UVOD V SVET p-ADIČNIH ŠTEVIL

BARBARA DRINOVEC DRNOVŠEK

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 11S80

V članku predstavimo pojem ultrametrične absolutne vrednosti in dokažemo nekaj njenih osnovnih lastnosti. Natančneje se ukvarjamo s p-adično absolutno vrednostjo na polju racionalnih števil in s p-adičnimi števili.

INTRODUCTION TO THE WORLD OF p-ADIC NUMBERS

We introduce the notion of an ultrametric absolute value on a field and present its fundamental properties. In particular, we study p-adic absolute value on the field of rational numbers and p-adic numbers.

Matematiki gradimo svoj svet iz pravil, ki jih imenujemo aksiomi. Aksiome povzamemo po lastnostih, ki jih v našem svetu pričakujemo. Če aksiome dobro izberemo, definirajo neprotislovno teorijo. Primer take teorije je evklidska geometrija. Zgodi se, da lahko katerega od aksiomov nadomestimo z drugim in dobimo drugačno neprotislovno teorijo. Na primer, če aksiom o vzporednici nadomestimo z aksiomom, ki zagotavlja, da skozi dano točko, ki ne leži na premici p, poteka več kot ena vzporednica k premici p, dobimo drugačno geometrijo, ki se imenuje *hiperbolična geometrija*.

V članku trikotniško neenakost, ki velja za običajno absolutno vrednost, nadomestimo z močnejšo lastnostjo, ki se imenuje ultrametrična lastnost. Tako dobimo absolutne vrednosti s presenetljivimi lastnostmi.

1. Absolutne vrednosti in metrike na $\mathbb{Q}$

Običajna evklidska razdalja med racionalnima številoma x in y je podana z $d(x, y) = |x - y|$ in je inducirana z običajno absolutno vrednostjo na $\mathbb{Q}$. Pravila, ki veljajo za običajno absolutno vrednost, združimo v definicijo absolutne vrednosti na poljubnem polju $\mathbb{F}$, to je na komutativnem obsegu. Seštevanje v $\mathbb{F}$ bomo označili s $+$, množenje pa s $\cdot$.

Definicija 1. Realno funkcijo $|\cdot|\colon \mathbb{F} \to \mathbb{R}$ imenujemo *absolutna vrednost*, če ima naslednje lastnosti:

(a) *nenegativnost*: $|a| \geq 0$ za vsak $a \in \mathbb{F}$;
(b) *neizrojenost*: $|a| = 0$ natanko tedaj, kadar je $a = 0$;
(c) *multiplikativnost*: $|a \cdot b| = |a||b|$ za vse $a, b \in \mathbb{F}$;
(d) *trikotniška neenakost*: $|a + b| \leq |a| + |b|$ za vse $a, b \in \mathbb{F}$.

Polje $\mathbb{F}$, na katerem je definirana absolutna vrednost $|\cdot|$, imenujemo *polje z absolutno vrednostjo*.

Označimo z $\underline{1}$ enoto za množenje v $\mathbb{F}$. Iz multiplikativnosti sledi, da je $|\underline{1}| = |\underline{1} \cdot \underline{1}| = |\underline{1}|^2$, in zaradi neizrojenosti od tod dobimo $|\underline{1}| = 1$. Hitro lahko preverimo, da je funkcija

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

absolutna vrednost na polju $\mathbb{F}$; imenujemo jo *trivialna absolutna vrednost*.

Na polju $\mathbb{F}$ z absolutno vrednostjo $|\cdot|$ definiramo preslikavo $d\colon \mathbb{F} \times \mathbb{F} \to \mathbb{R}$ s predpisom $d(a, b) = |a - b|$. Iz lastnosti (a), (b) in (d) v definiciji sledi, da je d metrika na $\mathbb{F}$. Tako postane vsako polje z absolutno vrednostjo metrični prostor.

