# Jednadžbe u p-adskim brojevima

**Dublec, Dragana**

**Master's thesis / Diplomski rad**

**2016**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:217:897113

**SVEUČILIŠTE U ZAGREBU**
**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**
**MATEMATIČKI ODSJEK**

Dragana Dublec

# JEDNADžBE U $P$-ADSKIM BROJEVIMA

Diplomski rad

Voditelj rada:
izv. prof. dr. sc Filip Najman

Zagreb, studeni, 2016.

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. _____

*Zahvaljujem svome mentoru izv. prof. dr. dc Filipu Najmanu na zanimljivoj temi, pomoći, razumijevanju i strpljenju. Veliko hvala mojoj obitelji i prijateljima koji su mi pružali veliku podršku tijekom pisanja ovoga rada, kao i cjelokupnog studiranja.*

# Sadržaj

# Uvod

Glavni cilj ovoga rada je rješavanje jednadžbi čiji su koeficijenti i nepoznanice $p$-adski cijeli brojevi, te kako od rješenja modulo $p$ doći do pravoga rješenja takve jednadžbe.

U prvom poglavlju ćemo se baviti $p$-adskim poljima i $p$-adskim brojevima, pri čemu je $p$ prost broj. Na početku ćemo promatrati analogiju između prstena cijelih brojeva, $\mathbb{Z}$, zajedno s poljem razlomaka $\mathbb{Q}$ i prstenom polinoma s koeficijentima iz skupa kompleksih brojeva, $\mathbb{C}[X]$, zajedno s poljem razlomaka od $\mathbb{C}[X]$ koja je bila glavna motivacija Henselu za uvođenje $p$-adskih brojeva. Nakon toga definirati ćemo prsten $\mathbb{Z}_p$ i $p$-adske cijele brojeve, te polje $\mathbb{Q}_p$ i $p$-adske brojeve. Zatim promotriti i neka svojstva koja vrijede u prstenu $\mathbb{Z}_p$ i polju $\mathbb{Q}_p$ koja nam mogu pomoći pri rješavanju jednadžbi čiji su koeficijenti $p$-adski cijeli brojevi. Nakon toga pozabavit ćemo se $p$-adskom apsolutnom vrijednošću koju smo definirali na sljedeći način: $|x|_p = \left\{ \begin{array}{ll} p^{-v_p} & \text{za } x \neq 0 \\ 0 & \text{za } x = 0 \end{array} \right\}$ pri čemu se $x$ može prikazati u oblik $x = p^{v_p}\frac{n}{m}$, gdje je $v_p, n \in \mathbb{Z}$, a $m$ je pozitivan cijeli broj te vrijedi da su $m, n$ s $p$ realativno prosti brojevi, tj. $(p, n) = 1, (p, m) = 1$, a s $v_p$ smo označili $p$-adsku valuaciju. Pokazat ćemo kako i uz pomoć tako definirane $p$-adske apsolutne vrijednosti možemo definirati presten $\mathbb{Z}_p$ i polje $\mathbb{Q}_p$. Zatim ćemo iskazati i dokazati teorem Ostrowskog koji nam kaže da je svaka netrijvijalna apsoluna vrijednost na $\mathbb{Q}$ ekvivalnetna običnoj apsolutnoj vrijednosti ili p-adskoj apsolutnoj vrijednosti za neki prost broj $p$. Na kraju poglavlja dati ćemo kratki pregled zanimljivih "dobrih" i "loših" svojstva $p$-adskih brojeva, neka od njih ćemo i dokazati.

U drugom poglavlju ćemo na početku prikazati kako zbrajamo, oduzimmao i množimo u polju $\mathbb{Q}_p$, te pokazati da postoji drugi korijen od $a = a_0 + a_1p + a_2p^2 + \cdots \in \mathbb{Z}_p^x$ ako je $a_0$ kvadratni ostatak (mod $p$), gdje je je $b = b_0 + b_1p + b_2p^2 + \cdots \in \mathbb{Z}_p$. Zatim ćemo riješiti konkretne primjere kongruencija modulo $p^n$, te prikazati način rješavanja opće kongruencije $x^2 \equiv a (\text{mod } p^n)$, gdje je $p$ neparan prost broja, a $a$ neki cijeli broj koji je relativno prost s $p$. Nakon toga promatrat ćemo vezu između nultočaka polinoma s koeficijentima u $\mathbb{Z}_p$ i polinoma dobivenih redukcijom ( mod $p^n$),

čiji su koeficijenti u $A_n = \mathbb{Z}/p^n\mathbb{Z}$. Zatim ćemo pokazati kako od rješenja $p$-adskih jednadžbi (mod $p^n$) doći do pravih rješenja, s koeficijentima u $\mathbb{Z}_p$.

U posljednjem poglavlju prikazati ćemo gdje se koriste $p$-adski brojevi za koje se u početku mislilo da neće imati primjenu u stvarnom svijetu. Iskazati i dokazati ćemo Strassmannov teorem koji ističe razliku između realne i $p$-adske analize.

# Poglavlje 1

# $p$-adski brojevi

U ovom poglavlju ćemo prvo definirati $p$-adske cijele brojeve, a zatim i prsten $p$-adskih cijelih brojeva, $\mathbb{Z}_p$, i polje njegovih razlomaka, $\mathbb{Q}_p$, te promotriti neka njihova svojstva. Nadalje, odredit ćemo $p$-adsku valuaciju broja te promotrit ćemo $p$-adsku apsolutnu vrijednost brojeva. Nakon toga ćemo iskaziti i dokazati teorem Ostrowskog za racionalne brojeva. Na kraju ovoga poglavlja pogledati ćemo još neka "dobra" i "loša" svojstva p-adskih brojeva.

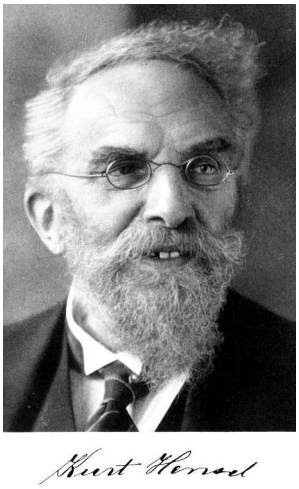
U cijelom diplomskom radu slovo $p$ označava prost broj.

## 1.1 Henselova analogija

U ovome potpoglavlju ukratko ćemo se upoznati s Kurtom Henselom te motivacijom za uvođenje $p$-adskih brojeva.

$p$-adske brojeve uveo je njemački matematičar Kurt Hensel krajem 19. stoljeća. Kurt Hensel rođen je 29.12.1861. godine u Konigsbergu u Pruskoj (danas poznatom kao Kaljingradu u Rusiji), a umro je 1.6.1941. u Marburg u Njemačkoj. Matematiku je studirao u Berlinu i Bonnu, gdje su mu predavali neki od najpoznatijih matematičara 19. stoljeća. Neki od njih su Lipschitz, Weierstrass, Borchardt, Kirchhoff, Helmholtz i Kronecker. Najveći utjecaj na Hensela imao je Kronecker pod čijem je mentorstvom doktorirao na Sveučilištu u Berlinu. Bavio se teorijom brojeva i algebrom.

Glavna motivacija za uvođenje $p$-adskih brojeva mu je bila analogija između prstena cijelih brojeva, $\mathbb{Z}$, zajedno s poljem razlomaka $\mathbb{Q}$ i prstenom polinoma s koeficijentima iz skupa kompleksih brojeva, $\mathbb{C}[X]$, zajedno s poljem razlomaka $\mathbb{C}[X]$. Naime, prsten $\mathbb{Z}$ i prsten $\mathbb{C}[X]$ imaju jedinstvenu faktorizaciju. Bilo koji cijeli broj možemo prikazati kao umnožak prostih brojeva, a bilo koji polinom možemo izraziti




Slika 1.1: K.Hensel (1861.-1941.)

na jednistveni način kao

$$P(X) = a(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n),$$

gdje su $a, \alpha_1, \alpha_2, \dots \alpha_n$ kompleksni brojevi. Dakle, glavna analogija koju je Hensel istraživao je: prosti cijeli brojevi $p \in \mathbb{Z}$, su analgoni linearnih polinoma $X - \alpha \in \mathbb{C}[X]$. Neka imamo polinom $P(X)$ i $\alpha \in \mathbb{C}$, tada ga možemo (Taylorovim razvojem) zapisati u obliku

$$P(X) = \sum_{i=0}^{n} a_i (X - \alpha)^i, a_i \in \mathbb{C}.$$

Analogno, možemo zapisati i cijele brojeve. Neka je $m$ pozitivan cijeli broj, a $p$ prost broj. Tada možemo broj $m$ zapisati u "u bazi $p$" kao

$$m = \sum_{i=0}^{n} a_i p^i, a_i \in \mathbb{Z},$$

pri čemu je $0 \leq a_i \leq p - 1$.

Razlog zašto je zanimljivo promatrati takav razvoj je to što nam daje "lokalne" informacije, tj. u takvom razvoju potencija od $(X - \alpha)$ pokazuje je su li $\alpha$ nultočke polinom $P(X)$, i to kojeg reda. Slično je i kod cijelih brojeva, razvoj u bazi $p$ pokazat će nam je li $m$ dijeljiv s $p$, i to s kojim redom.

Nadalje, možemo promatrati i Laurentov razvoj

$$f(X) = \sum_{i \leq n_0} a_i (X - \alpha)^i,$$

tako bilo koja racionalna funkcija može biti proširena u red ovakve vrste u odnosu na svaki "prosti" $(X - \alpha)$. S algebarske točke gledišta imamo dva polja, polje svih racionalnih funkcija, $\mathbb{C}[X]$, i polje $\mathbb{C}((X - \alpha))$ koje se sastoji od svih Laurentovih redova u $(X - \alpha)$. Tada funkcija

$$f(x) \to \text{proširena oko } (X - \alpha)$$

definira upotpunjenje polja

$$\mathbb{C}(X) \to \mathbb{C}((X - \alpha)).$$

Točnije rečeno, Henselova ideja je bila proširiti analogiju između $\mathbb{Z}$ i $\mathbb{C}[X]$ uključujući i izgradnju takvih proširenja. Podsjetimo se da je izbor $\alpha$ analogan izboru prostog broja $p$. Sada već znamo kako izgleda proširenje za pozitivan cijeli broj $m$, prikažemo ga samo u bazi $p$. To možemo proširiti i na racionalne brojeve

$$x = \frac{a}{b} = \sum_{n \leq n_0} a_n p^n$$

tako dobijemo za svaki racionalni broj $x$ konačan jednostrani Laurentov red u potencijama $p$, koje ćemo zvati ***p-adska proširenja od*** $x$ .

S obzirom da je skup svih konačnih jednostranih Laurentovih redova u potenciji $p$ polje, označeno s $\mathbb{Q}_p$, da smo na sličan način dobili funkciju

$$f(x) \to \text{proširena oko } (X - \alpha)$$

koja definira upotpunjenje polja

$$\mathbb{Q} \to \mathbb{Q}_p.$$

Dakle, Henselova ideja o analogiji se pokazala ostvarivom.

## 1.2 Prsten $\mathbb{Z}_p$ i polje $\mathbb{Q}_p$

U ovome potpoglavlju izreći ćemo osnovne definicije i svojstva prstena cijelih brojeva, $\mathbb{Z}_p$, i polja njegovih razlomaka, $\mathbb{Q}_p$.

Za početak prisjetimo se na koji način zapisujemo cijeli broj u nekoj bazi, npr. zapišimo broj 22 u bazi 3. Kako bi to mogli učiniti prisjetimo se teorema o dijeljenju s ostatkom.

**Teorem 1.2.1.** *Za proizvoljan prirodan broj $a$ i cijeli broj $b$ postoje jedinstveni cijeli brojevi $q$ i $r$ takvi da je $b = qa + r, 0 \leq r < a$.*

Dakle, imamo sljedeće:

$$22 = 7 \cdot 3 + 1$$

$$7 = 2 \cdot 3 + 1$$

$$2 = 0 \cdot 3 + 2$$

Zapis broja 22 u bazi 3 je $211_{(3)}$. Odnosno, imamo da je $22 = 1 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2$. Na taj način smo broj 22 zapisali u bazi 3.
Općenito, svaki cijeli broj možemo zapisati u bilo kojoj bazi, pa tako i u bazi $p$ gdje $p$ označava neki prosti broj.

Neka je $p$ prost broj. Dani cijeli broj $n$ možemo zapisati u bazi $p$:

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k, 0 \leq a_i < p.$$

Na sličan način ćemo definirati $p$-adski cijeli broj.

**Definicija 1.2.2.** *$p$-adski cijeli broj je (formalni) red*

$$a = a_0 + a_1 p + a_2 p^2 + \ldots$$

*gdje je $0 \leq a < p$.*

Skup $p$-adskih cijelih brojeva označavamo sa $\mathbb{Z}_p$. Ako bi neki element $\alpha \in \mathbb{Z}_p$ smanjili na njegovu $k$-ati izraz

$$\alpha_k = a_0 + a_1 p + \cdots + a_{k-1} p^{k-1}$$

dobili bi dobro definirani element iz skupa $\mathbb{Z}/p^k\mathbb{Z}$. Na taj način smo dobili preslikavanje

$$\mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$$

Niz od $\alpha_k$ za $k > 0$, takav da je $\alpha_k \bmod p^{k'} \equiv \alpha_{k'}$ za svaki $k' < k$ definira jedinstveni $p$-adski cijeli broj $\alpha \in \mathbb{Z}$ ( ako počinjemo s $k = 1, \alpha_1 = a_0$, tada za $k = 2$, trebamo imati $\alpha_2 = a_0 + a_1 p$ da bi to bila parcijalna suma dosljedna $\alpha_1$). Na taj način smo dobili bijekciju

$$\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^k\mathbb{Z}.$$

Limes kod kojega je strijelica okrenuta nalijevo nazivamo *inverzni* ili *projektivni* limes. Dakle, ovdje imamo inverzni (projektivni) limes prstenova (obzirom da je $\mathbb{Z}/p^k\mathbb{Z}$ prsten).

Matematički to sve možemo zapisati na sljedeći način.

Neka je $A_n = \mathbb{Z}/p^n\mathbb{Z}$, za svaki $n \geq 1$, prsten klasa cijelih brojeva ($\bmod p^n$). Tada možemo definirati preslikavanje $\phi_n : A_n \to A_{n-1}, n \geq 2$, na sljedeći način:
$\phi_n(a) = a(\bmod\ p^{n-1}), \forall a \in A_n$. Tako definirano preslikavanje očigledno je surjekcija te mu je jezgra $p^{n-1}A_n$. Lako se dokaže da je to preslikavanje je homomorfizam. Po definiciji homomorfizma trebamo provjeriti vrijede li sljedeće jednakosti:

- $\phi_n(a + b) = \phi_n(a) + \phi_n(b), \forall a, b \in A_n$
- $\phi_n(a \cdot b) = \phi_n(a) \cdot \phi_n(b), \forall a, b \in A_n$
- $\phi_n(1_{A_n}) = 1_{A_{n-1}}$

Uzmimo $a, b \in A_n$. Pogledajmo vrijede li prethodne jednakosti.
$\phi_n(a + b) =$ {po definiciji $\phi_n$}$= a + b(\bmod\ p^{n-1}) \equiv$ {po svojstvu kongurencije: za $\forall x, y \in \mathbb{Z}$, $x + y(\bmod\ m) \equiv x(\bmod\ m) + y(\bmod\ m)$}$\equiv a(\bmod\ p^{n-1}) + b(\bmod\ p^{n-1}) =$ {po definiciji $\phi_n$}$= \phi_n(a) + \phi_n(b)$

$\phi_n(a \cdot b) =$ {po definiciji $\phi_n$}$= a \cdot b(\bmod\ p^{n-1}) \equiv$ {po svojstvu kongurencije: za $\forall x, y \in \mathbb{Z}, x \cdot y(\bmod\ m) \equiv x(\bmod\ m) \cdot y(\bmod\ m)$}$\equiv a(\bmod\ p^{n-1}) \cdot b(\bmod\ p^{n-1}) =$ {po definiciji $\phi_n$}$= \phi_n(a) \cdot \phi_n(b)$

$\phi_n(1_{A_n}) = 1(\bmod\ p^{n-1}) = 1_{A_{n-1}}$

Dakle, dokazali smo da je vrijede sve tri jednakosti pa je to preslikavanje homomorfizam.

Tada niz

$$\ldots \to A_n \to A_{n-1} \to \ldots \to A_2 \to A_1$$

s odgovarajućim homomorfizmima formira "projektivni (inverzni) sistem", indeksiran prirodnim brojevima.

