ako je $\{s_i\}$ proizvoljan rastući niz u $\mathbb{N}_0$, onda je i niz $\{p^{s_i}\}$ također rastući, pa je $n^{s_i} = m^{s_i} \cdot p^{s_i}$ djeljiv sa sve većom potencijom od p, tj. p-adski teži u nulu

$\Rightarrow$ za svaki rastući niz $\{s_i\}$ u $\mathbb{N}_0$ vrijedi: $n^{s_i} \to 0$ p-adski

Ako je $(s \in \mathbb{Z}_p/\mathbb{N}_0)$, onda je njegova p-adska ekspanzija beskonačna suma bez negativnih potencija od p, pa niz $s_i = a_0 + a_1 \cdot p + ... + a_i \cdot p^i$ p-adski teži ka s. Ali znamo da $s_i \to +\infty$ u $\mathbb{N}$, pa onda imamo kao gore: $n^{s_i} \to 0$ p-adski.

Ako bismo željeli neprekidnost, moralo bi iz $|s - s_i|_p \to 0$ slijediti: $|n^s - n^{s_i}|_p \to 0$. Ali kako $n^{s_i} \to 0$ (p-adski), jedina mogućnost je $n^s = 0$, što nema smisla.

Lema 2.2.3. *Ako je* $(n \in \mathbb{Z}_p)$ *i, specijalno,* $|n|_p = 1$, *onda se funkcija* $f : \mathbb{N}_0 \to \mathbb{Z}_p$ *zadana s:* $f(s) = n^s$ *može na jedinstven način proširiti po neprekidnosti na čitav* $\mathbb{Z}_p$.

Dokaz.
Neka je $(n \in \mathbb{Z}_p)$ proizvoljan, to jest: $n = a_0 + a_1 p + a_2 p^2 + ...$ i $|n|_p \leq 1$.

1. slučaj: $|n|_p < 1$

$\Rightarrow \quad 1/p^{ord_p(n)} < 1/p^0 \quad \Rightarrow \quad ord_p(n) > 0 \quad \Rightarrow \quad p \mid n \quad \Rightarrow \quad a_0 = 0$

$\Rightarrow \quad n = a_1 p + a_2 p^2 + ... = p \cdot (a_1 + a_2 p + ...)$ $(**)$

Kao i diskusiji s početka ovog poglavlja:

za $s' = s + p^N, s = 0, s' = p^N$:

$$\Rightarrow \quad |f(s) - f(s')|_p = \left|n^s - n^{s'}\right|_p = \left|1 - n^{p^N}\right|_p = (**) = \left|1 - [p \cdot (a_1 + a_2 p + ...)]^{p^N}\right|_p =$$

$$= \frac{1}{p^0} = 1$$

$\Rightarrow$ iako su s i s' (p-adski) blizu, n^s i $n^{s'}$ nisu $\Rightarrow$ ovaj slučaj ne valja

2. slučaj: $|n|_p = 1$, tj. $(n \in \mathbb{Z}_p^\times)$

$\Rightarrow \quad 1/p^{ord_p(n)} = 1/p^0 \quad \Rightarrow \quad ord_p(n) = 0 \quad \Rightarrow \quad p \nmid n$

slučaj 2(a): $n \equiv 1 \pmod p$

$$\Rightarrow \quad n = 1 + a_1 p + a_2 p^2 + ... = 1 + p \cdot \underbrace{(a_1 + a_2 p + ...)}_{=: m \in \mathbb{Z}_p} = 1 + m \cdot p$$

$\Rightarrow$ nastavljamo dalje posve analogno kao u 1. slučaju diskusije s početka ovog poglavlja

$\Rightarrow$ ovaj slučaj valja

slučaj 2(b): $n \equiv k \pmod p$ za neki $(k \in \{2, 3, ..., p-1\})$

$\Rightarrow$ raspisujemo sve posve analogno kao u 2. slučaju diskusije s početka ovog poglavlja

$\Rightarrow$ ovaj slučaj valja

Vidimo da, ako je $(n \in \mathbb{Z}_p)$, onda se funkcija $f : \mathbb{N}_0 \to \mathbb{Z}_p$ zadana s: $f(s) = n^s$ može na jedinstven način proširiti po neprekidnosti na čitav $\mathbb{Z}_p$ samo ako je $|n|_p = 1$, tj. samo ako je $(n \in \mathbb{Z}_p^x)$. □

Lema 2.2.4. *Ako je* $(n \in \mathbb{N}), (p \nmid n)$, *onda se funkcija* $f : \mathbb{N}_0 \to \mathbb{Z}_p$ *zadana s:* $f(s) = 1/n^s$ *može na jedinstven način proširiti po neprekidnosti na čitav* $\mathbb{Z}_p$.

Pogrešan način za p-adsku interpolaciju Riemannove zeta funkcije $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ bio bi da se interpolira svaki sumand pojedinačno, i da se onda pozbroje rezultati. No to neće funkcionirati jer čak i oni sumandi koji se mogu interpolirati (to su, prema prethodnoj lemi, oni sumandi za koje $p \nmid n$) čine beskonačnu sumu koja divergira u $\mathbb{Z}_p$.
Ako bismo to nakratko "zaboravili" pa išli gledati svaki sumand pojedinačno, prvo bismo se morali riješiti sumanada oblika $\frac{1}{n^s}$ gdje $p \mid n$ jer želimo da nam ostanu samo oni sumandi koje možemo interpolirati. Imamo:

$$\begin{aligned}\zeta(s) &= \sum_{n=1, p\nmid n}^{\infty} \frac{1}{n^s} + \sum_{n=1, p\mid n}^{\infty} \frac{1}{n^s} = \\ &= [p \mid n \Rightarrow n = m \cdot p] = \sum_{n=1, p\nmid n}^{\infty} \frac{1}{n^s} + \sum_{m=1}^{\infty} \frac{1}{m^s p^s} = \\ &= \sum_{n=1, p\nmid n}^{\infty} \frac{1}{n^s} + \frac{1}{p^s} \cdot \sum_{m=1}^{\infty} \frac{1}{m^s} = \sum_{n=1, p\nmid n}^{\infty} \frac{1}{n^s} + \frac{1}{p^s} \cdot \zeta(s)\end{aligned}$$

$$\Rightarrow \quad \zeta(s) = \frac{1}{1 - \frac{1}{p^s}} \cdot \sum_{n=1, p\nmid n}^{\infty} \frac{1}{n^s}$$

Označimo: $\zeta^*(s) = \sum_{n=1, p\nmid n}^{\infty} \frac{1}{n^s} = \left(1 - \frac{1}{p^s}\right) \cdot \zeta(s)$. Ovaj postupak naziva se "izbacivanje p-Euler faktora". Naime, funkcija $\zeta(s)$ ima jednu poznatu ekspanziju (koju ćemo dokazati u sljedećoj propoziciji):

$$\zeta(s) = \prod_{prosti\ brojevi\ q} \frac{1}{1 - \frac{1}{q^s}}$$

Faktor $\frac{1}{1-\frac{1}{q^s}}$ koji odgovara prostom broju q naziva se **"q-Euler faktor"**. Dakle, množenje funkcije $\zeta(s)$ sa $1 - \frac{1}{p^s}$ će rezultirati "izbacivanjem" p-Euler faktora:

$$\zeta^*(s) = \left(1 - \frac{1}{p^s}\right) \cdot \zeta(s) = \prod_{prosti\ brojevi\ q \neq p} \frac{1}{1 - \frac{1}{q^s}}$$

Propozicija 2.2.5. *Vrijedi:*

$$\zeta(s) = \prod_{prosti\ brojevi\ p} \frac{1}{1-\frac{1}{p^s}} \qquad za\ \ (s>1)$$

Dokaz.
Uz oznake: $\mathcal{P} := \{2,3,5,7,11,...\}$ = skup svih prostih brojeva, p_n = n-ti po redu prosti broj $(p_1=2, p_2=3, p_3=5, ...)$, imamo:

$$\prod_{p\in\mathcal{P}} \frac{1}{1-\frac{1}{p^s}} = \prod_{n=1}^{\infty} \frac{1}{1-\frac{1}{{p_n}^s}} =$$

$$= \prod_{n=1}^{\infty}\left(\sum_{k=0}^{\infty}\left(\frac{1}{p_n^s}\right)^k\right) = \left(1+\frac{1}{p_1^s}+\frac{1}{p_1^{2s}}+...\right)\cdot\left(1+\frac{1}{p_2^s}+\frac{1}{p_2^{2s}}+...\right)\cdot ... =$$

$\uparrow$

zbog: $s>1 \Rightarrow p_n^s > p_n \Rightarrow \frac{1}{p_n^s} < \frac{1}{p_n} \Rightarrow \left|\frac{1}{p_n^s}\right| < \left|\frac{1}{p_n}\right| < 1\ (\forall n\in\mathbb{N})(\forall p_n\in\mathcal{P})$

= [lokalno uniformna konvergencija nam omogućava grupiranje faktora] =

$$= 1 + \left(\sum_{1\le i} \frac{1}{p_i^s}\right) + \left(\sum_{1\le i\le j} \frac{1}{p_i^s p_j^s}\right) + \left(\sum_{1\le i\le j\le k} \frac{1}{p_i^s p_j^s p_k^s}\right) + ... =$$

$$= \left\{ \begin{array}{l} \text{svaki produkt potencija prostih brojeva se pojavljuje u točno jednom} \\ \text{nazivniku i tako u svim mogućim kombinacijama, a znamo da se} \\ \text{svaki prirodni broj može na jedinstven način prikazati kao produkt} \\ \text{potencija prostih brojeva } \Rightarrow \text{ u ovim nazivnicima se nalaze svi} \\ \text{prirodni brojevi i to se sve sumira} \end{array} \right\} =$$

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

□

2.3 Topologija na $\mathbb{Q}_p$ i p-adske distribucije

Baza otvorenih skupova metričkog prostora $\mathbb{Q}_p$ sastoji se od svih skupova oblika:

$a + (p^N) \coloneqq a + p^N \cdot \mathbb{Z}_p = \left\{(x \in \mathbb{Q}_p) : |x - a|_p < \frac{1}{p^N}\right\}$ za neke $(a \in \mathbb{Q}_p),(N \in \mathbb{Z})$.
Tako definiran skup $a + (p^N)$ još nazivamo i **intervalom**, a on je zapravo otvorena kugla u $\mathbb{Q}_p$ oko točke a radijusa $\frac{1}{p^N}$ $\left(a + (p^N) = K(a, \frac{1}{p^N})\right)$. Dakle, svaki otvoreni skup u $\mathbb{Q}_p$ je unija skupova tog oblika.
Znamo da je skup $(A \subseteq \mathbb{Q}_p)$ otvoren ako za svaku njegovu točku x postoji neka otvorena kugla $K(x, r) = \{(y \in \mathbb{Q}_p) : |x - y|_p < r\}$ za neki $(r > 0)$ koja je čitava sadržana u tom skupu. A kako znamo da p-adska norma može poprimiti samo vrijednosti iz skupa $\{0, p^n : (n \in \mathbb{Z})\}$ i zanimaju nas samo radijusi koji su veći od nule, dovoljno je promatrati $K(x, r)$ samo za $r = p^n$, $(n \in \mathbb{Z})$.

Propozicija 2.3.1. *Svaka otvorena kugla u $\mathbb{Q}_p$ je također i zatvorena.*

Dokaz.

$$a + (p^N) = K\left(a, \frac{1}{p^N}\right) = \left\{(x \in \mathbb{Q}_p) : |x - a|_p < \frac{1}{p^N}\right\} =$$
$$= \left\{(x \in \mathbb{Q}_p) : |x - a|_p \leq \frac{1}{p^{N+1}}\right\} = \overline{K}\left(a, \frac{1}{p^{N+1}}\right)$$

□

Lema 2.3.2. *Skup $\mathbb{Z}_p$ je otvoren.*

Dokaz.

$\mathbb{Z}_p = a + p^N \cdot \mathbb{Z}_p = a + (p^N)$ uz $a = 0, N = 0$

□

Propozicija 2.3.3. *Skup $\mathbb{Z}_p$ je **sekvencijalno (nizovno) kompaktan**, to jest svaki niz u $\mathbb{Z}_p$ ima konvergentan podniz.*

Dokaz.
Neka je $(x_k)_k$ proizvoljan niz u $\mathbb{Z}_p$, te neka je p-adska ekspanzija od x_k dana s: $x_k = a_0^k + a_1^k \cdot p + a_2^k \cdot p^2 + ... = ...a_2^k a_1^k a_0^k$.
Znamo da postoji samo konačno mnogo mogućnosti za izbor a_0^k (preciznije, znamo da je $a_0^k \in \{0, 1, ..., p - 1\}$).
$\Rightarrow$ $(\exists b_0 \in \{0, 1, ..., p - 1\})$ i postoji podniz $(x_{0k})_k$ od $(x_k)_k$ t.d. je zadnja znamenka svakog x_{0k}-a uvijek b_0
Analogno, $(\exists b_1 \in \{0, 1, ..., p - 1\})$ i postoji podniz $(x_{1k})_k$ od $(x_{0k})_k$ t.d. je zadnja

znamenka svakog x_{1k}-a uvijek b_0, a predzadnja uvijek b_1.
Nastavivši tako dalje dobivamo niz $b_0, b_1, b_2, ...$ i niz nizova:

$$x_{00}, x_{01}, x_{02}, ...$$
$$x_{10}, x_{11}, x_{12}, ...$$
$$\vdots$$

t.d. je svaki niz podniz prethodnog niza, te svaki element n-tog niza (onog iz n-tog reda, $(x_{nk})_k$) završava znamenkama $b_n...b_1b_0$.
$\Rightarrow$ $(\forall j = 0, 1, 2, ...)$ je $\left(x_{jj} \in \{x_{j-1,j}, x_{j-1,j+1}, ...\}\right)$
$\Rightarrow$ dijagonalni podniz $x_{00}, x_{11}, x_{22}, ...$ je podniz originalnog niza $(x_k)_k$ i očito konvergira prema $...b_3b_2b_1b_0$
Kako je niz $(x_k)_k$ bio proizvoljan, zaključujemo da svaki niz u $\mathbb{Z}_p$ ima podniz koji konvergira prema nekom elementu iz $\mathbb{Z}_p$.
$\Rightarrow$ $\mathbb{Z}_p$ je uistinu sekvencijalno kompaktan □

U metričkom je prostoru svojstvo sekvencijalne kompaktnosti ekvivalentno svojstvu kompaktnosti: skup je **kompaktan** ako svaki njegov otvoreni pokrivač ima konačan potpokrivač. Prisjetimo se, **pokrivač** skupa X je $\mathcal{U} = \{U_\alpha : (\alpha \in I)\}$ za kojeg vrijedi:

$$X \subseteq \bigcup_{\alpha \in I} U_\alpha,$$

Pokrivač $\mathcal{U}$ je otvoren (odnosno konačan) ako je svaki U_α otvoren (odnosno konačan).

Potpokrivač pokrivača $\mathcal{U}$ skupa X je $\mathcal{V} = \{U_\alpha : (\alpha \in J)\}$ za kojeg vrijedi:

$$(J \subseteq I), \quad X \subseteq \bigcup_{\alpha \in J} U_\alpha \subseteq \bigcup_{\alpha \in I} U_\alpha.$$

Lema 2.3.4. *Skup $\mathbb{Z}_p$ je kompaktan.*

Dokaz.
Znamo da je $\mathbb{Z}_p$ metrički prostor, da je kod metričkog prostora "biti sekvencijalno kompakatan" ekvivalentno s "biti kompaktan", te iz propozicije 2.3.3 znamo da je $\mathbb{Z}_p$ sekvencijalno kompaktan. Iz navedenih činjenica slijedi tvrdnja leme. □

Lema 2.3.5. *Svaka otvorena kugla $a + (p^N) = K(a, p^{-N})$ u $\mathbb{Q}_p$ može se prikazati kao disjunktna unija p otvorenih kugala radijusa $p^{-(N+1)}$.*

Dokaz.
$a + (p^N) = \left\{(x \in \mathbb{Q}_p) : |x - a|_p < p^{-N}\right\} = K(a, p^{-N})$
Vrijedi:

$$\begin{aligned} x \in a + (p^N) &\Leftrightarrow |x - a|_p < p^{-N} \\ &\Leftrightarrow \frac{1}{p^{ord_p(x-a)}} < \frac{1}{p^N} \\ &\Leftrightarrow ord_p(x - a) > N \\ &\Leftrightarrow x - a = \underbrace{a_{N+1} \cdot p^{N+1} + a_{N+2} \cdot p^{N+2} + ...}_{\text{razlikujemo za } \; a_{N+1} = 0, 1, ..., p-1} \end{aligned}$$

Dakle:

$$\begin{aligned} a + (p^N) &= \bigsqcup_{b=0}^{p-1} \left\{(x \in \mathbb{Q}_p) : x - a = b \cdot p^{N+1} + a_{N+2} \cdot p^{N+2} + ...\right\} = \\ &= \bigsqcup_{b=0}^{p-1} \left\{(x \in \mathbb{Q}_p) : x - a - b \cdot p^{N+1} = a_{N+2} \cdot p^{N+2} + ...\right\} = \\ &= \bigsqcup_{b=0}^{p-1} \left\{(x \in \mathbb{Q}_p) : ord_p(x - a - b \cdot p^{N+1}) \geq N + 2 > N + 1\right\} = \\ &= \bigsqcup_{b=0}^{p-1} \left\{(x \in \mathbb{Q}_p) : \left|x - (a + b \cdot p^{N+1})\right|_p < \frac{1}{p^{N+1}}\right\} = \end{aligned}$$

$$= \bigsqcup_{b=0}^{p-1} K\left(a + b \cdot p^{N+1}, \frac{1}{p^{N+1}}\right) = \bigsqcup_{b=0}^{p-1} a + b \cdot p^{N+1} + (p^{N+1})$$

□

Napomena 2.3.6. *Specijalno, jednu otvorenu kuglu radijusa* p^{-M} *možemo prikazati kao disjunktnu uniju* p *otvorenih kugala radijusa* $p^{-(M+1)}$. *Zatim svaku od tih* p *otvorenih kugala radijusa* $p^{-(M+1)}$ *možemo prikazati kao disjunktnu uniju* p *otvorenih kugala radijusa* $p^{-(M+2)}$. *Nastavivši tako dalje, dobivamo da se* $(\forall N > M)$ *otvorena kugla radijusa* p^{-M} *može prikazati kao disjunktna unija* p^{N-M} *(tj. konačno mnogo) otvorenih kugala radijusa* p^{-N}.

