

**STUDENTSKA NATJECANJA IZ MATEMATIKE**  
 **$p$ -ADSKA ANALIZA I PRIMJENE**

1. UVOD

**Definicija 1.1.** *Neka je  $K$  polje. Funkcija  $|\cdot| : K \rightarrow \mathbb{R}$  se zove apsolutna vrijednost ako za sve  $x, y \in K$  vrijedi:*

- 1)  $|x| \geq 0$  i  $(|x| = 0 \iff x = 0)$
- 2)  $|xy| = |x| \cdot |y|$
- 3)  $|x + y| \leq |x| + |y|$  (*nejednakost trokuta*).

Npr. funkcija  $|\cdot| : \mathbb{Q} \rightarrow \mathbb{Q}$  dana formulom

$$|x| = \begin{cases} x & \text{ako je } x \geq 0 \\ -x & \text{ako je } x < 0 \end{cases}$$

naziva se standardna apsolutna vrijednost. Koristili ste ju za definiciju nekih osnovnih pojmova iz realne analize kao što su limes, konvergencija, Cauchyjev niz... Kad malo detaljnije pogledate koja svojstva od  $|\cdot|$  se koriste u dokazima, vidjet ćete da su to svojstva 1)-3) iz definicije apsolutne vrijednosti pa se možemo zapitati postoje li možda neke druge (nestandardne) apsolutne vrijednosti na  $\mathbb{Q}$ ? Ako postoje, kako bi izgledala analiza koja bi bila bazirana na njima?

Uskoro ćemo vidjeti da je odgovor na prvo pitanje potvrđan, postoje takozvane  $p$ -adske apsolutne vrijednosti. Analiza koja se bazira na njima se zove  $p$ -adska analiza. Zanimljivo je što su ideje koje susrećemo u  $p$ -adskoj analizi slične idejama iz realne analize iako je priroda, odnosno motivacija iza ovih teorija potpuno različita (npr. realna analiza je vezana uz modeliranje fizikalnih fenomena dok se  $p$ -adska analiza primjenjuje u teoriji brojeva). Nakon što obradimo osnovne pojmove iz teorije primjenit ćemo ih na neke konkretne probleme iz teorije brojeva.

Prisjetimo se prvo kako koristeći standardnu apsolutnu vrijednost na polju racionalnih brojeva možemo konstruirati polje realnih brojeva.

2.  $\mathbb{R}$  KAO UPOTPUNJENJE OD  $\mathbb{Q}$

Neka je  $\mathcal{R} = \{(a_n)_n : (a_n)_n \text{ je Cauchyjev niz u } \mathbb{Q}\}$ . Lako se vidi da je  $\mathcal{R}$  zatvoren na operacije zbrajanja i množenja:

$$\begin{aligned} (x_n)_n + (y_n)_n &= (x_n + y_n)_n \\ (x_n)_n \cdot (y_n)_n &= (x_n y_n)_n. \end{aligned}$$

Kažemo da su dva niza  $(x_n)_n, (y_n)_n \in \mathcal{R}$  ekvivalentna, pišemo  $(x_n)_n \sim (y_n)_n$ , ako je  $\lim(x_n - y_n) = 0$ . Neka je  $\mathbb{R} = \mathcal{R}/\sim$  skup klasa ekvivalencija Cauchyjevih nizova. Može se provjeriti da  $\mathbb{R}$  uz operacije zbrajanja i množenja te prirodni uređaj (npr.  $(x_n)_n > (y_n)_n \iff x_n - y_n > 0$  za dovoljno velike  $n$ ) zadovoljava aksiome polja realnih brojeva.

Ovaj postupak konstrukcije polja  $\mathbb{R}$  iz polja  $\mathbb{Q}$  se naziva upotpunjenje polja  $\mathbb{Q}$  u odnosu na standardnu apsolutnu vrijednost. Na analogan način možemo konstruirati upotpunjenje polja  $\mathbb{Q}$  u odnosu na bilo koju apsolutnu vrijednost, samo u svim definicijama i dokazima zamijenimo te dvije apsolutne vrijednosti.