**Definicija 1.2.3.** *Prsten p-adskih cijelih brojeva $\mathbb{Z}_p$ je projektivni (inverzni) limes sistema $(A_n, \phi_n)$ definiranog kao gore.*

Iz definicije možemo vidjeti da je element prstena $\mathbb{Z}_p = \varprojlim(A_n, \phi_n)$ niz $x = (\ldots, x_n, x_{n-1}, \ldots, x_2, x_1)$, pri čemu je $x_n \in A_n$, za $\forall n \geq 1$ i $\phi_n(x_n) = x_{n-1}$, za $\forall n \geq 2$. Obzirom na to, možemo zaključiti da je zbrajanje i množenje u prstenu $\mathbb{Z}_p$ definirani, standarno, po koordinatama. Kako zbrajamo i množimo brojeve u $\mathbb{Z}_p$ vidjet ćemo u idućem poglavlju. Dakle, drugim riječima prsten $\mathbb{Z}_p$ je potprsten direktnog produkta $\prod_{n\geq 1} A_n$ s navedenim svojstvima.

Nadalje, ispitajmo i neka svojstva prstena $\mathbb{Z}_p$ koja će nam koristiti pri rješavanju jednadžbi.

Neka je $\epsilon : \mathbb{Z}_p \to A_n$ funkcija definirana na sljedeći način:

$$\epsilon_n(x) = x_n,$$

za $x \in \mathbb{Z}_p$.

**Definicija 1.2.4.** *Za niz grupa i homomorfizama*

$$\cdots \to G_{n+1} \overset{f_{n+1}}{\to} G_n \overset{f_n}{\to} G_{n-1} \to \cdots$$

*kažemo da je egzaktan ako je je* $\operatorname{Im} f_{n+1} = \operatorname{Ker} f_n$ *za sve* $n$.

Niz

$$0 \to A \overset{\alpha}{\to} B \overset{\beta}{\to} C \to 0$$

je egzaktan ako i samo ako je $\alpha$ monomorfizam, $\beta$ epimorfizam i $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. Tada $\beta$ inducira izomorfizam $C \cong B/\operatorname{Im}\alpha$. Takav se niz naziva kratki egzaktni niz.

**Propozicija 1.2.5.** *Niz* $0 \to \mathbb{Z}_p \overset{p^n}{\to} \mathbb{Z}_p \overset{\epsilon_n}{\to} A_n \to 0$ *je egzaktni niz Abelovih grupa.*

*Dokaz.* Kako bismo dokazali prethodnu propoziciju, po definiciji egzaktnog niza, trebamo provjeriti vrijede li sljedeće jednakosti:

1. $\operatorname{Ker}(p^n) = 0$
2. $\operatorname{Im}(p^n) = \operatorname{Ker}(\epsilon_n)$
3. $\operatorname{Im}(\epsilon_n) = A_n$

Dokažimo da jednakosti vrijede.

1. Da bi dokazali jednakost $\operatorname{Ker}(p^n) = 0$ prvo moramo dokazati da je množenje s $p$ u prstenu $\mathbb{Z}_p$ injektivno. Iz toga nam odmah slijedi da je i množenje sa $p^n$ injektivno u $\mathbb{Z}_p$, odnosno da vrijedi jednakost. Uzmimo neki $x = (x_n) \in \mathbb{Z}_p$ takav da je $px = 0$. Kako bismo dokazali traženu injektivnost, trebamo pokazati da je tada $x = 0$. Iz

$px = 0$ slijedi nam da je $px_{n+1} = 0, \forall n$. Sada je očito da je $x_{n+1} = p^n y_{n+1}$, za neki $y_{n+1} \in A_n$. Dakle, imamo:

$$x_n = \phi_{n+1}(x_{n+1}) = \phi_{n+1}(p^n y_{n+1}) = 0$$

jer je $\phi_{n+1}$ homomorfizam s jezgrom $p^n A_{n+1}$. Dakle, za $\forall n$ vrijedi da je $x_n = 0$ pa je onda i $x = 0$, čime smo dokazali tvrdnju, tj. vrijedi da je $\mathrm{Ker}(p^n) = 0$.

2. Znamo da je $\mathrm{Im}(p^n) = p^n\mathbb{Z}_p$. Dakle, element iz $\mathrm{Im}(p^n)$ je oblika $p^n x$, gdje je $x = (x_n) \in \mathbb{Z}_p$. Uzmimo neki element $p^n x \in \mathrm{Im}(p^n)$. Tada je $\epsilon_n(p^n x) = p^n x_n = 0$, tj. $\mathrm{Im}(p^n) \subseteq \mathrm{Ker}(\epsilon_n)$.

Obratno, ako je $x = (x_m) \in \mathrm{Ker}(\epsilon_m)$, imamo $x_m = 0$ u $A_m$, odnosno $p^m$ dijeli $x_m$. Iz toga slijedi da je $x_m \equiv 0 (\mathrm{mod} p^n), \forall m \geq n$. Znači, postoji dobro definiran $y_{m-n} \in A_{m-n}$ takav da je njegova slika po izomorfizmu $A_{m-n} \to p^n\mathbb{Z}/p^m\mathbb{Z} \subset A_m$ zadovoljava $x_m = p^n y_{m-n}$. Ti $y_i$ definiraju element $y$ iz $\mathbb{Z}_p = \varprojlim A_i$, i odmah možemo vidjeti da je $p^n y = x$, odnosno da je $x \in p^n\mathbb{Z}_p = \mathrm{Im}(p^n)$. Dakle, $\mathrm{Ker}(\epsilon_n) \supseteq \mathrm{Im}(p^n)$.

Pokazali smo da je $\mathrm{Im}(p^n) \subseteq \mathrm{Ker}(\epsilon_n)$ i da je $\mathrm{Ker}(\epsilon_n) \supseteq \mathrm{Im}(p^n)$. Dakle, $\mathrm{Im}(p^n) = \mathrm{Ker}(\epsilon_n)$.

3. Istinitost treće jednakosti je očigledna. Preslikavanje $\epsilon_n$ je surjekcija, stoga je $\mathrm{Im}(\epsilon_n) = A_n$. Dakle, tvrdnja vrijedi.

Dokazali smo da vrijede sve tri jednakosti čime je propozicija u potpunosti dokazana.

□

Obzirom da je promatrani egzaktni niz kratki egzaktni niz Abelovih grupa, vrijedi:

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong A_n,$$

odnosno

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z},$$

stoga možemo identificirati $\mathbb{Z}_p/p^n\mathbb{Z}_p$ sa $\mathbb{Z}/p^n\mathbb{Z}$.

Sljedeća propozicija nam govori koji su invertibilni elementi u $\mathbb{Z}_p$ te o prikazu bilo kojeg elementa iz $\mathbb{Z}_p$ pomoću njih.

**Propozicija 1.2.6.** *(a) Da bi neki element iz $\mathbb{Z}_p$ (odnosno iz $A_n$) bio invertibilan nužno i dovoljno je da nije dijeljiv s $p$.*

*(b) Ako s $\mathbb{U}$ označimo grupu invertibilnih elemenata iz $\mathbb{Z}_p$, tada svaki element iz $\mathbb{Z}_p$ različit od nule može se na jedinstveni način napisati u obliku $p^n u$, gdje je $u \in \mathbb{U}$ i $n \geq 0$. (Takav element iz $\mathbb{U}$ zovemo p-adska jedinica.)*

*Dokaz.* Da bi dokazali tvrdnju pod (a) dovoljno je dokazati da tvrdnja vrijedi za sve $A_n$ jer iz nje odmah slijedi tvrdnja i za $\mathbb{Z}_p$.

(a) Neka je $x \in A_n$ koji nije djeljiv sa $p$, tj. koji ne pripada skupu $pA_n$. Nadalje, trebamo pronaći $t \in A_n$ takav da vrijedni $xt = 1$, čime ćemo pokazati da je $x$ invertibilan. Znamo da slika od $x$ u $A_1 = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ nije nula, pa je invertibilna. Stoga, postoje $y, z \in A_n$ takvi da je $xy + pz = (x, p) = 1$, odnosno takvi da je $xy = 1 - zp$. Sada imamo sljedeće:

$$xy(1+pz+p^2z^2+\cdots+p^{n-1}z^{n-1}) = (1-pz)(1+pz+p^2z^2+\cdots+p^{n-1}z^{n-1}) = 1-p^nz^n = 1$$

jer je $p^nz^n = 0$ u $A_n$.

Stoga, ako stavimo da je $t = y(1 + pz + \cdots + p^{n-1}z^{n-1})$, vidimo da je onda $t \in A_n$ i da vrijedi $xt = 1$. Dakle, pronašli smo traženi $t$. Obrat slijedi iz definicije invertibilnosti.

(b) Neka je $x \in \mathbb{Z}_p$ proizvoljan element različit od nule. Tada postoji najveći $n \in \mathbb{N}$ za koji je $x_n = 0$ (ako bi neki član niza $x$ bio nula, onda bi i svi prethodni članovi bili jednaki nuli zbog svojstva niza da je $\phi_n(x_n) = x_{n-1}$ pa za $x \neq 0$ mora postojati član najvećeg indeksa koji je jednak nuli) ili su svi članovi različiti od 0 i tad uzimamo da je $n = 0$. U tom slučaju $x$ je djeljiv sa $p^n$, ali nije djeljiv sa $p^{n+1}$ pa ga možemo zapisati u obliku $x = p^nu$, pri čemu je $n \geq 0$, a $u \in \mathbb{Z}_p$ nije djeljiv s $p$. Tada po (a) $u$ je invertibilan, odnosno $u \in U$, čime je dokazano postojanje traženog prikaza. Jedinstvenost prikaza je očigledna. Dakle, (b) dio propozicije je dokazan. □

Kako bi lakše koristili se ovim prikazom elemenata uvesti ćemo novu oznaku.

Neka je $x \in \mathbb{Z}_p, x \neq 0$. Napišimo ga u obliku $p^nu$, gdje je $u \in \mathbb{U}$ i $n \geq 0$. Tada $n$ nazivamo *p-adskom valuacijom* od $x$ i označavamo ju sa $v_p(x)$, tj. $p$-adska valuacija označava najveću potenciju od $p$ koja dijeli $x$. Naprimjer, $v_2(96) = 5$ jer $2^5$ dijeli 96 ($96 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^5 \cdot 3$). Oznaku za cijeli $\mathbb{Z}_p$ proširujemo tako da stavimo $v_p(0) = +\infty$. Sada imamo:

$$v_p(xy) = v_p(x) + v_p(y)$$

i

$$v_p(x + y) \geq inf(v_p(x), v_p(y)).$$

Lako se provjeri da je $\mathbb{Z}_p$ integralna domena. Prisjetimo se što znači da je neki prsten integralna domena. Za prsten $R$ kažemo da je integralna domena ako nema

ni lijevih ni desnih djelitelja nule, tj. ako za $x, y \in R$ vrijedi da je $xy = 0$ , onda je $x = 0$ ili $y = 0$. Neka su $x, y \in \mathbb{Z}_p$ takvi da je $x, y \neq 0$. Postoje $u_1, u_2 \in U$ takvi da $x = p^n u_1, y = p^n u_2, n \geq 0$. Pomnožimo $x$ i $y$, $x \cdot y = p^n u_1 \cdot p^n u_2 = p^{2n} u_1 u_2 \neq 0$ jer $p^{2n} \neq 0, u_1, u_2 \neq 0$. Dokazali smo da je umnožak dva elementa iz $\mathbb{Z}_p$ različita od 0 različit od 0, tj. bit će jednak nuli samo ako je jedan od njih jednak nuli. Dakle, $\mathbb{Z}_p$ je integralna domena.

Do sada smo promatrali $p$-adske cijele brojeve i prsten $\mathbb{Z}_p$. Osim $p$-adskih cijelih brojeva možemo promatrati i razlomke, tj. rješenja jednadžbi $ax + b = 0$ pri čemu $p$ ne dijeli $b$, a znamo da je tada $x = a/b \in \mathbb{Z}_p$. Doista, postoji inverzni element $b^{-1} \in \mathbb{Z}/p^k\mathbb{Z}$ i niz $ab^{-1}$ koji konvergiram prema nekom $x \in \mathbb{Z}_p$ takav da je $bx = a$. Odnosno, $\frac{1}{p} \notin \mathbb{Z}_p$, jer za sve $x \in \mathbb{Z}_p$ imamo da je $(px)_1 = 0$. Stoga, opće $p$-adske brojeve definiramo na sljedeći način.

**Definicija 1.2.7.** *$p$-adski brojevi su redovi oblika* $a_n \frac{1}{p^n} + a_{n-1} \frac{1}{p^{n-1}} + \cdots + a_0 + a_1 p + \ldots$.

Skup svih $p$-adskih brojeva označavamo s $\mathbb{Q}_p$. Vrijedi da je $\mathbb{Q}_p$ polje. Imamo inkluziju iz $\mathbb{Q}$ u $\mathbb{Q}_p$. Doista, ako je $x \in \mathbb{Q}$, tada postoji $N \geq 0$ takav da je $p^N x \in \mathbb{Z}_p$. Drugim riječima, polje $\mathbb{Q}$ možemo promatati kao potpolje od polja $\mathbb{Q}_p$.

Dakle, polje $\mathbb{Q}_p$ možemo definirati na sljedeći način.

**Definicija 1.2.8.** *Polje $p$-adskih brojeva, $\mathbb{Q}_p$, je polje razlomaka prstena $\mathbb{Z}_p$.*

Možemo odmah vidjeti da je $\mathbb{Q}_p = \mathbb{Z}[p^{-1}]$. Iz toga i iz (b) dijela prethodne propozicije slijedi da svaki element $x \in \mathbb{Q}_p^*$ ima jedinstveni prikaz u obliku $p^n u$, gdje je $n \in \mathbb{Z}, u \in U$. Ovdje isto $n$ nazivamo $p$-adskom valuacijom i označavamo ju s $v_p(x)$. Stoga, očito vrijedi :

$$v_p(x) \geq 0 \Leftrightarrow x \in \mathbb{Z}_p.$$

**Primjer 1.2.9.** *Zapišimo razlomak $-\frac{3}{2}$ u bazi 3. Znamo da je razlomak $-\frac{3}{2}$ rješenje jednadžbe $2x + 3 = 0$. Pitamo se da li postoji rješenje te jednadžbe u $\mathbb{Z}_3$? Razlomak $-\frac{3}{2}$ možemo zapisati u obliku $\frac{3}{-2}$. Nadalje,*

$$\frac{3}{-2} = \frac{3}{1-3} = 3 \cdot \frac{1}{1-3}.$$

*Znamo da vrijedi*

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

*Početni razlomak možemo onda zapisat kao*

$$3 \cdot \frac{1}{1-3} = 3(1 + 3 + 3^2 + \ldots)$$

*Odnosno,*

$$-\frac{3}{2} = 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \dots$$

## 1.3 $p$-adska apsolutna vrijednost

U ovome potpoglavlju dat ćemo definiciju $p$-adske apsolutne vrijednosti i opisati neka njena svojstva, te izreći i dokazati teorem Ostrowskog.

Za početak, prisjetimo se definicije standarne apsolutne vrijednosti.

**Definicija 1.3.1.** *Neka je $K$ polje. Funkcija $|\cdot| : K \to \mathbb{R}$ se zove apsolutna vrijednost ako za sve $x, y \in K$ vrijedi:*
$|x| \geq 0$, $|x| = 0$ *ako i samo ako* $x = 0$,
$|xy| = |x||y|$
$|x + y| \leq |x| + |y|$ *(nejednakost trokuta).*

**Definicija 1.3.2.** *Za apsolutnu vrijednost $|\cdot|$ na $K$ kažemo da je nearhimedska ako uz nejednakost trokuta vrijedi i "jača" nejdnakost:*

$$|x + y| \leq \max\{|x|, |y|\},$$

*za svaki $a, b \in K$.*
*Ako apsolutna vrijednost nije nearhimedska, kažemo da je arhimedska.*

Standarnu apsolutnu vrijednost smo koristili za definiciju nekih osnovnih pojmaova iz realne analize kao što su limesi, konvergencija, Cauchyjev niz i ostalo. Dakle, na standarnoj apsolutnoj vrijednosti bazira se realna analiza. Obzirom na $p$-adske brojeve vidjet ćemo da postoji i $p$-adska apsolutna vrijednost te koja su neka njena svojstva i uloga. Također, u prethodnom potpoglavlju smo uveli $p$-adske brojeva pomoću zapisa broja u bazi $p$ te smo uveli prsten $\mathbb{Z}_p$ i polje $\mathbb{Q}_p$, u ovom potpoglavlju ćemo vidjeti da i prsten $\mathbb{Z}_p$ i polje $\mathbb{Q}_p$ možemo uvesti i pomoću $p$-adske apsolutne vrijednosti.

