МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД

из предмета

Анализа са алгебром

на тему

p-адски бројеви

Ученик:
Урош Миленковић, IV_d

Ментори:
Стеван Гајовић
Милош Ђорић

Београд, мај 2018.

Садржај

1 Увод

У овом раду проучићемо поље $\mathbb{Q}_p$ које називамо пољем p-адских бројева. Почећемо од апсолутних вредности, и приметити да на пољу рационалних бројева постоје неке необичне апсолутне вредности, са особина са којима се не сусрећемо у средњој школи. Онда ћемо, почевши од тих апсолутних вредности формирати наше поље p-адских бројева, и разматрати теореме које нам дају нуле неких полинома у овом пољу. Доказаћемо Хенселову лему, једну од најважнијих теорема у модерној теорији бројева. На крају ћемо видети како ове бројеве можемо искористити за решавање неких елементарно формулисаних проблема проблема, међу којима су представљање природног броја у облику збира квадрата природних бројева.

2 Основе

Дефиниција 2.1. *Апсолутна вредност* на пољу $\mathbb{F}$ је функција

$$|\cdot| : \mathbb{F} \to \mathbb{R}_+$$

која задовољава следећа својства:

(i) $|x| = 0 \iff x = 0$

(ii) $|xy| = |x| \cdot |y|$ за све $x, y \in \mathbb{F}$

(iii) $|x + y| \leq |x| + |y|$ за све $x, y \in \mathbb{F}$

Испоставља се да постоје два важна типа апсолутних вредности, а разликоваће се по следећој дефиницији:

Дефиниција 2.2. За апсолутну вредност $|\cdot|$ на пољу $\mathbb{F}$ кажемо да је *неархимедска* ако задовољава додатни услов:

(iv) $|x + y| \leq \max\{|x|, |y|\}$ за све $x, y \in \mathbb{F}$.

У супротном, апсолутна вредност је *архимедска*.

Један пример апсолутне вредности је класична апсолутна вредност $|\cdot|$ на пољу $\mathbb{Q}$, дефинисана са

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

Очигледно је да је ова апсолутна вредност архимедска.
Још један пример је тривијална апсолутна вредност, дата са

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

Она је дефинисана на сваком пољу, и неархимедска је.

2.1 Апсолутне вредности на пољу

Сада ћемо дефинисати апсолутне вредности које су најбитније за овај рад, и на којима се сами p-адски бројеви заснивају.
Нека је p фиксиран прост број, и нека је $n \in \mathbb{Z}$ произвољан. Број $v \in \mathbb{N}$, такав да је $n = p^v n'$ и $(p, n') = 1$ је јединствено одређен. Такође, ако је $\frac{a}{b} \in \mathbb{Q}$ неки разломак, број $v \in \mathbb{Z}$ такав да је $\frac{a}{b} = p^v \frac{a'}{b'}$ и $(p, a'b') = 1$ је јединствен. Водећи се овим, дефинишемо:

Дефиниција 2.1.1. Нека је $p \in \mathbb{Z}$ фиксиран прост број. Тада је *p-адска валуација* на $\mathbb{Q}$ функција

$$v_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$$

дефинисана са: за $n \in \mathbb{Z} \setminus \{0\}$, $v_p(n)$ је јединствен природан број такав да

$$n = p^{v_p(n)} n'$$

где $p \nmid n'$. За рационални број $x = \dfrac{a}{b}$ дефинишемо

$$v_p(x) = v_p(a) - v_p(b).$$

Често је погодно дефинисати и $v_p(0) = +\infty$, што је и логично, јер се 0 бесконачно много пута може делити са p.
Из дефиниције p-адске валуације се види да је $v_p(x)$ јединствен цео број такав да је

$$x = p^{v_p(x)} \cdot \frac{a}{b}$$

такав да $p \nmid ab$, баш како смо хтели.

Пример 1. У овом примеру ћемо одредити неке p-адске валуације, да бисмо стекли утисак о њима:

1. $v_7\left(\dfrac{5}{147}\right) = v_7(5) - v_7(147) = 0 - v_7(3 \cdot 7^2) = -2;$

2. $v_5(1000) = v_5(8 \cdot 5^3) = 3;$

3. $v_{11}\left(\dfrac{5324}{165}\right) = v_{11}(5324) - v_{11}(165) = v_{11}(4 \cdot 11^3) - v_{11}(15 \cdot 11) = 3 - 1 = 2.$

Следећа лема даје нека основна својства p-адске валуације, која ће касније бити корисна.

Лема 2.1.1. *За све $x, y \in \mathbb{Q}$ важе:*

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

(ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Доказ. Доказ се заснива на исписивању факторизација бројева x и y:

(i) Како је $xy = p^{v_p(x)}x' \cdot p^{v_p(y)}y' = p^{v_p(x)+v_p(y)} \cdot x'y'$, следи да $v_p(xy) = v_p(x) + v_p(y)$.

(ii) Нека је $v_p(x) \geq v_p(y)$. Тада $x + y = p^{v_p(x)}x' + p^{v_p(y)}y' = p^{v_p(y)} \cdot (p^{v_p(x)-v_p(y)}x' + y')$, па следи $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$, где се једнакост постиже ако $p \nmid p^{v_p(x)-v_p(y)}x' + y'$.

□

Видимо да су ова својства јако слична условима (ii) и (iv) у дефиницији апсолутне вредности, осим што је производ претворен у збир, а неједнакост обрнута. Неједнакост можемо вратити мењањем знака, а збир превести у производ стављањем га у експонент. Ово сугерише следећу, кључну дефиницију:

Дефиниција 2.1.2. За $x \in \mathbb{Q}$, дефинишемо p-адску апсолутну вредност $|\cdot|_p$ од x са:

$$|x|_p = p^{-v_p(x)}$$

за $x \neq 0$, и $|0|_p = 0$.

Често, независно од ове дефиниције, кажемо да наша уобичајена апсолутна вредност $|\cdot|$ одговара апсолутној вредности код бесконачног простог броја $p = \infty$.

Проверимо да ово заиста јесте апсолутна вредност. Својство (i) следи директно из дефиниције, јер $p^{-v_p(x)} \neq 0$. Друго својство следи из претходне леме, а треће следи из четвртог, које такође следи из леме. Дакле, ово јесте апсолутна вредност, и то неархимедска.

За разлику од p-адске валуације, p-адска апсолутна вредност је мала за бројеве који су јако дељиви са p, другим речима, она је мера дељивости неког броја са бројем p.

Пример 2. Сада ћемо одредити p-адске апсолутне вредности неких бројева, и потврдити претходно тврђење:

1. $|99|_3 = |3^2 \cdot 11|_3 = 3^{-2}$;
2. $|201684|_7 = |2^2 \cdot 3 \cdot 7^5|_7 = 7^{-5}$;
3. $\left|\frac{64}{4375}\right|_5 = |2^6 \cdot 5^{-4} \cdot 7^{-1}|_5 = 5^4$.

Записујемо да је $\lim_{n\to\infty} |p^n|_p = 0$, јер је $|p^n|_p = p^{-n}$.

2.2 Основна својства

Сада ћемо видети основна својства апсолутних вредности, дата у следећој леми:

Лема 2.2.1. *Нека је дата апсолутна вредност $|\cdot|$ на пољу $\mathbb{F}$. Тада:*

(i) $|1| = 1$

(ii) $|x^n| = 1 \Rightarrow |x| = 1$

(iii) $|-1| = 1$

(iv) $|-x| = |x|$

Доказ. (i) Имамо да је $|1| = |1^2| = |1|^2$, па како је $|1| \in \mathbb{R}_+$, и једино позитивно решење једначине $t^2 = t$ је $t = 1$, следи $|1| = 1$.

(ii) Слично као (i), важи $1 = |x^n| = |x|^n$, и једино позитивно решење једначине $t^n = 1$ је $t = 1$, следи $|x| = 1$.

(iii) $|(-1)^2| = |1| = 1$, па $|-1| = 1$.

(iv) $|-x| = |(-1) \cdot x| = |-1| \cdot |x| = |x|$.

□

Следећа теорема даће бољи увид у неархимедске апсолутне вредности, јер ћемо видети потребан и довољан услов да је апсолутна вредност неархимедска. Пре тога, за дато поље $\mathbb{F}$ дефинисаћемо пресликавање $\mathbb{Z} \to \mathbb{F}$ са

$$n \mapsto \begin{cases} \underbrace{1+1+\cdots+1}_{\text{n}} & n > 0 \\ 0 & n = 0 \\ -\underbrace{(1+1+\cdots+1)}_{\text{n}} & n < 0 \end{cases}$$

Овде је 1 заправо јединица из поља. Видимо да је, на пример, за $\mathbb{F} = \mathbb{Q}$ ово само скуп целих бројева.