*Napomena.*

- a)  $\mathbb{Q} \subset \mathbb{R}$ ,  $q \mapsto (q, q, \dots, q, \dots)$ ,  $\mathbb{Q}$  je gust u  $\mathbb{R}$   
 b)  $|\cdot|$  možemo proširiti do apsolutne vrijednosti na  $\mathbb{R}$ ,  $|\cdot| : \mathbb{R} \rightarrow \mathbb{R}$ , formulom  $|(a_n)_n| := (|a_n|)_n$ .

### 3. NEARHIMEDSKA APSOLUTNA VRIJEDNOST NA $\mathbb{Q}$

**Definicija 3.1.** Za apsolutnu vrijednost  $|\cdot|$  na  $K$  kažemo da je nearhimedska ako uz nejednakosti trokuta vrijedi i “jača” nejednakost:

$$|a + b| \leq \max\{|a|, |b|\} \quad \forall a, b \in K.$$

Ako apsolutna vrijednost nije nearhimedska, kažemo da je arhimedska.

Neka je  $p$  prost broj. Za  $n \in \mathbb{Z}$  s  $\text{ord}_p(n)$  označavamo točnu potenciju od  $p$  koja dijeli  $n$ , tj.  $p^{\text{ord}_p(n)} \mid n$ . Npr.  $\text{ord}_3(-12) = 1$ . Za  $\frac{a}{b} \in \mathbb{Q}$  definiramo

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

Npr.  $|\frac{7}{12}|_3 = 3$ ,  $|p^{100}|_p = p^{-100}$ .

**Propozicija 3.2.**  $|\cdot|$  je nearhimedska apsolutna vrijednost na  $\mathbb{Q}$ . Naziva se  $p$ -adska apsolutna vrijednost.

Ako je  $|\cdot|$  apsolutna vrijednost, onda je i  $|\cdot|^\alpha$  apsolutna vrijednost za svaki  $\alpha \in \mathbb{R}^\times$ . Takve dvije apsolutne vrijednosti induciraju istu topologiju na  $K$  (imaju jednake Cauchyjeve nizove) pa kažemo da su ekvivalentne.

**Teorem 3.3** (Ostrowski). Svaka netrivialna apsolutna vrijednost na  $\mathbb{Q}$  je ekvivalentna običnoj apsolutnoj vrijednosti ili  $p$ -adskoj apsolutnoj vrijednosti za neki prost broj  $p$ .

### 4. $p$ -ADSKI BROJEVI I $p$ -ADSKI CIJELI BROJEVI

**Definicija 4.1.** 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  $|\cdot|_p$ . Skup

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

zovemo prsten  $p$ -adskih brojeva.

*Napomena.* Lako se provjeri da je skup  $\mathbb{Z}_p$  zatvoren u odnosu na zbrajanje i množenje te da zadovoljava uobičajene aksiome prstena. Također, za  $x = (x_n)_n \in \mathbb{Q}_p$ , imamo da je  $|x|_p = \lim |x_n|_p$ .

Kako “izgledaju” elementi od  $\mathbb{Q}_p$  i  $\mathbb{Z}_p$ ? Npr. znamo  $\mathbb{Q} \subset \mathbb{Q}_p$  i  $\mathbb{Z} \subset \mathbb{Z}_p$ .

Prije nego što odgovorimo na ovo pitanje istražiti ćemo neka svojstva specifična za nearhimedske apsolutne vrijednosti.

**Lema 4.2.** Neka su  $a, b \in \mathbb{Q}_p$ . Ako je  $|a|_p > |b|_p$  onda je  $|a + b|_p = |a|_p$ .

*Proof.* Iz nejednakosti trokuta i pretpostavke leme slijedi  $|a + b|_p \leq |a|_p$ . Imamo

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

Kako je  $|a|_p > |b|_p$  slijedi da je  $|a|_p \leq |a + b|_p$  pa tvrdnja slijedi.  $\square$

**Lema 4.3.** Neka su  $x_1, \dots, x_n \in \mathbb{Q}_p$ . Tada vrijedi

$$|x_1 + \dots + x_n|_p \leq \max\{|x_1|_p, \dots, |x_n|_p\}.$$

*Proof.* Koristeći nearhimedsku nejednakost trokuta, tvrdnja se dokaže indukcijom po  $n$ .  $\square$

**Lema 4.4.** Neka je  $K(s, r) = \{x \in \mathbb{Q}_p : |x - s|_p \leq r\}$  krug radijusa  $r > 0$  sa središtem u  $s \in \mathbb{Q}_p$ . Tada je svaki  $x \in K(s, r)$  središte tog istog kruga.