Pogledajmo sljedeći primjer. Neka je $p$ prost broj. Za $n \in \mathbb{Z}$ s $v_p(n)$ označavamo $p$-adsku valuaciju broja $n$. Prisjetimo se, $p$-adska valuacija $v_p$ označava najveću potenciju od $p$ koja dijeli $n$, tj. $p^{v_p(n)} | n$. Za $\frac{a}{b} \in \mathbb{Q}$ definiramo

$$\left|\frac{a}{b}\right| = \begin{cases} 0 & \text{ako je } \frac{a}{b} = 0 \\ p^{-(v_p(a) - v_p(b))} & \text{inače} \end{cases}$$

**Primjer 1.3.3.** *Npr.* $|\frac{7}{12}|_3 = |\frac{7}{2^2 \cdot 3}|_3 = 3^{-(0-1)} = 3^1 = 3, |\frac{7}{14}|_7 = 7^{-(1-1)} = 7^0 = 1,$

$$|p^{-42}|_p = p^{42}, |p^{100}|_p = p^{-100},$$

$$\left|\frac{63}{550}\right|_p = |2^{-1} \cdot 3^2 \cdot 5^{-2} \cdot 7 \cdot 11^{-1}|_p = \begin{cases} 2 & ako\ je\ p = 2 \\ 1/9 & ako\ je\ p = 3 \\ 25 & ako\ je\ p = 5 \\ 1/7 & ako\ je\ p = 7 \\ 11 & ako\ je\ p = 11 \\ 1 & ako\ je\ p \geq 13 \end{cases}$$

Na taj način definiramo $p$-adsku apsolutnu vrijednost.

**Definicija 1.3.4.** *Neka je $\mathbb{Q}$ polje racionalnih brojeva. Svaki racionalan broj $x \neq 0$ može se prikazati u obliku $x = p^{v_p}\frac{n}{m}$, gdje je $v_p, n \in \mathbb{Z}$, a $m$ je pozitivan cijeli broj te vrijedi da su $m, n$ s $p$ realativno prosti brojevi, tj. $(p, n) = 1, (p, m) = 1)$ pri čemu je $p$ neki fiksni prosti broj. $p$-adsku apsoutnu vrijednost od $x$ definiramo kao*

$$|x|_p = \begin{cases} p^{-v_p} & za\ x \neq 0 \\ 0 & za\ x = 0 \end{cases}$$

Uočimo još da takva definicija od $|x|_p$, (vidi prethodni primjer) ima posljedicu da velike potencije od $p$ postaju male, i obrnuto, da male potencije od $p$ postaju velike.

**Primjer 1.3.5.** *Odredimo $p$-adsku apsolutnu vrijednost sljedećih racionalnih brojeva za fiksni prosti broj $p$, $p = 3$.*
*a)* $|\frac{5}{18}|_3 =?$
*b)* $|\frac{3}{16}|_3 =?$
*c)* $|\frac{5}{18} + \frac{3}{16}|_3 =?$

*Rješenje:*
*a)* $|\frac{5}{18}|_3 = 9$
*b)* $|\frac{3}{16}|_3 = \frac{1}{3}$
*c)* $|\frac{5}{18} + \frac{3}{16}|_3 = |\frac{67}{144}|_3 = 9$

*Uočimo da je* $|\frac{5}{18} + \frac{3}{16}|_3 = |\frac{5}{18}|_3 = max\{|\frac{5}{18}|_3, |\frac{3}{16}|_3\}$

Iz prethodnog primjera možemo uočiti da za $p$-adsku apsolutnu vrijednost vrijedi

$$|x + y|_p \leq max\{|x|_p, |y|_p\}$$

pri čemu su $x, y \in \mathbb{Q}$. Odnosno, da je $p$-adska apsolutna vrijednost nearhimedska. Time dolazimo i do sljedeće propozicije.

**Propozicija 1.3.6.** $|\cdot|$ *je nearhimedska apsolutna vrijednost na* $\mathbb{Q}$. *Naziva se p-adska apsolutna vrijednost.*

Jedan od važnijh teorema što se stiće apsolutne vrijednost je teorem Ostrowskog koji povezuje svaku netrivijalnu apsolutnu vrijednost na polju $\mathbb{Q}$ i $p$-adsku apsolutnu vrijednost. Kako bi ga iskazali i dokazali, najprije moramo dati dobru definiciju kada su dvije apsolutne vrijednosti "jednake", tj. ekvivalentne. Definirajmo kada su dvije apsolutne vrijednosti "jednake" na nekom polju K.

**Definicija 1.3.7.** *Za dvije apsolutne vrijednosti* $|\cdot|_1, |\cdot|_2$ *na polju* $\mathbb{K}$ *su ekvivalentne ako je* $|\cdot|_1 = |\cdot|_2^s$ *za neki* $s > 0$. *(Obje definiraju istu topologiju na* $\mathbb{K}$*.)*

**Primjer 1.3.8.** *Neka je p prosti broj. Svaki* $0 \neq a \in \mathbb{Q}$ *možemo zapisati u obliku* $a = p^m \frac{b}{c}$, *gdje su* $m, b, c \in \mathbb{Z}$ *i za koje vrijedi da je* $(bc, p) = 1$. *Definiramo* $|a|_p = \frac{1}{p^m}$ *i* $|0|_p = 0$, *tada je* $|\cdot|_p$ *nearhimedska vrijednost na* $\mathbb{Q}$. *Imajmo na umu da za različite proste brojeve p i q, apsolutne vrijednosti* $|\cdot|_p$ *i* $|\cdot|_q$ *nisu ekvivalentne. Za* $z \in \mathbb{C}$, *definiramo* $|z|_\infty = |z|$ *(običnoj apsolutnoj vrijednosti). Tada* $|\cdot|_\infty$ *je arhimedska vrijednost na* $\mathbb{C}$ *(nije ekvivalentna s* $|\cdot|_p$ *za svaki p).*

**Teorem 1.3.9.** *Teorem Ostrowskog za polje* $\mathbb{Q}$
*Svaka netrijvijalna apsoluna vrijednost na* $\mathbb{Q}$ *je ekvivalnetna običnoj apsolutnoj vrijednosti ili p-adskoj apsolutnoj vrijednosti za neki prost broj p.*

*Dokaz.* Neka je $|\cdot|$ netrivijalna apsolutna vrijednost na $\mathbb{Q}$. Razmotrit ćemo moguće slučajeve.
a) Pretpostavimo, prvo da je $|\cdot|$ arhimedska apsolutna vrijednost. Želimo, u ovom slučaju, pokazati da je ekvivalentna sa "običnom" ($\infty$-adskom) apsolutnom vrijednosti. Neka je $n_0$ najmanji pozitivan cijeli broj za koji je $|n_0| > 1$ (postoji samo jedan takav jer bi u protivnom apsolutna vrijednost $|\cdot|$ bila nearhimedska). Sada, naravno, možemo pronaći pozitivan realan broj $\alpha$ takav da vrijedi

$$|n_0| = n_0^\infty.$$

(Pronalaženje formule za $\alpha$ je jednostavna vježba s logaritmima.) Tvrdimo da će se pomoću takve $\alpha$ ostvariti ekvivalencija između $|\cdot|$ i $|\cdot|_\infty$. Znači, želimo pokazati da za svaki $x \in \mathbb{Q}$ vrijedi $|x| = |x|_\infty^\alpha$. Obzirom na poznata svojstva apsolutne vrijednosti, to će slijediti ako znamo da vrijedi za pozitivne cijele brojeve, tj. ako pokažemo da je $|n| = n^\alpha$ za bilo koji pozitivan cijeli broj.

Znamo da jednakost vrijedi za $n = n_0$. Da bi to dokazali u cijelosti, iskoristit ćemo mali trik. Uzmimo proizvoljan cijeli broj $n$ i napišimo ga u "bazi $n_0$", tj. u obliku

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k,$$

za $0 \leq a_i \leq n_0 - 1, a_k \neq 0$. Primjetimo da je $k$ određen s nejednakošću $n_0^k \leq n < n_0^{k+1}$, iz koje slijedi da je

$$k = \left\lfloor \frac{\log n}{\log n_0} \right\rfloor,$$

gdje $\lfloor x \rfloor$ označava "pod" od $x$, tj. najveći cijeli broj koji je manji ili jednak $x$. Sada djelujumo apsolutnom vrijednost $||$ na $n$. Dobivamo da je

$$|n| = |a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k| \leq |a_0| + |a_1| n_0^\alpha + |a_2| n_0^{2\alpha} + \cdots + |a_k| n_0^{k\alpha}.$$

Kako smo odabrali $n_0$ kao najmanji cijeli broj čija je apsolutna vrijednost veća od 1, znamo da je $|a_i| \leq 1$, tako dobivamo da je

$$|n| \leq 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{k\alpha} = n_0^{k\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-k\alpha}) \leq n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} = n_0^{k\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1}.$$

Ako bi uveli supstituciju $C = \frac{n_0^\alpha}{n_0^\alpha - 1}$ (možemo primjetiti da je to pozitivan broj), onda možemo prethodnu nejednakost pročitati kao

$$|n| \leq C n_0^{k\alpha} \leq C n^\alpha.$$

Sada možemo iskorisititi trik. Ova formula vrijedi za svaki $n$ (budući da smo ga odabrali proizvoljno); primjenjujući ga na cijeli broj oblika $n^N$ dobivamo

$$|n^N| \leq C n^{N\alpha}$$

(ključna stvar je da broj $C$ ne ovisi o $n$ - možemo iz definicije $C$ vidjeti da ne ovisi). Uzimajući $N$-ti korijen, dobivamo

$$|n| \leq \sqrt[N]{C} n^\alpha.$$

Budući da vrijedi za svaki $N$, možemo ustiti da $N \to \infty$, iz čega slijedi da $\sqrt[N]{C} \to 1$ i tako dobivamo nejednakosti: $|n| \leq n^\alpha$. To je polovica onoga što želimo. Sada trebamo pokazati da nejednakost vrijedi i u drugom smjeru, tj. da vrijedi i $|n| \geq n^\alpha$. Za to, vraćamo se natrag izrazu zapisanog u bazi $n_0$

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k.$$

Budući da je $n_0^{k+1} < n \geq n_0^k$, dobivamo

$$n_0^{(k+1)\alpha} = |n_0^{k+1}| = |n + n_0^{k+1} - n| \leq |n| + |n_0^{k+1} - n|$$

($||$ je arhimedska), tako da dobivamo da je

$$|n| \geq n_0^{(k+1)\alpha} - |n_0^{k+1} - n| \geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha,$$

gdje možemo iskoristiti nejednakost dokazanu u prethodnom odlomku. Sada, kako je $n \geq n_0^k$, slijedi da je

$$|n| \geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha = n_0^{(k+1)\alpha}\left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) = C' n_0^{(k+1)\alpha} > C' n^\alpha,$$

i još jednom $C' = 1 - \left(1 - \frac{1}{n_0}\right)^\alpha$ je pozitivan broj koji ne ovisi o $n$. Koristeći upravo isti trik kao i prije, dobili smo obrnutu nejednakost $|n| \geq n^\alpha$. Obzirom da smo pokazali da je $|n| \geq n^\alpha$ i $|n| \leq n^\alpha$, slijedi da je $|n| = n^\alpha$. To dokazuje da je $||$ ekvivalentna "običnoj" apsolutnoj vrijednosti $||_\infty$, kao što smo i tvrdili.

(b) Sada pretpostavimo da $|\cdot|$ je nearhimedska. Tada, kako smo pokazali, imamo $|n| \leq 1$ za svaki cijeli broj $n$. Kako je $|\cdot|$ netrivijalna, mora postojati najmanji cijeli broj $n_0$ takav da je $|n_0| < 1$. Prva stvar koju treba ustanoviti je da $n_0$ mora biti prosti broj. Da bi to vidjeli, pretpostavimo da je $n_0 = a \cdot b$ gdje su $a$ i $b$ manji od $n_0$. Zatim, po našem izboru za $n_0$, imali bismo $|a| = |b| = 1$ i $|n_0| < 1$. što ne može biti. Dakle, $n_0$ je prost, pa nazovimo ga, tj. označimo ga kao što i inače označavamo proste brojeve s $p$, $n_0 = p$. Sada, naravno, želimo pokazati da je $||$ ekvivalentna sa $p$-adskom apsolutnom vrijednosti, gdje je $p$ prost.
Sljedeći korak je pokazati da ako $n \in \mathbb{Z}$ nije djeljiv s $p$, onda je $|n| = 1$. To nije preteško za pokazati.Ako $n$ podijelimo s $p$ imat ćemo ostatak, tako da možemo zapisati

$$n = rp + s$$

gdje je $0 < s < p, r, s \in \mathbb{Z}$. Obzirom na minimalnost $p$-a, imamo da je $|s| = 1$. Također, imamo sa je $|rp| < 1$, jer je $|r| \leq 1$ (jer je $||$ nearhimedska a) i $|p| < 1$ (po konstrukciji). Budući da je $||$ nearhimedska (i stoga su "svi trokuti jednakokračni"), slijedi da je $|n| = 1$. Konačno, svaki dani $n \in \mathbb{Z}$, zapišimo kao $n = p^v n'$ za $p \nmid n'$. Tada

$$|n| = |p^v n'| = |p^v||n'| = |p|^v = c^{-v},$$

gdje je $c = |p|^{-1} > 1$. Dakle, $||$ je ekvivalentna $p$-adskoj apsolutnoj vrijednosti, kako smo i tvrdili. □

Ovaj teorem je glavni razlog za razmišljanje o "običnoj" apsolutnoj vrijednosti $||_\infty$ (ili o inkluziji $\mathbb{Q} \hookrightarrow \mathbb{R}$ odakle dolazi) kao nekoj vrsti "prostog broja" u $\mathbb{Q}$. Poanta je u tome da je onda istina da svaka apsolutna vrijednost na $\mathbb{Q}$ "dolazi iz" (konačnog ili beskonačnog) prostog broja. Postoji mnogo situacija u aritmetici gdje je korisno

raditi s "svim prostim brojevima", tj. koristiti podatke dobivene od svih apsolutnih vrijednosti na $\mathbb{Q}$. Što se tiće općeg "osjećaja", realna apsolutna vrijednost daje informacije vezane uz *sign*, dok druge apsolutne vrijednosti daju informacijee vezane za vrijednosti prostih brojeva. Sljedeća propozicija je fundamentalni primjer toga koja povezuje običnu apsolutnu vrijednost na $\mathbb{Q}$ sa $p$-adskom apsolutnom vrijednosti.

**Propozicija 1.3.10.** ***(Produktna formula)*** *Neka je $0 \neq \alpha \in \mathbb{Q}$. Tada je*

$$\prod_{p \leq \infty} |\alpha|_p = 1,$$

*gdje je $p \in \{\infty, 2, 3, 5, 7, \dots\}$ i $|\alpha|_\infty$ je realna apsolutna vrijednost od $\alpha$.*

*Dokaz.* Dokazat ćemo samo slučaj kad je $\alpha$ pozitivan cijeli broj jer opći slučaj slijedi iz njega. Stoga, neka je $\alpha$ pozitivan cijeli broj. Znamo da svaki pozitivan cijeli broj možemo prikazati kao umnožak svojih prostih faktora. Stoga,

$$\alpha = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}.$$

Tada imamo da je

$$\begin{cases} |\alpha|_q = 1 & \text{ako je } q \neq p_i \\ |\alpha|_{p_i} = p_i^{-a_i} & \text{ako je } i = 1, ..., k \\ |\alpha|_\infty = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \end{cases}$$

Rezultat tada slijedi. □

U biti ako znamo sve apsolutne vrijednosti osim jedne, produktna formula nam omogućuje da ju odredimo. To se ispostavilo iznenađujuće važno u mnogim primjenama. Imjaući na umu da sličan rezultat vijedi i za konačna proširenja $\mathbb{Q}$, osim što u tom slučaju moramo koristiti nekoliko "beskonačnih prosti broj" (zapravo po jedan za svako drugačije upotpunjenje $\mathbb{R}$ i $\mathbb{C}$).

Obzirom da smo na početku ovog potpoglavlja rekli da ćemo pokazati na koji način možemo uvesti prsten $\mathbb{Z}_p$ i polje $\mathbb{Q}_p$ pomoću p-adske apsolutne vrijednosti, definirajmo ih na sljedeći način.