Теорема 2.2.1. *Нека је $A \subset \mathbb{F}$ слика $\mathbb{Z}$ у $\mathbb{F}$. Апсолутна вредност $|\cdot|$ на $\mathbb{F}$ је неархимедска ако и само ако $|a| \leq 1$ за све $a \in A$.*

Доказ. $\underline{\Rightarrow}$: Знамо да је $|\pm 1| = 1$, па, за неархимедску $|\cdot|$ следи

$$|a \pm 1| \leq \max\{|a|, 1\}.$$

Одавде индукцијом следи да је за $a \in A$ заиста $|a| \leq 1$.
$\underline{\Leftarrow}$: Претпоставимо да је $|a| \leq 1$ за све $a \in A$. Треба доказати да за свака два $x, y \in \mathbb{F}$ важи $|x + y| \leq \max\{|x|, |y|\}$. Ако је $y = 0$, овде важи једнакост. У супротном, дељењем израза са $|y|$, видимо да треба доказати еквивалентну неједнакост:

$$\left|\frac{x}{y} + 1\right| \leq \max\left\{\left|\frac{x}{y}\right|, 1\right\},$$

а како $\dfrac{x}{y}$ може узети све вредности из $\mathbb{F}$, довољно је доказати да за $x \in \mathbb{F}$:

$$|x + 1| \leq \max\{|x|, 1\}.$$

Нека је сада $m \in \mathbb{N}$. Тада

$$\begin{aligned}
|x+1|^m = |\sum_{k=0}^{m} \binom{m}{k} x^k| \leq \\
\leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |x^k| \leq \\
\leq \sum_{k=0}^{m} |x^k| = \\
= \sum_{k=0}^{m} |x|^k \leq \\
\leq (m+1)\max\{1, |x|^m\}
\end{aligned}$$

Коришћено је $\left|\binom{m}{k}\right| \leq 1$ јер $\binom{m}{k} \in A$, као и то да је, ако је $x > 1$, највећи од $|x|^k$ једнак $|x|^m$, а 1 у супротном. Сада, узимањем m-тог корена обе стране, добијамо да је

$$|x+1| \leq \sqrt[m]{m+1}\max\{|x|, 1\}.$$

Ова једнакост заправо важи за све $m \in \mathbb{N}$, а знамо да је

$$\lim_{m\to+\infty} \sqrt[m]{m+1} = 1.$$

Дакле, ако пустимо да $m \to \infty$, добијамо да

$$|x+1| \leq \max\{|x|, 1\},$$

што је жељена неједнакост. □

Ова теорема даје бољи увид у разлику између архимедских и неархимедских апсолутних вредности. Архимедске апсолутне вредности имају следеће својство: *Архимедско својство: Ако су $x, y \in \mathbb{F}, x \neq 0$, постоји $n \in \mathbb{N}$ такав да $|nx| > |y|$.* Оно важи за уобичајену апсолутну вредност на $\mathbb{Q}$, и $\mathbb{R}$.
Ово својство тврди да постоје произвољно велики цели бројеви, односно да је

$$\sup\{|n| : n \in \mathbb{Z}\} = +\infty.$$

Дакле, претходна теорема тврди:

Последица 2.2.1.1. *Апсолутна вредност $|\cdot|$ је неархимедска ако и само ако*

$$\sup\{|n| : n \in \mathbb{Z}\} = 1.$$

2.3 Топологија

Апсолутна вредност се на пољу уводи да би се стекао осећај величине бројева у том пољу. Да бисмо причали о растојањима између бројева, потребно је увести метрику.

Дефиниција 2.3.1. *Метрика* на пољу $\mathbb{F}$ је функција

$$d : \mathbb{F} \times \mathbb{F} \to \mathbb{R}_+$$

за коју важе:

(i) За $x, y \in \mathbb{F}$, $d(x, y) \geq 0$ и $d(x, y) = 0 \iff x = y$;

(ii) За $x, y \in \mathbb{F}$, $d(x, y) = d(y, x)$;

(iii) За $x, y, z \in \mathbb{F}$, $d(x, z) \leq d(x, y) + d(y, z)$.

Последњи део теореме назива се неједнакост троугла, пошто каже да је најмањи пут између две тачке (броја), права линија, односно њихово растојање. Простор над којим је дефинисана метрика је *метрички простор*. Ако имамо познату апсолутну вредност на пољу, лако можемо направити метрику.

Теорема 2.3.1. *Нека је $\mathbb{F}$ поље са апсолутном вредношћу $|\cdot|$. Растојање $d(x, y)$ између два броја $x, y \in \mathbb{F}$ дефинишемо са*

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

Функција $d(x, y)$ је тада метрика индукована апсолутном вредношћу $|\cdot|$

Доказ. Треба проверити да функција d задовољава услове из дефиниције метрике.

(i) За $x, y \in \mathbb{F}$, $d(x, y) = |x - y| \geq 0$ и $d(x, y) = |x - y| = 0 \iff x = y$;

(ii) За $x, y \in \mathbb{F}$, $d(x, y) = |x - y| = |y - x| = d(y, x)$;

(iii) За $x, y, z \in \mathbb{F}$, $d(x, z) = |x-z| = |(x-y)+(y-z)| \leq |x-y|+|y-z| = d(x, y)+d(y, z)$. □

Такође, чињеницу да је апсолутна вредност неархимедска лако преводимо на језик метрике, преко следеће леме.

Лема 2.3.1. *Нека је $|\cdot|$ апсолутна вредност дефинисана на пољу $\mathbb{F}$, са метриком $d(\cdot, \cdot)$. Онда је $|\cdot|$ неархимедска ако и само ако, за све $x, y, z \in \mathbb{F}$ важи*

$$d(x, y) \leq \max\{d(x, z), d(z, y)\}$$

Доказ. $\underline{\Rightarrow}$: Применом неархимедског својства на једнакост

$$(x-y) = (x-z) + (z-y).$$

$\underline{\Leftarrow}$: У задатој неједнакости, ставимо $y = -y_1$ и $z = 0$:

$$|x + y_1| = |x - y| = d(x,y) \leq \max\{d(x,z), d(z,y)\} = \max\{d(x,0), d(0,-y_1)\} =$$

$$= \max\{|x|, |y_1|\} = \max\{|x|, |y|\}.$$

□

Ова неједнакост се зове *ултраметричка неједнакост*, а метрика за коју је тачна се назива *ултраметрика*. Простор који она дефинише назива се *ултраметрички простор*, чију ћемо геометрију сада мало истражити.

Теорема 2.3.2. *Нека је $|\cdot|$ неархимедска апсолутна вредност дефинисана на пољу $\mathbb{F}$. Ако $x, y \in \mathbb{F}$ и $|x| \neq |y|$, онда*

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

Доказ. Можемо претпоставити да је $|x| > |y|$. Онда је

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

Такође, како је $x = (x + y) - y$, имамо

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

али како $|x| > |y|$, претходна неједнакост може да важи само ако

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

Одавде је

$$|x + y| \geq |x|,$$

па следи да је $|x| = |x + y|$. □

Ово даје неочекивану и занимљиву последицу:

Последица 2.3.2.1. *У ултраметричком простору, сви троуглови су једнакокраки.*

Доказ. Нека су x, y, z три елемента нашег простора. Дужине страница троугла са овим теменима су $|x-y|, |y-z|, |z-x|$, а знамо да је $(x-y)+(y-z) = (x-z)$, одакле, ако је $|x-y| \neq |y-z|$, по претходној теореми следи да је $|x-z|$ једнак већем од та два броја. У сваком случају, две странице су једнаке. □

Пример 3. Посматрајмо претходни резултат на примеру p-адске апсолутне вредности, за целе бројеве x, y. Нека је $v_p(x) = a$ и $v_p(y) = b$. Знамо да је онда $x = p^a x'$ и $y = p^b y'$, и да $p \nmid x'y'$. Добијамо да је $|x| = p^{-a}$ и $|y| = p^{-b}$. Нека је $|x| > |y|$ (можемо узети без умањења општости, у супротном је $|x| = |y|$) и нека $b = a + c$. Тада

$$x + y = p^a x' + p^{a+c} y' = p^a (x' + p^c y').$$

Пошто $p \nmid x'$, знамо да $p \nmid x' + p^c y'$, одакле $v_p(x + y) = a$, па $|x + y| = p^{-a} = |x|$.
У сваком случају, две од три апсолутне вредности $|x|, |y|$ и $|x + y|$ су једнаке.

Пример 4. Посматрајмо 7-адску метрику на $\mathbb{Q}$, и троугао са теменима $x = \dfrac{2}{21}, y = \dfrac{1}{7}, z = \dfrac{3}{7}$. Његове странице су $\left|\dfrac{1}{7} - \dfrac{2}{21}\right| = \left|\dfrac{1}{21}\right| = 7$, $\left|\dfrac{1}{7} - \dfrac{3}{7}\right| = \left|\dfrac{2}{7}\right| = 7$, $\left|\dfrac{2}{21} - \dfrac{3}{7}\right| = \left|\dfrac{1}{3}\right| = 1$

Такође, важан део метричких простора су лопте.

Дефиниција 2.3.2. Нека је $\mathbb{F}$ метрички простор са метриком $d(\cdot, \cdot)$. Нека је $a \in \mathbb{F}$ елемент поља и $r \in \mathbb{R}_+$ један елемент.
Отворена лопта полупречника r је скуп

$$B(a, r) = \{x \in \mathbb{F} : d(x, a) < r\}.$$

Затворена лопта полупречника r је скуп

$$\overline{B}(a, r) = \{x \in \mathbb{F} : d(x, a) \leq a\}.$$

Пре него што видимо својства лопти, дефинишимо отворене и затворене скупове:

Дефиниција 2.3.3. Скуп U је *отворен* ако свака тачка из U припада отвореној лопти која је садржана у U. Скуп је *затворен* ако је његов комплемент отворен.

Сада ћемо видети да и лопте показују нека неочекивана својства у ултраметричким просторима.

Теорема 2.3.3. *Нека је $\mathbb{F}$ поље са неархимедском апсолутном вредношћу.*

(i) Ако $b \in B(a, r)$ онда $B(a, r) = B(b, r)$.

(ii) Ако $b \in \overline{B}(a, r)$ онда $\overline{B}(a, r) = \overline{B}(b, r)$.

(iii) Скуп $B(a, r)$ је и затворен и отворен.

(iv) Скуп $\overline{B}(a, r)$ је и затворен и отворен, ако $r \neq 0$.

Овде ћемо доказати за нас најважнија прва два својства, али остала својства се не доказују тешко.