Propozicija 2.3.7. *Svaka kugla u $\mathbb{Z}_p$ je kompaktan skup.*

Dokaz.
Neka je $K\left(a, p^{-N}\right)$ proizvoljna otvorena kugla u $\mathbb{Z}_p$.
Vrijedi: $K\left(a, p^{-N}\right) = \underbrace{\overline{K}\left(a, p^{-(N+1)}\right)}_{\text{zatvoren}} \subseteq \underbrace{\mathbb{Z}_p}_{\text{kompaktan}}$.
$\Rightarrow$ $\overline{K}\left(a, p^{-(N+1)}\right)$ je zatvoren podskup kompaktnog skupa pa je i sam kompaktan
$\Rightarrow \left[K\left(a, p^{-N}\right) = \overline{K}\left(a, p^{-(N+1)}\right)\right] \Rightarrow$ $K\left(a, p^{-N}\right)$ je kompaktan skup, a kako je to bila proizvoljna kugla, tvrdnja vrijedi
Za zatvorene kugle je dokaz analogan. □

Lema 2.3.8. *Ako se dvije kugle u $\mathbb{Q}_p$ sijeku, one su koncentrične. Specijalno, ako se sijeku dvije kugle istog radijusa, tada se one podudaraju.*

Dokaz.
Neka su $K(a, \epsilon_1)$ i $K(b, \epsilon_2)$ proizvoljne otvorene kugle u $\mathbb{Q}_p$ koje se sijeku.
$\Rightarrow$ $(\exists c \in K(a, \epsilon_1) \cap K(b, \epsilon_2))$
Kako je (prema primjeru 1.2.19) kod svake ne-Arhimedske norme (pa tako i p-adske) svaka točka svake kugle središte, slijedi da je: $K(a, \epsilon_1) = K(c, \epsilon_1)$, $K(b, \epsilon_2) = K(c, \epsilon_2)$.
Dakle, ako se dvije otvorene kugle u $\mathbb{Q}_p$ sijeku, one su koncentrične.
Za zatvorene kugle je dokaz posve analogan. □

Propozicija 2.3.9. *Vrijedi:*

$$\textit{otvoreni } (X \subseteq \mathbb{Z}_p) \textit{ je kompaktan } \Leftrightarrow X = \bigsqcup_{i=1,\ldots,n} K\left(a_i, p^{-N_{a_i}}\right) = \bigsqcup_{i=1,\ldots,n} a_i + (p^{N_{a_i}}).$$

Dokaz.
Neka je $(X \subseteq \mathbb{Z}_p)$ proizvoljan otvoreni skup.
$\Rightarrow$ X je unija otvorenih kugala, tj. $X = \bigcup_{a \in X} K\left(a, p^{-N_a}\right)$ $(*)$

Smjer $\Rightarrow$
Pretpostavljamo da je X kompaktan.
$\Rightarrow$ svaki otvoreni pokrivač od X ima konačan potpokrivač (1)

Iz $(*)$ slijedi da je $\left\{K\left(a, p^{-N_a}\right) : (a \in X)\right\}$ otvoreni pokrivač od X.

Zbog tvrdnje (1) on ima konačan potpokrivač, recimo: $X = \bigcup_{i=1}^{n} K\left(a_i, p^{-N_i}\right)$.
Dakle, X je konačna unija otvorenih otvorenih kugala. A mi želimo dobiti da je X konačna DISJUNKTNA unija otvorenih kugala.
Dokaz ide indukcijom po n (tj. po broju tih kugala):

$n = 1 \Rightarrow$ imamo samo jednu kuglu $\Rightarrow$ tvrdnja očito vrijedi

$n = 2 \Rightarrow X = K\left(a_1, p^{-N_1}\right) \cup K\left(a_2, p^{-N_2}\right)$

1. slučaj: $K\left(a_1, p^{-N_1}\right)$ i $K\left(a_2, p^{-N_2}\right)$ su disjunktne $\Rightarrow$ tvrdnja vrijedi

2. slučaj: $K\left(a_1, p^{-N_1}\right)$ i $K\left(a_2, p^{-N_2}\right)$ se sijeku $\Rightarrow$ $(\exists c)$ iz presjeka

Prema lemi 2.3.8, $K\left(a_1, p^{-N_1}\right) = K\left(c, p^{-N_1}\right)$, $K\left(a_2, p^{-N_2}\right) = K\left(c, p^{-N_2}\right)$.

$$\Rightarrow X = K\left(a_1, p^{-N_1}\right) \cup K\left(a_2, p^{-N_2}\right) = K\left(c, p^{-N_1}\right) \cup K\left(c, p^{-N_2}\right) = K\left(c, max\{p^{-N_1}, p^{-N_2}\}\right)$$

$\Rightarrow$ imamo samo jednu kuglu $\Rightarrow$ tvrdnja vrijedi

Pretpostavljamo da tvrdnja vrijedi ako X možemo pokriti s n kugala, za neki $(n \in \mathbb{N})$.

$n + 1 \Rightarrow X = \bigcup_{i=1}^{n+1} K\left(a_i, p^{-N_i}\right)$

Označimo: $X_1 := \bigcup_{i=1}^{n} K\left(a_i, p^{-N_i}\right)$.

Prema pretpostavci indukcije, X_1 se može prikazati kao konačna disjunktna unija kugala, tj. $(\exists c_1, ..., c_m)$ t.d. $X_1 = \bigsqcup_{i=1}^{m} K\left(c_i, p^{-M_i}\right)$.

Neka je p^{-N} dovoljno mali da vrijedi: $p^{-N} < p^{-M_1}, ..., p^{-M_m}, p^{-N_{n+1}}$.

Slijedi: $(N > M_i)$ $(\forall i \in \{1, ..., m\})$ i $(N > N_{n+1})$.

Sada iz napomene 2.3.6 slijedi: $K\left(c_i, p^{-M_i}\right) = \bigsqcup_{j} K\left(d_{ij}, p^{-N}\right)$ i

$K\left(a_{n+1}, p^{-N_{n+1}}\right) = \bigsqcup_{r} K\left(d_r, p^{-N}\right)$, pri čemu su to konačne (disjunktne) unije.

$$\Rightarrow X_1 = \bigsqcup_{i=1}^{m} K\left(c_i, p^{-M_i}\right) = \bigsqcup_{i=1}^{m} \bigsqcup_{j} K\left(d_{ij}, p^{-N}\right)$$

$\Rightarrow X_1$ je konačna disjunktna unija kugala jednakih radijusa

Sada gledamo što se dešava kad kugle $K\left(d_r, p^{-N}\right)$ dodajemo skupu X_1.

Ako je kugla $K\left(d_r, p^{-N}\right)$ disjunktna sa svakom kuglom $K\left(d_{ij}, p^{-N}\right)$, samo ju dodamo u uniju (tj. u skup X_1).
Ako kugla $K\left(d_r, p^{-N}\right)$ siječe neku kuglu $K\left(d_{ij}, p^{-N}\right)$, tada zbog specijalnog slučaja iz propozicije 2.3.8 vrijedi: $K\left(d_r, p^{-N}\right) = K\left(d_{ij}, p^{-N}\right)$ te tada ne dodajemo $K\left(d_r, p^{-N}\right)$ u uniju (jer se ona tamo već nalazi).
Postupak ponavljamo sve dok ne iscrpimo sve kugle iz $K\left(a_{n+1}, p^{-N_{n+1}}\right)$.

$$\Rightarrow \quad X = X_1 \cup K\left(a_{n+1}, p^{-N_{n+1}}\right) = \left(\bigsqcup_{i=1}^{m} \bigsqcup_{j} K\left(d_{ij}, p^{-N}\right)\right) \cup \left(\bigsqcup_{r} K\left(d_r, p^{-N}\right)\right) =$$

$$= \text{ [zbog gornjih komentara] } = \underbrace{\bigsqcup_{i=1}^{m} \bigsqcup_{j} K\left(d_{ij}, p^{-N}\right)}_{\text{konačna disjunktna unija}} \underbrace{\bigsqcup_{r'} K\left(d_{r'}, p^{-N}\right)}_{\substack{\text{konačna unija onih kugala} \\ \text{iz } K\left(a_{n+1}, p^{-N_{n+1}}\right) \\ \text{koje su disjunktne sa} \\ \text{svakom } K\left(d_{ij}, p^{-N}\right)}}$$

Vidimo da je sada X konačna disjunktna unija kugala pa tvrdnja vrijedi.

Smjer $\Leftarrow$

Pretpostavljamo da je $X = \bigsqcup_{i=1,\ldots,n} K\left(a_i, p^{-N_i}\right)$. Želimo pokazati da je X kompaktan.
Iz propozicije 2.3.7 slijedi da je svaka kugla $K\left(a_i, p^{-N_i}\right)$ kompaktna, a to nam je dovoljno jer onda za svaki otvoreni pokrivač $\mathcal{U} = \{U_\alpha : (\alpha \in I)\}$ od X vrijedi:

$$(\forall i = 1, \ldots, n) \ (\exists I_i \subseteq I) \text{ t.d. } \quad K\left(a_i, p^{-N_i}\right) \subseteq \bigcup_{\alpha \in I_i} U_\alpha$$

$\Rightarrow$ $\mathcal{U} = \{U_\alpha : (\alpha \in I_i)\}$ je otvoreni pokrivač od $K\left(a_i, p^{-N_i}\right)$, a kako je ta kugla kompaktna, on ima konačan potpokrivač, tj. $(\exists J_i \subseteq I_i)$ t.d. $K\left(a_i, p^{-N_i}\right) \subseteq \bigcup_{\alpha \in J_i} U_\alpha$

$$\Rightarrow \quad X = \bigsqcup_{i=1}^{n} K\left(a_i, p^{-N_i}\right) \subseteq \bigsqcup_{i=1}^{n} \left(\bigcup_{\alpha \in J_i} U_\alpha\right) \subseteq \bigcup_{\alpha \in I} U_\alpha$$

$\Rightarrow$ $\{U_\alpha : (\alpha \in J_i), (i = 1, \ldots, n)\}$ je konačan potpokrivač pokrivača $\{U_\alpha : (\alpha \in I)\}$ od X, a kako je taj pokrivač bio proizvoljan, slijedi da je X kompaktan

□

Lema 2.3.10. *Otvoren podskup od $\mathbb{Q}_p$ je kompaktan ako i samo ako se može prikazati kao konačna unija otvorenih kugala. Takvu specijalnu vrstu otvorenih skupova nazivamo* ***kompaktno-otvorenim*** *skupovima.*

Dokaz.
Smjer $\Rightarrow$ se pokaže posve isto kao i analogna tvrdnja u dokazu propozicije 2.3.9.

Smjer $\Leftarrow$:
Posve analogno kao i u propoziciji 2.3.9 se pokaže da, ako se neki otvoreni podskup od $\mathbb{Q}_p$ može prikazati kao konačna unija otvorenih kugala, onda se može prikazati i kao konačna disjunktna unija otvorenih kugala. Sada je, kao i u dokazu propozicije 2.3.9, dovoljno pokazati da je svaka otvorena kugla (ovaj put u $\mathbb{Q}_p$, a ne u $\mathbb{Z}_p$) kompaktna. A kako znamo da je svaki podskup metričkog prostora kompaktan ako i samo ako je sekvencijalno kompaktan, slijedi da je dovoljno pokazati da je svaka otvorena kugla u $\mathbb{Q}_p$ sekvencijalno kompaktna.
Neka je $K(a,r)$ proizvoljna otvorena kugla u $\mathbb{Q}_p$. To znači da je $(a \in \mathbb{Q}_p)$, $r = \frac{1}{p^N}$ za neki $(N \in \mathbb{Z})$.

1. slučaj: $N \geq 0$

Znamo da je $K(a,r)$ je nastala translacijom kugle $K(0,r)$ za a.

$\Rightarrow [N \geq 0] \Rightarrow \quad p^N \geq p^0 = 1 \;\Rightarrow\; r = \dfrac{1}{p^N} \leq 1$

$\Rightarrow \quad K(0,r) = \{(x \in \mathbb{Q}_p) : |x|_p = |x-0|_p < r \leq 1\} \;\Rightarrow\; K(0,r) \subseteq \mathbb{Z}_p$

$\Rightarrow [\mathbb{Z}_p$ sekvencijalno kompaktan$] \Rightarrow \quad K(0,r)$ sekvencijalno kompaktna

Neka je (x_n) proizvoljan niz iz $K(a,r)$.

Kako je $K(a,r)$ nastala translacijom od $K(0,r)$ za a, postoji neki niz $(x_{n'})$ iz $K(0,r)$ t.d. je $x_n = x_{n'} + a$. Budući da je $x_{n'}$ niz iz $K(0,r)$ koja je sekvencijalno kompaktna, on ima neki konvergentan podniz, iz čega slijedi da i (x_n) ima konvergentan podniz.

2. slučaj: $N < 0$

$\Rightarrow \quad p^N < p^0 = 1 \;\Rightarrow\; r = \frac{1}{p^N} > 1 \;\Rightarrow\; r = p^M$ za neki $(M > 0)$

Prvo ćemo pokazati da je $K(0,r)$ sekvencijalno kompaktna.

Neka je (y_n) proizvoljan niz iz $K(0,r)$. $\Rightarrow \; |y_n|_p < r = p^M$

Definiramo: $(y_{n'}) \coloneqq (p^M \cdot y_n)$.

$\Rightarrow \quad |y_{n'}|_p = \left|p^M\right|_p \cdot |y_n|_p = \dfrac{|y_n|_p}{p^M} < \dfrac{p^M}{p^M} = 1 \;\Rightarrow\; y_{n'} \in K(0,1)$, a znamo:

$K(0,1) \subseteq \mathbb{Z}_p \;\Rightarrow\; K(0,1)$ sekvencijalno kompaktna.

$\Rightarrow$ $(y_{n'})$ ima neki konvergentan podniz
$\Rightarrow$ (y_n) ima neki konvergentan podniz, a kako je to bio proizvoljan niz iz $K(0,r)$, slijedi da je $K(0,r)$ uistinu sekvencijalno kompaktna.

Znamo da svaki niz (x_n) iz $K(a,r)$ ima opći član oblika: $x_n = x_{n'} + a$, gdje je $(x_{n'})$ neki niz iz $K(0,r)$, a upravo smo pokazali da $(x_{n'})$ ima konvergentan podniz, pa zaključujemo da i svaki niz (x_n) iz $K(a,r)$ ima konvergentan podniz, to jest da je $K(a,r)$ sekvencijalno kompaktna. Time je dokaz gotov.

□

Definicija 2.3.11. *Neka su* X *i* Y *dva topološka prostora. Za funkciju* $f : X \to Y$ *kažemo da je* ***lokalno konstantna*** *ako svaka točka njene domene ima neku okolinu* $(U \subseteq X)$ *takvu da je* $f(U) \in Y$ *konstanta.*

Propozicija 2.3.12. *Svaka lokalno konstantna funkcija je ujedno i neprekidna.*

Dokaz.
Neka su X i Y dva topološka prostora. Funkcija $f : X \to Y$ je neprekidna u točki $(x \in X)$ ako za svaku okolinu V točke $f(x)$ postoji neka okolina U točke x t.d. $(f(U) \subseteq V)$.
Mi pretpostavljamo da je naša promatrana funkcija f lokalno konstantna, te možemo označiti: $f(X) = \{c_1, c_2, c_3, ...\}$.
Neka je $(x \in X)$ proizvoljan. Znamo da $(\exists i)$ t.d. $f(x) = c_i$. Za svaku okolinu V točke $f(x) = c_i$ postoji okolina $U := f^{-1}(\{c_i\})$ točke x (prema definiciji lokalne konstantnosti) za koju vrijedi: $f(U) = f(x) = c_i \subseteq V$, pa vidimo da je funkcija f neprekidna u točki x, a kako je točka x bila proizvoljna, slijedi da je f neprekidna u svakoj točki pa tvrdnja vrijedi. □

Kod nas će promatrani skup X biti kompaktno-otvoren podskup od $\mathbb{Q}_p$ (najčešće $\mathbb{Z}_p$ ili $\mathbb{Z}_p^x$), pa će imati mnogo netrivijalnih lokalno konstantnih funkcija (to su one lokalno konstantne funkcije koje nisu konstantne). Štoviše, funkcija $f : X \to \mathbb{Q}_p$ je lokalno konstantna točno onda kada se može prikazati kao linearna kombinacija karakterističnih funkcija kompaktno-otvorenih skupova, što ćemo dokazati u sljedećoj propoziciji.

Propozicija 2.3.13. *Neka je* $(X \subseteq \mathbb{Q}_p)$ *kompaktno-otvoren te neka je zadana funkcija* $f : X \to \mathbb{Q}_p$. *Tada vrijedi:*
f *je lokalno konstantna* $\Leftrightarrow$ $f = \alpha_1 \cdot f_1 + ... + \alpha_n \cdot f_n$ *za neke* $(n \in \mathbb{N})$, $(\alpha_i \in \mathbb{Q}_p)$, $(U_i \subseteq X)$ *kompaktno-otvoren,* $f_i = \chi_{U_i}$.

Dokaz.
Smjer $\Leftarrow$
Pretpostavljamo da je $f = \alpha_1 \cdot f_1 + ... + \alpha_n \cdot f_n$ za neke $(n \in \mathbb{N})$, $(U_i \subseteq X)$ kompaktno-otvoren, $(\alpha_i \in \mathbb{Q}_p)$, $f_i = \chi_{U_i}$.
Neka je $(x \in X)$ proizvoljan. Želimo pokazati da postoji okolina U točke x t.d. $f(U) = konst$.