Posebej nas bodo zanimale ultrametrične absolutne vrednosti:

Definicija 2. Naj bo $\mathbb{F}$ polje z absolutno vrednostjo $|\cdot|$. Pravimo, da je absolutna vrednost *ultrametrična*, če velja

$$|a + b| \leq \max\{|a|, |b|\} \quad \text{za vse} \quad a, b \in \mathbb{F}\,. \tag{1}$$

Ultrametrična lastnost je močnejša od trikotniške neenakosti, saj je večje od števil $|a|$ in $|b|$ gotovo manjše od njune vsote $|a| + |b|$. V nadaljevanju bomo spoznali primer ultrametrične absolutne vrednosti na polju racionalnih števil.

Naj bo n celo število in p praštevilo. Z $\operatorname{red}_p n$ označimo najvišjo potenco števila p, ki deli n. Torej velja

$$\operatorname{red}_p n = k \iff (p^k \mid n \quad \text{in} \quad p^{k+1} \nmid n)\,.$$

Racionalno število x zapišemo v obliki ulomka $x = m/n$ in definiramo $\operatorname{red}_p x = \operatorname{red}_p m - \operatorname{red}_p n$. Opazimo, da definicija ni odvisna od tega, kako x predstavimo z ulomkom. Preslikavo $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}$ definiramo s predpisom

$$|x|_p = \begin{cases} p^{-\operatorname{red}_p x}\,; & x \neq 0 \\ 0\,; & x = 0 \end{cases}\,.$$

Tako je na primer $|12|_2 = \left|2^2 \cdot 3\right|_2 = 2^{-2}$ in $\left|\frac{8}{21}\right|_3 = \left|\frac{8}{3 \cdot 7}\right|_3 = 3$.

Trditev 1. *Naj bo p praštevilo. Potem je $|\cdot|_p$ ultrametrična absolutna vrednost na polju $\mathbb{Q}$.*

Absolutno vrednost $|\cdot|_p$ imenujemo *p-adična absolutna vrednost.*

Dokaz. Lastnosti (a), (b) in (c) sledijo neposredno iz definicije. Dokažimo še lastnost (1). Izberimo poljubna $x, y \in \mathbb{Q}$. Če je katerokoli od števil $|x|_p$, $|y|_p$ ali $|x+y|_p$ enako 0, neenakost velja. Zato bomo v nadaljevanju predpostavili, da so vsa tri števila x, y in $x+y$ neničelna. Števili x in y zapišemo kot okrajšana ulomka $x = \frac{m}{n}$ in $y = \frac{k}{l}$. Potem je

$$\operatorname{red}_p(x+y) = \operatorname{red}_p \frac{ml+nk}{nl} = \operatorname{red}_p(ml+nk) - \operatorname{red}_p n - \operatorname{red}_p l\,.$$

Ker najvišja potenca, ki deli vsoto, ni manjša od najvišje potence, ki deli oba člena v vsoti, dobimo

$$\begin{aligned}\operatorname{red}_p(x+y) &\geq \min\{\operatorname{red}_p(ml), \operatorname{red}_p(nk)\} - \operatorname{red}_p n - \operatorname{red}_p l = \\ &= \min\{\operatorname{red}_p m + \operatorname{red}_p l, \operatorname{red}_p n + \operatorname{red}_p k\} - \operatorname{red}_p n - \operatorname{red}_p l = \\ &= \min\{\operatorname{red}_p m - \operatorname{red}_p n, \operatorname{red}_p k - \operatorname{red}_p l\} = \\ &= \min\left\{\operatorname{red}_p \frac{m}{n}, \operatorname{red}_p \frac{k}{l}\right\} = \min\{\operatorname{red}_p x, \operatorname{red}_p y\}\,.\end{aligned}$$

Zato je $p^{\operatorname{red}_p(x+y)} \geq \min\{p^{\operatorname{red}_p x}, p^{\operatorname{red}_p y}\}$. Sedaj upoštevamo definicijo absolutne vrednosti in dobimo

$$|x+y|_p = p^{-\operatorname{red}_p(x+y)} \leq \max\left\{p^{-\operatorname{red}_p x}, p^{-\operatorname{red}_p y}\right\} = \max\{|x|_p, |y|_p\}\,. \qquad \blacksquare$$

Pravimo, da sta absolutni vrednosti ekvivalentni, če inducirata ekvivalentni metriki. Absolutne vrednosti na polju racionalnih števil karakterizira naslednji izrek:

Izrek 2 (Ostrowski). *Netrivialna absolutna vrednost na $\mathbb{Q}$ je ekvivalentna bodisi običajni bodisi p-adični za neko praštevilo p.*

Elementaren dokaz tega izreka najdemo na primer v [3], konstrukcijo p-adične absolutne vrednosti pa v [2, 3, 4].