Доказ. (i) По дефиницији је $b \in B(a,r) \iff |b-a| < r$. Нека је сада $x \in B(a,r)$. Неархимедско својство каже да је

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

па $x \in B(b,r)$, одакле је $B(a,r) \subset B(b,r)$. Слично је, за $x \in B(b,r)$

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

следи $x \in B(a,r)$, па и $B(b,r) \subset B(a,r)$. Дакле, $B(a,r) = B(b,r)$

(ii) Исти доказ као и (i), заменом $\leq$ са $<$. □

3 p-адски бројеви

3.1 Апсолутне вредности на $\mathbb{Q}$

Видели смо неке примере апсолутних вредности на $\mathbb{Q}$ до сада:

1. Тривијалну апсолутну вредност
2. Класичну апсолутну вредност, коју ћемо звати још и апсолутна вредност код бесконачности
3. p-адску апсолутну вредност

Следећом лемом ћемо видети које апсолутне вредности можемо сматрати еквивалентим, али пре тога нам треба сама дефиниција еквиваленције апсолутних вредности.

Дефиниција 3.1.1. Апсолутне вредности $|\cdot|_1$ и $|\cdot|_2$ су *еквивалентне* на пољу $\mathbb{F}$ ако дефинишу исту топологију на том пољу, то јест сваки отворени скуп у топологији $|\cdot|_1$ је отворен и у топологији дефинисаној са $|\cdot|_2$, и обрнуто.

Лема 3.1.1. *Нека су $|\cdot|_1$ и $|\cdot|_2$ апсолутне вредности на пољу $\mathbb{F}$. Следеће тврдње су тада еквивалентне:*

(i) $|\cdot|_1$ *и* $|\cdot|_2$ *су еквивалентне*

(ii) за свако $x \in \mathbb{F}$ *је* $|x|_1 < 1 \iff |x|_2 < 1$

(iii) постоји позитиван реалан број α *такав да за свако* $x \in \mathbb{F}$ *важи*

$$|x|_1 = |x|_2{}^{\alpha}.$$

Доказ. Доказ спроводимо у три дела, тако што доказујемо круг импликација $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.
$\underline{(i) \Rightarrow (ii)}$: Ако су $|\cdot|_1$ и $|\cdot|_2$ еквивалентне, сваки низ који конвергира у односу на $|\cdot|_1$ конвергира и у односу на $|\cdot|_2$, па тада:

$$|x|_1 < 1 \iff \lim_{n\to\infty} |x^n|_1 = 0 \iff \lim_{n\to\infty} |x^n|_2 = 0 \iff |x|_2 < 1.$$

$\underline{(ii) \Rightarrow (iii)}$: Лако се види да ако је $|\cdot|_1$ тривијална, онда је и $|\cdot|_2$ тривијална (и обрнуто), па (iii) тривијално важи.
Нека је сада $|\cdot|_1$ нетривијална апсолутна вредност на $\mathbb{F}$. Нека је $x_0 \in \mathbb{F}$ са $x_0 \neq 0$ такво да $|x_0|_1 < 1$. По претпоставци је и $|x|_2 < 1$, па постоји $\alpha > 0$ тако да је $|x_0|_1 = |x_0|_2{}^{\alpha}$. Нека је $x \in \mathbb{F}$ неки елемент поља. Испитаћемо прво неке случајеве који би касније сметали:

- ако $|x|_1 = |x_0|_1$, онда је и $|x|_2 = |x_0|_2^{\alpha}$ (иначе је или $\left|\frac{x}{x_0}\right|_2 < 1$ или $\left|\frac{x_0}{x}\right|_2 < 1$, контрадикција са $|x|_1 = |x_0|_1$ због (ii)). Следи $|x|_1 = |x_0|_1 = {|x_0|_2}^{\alpha} = {|x|_2}^{\alpha}$.
- ако $|x|_1 = 1$ из (ii) одмах следи да је $|x|_2 = 1$ па је $|x|_1 = 1 = 1^{\alpha} = {|x|_2}^{\alpha}$.
- ако је $x = x_0^n$, за $n \in \mathbb{N}$ онда је и $|x|_1 = |x|_2^{\alpha}$.

Претпоставимо сада да је $|x|_i \neq 1$ и $|x|_i \neq |x_0|_i$, за $i = 1, 2$. Нека је $\beta \in \mathbb{R}$ такво да је $|x|_1 = {|x|_2}^{\beta}$. За $n \in \mathbb{Z}$ је $|x^n|_1 = {|x^n|_2}^{\beta}$, па можемо узети да је $|x|_1 < 1$ (у супротном заменимо са x^{-1}). Из (ii) је онда и $|x|_2 < 1$. Узмимо неки пар природних бројева m, n. За њих је:

$$ {|x|_1}^n < {|x_0|_1}^m \iff \left|\frac{x^n}{{x_0}^m}\right|_1 < 1 \iff \left|\frac{x^n}{{x_0}^m}\right|_2 < 1 \iff {|x|_2}^n < {|x_0|_2}^m. $$

Одавде логаритмовањем следи да је

$$ \frac{n}{m} > \frac{\log |x_0|_1}{\log |x|_1} \iff \frac{n}{m} > \frac{\log |x_0|_2}{\log |x|_2}. $$

Како су рационални бројеви густи у реалним, из ове еквиваленције следи да је

$$ \frac{\log |x_0|_1}{\log |x|_1} = \frac{\log |x_0|_2}{\log |x|_2}. $$

Одавде је и

$$ \alpha = \frac{\log |x_0|_1}{\log |x_0|_2} = \frac{\log |x|_1}{\log |x|_2} = \beta. $$

$\underline{(iii) \Rightarrow (i)}$: Нека је $r \in \mathbb{R}_+$, и $a \in \mathbb{F}$. Онда је:

$$ x \in B_{|\cdot|_1}(a, r) \iff |x-a|_1 < r \iff |x-a|_2^{\alpha} < r \iff |x-a|_2 < r^{1/\alpha} \iff x \in B_{|\cdot|_2}(a, r^{1/\alpha}). $$

Дакле, свака отворена лопта у односу на $|\cdot|_1$ је отворена и у односу на $|\cdot|_2$, па су њихове топологије исте. □

Следећа теорема каже да јединe апсолутне вредности на $\mathbb{Q}$ јесу управо оне које смо видели кроз примере:

Теорема 3.1.1 (Островски)**.** *Свака нетривијална апсолутна вредност на $\mathbb{Q}$ је еквивалентна некој од $|\cdot|_p$, $p \leq \infty$.*

Доказ. Доказаћемо теорему за нама важнији случај неархимедске апсолутне вредности. Нека је $|\cdot|$ нека апсолутна вредност на $\mathbb{Q}$ која је неархимедска. Показали смо, да за целе n, имамо $|n| \leq 1$. Нека је n_0 најмањи природан број такав да је $n_0 < 1$ (мора постојати такав јер је $|\cdot|$ нетривијална).

Приметимо да је n_0 прост број, у супротном, напишимо $n_0 = ab$, где су a, b природни бројеви мањи од n_0. Пошто је n_0 најмањи природан број са апсолутном вредношћу мањом од 1, следи $|a| = |b| = 1$, али тада $1 > |n_0| = |ab| = |a||b| = 1$, контрадикција. Ставимо сада $p = n_0$.
Нека је $n \in \mathbb{Z}$ такав да $p \nmid n$. Напишимо $n = rp + s$, где $0 < s < p$. Због минималности p је онда $|s| = 1$, а због $|r| \leq 1$ је и $|rp| < 1$. Како је $|\cdot|$ неархимедска, и по теореми 2.3.2. је $|n| = 1$.
Напишимо сада произвољно $n \in \mathbb{Z}$ као $n = p^v n'$, где $p \nmid n'$. Тада

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

где смо ставили $c = |p^{-1}| > 1$. Како ово важи за све целе n, лако се добија да важи и за све рационалне бројеве. Следи да је $|\cdot|$ еквивалентна p-адској апсолутној вредности. □

Теорема 3.1.2 (Формула производа)**.** *За свако $x \in \mathbb{Q} \setminus \{0\}$ имамо*

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

где се производ узмиа по свим простим бројевима.

Доказ. Довољно је доказати теорему за природне бројеве, заиста, ако формула важи за $a, b \in \mathbb{N}$, онда

$$\prod_{p \leq \infty} \left|\pm\frac{a}{b}\right|_p = \frac{\prod_{p \leq \infty} |a|_p}{\prod_{p \leq \infty} |b|_p} = 1.$$

Нека је сада $n \in \mathbb{N}$ са канонском факторизацијом $n = \prod_{i=1}^{k} {p_i}^{a_i}$. Тада је

$$\begin{cases} |n|_q = 1 & q \neq p_i \\ |n|_{p_i} = {p_i}^{-a_i} & i = 1, 2, \ldots, k \\ |n|_\infty = \prod_{i=1}^{k} {p_i}^{a_i} \end{cases}$$

Формула директно следи. □

Видимо да, када бисмо имали информацију о неком броју кроз све апсолутне вредности сем једне, могли бисмо да одредимо и преосталу.

3.2 Комплетирања $\mathbb{Q}$

Коначно смо спремни да причамо о p-адским бројевима, тачније о p-адским пољима $\mathbb{Q}_p$. Пре свега сетићемо се како смо конструисали скуп $\mathbb{R}$ од $\mathbb{Q}$ и $|\cdot|_\infty$. Приметили смо да у њему постоје „рупе“, то јест бројеви који би требало да буду лимеси неких низова који конвергирају, али нису постојали у $\mathbb{Q}$. Формално, правили смо низ бројева који је конвергирао у односу на $|\cdot|_\infty$, али његов лимес није постојао у $\mathbb{Q}$. Слично томе, уводимо поље $\mathbb{Q}_p$ које ће попунити рупе у $\mathbb{Q}$, али у односу на $|\cdot|_p$.
Следећом дефиницијом формализоваћемо значење претходног пасуса.

Дефиниција 3.2.1. Нека је $\mathbb{F}$ поље и $|\cdot|$ апсолутна вредност на њему.