1. slučaj: $(\exists K \subseteq \{1, ..., n\})$ t.d. je $(x \in U_i)(\forall i \in K)$ i $(x \notin U_i)(\forall i \notin K)$

Znamo da je svaki U_i otvoren skup pa je on neka unija otvorenih kugala.

$\Rightarrow$ $(\forall i \in K)$ postoji neka otvorena kugla $(K(a_i, r_i) \subseteq U_i)$ t.d. $(x \in K(a_i, r_i))$

$\Rightarrow$ kugle $K(a_i, r_i)$ se sijeku u točki x $(\forall i \in K)$ pa su prema lemi 2.3.8 koncentrične i vrijedi: $K(a_i, r_i) = K(x, r_i)$

$\Rightarrow$ $U := K\left(x, \min_{i \in K}\{r_i\}\right)$ je okolina točke x za koju vrijedi:

$$f(U) = \{f(y) : (y \in U)\} = \left\{ \sum_{i \in K} \alpha_i \cdot 1 : (y \in U) \right\} = \sum_{i \in K} \alpha_i = konst.$$

$\Rightarrow$ kako je točka domene bila proizvoljna, slijedi da je f je lokalno konstantna

2. slučaj: $(x \notin U_i)(\forall i = 1, ..., n)$

Svaki U_i je kompaktno-otvoren, što znači da se može prikazati kao konačna unija otvorenih kugala, a znamo da je svaka otvorena kugla također i zatvorena, te da je konačna unija zatvorenih skupova zatvoren skup. Dakle, svaki U_i je zatvoren, pa je i $\bigcup_{i=1}^{n} U_i$ također zatvoren.

$\Rightarrow$ $U := X \setminus \left(\bigcup_{i=1}^{n} U_i \right)$ je otvoren skup pa je unija kugala, a znamo da je $(x \in U)$

$\Rightarrow$ postoji neka kugla $(K(a, r) \subseteq U)$ t.d. $x \in K(a, r)$

$\Rightarrow$ U je okolina točke x za koju vrijedi: $(y \in U) \Rightarrow f(y) = 0 = konst.$

Smjer $\Rightarrow$

Pretpostavljamo da je f lokalno konstantna. Želimo pokazati da se ona može prikazati kao linearna kombinacija karakterističnih funkcija kompaktno-otvorenih skupova.
Označimo: $C = f(X) = \{c_1, c_2, ...\}$.
Kako je f lokalno konstantna te $f : X \to f(X) = C$ surjekcija (ali nije injekcija jer je lokalno konstantna), vrijedi da su skupovi $U_i := f^{-1}(\{c_i\}) \subseteq X$ otvoreni (jer su to okoline iz definicije lokalno konstantne funkcije) i međusobno su disjunktni i vrijedi: $X = \bigsqcup_i U_i$
$\Rightarrow$ $\{U_1, U_2, ...\}$ je otvoreni disjunktni pokrivač od X, pa zbog kompaktnosti od X on ima konačan
potpokrivač što znači da postoji neki konačan $(I \subseteq \{1, 2, 3, ...\})$ takav da:

$$X \subseteq \bigsqcup_{i\in I} U_i \subseteq \bigsqcup_{i} U_i \subseteq X \quad \Rightarrow \quad X = \bigsqcup_{i\in I} U_i = \bigsqcup_{i} U_i = X \quad \Rightarrow \quad \bigsqcup_{i\in I} U_i = \bigsqcup_{i} U_i$$

$\Rightarrow$ $C = f(X)$ je konačan skup; označimo mu kardinaltet s n
$\Rightarrow$ $\{U_1, ..., U_n\}$ je konačni otvoreni disjunktni pokrivač od X
$\Rightarrow$ $f = c_1 \cdot f_1 + ... + c_n \cdot f_n$ uz: $f_i = \chi_{U_i}$, U_i otvoren
Preostaje još samo pokazati da su skupovi U_i kompaktni.
Iz propozicije 2.3.12 slijedi da je funkcija $f : X \to \mathbb{Q}_p$ neprekidna, a znamo da je $\mathbb{Q}_p$ metrički prostor, pa je skup $\left(\{c_i\} \subseteq \mathbb{Q}_p\right)$ zatvoren, što povlači da je i skup $U_i = f^{-1}(\{c_i\})$ zatvoren (jer znamo da je praslika zatvorenog skupa po neprekidnoj funkciji zatvoren skup). Vrijedi:
$U_i \subseteq X$ $\Rightarrow$[zatvoreni podskup kompaktnog skupa je kompaktan]$\Rightarrow$ U_i je kompaktan $\square$

Neka je od sada pa nadalje X kompaktno-otvoren podskup od $\mathbb{Q}_p$, primjerice $\mathbb{Z}_p$ ili $\mathbb{Z}_p^\times$.

Definicija 2.3.14. ***p-adska distribucija*** *μ na X je $\mathbb{Q}_p$-linearan homomorfizam vektorskih prostora s $\mathbb{Q}_p$-vektorskog prostora lokalno konstantnih funkcija na X na $\mathbb{Q}_p$. Ako je $f : X \to \mathbb{Q}_p$ lokalno konstantna, pisat ćemo $\int f\,\mu$ umjesto $\mu(f)$ za vrijednost od μ u f.*

Ekvivalentna definicija kaže da je p-adska distribucija μ na X aditivno preslikavanje sa skupa kompaktno-otvorenih skupova u $\mathbb{Q}_p$ na $\mathbb{Q}_p$. To znači da, ako je $(U \subset X)$ disjunktna unija kompaktno-otvorenih skupova $U_1, ..., U_n$, onda vrijedi:
$\mu(U) = \mu(U_1) + ... + \mu(U_n)$.
Pod "ekvivalentne definicije" mislimo na to da se svaki μ definiran na drugi način može

na jedinstven način "proširiti" do μ-a definiranog na prvi način, i svaki se μ definiran na prvi način može na jedinstven način "restringirati" do μ-a definiranog na drugi način. Preciznije, ako imamo distribuciju μ definiranu na prvi način, za svaki kompaktno-otvoren skup U na sljedeći način možemo dobiti distribuciju definiranu na drugi način (koju ćemo također označavati sa μ):

$$\mu(U) = \int (\text{karakteristična funkcija od } U)\, \mu$$

Ako imamo distribuciju μ definiranu na drugi način, za svaki kompaktno-otvoren skup U možemo dobiti distribuciju definiranu na prvi način (koju ćemo također označavati sa μ) tako da prvo stavimo:

$$\int (\text{karakteristična funkcija od } U)\, \mu = \mu(U),$$

te potom definiramo $\int f\,\mu$ za lokalno konstantnu funkciju f tako da f zapišemo kao linearnu kombinaciju karakterističnih funkcija:

$$\text{"}\mu(f)\text{"} = \int (f)\,\mu = [f \text{ lokalno konstantna}] = \int (\alpha_1 \cdot \chi_{U_1} + ... + \alpha_n \cdot \chi_{U_n})\,\mu =$$
$$= \alpha_1 \cdot \int (\chi_{U_1})\,\mu + ... + \alpha_n \cdot \int (\chi_{U_n})\,\mu = \alpha_1 \cdot \mu(U_1) + ... + \alpha_n \cdot \mu(U_n)$$

Propozicija 2.3.15. *Svako preslikavanje μ sa skupa svih otvorenih kugli sadržanih u X u skup $\mathbb{Q}_p$ za koje vrijedi:*

$$a + (p^N) \subset X \quad \Rightarrow \quad \mu\left(a + (p^N)\right) = \sum_{b=0}^{p-1} \mu\left(a + bp^N + (p^{N+1})\right)$$

može se na jedinstven način proširiti do p-adske distribucije na X.

Dokaz ove propozicije može se naći na 32. stranici literature **[Koblitz]**.

Navodimo neke primjere p-adskih distribucija:

(1) **Haarova distribucija** μ_{Haar} dana je s:

$$\mu_{Haar}\left(a + (p^N)\right) := \frac{1}{p^N}.$$

μ_{Haar} se može proširiti do distribucije na $\mathbb{Z}_p$ primjenom propozicije 2.3.15 zbog:

$$\sum_{b=0}^{p-1} \mu_{Haar}\left(a + bp^N + (p^{N+1})\right) = \sum_{b=0}^{p-1} \frac{1}{p^{N+1}} = \underbrace{\frac{1}{p^{N+1}} + ... + \frac{1}{p^{N+1}}}_{\text{p puta}} = p \cdot \frac{1}{p^{N+1}} =$$

$$= \frac{1}{p^N} = \mu_{Haar}\left(a + (p^N)\right)$$

(2) **Diracova distribucija** μ_α koncentrirana u fiksiranoj točki $(\alpha \in \mathbb{Z}_p)$ dana je s:

$$\mu_\alpha(U) := \begin{cases} 1, & (\alpha \in U) \\ 0, & \text{inače} \end{cases}$$

(3) **Mazurova distribucija** μ_{Mazur} je, uz pretpostavku bez smanjenja općenitosti da se pri pisanju $a + (p^N)$ uzima: $(a \in \mathbb{Z}), (0 \leq a \leq p^N - 1),$ dana s:

$$\mu_{Mazur}\left(a + (p^N)\right) := \frac{a}{p^N} - \frac{1}{2}$$

2.4 Bernoullijeve distribucije

Započet ćemo definiranjem **Bernoullijevih polinoma** $B_k(x)$ kao $k!$ pomnoženo s koeficijentom (to je zapravo polinom) koji se nalazi uz t^k u Taylorov razvoju u red sljedeće funkcije dviju varijabli:

$$F(t,x) := \frac{t \cdot \mathrm{e}^{xt}}{\mathrm{e}^t - 1} = \frac{t}{\mathrm{e}^t - 1} \cdot \mathrm{e}^{xt} = \left(\sum_{k=0}^{\infty} B_k \cdot \frac{t^k}{k!}\right) \cdot \left(\sum_{k=0}^{\infty} \frac{(xt)^k}{k!}\right) = \sum_{k=0}^{\infty} B_k(x) \cdot \frac{t^k}{k!}$$

Prvih nekoliko Bernoullijevih polinoma: $B_0(x) = 1,\ B_1(x) = x - \frac{1}{2}, B_2(x) = x^2 - x + \frac{1}{6}.$

Pretpostavljat ćemo da kod $a + (p^N)$ vrijedi: $0 \leq a \leq p^N - 1$.

Fiksirajmo sada neki $(k \in \mathbb{N}_0)$ i definirajmo preslikavanje $\mu_{B,k}$ na intervalima $a + (p^N)$ na sljedeći način:

$$\mu_{B,k}\left(a + (p^N)\right) := p^{N(k-1)} \cdot B_k\left(\frac{a}{p^N}\right)$$

Propozicija 2.4.1. *$\mu_{B,k}$ se može proširiti do distribucije (**k-ta Bernoullijeva distribucija**) na $\mathbb{Z}_p$.*

Dokaz.
Prema propoziciji 2.3.15, dovoljno je pokazati:

$$\mu_{B,k}\left(a + (p^N)\right) = \sum_{b=0}^{p-1} \mu_{B,k}\left(a + bp^N + (p^{N+1})\right).$$

Znamo da vrijedi:

$$\begin{aligned}
&\mu_{B,k}\left(a + (p^N)\right) = \sum_{b=0}^{p-1} \mu_{B,k}\left(a + bp^N + (p^{N+1})\right) \quad \Leftrightarrow \\
&\Leftrightarrow \quad \left[\text{zbog:} \quad \mu_{B,k}\left(a + (p^N)\right) = p^{N(k-1)} \cdot B_k\left(\frac{a}{p^N}\right)\right] \quad \Leftrightarrow \\
&\Leftrightarrow \quad p^{N(k-1)} \cdot B_k\left(\frac{a}{p^N}\right) = \sum_{b=0}^{p-1} \mu_{B,k}\left(a + bp^N + (p^{N+1})\right) \\
&\Leftrightarrow \quad B_k\left(\frac{a}{p^N}\right) = \frac{\sum_{b=0}^{p-1} \mu_{B,k}\left(a + bp^N + (p^{N+1})\right)}{p^{N(k-1)}} \\
&\Leftrightarrow \quad \left[\text{zbog:} \quad \mu_{B,k}\left(a + (p^N)\right) = p^{N(k-1)} \cdot B_k\left(\frac{a}{p^N}\right)\right] \\
&\Leftrightarrow \quad B_k\left(\frac{a}{p^N}\right) = \frac{\sum_{b=0}^{p-1} p^{(N+1)(k-1)} \cdot B_k\left(\frac{a+bp^N}{p^{N+1}}\right)}{p^{N(k-1)}} \\
&\Leftrightarrow \quad \left[\text{uz oznaku:} \quad \alpha = \frac{a}{p^{N+1}} \text{ je:} \quad B_k\left(\frac{a}{p^N}\right) = B_k\left(\alpha \cdot p\right)\right] \quad \Leftrightarrow
\end{aligned}$$

$$\Leftrightarrow \quad B_k(\alpha \cdot p) = \frac{\sum_{b=0}^{p-1} p^{(N+1)(k-1)} \cdot B_k\left(\frac{a+bp^N}{p^{N+1}}\right)}{p^{N(k-1)}} = p^{k-1} \cdot \sum_{b=0}^{p-1} B_k\left(\frac{a+bp^N}{p^{N+1}}\right) =$$

$$= p^{k-1} \cdot \sum_{b=0}^{p-1} B_k\left(\frac{a}{p^{N+1}} + \frac{b}{p}\right) = p^{k-1} \cdot \sum_{b=0}^{p-1} B_k\left(\alpha + \frac{b}{p}\right)$$

$$\Leftrightarrow \quad \left[\text{zbog:} \quad B_k(x) = (k!) \cdot \left(\text{koef. uz} \quad t^k \quad \text{iz} \quad \frac{t \cdot \mathrm{e}^{xt}}{\mathrm{e}^t - 1}\right), \ \text{ovdje uz:} \quad x = \alpha + \frac{b}{p}\right] \quad \Leftrightarrow$$

$$\Leftrightarrow \quad B_k(\alpha \cdot p) = p^{k-1} \cdot \sum_{b=0}^{p-1} (k!) \cdot \left(\text{koef. uz} \quad t^k \quad \text{iz} \quad \frac{t \cdot \mathrm{e}^{t\cdot\left(\alpha+\frac{b}{p}\right)}}{\mathrm{e}^t - 1}\right)$$

$$\Leftrightarrow \quad B_k(\alpha \cdot p) = (k!) \cdot \left(\text{koef. uz} \quad t^k \quad \text{iz} \quad p^{k-1} \cdot \sum_{b=0}^{p-1} \frac{t \cdot \mathrm{e}^{t\cdot\left(\alpha+\frac{b}{p}\right)}}{\mathrm{e}^t - 1}\right)$$

Zbog:

$$p^{k-1} \cdot \sum_{b=0}^{p-1} \frac{t \cdot \mathrm{e}^{t\cdot\left(\alpha+\frac{b}{p}\right)}}{\mathrm{e}^t - 1} = \frac{p^{k-1} \cdot t \cdot \mathrm{e}^{t\cdot\alpha}}{\mathrm{e}^t - 1} \cdot \sum_{b=0}^{p-1} \mathrm{e}^{\frac{bt}{p}} =$$

$$= \frac{p^{k-1} \cdot t \cdot \mathrm{e}^{t\cdot\alpha}}{\mathrm{e}^t - 1} \cdot \left(1 + \mathrm{e}^{\frac{t}{p}} + \mathrm{e}^{\frac{2t}{p}} + ... + \mathrm{e}^{\frac{(p-1)t}{p}}\right) =$$

$$= \left\{\text{uz} \quad x = \mathrm{e}^{\frac{t}{p}} \ \text{je:} \quad 1 + \mathrm{e}^{\frac{t}{p}} + ... + \mathrm{e}^{\frac{(p-1)t}{p}} = 1 + x + ... + x^{p-1} = \frac{x^{(p-1)+1} - 1}{x - 1} = \right.$$

$$\left. = \frac{x^p - 1}{x - 1} = \frac{\mathrm{e}^{p\cdot\frac{t}{p}} - 1}{\mathrm{e}^{\frac{t}{p}} - 1} = \frac{\mathrm{e}^t - 1}{\mathrm{e}^{\frac{t}{p}} - 1}\right\} =$$

$$= \frac{p^{k-1} \cdot t \cdot \mathrm{e}^{t\cdot\alpha}}{\mathrm{e}^t - 1} \cdot \frac{\mathrm{e}^t - 1}{\mathrm{e}^{\frac{t}{p}} - 1} = \frac{p^{k-1} \cdot t \cdot \mathrm{e}^{t\cdot\alpha}}{\mathrm{e}^{\frac{t}{p}} - 1} =$$

$$= \frac{\frac{p^k}{p} \cdot t \cdot \mathrm{e}^{t\cdot\alpha\cdot\frac{p}{p}}}{\mathrm{e}^{\frac{t}{p}} - 1} = \frac{p^k \cdot \frac{t}{p} \cdot \mathrm{e}^{(p\alpha)\cdot\frac{t}{p}}}{\mathrm{e}^{\frac{t}{p}} - 1} =$$

$$= \left[\text{uz oznake:} \quad T = \frac{t}{p}, \ X = p\alpha\right] = p^k \cdot \frac{T \cdot \mathrm{e}^{XT}}{\mathrm{e}^T - 1} =$$

$$= [\text{def. od} \quad B_j(x)] = p^k \cdot \sum_{j=0}^{\infty} B_j(X) \cdot \frac{T^j}{j!} =$$

$$= p^k \cdot \sum_{j=0}^{\infty} B_j(p\alpha) \cdot \frac{(t/p)^j}{j!}$$

tvrdnja propozicije vrijedi ako i samo ako:

$$B_k(\alpha \cdot p) = (k!) \cdot \left(\text{koef. uz } \; t^k \; \text{ iz } \; p^k \cdot \sum_{j=0}^{\infty} B_j(p\alpha) \cdot \frac{(t/p)^j}{j!} \right) =$$

$$= [j = k] = (k!) \cdot \left(p^k \cdot B_k(p\alpha) \cdot \frac{(1/p)^k}{k!} \right) =$$

$$= p^k \cdot B_k(p\alpha) \cdot \left(\frac{1}{p} \right)^k = B_k(p\alpha)$$

□

Primjenom formule:

$$\mu_{B,k}\left(a + (p^N)\right) = p^{N(k-1)} \cdot B_k\left(\frac{a}{p^N}\right)$$

za prvih nekoliko $B_k(x)$ dobivamo sljedeće interesantne rezultate:

$$\mu_{B,0}\left(a + (p^N)\right) = p^{N(-1)} \cdot B_0\left(\frac{a}{p^N}\right) = [B_0(x) = 1] = p^{-N} \quad \Rightarrow \quad \mu_{B,0} = \mu_{Haar}$$

$$\mu_{B,1}\left(a + (p^N)\right) = p^0 \cdot B_1\left(\frac{a}{p^N}\right) = B_1\left(\frac{a}{p^N}\right) = \left[B_1(x) = x - \frac{1}{2}\right] = \frac{a}{p^N} - \frac{1}{2} \quad \Rightarrow \quad \mu_{B,1} = \mu_{Mazur}$$

2.5 Mjere i integracija

Definicija 2.5.1. *Za p-adsku distribuciju μ na X kažemo da je to **mjera** ako su njene vrijednosti na kompaktno-otvorenim skupovima $(U \subset X)$ ograničene nekom konstantom $(B \in \mathbb{R})$, tj. ako vrijedi:*

$$|\mu(U)|_p \leq B \quad (\forall \text{ kompaktno-otvorene } \; U \subset X).$$

Diracova distribucija μ_α za fiksirani $(\alpha \in \mathbb{Z}_p)$ jest mjera, ali nijedna Bernoullijeva distribucija nije mjera.