**Definicija 1.3.11.** *Upotpunjenje od $\mathbb{Q}$ u odnosu na $|\cdot|_p$ označavamo sa $\mathbb{Q}_p$ i zovemo polje p-adskih brojeva. Proširenje od $|\cdot|_p$ na $\mathbb{Q}_p$ označavamo sa $|\cdot|$. Skup*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

*zovemo prsten p-adskih brojeva.*

Nadalje, pogledajmo još neka specifična svojstva za nearhimedsku apsolutnu vrijednost te zašto elemente iz $\mathbb{Z}_p$ i $\mathbb{Q}_p$ možemo prikazati na jedinstveni način kao redove u prethodnom poglavlju.

**Lema 1.3.12.** *Neka su $a, b \in \mathbb{Q}_p$. Ako je $|a|_p > |b|_p$ onda je $|a+b|_p = |a|_p$.*

*Dokaz.* Iz nejednkosti trokuta i pretpostavke leme slijedi da je $|a+b|_p \leq |a|_p$. Imamo

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

Kako je $|a|_p > |b|_p$ slijedi da je $|a|_p \leq |(a+b)-b|_p$ pa tvdnja slijedi. □

**Lema 1.3.13.** *Neka su $a_1, a_2, \ldots, a_n \in \mathbb{Q}_p$. Tada vrijedi*

$$|a_1 + a_2 + \cdots a_n|_p \leq \max\{|a_1|_p, |a_2|_p, \cdots, |a_n|_p\}.$$

*Dokaz.* Koristeći nejednakost trokuta i prethodnu lemu, tvrdnja se dokaže indukcijom po $n$. Provjerimo bazu indukcije: $n = 2$ Neka su $a_1, a_2 \in \mathbb{Q}_p$. Pogledajmo ćemu je jednaka $|a_1 + a_2|_p$. Po prethodnoj lemi imamo da je $|a_1 + a_2|_p = |a_1|_p$ ako je $|a_1|_p > |a_2|_p$, odnosno da je $|a_1 + a_2|_p = |a_2|_p$ ako je $|a_2|_p > |a_1|_p$. Dakle, općenito, vrijedi da je $|a_1 + a_2|_p \leq \max\{|a_1|_p, |a_2|_p\}$.
Pretpostavimo da tvrdnja vijedi za neko $k \in \mathbb{N}$, tj. da vrijedi $|a_1 + a_2 + \cdots a_k|_p \leq \max\{|a_1|_p, |a_2|_p, \ldots, |a_k|_p\}$.
Provjerimo da li tvrdnja vrijedi i za $k+1 \in \mathbb{N}$. Pitamo se da li vijedi sljedeća nejednakost $|a_1 + a_2 + \cdots + a_k + a_{k+1}|_p \leq \max\{|a_1|_p, |a_2|_p, \cdots, |a_k|_p, |a_{k+1}|_p\}$.

$$|a_1 + a_2 + \cdots + a_k + a_{k+1}|_p \leq |a_1 + a_2 + \cdots + a_k|_p + |a_{k+1}|_p$$

(po nejednakosti tokuta)

$$\leq \max\{|a_1|_p, |a_2|_p, \ldots, |a_k|_p\} + |a_{k+1}|_p$$

(po pretpostavci indukcije)

$$\leq \max\{|a_1|_p, |a_2|_p, \cdots, |a_k|_p, |a_{k+1}|_p\}$$

(po prethodnoj lemi imamo da je $|a_1+a_2+\cdots+a_k+a_{k+1}|_p = \leq \max\{|a_1|_p, |a_2|_p, \ldots, |a_k|_p\}$ ako je $|a_{k+1}|_p < \max\{|a_1|_p, |a_2|_p, \ldots, |a_k|_p\}$ , a ako je $|a_{k+1}|_p \geq \max\{|a_1|_p, |a_2|_p, \ldots, |a_k|_p\}$ onda je $|a_1 + a_2 + \cdots + a_k + a_{k+1}|_p = |a_{k+1}|_p$. Dakle, općenito vrijedi da je $|a_1 + a_2 + \cdots + a_k + a_{k+1}|_p \leq \max\{|a_1|_p, |a_2|_p, \cdots, |a_k|_p, |a_{k+1}|_p\}$.
Po aksiomu matematičke indukcije dokazali smo da tvrdnja je istinita za bazu indukcije i po pretpostavci je istinita za svaki sljedeći prirodan broj stoga, tvrdnja vrijedi.

□

Iz definicije $p$-adskog cijelog broja (definicija 1.2.2.) slijedi nam i sljedeća propozicija.

**Propozicija 1.3.14.** *Neka je* $(x_k)_{k\in\mathbb{N}_0}, x_k \in \{0,1,\dots,p-1)\}$. *Tada je*

$$\alpha = \sum_{k=0}^{\infty} x_k p^k \in \mathbb{Z}_p.$$

*Dokaz.* Da bi dokazali da je $\alpha$ iz $\mathbb{Z}_p$ promotrit ćemo niz parcijalnih suma $a_n = \sum_{k=0}^{\infty} x_k p^k$ reda $\alpha = \sum_{k=0}^{\infty} x_k p^k$. Doakžimo da je taj niz Cauchyjev u odnosu na $|\cdot|_p$. Neka je $\epsilon > 0$ i neka je $n_0$ takav da je $p^{-n_0} < \epsilon$. Za sve $m > n > n_0$ imamo

$$|a_m - a_n| = |\sum_{k=n+1}^{\infty} x_k p^k|_p = |p^{n+1}|_p \cdot |\sum_{k=n+1}^{\infty} x_k p^{k-n-1}|_p \leq \frac{1}{p^{n+1}} < \epsilon.$$

Dakle, $\alpha \in \mathbb{Q}_p$. Budući da je $|a_k|_p \leq 1$ za sve $k$, $|\alpha|_p = \lim_k |c_k|_p \leq 1$ pa je $\alpha \in \mathbb{Z}_p$. □

**Primjer 1.3.15.** $\frac{1}{1+p} = 1-p+p^2-p^3+\cdots = 1+p(p-1)+p^3(p-1)+\cdots+p^{2k+1}(p-1)+\cdots \in \mathbb{Z}_p$. *Iz ovakvog zapisa možemo vidjeti da su p-adske znamenke broja* $\frac{1}{1+p}$ *su* $(1, p-1, 0, p-1, 0, p-1, \dots)$.

Uočimo da za $\alpha \in \mathbb{Q}_p$ i $n \in \mathbb{Z}$ takav da je $|\alpha|_p \leq p^n$ vrijedi da je $p^n \cdot \alpha \in \mathbb{Z}_p$. Zbog toga, ako znamo kako "izgledaju" elementi iz $\mathbb{Z}_p$ odmah znamo i kakvog su oblika i elementi iz $\mathbb{Q}_p$.

Osim prethodne propozicije, vrijedi i njen obrat, tj. da se svaki element iz $\mathbb{Z}_p$ može na jedinstveni način prikazati u obliku $\sum_{k=0}^{\infty} x_k p^k$. Da bi dokazali obrat trebamo znati još neke činjenice o $\mathbb{Q}_p$.

**Propozicija 1.3.16.** *a)* $\mathbb{Q}$ *je gust u* $\mathbb{Q}_p$.
*b)* $\mathbb{Q}_p$ *je potpun (tj. svaki Cauchyjev niz u* $\mathbb{Q}_p$ *je konvergentan).*

*Dokaz.* a) Neka je $\alpha \in \mathbb{Q}_p, \alpha = (a_n)_n$, gdje su $a_n \in \mathbb{Q}$ i neka je $\epsilon > 0$. Budući da je niz $(a_n)_n$ Cauchyjev, za dani $\epsilon > 0$ postoji $n_0 \in \mathbb{N}$ takav da je za sve $m, n \leq n_0$ vrijedi $|\alpha_m - \alpha_n|_p < \epsilon$. Neka je $\beta = (a_{n_0}, a_{n_0}, \dots, a_{n_0}, \dots) \in \mathbb{Q} \subset \mathbb{Q}_p$. Pokažimo da je $|\alpha - \beta|_p < \epsilon$. Po definiciji treba dokazati da je $\lim_k |a_n - a_{n_0}|_p \leq \epsilon$. Za $n > n_0$ vrijedi da je $|a_n - a_{n_0}|_p < \epsilon$ pa tvrdnja slijedi.
b) Dokaz se nalazi u sljedećem poglavlju. □

Analogno se dokaže i da je $\mathbb{Z}$ gust u $\mathbb{Z}_p$, pa imamo sljedeću propoziciju.

**Propozicija 1.3.17.** *$\mathbb{Z}$ gust u $\mathbb{Z}_p$.*

*Dokaz.* Neka je $z \in \mathbb{Z}_p, z \neq 0$ i neka je $\epsilon > 0$. Skup svih $x \in \mathbb{Q}_p$ za koje je $|x|_p = |z|_p$ je otvoren. Obzirom da je $\mathbb{Q}$ gust u $\mathbb{Q}_p$, postoji $\frac{a}{b} \in \mathbb{Q}$ u ovom skupu takav da je $|\frac{a}{b} - z|_p < \epsilon$. Imajmo na umu da $|\frac{a}{b}|_p = |z|_p$ implicira sa $p \nmid b$. Stoga za bilo koji $N > 0$ postoji cijeli broj $b'$ takav da je $bb' \equiv 1 \bmod p^N$. Tada za dovoljno veliki $N$ imamo,

$$|\frac{a}{b} - ab'|_p = |\frac{a}{b}|_p|1 - bb'|_p \leq p^{-N} < \epsilon.$$

Sada,

$$|ab' - z|_p = |ab' - \frac{a}{b} + \frac{a}{b} - z|_p \leq \max\left(|ab' - \frac{a}{b}|_p, |\frac{a}{b} - z|_p\right) < \epsilon.$$

Time je propozicija dokazana. □

Možemo primjetiti da za sve $x, y \in \mathbb{Z}$ i $m \in \mathbb{Z}$ vrijedi da je

$$x \equiv y(\mathrm{mod} p^m) \Leftrightarrow |x - y|_p \leq p^m.$$

Motivirani time možemo definirati sljedeće. Za sve $x, y \in \mathbb{Z}_p$ vrijedi

$$x \equiv y(\mathrm{mod} p^m) \Leftrightarrow \frac{x - y}{p^m} \in \mathbb{Z}_p.$$

To znači da su dva elementa $x, y \in \mathbb{Z}_p$ "blizu" ako su kongruentni modulo "velikoj" potenciji od $p$.

Nadalje, koristeći ovu definiciju, činjenicu da je $\mathbb{Z}$ gust u $\mathbb{Z}_p$ možemo zapisati na sljedeći način.

**Lema 1.3.18.** *Za svaki $\alpha \in \mathbb{Z}_p$ i za svaki $m \in \mathbb{N}$ postoji jedinstveni $a_m \in \mathbb{Z}$ takav da je*

$$\alpha \equiv a_m(\mathrm{mod} p^m)$$

*i $0 \leq a_m \leq p^m$.*

Sada možemo dokazati obrat propozicije 1.3.14.

**Propozicija 1.3.19.** *Svaki element $\alpha \in \mathbb{Z}_p$ se može na jedinstveni način prikazati kao red*

$$\alpha = \sum_{k=0}^{\infty} b_k p^k,$$

*gdje su $b_k \in \{0, 1, \ldots, p-1\}$ za sve $k$.*

*Dokaz.* Neka je $\alpha \in \mathbb{Z}_p$. Prema prethodnoj lemi postoji niz $(a_m)_m \in \mathbb{Z}$ takav da je $\alpha \equiv a_m (\mathrm{mod} p^m)$ za sve $m$. Kako su $0 \leq a_m \leq p^m$, postoji niz $(b_m)_m, b_m \in \{0, 1, \ldots, p-1\}$ takav da je $a_{m+1} = b_m p^m + a_m$. Lako se provjeri da je $\alpha = \sum_{k=0}^{\infty} b_k p^k$. (kako?) □

Analogno tome imamo sljedeću propoziciju.

**Korolar 1.3.20.** *Svaki element $\alpha \in \mathbb{Q}_p$ se može na jedinstveni način prikazati kao red*

$$\alpha = \sum_{k \geq -k_0}^{\infty} b_k p^k,$$

*gdje su $b_k \in \{0, 1, \ldots, p-1\}$ za sve $k$ i $-k_0 = v_p(x)$.*

*Dokaz.* Sve što bi rebalo provjeriti je tvrdnja o $v_p(x)$ koja je jasna sama po sebi. □

## 1.4 Svojstva $p$-adskih brojeva

U ovome potpoglavlju navest ćemo neka "dobra" i "loša" svojstva $p$-adskih brojeva.

Ultra-metrika nejednakosti trokuta daje nam zanimljivu razliku između realne i $p$-adske analize. Sljedeća svojstva $p$-adskih brojeva čine pravce u $p$-adskoj analizi koji su jednostavniji nego realnoj analizi.

1. **Svi trokuti su jedakokračni.**
   Da bi dokazali da je ta tvrdnja istinita potrebna nam je sljedeća propozicija.

   **Propozicija 1.4.1.** *Neka je $\mathbb{K}$ polje i neka je $|\cdot|$ nearhimedska apsolutna vrijednost na $\mathbb{K}$. Ako su $x, y \in K$ pri čemu vrijedi $|x| \neq |y|$, tada je*

   $$|x + y| = \max\{|x|, |y|\}.$$

   *Dokaz.* Uzmimo proizvoljan $x$ i $y$, pretpostavimo da je $|x| > |y|$ (možemo zamijeniti $x$ i $y$ ako je potrebno). Znamo da tada vrijedi

   $$|x + y| \leq |x| = \max\{|x|, |y|\}.$$

   S druge strane $x$ možemo zapisati kao $x = (x + y) - y$, tako da imamo

   $$|x| \leq \max\{|x + y|, |y|\}.$$

Kako znamo da je $|x| > |y|$, ova nejednakost će ostati vrijediti samo ako

$$\max\{|x+y|, |y|\} = |x+y|.$$

To nam daje obrnutu nejednakost $|x| \leq |x+y|$, i iz nje (koristeći i prvu nejednakost) zaključujemo da je $|x| = |x+y|$. □

Dokažimo sada početnu tvrdnju.

*Dokaz.* Neka su $x, y, z$ tri elementa ultrametričkog prostora (vrhovi trokuta). Duljine stranica trokuta dane su sa sljedeće tri jednakosti

$$d(x,y) = |x-y|$$

$$d(y,z) = |y-z|$$

$$d(x,z) = |x-z|$$

Znamo da vrijedi $(x-y)+(y-z) = (x-z)$ pa se možemo pozvati na propoziciju koja nam kaže da ako je $|x-y| \neq |y-z|$, tada $|x-z|$ je jednako većoj od tih udaljenosti. U svakom slučaju, dvije "stranice" su jednake. □

2. **Svaka točka kugle $B(a,r) = \{x \in \mathbb{Q}_p : |x-a|_p \leq r\}$ je središte te kugle. Kugla $B(a,r)$ je i otvorena i zatvorena. Svake dvije kugle su ili disjunktne ili jedna sadrži drugu.**

Dokažimo prvu tvrdnju koja tvrdi da je svaka točka koja je sadržana u kugli $B(a,r)$ je centar te kugle. Po definiciji, $b \in B(a,r)$ ako i samo ako $|b-a|_p \leq r$. Sada, uzimajući bilo koji $x$ za koji je $|x-a|_{\leq} r$, nearhimedska svojstva kažu nam da je

$$|x-b|_p \leq \max\{|x-a|_p, |b-a|_p\} \leq r,$$

tako da je $x \in B(b,r)$; To nam pokazuje da je $B(a,r) \subset B(b,r)$. Zamjenom $a$ i $b$, dobijemo suprotnu inkluziju. Tako da su te dvije kugle jednake, $B(a,r) = B(b,r)$.