(i) Низ $(x_n)_{n=1}^{\infty} \in \mathbb{F}$ је *Кошијев* ако

$$(\forall \epsilon > 0)(\exists M \in \mathbb{N})(m, n \geq M \implies |x_n - x_m| < \epsilon).$$

(ii) Поље $\mathbb{F}$ је *комплетно* у односу на $|\cdot|$ ако сваки Кошијев низ елемената из $\mathbb{F}$ конвергира у $\mathbb{F}$.

(iii) Подскуп $S \subset \mathbb{F}$ је *густ* у $\mathbb{F}$ ако

$$(\forall \epsilon > 0)(\forall x \in \mathbb{F})B(x, \epsilon) \cap S \neq \emptyset.$$

Сада видимо право значење почетног пасуса, поље $\mathbb{Q}$ није комплетно у односу на $|\cdot|_\infty$, па га „надограђујемо“ пољем $\mathbb{R}$, и још важи да је $\mathbb{Q}$ густ у $\mathbb{R}$. Кажемо да је $\mathbb{R}$ комплетирање поља $\mathbb{Q}$.

Поента овог поглавља је да видимо да ништа од овога није специјалино за $|\cdot|_\infty$, заправо, за сваку апсолутну вредност $|\cdot|_p$, постоји комплетирање поља $\mathbb{Q}$ пољем $\mathbb{Q}_p$. За почетак ћемо видети да Кошијеви низови у односу на неархимедске апсолутне величине показују једну корисну особину:

Лема 3.2.1. *Низ $(x_n)_{n=1}^{\infty}$ је Кошијев у односу на неархимедску апсолутну вредност $|\cdot|$ ако и само ако је*

$$\lim_{n \to +\infty} |x_{n+1} - x_n| = 0.$$

Доказ. Ако је низ Кошијев, онда специјално важи и $|x_{n+1} - x_n| \to 0$ за $n \to \infty$.

За други смер, нека је $m = n + r$. Тада је

$$|x_m - x_n| = |\sum_{k=n}^{n+r-1} (x_{k+1} - x_k)| \leq \max\{|x_{n+r} - x_{n+r-1}|, \ldots, |x_{n+1} - x_n|\},$$

па следи да је низ Кошијев. □

Пример 5. Лако је видети да ово не важи за нашу $|\cdot|_\infty$. Знамо да ред

$$\sum_{k=1}^{\infty} \frac{1}{k}$$

дивергира, јер низ парцијалних сума $(S_n)_{n=1}^{\infty}$ дивергира, али $|S_{n+1} - S_n| = \left|\frac{1}{n+1}\right| \to 0$ када $n \to \infty$.

Сада можемо прећи на следећу лему којом ћемо показати да рационалне бројеве заиста треба комплетирати:

Лема 3.2.2. *Поље $\mathbb{Q}$ није комплетно у односу ни на једну нетривијалну апсолутну вредност дефинисану над њим.*

Доказ. Знамо да $\mathbb{Q}$ није комплетно у односу на $|\cdot|_\infty$, па ћемо доказати да, за $|\cdot| = |\cdot|_p$ постоји Кошијев низ који није конвергентан. Видећемо да треба разликовати случајеве $p = 2$ и $p \neq 2$.

- $\underline{p \neq 2:}$ Нека је $a \in \mathbb{Z}$ такав да
  - a није квадрат у $\mathbb{Q}$;
  - $p \nmid a$;
  - a је квадратни остатак по модулу p.

  Дефинишимо, аналогно као када показујемо да $\mathbb{Q}$ није комплетно у односу на $|\cdot|_\infty$, низ који тежи корену из a. (Односно када би лимес постојао, био би квадратни корен из a, али по услову тај број није елемент $\mathbb{Q}$.)

  - Нека је $x_0^2 \equiv a \pmod{p}$;
  - Нека је x_n такво да

  $$x_n \equiv x_{n-1} \pmod{p^n} \text{ и } x_n^2 \equiv a \pmod{p^{n+1}}$$

  Докажимо да је могуће наћи овакав низ, претпоставимо да можемо наћи све такве x_i за $i = 1, 2, \ldots, n-1$ и покажимо да постоји задовољавајуће x_n. Ако би постојало, могли бисмо да напишемо $x_n = x_{n-1} + p^n c$, што би убацивањем у $x_n^2 \equiv a \pmod{p^{n+1}}$ дало

  $$x_{n-1}^2 + 2x_{n-1}p^n c + p^{2n}c^2 \equiv a \pmod{p^{n+1}},$$

  и како је $p^{2n}c^2 \equiv 0 \pmod{p^{n+1}}$,, следи

  $$x_{n-1}^2 + 2x_{n-1}p^n c \equiv a \pmod{p^{n+1}}.$$

  Знамо да је $x_{n-1}^2 \equiv a \pmod{p^n}$ одакле знамо да је и $x_{n-1}^2 = a + p^n d$ што враћањем даје

  $$p^n d + 2x_{n-1}p^n c \equiv 0 \pmod{p^{n+1}},$$

  и скраћивањем p^n

  $$d + 2cx_{n-1} \equiv 0 \pmod{p}.$$

  Одавде, за дато d, постоји одговарајуће c јер $p \nmid x_{n-1}$ које онда одређује и x_n. (Овде је било неопходно да је p непаран прост.)
  Проверимо сада да конструисани низ заиста јесте Кошијев, где ћемо искористити претходну лему. По конструкцији је

  $$|x_{n+1} - x_n| = |kp^{n+1}| \leq p^{-(n+1)} \to 0,$$

одакле x_n јесте Кошијев. Али, знамо да

$$|x_n^2 - a| = |bp^{n+1}| \leq p^{-(n+1)} \to 0,$$

што значи да ако лимес постоји, једнак је корену из a. Међутим, a смо изабрали тако да није квадрат у $\mathbb{Q}$, па лимес не постоји, односно, $\mathbb{Q}$ није комплетно.

- $\underline{p = 2}$: Посматрајући први случај, видимо да ако је d непарно, одговарајуће c не постоји. Зато ћемо покушати да коефицијент уз c променимо у неки непарни. Видели смо да 2 потиче од x_n^2, па ћемо сада модификовати доказ тако да имамо x_n^3. То радимо тако што дефинишемо сличан низ, стављајући $a = 3$, и конструишући низ чији би лимес био кубни корен из a.

  – Нека је $x_0^3 \equiv 3 \pmod{2}$ (одмах следи $x_0 \equiv 1 \pmod{2}$);

  – Нека је x_n такво да

  $$x_n \equiv x_{n-1} \pmod{2^n} \text{ и } x_n^3 \equiv 3 \pmod{2^{n+1}}.$$

  Као малопре добијамо (за слично дефинисане c и d, односно $x_n = x_{n-1} + 2^n c$ и $x_{n-1}^3 = a + 2^n d$) да мора бити $d \equiv -x_{n-1}^2 c \pmod{2}$, а одговарајуће c сада очигледно постоји.
  Потпуно аналогно првом случају видимо да је овај низ Кошијев, и долазимо до контрадикције.

Следи да $\mathbb{Q}$ заиста није комплетно у односу на било коју нетривијалну апсолутну вредност дефинисану над њим. □

Управо смо видели да $\mathbb{Q}$ није комплетно у односу на $|\cdot|_p$. Тако, аналогно као што комплетирамо $\mathbb{Q}$ у односу на уобичајену апсолутну вредност и добијамо $\mathbb{R}$, комплетирамо $\mathbb{Q}$ и у односу на $|\cdot|_p$ и добијамо $\mathbb{Q}_p$. Из овог разлога ћемо често $\mathbb{R}$ обележавати са $\mathbb{Q}_\infty$ (рекли смо да уобичајену апсолутну вредност обележавамо са $|\cdot|_\infty$).

3.3 Особине $\mathbb{Q}_p$

До сада смо видели само да $\mathbb{Q}_p$ постоји, сада ћемо систематизовати наша знања о овом пољу. Полазимо од неких основних чињеница:

- Постоји апсолутна вредност $|\cdot| = |\cdot|_p$ на $\mathbb{Q}_p$ и $\mathbb{Q}_p$ је комплетно у односу на њу.
- Постоји пресликавање $\mathbb{Q} \mapsto \mathbb{Q}_p$ чија је слика густа у $\mathbb{Q}_p$, и апсолутна вредност над овом сликом се поклапа са p-адском.
- Скупови могућих апсолутних вредности елемената из $\mathbb{Q}$ и $\mathbb{Q}_p$ су исти:

$$\{x \in \mathbb{R}_+ : (\exists \lambda \in \mathbb{Q})\ x = |\lambda|_p\} = \{x \in \mathbb{R}_+ : (\exists \lambda \in \mathbb{Q}_p)\ x = |\lambda|_p\}.$$

Од сада ћемо поменуту слику поља $\mathbb{Q}$ управо поистоветити са самим пољем. А другим речима, треће својство каже:

Лема 3.3.1. *За свако $x \in \mathbb{Q}_p \setminus \{0\}$ постоји цео број $v_p(x)$ такав да је $|x|_p = p^{-v_p(x)}$, односно p-адска валуација се проширује на $\mathbb{Q}_p$.*

Следеће што радимо је увођење p-адских целих бројева и основни преглед њихових својстава.

Дефиниција 3.3.1. Прстен p-адских целих бројева је скуп

$$\mathbb{Z}_p = B(0,1) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Теорема 3.3.1. *За $\mathbb{Z}_p$ важе следеће чињенице:*

(i) $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid b\right\}$

(ii) Пресликавање $\mathbb{Z} \mapsto \mathbb{Z}_p$ има густу слику. Заправо, за $x \in \mathbb{Z}_p$ и $n \geq 1$ постоји јединствено $\alpha \in \mathbb{Z}$ са $0 \leq \alpha \leq p^n - 1$ и $|x - \alpha|_p \leq p^{-n}$.