Postoji standardna metoda (tzv. **"regularizacija"**) koja "pretvara" Bernoullijeve

distribucije u mjere. No prvo moramo uvesti notaciju.

Ako je μ distribucija i $(\alpha \in \mathbb{Q}_p)$, onda sa $\alpha\mu$ označavamo distribuciju čija je vrijednost na svakom kompaktno-otvorenom skupu U jednaka: $(\alpha\mu)(U) = \alpha \cdot \mu(U)$.
Ako je $(U \subset \mathbb{Q}_p)$ kompaktno-otvoren skup i $(\alpha \in \mathbb{Q}_p)$, $(\alpha \neq 0)$, onda uzimamo: $\alpha U \coloneqq \{\alpha x : (x \in U)\} \subseteq \mathbb{Q}_p$.

Lako se vidi da:

– zbroj dvaju distribucija (odn. mjera) je distribucija (odn. mjera) (2.2)
– produkt skalara i distribucije (odn. mjere) je distribucija (odn. mjera) (2.3)
– $(\alpha \in \mathbb{Z}_p^\times)$, μ je distribucija (odn. mjera) na $\mathbb{Z}_p \Rightarrow \mu'(U) \coloneqq \mu(\alpha U)$ je distribucija (odn. mjera) na $\mathbb{Z}_p$ (2.4)

Definicija 2.5.2. *Neka je* $(\alpha \in \mathbb{Z})$, $(\alpha \neq 1)$ *t.d.* $p \nmid \alpha$. ***Regularizirana Bernoullijeva distribucija*** *na* $\mathbb{Z}_p$ *(koju ćemo označavati s* $\mu_{B,k,\alpha}$ *ili, kraće,* $\mu_{k,\alpha}$*) definira se za kompaktno-otvoreni skup* U *kao:*

$$\mu_{k,\alpha}(U) \coloneqq \mu_{B,k}(U) - \frac{1}{\alpha^k} \cdot \mu_{B,k}(\alpha U).$$

Uskoro ćemo pokazati da je $\mu_{k,\alpha}$ mjera, ali za sad ćemo napomenuti da je svakako distribucija prema 2.3 i 2.4.

Propozicija 2.5.3. $(\forall \alpha \in \mathbb{Z}_p^x)$ *i* $(\forall$ *kompaktno-otvorene* $U)$ *vrijedi:*

$$\mu_{Haar}(U) = \mu_{Haar}(\alpha U).$$

Dokaz.
Kako je U kompaktno-otvoren, može se prikazati kao konačna disjunktna unija intervala, pa je zbog aditivnosti od μ_{Haar} dovoljno pokazati da tvrdnja vrijedi za svaki $U = a+(p^N)$.

Mi želimo izračunati $\mu_{Haar}(\alpha U)$, a μ_{Haar} znamo evaluirati samo za intervale.
$\Rightarrow$ želimo prikazati αU kao neki interval $b + (p^M)$ i to takav da vrijedi:

$$\frac{1}{p^M} = \mu_{Haar}(b + (p^M)) = \mu_{Haar}(\alpha U) = \mu_{Haar}(U) = \mu_{Haar}(a + (p^N)) = \frac{1}{p^N},$$

tj. da vrijedi: $M = N$, odnosno: $\alpha U = b + (p^N)$.

$\underline{\alpha U \subseteq b + (p^N)}$

Znamo da je: $\alpha U = \{\alpha x : (x \in U)\} = \left\{\alpha x : \left(x \in a + (p^N)\right)\right\} = \left\{\alpha x : |x - a|_p < \frac{1}{p^N}\right\}$.

$\Rightarrow$ za proizvoljni $(y \in \alpha U)$ $(\exists x)$ za kojeg je $|x - a|_p < \frac{1}{p^N}$ i $y = \alpha x$

Uzevši $b := \alpha a$ dobivamo: $|y - b|_p = |\alpha x - \alpha a|_p = \underbrace{|\alpha|_p}_{=1} \cdot |x - a|_p < \frac{1}{p^N}$

$\Rightarrow$ $y \in \alpha a + (p^N)$

Kako je $(y \in \alpha U)$ bio proizvoljan, tvrdnja vrijedi.

$\underline{b + (p^N) \subseteq \alpha U}$

Neka je $(y \in \alpha a + (p^N))$ proizvoljan. $\Rightarrow$ $|y - \alpha a|_p < \frac{1}{p^N}$

Kako je $|\alpha|_p = 1 \neq 0$, znamo da je $\alpha \neq 0$ pa možemo uzeti: $x := \frac{y}{\alpha}$. Sada vrijedi:

$$|x - a|_p = \left|\frac{y}{\alpha} - a\right|_p = \frac{|y - \alpha a|_p}{|\alpha|_p} < [|\alpha|_p = 1] < \frac{1}{p^N}$$

$\Rightarrow$ za y smo našli neki $(x \in a + (p^N) = U)$ t.d. je $y = \alpha x$

$\Rightarrow$ $(y \in \alpha U)$, a kako je y bio proizvoljan, tvrdnja vrijedi □

Lema 2.5.4. $\mu_{0,\alpha}(U) = 0 \quad (\forall U)$.

Dokaz.

$$\begin{aligned}
\mu_{0,\alpha}(U) &= \mu_{B,0}(U) - \frac{1}{\alpha^0} \cdot \mu_{B,0}(\alpha U) = \\
&= \mu_{B,0}(U) - \mu_{B,0}(\alpha U) = \\
&= \mu_{Haar}(U) - \mu_{Haar}(\alpha U) = \\
&= \mu_{Haar}(U) - \underbrace{\mu_{Haar}(U)}_{\text{prema prethodnoj propoziciji}} = \\
&= 0
\end{aligned}$$

□

Lema 2.5.5. *Vrijedi:*

$$\mu_{1,\alpha}\left(a + (p^N)\right) = \frac{1}{\alpha}\left\lfloor \frac{\alpha a}{p^N} \right\rfloor + \frac{(1/\alpha) - 1}{2}.$$

Dokaz ove leme može se naći na 36. stranici literature **[Koblitz]**.

Propozicija 2.5.6. *Za sve kompaktno-otvorene skupove* $(U \subset \mathbb{Z}_p)$ *vrijedi:*

$$\left|\mu_{1,\alpha}(U)\right|_p \leq 1$$

Dokaz.
Vrijedi:

$$\left|\frac{\frac{1}{\alpha}-1}{2}\right|_p = \frac{1}{|2|_p}\cdot\left|\frac{1}{\alpha}-1\right|_p$$

Ako je $(p \neq 2)$, onda je: $\frac{1}{|2|_p} = \frac{1}{1} = 1 \leq 1$, pa vrijedi:

$$\left|\frac{\frac{1}{\alpha}-1}{2}\right|_p = \underbrace{\frac{1}{|2|_p}}_{\leq 1}\cdot\left|\frac{1}{\alpha}-1\right|_p =$$

$$\leq max\left\{\frac{1}{|\alpha|_p}, |1|_p\right\} = max\left\{\frac{1}{|\alpha|_p}, 1\right\} =$$

$$= \left[|\alpha|_p = 1\right] = max\{1,1\} = 1$$

Ako je $(p = 2)$, onda:

Pretpostavka ove sekcije je bila da $p \nmid \alpha$, pa onda $2 \nmid \alpha$.

$\Rightarrow\ 2 \nmid \frac{1}{\alpha}\ \Rightarrow\ \frac{1}{\alpha} \equiv 1 (\text{mod } 2) \Rightarrow\ \frac{1}{\alpha} - 1 \equiv 0 (\text{mod } 2)$

$\Rightarrow\ \frac{1}{\alpha} - 1 = 2a$ za neki a koji može, ali ne mora biti djeljiv s 2

$\Rightarrow\ \frac{\frac{1}{\alpha}-1}{2} = \frac{2a}{2} = a\ \Rightarrow\ \left|\frac{\frac{1}{\alpha}-1}{2}\right|_p = \left|\frac{\frac{1}{\alpha}-1}{2}\right|_2 = \frac{1}{2^{\text{nešto } \geq 0}} \leq \frac{1}{2^0} = \frac{1}{1} = 1$

Dakle, u svakom slučaju je $\left(\frac{\frac{1}{\alpha}-1}{2} \in \mathbb{Z}_p\right)$.
A znamo da prema lemi 2.5.5 vrijedi:

$$\mu_{1,\alpha}\left(a + (p^N)\right) = \frac{1}{\alpha}\left\lfloor\frac{\alpha a}{p^N}\right\rfloor + \frac{(1/\alpha)-1}{2},$$

pa imamo:

$$\mu_{1,\alpha}\left(a + (p^N)\right) = \underbrace{\underbrace{\frac{1}{\alpha}}_{\in \mathbb{Z}_p}\cdot\underbrace{\left\lfloor\frac{\alpha a}{p^N}\right\rfloor}_{\in \mathbb{Z}} + \underbrace{\frac{(1/\alpha)-1}{2}}_{\in \mathbb{Z}_p}}_{\in \mathbb{Z}_p}$$

$$\Rightarrow \quad \mu_{1,\alpha}\left(a+(p^N)\right) \in \mathbb{Z}_p \quad \Rightarrow \quad \left|\mu_{1,\alpha}\left(a+(p^N)\right)\right|_p \leq 1 \tag{2.5}$$

Kako se svaki kompaktno-otvoren skup U može prikazati kao konačna disjunktna unija intervala I_i, slijedi:

$$\begin{aligned}
\left|\mu_{1,\alpha}(U)\right|_p &= \left|\mu_{1,\alpha}\left(\bigsqcup_i I_i\right)\right|_p = \\
&= [\text{distribucija je aditivna funkcija}] = \left|\sum_i \mu_{1,\alpha}(I_i)\right|_p = \\
&\leq max\left\{\left|\mu_{1,\alpha}(I_i)\right|_p\right\} \leq [\ 2.5] \leq 1
\end{aligned}$$

□

Dakle, vrijednosti od $\mu_{1,\alpha}$ na kompaktno-otvorenim skupovima su ograničene nekom konstantom (konstantom 1), pa je ona mjera.

Lema 2.5.7. *Vrijedi:*

$$B_k(x) = \sum_{i=0}^{k} \binom{k}{i} \cdot B_i \cdot x^{k-i}.$$

Specijalno, $B_k(0) = B_k$.

Dokaz.

$$\begin{aligned}
\frac{t\cdot \mathrm{e}^{xt}}{\mathrm{e}^t-1} &= \left(\sum_{k=0}^{\infty}\frac{B_k}{k!}\cdot t^k\right)\cdot\left(\sum_{k=0}^{\infty}\frac{x^k}{k!}\cdot t^k\right) = \\
&= \left[\left(\sum_{k=0}^{\infty} a_k\cdot t^k\right)\cdot\left(\sum_{k=0}^{\infty} b_k\cdot t^k\right) = \sum_{k=0}^{\infty} c_k\cdot t^k, \text{ pri čemu je: } c_k = \sum_{i=0}^{k} a_i\cdot b_{k-i}\right] = \\
&= \sum_{k=0}^{\infty}\left(\sum_{i=0}^{k}\frac{B_i}{i!}\cdot\frac{x^{k-i}}{(k-i)!}\right)\cdot t^k
\end{aligned}$$

$$\begin{aligned}
\Rightarrow \quad B_k(x) &= (k!)\cdot\left(\text{koeficijent uz } t^k \text{ u } \frac{t\cdot \mathrm{e}^{xt}}{\mathrm{e}^t-1}\right) = (k!)\cdot\left(\sum_{i=0}^{k}\frac{B_i}{i!}\cdot\frac{x^{k-i}}{(k-i)!}\right) = \\
&= \left[\binom{k}{i} = \frac{k!}{(i!)\cdot(k-i)!}\right] = \sum_{i=0}^{k}\binom{k}{i}\cdot B_i\cdot x^{k-i}
\end{aligned}$$

Time je prva tvrdnja dokazana.

Slijedi druga tvrdnja:

$$B_k(0) = [\text{def.}] = (k!) \cdot \left(\text{koeficijent uz } \; t^k \; \text{ u } \; \frac{t \cdot \mathrm{e}^0}{\mathrm{e}^t - 1} = \frac{t}{\mathrm{e}^t - 1} \right) =$$

$$= (k!) \cdot \left(\text{koeficijent uz } \; t^k \; \text{ u } \; \sum_{k=0}^{\infty} \frac{B_k}{k!} \cdot t^k \right) =$$

$$= (k!) \cdot \frac{B_k}{k!} = B_k$$

□

Navodimo jednu važnu kongruenciju koja povezuje $\mu_{k,\alpha}$ i $\mu_{1,\alpha}$.

Teorem 2.5.8. *Neka je* d_k *najmanji zajednički nazivnik koeficijenata iz polinoma* $B_k(x)$, *tj.* $d_1 = 2$, $d_2 = 6$, $d_3 = 2$, *i tako dalje.*
Tada vrijedi:

$$d_k \mu_{k,\alpha}\left(a + (p^N)\right) \equiv d_k k a^{k-1} \mu_{1,\alpha}\left(a + (p^N)\right) \; (mod \;\; p^N)$$

Dokaz ovog teorema može se naći na stranicama 37-38 literature **[Koblitz]**.

Korolar 2.5.9. $\mu_{k,\alpha}$ *je mjera* $(\forall k = 1, 2, 3, ..)\ (\forall \alpha \in \mathbb{Z})\ (\alpha \notin p \cdot \mathbb{Z})\ (\alpha \neq 1)$.

Dokaz.

Zapravo želimo pokazati da je $\mu_{k,\alpha}\left(a + (p^N)\right)$ ograničeno nekom konstantom.

Označimo: $A := \mu_{k,\alpha}\left(a + (p^N)\right)$, $B := k \cdot a^{k-1} \mu_{1,\alpha}\left(a + (p^N)\right)$.

TM 2.5.8 nam daje: $d_k \cdot A \equiv d_k \cdot B \pmod{p^N} \;\Rightarrow\; d_k \cdot A = d_k \cdot B + p^N \cdot w, \;\; (w \in \mathbb{Z}_p)$

$\Rightarrow \; |d_k \cdot A|_p = \left| d_k \cdot B + p^N \cdot w \right|_p$

$$\Rightarrow \; |A|_p = \left| B + \frac{p^N \cdot w}{d_k} \right|_p \leq max\left\{ |B|_p, \left| \frac{p^N \cdot w}{d_k} \right|_p \right\} =$$

$$= \left\{ \left| \frac{p^N \cdot w}{d_k} \right|_p = \frac{1}{p^{ord_p\left(p^N \cdot w\right) - ord_p(d_k)}} \leq \frac{1}{p^{N - ord_p(d_k)}} = \frac{1}{p^{ord_p(p^N) - ord_p(d_k)}} = \left| \frac{p^N}{d_k} \right|_p \right\} =$$

$$\leq max\left\{ |B|_p, \left| \frac{p^N}{d_k} \right|_p \right\}$$

$$\Rightarrow \left|\mu_{k,\alpha}\left(a+(p^N)\right)\right|_p \leq max\left\{ \ |B|_p, \left|\frac{p^N}{d_k}\right|_p \right\} = max\left\{ \left|k\cdot a^{k-1}\cdot \mu_{1,\alpha}\left(a+(p^N)\right)\right|_p, \ \left|\frac{p^N}{d_k}\right|_p \ \right\} =$$

$$= \left\{ \ \left|\frac{p^N}{d_k}\right|_p = \frac{1}{p^N\cdot |d_k|_p} \leq \frac{1}{|d_k|_p} \ \right\} =$$

$$= \left\{ \ (k\cdot a^{k-1}\in \mathbb{Z}_p) \ \Rightarrow \ \left|k\cdot a^{k-1}\right|_p \leq 1 \ \right\} =$$

$$\leq max\left\{ \underbrace{\left|\mu_{1,\alpha}\left(a+(p^N)\right)\right|_p}_{\leq 1}, \ \left|\frac{1}{d_k}\right|_p \right\} =$$

$$\left\{ \ ord_p(d_k)\geq 0 \ \Rightarrow \ -ord_p(d_k)\leq 0 \ \Rightarrow \ p^{-ord_p(d_k)}\leq 1 \ \Rightarrow \ \right\}$$

$$\left\{ \ \Rightarrow \ \left|\frac{1}{d_k}\right|_p = \frac{1}{p^{ord_p(1)-ord_p(d_k)}} = \frac{1}{p^{-ord_p(d_k)}} \geq 1 \ \right\}$$

$$\left\{ \ \Rightarrow \ max\left\{ \left|\mu_{1,\alpha}\left(a+(p^N)\right)\right|_p, \ \left|\frac{1}{d_k}\right|_p \right\} = \left|\frac{1}{d_k}\right|_p \geq 1 \ \right\}$$

$$= \left|\frac{1}{d_k}\right|_p, \ \text{što je konstanta jer je } \ d_k \ \text{ fiksiran}$$

□

Ali postavlja se pitanje čemu sve to - zašto smo morali modificirati (tj. "regularizirati") Bernoullijeve distribucije da dobijemo mjere? Odgovor je sljedeći: za distribuciju μ koja nije mjera (tj. nije ograničena) se po definiciji integral $\int f\,\mu$ definira za lokalno konstantne funkcije f, ali nailazimo na probleme kada pokušamo upotrijebiti limese Riemannovih suma kako bismo proširili integraciju na sve neprekidne funkcije f.