2. Lastnosti ultrametričnih absolutnih vrednosti

Najprej pokažimo, da v oceni (1) velja enačaj, če je $|a| \neq |b|$.

Lema 3. *Naj bo $\mathbb{F}$ polje z ultrametrično absolutno vrednostjo $|\cdot|$. Potem je vsak trikotnik v $\mathbb{F}$ enakokrak, to pomeni, da sta za poljubne elemente $a, b, c \in \mathbb{F}$ vsaj dve od števil $|a-b|$, $|b-c|$, $|c-a|$ enaki. Velja sklep*

$$|a| \neq |b| \Longrightarrow |a+b| = \max\{|a|, |b|\} \quad \textit{za vse} \quad a, b \in \mathbb{F}\,. \tag{2}$$

Dokaz. Najprej pokažimo, da iz (2) sledi, da je vsak trikotnik enakokrak. Izberimo poljubne tri elemente $a, b, c \in \mathbb{F}$ – oglišča trikotnika. Če je $|a-b| = |b-c|$, je dani trikotnik enakokrak. Sicer vzamemo $a' = a-b$ in $b' = b-c$ in iz (2) sklepamo, da je $|a-c| = |a'+b'| = \max\{|a'|, |b'|\} = \max\{|a-b|, |b-c|\}$ in spet lahko ugotovimo, da je trikotnik, ki ga razpenjajo a, b in c, enakokrak.

Dokažimo še (2). Izberimo poljubna elementa $a, b \in \mathbb{F}$ in denimo, da $|a| \neq |b|$. Predpostaviti smemo, da je

$$|a| < |b|\,,$$

sicer zamenjamo vlogi a in b. Dokazati moramo, da je $|a+b| = |b|$. Upoštevamo ultrametrično lastnost in manjše število nadomestimo z večjim

$$|a+b| \leq \max\{|a|, |b|\} = |b|\,.$$

Po preoblikovanju izraza upoštevamo ultrametrično lastnost, manjše število nadomestimo z večjim ter nazadnje upoštevamo prejšnjo oceno

$$|b| = |(a+b)-a| \leq \max\{|a+b|, |a|\} \leq \max\{|a+b|, |b|\} \leq |b|\,.$$

Ker sta začetek in konec enaka, povsod velja enačaj. Torej je $|b| = \max\{|a+b|, |a|\}$. Ker je $|a| < |b|$, lahko sklepamo, da je $|a+b| = |b|$. ∎

Osnovne lastnosti ultrametričnih absolutnih vrednosti so tema prvih poglavij v [2, 3].

Delne vsote harmonične vrste $H_m = 1 + \frac{1}{2} + \cdots + \frac{1}{m}$ imenujemo *harmonična števila*. Ker je harmonična vrsta divergentna vrsta s pozitivnimi členi, je zaporedje harmoničnih števil navzgor neomejeno. Z uporabo zgornje leme bomo na preprost način dokazali naslednjo lastnost harmoničnih števil, ki je bila prvič dokazana v [5].

Trditev 4. *Harmonično število H_m ni naravno število za noben $m \geq 2$.*

Dokaz. Ker je $m \geq 2$, obstaja največje naravno število n, za katero velja $2^n \leq m$. Potem je

$$\left|\frac{1}{2^n}\right|_2 = 2^n \quad \text{in} \quad \left|\frac{1}{k}\right|_2 < 2^n \quad \text{za vse} \quad k \in \{1, 2, \ldots, m\} \setminus \{2^n\}.$$