*Proof.* Neka je  $x \in K(s, r)$ . Pokažimo da je  $x$  središte tog kruga. Za  $a \in K(s, r)$  vrijedi  $|x - a|_p \leq \max\{|x - s|_p, |a - s|_p\} \leq r$ . Obratno, neka je  $a \in \mathbb{Q}_p$  takav da je  $|x - a|_p \leq r$ . Tada je  $|s - a|_p \leq \max\{|s - x|_p, |x - a|_p\} \leq r$ . □

*Primjer.* Neka su  $a_0, \dots, a_n \in \{0, 1, \dots, p-1\}$ . Tada je  $|a_0 + a_1p + \dots + a_np^n|_p = p^{-i}$  gdje je  $i$  najmanji indeks za koji je  $a_i \neq 0$ . Npr.  $|3 + 2 \cdot 3^2 + 1 \cdot 3^6|_3 = 3^{-1}$ .

**Propozicija 4.5.** Neka je  $(b_k)_{k \in \mathbb{N}_0}$ ,  $b_k \in \{0, 1, \dots, p-1\}$ . Tada je

$$(4.1) \quad \alpha = \sum_{k=0}^{\infty} b_k p^k$$

element prstena  $\mathbb{Z}_p$ .

*Proof.* Promotrimo niz parcijalnih suma  $c_n = \sum_{k=0}^n b_k p^k$  reda (4.1). Dokažimo da je taj niz Cauchyjev u odnosu na  $|\cdot|_p$ . Neka je  $\epsilon > 0$  i neka je  $n_0 \in \mathbb{N}$  takav da je  $p^{-n_0} < \epsilon$ . Za sve  $m > n > n_0$  imamo

$$|c_m - c_n|_p = \left| \sum_{k=n+1}^m b_k p^k \right|_p = |p^{n+1}|_p \cdot \left| \sum_{k=n+1}^m b_k p^{k-n-1} \right|_p \leq \frac{1}{p^{n+1}} \cdot 1 < \epsilon.$$

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

*Primjer.*

$$\frac{1}{1+p} = 1 - p + p^2 - p^3 + \dots = 1 + p(p-1) + p^3(p-1) + \dots + p^{2k+1}(p-1) + \dots \in \mathbb{Z}_p.$$

$p$ -adske znamenke broja  $\frac{1}{1+p}$  su  $(1, p-1, 0, p-1, 0, p-1, \dots)$ .

*Napomena.* Primjetimo da za  $\alpha \in \mathbb{Q}_p$  i  $n \in \mathbb{Z}$  takav da je  $|\alpha|_p \leq p^n$  vrijedi da je  $p^n \cdot \alpha \in \mathbb{Z}_p$ , pa je dovoljno istražiti kako "izgledaju" elementi iz  $\mathbb{Z}_p$ .

Vrijedi i obrat gornje propozicije, svaki element iz  $\mathbb{Z}_p$  se može prikazati u obliku (4.1). No, da bi to dokazali trebaju nam još neke činjenice o  $\mathbb{Q}_p$ .

**Propozicija 4.6.**

- 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).

*Proof.* 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  $m, n \geq n_0$  vrijedi  $|a_m - a_n|_p < \epsilon$ . Neka je  $\beta = (a_{n_0}, a_{n_0}, \dots, a_{n_0}, \dots) \in \mathbb{Q} \subset \mathbb{Q}_p$ . Pokažimo da je  $|\alpha - \beta|_p \leq \epsilon$ . Po definiciji treba dokazati  $\lim_n |a_n - a_{n_0}|_p \leq \epsilon$ . Za  $n > n_0$  vrijedi  $|a_n - a_{n_0}|_p < \epsilon$  pa tvrdnja slijedi. b) Za vježbu. □

*Napomena.* Slično se pokaže da je  $\mathbb{Z}$  gust u  $\mathbb{Z}_p$ .

Primjetimo da je za sve  $x, y \in \mathbb{Z}$  i  $m \in \mathbb{N}$

$$x \equiv y \pmod{p^m} \iff |x - y|_p \leq p^{-m}.$$

Motivirani time, za sve  $x, y \in \mathbb{Z}_p$  i  $m \in \mathbb{N}$  definiramo

$$x \equiv y \pmod{p^m} \iff \frac{x - y}{p^m} \in \mathbb{Z}_p.$$

(Dva elementa  $x, y \in \mathbb{Z}_p$  su "blizu", ako su kongruentni modulo "velikoj" potenciji od  $p$ .)