"Mjera" nije dobra i ne bismo je smjeli zvati mjerom ako ne možemo integrirati neprekidne funkcije s obzirom na nju.

U sljedećem teoremu ćemo pokazati da ograničene distribucije uistinu možemo s punim pravom zvati mjerom.

Prisjetimo se, X je kompaktno-otvoren podskup od $\mathbb{Q}_p$, primjerice $\mathbb{Z}_p$ ili $\mathbb{Z}_p^\times$ (radi jednostavnosti, uzmimo $X\subset\mathbb{Z}_p$).

Teorem 2.5.10. *Neka je* μ *p-adska mjera na* X *i* $f : X \to \mathbb{Q}_p$ *neprekidna funkcija. Tada Riemannove sume:*

$S_{N,\{x_{a,N}\}}(f) := \sum_{\substack{0\le a<p^N,\\ a+(p^N)\subset X}} f(x_{a,N})\cdot\mu\left(a+(p^N)\right)$, *pri čemu je* $(x_{a,N} \in a+(p^N))$ *proizvoljna točka kada* $N \to \infty$ *konvergiraju prema limesu* $(a \in \mathbb{Q}_p)$ *koji ne ovisi o odabiru točaka* $\{x_{a,N}\}$.

Dokaz.
Pretpostavimo da je $|\mu(U)|_p \le B$ za sve kompaktno-otvorene $(U \subset X)$.
Prvo ćemo za $(M > N)$ procijeniti $\left|S_{N,\{x_{a,N}\}} - S_{M,\{x_{a,M}\}}\right|_p$.

Prvo ćemo dokazati pomoćnu tvrdnju koja kaže da se $(\forall M > N)$ $S_{N,\{x_{a,N}\}}$ može zapisati kao:

$$S_{N,\{x_{a,N}\}} = \sum_{\substack{0\le a<p^M\\ a+(p^M)\subset X}} f(x_{\overline{a},N})\cdot\mu\left(a+(p^M)\right),$$

pri čemu je $\overline{a}$ najmanji nenegativni ostatak od a modulo p^N.
Radi jednostavnosti, uzet ćemo da je $M = N+1$. Sličan argument možemo upotrijebiti i za proizvoljan $M > N$ (samo ponovimo ovo nekoliko puta). Prema definiciji je:

$$S_{N,\{x_{a,N}\}} = \sum_{\substack{0\le a<p^N\\ a+(p^N)\subset X}} f(x_{a,N})\cdot\mu\left(a+(p^N)\right) \tag{2.6}$$

Također, znamo da vrijedi:

$$a+(p^N) = \bigsqcup_{j=0}^{p-1} a + j\cdot p^N + (p^{N+1}).$$

Zbog aditivnosti od μ je sada:

$$\mu\left(a+(p^N)\right) = \sum_{j=0}^{p-1}\mu\left(\underbrace{a+j\cdot p^N}_{=:\,a'_j}+(p^{N+1})\right) = \sum_{j=0}^{p-1}\mu\left(a'_j+(p^{N+1})\right) \tag{2.7}$$

Na primjer,

$$a = a_0 + a_1\cdot p + a_2\cdot p^2 + \ldots + a_{N-1}\cdot p^{N-1}$$
$$\Rightarrow\quad a'_j = a_0 + a_1\cdot p + a_2\cdot p^2 + \ldots + a_{N-1}\cdot p^{N-1} + j\cdot p^N$$

pa uz oznaku da je $\overline{b}$ ostatak pri dijeljenju broja b brojem p^N, imamo: $\overline{a'_j} = a$.

$$\Rightarrow\quad f\left(x_{\overline{a'_j},N}\right) = f(x_{a,N}) \tag{2.8}$$

Dobivamo:

$$S_{N,\{x_{a,N}\}} = [\text{zbog } 2.6] = \sum_{\substack{0\le a<p^N \\ a+(p^N)\subset X}} f(x_{a,N})\cdot\mu\left(a+(p^N)\right) =$$

$$= [\text{zbog } 2.7] = \sum_{\substack{0\le a<p^N \\ a+(p^N)\subset X}} f(x_{a,N})\cdot\left(\sum_{j=0}^{p-1}\mu\left(a'_j+(p^{N+1})\right)\right) =$$

$$= [\text{zbog } 2.8] = \sum_{\substack{0\le a<p^N \\ a+(p^N)\subset X}} \sum_{j=0}^{p-1} f\left(x_{\overline{a'_j},N}\right)\cdot\mu\left(a'_j+(p^{N+1})\right) =$$

$$= \sum_{j=0}^{p-1}\sum_{\substack{0\le a<p^N \\ a+(p^N)\subset X}} f\left(x_{\overline{a'_j},N}\right)\cdot\mu\left(a'_j+(p^{N+1})\right) =$$

$$= \left\{\begin{array}{l} \text{to je suma po svim } a'_j\text{-ovima (za sve } a\text{-ove t.d. } 0\le a<p^N \text{ i} \\ a+(p^N)\subset X\ ) \text{ i po svim } j\text{-ovima od 0 do } p-1, \text{ a svaki } a'_j \text{ je} \\ \text{oblika: } a'_j = \underbrace{a}_{<p^N} + \underbrace{j\cdot p^N}_{<p^{N+1}} < p^{N+1}, \text{ tj. za njega vrijedi: } 0\le a'_j<p^{N+1} \end{array}\right\} =$$

$$= \sum_{\substack{0\le A<p^{N+1} \\ A+(p^{N+1})\subset X}} f(x_{\overline{A},N})\cdot\mu\left(A+(p^{N+1})\right) = \sum_{\substack{0\le a<p^{N+1} \\ a+(p^{N+1})\subset X}} f(x_{\overline{a},N})\cdot\mu\left(a+(p^{N+1})\right)$$

Sada ćemo pretpostaviti da je N dovoljno velik da, čim je $x\equiv y\ (\text{mod}\ p^N)$, vrijedi: $|f(x)-f(y)|_p<\epsilon$. Naime, na kompaktnom skupu neprekidnost povlači uniformnu neprekidnost, a uniformna neprekidnost znači da, ako su x i y dovoljno blizu, onda su $f(x)$ i $f(y)$ proizvoljno blizu.
Sada:

$$\left|S_{N,\{x_{a,N}\}} - S_{M,\{x_{a,M}\}}\right|_p = \left|\sum_{\substack{0\le a<p^M \\ a+(p^M)\subset X}} \left[f(x_{\overline{a},N}) - f(x_{\overline{a},M})\right]\cdot\mu\left(a+(p^M)\right)\right|_p =$$

$$\le max\left\{\underbrace{\left|f(x_{\overline{a},N}) - f(x_{\overline{a},M})\right|_p}_{<\epsilon \text{ zbog } 2.9 \text{ (ispod)}}\cdot \underbrace{\left|\mu\left(a+(p^M)\right)\right|_p}_{\le B \text{ prema pretp.}}\right\} =$$

$$\le \epsilon\cdot B$$

$\Rightarrow$ niz Riemannovih suma $\left(S_{N,\{x_{a,N}\}}\right)_N$ je Cauchyjev, pa (kako je $\mathbb{Q}_p$ potpun prostor), taj niz ima limes
Taj je limes neovisan o $\{x_{a,N}\}$:

$$\left|S_{N,\{x_{a,N}\}} - S_{N,\{x'_{a,N}\}}\right|_p = \left|\sum_{\substack{0\le a<p^N \\ a+(p^N)\subset X}} \left[f(x_{a,N}) - f(x'_{a,N})\right]\cdot \mu\left(a+(p^N)\right)\right|_p =$$

$$\le \max_a \left\{ \underbrace{\left|f(x_{a,N}) - f(x'_{a,N})\right|_p}_{<\epsilon \text{ zbog 2.10 (ispod)}} \cdot \underbrace{\left|\mu\left(a+(p^N)\right)\right|_p}_{\le B \text{ prema pretp.}} \right\} =$$

$$\le \epsilon \cdot B$$

Za dokaz teorema nam preostaje dokazati korištene tvrdnje 2.9 i 2.10:

$$\left|x_{\overline{a},N} - x_{\overline{a},M}\right|_p = \left|x_{\overline{a},N} - \overline{a} + \overline{a} - x_{\overline{a},M}\right|_p =$$

$$\le max\left\{ \underbrace{\left|x_{\overline{a},N} - \overline{a}\right|_p}_{\le \frac{1}{p^N}}, \underbrace{\left|\overline{a} - x_{\overline{a},M}\right|_p}_{< \frac{1}{p^M} \le \frac{1}{p^N}} \right\} \le \frac{1}{p^N}$$

$$\Rightarrow \quad x_{\overline{a},N} \equiv x_{\overline{a},M} (\text{mod } \ p^N) \tag{2.9}$$

$$\left|x_{a,N} - x'_{a,N}\right|_p = \left|x_{a,N} - a + a - x'_{a,N}\right|_p =$$

$$\le max\left\{ \underbrace{\left|x_{a,N} - a\right|_p}_{< \frac{1}{p^N}}, \underbrace{\left|x'_{a,N} - a\right|_p}_{< \frac{1}{p^N}} \right\} < \frac{1}{p^N}$$

$$\Rightarrow \quad x_{a,N} \equiv x'_{a,N} (\text{mod } \ p^N) \tag{2.10}$$

□

Definicija 2.5.11. *Ako je $f : X \to \mathbb{Q}_p$ neprekidna funkcija i μ mjera na X,* ***integral*** *$\int f\,\mu$ definiramo kao limes niza Riemannovih suma. (U prethodnom je teoremu dokazano postojanje tog limesa.)*
Ako je f lokalno konstantna, tada se prijašnja i sadašnja definicija tog integrala podudaraju.

Direktno iz dane definicije slijede sljedeće tvrdnje:

Propozicija 2.5.12. *Ako je* $f : X \to \mathbb{Q}_p$ *neprekidna funkcija t.d.* $|f(x)|_p \leq A \quad (\forall x \in X)$ *i* $\mu(U) \leq B$ *za sve kompaktno-otvorene* $(U \subset X)$, *onda vrijedi:*

$$\left| \int f \, \mu \right|_p \leq A \cdot B$$

Korolar 2.5.13. *Ako su* $f, g : X \to \mathbb{Q}_p$ *neprekidne funkcije t.d.* $|f(x) - g(x)|_p \leq \epsilon$ $(\forall x \in X)$ *i* $\mu(U) \leq B$ *za sve kompaktno-otvorene* $(U \subset X)$, *onda vrijedi:*

$$\left| \int f \, \mu - \int g \, \mu \right|_p \leq \epsilon \cdot B$$

Drugim riječima, ako su dvije funkcije "blizu", blizu su i njihovi integrali.

Lema 2.5.14. *Vrijedi:*

$$\mu_{B,k}(\mathbb{Z}_p) = B_k.$$

Dokaz.

$$\begin{aligned}
\mu_{B,k}(\mathbb{Z}_p) &= \mu_{B,k}\left(0 + p^0 \cdot \mathbb{Z}_p\right) = \mu_{B,k}\left(0 + (p^0)\right) = \\
&= \left[\mu_{B,k}\left(a + (p^N)\right) = p^{N(k-1)} \cdot B_k\left(\frac{a}{p^N}\right), \text{ ovdje uz: } a = N = 0 \right] = \\
&= p^0 \cdot B_k\left(\frac{0}{p^0}\right) = B_k(0) = \\
&= [\text{prema lemi } 2.5.7] = B_k
\end{aligned}$$

□

Lema 2.5.15. *Vrijedi:*

$$\mu_{B,k}(p \cdot \mathbb{Z}_p) = p^{k-1} \cdot B_k.$$

Dokaz.

$$\begin{aligned}\mu_{B,k}(p\cdot\mathbb{Z}_p) &= \mu_{B,k}\left(0+p^1\cdot\mathbb{Z}_p\right) = \mu_{B,k}\left(0+(p^1)\right) = \\ &= \left[\mu_{B,k}\left(a+(p^N)\right) = p^{N(k-1)}\cdot B_k\left(\frac{a}{p^N}\right),\ \text{ovdje uz:}\ \ a=0, N=1\right] = \\ &= p^{k-1}\cdot B_k\left(\frac{0}{p^1}\right) = p^{k-1}\cdot B_k(0) = [\text{prema lemi } 2.5.7] = p^{k-1}\cdot B_k\end{aligned}$$

□

Lema 2.5.16. *Vrijedi:*

$$\mu_{B,k}(\mathbb{Z}_p^\times) = B_k\cdot\left(1-p^{k-1}\right).$$

Dokaz.

$$\begin{aligned}\text{Znamo:}\ \ \mathbb{Z}_p &= \left\{(x\in\mathbb{Q}_p) : |x|_p \le 1\right\} = \left\{(x\in\mathbb{Q}_p) : |x|_p \in \left\{0, 1, \frac{1}{p^n}(n\in\mathbb{N})\right\}\right\} \\ \mathbb{Z}_p^\times &= \left\{(x\in\mathbb{Q}_p) : |x|_p = 1\right\} = \left\{(x\in\mathbb{Q}_p) : |x|_p \in \{1\}\right\} \\ p\cdot\mathbb{Z}_p &= \left\{(x = p\cdot y\in\mathbb{Q}_p) : y\in\mathbb{Z}_p\right\} = \\ &= \left\{(x = p\cdot y\in\mathbb{Q}_p) : |x|_p = |p\cdot y|_p = |p|_p\cdot|y|_p \le |p|_p = \frac{1}{p}\right\} = \\ &= \left\{(x\in\mathbb{Q}_p) : |x|_p \le \frac{1}{p}\right\} = \left\{(x\in\mathbb{Q}_p) : |x|_p \in \left\{0, \frac{1}{p^n}(n\in\mathbb{N})\right\}\right\}\end{aligned}$$

Zato: $\mathbb{Z}_p = \left(p\cdot\mathbb{Z}_p\right) \bigsqcup \left(\mathbb{Z}_p^\times\right)$.

$\Rightarrow$ zbog aditivnosti od $\mu_{B,k}$ vrijedi: $\mu_{B,k}(\mathbb{Z}_p) = \mu_{B,k}(p\cdot\mathbb{Z}_p) + \mu_{B,k}(\mathbb{Z}_p^\times)$

$\Rightarrow$ $\mu_{B,k}(\mathbb{Z}_p^\times) = \mu_{B,k}(\mathbb{Z}_p) - \mu_{B,k}(p\cdot\mathbb{Z}_p) =$

$$= [\text{leme } 2.5.14 \text{ i } 2.5.15] = B_k - p^{k-1}\cdot B_k = B_k\cdot\left(1-p^{k-1}\right)$$

□

Propozicija 2.5.17. *Vrijedi:*

$$\mu_{k,\alpha}\left(\mathbb{Z}_p^\times\right) = (1-p^{k-1})\cdot B_k\cdot\left(1-\frac{1}{\alpha^k}\right)$$

Dokaz.

Znamo: $\mu_{k,\alpha}\left(\mathbb{Z}_p^\times\right) = \mu_{B,k}\left(\mathbb{Z}_p^\times\right) - \dfrac{\mu_{B,k}\left(\alpha\cdot\mathbb{Z}_p^\times\right)}{\alpha^k}.$ (2.11)

Sada ćemo dokazati pomoćnu tvrdnju koja kaže da vrijedi: $\alpha\cdot\mathbb{Z}_p^\times = \mathbb{Z}_p^\times$.

$\subseteq$

Neka je $(y = \alpha\cdot x \in \alpha\cdot\mathbb{Z}_p^\times)$ proizvoljan. $\Rightarrow$ $|x|_p = 1$

$|y|_p = |\alpha\cdot x|_p = \underbrace{|\alpha|_p}_{\substack{=1 \text{ jer} \\ p\nmid\alpha}}\cdot\underbrace{|x|_p}_{=1} = 1 \Rightarrow (y\in\mathbb{Z}_p^\times)$

$\supseteq$

Neka je $(x\in\mathbb{Z}_p^\times)$ proizvoljan. $\Rightarrow$ $|x|_p = 1$

$\Rightarrow \left|\dfrac{x}{\alpha}\right|_p = \dfrac{|x|_p}{|\alpha|_p} = \dfrac{1}{1} = 1 \Rightarrow \dfrac{x}{\alpha}\in\mathbb{Z}_p^\times$, a znamo da je $x = \alpha\cdot\left(\dfrac{x}{\alpha}\right)$

$\Rightarrow x\in\alpha\cdot\mathbb{Z}_p^\times$

Time je pomoćna tvrdnja dokazana.