Zato iz ultrametrične lastnosti sledi

$$\left|H_m - \frac{1}{2^n}\right|_2 = \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{2^n - 1} + \frac{1}{2^n + 1} + \cdots + \frac{1}{m}\right|_2 \leq$$
$$\leq \max\left\{|1|_2, \left|\frac{1}{2}\right|_2, \ldots, \left|\frac{1}{2^n - 1}\right|_2, \left|\frac{1}{2^n + 1}\right|_2, \ldots, \left|\frac{1}{m}\right|_2\right\} < 2^n.$$

Sedaj pa z uporabo (2) dobimo

$$|H_m|_2 = \left|H_m - \frac{1}{2^n} + \frac{1}{2^n}\right|_2 = \max\left\{\left|H_m - \frac{1}{2^n}\right|_2, \left|\frac{1}{2^n}\right|_2\right\} = 2^n.$$

Dokazali smo, da je $|H_m|_2 > 1$, zato H_m ni naravno število. ∎

Za običajno absolutno vrednost na $\mathbb{Q}$ ali $\mathbb{R}$ pravimo, da ima *arhimedsko lastnost*; to pomeni, da za poljubni števili $x, y \in \mathbb{Q}$, $x \neq 0$, obstaja tako število $n \in \mathbb{N}$, za katero velja $|nx| > |y|$. V posebnem primeru od tod sledi, da so naravna števila poljubno velika. Definicijo lahko smiselno razširimo na katerokoli polje z absolutno vrednostjo.

V nadaljevanju tega razdelka bomo dokazali, da je absolutna vrednost, ki ni arhimedska, ultrametrična in obratno, da je absolutna vrednost, ki ni ultrametrična, arhimedska. Dokaz bomo povzeli po [2].

V vsakem polju $\mathbb{F}$ lahko zagledamo naravna števila takole: Označimo z $\underline{1}$ enoto za množenje v $\mathbb{F}$. Ker je polje $\mathbb{F}$ zaprto za seštevanje, je $\underline{1} + \underline{1} \in \mathbb{F}$ in ta element označimo z $\underline{2}$. Induktivno nadaljujemo. Denimo, da smo že konstruirali $\underline{n}$. Potem definiramo $\underline{n+1} = \underline{n} + \underline{1}$. Natančneje, konstruirali smo homomorfizem aditivne grupe $(\mathbb{Z}, +)$ v aditivno grupo $(\mathbb{F}, +)$.

Izrek 5. *Absolutna vrednost $|\cdot|$ na polju $\mathbb{F}$ je ultrametrična natanko tedaj, kadar je $|\underline{n}| \leq 1$ za vse $n \in \mathbb{N}$.*

Dokaz. Denimo, da je $|\cdot|$ ultrametrična absolutna vrednost na $\mathbb{F}$. Z indukcijo dokažimo, da je $|\underline{n}| \leq 1$ za vse $n \in \mathbb{N}$. V katerikoli absolutni vrednosti velja

$|\underline{1}| = 1$. Denimo, da je $|\underline{n}| \leq 1$ za neki $n \in \mathbb{N}$. Zaradi ultrametrične lastnosti absolutne vrednosti velja

$$|\underline{n+1}| = |\underline{n} + \underline{1}| \leq \max\{|\underline{n}|, 1\} = 1\,.$$

Torej po načelu popolne indukcije ocena velja za vse $n \in \mathbb{N}$.

Pokažimo še, da velja obratno. Denimo, da je $|\underline{n}| \leq 1$ za vse $n \in \mathbb{N}$. Dokazati moramo, da velja $|a+b| \leq \max\{|a|, |b|\}$ za vse $a, b \in \mathbb{F}$. Če je $b = 0$, neenakost velja. V nasprotnem primeru lahko delimo z b in dobimo $|\frac{a}{b} + \underline{1}| \leq \max\{|\frac{a}{b}|, 1\}$. Zato je dovolj, da dokažemo, da za vse $a \in \mathbb{F}$ velja $|a + \underline{1}| \leq \max\{|a|, 1\}$. Ker je $\mathbb{F}$ polje, velja binomska formula in zato za $a \in \mathbb{F}$ in $m \in \mathbb{N}$ velja

$$|a + \underline{1}|^m = |(a+\underline{1})^m| = \left|\sum_{k=0}^{m} \binom{m}{k} a^k\right| \leq \sum_{k=0}^{m} \left|\underline{\binom{m}{k}}\right| |a|^k.$$