(iii) За свако $x \in \mathbb{Z}_p$ постоји јединствени низ $(\alpha_n)_{n=1}^{\infty}$ чији је лимес x и за који

- *$\alpha_n \in \mathbb{Z}$ и $0 \leq \alpha_n \leq p^n - 1$;*
- *За све $n \in \mathbb{N}$ је $\alpha_n \equiv \alpha_{n-1} \pmod{p^n}$.*

Доказ. (i) За скраћене разломке $\frac{a}{b}$ са $p \mid b$ је $\left|\frac{a}{b}\right|_p > 1$

(ii) Нека је $x \in \mathbb{Z}_p$ и $n \in \mathbb{N}$. Како је $\mathbb{Q}$ густ у $\mathbb{Q}_p$, постоји $\frac{a}{b} \in \mathbb{Q}$ који је довољно близу x, односно

$$\left|x - \frac{a}{b}\right| \leq p^{-n} < 1.$$

Треба доказати да заправо можемо да изаберемо довољно близак цео број уместо рационалног броја. За овако дефинисано $\frac{a}{b}$ је

$$\left|\frac{a}{b}\right|_p \leq \max\left\{|x|_p, \left|x - \frac{a}{b}\right|_p\right\} \leq 1$$

што значи да је $\frac{a}{b} \in \mathbb{Z}_{(p)}$, то јест $p \nmid b$. Дакле, постоји $b' \in \mathbb{Z}$ такав да је $bb' \equiv 1 \pmod{p^n}$. Одавде знамо да је

$$\left|\frac{a}{b} - ab'\right|_p = \left|\frac{a}{b}\right|_p \cdot |1 - bb'|_p \leq 1 \cdot p^{-n} = p^{-n},$$

и $ab' \in \mathbb{Z}$. Остаје још да докажемо да можемо наћи цео број између 0 и $p^n - 1$. Изаберимо јединствено α за које је

$$0 \leq \alpha \leq p^n - 1 \text{ и } \alpha \equiv ab' \pmod{p^n}.$$

Тада је $|ab' - \alpha|_p = |cp^n|_p \leq p^{-n}$, и добијамо да је

$$|x - \alpha|_p \leq \max\left\{\left|x - \frac{a}{b}\right|_p, \left|\frac{a}{b} - ab'\right|_p, |ab' - \alpha|_p\right\} \leq p^{-n}.$$

(iii) Поновимо део (ii) за бројеве $n = 1, 2, \ldots$ □

Следећа лема биће неопходна за касније доказе:

Лема 3.3.2. *За свако $x \in \mathbb{Q}_p$ постоји $n \in \mathbb{N}_0$ такво да $p^n x \in \mathbb{Z}_p$.*

Доказ. Нека $x \in \mathbb{Q}_p$. Знамо да можемо израчунати његову p-адску валуацију $v_p(x)$. Ако је $v_p(x) \geq 0$, већ $x \in \mathbb{Z}_p$. У супротном

$$v_p(p^{-v_p(x)}x) = -v_p(x) + v_p(x) = 0,$$

па $p^{-v_p(x)}x \in \mathbb{Z}_p$. □

За сада сваки опис поља $\mathbb{Q}_p$ био је помало апстрактан, а сада ћемо видети како да записујемо елементе овог поља на донекле сличан начин нашег децималног записивања елемената $\mathbb{R}$.

Пођимо од p-адског целог броја x. Показали смо да постоји низ целих бројева $(\alpha_n)_{n=1}^{\infty}$ који конвергира ка x такав да

- $\alpha_n \equiv x \pmod{p^n}$;
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$;
- $0 \leq \alpha_n \leq p^n - 1$.

Посматрајмо елементе овог низа у бази p. Ово радимо јер је број по модулу p^n исти као број добијен од његових последњих n цифара. Следи да други од ових услова значи да је последњих n цифара бројева α_{n+1} и α_n исто. Закључујемо онда да постоји низ бројева $(c_n)_{n=0}^{\infty}$ такав да је

$$\alpha_n = \sum_{k=0}^{n} c_k p^k$$

и да су бројеви c_k цели бројеви између 0 и $p - 1$. Дакле, логично би било ставити да је

$$x = \sum_{k=0}^{\infty} c_k p^k.$$

Да бисмо могли да x поистоветимо са овим редом, треба доказати да он конвергира баш ка x.

Лема 3.3.3. *За свако $x \in \mathbb{Z}_p$, ред*

$$\sum_{k=0}^{\infty} c_k p^k$$

дефинисиан као горе, конвергира ка x.

Доказ. Ред тежи ка x ако низ парцијалних сума тежи ка x, а парцијалне суме су у овом случају баш α_n. □

Дакле, важи и следећа лема:

Лема 3.3.4. *Свако $x \in \mathbb{Z}_p$ се може јединствено записати у облику*

$$x = \sum_{k=0}^{\infty} c_k p^k,$$

где $0 \leq c_k \leq p-1$.

Доказ. Доказали смо све, осим јединствености. Али, знамо да су α_n јединствени, што повлачи да су c_n јединствени (цифре α_n у бази p). □

Последица 3.3.4.1. *Свако $x \in \mathbb{Q}_p$ се може јединствено записати у облику*

$$x = \sum_{k=-n_0}^{\infty} c_k p^k,$$

где $0 \leq c_k \leq p-1$ и $v_p(x) = -n_0$.

Доказ. По **Леми 3.3.3.** знамо да за свако $x \in \mathbb{Q}_p$ постоји $n_0 \in \mathbb{N}_0$ такво да је $p^{n_0}x \in \mathbb{Z}_p$. (Штавише, лема каже и да се може узети $-n_0 = v_p(x)$.) Дакле можемо јединствено записати

$$p^{n_0}x = \sum_{k=-n_0}^{\infty} c_k p^{k+n_0}.$$

Дељењем обе стране са p^{n_0} добијамо резултат. □

На ову тему биће више речи у следећем поглављу.

3.4 Хенселова лема

Долазимо до најважније алгебарске особине p-адских бројева, Хенселове леме. Она ће нам дати да у великом броју случајева лако видимо да ли полином има нуле у $\mathbb{Z}_p$. Пре тога докажимо једну лему.

Лема 3.4.1. *За дати полином $F(X) \in \mathbb{Z}_p[X]$ постоји полином $G(X,Y) \in \mathbb{Z}_p[X,Y]$ такав да важи*

$$F(X+Y) = F(X) + F'(X)Y + G(X,Y)Y^2.$$

Доказ. Нека је $F(X) = \sum_{k=0}^{d} c_k X^k$. Онда

$$F(X+Y) = \sum_{k=0}^{d} c_k (X+Y)^k = c_0 + \sum_{k=1}^{d} c_k (X^k + kX^{k-1}Y + G_k(X,Y)Y^2,$$

где су полиноми $G_k(X,Y) \in \mathbb{Z}_p[X,Y]$ на основу биномне формуле. Сада је

$$F(X+Y) = \sum_{k=0}^{d} c_k X^k + \sum_{k=1}^{d} k c_k X^{k-1} Y + \sum_{k=1}^{d} c_k G_k(X,Y) Y^2 = F(X) + F'(X)Y + G(X,Y)Y^2,$$

где смо заменили $G(X,Y) = \sum_{k=1}^{d} c_k G_k(X,Y) \in \mathbb{Z}_p[X,Y]$. □

Овом лемом смо видели практично проширење Тејлорове формуле на $\mathbb{Z}_p$. Сада прелазимо на Хенселову лему:

Лема 3.4.2 (Хенсел)**.** *Нека је $F(X) \in \mathbb{Z}_p[X]$ полином. Ако постоји $\alpha_1 \in \mathbb{Z}_p$ такво да је*

$$F(\alpha_1) \equiv 0 \pmod{p} \quad u \quad F'(\alpha_1) \not\equiv 0 \pmod{p},$$

постоји $\alpha \in \mathbb{Z}_p$ такав да

$$F(\alpha) = 0 \quad u \quad \alpha_1 \equiv \alpha \pmod{p}.$$

Доказ. Да бисмо доказали ову лему, индукцијом ћемо конструисати низ $(\alpha_n)_{n=1}^{\infty}$ чији ће лимес бити тражено α. Ако имамо бројеве $\alpha_1, \alpha_2, \ldots, \alpha_n$ наћи ћемо број α_{n+1} за који

- $F(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}}$
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$

Базу индукције смо задали у условима леме. За дато α_n потражимо α_{n+1} у облику

$$\alpha_{n+1} = \alpha_n + p^n t_n \quad \text{где} \quad t_n \in \mathbb{Z}_p.$$

Хоћемо такво t_n да важи

$$F(\alpha_n + p^n t_n) \equiv 0 \pmod{p^{n+1}}.$$

По **Леми 3.3.1** знамо да је

$$F(\alpha_n + p^n t_n) = F(\alpha_n) + F'(\alpha_n) t_n p^n + G(\alpha_n, p^n t_n) p^{2n} t_n^2 \equiv F(\alpha_n) + F'(\alpha_n) t_n p^n \pmod{p^{n+1}},$$

јер је $2n \geq n+1$. Напишимо $F(\alpha_n) = p^n x$, што можемо због индуктивне хипотезе. Такође, фактори $F'(\alpha_n) p^n t_n$ нас занимају само по модулу p^{n+1}, па како је $\alpha_n \equiv \alpha_1 \pmod{p}$ онда је и $F'(\alpha_n) p^n t_n \equiv F'(\alpha_1) p^n t_n \pmod{p^{n+1}}$. Коначно добијамо да је

$$F(\alpha_n + p^n t_n) \equiv F(\alpha_n) + F'(\alpha_n) t_n p^n \equiv p^n x + F'(\alpha_1) t_n p^n \pmod{p^{n+1}}$$

што скраћивањем са p^n даје да треба наћи t_n такво да је

$$x + F'(\alpha_1) t_n \equiv 0 \pmod{p}.$$

Како је $F'(\alpha_1) \not\equiv 0 \pmod{p}$, овакво t_n можемо наћи, па имамо дефинисан Кошијев низ $(\alpha_n)_{n=1}^{\infty}$. (Кошијев због првог услова који задовољава.) Пошто је $\mathbb{Q}_p$ комплетно поље, овај низ има граничну вредност у $\mathbb{Q}_p$, и сви његови чланови имају апсолутне вредности највише 1, па је то случај и са његовим лимесом, и зато ће остати у $\mathbb{Z}_p$, то јест $\alpha = \lim_{n\to\infty} \alpha_n \in \mathbb{Z}_p$.
Докажимо да овакво α задовољава услове леме. За $m > n$ је $|\alpha_m - \alpha_n|_p \leq p^{-n}$ где узимањем лимеса када $m \to \infty$ добијамо $|\alpha - \alpha_n|_p \leq p^{-n}$ па је $\alpha \equiv \alpha_n \pmod{p^n}$. Дакле

$$F(\alpha) \equiv F(\alpha_n) \pmod{p^n}, \quad \text{односно} \quad |F(\alpha)| \leq p^{-n}.$$

Како ово важи за све $n \geq 1$, следи $F(\alpha) = 0$. □

Постоји следећа, јача варијација Хенселове леме, коју овде дајемо без доказа.