$\Rightarrow \mu_{B,k}\left(\alpha\cdot\mathbb{Z}_p^\times\right) = \mu_{B,k}\left(\mathbb{Z}_p^\times\right) = [\,2.5.16] = (1-p^{k-1})\cdot B_k$

$\Rightarrow \mu_{k,\alpha}\left(\mathbb{Z}_p^\times\right) = [\,2.11] = \mu_{B,k}\left(\mathbb{Z}_p^\times\right) - \dfrac{\mu_{B,k}\left(\alpha\cdot\mathbb{Z}_p^\times\right)}{\alpha^k} = (1-p^{k-1})\cdot B_k\cdot\left(1-\dfrac{1}{\alpha^k}\right)$

□

2.6 p-adska zeta funkcija

Ako je X proizvoljan kompaktno-otvoreni podskup od $\mathbb{Z}_p$, svaka mjera μ na $\mathbb{Z}_p$ se može restringirati na X. Dakle, definiramo mjeru μ^* na X na sljedeći način: $\mu^*(U) := \mu(U)$ za sve kompaktno-otvorene $(U\subseteq X)$. Vrijedi:

$$\int_X f\,\mu := \int f\,\mu^* = \int f\cdot(\text{karakteristična funkcija od X})\,\mu.$$

Bili smo rekli u sekciji 2 da zapravo želimo interpolirati faktor $-\frac{B_k}{k}$. Vrijedi:

$$\int_{\mathbb{Z}_p} 1 \cdot \mu_{B,k} = \mu_{B,k}(\mathbb{Z}_p) = [\text{lema } 2.5.14] = B_k. \tag{2.12}$$

Dakle, ono što ćemo zapravo interpolirati je $-\left(\frac{1}{k}\right) \cdot \int_{\mathbb{Z}_p} 1 \cdot \mu_{B,k}$.

Za različite k distribucije $\mu_{B,k}$ nisu povezane na neki očit način, ali su zato regularizirane mjere $\mu_{k,\alpha}$ i $\mu_{1,\alpha}$ povezane preko teorema 2.5.8.
Vrijedi sljedeći korolar teorema 2.5.8 i 2.5.10:

Propozicija 2.6.1. *Neka je funkcija* $f : \mathbb{Z}_p \to \mathbb{Z}_p$ *zadana s:* $f(x) = x^{k-1}$, *pri čemu je* $(k \in \mathbb{N})$ *fiksiran. Također, neka je* $(X \subseteq \mathbb{Z}_p)$ *kompaktno-otvoren. Tada vrijedi:*

$$\int_X 1 \cdot \mu_{k,\alpha} = k \cdot \int_X f \cdot \mu_{1,\alpha}$$

Dokaz.

$$\mu_{k,\alpha}\left(a + (p^N)\right) \equiv [TM\ 2.5.8] \equiv k \cdot a^{k-1} \cdot \mu_{1,\alpha}\left(a + (p^N)\right) (\text{mod } \ p^{N-ord_p(d_k)})$$

Pretpostavimo da je N dovoljno velik da se X može prikazati kao unija intervala oblika $a + (p^N)$. Vrijedi:

$$\begin{aligned}\int_X 1 \cdot \mu_{k,\alpha} &= [\text{def. integrala preko Riemannovih suma}] = \sum_{\substack{0 \le a < p^N \\ a+(p^N) \subset X}} \mu_{k,\alpha}\left(a + (p^N)\right) = \\ &\equiv \sum_{\substack{0 \le a < p^N \\ a+(p^N) \subset X}} k \cdot a^{k-1} \cdot \mu_{1,\alpha}\left(a + (p^N)\right) \ (\text{mod } \ p^{N-ord_p(d_k)}) = \\ &= [f(a) = a^{k-1}] = k \cdot \sum_{\substack{0 \le a < p^N \\ a+(p^N) \subset X}} f(a) \cdot \mu_{1,\alpha}\left(a + (p^N)\right)\end{aligned}$$

Puštanjem limesa $N \to \infty$ dobivamo:

$$\int_X 1 \cdot \mu_{k,\alpha} = k \cdot \int_X f \cdot \mu_{1,\alpha}$$

□

Uzimanjem notacije x^{k-1} umjesto f i integriranjem po x-u dobivamo sljedeći zapis prethodne propozicije:

$$\int_X 1 \cdot \mu_{k,\alpha} = k \cdot \int_X x^{k-1} \cdot \mu_{1,\alpha} \tag{2.13}$$

Prema rezultatima iz sekcije 2, izraz x^{k-1} (za neki fiksirani x) možemo interpolirati samo
ako vrijedi: $p \nmid x$. A to će vrijediti za sve x-eve iz naše domene integracije samo ako uzmemo: $X = \mathbb{Z}_p^\times$.
Dakle, tvrdimo da se izraz $\int_{\mathbb{Z}_p^\times} x^{k-1}\,\mu_{1,\alpha}$ može interpolirati. Za to ćemo primijeniti korolar 2.5.13 koji kaže sljedeće:
Ako su $f, g : X \to \mathbb{Q}_p$ neprekidne funkcije t.d. $|f(x) - g(x)|_p \leq \epsilon$ $(\forall x \in X)$ i $\mu(U) \leq B$ za sve kompaktno-otvorene $(U \subset X)$, onda vrijedi:

$$\left| \int f\,\mu - \int g\,\mu \right|_p \leq \epsilon \cdot B$$

Specijalno, kod nas će biti: $g(x) = x^{k-1}$, $X = \mathbb{Z}_p^\times$, $\mu = \mu_{1,\alpha}$. Iz propozicije 2.5.6 znamo da je u tom slučaju $B = 1$. Dakle, ako $(\forall x \in \mathbb{Z}_p^\times)$ vrijedi: $\left|f(x) - x^{k-1}\right|_p \leq \epsilon$, onda vrijedi:

$$\left| \int_{\mathbb{Z}_p^\times} f \cdot \mu_{1,\alpha} - \int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \mu_{1,\alpha} \right|_p \leq \epsilon \tag{2.14}$$

Stavit ćemo: $f(x) = x^{k'-1}$, gdje je, prema 2. slučaju diskusije s početka sekcije 2,
$k' \equiv k \pmod{p-1}$ i $k' \equiv k \pmod{p^N}$. Specijalno, ako te dvije kongruencije zapišemo kao jednu, to će biti: $k' \equiv k \pmod{(p-1)p^N}$.
Prema 2.1 sada vrijedi:

$$\left|x^{k'-1} - x^{k-1}\right|_p \leq \frac{1}{p^{N+1}}, \quad (\forall x \in \mathbb{Z}_p^\times).$$

Ako sada kod 2.14 uzmemo $\epsilon = \frac{1}{p^{N+1}}$, dobivamo:

$$\left| \int_{\mathbb{Z}_p^\times} x^{k'-1} \cdot \mu_{1,\alpha} - \int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \mu_{1,\alpha} \right|_p \leq \frac{1}{p^{N+1}}.$$

Dobili smo: ako su $k-1$ i $k'-1$ blizu (tj. $k' \equiv k \pmod{p^N}$) i još vrijedi dodatni uvjet $k' \equiv k \pmod{p-1}$, onda su i $\int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \mu_{1,\alpha}$ i $\int_{\mathbb{Z}_p^\times} x^{k'-1} \cdot \mu_{1,\alpha}$ također blizu. Dakle, kao i u 2. slučaju diskusije s početka sekcije 2, slijedi da se uz fiksirani $(s_0 \in \{0, 1, 2, ..., p-2\})$ funkcija u varijabli $(k \in S_{s_0})$ dana s: $\int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \mu_{1,\alpha}$ može na jedinstven način proširiti do neprekidne funkcije (u varijabli s) na čitavom $\mathbb{Z}_p$ na sljedeći način (gdje je $\{s_i\}$ proizvoljan niz iz $\mathbb{N}$ koji p-adski teži prema s):

$$\int_{\mathbb{Z}_p^\times} x^{s-1} \cdot \mu_{1,\alpha} = \lim_{i\to\infty} \int_{\mathbb{Z}_p^\times} x^{s_i-1} \cdot \mu_{1,\alpha}. \tag{2.15}$$

Dakle, upravo smo dobili da se može interpolirati funkcija:

$$\int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \mu_{1,\alpha} = [\ 2.13] = \frac{1}{k} \cdot \int_{\mathbb{Z}_p^\times} 1 \cdot \mu_{k,\alpha}, \tag{2.16}$$

a nas (kako je spomenuto ranije) zanima interpolacija izraza $-\frac{B_k}{k}$. Dakle, moramo nekako "povezati" ta dva izraza:

$$\left(\frac{1}{k}\right) \cdot \int_{\mathbb{Z}_p^\times} 1 \cdot \mu_{k,\alpha} = \left(\frac{1}{k}\right) \cdot \mu_{k,\alpha}(\mathbb{Z}_p^\times) = [prop.\ 2.5.17] = \left(\frac{1}{k}\right) \cdot (1-p^{k-1}) \cdot B_k \cdot \left(1 - \frac{1}{\alpha^k}\right) =$$

$$= (1-p^{k-1}) \cdot \left(\frac{1}{\alpha^k} - 1\right) \cdot \left(-\frac{B_k}{k}\right) = (1-p^{k-1}) \cdot \left(\alpha^{-k} - 1\right) \cdot \left(-\frac{B_k}{k}\right)$$

$$\Rightarrow \quad (1-p^{k-1}) \cdot \left(-\frac{B_k}{k}\right) = \frac{1}{\alpha^{-k}-1} \cdot \left(\frac{1}{k}\right) \cdot \int_{\mathbb{Z}_p^\times} 1 \cdot \mu_{k,\alpha} =$$

$$= [\ 2.16] = \frac{1}{\alpha^{-k}-1} \cdot \int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \mu_{1,\alpha} \tag{2.17}$$

To je ono "uklanjanje p-Eulerovog faktora" o kojem smo pričali u sekciji 2 - kako ne možemo interpolirati n^s kad $p \mid n$, moramo ukloniti p-Eulerov faktor iz ζ-funkcije prije nego je interpoliramo. Ali p-Eulerov faktor nije $\frac{1}{1-p^{-k}}$ (kako bi nam se na prvu moglo činiti zbog diskusije u sekciji 2), nego $\frac{1}{1-p^{k-1}}$. To je kao da smo, umjesto $\zeta(k)$, zapravo interpolirali $\zeta(1-k)$, iako do sada još nismo rekli što to točno znači za pozitivne k. Zato uvodimo sljedeću definiciju:

Definicija 2.6.2. *Za* $(k \in \mathbb{N})$ *definiramo:*

$$\zeta_p(1-k) := (1-p^{k-1}) \cdot \left(-\frac{B_k}{k}\right)$$

tako da vrijedi:

$$\zeta_p(1-k) = (1-p^{k-1}) \cdot \left(-\frac{B_k}{k}\right) = [\ 2.17] = \frac{1}{\alpha^{-k}-1} \cdot \int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \mu_{1,\alpha}. \tag{2.18}$$

Time smo Riemannovu zeta funkciju proširili s $\mathbb{N}$ na $\mathbb{Z}$.
Uočimo da izraz s desne strane jednakosti u 2.18 ne ovisi o izboru parametra α jer je jednak konstanti $(1-p^{k-1}) \cdot \left(-\frac{B_k}{k}\right)$.

Definicija 2.6.3. *Fiksirajmo neki* $(s_0 \in \{0,1,2,...,p-2\})$. *Za* $(s \in \mathbb{Z}_p)$ *(specijalno,* $s_0 = 0 \Rightarrow s \neq 0$*) definiramo:*

$$\zeta_{p,s_0}(s) \coloneqq \frac{1}{\alpha^{-(s_0+(p-1)\cdot s)}-1} \cdot \int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)\cdot s-1} \cdot \mu_{1,\alpha}.$$

U definiciji smo isključili slučaj $s_0 = 0, s = 0$ jer je tada $\alpha^{-(s_0+(p-1)\cdot s)} = 1$ pa je nazivnik jednak nuli.
Ova definicija je dobra - znamo da je $\int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)\cdot s-1} \cdot \mu_{1,\alpha}$ dobro definirano zbog 2.15, a $\alpha^{-(s_0+(p-1)\cdot s)} = \alpha^{-s_0} \cdot \left(\alpha^{p-1}\right)^{-s}$ se za $(s \in \mathbb{Z}_p)$ također definira uzimanjem proizvoljnog niza $\{s_i\}$ iz $\mathbb{N}$ koji p-adski teži prema s zbog leme 2.2.4.

Drugi način da se definira $\zeta_{p,s_0}(s)$ je sljedeći:

$$\zeta_{p,s_0}(s) = \lim_{s_i \to s} \left(1-p^{s_0+(p-1)\cdot s_i-1}\right) \cdot \left(-\frac{B_{s_0+(p-1)\cdot s_i}}{s_0+(p-1)\cdot s_i}\right).$$

Lako se vidi da za $(k \in \mathbb{N})$ takav da $k \equiv s_0 \pmod{p-1}$ (tj. za $k = s_0 + (p-1)\cdot k_0$) vrijedi:

$$\zeta_{p,s_0}(k_0) = [\ 2.18] = \zeta_p(1-k) = [def.\ 2.6.2] = (1-p^{k-1}) \cdot \left(-\frac{B_k}{k}\right) \tag{2.19}$$

O ζ_{p,s_0} razmišljamo kao o p-adskim "granama" od ζ_p (po jedna za svaku klasu kongruencije modulo $p-1$). Ali nas zanimaju samo parne klase kongruencije $(s_0 = 0,2,...,p-1)$ jer neparne klase kongruencije $(s_0 = 1,3,...,p-2)$ daju nul-funkciju budući da za takve s_0 uvijek vrijedi: $B_{s_0+(p-1)\cdot k_i} = 0$ (jer je $s_0 + (p-1)\cdot s_i > 1$ i neparno).

Teorem 2.6.4. *Za fiksirane* p *i* s_0*, funkcija* $\zeta_{p,s_0}(s)$ *je neprekidna te ne ovisi o izboru parametra* $(\alpha \in \mathbb{Z})$, $(p \nmid \alpha)$, $(\alpha \neq 1)$ *koji se javlja u njenoj definiciji.*

Dokaz.
Funkcija $\zeta_{p,s_0}(s)$ je neprekidna jer je $\int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)\cdot s-1} \cdot \mu_{1,\alpha}$ neprekidna funkcija prema 2.15, te je $\frac{1}{\alpha^{-(s_0+(p-1)\cdot s)}}$ neprekidna jer je $\alpha^{-(s_0+(p-1)\cdot s)} = \alpha^{-s_0} \cdot \left(\alpha^{p-1}\right)^{-s}$ neprekidna prema lemi 2.2.4.

Preostaje pokazati da $\zeta_{p,s_0}(s)$ ne ovisi o izboru parametra α. Neka je $(\beta \in \mathbb{Z})$ t.d. $(\beta \neq \alpha, 1)$, $(p \nmid \beta)$.
Funkcije:

$$\frac{1}{\alpha^{-(s_0+(p-1)\cdot s)} - 1} \cdot \int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)\cdot s-1} \cdot \mu_{1,\alpha}$$

i

$$\frac{1}{\beta^{-(s_0+(p-1)\cdot s)} - 1} \cdot \int_{\mathbb{Z}_p^\times} x^{s_0+(p-1)\cdot s-1} \cdot \mu_{1,\beta}$$

se poklapaju kad god je $s_0 + (p-1)\cdot s = k$ prirodni broj, tj. kad god je $(s \in \mathbb{N}_0)$ (a, ako je $s_0 = 0$, onda $(s \in \mathbb{N})$) jer su tada obje funkcije jednake $(1 - p^{k-1}) \cdot (-B_k/k)$ prema 2.18 i komentaru koji ga slijedi.
To je dovoljno da možemo tvrditi da su te dvije funkcije jednake jer, kako je $\mathbb{N}_0$ gust u $\mathbb{Z}_p$ prema lemi 2.2.1, svake dvije neprekidne funkcije čija je domena $\mathbb{Z}_p$ i koje se podudaraju na $\mathbb{N}_0$ su jednake. □

Taj nam teorem u konačnici daje traženu p-adsku interpolaciju Riemannove zeta funkcije jer, uz to što smo već objasnili da je p-adska zeta funkcija $\zeta_{p,s_0}(s)$ iz definicije 2.6.3 dobro definirana, sada znamo i da ta definicija ne ovisi o izboru parametra α koji se u njoj pojavljuje te da je tako dobivena funkcija neprekidna. To znači da s tako definiranom funkcijom ζ_{p,s_0} proširujemo Riemannovu zeta funkciju s gustog skupa $\mathbb{N}_0$ na čitav $\mathbb{Z}_p$.

Važno je napomenuti da funkcija $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ zadovoljava tzv. "funkcionalnu jednadžbu" koja uspostavlja odnos između njene vrijednosti u s i njene vrijednosti u $1 - s$:

$$\zeta(1-s) = \frac{2 \cdot \cos(\pi s/2) \cdot \Gamma(s)}{(2\pi)^s} \cdot \zeta(s). \tag{2.20}$$

1. slučaj - s je parni prirodni broj

Možemo uzeti: $s = 2k$. Vrijedi:

$$\zeta(1-s) = \zeta(1-2k) = [\ 2.20] = \frac{2 \cdot \cos(\pi k) \cdot \Gamma(2k)}{(2\pi)^{2k}} \cdot \zeta(2k) =$$

$$= \left\{ \begin{array}{l} \text{svojstvo koje ćemo dokazati nešto kasnije:} \\ k \text{ paran prirodni broj} \Rightarrow \ \Gamma(k) = (k-1)! \end{array} \right\} =$$

$$= \frac{2 \cdot \cos(\pi k) \cdot (2k-1)!}{(2\pi)^{2k}} \cdot \zeta(2k) =$$

$$= [\text{prop. } 2.1.3] = \frac{2 \cdot (-1)^k \cdot (2k-1)!}{(2\pi)^{2k}} \cdot (-1)^k \pi^{2k} \cdot \frac{2^{2k-1}}{(2k-1)!} \cdot \left(-\frac{B_{2k}}{2k}\right) =$$

$$= \frac{2}{(2)^{2k}} \cdot 2^{2k-1} \cdot \left(-\frac{B_{2k}}{2k}\right) =$$

$$= -\frac{B_{2k}}{2k}$$

2. slučaj - s je neparni prirodni broj veći od 1

(Prema definiciji zeta-funkcije, trebala nam je pretpostavka $(s > 1)$ da bi $\zeta(s)$ bilo konačno). U ovom slučaju vrijedi:

$$\zeta(1-s) = [\ 2.20] = \frac{2 \cdot \cos(\pi s/2) \cdot \Gamma(s)}{(2\pi)^s} \cdot \zeta(s) =$$

$$= [\text{za ovakve } s \text{ je } \cos(\pi s/2) = 0 \text{ pa čitava desna strana nestane }] = 0$$

Znamo da za takve s vrijedi: $B_s = 0$.