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

**Lema 4.7.** Za svaki  $\alpha \in \mathbb{Z}_p$  i za svaki  $m \in \mathbb{N}$  postoji jedinstven  $a_m \in \mathbb{Z}$  takav da je

$$\alpha \equiv a_m \pmod{p^m} \quad i \quad 0 \leq a_m \leq p^m.$$

Sada možemo dokazati obrat Propozicije 4.5.

**Propozicija 4.8.** Svaki element  $\alpha \in \mathbb{Z}_p$  se može na jedinstven način prikazati kao red

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

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

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

## 5. $p$ -ADSKA ANALIZA

$p$ -adska analiza je lakša od realne što zorno prikazuje sljedeća činjenica - nužan uvjet konvergencije reda u  $\mathbb{Q}_p$  je i dovoljan.

**Propozicija 5.1.** Neka je  $(a_k)_{k=0}^{\infty}$  niz u  $\mathbb{Q}_p$ . Tada

$$\text{red } \sum_{k=0}^{\infty} a_k \text{ konvergira} \iff \lim_k a_k = 0.$$

*Proof.* Pretpostavimo da  $\sum a_k$  konvergira k  $\alpha \in \mathbb{Q}_p$ . Tada je za svaki  $n \in \mathbb{N}$

$$a_n = \sum_{k=0}^n a_k - \sum_{k=0}^{n-1} a_k,$$

pa prelaskom na limes dobivamo  $\lim a_n = \alpha - \alpha = 0$ .

Pretpostavimo da je  $\lim a_n = 0$ . Neka je  $\alpha_n = \sum_{k=0}^n a_k$   $n$ -ta parcijalna suma reda  $\sum a_k$ . Pokažimo da je niz  $(\alpha_n)_n$  Cauchyjev. Neka je  $\epsilon > 0$ . Tada postoji  $n_0 \in \mathbb{N}$ , takav da za svaki  $k > n_0$  vrijedi  $|a_k|_p < \epsilon$ . Za sve  $m, n \in \mathbb{N}$ ,  $m > n \geq n_0$  vrijedi

$$|\alpha_m - \alpha_n|_p = \left| \sum_{k=n+1}^m a_k \right|_p \leq \max\{|a_{n+1}|_p, \dots, |a_m|_p\} < \epsilon.$$

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

Osim konvergencije, u  $p$ -adskoj analizi se ne moramo brinuti ni o redosljedu sumacije.

**Propozicija 5.2.** Neka je  $\sum_{k=0}^{\infty} a_k$  konvergentan red u  $\mathbb{Q}_p$  i neka je  $\sigma$  bijekcija sa  $\mathbb{N}_0$  u  $\mathbb{N}_0$ . Tada vrijedi

$$\sum_{k=0}^{\infty} a_{\sigma(k)} = \sum_{k=0}^{\infty} a_k.$$

*Proof.* Neka je  $S_m = \sum_{k=0}^m a_k - \sum_{k=0}^m a_{\sigma(k)}$ . Treba dokazati da je  $\lim_m S_m = 0$ . Neka je  $\epsilon > 0$ . Odaberimo  $n \in \mathbb{N}$  takav da je  $|a_k|_p < \epsilon$  za sve  $k \geq n$ . Neka je  $n_0$  takav da skup  $\{\sigma(0), \sigma(1), \dots, \sigma(n_0)\}$  sadrži skup  $\{0, 1, \dots, n\}$ . Tada za svaki  $m > n_0$ ,  $S_m$  sadrži samo elemente  $a_k$  čiji je indeks  $k > n$ , odnosno čija je apsolutna vrijednost manja od  $\epsilon$ . Kako je prema nearhimedskoj nejednakosti trokuta zbroj takvih elemenata manji od  $\epsilon$ , slijedi da je  $|S_m|_p < \epsilon$  za sve  $m > n_0$ .  $\square$