Лема 3.4.3 (Хенсел)**.** *Нека за полином $F(X) \in \mathbb{Z}_p[X]$ постоји елемент $\alpha_1 \in \mathbb{Z}_p$ такав да је*

$$|F(\alpha_1)|_p < |F'(\alpha_1)|_p^2.$$

Онда постоји јединствено $\alpha \in \mathbb{Z}_p$ такво да је

$$F(\alpha) = 0 \quad и \quad |\alpha - \alpha_1|_p < |F'(\alpha_1)|_p.$$

Уз то важе и

$$|\alpha - \alpha_1| = \left|\frac{F(\alpha_1)}{F'(\alpha_1)}\right|_p < |F'(\alpha_1)| \quad и \quad |F'(\alpha)|_p = |F'(\alpha_1)|_p.$$

Вреди напоменути да је доказ практично имплементација Њутнове методе из нумеричке анализе.

Хенселову лему ћемо сада видети у примени. Посматраћемо који корени из јединице постоје у $\mathbb{Z}_p$.

Дефиниција 3.4.1. Јединица у прстену $\mathbb{F}$ је сваки инвертибилни елемент u у том прстену, односно за њега постоји $v \in \mathbb{F}$ такво да је $uv = vu = 1$.

Групу свих јединица прстена $\mathbb{Z}_p$ обележаваћемо са $\mathbb{Z}_p^\times$ (да је скуп јединица стварно група је лако видети). Али ми знамо да је за $x \in \mathbb{Z}_p^\times \subset \mathbb{Z}_p$ онда $x^{-1} \in \mathbb{Z}_p^\times$ па је $|x|_p \geq 1 \Rightarrow |x^{-1}|_p \leq 1 \Rightarrow |x^{-1}|_p = 1 \Rightarrow |x|_p = 1$. Дакле, $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}$.
Сетимо се шта су заправо корени из јединице.

Дефиниција 3.4.2. Нека је $\mathbb{F}$ поље. За $\zeta \in \mathbb{F}$ кажемо да је *m-ти корен из јединице* ако $\zeta^m = 1$. Кажемо да је ζ *примитивни m-ти корен из јединице* ако још важи и $\zeta^n \neq 1$ за $0 < n < m$.

Хенселова лема даје следеће резултат:

Теорема 3.4.1. *За прост број p и $m \in \mathbb{N}$ који није дељив са p постоји примитивни m-ти корен из јединице у $\mathbb{Q}_p$ ако и само ако $m \mid p-1$.*
Такође, скуп свих $(p-1)$-их корена из јединице чини цикличну подгрупу $\mathbb{Z}_p^\times$.

Доказ. $\Leftarrow$: Претпоставимо да $m \mid p-1$. Ако $\zeta^m = 1$ онда и $\zeta^{p-1} = 1$, па посматрајмо полином $F(X) = X^{p-1} - 1$. Нека је $a \in \mathbb{Z} \subset \mathbb{Z}_p$ такав да $0 \leq a \leq p-1$. На основу мале Фермаове теореме је онда

$$F(a) = a^{p-1} - 1 \equiv 0 \pmod{p} \quad \text{и} \quad F'(a) = (p-1)a^{p-2} \equiv \ a^{-1} \pmod{p},$$

па на основу Хенселове леме знамо да за свако $a \in \{1, \ldots, p-1\}$ постоји по решење $\zeta_a \in \mathbb{Z}_p$ једначине $X^{p-1} - 1 = 0$ такво да $\zeta_a \equiv a \pmod{p}$. Дакле нашли смо $p-1$ корена јединице у прстену $\mathbb{Z}_p \subset \mathbb{Q}_p$. Са друге стране, знамо да је број корена полинома у било ком пољу највише једнак степену полинома, па овај полином има највише $p-1$ корена у $\mathbb{Q}_p$, па су $\zeta_1, \zeta_2, \ldots, \zeta_{p-1}$ управо сви њени корени. Лако се види да они чине подгрупу $\mathbb{Z}_p^\times$, а како је коначна подгрупа мултипликативне групе циклична, следи да је група $(p-1)$-их корена јединице циклична, реда $p-1$. Следи и да за свако $m \mid p-1$ постоји примитивни m-ти корен из јединице у $\mathbb{Q}_p$.
$\Rightarrow$: Нека је $m \in \mathbb{N}$ узајамно прост са p и нека је $\zeta \in \mathbb{Q}_p$ неки примитивни m-ти корен из јединице, то јест $\zeta^m = 1$. Онда је $|\zeta|_p^m = |\zeta^m|_p = |1|_p = 1$ односно $|\zeta|_p = 1$ па самим тим $\zeta \in \mathbb{Z}_p$. Нека је $0 \leq a_0 \leq p-1$ и $\zeta \equiv a_0 \pmod{p}$. У доказу другог смера видели смо да постоји јединствени $(p-1)$-и корен из јединице $\zeta_{a_0} \in \mathbb{Z}_p$ са $\zeta_{a_0} \equiv a_0 \pmod{p}$. Посматрајмо сада полином $F(X) = X^{(p-1)m} - 1$. Овај полином испуњава услове Хенселове леме за a_0, па има јединствени корен у $\mathbb{Z}_p$ конгруентан a_0 по модулу p. Али

$$F(\zeta) = (\zeta^m)^{p-1} - 1 = 0 = (\zeta^{p-1})^m - 1 = F(\zeta_{a_0}) \quad \text{и} \quad \zeta \equiv a_0 \equiv \zeta_{a_0} \pmod{p}.$$

Дакле мора бити $\zeta = \zeta_{a_0}$, па је ζ неки од $(p-1)$-их коренова јединице, и ако је он примитиван, онда $m \mid p-1$. □

Још једна важна примена Хенселове леме је у налажењу квадрата у $\mathbb{Q}_p$. Прво ћемо видети које $p-$адске јединице су квадрати.

Теорема 3.4.2. *Нека је $p \neq 2$ прост и нека је b јединица у $\mathbb{Z}_p$. Ако постоји a тако да $a^2 \equiv b \pmod{p}$ онда је b квадрат у $\mathbb{Z}_p$.*

Доказ. Посматрајмо полином $F(X) = X^2 - b$. Имамо да је $F(a) \equiv 0 \pmod{p}$ и $F'(a) = 2a \not\equiv 0 \pmod{p}$ (јер због $p \neq 2$ и $b \in \mathbb{Z}_p^\times$ имамо $b \not\equiv 0 \pmod{p}$ па и $a \not\equiv 0 \pmod{p}$). По Хенселовој леми следи да постоји $\alpha \in \mathbb{Z}_p$ тако да је $F(\alpha) = 0$. □

Приметимо да се свако $x \in \mathbb{Q}_p$ може записати у облику $x = p^{v_p(x)}x'$, где је x' p-адска јединица. Остаје још да видимо шта се дешава за $p = 2$. Морамо да искористимо јачу верзију Хенселове леме, с обзиром да је $F'(\alpha) = 2\alpha$ што је увек дељиво са 2.

Теорема 3.4.3. *Број $b \in \mathbb{Z}_2^\times$ је квадрат у $\mathbb{Z}_2^\times$ ако и само ако је $b \equiv 1 \pmod{8}$.*

Доказ. $\Leftarrow$: Нека $F(X) = X^2 - b$ и нека је $b \equiv 1 \pmod{8}$. Тада, за $\alpha_1 = 1$ важи $F(\alpha_1) \equiv 0 \pmod{8}$, па $|F(\alpha_1)|_2 \leq 2^{-3}$. Такође, $F'(\alpha_1) = 2\alpha_1 = 2$ па $|F'(\alpha_1)|_2^2 = |4|_2 = 2^{-2}$. Дакле, услови за употребу јаче верзије Хенселове леме су испуњени, па постоји α тако да $F(\alpha) = 0$.
$\Rightarrow$: Ако је $b = a^2$, онда је и a јединица у $\mathbb{Z}_2$. То значи да је $a = 1 + 2x$ (јер $a \equiv 1 \mod 2$) па $b = 1 + 4x + 4x^2 \equiv 1 + 4x(x+1) \equiv 1 \pmod{8}$. □

Теорема 3.4.4. *Нека је p прост. Елемент $x \in \mathbb{Q}_p$ је квадрат ако и само ако може бити записан у облику $x = p^{2n}y^2$ где је $y \in \mathbb{Z}_p^\times$.*

Доказ. Јасно је да је број $p^{2n}y^2$ квадрат у $\mathbb{Q}_p$. Са друге стране, ако је x квадрат, постоји z тако да $x = z^2$. Ставимо $z = p^n y$, $y \in \mathbb{Z}_p^\times$. Онда је $x = p^{2n}y^2$. □

3.5 Локално-глобални принцип

Примењујући Хенселову лему обично није тешко видети да ли неки полином има корене у $\mathbb{Z}_p$. Слично је тачно и за $\mathbb{R}$ где у зависности од знака полинома закључујемо о његовим коренима.