$\Rightarrow \quad -\frac{B_s}{s} = 0 \ \Rightarrow \ \zeta(1-s) = -\frac{B_s}{s}$, ali to samo znači da je $0 = 0$ pa nas taj slučaj ne zanima

Dakle, vidimo da za sve parne prirodne brojeve k vrijedi: $\zeta(1-k) = -\frac{B_k}{k}$. To znači da smo zapravo interpolirali Riemannovu zeta-funkciju u neparnim negativnim cijelim brojevima. Sada možemo uspostaviti odnos između ζ i ζ_p:

$(\forall k \in \mathbb{N}), (k > 1)$ vrijedi: $\zeta_p(1-k) = [def.] = (1-p^{k-1}) \cdot \underbrace{\left(-\frac{B_k}{k}\right)}_{=\zeta(1-k)} = (1-p^{k-1}) \cdot \zeta(1-k)$

Ako bismo zanemarili činjenicu da sve divergira, dobili bismo:

$$\zeta^*(1-k) = [\text{ranije def.}] = \prod_{prosti\ \ brojevi\ \ q\neq p} \frac{1}{1-\frac{1}{q^{1-k}}} = \prod_{prosti\ \ brojevi\ \ q\neq p} \frac{1}{1-q^{k-1}} =$$

$$= \frac{\prod_{prosti\ \ brojevi\ \ q} \left(\frac{1}{1-q^{k-1}}\right)}{\frac{1}{1-p^{k-1}}} =$$

$$= [\text{prop. } 2.2.5] = \frac{\zeta(1-k)}{\frac{1}{1-p^{k-1}}} =$$
$$= (1-p^{k-1}) \cdot \zeta(1-k),$$

pa vidimo da je p-Eulerov faktor spomenut u diskusiji nakon izraza 2.17 uistinu $\frac{1}{1-p^{k-1}}$.

Poglavlje 3

Gama funkcija

3.1 Definicija i osnovna svojstva

Definicija 3.1.1. ***Gama funkcija*** *definira se kao integral:*

$$\Gamma(z) = \int_0^\infty \left(t^{z-1} \cdot \mathrm{e}^{-t}\right) \cdot \, dt,$$

pri čemu je: $t^{z-1} := \mathrm{e}^{(z-1)\cdot ln(t)}$, $(ln(t) \in \mathbb{R})$, $(Re(z) > 0)$.

Naziv "gama funkcija" i njenu oznaku Γ uveo je A. M. Legendre.

Propozicija 3.1.2. *Gama integral:*

$$\Gamma(z) = \int_0^\infty \left(t^{z-1} \cdot \mathrm{e}^{-t}\right) \cdot \, dt$$

apsolutno konvergira na poluravnini $Re(z) > 0$ *gdje predstavlja* ***analitičku funkciju***.

Dokaz ove propozicije može se naći na stranicama 193-194 literature **[Freitag-Busam]**.

Lema 3.1.3. *Gama funkcija zadovoljava* ***funkcionalnu jednadžbu****:*

$$\Gamma(z+1) = z \cdot \Gamma(z), \qquad uz: \quad Re(z) > 0.$$

Dokaz.
Vrijedi:

$$\Gamma(z+1) = \int_0^\infty (t^z \cdot \mathrm{e}^{-t}) \cdot \, dt =$$
$$= \left\{ \begin{array}{ll} u = t^z & \Rightarrow \; du = z \cdot t^{z-1} \cdot dt \\ dv = \mathrm{e}^{-t} & \Rightarrow \; v = -\mathrm{e}^{-t} \end{array} \right\} = \underbrace{-\left(\frac{t^z}{\mathrm{e}^t}\right)\Big|_0^\infty}_{=0} + z \cdot \int_0^\infty \left(t^{z-1} \cdot \mathrm{e}^{-t}\right) \cdot \, dt =$$
$$= z \cdot \Gamma(z)$$

□

Specijalno, iz prethodne leme i činjenice: $\Gamma(1) = \int_0^\infty \mathrm{e}^{-t}\, dt = -\mathrm{e}^{-t}\Big|_0^\infty = 1$ dobivamo da $(\forall n \in \mathbb{N}_0)$ vrijedi:

$$\Gamma(n+1) = n \cdot \Gamma(n) = n \cdot \Big[(n-1) \cdot \Gamma(n-1)\Big] = (...) =$$
$$= n \cdot (n-1) \cdot ... \cdot 2 \cdot 1 \cdot \Gamma(1) = n \cdot (n-1) \cdot ... \cdot 2 \cdot 1 \cdot 1 = n!$$

Dakle, vidimo da gama funkcija interpolira faktorijele.

Imamo:

$$\Gamma(z) = [\text{prop. } 3.1.3] = \frac{\Gamma(z+1)}{z} = \Gamma(z+1) \cdot \frac{1}{z} =$$
$$= [\text{prop. } 3.1.3] = \frac{\Gamma(z+2)}{z+1} \cdot \frac{1}{z} = \frac{\Gamma(z+2)}{z(z+1)} =$$
$$= (...) = \frac{\Gamma(z+n+1)}{z \cdot (z+1) \cdot ... \cdot (z+n)} \tag{3.1}$$

Iz ovog rezultata vidimo da gama funkcija ima polove reda 1 u $0, -1, -2, -3, ...$, i da su pripadajući reziduumi (uz $n \in \mathbb{N}_0$):

$$Res(\Gamma; -n) = \lim_{z \to -n} \Big[(z - (-n)) \cdot \Gamma(z)\Big] = \lim_{z \to -n} \Big[(z+n) \cdot \Gamma(z)\Big] =$$
$$= [\,3.1] = \lim_{z \to -n} \Big[(z+n) \cdot \frac{\Gamma(z+n+1)}{z \cdot (z+1) \cdot ... \cdot (z+n)}\Big] =$$
$$= \lim_{z \to -n} \Big[\frac{\Gamma(z+n+1)}{z \cdot (z+1) \cdot ... \cdot (z+n-1)}\Big] =$$
$$= \frac{\Gamma(1)}{(-n) \cdot (-n+1) \cdot ... \cdot (-1)} =$$
$$= \frac{1}{(-1)^n \cdot n \cdot (n-1) \cdot ... \cdot (2) \cdot (1)} = \frac{1}{(-1)^n \cdot n!} = \frac{(-1)^n}{n!} \tag{3.2}$$

Kako znamo da je $\Gamma(z)$ dobro definirano za $Re(z) > 0$, tako vidimo da je $\Gamma(z+n+1)$ sa desne strane rezultata 3.1 dobro definirano za $Re(z+n+1) > 0$, tj. za $Re(z) > -(n+1)$. To zapravo znači da desna strana jednakosti u izrazu 3.1 ima šire područje definicije nego lijeva strana te jednakosti. Time smo zapravo dobili dobili analitičko proširenje po neprekidnosti gama funkcije sa skupa $\left\{(z \in \mathbb{C}) : Re(z) > 0\right\}$ na skup:

$$\left\{(z \in \mathbb{C}) : Re(z) > -(n+1),\ \ (z \neq 0, -1, -2, ..., -n),\ \ (n \in \mathbb{N}_0)\right\}.$$

Sve su te analitičke kontinuacije (za svaki n) jedinstvene pa zajedno daju analitičko proširenje po neprekidnosti gama funkcije koje ćemo također označavati s Γ.
Dakle, vidimo da se gama funkcija može na jedinstven način analitički proširiti na skup $\mathbb{C} \setminus \{0, -1, -2, ...\}$.

3.2 Veza gama funkcije i razvoja $sh(\pi x)$ u beskonačni produkt

Lema 3.2.1. *Funkcija $f(z) := \Gamma(z) \cdot \Gamma(1-z)$ je periodična do na predznak (tj. vrijedi: $f(z+1) = -f(z)$) te je perioda 2, ima polove reda 1 u svim cijelim brojevima i odgovarajući reziduumi su: $Res(f; -n) = (-1)^n$ uz $(n \in \mathbb{Z})$.*

Dokaz.
$\underline{f(z+1) = -f(z):}$

$$f(z+1) = \Gamma(z+1) \cdot \Gamma(-z) = [\text{lema } 3.1.3] = \Big[z \cdot \Gamma(z)\Big] \cdot \Gamma(-z)$$
$$-f(z) = -\Gamma(z) \cdot \Gamma(1-z) = [\text{lema } 3.1.3] = -\Gamma(z) \cdot \Big[-z \cdot \Gamma(-z)\Big] = z \cdot \Gamma(z) \cdot \Gamma(-z) = f(z+1) \tag{3.3}$$

$\underline{f \text{ je perioda 2:}}$

$$f(z+2) = f((z+1)+1) = [\ 3.3] = -f(z+1) = [\ 3.3] = -\Big[-f(z)\Big] = f(z)$$

$\underline{f \text{ ima polove reda 1 u svim cijelim brojevima:}}$
Prvo ćemo dokazati pomoćnu tvrdnju koja kaže da $\Gamma(1-z)$ ima polove reda 1 u svim prirodnim brojevima. Prisjetimo se, funkcija f ima pol reda n u točki z_0 ako vrijedi:

$\lim_{z\to z_0}\Big[(z-z_0)^n\cdot f(z)\Big]\in\mathbb{C}$ i $\lim_{z\to z_0}\Big[(z-z_0)^{n-1}\cdot f(z)\Big]=\infty.$

$$\lim_{z\to n}\Big[\Gamma(1-z)\Big]=[\,3.1\,]=\lim_{z\to n}\left[\frac{\Gamma(2+n-z)}{(1-z)\cdot(2-z)\cdot\ldots\cdot(n-z)\cdot(n+1-z)}\right]=\infty$$

$$\lim_{z\to n}\Big[(z-n)\cdot\Gamma(1-z)\Big]=[\text{kao i gore}]=\lim_{z\to n}\left[(z-n)\cdot\frac{\Gamma(2+n-z)}{(1-z)\cdot(2-z)\cdot\ldots\cdot(n-z)\cdot(n+1-z)}\right]=$$

$$=\lim_{z\to n}\left[\frac{\Gamma(2+n-z)\cdot(-1)}{(1-z)\cdot(2-z)\cdot\ldots\cdot(n-1-z)\cdot(n+1-z)}\right]=$$

$$=\frac{\Gamma(2)\cdot(-1)}{(1-n)\cdot(2-n)\cdot\ldots\cdot(-1)\cdot(1)}=\frac{\Gamma(2)}{(1-n)\cdot(2-n)\cdot\ldots\cdot(-2)\cdot(1)}\in\mathbb{C}$$

Time je pomoćna tvrdnja dokazana. Sada imamo:

$f(z)=\underbrace{\Gamma(z)}_{\substack{\text{polovi}\\ \text{reda}\\ 1\text{ u}\\ -n,\\ (n\in\mathbb{N}_0)}}\cdot\underbrace{\Gamma(1-z)}_{\substack{\text{polovi}\\ \text{reda}\\ 1\text{ u }n,\\ (n\in\mathbb{N})}}$, što povlači da f ima polove reda 1 u svim cijelim brojevima.

$\underline{Res(f;-n)=(-1)^n \text{ uz } (n\in\mathbb{Z}):}$

$$Res(f;-n)=Res\Big(\Gamma(z)\cdot\Gamma(1-z);-n\Big)=\lim_{z\to-n}\Big[(z+n)\cdot\Gamma(z)\cdot\Gamma(1-z)\Big]=$$

$$=\lim_{z\to-n}\Big[(z+n)\cdot\Gamma(z)\Big]\cdot\lim_{z\to-n}\Big[\Gamma(1-z)\Big]=$$

$$=[\,3.2\,]=\frac{(-1)^n}{n!}\cdot\lim_{z\to-n}\Big[\Gamma(1-z)\Big]=\frac{(-1)^n}{n!}\cdot\lim_{z\to n}\Big[\Gamma(1+z)\Big]=$$

$$=[\,3.1\,]=\frac{(-1)^n}{n!}\cdot\lim_{z\to n}\left[\frac{\Gamma(z+n+2)}{(1+z)\cdot(2+z)\cdot\ldots\cdot(n+1+z)}\right]=$$

$$=\frac{(-1)^n}{n!}\cdot\frac{\Gamma(2n+2)}{(1+n)\cdot(1+(n+1))\cdot\ldots\cdot(1+2n)}=$$

$$=\frac{(-1)^n}{n!}\cdot\frac{(2n+1)!}{\frac{(1+2n)!}{n!}}=\frac{(-1)^n}{n!}\cdot n!=(-1)^n$$

□

Lema 3.2.2. *Funkcija:*

$$F(z):=\frac{\pi}{\sin(\pi z)}$$

je periodična do na predznak (tj. vrijedi: $F(z+1)=-F(z)$) te je perioda 2, ima polove reda 1 u svim cijelim brojevima i odgovarajući reziduumi su: $Res(F;-n)=(-1)^n$ uz $(n\in\mathbb{Z})$.

Dokaz.
$\underline{F(z+1) = -F(z):}$

$$F(z+1) = \frac{\pi}{\sin(\pi(z+1))} = \frac{\pi}{\sin(\pi z + \pi)} = \frac{-\pi}{\sin(\pi z)} = -F(z) \tag{3.4}$$

$\underline{F \text{ je perioda } 2:}$

$$F(z+2) = \frac{\pi}{\sin(\pi(z+2))} = \frac{\pi}{\sin(\pi z + 2\pi)} = \frac{\pi}{\sin(\pi z)} = F(z)$$

$\underline{F \text{ ima polove reda 1 u svim cijelim brojevima:}}$

$$\lim_{z\to n}\Big[F(z)\Big] = \lim_{z\to n}\left[\frac{\pi}{\sin(\pi z)}\right] = \infty$$

$$\lim_{z\to n}\Big[(z-n)\cdot F(z)\Big] = \lim_{z\to n}\left[\frac{(z-n)\cdot\pi}{\sin(\pi z)}\right] = \text{[L'Hospital]} = \lim_{z\to n}\left[\frac{\pi\cdot 1}{\pi\cdot\cos(\pi z)}\right] = \frac{1}{(-1)^n} = (-1)^n \in \mathbb{C}$$

$\underline{Res(F;-n) = (-1)^n \text{ uz } (n\in\mathbb{Z}):}$

$$\begin{aligned} Res(F;-n) &= \lim_{z\to -n}\Big[(z+n)\cdot F(z)\Big] = \\ &= \lim_{z\to -n}\left[\frac{(z+n)\cdot\pi}{\sin(\pi z)}\right] = \text{[L'Hospital]} = \lim_{z\to -n}\left[\frac{\pi\cdot 1}{\pi\cdot\cos(\pi z)}\right] = \frac{1}{(-1)^n} = (-1)^n \end{aligned}$$

□

Propozicija 3.2.3. ***(Euler)*** *Za svaki* $(z\in\mathbb{C}\setminus\mathbb{Z})$ *vrijedi:*

$$\Gamma(z)\cdot\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}.$$

Dokaz.
Definiramo funkciju:

$$h(z) := \Gamma(z)\cdot\Gamma(1-z) - \frac{\pi}{\sin(\pi z)}.$$

Zapravo vrijedi (uz notaciju iz lema 3.2.1 i 3.2.2): $h = f - F$. (3.5)

Uočimo da za sve $(z\in\mathbb{C})$ za koje je $(x := Re(z) > 0)$ vrijedi: $|\Gamma(z)| \le \Gamma(x)$. Zato je funkcija Γ (pa onda i f) ograničena na svakoj okomitoj pruzi, pa onda specijalno i na

pruzi $(0 \le x \le 1), (|y| \ge 1)$. Još treba vidjeti da je i F ograničena na toj okomitoj pruzi. Vrijedi:

$$
\begin{aligned}
|sin(z)| &= \left[sh(z) = -i \cdot \sin(iz) \right] = \left| \frac{sh\left(\frac{z}{i}\right)}{-i} \right| = \left| sh\left(\frac{z}{i}\right) \right| = \\
&= \left\{ \frac{z}{i} = \frac{x + y \cdot i}{i} = \frac{x + y \cdot i}{i} \cdot \frac{i}{i} = \frac{(-y) + (x) \cdot i}{-1} = (y) + (-x) \cdot i \right\} = \\
&= |sh(y - x \cdot i)| = \left| \frac{e^{y - x \cdot i} - e^{-y + x \cdot i}}{2} \right| = \\
&= \left| \frac{e^{y} \cdot [\cos(-x) + i \cdot \sin(-x)] - e^{-y} \cdot [\cos(x) + i \cdot \sin(x)]}{2} \right| = \\
&= \left| \frac{e^{y} \cdot [\cos(x) - i \cdot \sin(x)] - e^{-y} \cdot [\cos(x) + i \cdot \sin(x)]}{2} \right| = \\
&= \left| \cos(x) \cdot \frac{e^{y} - e^{-y}}{2} - i \cdot \sin(x) \cdot \frac{e^{y} + e^{-y}}{2} \right| = \\
&= |\cos(x) \cdot sh(y) - i \cdot \sin(x) \cdot ch(y)| = \\
&\ge |-sh(y) + i \cdot ch(y)| \qquad \text{jer su } \sin \text{ i } \cos \ge -1 \\
&\ge |-sh(y) + i| \qquad \text{jer je } ch \ge 1 \\
&= |sh(y) - i| = \sqrt{sh^2(y) + (-1)^2} \ge \sqrt{sh^2(y) + 1} \ge \sqrt{sh^2(y)} = |sh(y)|
\end{aligned}
$$

Zato imamo:

$$
\begin{aligned}
&|sin(\pi z)| \ge |sh(\pi y)| \\
&\Rightarrow \quad |F(z)| = \left| \frac{\pi}{\sin(\pi z)} \right| = \frac{\pi}{|\sin(\pi z)|} \le \frac{\pi}{|\mathrm{sh}(\pi y)|} \le \frac{\pi}{|sh(\pi)|} = \text{konst.} \\
&\qquad\qquad\qquad\qquad\qquad\qquad \uparrow \\
&\qquad\qquad\qquad\qquad \text{jer za } |y| \ge 1 \text{ vrijedi: } |sh(y)| \ge |sh(1)|
\end{aligned}
$$

Dakle, pokazali smo da je i F ograničena na pruzi $(0 \le x \le 1), (|y| \ge 1)$, pa je onda i h ograničena na toj pruzi (kao razlika ograničenih funkcija).