Uporabimo predpostavko in opazimo, da je bodisi $|a| < 1$ bodisi $|a|^k \leq |a|^m$ za $k \leq m$, in izpeljemo

$$|a + \underline{1}|^m \leq \sum_{k=0}^{m} |a|^k \leq (m+1) \max\{1, |a|^m\}\,.$$

Od tod sledi

$$|a + \underline{1}| \leq \sqrt[m]{(m+1)}\, \max\{1, |a|\} \quad \text{za vse} \quad m \in \mathbb{N}\,, \quad a \in \mathbb{F}\,.$$

V limiti, ko pošljemo m v neskončno, dobimo

$$|a + \underline{1}| \leq \max\{1, |a|\} \quad \text{za vse} \quad a \in \mathbb{F}\,,$$

kar je bilo treba dokazati. ∎

Posledica 6. *Absolutna vrednost na polju $\mathbb{F}$ je ultrametrična natanko tedaj, kadar ni arhimedska.*

Ker je ultrametrična lastnost nasprotna arhimedski, jo pogosto imenujejo kar nearhimedska lastnost [2, 3].

Dokaz. Če je absolutna vrednost $|\cdot|$ arhimedska, potem obstaja naravno število $n \in \mathbb{N}$, za katero velja

$$|\underline{n}| = |\underline{n} \cdot \underline{1}| > |\underline{1}| = 1\,.$$

Od tod po izreku sledi, da $|\cdot|$ ni ultrametrična.

Če $|\cdot|$ ni ultrametrična, po izreku obstaja naravno število $n \in \mathbb{N}$, za katero velja $|\underline{n}| > 1$. Pokažimo, da je $|\cdot|$ arhimedska absolutna vrednost. Izberimo poljubna $a, b \in \mathbb{F}$, $a \neq 0$. Ker je $|\underline{n}| > 1$, so števila $|\underline{n}^l \cdot a| = |\underline{n}|^l |a|$ poljubno velika, če le izberemo dovolj velik $l \in \mathbb{N}$. Zato za dovolj velik l velja $|n^l a| > |b|$. Torej je $|\cdot|$ arhimedska absolutna vrednost. ∎

3. Napolnitev metričnega prostora $(\mathbb{Q}, |\cdot|_p)$

Iz analize vemo, da množica racionalnih števil $\mathbb{Q}$ z običajno metriko ni poln metrični prostor. Primer Cauchyjevega zaporedja, ki ne konvergira, je zaporedje desetiških približkov za $\sqrt{2}$. Vsak metričen prostor pa lahko vložimo v poln metričen prostor kot gost podprostor. Napolnitev metričnega prostora racionalnih števil $\mathbb{Q}$ z običajno metriko je metrični prostor realnih števil z običajno metriko. Napolnitev metričnega prostora $(\mathbb{Q}, |\cdot|_p)$ imenujemo *metrični prostor p-adičnih števil* in ga označimo s $\mathbb{Q}_p$. Oglejmo si, kdaj vrsta v tem metričnem prostoru konvergira. V primerjavi z običajno metriko v $\mathbb{R}$ je kriterij za konvergenco vrste v $\mathbb{Q}_p$ zelo preprost. Sledili bomo načinu v [3].

Izrek 7. *Naj bo p praštevilo in $\{a_n\}$ zaporedje p-adičnih števil. Potem je vrsta $\sum_{n=1}^{\infty} a_n$ konvergentna v $\mathbb{Q}_p$ natanko tedaj, kadar je $\lim_{n\to\infty} |a_n|_p = 0$.*

Dokaz. Ker so p-adična števila poln metričen prostor, je vrsta iz p-adičnih števil konvergentna natanko tedaj, kadar je zaporedje njenih delnih vsot $\{s_n\}$ Cauchyjevo.