Али, шта ако желимо коренове који су из $\mathbb{Q}$? Лако је видети, да ако постоји корен из $\mathbb{Q}$ онда постоји и у сваком $\mathbb{Q}_p$, $p \leq \infty$. Дакле, са сигурношћу можемо да тврдимо да рационални корен не постоји уколико постоји неко $p \leq \infty$ тако да нема p-адских коренова.

Дакле, оно што тврдимо је да ако постоји глобални корен, постоји и локални корен за свако $\mathbb{Q}_p$, $p \leq \infty$. Циљ овог поглавља је да видимо да ли некад можемо да закључимо обрнуто, то јест, ако постоји локални корен за свако $\mathbb{Q}_p$, да ли, и када то значи да постоји глобални корен (то јест корен у $\mathbb{Q}$).

Нажалост, постоје многи случајеви у којима ово није тачно. То показује следећи једноставан пример.

Пример 6. Једначина

$$(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$$

има корен за све $\mathbb{Q}_p$, $p \leq \infty$, а нема корен у $\mathbb{Q}$.
Да нема корене у $\mathbb{Q}$ је очигледно, као и да их има у $\mathbb{R}$. За $p = 2$, имамо да је $17 = 1 + 8 \cdot 2$ па постоји његов корен у $\mathbb{Q}_2$. За $p = 17$, $2 \equiv 6^2 \pmod{17}$ је квадратни остатак по модулу p. Коначно, ако је p неки други прост број, и 2 и 17 нису квадратни остаци модуло p, онда $34 = 17 \cdot 2$ јесте.

Ипак, овом темом се не бисмо бавили да не постоје примери када локално-глобални принцип успева.

Теорема 3.5.1 (Хасе-Минковски)**.** *Нека је*

$$F(X_1, X_2, \ldots, X_n) \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$$

хомогени полином другог степена по n променљивих. Једначина

$$F(X_1, X_2, \ldots, X_n) = 0$$

има нетривијално решење у $\mathbb{Q}$ ако и само ако има нетривијално решење у сваком $\mathbb{Q}_p$, $p \leq \infty$.

4 Аритметичке операције са p-адским бројевима

У овом поглављу видећемо како рачунати у пољу p-адских бројева. Као поље које комплетира $\mathbb{Q}$, у њему су дефинисане операције сабирања и множења. Да бисмо технички то урадили, p-адске бројеве ћемо записивати преко степених редова. Сабирање и множење функционишу исто као и код реалних бројева, са тим што преношење фунцкионише с лева на десно. Кроз неколико наредних примера видећемо како то радимо у пракси.

Пример 7. У овом примеру видимо како се множи и одузима у $\mathbb{Q}_7$.

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

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

$$\begin{array}{rccccccccccc}
 & 3 & \times & 7^{0} & + & 6 & \times & 7^{1} & + & 2 & \times & 7^{2} & + \cdots \\
\times & 4 & \times & 7^{0} & + & 5 & \times & 7^{1} & + & 1 & \times & 7^{2} & + \cdots \\
\hline
 & 5 & \times & 7^{0} & + & 4 & \times & 7^{1} & + & 4 & \times & 7^{2} & + \cdots \\
 & & & & & 1 & \times & 7^{1} & + & 4 & \times & 7^{2} & + \cdots \\
 & & & & & & & & & 3 & \times & 7^{2} & + \cdots \\
\hline
 & 5 & \times & 7^{0} & + & 5 & \times & 7^{1} & + & 4 & \times & 7^{2} & + \cdots
\end{array}$$

Пример 8. Видели смо да број $\sqrt{a}$ где $a \in \mathbb{N}$ постоји у $\mathbb{Q}_p$ ако је a квадратни остатак модуло p, за непаран p. Нађимо онда $\sqrt{6}$ у $\mathbb{Q}_5$. Треба нам низ $c_0, c_1, c_2, \ldots$, $0 \leq c_k \leq 4$ такав да

$$(c_0 + c_1 \times 5 + c_2 \times 5^2 + \cdots)^2 = 1 + 1 \times 5.$$

Упоређивањем коефицијената испред 5^0 видимо да треба $c_0^2 \equiv 1 \pmod 5$ па $c_0 = 1$ или 4. Узмимо $c_0 = 1$. Онда упоређујемо коефицијенте испред 5^1 и добијамо $2c_1 \times 5 \equiv 1 \times 5 \pmod{5^2}$ односно $2c_1 \equiv 1 \pmod 5$ одакле $c_1 = 3$. Настављањем овог процеса добијамо све остале c_k који су сви јединствено одређени претходним члановима низа. У овом случају је $c_2 = 0,\ c_3 = 4, \ldots$ Али, шта би се променило да смо узели $c_0 = 4$? Заправо се дешава исто што и у $\mathbb{R}$, за сваки број постоје две вредности које дигнуте на квадрат дају тај број, и овим бисмо добили другу од тих вредности (која је једнака негативној вредности прве вредности).

Пример 9. Нађимо сада неке вредности p-адских бројева:

(i) -1 у $\mathbb{Q}_p$

$$-1 = 0-1 = (0\times p^0+0\times p^1+\dots)-(1\times p^0+0\times p^1+\dots) = (p-1)\times p^0+(p-1)\times p^1+\dots$$

где се понавља цифра $p-1$ до бесконачности.

(ii) $-\dfrac{1}{6}$ у $\mathbb{Q}_7$:

Нека $\alpha = -\dfrac{1}{6}$, онда $6\alpha = -1$, па заменом α његовим степеним редом треба да

$$(6\times 7^0)(c_0\times 7^0 + c_1\times 7^1 + c_2\times 7^2 + \dots) = 6\times 7^0 + 6\times 7^1 + 6\times 7^2 + \dots.$$

Сада лако налазимо да је $\alpha = 1\times 7^0 + 1\times 7^1 + 1\times 7^2 + \dots$ где се јединица понавља до бесконачности.

(iii) $\dfrac{1}{1000}$ у $\mathbb{Q}_5$:

Нека $\alpha = \dfrac{1}{1000}$, онда $1000\alpha = 1$, па заменом α његовим степеним редом треба да

$$(3\times 5^3 + 1\times 5^4)(c_{-3}\times 5^{-3} + c_{-2}\times 5^{-2} + c_{-1}\times 5^{-1} + \dots) = 1\times 5^0.$$

Сада упоређивањемо коефицијената уз 5^0 добијамо $c_{-3} = 2$, упоређивањем коефицијената уз 5^1 добијамо $1 + 3c_{-2} + c_{-3} \equiv 0 \pmod 5$ одакле је $c_{-2} = 4$, све док не добијемо $\alpha = 2\times 5^{-3} + 4\times 5^{-2} + 1\times 5^1 + \dots$ а цифре 4 и 1 се понављају до бесконачности.

Пример 10. Сада ћемо испитати кардиналност $\mathbb{Z}_p$. Конструисаћемо функцију $f : \mathbb{Z}_p \to [0,1]$ која је *на*. Дефинишемо f на следећи начин

$$f(c_0 + c_1p + c_2p^2 + \dots) = \frac{c_0}{p} + \frac{c_1}{p^2} + \frac{c_2}{p^3} + \dots.$$

Ова функција погађа све бројеве из $[0,1]$ јер заправо од p-адског целог добијамо реални број у $[0,1]$ у основи p, па бројева у $\mathbb{Z}_p$ има непребројиво много, јер реалних бројева у $[0,1]$ има непребројиво много.

5 Примена p-адских бројева

У овом поглављу бавићемо се квадратним формама. Изведимо прво једну последицу теореме Хасе-Минковског.

Теорема 5.1. *Нека је*

$$F(X_1, X_2, \ldots, X_n) \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$$

хомогени полином другог степена по n променљивих. Једначина

$$F(X_1, X_2, \ldots, X_n) = a,$$

где $a \in \mathbb{Q}$ има решење у $\mathbb{Q}$ ако и само ако има нетривијално решење у сваком $\mathbb{Q}_p$, $p \leq \infty$.

И следећу теорему наводимо без доказа:

Теорема 5.2 (Давенпорт-Каселс)**.** *Нека је $F(X_1, \ldots, X_n)$ квадратна форма са целим коефицијентима. Претпоставимо да важи:*
За свако $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ постоји $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ тако да $F(x_1 - y_1, \ldots, x_n - y_n) < 1$.
Ако, за $n \in \mathbb{Z}$, $F(X_1, \ldots, X_n) = n$ има решење у $\mathbb{Q}$, има решење и у $\mathbb{Z}$.