Prisjetimo se, kažemo da funkcija g ima uklonjiv singularitet u točki z_0 ako vrijedi: $\lim_{z \to z_0} \left[(z - z_0) \cdot g(z) \right] = 0$, odnosno (ekvivalentno) ako vrijedi: $Res(g; z_0) = 0$.
Mi znamo da funkcije f i F imaju polove u integerima i da su odgovarajući reziduumi:

$Res(f;-n) = Res(F;-n) = (-1)^n$, uz $(n \in \mathbb{Z})$. Iz toga slijedi:

$$\begin{aligned} Res(h;n) &= \lim_{z\to n}\Big[(z-n)\cdot h(z)\Big] = \lim_{z\to n}\Big[(z-n)\cdot (f(z)-F(z))\Big] = \\ &= \lim_{z\to n}\Big[(z-n)\cdot f(z)\Big] - \lim_{z\to n}\Big[(z-n)\cdot F(z)\Big] = (-1)^{-n} - (-1)^{-n} = 0 \end{aligned}$$

Dakle, vidimo da funkcija h ima u integerima uklonjive singularitete.

(3.6)

Sada iz tvrdnje 3.6 slijedi da je funkcija h cijela. (Prisjetimo se, za kompleksnu funkciju kažemo da je cijela ako je analitička i definirana na čitavom $\mathbb{C}$).
Skup $(0 \le x \le 1),\ (|y| \le 1)$ je kompaktan, a funkcija h je na njemu neprekidna (jer se singulariteti od f i F pokrate) pa je ona tamo i ograničena.
Dakle, h je ograničena na $(0 \le x \le 1),\ (|y| \le 1)$ i na $(0 \le x \le 1),\ (|y| \ge 1)$, pa je ograničena na čitavoj pruzi $(0 \le x \le 1)$. A kako je periodična do na predznak (jer je, prema 3.5, razlika takvih funkcija), ograničena je i na čitavom $\mathbb{C}$.
Sada iz Liouvilleovog teorema (koji kaže da je svaka ograničena cijela funkcija konstantna) slijedi da je h konstantna. Sada imamo:

$$\begin{aligned} h(z) &= [h \text{ konstantna}] = h(z+1) = \\ &= [h \text{ periodična do na predznak}] = -h(z) \end{aligned}$$

Dobili smo: $h(z) = -h(z)$ i h je konstantna pa mora vrijediti: $h \equiv 0$ iz čega slijedi tvrdnja propozicije. □

Napokon dolazimo do dokaza propozicije 2.1.2 koju smo bili spominjali u 2. poglavlju. Prisjetimo se da je tvrdnja te propozicije sljedeća:
Za sve $(x \in \mathbb{R})$ beskonačni produkt:

$$\pi x \cdot \prod_{n=1}^{\infty}\left(1 + \frac{x^2}{n^2}\right)$$

konvergira i jednak je $sh(\pi x)$.

Konvergencija:

$$\pi x \cdot \prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right) = \left[x = \mathrm{e}^{ln(x)}\right] = exp\left\{ln\left[\pi x \cdot \prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right)\right]\right\} = exp\left\{ln(\pi x) + ln\left[\prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right)\right]\right\} =$$

$$= exp\left\{ln(\pi x) + \sum_{n=1}^{\infty} ln\left(1+\frac{x^2}{n^2}\right)\right\} = \mathrm{e}^{ln(\pi x)} \cdot exp\left\{\sum_{n=1}^{\infty} ln\left(1+\frac{x^2}{n^2}\right)\right\} =$$

$$= \pi x \cdot exp\left\{\sum_{n=1}^{\infty} ln\left(1+\frac{x^2}{n^2}\right)\right\} =$$

$$< \infty$$

$$\uparrow$$

$$\pi x < \infty \quad (\forall x),$$

$$\sum_{n=1}^{\infty}\left|ln\left(1+\frac{x^2}{n^2}\right)\right| \leq \left[ln(1+x) \leq x, \ \ (\forall x \geq 0)\right] \leq \sum_{n=1}^{\infty}\left|\frac{x^2}{n^2}\right| = \sum_{n=1}^{\infty}\frac{x^2}{n^2} = x^2 \cdot \underbrace{\sum_{n=1}^{\infty}\frac{1}{n^2}}_{\substack{\text{konvergentan}\\ \text{Dirichletov}\\ \text{red}}} < \infty$$

$$\Rightarrow \quad \text{red} \quad \sum_{n=1}^{\infty} ln\left(1+\frac{x^2}{n^2}\right) \text{ konvergira apsolutno pa i obično}$$

Taj produkt iznosi $sh(\pi x)$:
Znamo:

$$\Gamma(z) = \int_0^{\infty}\left(t^{z-1}\cdot \mathrm{e}^{-t}\right)\cdot dt = \lim_{n\to\infty}\left[\int_0^{n}\left(t^{z-1}\cdot \mathrm{e}^{-t}\right)\cdot dt\right] =$$

$$= \left[\mathrm{e}^{-x} = \lim_{n\to\infty}\left(1-\frac{x}{n}\right)^n\right] = \lim_{n\to\infty}\left[\int_0^{n}\left(t^{z-1}\cdot\left(1-\frac{t}{n}\right)^n\right)\cdot dt\right] \tag{3.7}$$

$$\int_0^{n}\left(t^{z-1}\cdot\left(1-\frac{t}{n}\right)^n\right)\cdot dt = \left\{\begin{array}{ll} u = \left(1-\frac{t}{n}\right)^n & \Rightarrow \ du = n\cdot\left(1-\frac{t}{n}\right)^{n-1}\cdot\left(\frac{-1}{n}\right)\cdot dt = -\left(1-\frac{t}{n}\right)^{n-1}\cdot dt \\ dv = t^{z-1} & \Rightarrow \ v = \frac{t^z}{z} \end{array}\right\} =$$

$$= \underbrace{\left(\frac{t^z}{z}\cdot\left(1-\frac{t}{n}\right)^n\right)\Big|_0^{n}}_{=0} + \int_0^{n}\left(\frac{t^z}{z}\cdot\left(1-\frac{t}{n}\right)^{n-1}\right)\cdot dt =$$

$$= \frac{1}{z} \cdot \int_0^n \left(t^z \cdot \left(1 - \frac{t}{n}\right)^{n-1} \right) \cdot \, dt =$$

$$= \left\{ \begin{array}{ll} u = \left(1 - \frac{t}{n}\right)^{n-1} & \Rightarrow \quad du = (n-1) \cdot \left(1 - \frac{t}{n}\right)^{n-2} \cdot \left(\frac{-1}{n}\right) \cdot dt \\ dv = t^z & \Rightarrow \quad v = \frac{t^{z+1}}{z+1} \end{array} \right\} =$$

$$= \frac{1}{z} \cdot \left[\underbrace{\left(1 - \frac{t}{n}\right)^{n-1} \cdot \frac{t^{z+1}}{z+1}\Big|_0^n}_{=0} + \frac{n-1}{n(z+1)} \cdot \int_0^n \left(t^{z+1} \cdot \left(1 - \frac{t}{n}\right)^{n-2} \right) \cdot \, dt \right] =$$

$$= (...) = \frac{n}{n(z)} \cdot \frac{n-1}{n(z+1)} \cdot \frac{n-2}{n(z+2)} \cdot ... \cdot \frac{1}{n(z+n-1)} \cdot \int_0^n \left(t^{z+n-1} \right) \cdot \, dt =$$

$$= \frac{n}{n(z)} \cdot \frac{n-1}{n(z+1)} \cdot \frac{n-2}{n(z+2)} \cdot ... \cdot \frac{1}{n(z+n-1)} \cdot \left(\frac{t^{z+n}}{z+n}\Big|_0^n \right) =$$

$$= \frac{n}{n(z)} \cdot \frac{n-1}{n(z+1)} \cdot \frac{n-2}{n(z+2)} \cdot ... \cdot \frac{1}{n(z+n-1)} \cdot \left(\frac{n^{z+n}}{z+n} \right) \tag{3.8}$$

$$\Rightarrow \quad \Gamma(z) = [\,3.7\,] = \lim_{n\to\infty} \left[\int_0^n \left(t^{z-1} \cdot \left(1 - \frac{t}{n}\right)^n \right) \cdot \, dt \right] =$$

$$= [\,3.8\,] = \lim_{n\to\infty} \left[\frac{n}{n(z)} \cdot \frac{n-1}{n(z+1)} \cdot \frac{n-2}{n(z+2)} \cdot ... \cdot \frac{1}{n(z+n-1)} \cdot \frac{n^{z+n}}{z+n} \right] =$$

$$= \lim_{n\to\infty} \left[\frac{n!}{n^n} \cdot \left(\prod_{k=0}^{n-1} \frac{1}{z+k} \right) \cdot \frac{n^{z+n}}{z+n} \right] = \lim_{n\to\infty} \left[\frac{n!}{n^n} \cdot \left(\prod_{k=0}^{n} \frac{1}{z+k} \right) \cdot n^{z+n} \right] =$$

$$= \lim_{n\to\infty} \left[\frac{n!}{n^n} \cdot \frac{1}{z} \cdot \left(\prod_{k=1}^{n} \frac{1}{z+k} \right) \cdot n^z \cdot n^n \right] = \lim_{n\to\infty} \left[\frac{n^z}{z} \cdot \prod_{k=1}^{n} \frac{k}{z+k} \right] =$$

$$= \lim_{n\to\infty} \left[\frac{n^z}{z} \cdot \prod_{k=1}^{n} \frac{1}{1+\frac{z}{k}} \right] \tag{3.9}$$

$$\Rightarrow \quad \Gamma(z) \cdot \Gamma(1-z) = \Big[\Gamma(z+1) = z \cdot \Gamma(z) \;\Rightarrow\; \Gamma(1-z) = -z \cdot \Gamma(-z) \Big] = \Gamma(z) \cdot (-z) \cdot \Gamma(-z) =$$

$$= [\,3.9\,] = \lim_{n\to\infty} \left[\frac{n^z}{z} \cdot \prod_{k=1}^{n} \frac{1}{\left(1+\frac{z}{k}\right) \cdot \left(1-\frac{z}{k}\right)} \cdot (-z) \cdot \frac{n^{-z}}{-z} \right] =$$

$$= \lim_{n\to\infty} \left[\frac{1}{z} \cdot \prod_{k=1}^{n} \frac{1}{1-\frac{z^2}{k^2}} \right] = \frac{1}{z} \cdot \prod_{k=1}^{\infty} \frac{1}{1-\frac{z^2}{k^2}} \tag{3.10}$$

Sada imamo:

$$\frac{\sin(\pi z)}{\pi} = [\text{prop. } 3.2.3] = \frac{1}{\Gamma(z)\cdot\Gamma(1-z)} = [\,3.10] = z\cdot\prod_{k=1}^{\infty}\left(1-\frac{z^2}{k^2}\right)$$

$$\Rightarrow \quad \frac{\sin(\pi z)}{\pi z} = \prod_{k=1}^{\infty}\left(1-\frac{z^2}{k^2}\right) \tag{3.11}$$

$$\Rightarrow \quad \prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right) = \prod_{n=1}^{\infty}\left(1-\frac{(ix)^2}{n^2}\right) = [\,3.11] = \frac{\sin(\pi i x)}{\pi i x} =$$

$$= \left[\,\sin(x) = \sum_{n=0}^{\infty}\frac{(-1)^n\cdot x^{2n+1}}{(2n+1)!}\right] = \sum_{n=0}^{\infty}\frac{(-1)^n\cdot(\pi i x)^{2n+1}}{(2n+1)!\cdot(\pi i x)} =$$

$$= \sum_{n=0}^{\infty}\frac{(-1)^n\cdot(\pi i x)^{2n}}{(2n+1)!} = \sum_{n=0}^{\infty}\frac{(\pi x)^{2n}}{(2n+1)!} = \frac{1}{\pi x}\cdot\sum_{n=0}^{\infty}\frac{(\pi x)^{2n+1}}{(2n+1)!} = \frac{sh(\pi x)}{\pi x}$$

Time je propozicija 2.1.2 dokazana.

Bibliografija

[Freitag-Busam] E. Freitag. R. Busam. *Complex Analysis*. 2nd. Berlin, Springer, 2009.

[Koblitz] N. Koblitz. *p-adic Numbers, p-adic Analyis, and Zeta-Functions*. 2nd. New York, Springer-Verlag, 1984.

Sažetak

Ovaj se diplomski rad bavi p-adskim brojevima i pruža svojevrstan uvod u p-adsku analizu. Cilj mu je definirati polje p-adskih brojeva $\mathbb{Q}_p$ te postaviti temelje za usustavljivanje p-adskog analogona skupa kompleksnih brojeva $\mathbb{C}$. Rad je podijeljen u tri poglavlja.

Prvom poglavlje započinjemo prisjećanjem na pojmove polja, metrike, norme i metričkih prostora. Zatim uvodimo novu vrstu udaljenosti kojom ćemo se baviti kroz ostatak rada - p-adsku udaljenost. Također razlikujemo norme s obzirom na to jesu li arhimedske ili nearhimedske. Definiramo ekvivalentne norme i metrike i dokazujemo razna njihova svojstva te spominjemo teorem Ostrowskog. Potom se prisjećamo konstrukcije kompleksnih brojeva te na sličan način konstruiramo polje p-adskih brojeva $\mathbb{Q}_p$. U ostatku poglavlja proučavamo njegovu aritmetiku i dokazujemo važnu Henselovu lemu.

U drugom poglavlju proučavamo Riemannovu ζ funkciju i njenu p-adsku interpolaciju. Započinjemo definiranjem Bernoullijevih brojeva B_k koji se javljaju u formuli za $\zeta(2k)$ koju potom dokazujemo. Nadalje, promatramo topologiju na $\mathbb{Q}_p$ te uvodimo kompaktno-otvorene skupove i lokalno konstantne funkcije. Njih zatim koristimo u definiciji p-adskih distribucija te navodimo nekoliko primjera istih. Dotičemo se i Bernoullijevih polinoma $B_k(x)$ i Bernoullijevih distribucija, te uvodimo mjere i integraciju u $\mathbb{Q}_p$. Koristeći uvedene distribucije i izraze za $\zeta(2k)$, definiramo p-adske interpolacije ζ-funkcije.

U trećem poglavlju govorimo o gama funkciji. Dajemo njenu definiciju i dokaz njenih osnovnih svojstava. Pritom se prisjećamo nekih pojmova iz područja kompleksne analize poput analitičkih funkcija, polova i reziduuma. Poglavlje završavamo upotrebom gama funkcije pri dokazivanju formule za razvoj hiperbolnog sinusa u beskonačni produkt koja se bila spominjala u drugom poglavlju.

Summary

This thesis focuses on p-adic numbers and provides a sort of an introduction to the p-adic analysis. Its main goal is to define the field of p-adic numbers $\mathbb{Q}_p$ and lay the foundation for introduction of the p-adic analogue of the set of complex numbers $\mathbb{C}$. The paper is divided into three chapters.

We begin the first chapter by recalling the concepts of fields, metrics, norms, and metric spaces. Then we introduce a new type of distance that we will deal with throughout the rest of the paper, namely p-adic distance. We also distinguish norms depending on whether they are Archimedean or non-Archimedean. We define equivalent norms and metrics, prove their various properties and mention the Ostrowski theorem. Then we recall the construction of complex numbers and in a similar way we construct the field of p-adic numbers $\mathbb{Q}_p$. In the rest of the chapter we study its arithmetic and prove the important Hensel lemma.

In the second chapter we study the Riemann ζ function and its p-adic interpolation. We start by defining the Bernoulli numbers B_k that appear in the formula for $\zeta(2k)$ which we then prove. Furthermore, we observe the topology on $\mathbb{Q}_p$ and introduce compact-open sets and locally constant functions. We then use them in the definition of p-adic distributions and give a few examples. We also touch on Bernoulli polynomials $B_k(x)$ and Bernoulli distributions, and introduce measures and integration in $\mathbb{Q}_p$. Using the introduced distributions and expressions for $\zeta(2k)$, we define p-adic interpolations of the ζ-function.

In the third chapter we talk about the gamma function. We give its definition and proof of its basic properties. In doing so, we recall some concepts from the field of complex analysis such as analytical functions, poles and residues. We conclude the chapter by using the gamma function in proving the infinite product identity for hyperbolic sine that was mentioned in the second chapter.

Životopis

Rođena sam u Zagrebu 27. listopada 1996. godine. Pohađala sam Osnovnu školu Vladimir Nazor Budinšćina PŠ Hrašćina te je završila 2011. godine. Tijekom osnovne škole sudjelovala sam na natjecanjima iz matematike, engleskog jezika i povijesti. Godine 2015. završila sam opći smjer Gimnazije Antuna Gustava Matoša u Zaboku. Tijekom srednje škole sudjelovala sam na natjecanjima iz matematike, biologije i povijesti.

Godine 2015. upisala sam inženjerski smjer Preddiplomskog studija matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Godine 2019. završila sam preddiplomski studij te tako stekla titulu sveučilišne prvostupnice matematike. Potom sam na istom fakultetu upisala Diplomski sveučilišni studij Matematičke statistike koji trenutno pohađam.