Dokažimo i drugu tvrdnju koja kaže da je kugla $B(a,r) = \{x \in \mathbb{Q}_p : |x-a|_p \leq r\}$ i otvorena i zatvorena. Otvorena kugla $B(a,r)$ je uvijek otvoreni skup u bilo kojem metričkom prostoru, pa tako i u ultrametričkom prostoru u kojem imamo nearhimedsku apsolutnu vrijednost, točnije $p$-adsku. Imamo dokaz u jednom redu ( iz definicije se vidi da vrijedi): svaki $x \in B(a,r)$ nalazi se u kugli $B(a,r)$ koja je sadržana u $B(a,r)$. Ono što trebamo dokazati je da je i zatvoreni skup kada smo u nearhimedskom prostoru. To ćemo dokazati tako da uzmemo

neki $x$ s ruba kugle $B(a,r)$; to znači da bilo koja otvorena kugla u središtu $x$ mora sadržavati točke koje su u $B(a,r)$. Odaberimo broj $s \leq r$, i pogledajmo otvorenu kuglu $B(x,s)$ sa središtem u $x$ i radijusom $s$. Kako je $x$ rubna točka, $B(a,r) \cap B(x,s) \neq \emptyset$, tako da postoji neki element

$$y \in B(a,r) \cap B(x,s).$$

To znači da je $|x-a|_p < r$ i $|y-x|_p < s \leq r$. Primjenjujući nearhimedsku ($p$-adsku) nejednakost, dobivamo

$$|x-a|_p \leq \max\{|x-y|_p, |y-a|_p\} < \max\{s,r\} \leq r,$$

tako da $x \in B(a,r)$. To pokazuje da je svaka rubna točka kugle $B(a,r)$ pripada kugli $B(a,r)$, što znači da je $B(a,r)$ zatvoren skup.

Na kraju, dokažimo i posljednju tvrdnju koja nam kaže da su dvije kugle ili disjunktne ili je jedna sadržana u drugoj. Neka su $B_1$ i $B_2$ dvije kugle definirane na sljedeći način: $B_1(a,r) = \{x \in \mathbb{Q}_p : |x-a|_p \leq r\}$, $B(b,s) = \{x \in \mathbb{Q}_p : |x-b|_p \leq s\}$. Pretpostavimo da je $r \leq s$ ( inače ih zamijenimo). Ako presjek te dvije kugle nije prazan, tada postoji $c \in B(a,r) \cap B(b,s)$. Tada znamo, iz prve tvrdnje, da je $B(a,r) = B(c,r)$ i $B(b,s) = B(c,s)$. Stoga,

$$B(a,r) = B(c,r) \cap B(c,s) = B(b,s),$$

kako smo tvrdili. Ako je njihov presjek prazan, tada su disjunktne.

3. $|\cdot|_{p_1} \nsim |\cdot|_{p_2}$ **ako** $p_1 \neq p_2$**. To znači da svaki prosti broj** $p$ **generira svoje polje** $p$**-adskih brojeva** $\mathbb{Q}_p$**.**
Odnosno, tvrdimo da za različite proste brojeve $p$ i $q$ polja $\mathbb{Q}_p$ i $\mathbb{Q}_q$ nisu izomorfna. Dokažimo to! Možemo pretpostaviti da je $p$ neparan prost broj. Pretpostavimo i da je $q$ neparan prost broj. Neka je $n$ kvadratni ne-ostatak od (mod $q$). Pomoću Kineskog teorema o ostatku možemo pronaći $k, l \in \mathbb{N}$ takve da je $1 + kp = n + lq$. Stoga, za $a = 1 + kp$ imamo $\left(\frac{a}{p}\right) = \left(\frac{1}{p}\right) = 1$ dok je $\left(\frac{a}{p}\right) = \left(\frac{n}{p}\right) = -1$. Lako se pokaže da je $\sqrt{a} \in \mathbb{Q}_p$, ali $\sqrt{a} \notin \mathbb{Q}_q$. Dakle, ako bi postajao izomorfizam $\phi : \mathbb{Q}_p \to \mathbb{Q}_q$, tada bi imali

$$\phi(\sqrt{a})^2 = \phi(\sqrt{a}^2) = \phi(a) = \phi(1+1+\cdots+1) = a,$$

tako da će $\phi(\sqrt{a})$ biti jednak drugom korijenu $a$ iz $\mathbb{Q}_q$ što je kontradikcija.
Slično se pokaže i za paran prost broj $q$ tj. za $q = 2$. Ako je $q = 2$ tada možemo pronaći $a = 1 + kp = 3 + 4l$, takav da je ponovno $\sqrt{a} \in \mathbb{Q}_p$ , ali $\sqrt{a} \notin \mathbb{Q}_2$, tako da vrijedi isti argument kao i u prethodnom slučaju.

4. **Jednadžba $x^2 = -1$ ima rješenje za $x \in \mathbb{Q}_p$ ako je $p = 1(\text{mod}4)$.**
Da bi dokazali to, trebamo riješiti kongruenciju $x^2 \equiv -1(\text{ mod } p)$. Ako je $p = 2$, onda je $x = 1$ jedno rješenje jer vrijedi $1 \equiv -1(\text{mod } 2)$. Nadalje, krenimo od toga da je $p \equiv 1(\text{mod}4)$. To znači da je $p - 1$ dijeljivo s 4, odnosno da je $\frac{p-1}{2}$ paran broj. Pokušajmo rješenje kongruencije $x^2 \equiv -1(\text{mod } p)$ eksplicitno konstruirati pomoću Wilsonovog teorema koji nam kaže da ako je $p$ prost broj, onda je $(p-1)! \equiv -1(\text{mod } p)$. Ako uspijemo, onda smo dokazali početnu tvrdnju. Stoga, neka je $(p-1)! \equiv -1(\text{mod } p)$. Zapišimo lijevu stranu u obliku umnoška:
$$(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2})(\frac{p+1}{2} \cdots (p-1)) \equiv -1(\text{mod } p)$$
Uočimo da u jednoj i drugoj zagradi imamo isti broj faktora, i to $\frac{p-1}{2}$ faktora. Faktore iz drzge zagrade možemo zapisati i na drugačiji način.
$$(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2})((\frac{p+1}{2} - p) \cdots (p-1-p)) \equiv -1(\text{mod } p)$$
Iskoristili svojstvo kongruencije, tj. da vrijedi $\frac{p+1}{2} \equiv \frac{p+1}{2} - p(\text{mod } p), \ldots, (p-1) \equiv (p-1) - p(\text{mod } p)$. Nadalje, iz druge zagrade možemo izlučiti $-1$, pa dobivamo
$$(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2})(-1)^{\frac{p-1}{2}}(\frac{p-1}{2} \cdots 1) \equiv -1(\text{mod } p)$$
Obzirom da je $\frac{p-1}{2}$ paran broj, $(-1)^{\frac{p-1}{2}} = 1$, stoga dobivamo
$$(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2})(1 \cdots \frac{p-1}{2}) \equiv -1(\text{mod } p)$$
$$[(\frac{p-1}{2})!]^2 \equiv (\text{mod } p)$$
Dakle, početna kongruencija ima rješenje za $p = 1(\text{mod } p)$ i jednako je $x = (\frac{p-1}{2})!$.

5. **Niz $\{x_n\}$ u $\mathbb{Q}_p$ je Cauchyjev ako i samo ako $|x_{n+1} - x_n|_p \to 0$ kad $n \to \infty$. To ima korisnu posljedicu da suma $\sum_{k=0}^{\infty} x_k$ gdje je $\{x_k\}$ niz u $\mathbb{Q}_p$ konvergira ako i samo ako pojedini izrazi teže u 0,tj. $\lim_{k\to\infty} x_k = 0$.**
Dokažimo tvrdnju da je niz $\{x_n\}$ u $\mathbb{Q}_p$ Cauchyjev ako i samo ako $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$. Prisjetimo se prvo što nam kaže definicije Cauchyjevog niza, za neki niz elemenata $x_n \in K$, $K$ polje, nazivamo Cauchyjevim nizom

ako se za svaki $\epsilon > 0$ može pronaći ograda $M$ takva da je $|x_n - x_m| < \epsilon$ za proizvoljne $m, n \geq M$. Obzirom na nju, trebamo vidjeti da li postoji neki broj od kojeg je $|x_{n+1} - x_n|_p$ manje ili jednako. Ako je $m = n + r > n$ za $m, n, r \in \mathbb{Q}$, dobijemo da je

$$|x_m - x_n|_p = |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + x_{n+r-2} + \cdots + x_{n+1} - x_n|_p$$

$$\leq \max\{|x_{n+r} - x_{n+r-1}|_p, |x_{n+r-1} - x_{n+r-2}|_p, \ldots, |x_{n+1} - x_n|_p\} < \epsilon,$$

jer je $||_p$ nearhimedska apsolutna vijednost. Tvrdnja iz toga odmah slijedi.

Pokažimo da je red $\sum_{k=0}^{\infty} x_k$ konvergentan. Znamo da je red konvergentan kad je niz parcijalnih suma konvergentan. Dokažimo prvo prvi smjer. Pretpostavimo da $\sum x_k$ konvergira k $\alpha \in \mathbb{Q}_p$. Tada je za svaki $n \in \mathbb{N}$

$$x_n = \sum_{k=0}^{n} x_k - \sum_{k=0}^{n-1} x_k,$$

pa prelaskom na limes dobivamo $\lim x_n = \alpha - \alpha = 0$. dokažimo sada i drugi smjer. Pretpostavimo da je $\lim x_n = 0$. Neka je $\alpha_n = \sum_{k=0}^{n} x_k$ $n$-ta parcijalna suma reda $\sum a_k$. Pokažimo da je taj niz Cauchyjev. Neka je $\epsilon > 0$. Tada postoji $n_0 \in \mathbb{N}$, takav da za svaki $k > n_0$ vrijedi $|x_k|_p < \epsilon$. Za sve $m, n \in \mathbb{N}, m > n \geq n_0$ vrijedi

$$|\alpha_m - \alpha_n|_p = |\sum_{k=n+1}^{m} x_k|_p \leq \max\{|x_{n+1}|_p, \ldots, |x_m|_p\} \leq \epsilon.$$

Dakle, niz $(\alpha_n)_n$ je Cauchyjev pa tvrdnja slijedi iz potpunosti polja $\mathbb{Q}_p$.

6. (Studenski san) $\sum_{n=1}^{\infty} a_n < \infty$ **ako i samo ako** $a_n \to 0$**.**

Kako $|n!|_p \to 0$ imamo, naprimjer,

$$\sum_{n=0}^{\infty} (-1)^n n!(n+2) = 1, \qquad \sum_{n=0}^{\infty} (-1)^n n!(n^2 - 5) = -3.$$

Suma $\sum_{n=0}^{\infty} n!$ postoji u svakom $\mathbb{Q}_p$. Problem, tj. pitanje koje se postavlja za tu sumu glasi: "Je li racionalna za neki prosti broj $p$?". Do danas nije riješen taj problem, postavljen je 1971., jer nije poznato je li $\sum_{n=0}^{\infty} n! = 0$ u svakom polju $\mathbb{Q}_p$.

7. **Za neki $x \in \mathbb{Q}$, imamo**
$$|x| \prod_{p:prost} |x|_p = 1.$$
Ova formula se koristi za rješavanje nekoliko problema u teoriji brojeva, mnogi od njih koriste Hasseov lokalni-globalni princip, koji grubo navodi da se jednadžba može riješiti u racionalnim brojevima ako i samo ako se može riješiti u realnim brojevima i u $p$-adskim brojevima za svaki prosti broj $p$.

Sada navedimo i neka "loša" svojstva p-adskih brojeva, koja u "kompliciranija" u $p$-adskoj analizi.

1. **Polje $\mathbb{Q}_p$ nije uređeno.**
2. **Polje $\mathbb{Q}_p$ nije usporedivo s** $\mathbb{R}$, naprimjer $\sqrt{7} \notin \mathbb{Q}_5$, ali $i \in \mathbb{Q}_5$.
3. **Polje $\mathbb{Q}_p$ nije algebarski zatvoreno.**
Ali $|\cdot|_p$ se može jedinstveno proširiti do algebarski zatvorenog polja $\mathbb{Q}_p^a$ i tada uređeni par $(\mathbb{Q}_p^a, |\cdot|_p)$ zovemo polje $p$-adskih kompleksnih brojeva i označavamo s $\mathbb{C}_p$. Polje $\mathbb{C}_p$ nije lokalno kompaktno, ali je seperabilno i algebarski zatvoreno.

Definirajmo funkcije $\exp_p(x)$ i $\log_p(x)$. Neka je $a \in \mathbb{Q}_p$ i $r > 0$ te neka je
$$B(a, r) = \{x \in \mathbb{Q}_p : |x - a|_p < r\}.$$
$p$-adsku logaritamsku funkciju definiramo redom
$$\log_p(x) = \log_p(1 + (x-1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n},$$
koji konvergira za $x \in B(1,1)$. $p$-adsku eksponencijalnu funkciju definiramo redom
$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$
koji konvergira za $x \in B(0, p^{-1/(p-1)})$. Neka je $x \in B(0, p^{-1/(p-1)})$, tada je
$$|\exp_p(x)|_p = 1, \quad |\exp_p(x) - 1|_p = |x|_p, \quad |\log_p(1+x)|_p = |x|_p,$$
$$\log_p(\exp_p(x)) = x, \quad \exp_p(\log_p(1+x)) = 1 + x.$$

4. Neke "dobre" funkcije postanu "loše". Naprimjer, logaritamska i eksponencijalna funkcija su "dobre" u realnoj analizi, ali u $p$-adskoj analizi i nisu baš. Kada smo ih definirali vidjeli smo da je $p$-adska eksponencijalna funkcija definirana samo na kugli $B(a,r) = \{x \in \mathbb{Q}_p : |x-a|_p < r\}$, a $p$-adska logaritamska funkcija samo na kugli $B(1,1)$.

# Poglavlje 2

# Jednadžbe u $p$-adskim brojevima

U ovome poglavlju prvo ćemo vidjeti na koji način se izvode operacije zbrajanja, oduzimanja, množenja i dijeljenja u polju $\mathbb{Q}_p$ kroz nekoliko konkretnih primjera. Nakon toga, ćemo pokazati kroz primjere rješavanje kongurencija modulo $p^n$. Na kraju ovoga poglavlja, proučit ćemo $p$-adske jednadžbe čiji su koeficijenti $p$-adski cijeli brojevi, te pokazati kako se od rješenja ( mod $p^n$) dolazi do pravog rješenja jednadžbe.

## 2.1 Računanje u polju $\mathbb{Q}_p$

U ovome potpoglavlju pokazat ćemo primjere zbrajanja, oduzimanja, množenja u polju $\mathbb{Q}_p$, te pogledati kad postoji drugi korijen u $\mathbb{Q}_p$.

### Negacija

Ako je $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$, tada je

$$-a = p^k\left((p - a_0) + \sum_{i=1}^{\infty}(p - 1 - a_i)p^i\right),$$

što se može provjeriti zbrajajući $a$ i $-a$ (i dobivajući 0!). Treba samo imati na umu da su svi $a_i \in \{0, 1, 2, \ldots, p-1\}$ i $a_0 \neq 0$ te da isto vrijedi i za znamenke broja $-a$.

### Recipročni brojevi

Ako je $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$, tada je

$$\frac{1}{a} = p^{-k}(a'_0 + a'_1 p + \cdots + a'_i p^i + \ldots)$$

gdje se svaki $i$ prve $i$ znamenke $a'_0, a'_1, \ldots, a'_i$ mogu izračunati na sljedeći način: stavimo da je $a'_0 + a'_1 p + \cdots + a'_i p^i = N$, $N' \in \mathbb{N}$ za koji vrijedi da je $N' < p^{i+1}$ računamo tako da rješimo kongruenciju $NN' \equiv 1 (\text{mod } p^{i+1})$. Tada zapis $N'$ u bazi $p$ kao $N' = a'_0 + a'_1 p + \cdots + a'_i p^i$ daje nam $a'_0, a'_1, \ldots, a'_i$.

## Zbrajanje i oduzimanje

Ako je $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$ i $a' = p^k(\sum_{i=0}^{\infty} a'_i p^i)$ (za neki $k$), tada $a + a' = p^k((a_0 + a'_0) + (a_1 + a'_1)p + \cdots + (a_i + a'_i)p^i + \ldots)$, gdje onda "prijenos" treba biti izveden kako bismo dobili znamenke od $a + a'$ u $\{0, 1, \ldots, p-1\}$. Ako je $a' = p^{k'}(\sum_{i=0}^{\infty} a'_i p^i)$ za $k' < k$ tada možemo povećati proširenje (ekspanziju) od $a'$ s početnom nulom tako da opet možemo pretpostaviti da je $k = k'$, at the expense of no longer having $a'_0$ nonzero. Tada se zbrajanje može izvesti kao i gore.