Vzamemo $n > m$ in z upoštevanjem ultrametrične lastnosti p-adične absolutne vrednosti dobimo

$$|s_n - s_m|_p = |a_n + a_{n-1} + \cdots + a_{m+1}|_p \leq \max\{|a_n|_p, |a_{n-1}|_p, \ldots, |a_{m+1}|_p\}.$$

Če je $\lim_{n\to\infty} |a_n|_p = 0$, od tod sledi, da je zaporedje $\{s_n\}$ Cauchyjevo.

Denimo, da zaporedje $\{|a_n|_p\}$ ne konvergira k 0. Izberimo poljuben $\epsilon > 0$. Potem za vsak še tako velik n_0 obstaja $n > n_0$, da je $|a_n|_p > \epsilon$. Torej je

$$|s_n - s_{n-1}|_p = |a_n|_p > \epsilon$$

in zato zaporedje $\{s_n\}$ ni Cauchyjevo. ∎

Posledica 8. *Naj bo p praštevilo, $m \in \mathbb{Z}$ in $a_n \in \{0, 1, \ldots, p-1\}$ za $n \geq m$. Potem vrsta $\sum_{n=m}^{\infty} a_n p^n$ konvergira v $\mathbb{Q}_p$.*

Dokaz. Izračunajmo absolutno vrednost neničelnega člena v vrsti $|a_n p^n|_p = p^{-n}$. Torej zaporedje absolutnih vrednosti členov v vrsti konvergira proti 0, zato po izreku vrsta konvergira. ∎

Primer. Vrsta $\sum_{n=1}^{\infty} 5^n$ je po posledici konvergentna v $\mathbb{Q}_5$. Poenostavimo njeno delno vsoto

$$s_m = 1 + 5 + \cdots + 5^m = \frac{5^{m+1} - 1}{5 - 1} = \frac{5^{m+1}}{4} - \frac{1}{4}.$$

Ker je $\lim_{m\to\infty} \left|\frac{5^{m+1}}{4}\right|_5 = \lim_{m\to\infty} 5^{-m-1} = 0$, zaporedje $\{s_m\}$ v metričnem prostoru p-adičnih števil konvergira k $-\frac{1}{4}$. Zato je vsota dane vrste $-\frac{1}{4}$.

V nadaljevanju bomo vsako p-adično število predstavili kot vsoto take vrste. Vemo, da lahko vsako realno število zapišemo v decimalni obliki, to je pravzaprav v obliki vrste: $x \in \mathbb{R}$ zapišemo v decimalni obliki

$$x = d{,}d_1 d_2 \ldots = d + \sum_{j=1}^{\infty} d_j 10^{-j}, \quad \text{kjer je} \quad d_j \in \{0, 1, \ldots, 9\}.$$

Drugače od decimalnega zapisa, ki ni enoličen, je razvoj p-adičnih števil v vrsto enoličen.

Izrek 9. *Naj bo p praštevilo in $\alpha \in \mathbb{Q}_p$. Potem obstajajo enolično določena števila $m \in \mathbb{Z}$ in $a_n \in \{0, 1, \ldots, p-1\}$ za $n \geq m$, za katera velja*

$$\alpha = \sum_{n=m}^{\infty} a_n p^n.$$

Dokažimo pomožno lemo.

Lema 10. *Naj bo p praštevilo in $\alpha \in \mathbb{Q}_p$, za katerega je $|\alpha|_p \leq 1$. Potem obstaja število $a \in \{0, 1, \ldots, p-1\}$, za katero je $|\alpha - a|_p \leq \frac{1}{p}$.*

Dokaz. Lemo najprej dokažemo v primeru, da je α racionalno število. Potem lahko α zapišemo kot okrajšan ulomek $\alpha = \frac{k}{l}$. Ker je $\left|\frac{k}{l}\right|_p \leq 1$, p ne deli l, in ker je p praštevilo, sta si števili p in l tuji. Zato obstajata celi števili $s, t \in \mathbb{Z}$, za kateri velja $sl + tp = 1$. Označimo z a ostanek števila ks pri deljenju s p, tj. $ks = mp + a$, kjer je $m \in \mathbb{Z}$ in $a \in \{0, 1, \ldots, p-1\}$. Po definiciji p-adične absolutne vrednosti izračunamo

$$\left|\frac{k}{l} - ks\right|_p = \left|\frac{k}{l}\right|_p |1 - sl|_p = \left|\frac{k}{l}\right|_p |tp|_p \leq |t|_p \frac{1}{p} \leq \frac{1}{p}\,.$$

Upoštevamo ultrametrično lastnost in dobimo

$$|\alpha - a|_p = \left|\frac{k}{l} - ks + mp\right|_p \leq \max\left\{\left|\frac{k}{l} - ks\right|_p, |mp|_p\right\} \leq \frac{1}{p}\,.$$

S tem je za racionalne α lema dokazana.