Posebno će nas zanimati redovi potencija,

$$f(x) = \sum_{k=0}^{\infty} a_k (x - x_0)^k,$$

gdje je  $x_0, a_k \in \mathbb{Q}_p$  za sve  $k$ . Koristeći Propoziciju 5.1 možemo lako okarakterizirati područje konvergencije ovog reda. Vrijedi

$$f(x) \text{ konvergira na } K(x_0, p^{-m}) \iff \lim_k |a_k|_p p^{-mk} = 0.$$

Posebno,  $f(x)$  konvergira na  $\mathbb{Z}_p = B(0, 1)$  ako i samo ako  $\lim_k |a_k|_p = 0$ . Promotrimo skup redova potencija koji konvergiraju na  $\mathbb{Z}_p$

$$\mathcal{O} = \left\{ \sum_{k=0}^{\infty} a_k x^k : a_k \in \mathbb{Z}_p \text{ za sve } k \geq 0, \lim_k |a_k|_p = 0 \right\}.$$

Lako se vidi da je ovaj skup prsten u odnosu na zbrajanje i množenje redova potencija. Također  $\mathcal{O}$  sadrži polinome  $\mathbb{Z}_p[x]$ .

Red  $f(x)$  ima konačno mnogo nultočaka koje su iz  $\mathbb{Z}_p$ . Gornja ograda za njihov broj se može odrediti iz apsolutnih vrijednosti koeficijenata reda koristeći sljedeći teorem.

**Teorem 5.3** (Strassman). *Neka je  $f(x) = \sum_{k=0}^{\infty} a_k x^k \in \mathcal{O}$  red potencija različit od 0. Neka je  $k_0$  indeks takav da vrijedi*

$$|a_k|_p \leq |a_{k_0}|_p \text{ za sve } k \leq k_0, |a_k|_p < |a_{k_0}|_p \text{ za sve } k > k_0.$$

Tada  $f(x)$  ima najviše  $k_0$  nultočaka u  $\mathbb{Z}_p$ .

## 6. STRASSMANOV TEOREM I DIOFANTSKE JEDNADŽBE

Primjenu  $p$ -adske analize na diofantske jednadžbe ćemo ilustrirati na sljedećem primjeru.

*Primjer.* (Ostrava 2015.) Odredite sve parove prirodnih brojeva  $(m, t)$  koji zadovoljavaju jednadžbu

$$5^t = 6m^2 + 1.$$

Promatrajući jednadžbu modulo 3, vidimo da  $t$  mora biti paran, npr.  $t = 2n$ . Jednadžbu možemo faktorizirati na sljedeći način:

$$\begin{aligned} 5^{2n} &= (1 - m\sqrt{-6})(1 + m\sqrt{-6}) \\ (1 - 2\sqrt{-6})^n (1 + 2\sqrt{-6})^n &= (1 - m\sqrt{-6})(1 + m\sqrt{-6}). \end{aligned}$$

Ovo sad možemo interpretirati kad jednadžbu u  $\mathbb{Z}[\sqrt{-6}]$  pa koristeći teoriju djeljivosti tog prstena zaključujemo

$$(6.1) \quad 1 - m\sqrt{-6} = \pm(1 \pm 2\sqrt{-6})^n.$$

Malo detaljnije (ako niste upoznati s osnovama algebarske teorije brojeva ovaj odjeljak možete preskočiti),  $\mathbb{Z}[\sqrt{-6}]$  nije prsten jedinstvene faktorizacije (njegov broj klasa je 2), pa gornja tvrdnja ne slijedi direktno iz činjenice da su brojevi  $1 - m\sqrt{-6}$  i  $1 + m\sqrt{-6}$  relativno prosti nego je još potrebno primjetiti da ideal (5) ima dva prosta faktora (to su  $(5, 2 + \sqrt{-6})$  i  $(5, 3 + \sqrt{-6})$ , gdje  $(a, b)$  označava ideal generiran sa  $a, b \in \mathbb{Z}[\sqrt{-6}]$ ) i da 5 ne dijeli brojeve  $1 - m\sqrt{-6}$  i  $1 + m\sqrt{-6}$ . Tvrdnja onda slijedi iz jedinstvene faktorizacije ideala u  $\mathbb{Z}[\sqrt{-6}]$ .