**Primjer 2.1.1.** *Zbroji dane brojevi $a$ i $b$ u polju $\mathbb{Z}_3$ pri čemu su oba broja zapisana u bazi 3. Neka je $a = 2 + 1 \cdot 3 + \ldots$, a $b = 1 + 2 \cdot 3 + \ldots$.*
*Imamo $a_1 \equiv 2 \text{ mod } 3$ i $b_1 \equiv 1 \text{ mod } 3$, prema tome*

$$(a + b)_1 = a_1 + b_1 = 3 \equiv 0 \text{ mod } 3.$$

*Tada $a_2 \equiv 5 \text{ mod } 3^2$ i $b_2 \equiv 7 \text{ mod } 3^2$, tako da je*

$$(a + b)_2 = a_2 + b_2 = 12 \equiv 3 \text{ mod } 3^2.$$

*Tako se dobije da je*

$$a + b = 0 + 1 \cdot 3 + \cdots \in \mathbb{Z}_3.$$

## Množenje

Množenje je slično zbrajanju. Tako množenjem $a = p^k(\sum_{i=0}^{\infty} a_i p^i)$ s $a' = p^{k'}(n \sum_{i=0}^{\infty} a'_i p^i)$ dobivamo da je

$$a \cdot a' = p^{k+k'}(a_0 a'_0 + (a_1 a'_0 + a_0 a'_1)p + \cdots + (\sum_{j=0}^{i} a_j a'_{i-j})p^i + \ldots),$$

gdje se onda ovaj izraz može staviti u standarni oblik.

**Primjer 2.1.2.** *Pomnoži dane brojevi $a$ i $b$ u polju $\mathbb{Z}_3$ pri čemu su oba broja zapisana u bazi 3. Neka je $a = 2 + 1 \cdot 3 + \ldots$, a $b = 1 + 2 \cdot 3 + \ldots$.*

*Imamo da je* $a_0 \equiv 2 \bmod 3$, *a* $b_0 \equiv 1 \bmod 3$, *prema tome*

$$(a \cdot b)_0 = a_0 \cdot b_0 \equiv 2 \bmod 3.$$

*Nadalje,* $a_1 \equiv 5 \bmod 3^2$, *a* $b_1 \equiv 7 \bmod 3^2$, *tada imamo da je*

$$a_1 b_0' + a_0 b_1 = 5 \equiv 2 (\bmod\ 3)$$

*Tako da se dobije da je*

$$a \cdot b = 2 + 2 \cdot 3 + \cdots \in \mathbb{Z}_3$$

## Postojanje drugog korijen u $\mathbb{Q}_p$

Razlikujemo dva slučaja: $p$ je neparan prost broj te $p$ je paran prost broj, tj. $p = 2$.

Promotrimo prvo slučaj kada je $p$ neparan prost broj. Prvo ćemo promotriti $p$-adsku jedinicu $a = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$, gdje je $p$ neparan broj. Pitamo se koji takav $a$ ima drugi korijen u polju $\mathbb{Q}_p$. Dakle, ako je $a = b^2$, gdje je $b = b_0 + b_1 p + b_2 p^2 + \cdots \in \mathbb{Z}_p$, tada, računajući modulo $p$ vidjet ćemo da je $a_0 \equiv b_0^2 (\bmod\ p)$, tako da $a_0$ mora biti kvadratni ostatak (mod $p$). U ovom slučaju pomoći će nam metoda iz sljedećeg poglavlja da odredimo $b$. Imajmo na umu da ako u bilo kojoj fazi pokušavamo konstruirati $b (\bmod\ n)$, tada trebamo samo odrediti $a (\bmod\ n)$ tako da uvijek možemo raditi s cijelim brojevima umjesto sa $p$-adskm cijelim brojevima. S druge strane, ako je $a_0$ kvadratni ne-ostatak, tada $a$ nema drugi korijen u $\mathbb{Q}_p$.

**Primjer 2.1.3.** *Odredimo* $\sqrt{6}$ *u polju* $\mathbb{Q}_5$.

*Zapišimo* $\sqrt{6} = b_0 + b_1 \cdot 5 + b_2 \cdot 5^2 + \ldots$. *Tada, kvadriranjem i određivanjem* mod 5, *dobivamo da je* $b_0^2 \equiv 1 (\bmod\ p)$, *tako da je* $b_0 = 1$ *ili* 4. *Uzmimo da je* $b_0 = 1$ *( 4 će nam dati drugi kvadratni korijen). Nadalje, određujući* mod $5^2$, *imamo*

$$\begin{gathered} 6 \equiv (1 + b_1 \cdot 5)^2 \pmod{5^2} \\ 6 \equiv 1 + 10 b_1 \pmod{5^2} \\ 1 \equiv 2 b_1 \pmod{5}, \end{gathered}$$

*iz čega dobivamo da je* $b_1 = 3$. *Radeći istu stvar s* mod $5^3$ *dobivamo*

$$\begin{gathered} 6 \equiv (1 + 3 \cdot 5 + b_2 \cdot 5^2)^2 \pmod{5^3} \\ 6 \equiv 16^2 + 23 b_2 \cdot 5^2 \pmod{5^3} \\ -250 \equiv 32 b_2 \cdot 5^2 \pmod{5^3} \\ 0 \equiv 32 b_2 \pmod{5}, \end{gathered}$$

*dobivamo da je* $b_2 = 0$. *Određujući* mod $5^4$ *dobivamo da je* $b_3 = 4$, *i tako dalje. Na kraju dobivamo da je* $\sqrt{6} = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + \ldots$

Sljedeće treba uzeti u obzir općeniti $p$-adski broj $a = p^k(a_0 + a_1p + a_2 \cdot p^2 + \dots)$. Ako je $a = b^2$, tada $|a|_p = |b|_p^2$, samo ako je $|b|_p = |a|_p^{-k/2} = p^{-k/2}$. Ali vrijednosti elemenata iz $\mathbb{Q}_p$ su cijele potencije broja $p$, tako da ako je $k$ neparan broj, tada $b \notin \mathbb{Q}_p$. Ali ako je $k$ paran, tada ne postoji problem, i $a$ će imati kvadratni korijen $b = p^{k/2}(b_0 + b_1p + \dots) \in \mathbb{Q}_p$ ako i samo ako $a_0$je kvadratni ostatak (mod $p$).

Promotrimo sada drugi slučaj, kad je $p$ paran prost broj. Dakle, promotrimo 2-adske jedinice $a = 1 + a_1 \cdot 2 + a_2 \cdot 2^2 + \dots \in \mathbb{Z}_2$. Ako je $a = b^2$, gdje je $b = b_0 + b_1 2^1 + b_2 2^2 + \dots \in \mathbb{Z}_2$, računajući modulo 8, imamo $b^2 \equiv \pmod 8$, tako da moramo imati i $a \equiv 1(\text{mod}8)$, što nam daje da je $a_1 = a_2 = 0$. Na analogan način kao u prethodnom slučaju možemo konstruirati $b$ S druge strane, ako $a \neq 1 \bmod 8$), tada $a$ nema kvadratni korijen u polju $\mathbb{Q}_2$.
Za općeniti 2-adski broj $a = 2^k(1 + a_1 2 + a_2 2^2 + \dots)$, vidimo da je, slično kao i u slučaju gdje je $p$ neparan broj, $a$ će imati kvadratni korijen u $\mathbb{Q}_2$ ako i samo ako $k$ je paran i $a_1 = a_2 = 0$.

## 2.2 Rješavanje kongurencija modulo $p^n$

U ovome potpoglavlju ćemo pogledati neke primjere rješavanja kongurencija modulo $p^n$. Naime, $p$-adski brojevi koje smo konstruirali su usko povezani s problemom rješavanja kongruencija modulo potencije od $p$. Naime, možemo reći da je rješavanje kongurencija modulo $p^n$ uvod u rješavanje $p$-adskih jednadžbi.

Krenimo s najlakšim mogućim slučajem, tj. s jednadžbom koja ima rješenja u $\mathbb{Q}$ kao što je jednadžba

$$X^2 = 25.$$

Želimo ju promotriti modulo $p^n$ za svaki $n$, tj. riješiti kongruenciju

$$X^2 \equiv 25(\text{mod } p^n).$$

Znamo da početna jednadžba ima rješenja u skupu cijelih brojeva: $X = \pm 5$. To nam automatski daje i rješenje kongruencije za svaki $n$, samo trebamo staviti $X \equiv \pm 5(\text{mod } p^n)$, za svaki $n$.

Nadalje, pokušajmo razumijeti to rješenje malo bolje sa $p$-adske točke gledišta. Kako bi si olakšali, uzmimo da je $p = 3$. Krenut ćemo od ponovnog zapisivanja našeg rješenja pomoću predstavnika klase ostataka modulo $3^n$, tj. brojeva između 0 i $3^{n-1}$.

Prvo rješenje $X = 5$ nam daje:

$$X \equiv 2(\text{mod } 3),$$

$$X \equiv 5 = 2 + 3(\text{mod } 9),$$

$$X \equiv 5 = 2 + 3(\text{mod } 27),$$

itd.

što se nikada više ne mijenja, te time nam samo daje 3-adsko proširenje ovog rješenja:

$$X = 5 = 2 + 1 \cdot 3.$$

Retultati za drugo rješenje, $X = -5$, su malo zanimljiviji; predstavnici su

$$X \equiv -5 \equiv 1(\text{mod } 3)$$

$$X \equiv -5 \equiv 4 = 1 + 3(\text{mod } 9)$$

$$X \equiv -5 \equiv 22 = 1 + 3 + 2 \cdot 9(\text{mod } 27)$$

$$X \equiv -5 \equiv 76 = 1 + 3 + 2 \cdot 9 + 2 \cdot 27(\text{mod } 81)$$

itd.

Nastavljajući na isti način dobivamo 3-adsko proširenje rješenja, koje je u ovom slučaju malo zanimljivije jer je beskonačno:

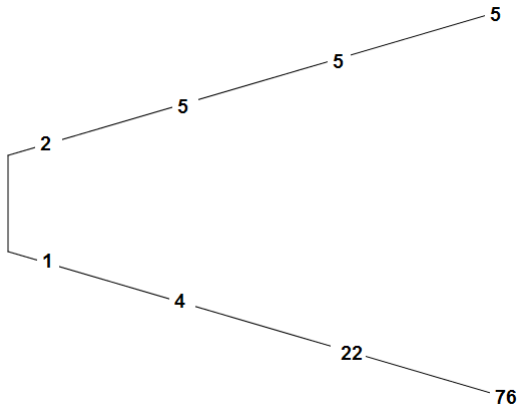
$$X = -5 = 1 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

Uočimo da su dva sustava rješenja "koherentna" odnosno povezana, u smislu da kad pogledamo, recimo, $X = 76$ (što je rješenje modulo $3^4$) i redukcije modulo $3^3$, dobivamo $X = 22$ (što je rješenje modulo $3^3$). Dajmo formalnu definiciju toga.

**Definicija 2.2.1.** *Neka je $p$ prosti broj. Kažemo da je niz cijelih brojeva $\alpha_n$ takav da je $0 \leq \alpha_n \leq p^n - 1$ koherentan, ako za svaki $n \geq 1$, imamo*

$$\alpha_{n+1} \equiv \alpha_n(\text{mod } p^n).$$

*Ako trebam istaknuti izbor $p$, reći ćemo da je niz $p$-adski koherentan.*




Slika 2.1: Rješenje od $X^2 \equiv 25 (\text{mod } 3^n)$

Možemo zamisliti da se rješenja dva koherentna niza mogu prikazati kao grane stabla (vidi sliku 2.1). Naravno, to je sve prilično očito u slučaju koji smo promatrali, budući da su nizovi rješenja jednostavno povezani zato što su to rješenja u $\mathbb{Z}$ (76 je kongruentno s 22 samo zato što su oboje kongruentni sa $-5$). Dakle, jedina prava informacija koju smo prikupili je veza između izražavanja korijena kao povezanog niza i dobivanja njihovih $p$-adskih proširenja.

Stvari postaju mnogo zanimljivije ako slijedimo isti proces s jednadžbom koja nema racionalnih korijena. Naprimjer, uzmimo sustav kongruencija

$$X^2 \equiv 2 (\text{mod } 7^n), \ n = 1, 2, 3, \ldots$$

Za $n = 1$ rješenja su $X \equiv 3 (\text{mod } 7)$ i $X \equiv 4 \equiv -3 (\text{mod } 7)$. Pri traženju rješenja za $n = 2$, trebamo imati na umu da njihove redukcije modulo 7 moraju biti rješenja za $n = 1$. Stoga, postaviti ćemo da je $X = 3 + 7k$ ili $X = 4 + 7k$ i riješit ćemo po $k$:

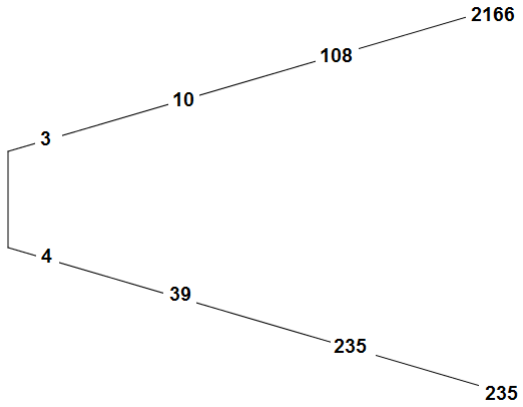
$$(3 + 7k)^2 \equiv 2 (\text{mod } 49)$$

$$9 + 42k \equiv 2 (\text{mod } 49)$$

(primijetimo da je izraz koji uključuje $(7k)^2$ je kongruentan nuli)

$$7 + 42k \equiv 0 (\text{mod } 49)$$

$$1 + 6k \equiv 0 (\text{mod } 7)$$




Slika 2.2: Rješenje od $X^2 \equiv 2(\text{mod } 7^n)$

$$k \equiv 1(\text{mod } 7)$$

što, obzirom kako je $X = 3 + 7k$, daje nam rješenje $X = 10(\text{mod } 49)$. Koristeći $X = 4 + 7k$ dobivamo drugo rješenje $X \equiv 39 \equiv -10(\text{mod } 49)$.

Opet, rješenja se mogu prikazati kao grane na stablu (vidi sliku 2.2). Međutim, ovaj put ne možemo unaprijed predvidjeti koji će se brojevi pojavljivati; umjesto toga, sve što možemo učiniti je uvjeriti se da će se proces nastaviti sve dok mi to želimo. Činjenica da se pronalaženje korijena može nastaviti u nedogled pokazuje da postoje dva koherentna niza rješenja:

$$x_1 = (3, 10, 108, 2166, \dots)$$

i

$$x_2 = (4, 39, 235, 235, \dots) = (-3, -10, -108, -2166, \dots) = -x_1.$$

Kao i prije, svaki broj možemo proširiti u svaki 7-adski niz. Činjenica da je niz koherentan znači da je proširenje od svakog korijena skraćenje od proširenja sljedećeg korijena, tako da, naprimjer,

$$3 = 3$$

$$10 = 3 + 1 \cdot 7$$

$$108 = 3 + 1 \cdot 7 + 2 \cdot 49$$

To nam daje dva 7-adska broja:

$$x_1 = 3 + 1 \cdot 7 + 2 \cdot 49 + 6 \cdot 343 + \dots$$

i

$$x_2 = 4 + 5 \cdot 7 + 4 \cdot 49 + 0 \cdot 343 + \cdots = x_1.$$

To vjerojatno nosi ponavljanja: ne tvrdimo da možemo predvidjeti ovdje neki obrazac. Sve što znamo je da možemo nastaviti s obrascem onoliko dugo koliko je potrebno, ako imamo dovoljno vremena i strpljenja. To je kao i pronalaženje decimalnog proširenja kvadratnog korijena od 2: možemo dobiti što bliže onome što želimo i to možemo dokazati, iako ne možemo predvidjeti kakvo će proširenje zapravo biti.
U svakom slučaju, dobili smo dva 7-adska broja i oni su doista korijeni jednadžbe $X^2 = 2$ u polju $\mathbb{Q}_7$, u uobičajenom smislu.

Izjednačenost između rješavanja nizova kongruencije modulo sve veće potencije broja $p$ i rješavanja odgovarajuće jednadžbe u $\mathbb{Q}_p$ je vrlo bliska. Upravo je to jedan od važnijih razloga za korištenje $p$-adske metode u teoriji brojeva.