Sedaj izberemo poljuben $\alpha \in \mathbb{Q}_p$, za katerega je $|\alpha|_p \leq 1$. Ker je metrični prostor p-adičnih števil napolnitev metričnega prostora racionalnih števil s p-adično metriko, lahko poljubno blizu p-adičnemu številu najdemo racionalno število. Zato obstaja racionalno število $\beta \in \mathbb{Q}$, za katero velja $|\alpha - \beta|_p \leq \frac{1}{p}$. Z upoštevanjem ultrametrične lastnosti p-adične absolutne vrednosti dobimo $|\beta|_p = |\beta - \alpha + \alpha|_p \leq \max\{|\alpha - \beta|_p, |\alpha|_p\} \leq 1$. Po že dokazanem obstaja $a \in \{0, 1, \ldots, p-1\}$, za katerega je $|\beta - a|_p \leq \frac{1}{p}$. Še enkrat uporabimo ultrametrično lastnost absolutne vrednosti in dobimo

$$|\alpha - a|_p = |\alpha - \beta + \beta - a|_p \leq \max\{|\alpha - \beta|_p, |\beta - a|_p\} \leq \frac{1}{p}\,. \qquad \blacksquare$$

Dokaz (izreka 9). Najprej bomo dokazali obstoj razvoja p-adičnega števila v vrsto in nato enoličnost tega zapisa. Denimo, da je $|\alpha|_p \leq 1$. Števila a_n konstruiramo induktivno. Po lemi obstaja $a_0 \in \{0, 1, \ldots, p-1\}$, za katerega je

$$|\alpha - a_0|_p \leq \frac{1}{p}\,.$$

Denimo, da smo že konstruirali $a_0, a_1, \ldots, a_m \in \{0, 1, \ldots, p-1\}$, za katere je

$$\left|\alpha - \sum_{n=0}^{m} a_n p^n\right|_p \leq \frac{1}{p^{m+1}}\,. \tag{3}$$

Potem je $\left|p^{-(m+1)}\alpha - \sum_{n=0}^{m} a_n p^{n-m-1}\right|_p \leq 1$ in po lemi obstaja $a_{m+1} \in \{0, 1, \ldots, p-1\}$, za katerega je $\left|p^{-(m+1)}\alpha - \sum_{n=0}^{m} a_n p^{n-m-1} - a_{m+1}\right|_p \leq \frac{1}{p}$, to pomeni, da je

$$\left|\alpha - \sum_{n=0}^{m} a_n p^n - a_{m+1}p^{m+1}\right|_p \leq \frac{1}{p^{m+2}}\,,$$

kar zaključi induktivno konstrukcijo. Iz posledice 8 sledi, da je vrsta $\sum_{n=0}^{\infty} a_n p^n$ konvergentna, in iz ocene (3), da je njena vsota enaka α.

Če je $|\alpha|_p > 1$, obstaja celo število m, za katero je $|p^m\alpha| \leq 1$, in iz razvoja števila $p^m\alpha$ dobimo ustrezni razvoj za α.