Nakon uspoređivanja odgovarajućih koeficijenata u (6.1) dobivamo

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} (\pm 2\sqrt{-6})^{2k} = \pm 1, \text{ odnosno}$$

$$\sum_{k=0}^{\infty} \binom{n}{2k} (-24)^k = \pm 1.$$

Primjetimo da funkciju

$$f(n) = \sum_{k=0}^{\infty} \binom{n}{2k} (-24)^k,$$

možemo proširiti sa prirodnih brojeva na  $\mathbb{Z}_2$ . Naime, lako se provjeri da je za sve  $n \in \mathbb{Z}_2$ ,  $\binom{n}{2k} := \frac{n(n-1)\cdots(n-2k+1)}{(2k)!} \in \mathbb{Z}_2$ , pa red  $f(n)$  konvergira za svaki  $n \in \mathbb{Z}_2$  (opći član reda teži u 0).

Poznata je činjenica da je  $\text{ord}_2(2k)! = \lfloor \frac{2k}{2} \rfloor + \lfloor \frac{2k}{4} \rfloor + \cdots < \frac{2k}{2} + \frac{2k}{4} + \cdots = 2k$  iz čega slijedi da je  $\text{ord}_2 \frac{(-24)^k}{(2k)!} > 3k - 2k = k$ .

Koristeći Propoziciju 5.2 i prethodnu činjenicu funkciju  $f(n)$  možemo zapisati pomoću konvergentnog reda potencija u  $n$ , tj. kao

$$f(n) = \sum_{k=0}^{\infty} a_k n^k,$$

gdje je  $a_k \in \mathbb{Z}_2$  za svaki  $k$ .

Zanimaju na 2-adske nultočke reda  $f(n) \pm 1$ . Gornju ogradu za njihov broj ćemo dobiti preko Strassmanovog teorema.

Prema gornjoj analizi

$$f(n) \equiv 1 + \binom{n}{2} (-24) \pmod{2^3},$$

pa vrijedi  $f(n) \equiv -12n^2 + 12n + 1 \pmod{2^3}$ . Sad imamo dva slučaja. Ako za  $n_0 \in \mathbb{N}_0$  vrijedi  $f(n_0) = -1$ , iz Strassmanovog teorema primijenjenog na  $f(n) + 1 \equiv 2 - 12n^2 + 12n \pmod{2^3}$  slijedi da to nije moguće. Ako je  $f(n_0) = 1$ , onda primjenom Strassmanovog teorema na  $f(n) - 1 \equiv 12n - 12n^2 \pmod{2^3}$  dobivamo da postoje najviše dva takva rješenja. Lako se provjeri da su  $n_0 = 0$  i  $n_0 = 1$  rješenja dane jednadžbe iz čega slijedi da su  $(0, 0)$ ,  $(2, 2)$  i  $(-2, 2)$  jedina cjelobrojna rješenja polazne jednadžbe.

## 7. ZADACI

Rok za predaju rješenja je 1.7.2024. Trebate riješiti barem 4 zadatka.

**Zadatak 1** Odredite  $p$ -adski razvoj brojeva  $-1 \in \mathbb{Z}_p$  i  $\frac{1}{10} \in \mathbb{Q}_{11}$ . Je li  $\mathbb{Z}_p$  prebrojiv?

**Zadatak 2** Izračunajte

- $1 + p + p^2 + \cdots + p^n + \cdots \in \mathbb{Q}_p$
- $1 - p + p^2 - p^3 + \cdots + (-1)^n p^n + \cdots \in \mathbb{Q}_p$
- $1 + (p-1)p + p^2 + (p-1)p^3 + p^4 + (p-1)p^5 + \cdots \in \mathbb{Q}_p$ .

**Zadatak 3**

Neka je  $\alpha = \sum_{k=k_0}^{\infty} b_k p^k \in \mathbb{Q}_p$ , gdje je  $k_0 \in \mathbb{Z}$  i  $b_k \in \{0, \dots, p-1\}$  za svaki  $k \geq k_0$ . Ako je niz  $(b_k)$  periodičan u smislu da postoje  $d \in \mathbb{N}$  i  $m \in \mathbb{Z}$  takvi da je  $b_{k+d} = b_k$  za svaki  $k \geq m$ , dokažite da je  $\alpha \in \mathbb{Q}$ . Vrijedi li obrat?

**Zadatak 4** Definirajmo  $p$ -adsku eksponencijalnu funkciju i  $p$ -adski logaritam formulama

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \log_p(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} (x-1)^n.$$

Neka je  $p > 2$ .