Riješimo sada općenitu kongruenciju $x^2 \equiv a(\mathrm{mod} p^n)$.
Neka je $p$ neki neparan prosti broj i $a$ neka je neki cijeli broj koji je relaivno prost s brojem $p$. Tada, $x^2 \equiv a(\mathrm{mod}\ p)$ ima rješenje $x \in \mathbb{Z}$ ako i samo ako je $\left(\frac{a}{p}\right) = 1$. U ovom slučaju možemo pretpostaviti da je $b_0^2 \equiv a(\mathrm{mod}\ p)$. Tvrdimo da tada $x^2 \equiv a(\mathrm{mod}\ p^n)$ ima rješenje $x$ za svaki $n \in \mathbb{N}$.
Pretpostavimo da imamo rješenje $x$ od kongruencije $x^2 \equiv a(\mathrm{mod}\ p^n)$ za neki $n \leq 1$. Tada je $x$ relativno prost s $p$, tako da možemo pronaći $x_1 \equiv \frac{1}{2}(x + a/x)(\mathrm{mod}\, p^{2n})$. (To je standarna Newton-Raphson metoda $x_1 = x - f(x)/f'(x)$ za rješavanje jednadžbe $f(x) = 0$, primjenjena na polinom $f(x) = x^2 - a$, ali u (mod $p^{2n)}$ umjesto u $\mathbb{R}$ ili u $\mathbb{Q}$.) Tada

$$x_1 - x = -\frac{1}{2}\big(x - \frac{a}{x}\big) = -\frac{1}{2x}\big(x^2 - a\big) \equiv 0(\mathrm{mod}\ p^n),$$

i

$$x_1^2 - a = \frac{1}{4}\left(x^2 + 2a + \frac{a^2}{x^2}\right) - a = \frac{1}{4}\left(x - \frac{a}{x}\right)^2 = \frac{1}{4x^2}(x^2 - a)^2 \equiv 0(\mathrm{mod}\ p^{2n})$$

Dakle, počevši sa $x_0$ takvim da je $x_0^2 \equiv a(\mathrm{mod}\ p^{2^0})$, dobivamo slijed $x_1$ takav da je $x_1^2 \equiv a(\mathrm{mod}\ p^{2^1})$, $x_2$ takav da je $x_2^2 \equiv a(\mathrm{mod}\ p^{2^2}), \ldots, x_k$ takav da je $x_k \equiv a(\mathrm{mod}\ p^{2^k}), \ldots, x_{k+1}$ takav da je $x_{k+1} \equiv x_k(\mathrm{mod}\ p^{2^k})$. Dakle, zapisivanjem $x_i$ u bazi $p$, dobivamo

$x_0 = b_0$
$x_1 = b_0 + b_1 p$ recimo, određeno s (mod $p^2$)
$x_2 = b_0 + b_1 p + b_2 p^2 + b_3 p^3$ recimo, određeno s (mod $p^4$)
$x_3 = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4 + b_5 p^5 + b_6 p^6 + b_7 p^7$ recimo, određeno s ( mod $p^8$),
i tako dalje.

Dakle, je li u svakom slučaju $x_\infty = \sum_{i=1}^{\infty} b_i p^i$ korijen od $x^2 \equiv a(\bmod\ p^\infty)$? Ispada da je, da je $x_\infty$ korijen od jednadžbe $x^2 = a$ u polju $\mathbb{Q}_p$ $p$-adskih brojeva.

## 2.3 $p$-adske jednadžbe

U ovom potpoglavlju prvo ćemo vidjeti kakva je veza između nultočaka polinoma s koeficijentima u $\mathbb{Z}_p$ i polinoma dobivenih redukcijom $(\mathrm{mod} p^n)$, čiji su koeficijenti u $A_n$. Nakog toga promotrit ćemo kako od rješenja $p$-adskih jednadžbe $(\mathrm{mod} p^m)$ doći do pravih rješenja, s koeficijentima u $\mathbb{Z}_p$.

**Lema 2.3.1.** *Neka je $\cdots \to D_n \to D_{n-1} \to \cdots \to D_1$ projektivni sistem i neka je $D = \varprojlim D_n$ njegov projektivni limes. Ako su $D_n$ konačni i neprazni, onda je i $D$ neprazan.*

Dokaz leme se može naći u [8, str. 13].

**Napomena 2.3.2.** *Ako je $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ polinom s koeficijentima iz $\mathbb{Z}_p$ i ako je $n \in \mathbb{N}$, onda sa $f_n$ označavamo polinom s koeficijentima iz $A_n$ dobiven iz $f$ redukcijom* $(\mathrm{mod}\ p^n)$.

**Propozicija 2.3.3.** *Neka su $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ polinomi čiji su koeficijenti p-adski cijeli brojevi. Tada su sljedeće tvrdnje ekvivalentne:*
*(a) Polinomi $f^{(i)}$ imaju zajedničku nultočku u $(\mathbb{Z}_p)^m$.*
*(b) Polinomi $f^{(i)}$ imaju zajedničku nultočku u $(A_n)^m$, za $\forall n > 1$.*

*Dokaz.* Neka je $D$ skup zajedničkih nultočaka polinoma $f^{(i)}$ u $(\mathbb{Z}_p)^m$ i neka je $D_n$ skup nultočaka polinoma $f_n^{(i)}$ u $(A_p)^m, \forall n >$. Skupovi $D_n$ su konačni i imamo da je $D = \lim_{\leftarrow} D_n$. Po gornjoj lemi, $D$ je neprazan ako i samo ako su $D_n$ neprazni, što kaže i propozicija. Drugi smjer je očit, te smo time dokazali propoziciju. □

Definirajmo sada primitivan element.

**Definicija 2.3.4.** *Za element $x = (x_1, \ldots, x_m) \in (\mathbb{Z}_p)^m$ kažemo da je primitivan ako je neki $x_i$ invertibilan, tj. iz $U$. Odnosno, ako nisu svi $x_i$ djeljivi s p. Analogno se definiraju i primitivni elementi u $(A_n)^m$.*

U vezi njega imamo sljedeću propoziciju.

**Propozicija 2.3.5.** *Neka su $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ homogeni polinomi čiji su koeficijenti p-adski cijeli brojevi. Tada su sljedeće tvrdnje ekvivalentne:*
*(a) Polinomi $f^{(i)}$ imaju netrivijalnu zajedničku nultočku u $(\mathbb{Q}_p)^m$.*
*(b) Polinomi $f^{(i)}$ imaju zajedničku primitivnu nultočku u $(\mathbb{Z}_p)^m$.*
*(c) Polinomi $f^{(i)}$ imaju zajedničku primitivnu nultočku u $(A_n)^m$, za $\forall n > 1$.*

*Dokaz.* Dokažimo prvo da je (a) $\iff$ (b). Implikacija (b) $\Rightarrow$ (a) je triviljalno jasna (primitivna nultočka je po definiciji različita od nule). Dokažimo da vrijedi implikacija i obrtnuto, tj. implikacija (a) $\Rightarrow$ (b). Ako je $x = (x_1, x_2, \ldots, x_m)$ netrvijalna zajednička nultočka polinoma $f^{(i)}$ u $(\mathbb{Q}_p)^m$ stavimo

$$h = inf(v_p(x_1), \ldots, v_p(x_m))$$

i

$$y = p^{-h}x$$

Očito je, iz same definicije od $y$, da je $y$ primitivan element u $(\mathbb{Z}_p)^m$, kao i da je zajednička nultočka polinoma $f^{(i)}$ (homogeni su pa faktor $p^{-h}$ "ne smeta"), što je upravo tvrdnja (b). Dakle, i (a) $\Rightarrow$ (b) i (b) $\Rightarrow$ (a) pa je (a) $\iff$ (b).
(b) $\iff$ (c) slijedi iz gornje leme, analogno kao u dokazu prethodne propozicije. $\square$

Nadalje, dat ćemo rezultate koji poboljšavaju aproksimativna rješenja, odnosno promatrat ćemo kako od rješenja (mod $p^n$) doći do pravog rješenja jednadžbe s koeficijentima u $\mathbb{Z}_p$. Pri tome će nam trebati sljedeća lema, koja je $p$-adski analog Newtone metode.

**Lema 2.3.6.** *Neka je $f \in \mathbb{Z}_p[X]$ i $f'$ derivacija tog polinoma. Neka je $x \in \mathbb{Z}_p, n, k \in \mathbb{Z}$ takvi da je $0 \leq 2k < n, f(x) \equiv 0(\text{mod } p^n), v_p(f'(x)) = k$. Tada postoji $y \in \mathbb{Z}_p$ takav da vrijedi*

$$f(y) \equiv 0(\text{mod } p^{n+1}),\ v_p(f'(y)) = k,\ y \equiv x(\text{mod } p^{n-k}).$$

*Dokaz.* Uzmimo $y = x + p^{n-k}z, z \in \mathbb{Z}_p$. Takvim odabirom zadovoljeno je treće potrebno svojstvo. Odaberemo sad $z$ takav da i preostala dva svojstva budu zadovoljena. Iz Taylorovog teorema imamo:

$$f(y) = f(x) + (y-x)f'(x) + (y-x)^2\frac{f''(x)}{2} + \cdots = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a,$$

gdje je $a \in \mathbb{Z}_p$. Po pretpostavkama leme vrijedi $f(x) = p^n b$ i $f'(x) = p^k c$, pri čemu je $b \in \mathbb{Z}_p$ i $c \in \mathbb{U}$. Prema tome, možemo izabrati $z$ takav da vrijedi:

$$b + zc \equiv 0(\text{mod } p).$$

Pokažimo da uz takav $z$ odabrani $y$ zadovoljava i preostala dva svojstva.
Iz jednakosti $f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a$ dobivamo da je

$$f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a = p^n(b + zc) + p^{2n-2k}a \equiv 0(\text{mod}p^{n+1}),$$

zbog toga što je $b + zc \equiv 0 (\text{mod } p)$ i $n - 2k > 0$, odnosno $2n - 2k > n$. Time smo dokazali prvo željeno svojstvo.
Konačno, primjenom Taylorove formule na $f'$ odmah dobivamo:

$$f'(y) \equiv p^k c (\text{mod } p^{n-k}).$$

Sad iz $n > 2k$ imamo $n - k > k$, iz čega slijedi da je $f'(y) = p^k c$, gdje je $c \in \mathbb{U}$. Iz čega je vidljivo da je $v_p(f'(y)) = k$, čime je i drugo svojstvo dokazano pa je odabrani $y \in \mathbb{Z}_p$ upravo onaj traženi. Time smo dokazali ovu lemu. □

Uz pomoć prethodne leme dokazat ćemo jedan koristan teorem koji nam govori kako od rješenja $(\text{mod } p^n)$ dolazi do rješenja jednadžbe s koeficijentima u $\mathbb{Z}_p$.

**Teorem 2.3.7.** *Neka je $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x = (x_i) \in (\mathbb{Z}_p)^m$, $n, k, j \in \mathbb{Z}$ takvi da je $0 \leq j < m$. Pretpostavimo da je $0 \leq 2k < n$ i da je*

$$f(x) \equiv 0 (\text{mod} p^n), \; v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k.$$

*Tada postoji nultočka $y$ od $f \in (\mathbb{Z}_p)^m$ za koju vrijedi $y \equiv x (\text{mod} p^{n-k})$.*

*Dokaz.* Promotrit ćemo prvo slučaj kada je $m = 1$. Primjenjivši gornju lemu na $x^{(0)} = x$, dobivamo da je $x^{(1)} \in \mathbb{Z}_p$ kongurentan sa $x^{(0)} (\text{mod} p^{n-k})$ i za koji vrijedi

$$f(x^{(1)}) \equiv 0 (\text{mod} p^{n+1})$$

i

$$v_p(f'(x^{(1)})) = k.$$

Na dobiveni $x^{(1)}$ također možemo primijeniti lemu, uz zamijenu $n$ sa $n + 1$. Nastavljajući dalje tako, konstruiramo niz $x^{(0)}, x^{(1)}, \ldots, x^{(q)}, \ldots$ takav da je

$$x^{(q+1)} \equiv x^{(q)} (\text{mod} p^{n+q-k}), \; f(x^{(q)}) \equiv 0 (\text{mod} p^{n+q}).$$

Taj niz, uz metriku na $\mathbb{Z}_p$ definiranu sa $d(x, y) = e^{-v_p(x-y)}$, očigledno je Cauchyjev niz zbog jednakosti $x^{(q+1)} \equiv x^{(q)} (\text{mod} p^{n+q-k})$. Ujedno, taj niz je i konvergentan jer je $\mathbb{Z}_p$ uz promatranu metriku potpun metrički prostor. Dakle, postoji $y = \lim_q x^{(q)}$ i za njega, iz jednakosti $f(x^{(q)}) \equiv 0 (\text{mod} p^{n+q})$ očigledno vrijedi $f(y) = 0$ u $\mathbb{Z}_p$, a uzastopnm primjenom jednakosti $x^{(q+1)} \equiv x^{(q)} (\text{mod} p^{n+q-k})$ dobivamo da je $y \equiv x (\text{mod} p^{n-k})$. Prema tome, pronašli smo traženi $y$ i time je teorem dokazan za slučaj $m = 1$.
Promotrimo sad općeniti slučaj, tj. kada je $m > 1$. Općeniti slučaj možemo svesti na slučaj $m = 1$ prilagođavajući samo $x_j$. Preciznije, to ćemo napraviti na

sljedeći način. Neka je $\tilde{f} \in \mathbb{Z}_p[X_j]$ polinom u jednoj varijabli kojeg dobivamo iz $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ tako da $X_i$ zamijenimo s $x_i$ (odnosno koordinatama iz $x$), $\forall i \neq j$, odnosno $\tilde{f}(z) = f(x_1, \ldots, z, \ldots, x_m), \forall z \in X_j$. Primijenimo li iznad dokazano na $\tilde{f}$ i $x_j$ (zbog pretpostavki teorema zadovoljavaju potrebne uvijete), dobivamo da postoji $y_j \in \mathbb{Z}_p$ takav da vrijedi $\tilde{f}(y_j) = 0$ i $y_j \equiv x_j (\text{mod } p^{n-k})$. Ako sad stavimo $y_i = x_i, \forall i \neq j$, dobivamo element $y = (y_i)$ koji zadovoljava tražene uvijete. Doista, tada je $f(y) = f(x_1, \ldots, y_j, \ldots, x_m) = \tilde{f}(y_j) = 0$ i očigledno je $y \equiv x (\text{mod } p^{n-k})$, čime je teorem dokazan. □

Na kraju ćemo dokazati i neke korolare ovog teorema u kojima ćemo vidjeti njegovu uporabu u pojedinim specijalnim slučajevima.

**Korolar 2.3.8.** *Od svake jednostavne nultočke redukcije modulo p polinoma f možemo doći do nultočke od f s koeficijentima u* $\mathbb{Z}_p$.

*Dokaz.* Neka je $x$ jednostavna nultočka redukcije modulo $p$ polinoma $f$. Po definiciji, barem jedna parcijalna derivacija od $f$ modulo $p$ je različita od nule u $x$. U našem slučaju, s obzirom da promatramo polinom modulo $p$, to znači da možemo primijeniti teorem za $n = 1$ i $k = 0$ i iz toga direktno dobivamo traženu tvrdnju. □

**Korolar 2.3.9.** *Neka je* $p \neq 2$ *i* $f(X) = \sum_{i,j} a_{ij} X_i X_j$ *gdje je* $a_{ij} = a_{ji}, \forall i, j$ *kvadratna forma s koeficijentima u* $\mathbb{Z}_p$ *čija diskriminanta od* $\det(a_{ij})$ *je invertibilna. Neka je* $a \in \mathbb{Z}_p$. *Od svakog primitivnog rješenja jednadžbe* $f(x) \equiv a (\text{mod} p)$ *možemo doći do pravog rješenja.*

*Dokaz.* Obzirom na prethodni korolar, dovoljno je dokazati da nisu sve parcijalne derivacije od $f$ modulo $p$ jednake nuli u $x$; to znači da je $x$ jednostavna nultočka i iz prethodnog korolara slijedi tražena tvrdnja, pa dokažimo to.
Lakim računom dobivamo

$$\frac{\partial f}{\partial X_i} = 2 \sum_j a_{ij} X_j, \forall i.$$

Obzirom da je $\det(a_{ij})$ invertibilna, ona nije djeljiva sa $p$, a kako je $x = (x_i)$ primitivno rješenje, nisu svi $x_i$ djeljivi s $p$. Iz toga slijedi da postoji parcijalna derivacija od $f$ koja nije djeljiva sa $p$ u $x$, odnosno nije jednaka nula modulo $p$ u $x$, što je i trebalo dokazati. □

**Korolar 2.3.10.** *Neka je* $p = 2$ *i* $f(X) = \sum_{i,j} a_{ij} X_i X_j$ *gdje je* $a_{ij} = a_{ji}, \forall i, j$ *kvadratna forma s koeficijentima u* $\mathbb{Z}_2$ *i neka je* $a \in \mathbb{Z}_2$. *Neka je x primitivno rješenje od* $f(x) \equiv a (\text{ mod } 8)$. *Tada,od svakog takvog rješenja x možemo doći do pravog rješenja, uz uvjet da postoji parcijalna derivacija od f modulo 4 koja nije jednaka nuli u x. Taj uvijet je ispunjen ako je* $\det a_{ij}$ *invertibilna.*

*Dokaz.* Prva tvrdnja slijedi direktno iz teorema, za $n = 3$ i $k = 1$. Druga tvrdnja dokazuje se analogno kao i prethodni korolar, uzimajući u obzir faktor 2. □

# Poglavlje 3

# Primjena $p$-adskih brojeva

U ovome poglavlju dat ćemo kratki prikaz o primjeni $p$-adskih brojeva, te dokazati Strassmanov teorem koji se dokazuje upravo pomoću njih.