Dokažimo še enoličnost. Predpostavimo, da ima α dva različna razvoja v vrsto: $\alpha = \sum_{n=m}^{\infty} a_n p^n = \sum_{n=l}^{\infty} b_n p^n$. Definirajmo $a_k = 0$ za $k < m$ in $b_k = 0$ za $k < l$. Označimo s k_0 najmanjši indeks, za katerega sta števili a_k in b_k različni. Razliko $d = \left|\sum_{n=-\infty}^{k_0} a_n p^n - \sum_{n=-\infty}^{k_0} b_n p^n\right|_p$ izračunamo na dva načina. Ker je k_0 najmanjši indeks, za katerega sta števili a_k in b_k različni, je $d = \left|(a_{k_0} - b_{k_0})p^{k_0}\right|_p = p^{-k_0}$. Po drugi strani pa upoštevamo ultrametrično lastnost in dobimo

$$\begin{aligned} d &= \left|\sum_{n=-\infty}^{k_0} a_n p^n - \sum_{n=-\infty}^{k_0} b_n p^n\right|_p = \left|\sum_{n=m}^{k_0} a_n p^n - \alpha + \alpha - \sum_{n=l}^{k_0} b_n p^n\right|_p \leq \\ &\leq \max\left\{\left|\sum_{n=m}^{k_0} a_n p^n - \alpha\right|_p, \left|\alpha - \sum_{n=l}^{k_0} b_n p^n\right|_p\right\} = \\ &= \max\left\{\left|\sum_{n=k_0+1}^{\infty} a_n p^n\right|_p, \left|\sum_{n=k_0+1}^{\infty} b_n p^n\right|_p\right\} < \frac{1}{p^{k_0}}\,, \end{aligned}$$

kar je protislovje. Torej je zapis enoličen. ∎

Trditev 11. *Naj bo p praštevilo.*

(a) Množica p-adičnih števil $\mathbb{Q}_p$ je neštevna, zato je množica racionalnih števil njena prava podmnožica.

(b) Polje $\mathbb{Q}_p$ ni algebraično zaprto.

Dokaz. (a) Spomnimo bralca, da neštevnost množice realnih števil dokažemo z uporabo Cantorjevega diagonalnega trika. Predpostavimo, da je množica realnih števil števna; realna števila zapišemo v zaporedje in konstruiramo realno število, ki se na n-tem decimalnem mestu razlikuje od n-tega člena v zaporedju. To realno število ni člen zaporedja, kar je protislovje.

Podobno dokažemo, da množica vrst $\alpha = \sum_{n=m}^{\infty} a_n p^n$, kjer je $a_n \in \{0, 1, \ldots, p-1\}$ za $n \geq m$, ni števna. Ker je množica racionalnih števil števna, je njena prava podmnožica.

(b) V polju $\mathbb{Q}_p$ polinom $q(x) = x^2 - p$ nima ničel: denimo, da je $x \in \mathbb{Q}_p$ ničla polinoma q. Potem je $|x|_p = p^k$ za neki $k \in \mathbb{Z}$. Ker je x rešitev enačbe $x^2 = p$, je $|x|_p^2 = |p|_p$, od koder sledi $p^{2k} = p^{-1}$, kar je nemogoče. Torej polinom q v polju $\mathbb{Q}_p$ nima ničel, zato polje $\mathbb{Q}_p$ ni algebraično zaprto. ∎

Kot zanimivost omenimo, da lahko p-adično absolutno vrednost razširimo na algebraično zaprtje polja $\mathbb{Q}_p$, vendar to polje ni poln metričen prostor; šele njegova napolnitev $\mathbb{C}_p$ ustreza polju kompleksnih števil z običajno absolutno vrednostjo. Zahtevnejši bralec si o tem lahko prebere v [4].

LITERATURA

[1] Andrew Baker, *An Introduction to p-adic Numbers and p-adic Analysis*, 2007, http://www.maths.gla.ac.uk/~ajb/dvi-ps/padicnotes.pdf.

[2] Fernando Q. Gouvêa, *p-adic numbers. An introduction*, 2. izdaja, Universitext, Springer-Verlag, Berlin, 1997.

[3] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2. izdaja, Graduate Texts in Mathematics 58, Springer-Verlag, New York, 1984.

[4] Alain M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics 198, Springer-Verlag, New York, 2000.

[5] Leopold Theisinger, *Bemerkung über die harmonische Reihe*, Monatsh. Math. Phys. **26** (1915), str. 132–134.

[6] Jože Vrabec, *Metrični prostori*, Matematika – fizika 31, DMFA, Ljubljana, 1990.