- Odredite radijus konvergencije reda (odnosno domenu funkcije)  $\exp_p(x)$ .
- Odredite radijus konvergencije reda  $\log_p(x)$ .
- \* Vrijedi li  $\exp_p(x+y) = \exp_p(x)\exp_p(y)$  za sve  $x$  i  $y$  iz domene?

**Zadatak 5** ( $p$ -adaska verzija Newtonove metode)

Neka je  $f = a_n x^n + \dots + a_0 \in \mathbb{Z}_p[x]$ . Derivacija od  $f$  je  $f' = na_n x^{n-1} + \dots + a_1$ .

- Neka su  $a, x \in \mathbb{Z}_p$  i takvi da je  $x \equiv 0 \pmod{p^m}$  za neki  $m \in \mathbb{N}$ . Dokažite da je  $f(a+x) \equiv f(a) \pmod{p^m}$  i  $f(a+x) \equiv f(a) + f'(a)x \pmod{p^{2m}}$ . (Hint:  $f(a+x) \in \mathbb{Z}_p[x]$ .)
- Neka je  $x_0 \in \mathbb{Z}$  takav da je  $f(x_0) \equiv 0 \pmod{p}$  i  $f'(x_0) \not\equiv 0 \pmod{p}$ . Definirajte niz  $(x_n)_{n=0}^{\infty}$  rekursivno formulom

$$x_{n+1} := x_n - \frac{f(x_n)}{f'(x_n)} \text{ za } n \geq 0.$$

Dokažite da je  $x_n \in \mathbb{Z}_p$ ,  $f(x_n) \equiv 0 \pmod{p^{2^n}}$  i  $f'(x_n) \not\equiv 0 \pmod{p}$  za svaki  $n \geq 0$ .

- Dokažite da niz  $(x_n)$  konvergira nultočki od  $f$  u  $\mathbb{Z}_p$ .
- Dokažite da  $f$  ima točno jednu nultočku  $\xi \in \mathbb{Z}_p$  takvu da je  $\xi \equiv x_0 \pmod{p}$ .
- Koristeći prethodne tvrdnje odredite  $\sqrt{-7}$  u  $\mathbb{Q}_2$  na pet "decimala".

**Zadatak 6**

- Dokažite da za prirodne brojeve  $x$  i  $y$  te cijeli broj  $n \geq 0$  vrijedi

$$\binom{x+y}{n} = \sum_{k=0}^n \binom{x}{n-k} \binom{y}{k}.$$

- Dokažite istu formulu za  $x, y \in \mathbb{Z}_p$ .
- Neka je  $\beta \in \mathbb{Z}_p$  takav da je  $|\beta|_p \leq p^{-1}$  i neka su  $x, y \in \mathbb{Z}_p$ . Dokažite da je  $(1+\beta)^{x+y} = (1+\beta)^x (1+\beta)^y$ .

**Zadatak 7**

U ovom zadatku treba pokazati da se jedinični kvadrat ne može podijeliti na neparan broj trokuta jednake površine.

Neka je kvadrat podijeljen na  $n$  trokuta jednake površine. Označimo sa  $|\cdot|$  proširenje od  $|\cdot|_p$  na  $\mathbb{R}$ . To znači da se  $|\cdot|$  podudara sa  $|\cdot|_p$  na  $\mathbb{Q}$  i da zadovoljava uobičajene aksiome ne-arhimedske apsolute vrijednosti (kao i  $|\cdot|_p$ ).

- Obojite vrhove tih trokuta u tri boje, plavu, crvenu i zelenu, na sljedeći način:

$$P = \{(x, y) : |x| < 1, |y| < 1\}$$

$$C = \{(x, y) : |x| \geq 1, |x| \geq |y|\}$$

$$Z = \{(x, y) : |y| \geq 1, |y| > |x|\}.$$

Koristeći Spernerovu lemu dokažite da postoji trokut kojemu su svi vrhovi različitih boja.

- Dokažite da je za površinu  $P = 1/n$  tog trokuta vrijedi

$$|P| > 1,$$

odnosno da je  $n$  paran.

**Zadatak 8** Koristeći  $p$ -adsku analizu, dokažite da vrijednost izraza

$$\sum_{k=1}^{p-1} \frac{1}{(px+k)^2} \pmod{p^3}$$

ne ovisi o  $x \in \mathbb{N}$ .