Kada su $p$-adski brojevi bili uvedeni smatrali su se egzotičnim dijelom čiste matematike koji nisu imali primjenu. Danas to više nije tako. Obzirom da imaju zanimljivo svojstvo da su, oni kako bi rekli, bliski kada je njihova razlika djeljiva sa visokom potencijom broja $p$, što viša potencija to su bliže. To svojstvo omogućuje $p$-adskim brojevim za kodiranje informacije o kongruencijama na taj način se ispostavilo da ima snažnu primjenu u teoriji brojeva,, uključujući, npr. u dokazu Fermatovog posljednjeg teorema koji nam kaže da ne postoje prirodni brojevi $x, y, z$, takvi da je $x, y, z \neq 0$ i broj $n$ veći od 2 koji zadovoljavaju jednadzbu: $x^n + y^n = z^n$.

Postavlja se jedno pitanje, a to je koja je glavna razlika između realnog i $p$-adskog prostora. Odgovor na to je Arhimedov aksiom koji kaže da za svaka dva realna broja $a > 0$ i $b > 0$ postoji takav prirodni broj $n$ da je $nb > a$. Prema tome aksiomu neki dani veliki segment na ravnoj liniji može se nadmašiti dodavanjem uzastopnim malim segmentima duž iste linije. Ovaj aksiom vrijedi u skupu realnih brojeva, ali ne vrijedi u $\mathbb{Q}_p$. Međutim, to je fizički aksiom koji se odnosi na preces mjerenja. Zamjena broja iz polja $\mathbb{R}$ s brojem iz $\mathbb{Q}_p$ jednako je promijeni aksioma u kvantnoj fizici.

Prva istraživanja teorije $p$-adskog niza izazavala su istraživanja na $p$-adskoj kvantnoj mehanici i teoriji polja. Ta istraživanja izazvala su razvoj $p$-adske matematike u više smjerova: teorija distribucije, diferencijalne i pseudodiferencijalne jednadžbe, teoriju vjerojatnosti, spektralnu teoriju operatora u $p$-adskoj analogiji Hilbertovog prostora. Zastupljenost $p$-adskih brojeva po sekvencama njegovih kombinacija znamenki nam pruža mogućnost njihove primjene u sustavu za kodiranje informacija.

Stoga, $p$-adski modeli se mogu koristiti za opise mnogih informacijskih procesa. Posebno se mogu koristiti u kognitivnoj znanosti, psihologiji i socijologiji. Takvi modeli temeljeni su na $p$-adskim dinamčkim sustavima.

Osim Arhimedovog aksioma još nam jedan teorem ističe razliku između realne i $p$-adske analize, a to je Strassmannov teorem. On također ima primjenu u situacijama u kojima stvarno ne bi očekivali da će takav rezultat biti koristan. Njegov dokaz je jednostavan, no da bi ga dokazali potrebna nam je sljedeća lema.

**Lema 3.0.11.** *Neka je $k$ polje koje je potpuno na kojem vrijedi nearhimedska vijednost $|\cdot|$. Neka su $b_{ij} \in k$ za $i, j = 0, 1, 2, \ldots$ Pretpostavimo da za svaki $\epsilon > 0$ postoji $J(\epsilon)$ takav da je $|b_{ij}| < \epsilon$ kad je $\max(i, j) \leq J(\epsilon)$. Tada nizovi*

$$\sum_i \left( \sum_j b_{ij} \right) \qquad i \qquad \sum_j \left( \sum_i b_{ij} \right)$$

*konvergiraju i jednaki su.*

*Dokaz.* Imajmo na umu da u nearhimedskom slučaju niz konvergira ako i samo ako uvjeti koji se zbrajaju teže 0. Imamo da je $b_{ij} \to 0$ tako da

$$\sum_j b_{ij} \qquad i \qquad \sum_i b_{ij}$$

obje konvergiraju. Primjenom ultrametričke nejednakosti imamo da je

$$\left| \sum_j b_{ij} \right| \leq \max_j |b_{ij}| \overset{i \to \infty}{\to} 0,$$

tako da prva dvostruka suma konvergira, slično je i za drugu dvostruku sumu. Imajmo na umu da i za konačne sume razmještaj $i$ i $j$ nije bitan, posebno imamo

$$\sum_{i=0}^{J(\epsilon)} \left( \sum_{j=0}^{J(\epsilon)} b_{ij} \right) \qquad i \qquad \sum_{j=0}^{J(\epsilon)} \left( \sum_{i=0}^{J(\epsilon)} b_{ij} \right)$$

Ponovno, primjenom ultrametričke nejednakosti imamo

$$\left| \sum_{i=0}^{J(\epsilon)} \left( \sum_{j=0}^{J(\epsilon)} b_{ij} \right) - \sum_{j=0}^{\infty} \left( \sum_{i=0}^{\infty} b_{ij} \right) \right| = \left| \sum_i \sum_j b_{ij} \right|_{\max(i,j) > J(\epsilon)} \leq \max_{i,j,s.t.} |b_{ij}|_{\max(i,j) > J(\epsilon)} < \epsilon.$$

slično je i kad $i$ i $j$ zamijene mjesta.

$$\begin{aligned}
&\left|\sum_i\left(\sum_j b_{ij}\right)-\sum_j\left(\sum_i b_{ij}\right)\right| \\
&=\left|\textstyle\sum_i\left(\sum_j b_{ij}\right)-\sum_{i=0}^{J(\epsilon)}\left(\sum_{j=0}^{J(\epsilon)} b_{ij}\right)+\sum_{i=0}^{J(\epsilon)}\left(\sum_{j=0}^{J(\epsilon)} b_{ij}\right)-\sum_j\left(\sum_i b_{ij}\right)\right| \\
&\leq \max\left\{\left|\sum_{i=0}^{J(\epsilon)}\left(\sum_{j=0}^{J(\epsilon)} b_{ij}\right)-\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right\},\left\{\left|\sum_{i=0}^{J(\epsilon)}\left(\sum_{j=0}^{J(\epsilon)} b_{ij}\right)-\sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right|\right\} \\
&<\epsilon
\end{aligned}$$

Stoga su dva niza jednaka. □

Dakle, ne samo da je mnogo jednostavnije odrediti da li jedan niz konvergira $p$-adski, nego se je mnogo jednostavnije baviti s dvostrukim sumama. Što je lijepo. Sada kada imamo gornje rezultate, možemo dokazati i Strassmannov teorem.

**Teorem 3.0.12.** ***Strassmannov teorem*** *Neka je $k$ potpuno polje u odnosu na nearhimedsku apsolutnu vrijednost $|\cdot|$, i neka je*

$$f(X)=\sum_{n=0}^{\infty} f_n X^n$$

*Pretpostavimo da $f_n \to 0$, ali da nisu svi $f_n$ nule. Tada postoji konačan broj $b$-ova, $b \in \mathcal{O}_k$ takvih da je $f(b)=0$. Točnije, postoji najviše $N$ takvih $b$-ova, gdje je $N$ definiran sa*

- $|f_N|=\max|f_n|$
- $|f_n|<|f_N|$ *za sve* $n>N$.

*Odnosno, $N$ je indeks posljednjeg maksimalnog koeficijenta.*

Posebno ćemo se baviti slučajem kad je $k=\mathbb{Q}_p, \mathcal{O}_k=\mathbb{Z}_p, |\cdot|=|\cdot|_p$. Uspoređujući gornju situaciju za potencije nizova za sinus i kosinus, koji zadovoljavaju sve hipoteze nad poljem $\mathbb{R}$, ali samo koji imaju beskonačno mnogo nultočaka. To nije moguće u $\mathbb{Q}_p$. Dokaz Strassmannovog teorema se izdvodi indukcijom po $N$.

*Dokaz.* Pretpostavimo da je $N=0$. Ako je teorem istinit, funkcija $f$ neće imati nultočaka u prstenu cijelih brojeva, tako da možemo pretpostaviti da postoji $b \in \mathcal{O}_k$ za koji vrijedi da je $f(b)=0$. Tako da imamo

$$f_0=-\sum_{n\geq 1} f_n b^n.$$

Ali, koristeći ultrametričku nejednakost i činjenicu da je $|f_n| < |f_0|$ za sve $n > 0$ imamo da je

$$\left| \sum_{n\geq 1} f_n b^n \right| \leq max_{n\geq 1}|f_n| < |f_0|$$

što je kontradikcija. Tako da ne postoji takav $b$.

Dalje, promotrimo situaciju za neke $N < 0$. Pretpostavimo da je $f(b) = 0$ za neke $b \in \mathcal{O}_k$ i neka je $c \in \mathcal{O}_k$. Tada

$$f(c) = f(c) - f(b) = \sum_{n\geq 1} f_n(c^n - b^n) = (c-b)\sum_{n\geq 1}\sum_{j=1}^{n-1} f_n c^j b^{n-1-j}.$$

Po prethodno dokazanoj lemi možemo "srediti" ovu dvostruku sumu na sljedeći način

$$f(c) = (c-b)\sum_{j=1}^{\infty}\sum_{n\geq j} f_n b^{n-1-j}c^j = (c-b)\sum_{j=1}^{\infty} c^j \sum_{r\geq 0} f_{j+1+r}b^r.$$

Neka je

$$g(X) = \sum_{j\geq 1} g_j X^j$$

gdje je

$$g_j = \sum_{r\geq 0} f_{j+1+r}b^r,$$

tada je

$$f(c) = (c-b)g(c).$$

Sada, za sve $j$ imamo

$$|g_j| = \left| \sum_{r\geq 0} f_{j+1+r}b^r \right| \leq \max_{r\geq 0}|f_{j+1+r}b^r| \leq \max_{r\geq 0}|f_{j+1+r}| \leq |f_N|.$$

Također imamo i

$$|g_{N-1}| = \left| \sum_{r\geq 0} f_{N+r}b^r \right| = |f_N + f_{N+1}b + f_{N+2}b^2 + \ldots| = |f_N|.$$

Konačno, za $j > N-1$ imamo

$$|g_j| \leq \max_{r\geq 0}|f_{j+1+r}| < |f_N|.$$

Dakle, $g(X)$ zadovoljava pretopstavku teorema, ali za $N-1$ umjesto za $N$, tako da po pretpostavci indukcije $g(X)$ ima najviše $N-1$ nultočaka $c \in \mathcal{O}_k$. Ali $f(c) = 0$ podrazumijeva da je ili $c = b$ ili $g(c) = 0$, tako da $f(X)$ ima najviše $N$ nultočaka, po potrebi. □

Strassmannov teorem ima korisnu primjenu na diofantskim jednadžbama.

# Bibliografija


[1] Axel. G.R Turnquest, $p$-adic Numbers and solving $p$-adic equations, dostupno na $https://www.math.washington.edu/\ morrow/336\_12/papers/axel.pdf$ (srpanj, 2016.)

[2] G. Bachman, Introduction to $p$-adic Numbers and valuation theory, Academic Press, 1964.

[3] F. Q. Guevea, $p$-adic Numbers, Springer, 1997.

[4] N. Koblitz, $p$-adic Numbers, $p$-adic Analysis, and Zeta-Functions, Springer, 1984.

[5] $p$-adska analiza i primjene, dostupno na web.math.pmf.unizg.hr/nastava/studnatj/notes1.pdf, (kolovoz, 2016.)

[6] $p$-adic integers and $p$-adic numbers, dostupno na www.spms.ntu.edu.sg/ frederique/antchap5.pdf (srpanj, 2016.)

[7] U. A. Rozikov, What are $p$adic Numbers? What are They Used for?, dostupno na $www.asiapacific-mathnews.com/03/0304/0001\_0006.pdf$ (srpanj, 2016.)

[8] J.P Serre, A course in Aritmetic, Springe, 1973.

[9] Strassmann's theorem, dostupno na www.maths.bris.ac.uk/ malab/PDFs/Strassmann.pdf (srpanj, 2016.)

# Sažetak

U ovome diplomskom radu bavimo se $p$-adskm brojevima, pri čemu je naglasak na jednadžbama s $p$-adskim brojevima.

U prvom poglavlju uvodimo $p$-adske ciijele i $p$-adske brojeve promatrajući analogiju između prstena cijelih brojeva, $\mathbb{Z}$, zajedno s poljem razlomaka $\mathbb{Q}$ i prstenom polinoma s koeficijentima iz skupa kompleksih brojeva, $\mathbb{C}[X]$, zajedno s poljem razlomaka od $\mathbb{C}[X]$. Zatim u idućem potpoglavlju se bavimo $p$-adskom apsolutnom vijednošću u kojem dokazujemo i teorem Ostrowskog koji povezuje svaku netrivijalnu apsolutnu vrijednost na polju $\mathbb{Q}$ i $p$-adsku apsolutnu vrijednost. Na kraju prvog poglavlja dajemo kratki pregled "dobrih" i "loših" svojstava $p$-adskih brojeva uspoređujući ih s racionalnim brojevima.

U drugom poglavlju se prvo bavimo računanjem u $\mathbb{Q}_p$. Pri čemu posebnu pažnju dajemo postojanju drugog korijena u polju $\mathbb{Q}_p$. Već nam to predstavlja lagani uvod za jednadžbe s $p$-adskim brojevima. Nakon toga rješavamo kongruencije modulo $p^n$ koje sad već dovoljno "bliske" jednadžbama u $p$-adskim brojevima, da bi ih mogli smatrati jednadžbama s $p$-adskim brojevima. Zatim dajemo neke važne rezultate o rješenjima jednadžbi s $p$-adskim brojevima čiji su koeficijenti $p$-adski cijeli brojevi. Što je bio i cilj ovoga rada.

U zadnjem poglavlju dajemo kratki sažetak u kojem je vidljiva primjena $p$-adskih brojeva.

# Summary

In this thesis we deal with the $p$-adic numbers, with the emphasis on equations with $p$-adic numbers.

In the first chapter, we introduce the $p$-adic nad integers numbers by looking at the analogy between the ring of integers, $\mathbb{Z}$, together with the field of fractions $\mathbb{Q}$ and the ring of polynomials with coefficients from a set of complex numbers, $\mathbb{C}[X]$, together with the field of fractions of $\mathbb{C}[X]$. Then in the next subsection we deal with the $p$-adic absolute value in which we prove a theorem and Ostrowski that connects each nontrivial absolute value of the field $\mathbb{Q}$ and the $p$-adic absolute value. At the end of the first chapter we give a brief outline of "good" and "bad" properties of $p$-adskih numbers by comparing them with rational numbers.

In the second chapter, we first deal with calculations in $\mathbb{Q}_p$. Special attention is given to the existence of square roots in the field $\mathbb{Q}_p$. For us, this represent a slight introduction to the equation with $p$-adic numbers. After that we solve congruences modulo $p^n$ whichare now sufficiently "close" to equations in $p$-adic numbers to considered them equations in $p$-adic numbers. Then we give some important results about solutions of equations in $p$-adic numbers with coefficients being $p$-adic integers. This was the aim of this work.

The last chapter gives a brief summary in which is visible on application of $p$-adic numbers.

# Životopis

Dana 3.6.1991. godine sam se rodila u Virovitici. Od 1998. do 2006. godine pohađala sam Osnovnu školu Ivane Brlić Mažuranić Virovitica. Prve četiri godine u područnoj školi u Rezovcu, a druge četiri u matičnoj školi u Virovitici. Nakon toga upisala sam Gimnaziju Petra Preradovića Virovitica, smjer: prirodoslovno-matematički, završila sam ju 2010. godine. Iste godine upisla sam preddiplomski studije Matematike, smjer: nastavnički na Prirodoslovno-matematikčkom fakultetu u Zagrebu, koji sam završila 2014. godine. Nakon čega upisujem dipomski studij Matematike, smjer: nastavnički na istom fakultetu.