Нека су $a, b, c \in \mathbb{Q}$ и посматрајмо једначину

$$aX^2 + bY^2 + cZ^2 = 0.$$

Хоћемо да користимо теорему Хасе-Минковског да бисмо видели када она има нетривијална рационална решења. Видимо да можемо претпоставити да ниједан од a, b, c није нула (у супротном има решење када су две променљиве 0 а трећа ненула). Можемо претпоставити и да $a, b, c \in \mathbb{Z}$, иначе можемо помножити имениоцима разломака. Даље, можемо узети $(a, b, c) = 1$, у супротном скратимо заједничке факторе. Покажимо да можемо узети бесквадратне a, b, c, и да можемо отићи корак даље и претпоставити да су у паровима узајамно прости.
Ако $a = a'n^2$ онда се наша једначина трансформише у $a'(nX)^2 + bY^2 + cZ^2 = 0$ па ако она има решење, има га и полазна, и обрнуто.
Ако $(a, b) = k$,, следи да је k бесквадратни и $(k, c) = 1$. Ставимо $a = a'k$ и $b = b'k$. Онда се једначина трансформише у $a'kX^2 + b'kY^2 + cZ^2$, па видимо да $k \mid cZ^2$, одакле $k \mid Z^2$, па $k \mid Z$ (јер k није дељив квадратом осим 1). Ставимо $Z = kZ'$ па се једначина трансформише у $a'X^2 + b'Y^2 + ckZ'^2$. Следи да можемо претпоставити да су a, b, c у паровима узајамно прости. Желимо решења

$$aX^2 + bY^2 + cZ^2 = 0.$$

где су $a, b, c \in \mathbb{Z}$ у паровима прости, и нису дељиви квадратом осим 1. По теореми Хасе-Минковског, довољно је да видимо шта се дешава у $\mathbb{Q}_p$ за $p \leq \infty$. Ако је $p = \infty$, постоји нетривијално решење ако и само ако нису сви a, b, c истог знака.
Нека је сада p прост број који не дели ниједан од бројева a, b, c. Проучимо решења модуло p.

Теорема 5.3. *Нека је p непаран прост број, и нека су $a, b, c \in \mathbb{Z}$ у паровима узајамно прости цели бројеви који нису дељиви са p. Онда постоје $x_0, y_0, z_0 \in \mathbb{Z}_p$ који нису сви дељиви са p такви да*

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}.$$

Доказ. Како x, y, z пролазе кроз $0, \ldots, p-1$ имамо p^3 различитих тројки (x, y, z). Покушајмо да пребројимо оне које су решења

$$aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{p}.$$

Приметимо да је онда

$$(ax^2 + by^2 + cz^2)^{p-1} \equiv \begin{cases} 1 \pmod{p} & (x, y, z) \text{ није решење} \\ 0 \pmod{p} & (x, y, z) \text{ решење} \end{cases}$$

Дакле, ако је N укупан број тројки које нису решење, онда

$$N \equiv \sum_{(x,y,z)} (ax^2 + by^2 + cz^2)^{p-1} \pmod{p}.$$

Расписивањем израза са десне стране добија се сума израза облика

$$\sum_{(x,y,z)} ax^{2i}y^{2j}z^{2k}$$

где $a \in \mathbb{Z}$ и $i+j+k = p-1$. Доказаћемо да је свака од ових сума 0 по модулу p. Приметимо да је неки од i, j, k мањи од $p-1$ (ако су сви бар $p-1$ онда $2i+2j+2k \geq 3(p-1)$). Нека то важи за i. Онда нашу суму можемо да препишемо као

$$\sum_{(y,z)} \left(ay^{2j}z^{2k} \sum_{x} x^{2i} \right).$$

Међутим, $\sum_{x=0}^{p-1} x^n \equiv 0 \pmod{p}$, па је и наша сума 0 модуло p, што даје $N \equiv 0 \pmod{p}$, па је и број тројки које јесу решење дељив са p (јер има p^3 тројки). Међутим, знамо да је тројка $(0, 0, 0)$ решење. Комбинијући две последње чињенице добијамо да постоји још бар једно решење. □

Из ове теореме лако изводимо следеће:

Последица 5.3.1. *Ако је p непаран прост број који не дели abc, онда једначина*

$$F(X, Y, Z) = aX^2 + bY^2 + cZ^2 = 0$$

има нетривијално решење у $\mathbb{Q}_p$.

Доказ. Видели смо да постоји тројка (x_0, y_0, z_0), где нису сви x_0, y_0, z_0 дељиви са p таква да је $F(x_0, y_0, z_0) \equiv 0 \pmod{p}$. Претпоставимо да $p \nmid a$, и ставимо $G(X) = aX^2 + by_0^2 + cz_0^2$. Онда је $G(x_0) \equiv 0 \pmod{p}$ и $G'(x_0) = 2x_0 \not\equiv 0 \pmod{p}$ па применом Хенселове леме на $G(X)$, постоји x тако да је $G(x) = 0$. Тада је (x, y_0, z_0) нетривијално решење једначине $F(X, Y, Z) = 0$. □

Остаје нам још случај $p = 2$ и $p \mid abc$.

Теорема 5.4. *Нека су a, b, c сви непарни. Тада једначина*

$$aX^2 + bY^2 + cZ^2 = 0$$

има нетривијално решење у $\mathbb{Q}_2$ ако и само ако је збир нека два од a, b, c дељив са 4.

Доказ. Ако постоји решење $(x, y, z) \in \mathbb{Q}_2$, можемо претпоставити да $\max\{|x|_2, |y|_2, |z|_2\} = 1$ (Ако имамо тројку која је решење, помножимо одговарајућим степеном двојке да добијемо овакво решење). Како су сви a, b, c непарни, разматрањем модуло 2, видимо да су тачно два од x, y, z 2−адске јединице, а један је дељив са 2. Претпоставимо да су y, z јединице. То значи да су њихови квадрати 1 модуло 4, а квадрат x је 0 модуло 4. Следи да је

$$b + c \equiv 0 \pmod{4}.$$

Нека сада $4 \mid b+c$. Ако $b+c \equiv 0 \pmod{8}$, онда је, за $x_0 = 0, y_0 = 1, z_0 = 1$, $x_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{8}$, а ако $b + c \equiv 4 \pmod{8}$, онда је, за $x_0 = 2, y_0 = 1, z_0 = 1$, $x_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{8}$. Свакако имамо услове за јачу Хенселову лему чијом применом добијамо да дата једначина има решење у $\mathbb{Q}_2$. □

Теорема 5.5. *Нека је један од a, b, c паран. Тада једначина*

$$aX^2 + bY^2 + cZ^2 = 0$$

има нетривијално решење у $\mathbb{Q}_2$ ако и само ако је збир нека два од a, b, c дељив са 8, *или збир сва три дељив са* 8.

С обзиром да се доказ изводи готово аналогно као доказ претходне теореме, овде га прескачемо.

Теорема 5.6. *Нека је p непаран прост број који дели a. Тада једначина*

$$aX^2 + bY^2 + cZ^2 = 0$$

има нетривијално решење у $\mathbb{Q}_p$ ако и само ако је $-b/c$ квадратни остатак модуло p.

Доказ. Претпоставимо да једначина има решење (x, y, z). Можемо да претпоставимо да $\max\{|y|_p, |z|_p\} = 1$ (у супротном поделимо или помножимо са одговарајућим p^k). Како $p \mid a$, следи да је $by^2 + cz^2 \equiv 0 \pmod{p}$, па следи да $|y|_p = |z|_p = 1$. Онда претходну конгруенцију можемо записати као $b + (z/y)^2 c \equiv 0 \pmod{p}$ па је $-b/c$ квадратни остатак. Ако је $-b/c$ квадратни остатак модуло p, ставимо $-b/c \equiv r^2 \pmod{p}$, и узмимо $y_0 = 1, z_0 = r, x_0 = 1$ Тада је $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}$. Како је још $y_0 \neq 0$ имамо услове за Хенселову лему, чијом применом добијамо да дата једначина има решење у $\mathbb{Q}_p$. □

Дакле, прошли смо све случајеве простих бројева p. Спајањем последњих неколико теорема у једну, добијамо следеће тврђење.

Теорема 5.7. *Нека су a, b, c у паровима узајамно прости бесквадратни цели бројеви. Једначина*

$$aX^2 + bY^2 + cZ^2 = 0$$

има нетривијална решења у $\mathbb{Q}$ ако и само ако су задовољени следећи услови:

(i) *a, b, c нису сви истог знака;*

(ii) *за сваки непаран прост број који дели a, постоји $r \in \mathbb{Z}$ такав да $b+r^2c \equiv 0 \pmod{p}$, и слично за непарне просте који деле b, c;*

(iii) *ако су a, b, c сви непарни, збир нека два од њих је дељив са 4;*

(iv) *ако је a паран, онда је неки од $b + c, a + b + c$ дељив са 8, и слично ако је неки од друга два паран.*

Сада посматрамо бројеве који су збир два квадрата из $\mathbb{Q}_p$. Ове бројеве посматрамо прво у $\mathbb{Z}_p$, а на крају применом претходне теореме тражимо такве бројеве и у $\mathbb{N}$.

Теорема 5.8. *За $p \equiv 1 \pmod{4}$, свако $t \in \mathbb{Z}_p$ се може записати као збир два квадрата из $\mathbb{Q}_p$.*

Доказ. Знамо да је -1 квадратни остатак по модулу p, па Хенселова лема каже да постоји $s \in \mathbb{Q}_p$ такво да је $s^2 + 1 = 0$. Онда је

$$(1 + t)^2 + (s(t - 1))^2 = 1 + 2t + t^2 - (t^2 - 2t + 1) = 4t,$$

па је

$$t = \left(\frac{1 + t}{2}\right)^2 + \left(\frac{s(1 - t)}{2}\right)^2$$

и бројеви $\dfrac{1 + t}{2}$ и $\dfrac{s(1 - t)}{2}$ су у $\mathbb{Q}_p$ јер $p \neq 2$. □

Теорема 5.9. *За $p \equiv 3 \pmod{4}$, број $t \in \mathbb{Z}_p$ је збир два квадрата из $\mathbb{Q}_p$ ако и само ако $2 \mid v_p(x)$.*

Доказ. Напишимо $t = p^v t'$ са $t' \in \mathbb{Z}_p^\times$ и $v \geq 0$. Докажимо да је могуће t' написати као збир два квадрата. Посматрајмо скупове

$$A = \{y^2 \pmod{p} : 0 \leq y \leq p - 1\}, \quad B = \{t' - x^2 \pmod{p} : 0 \leq x \leq p - 1\}.$$

Знамо да је $|A| = |B| = (p+1)/2$ (јер је $y^2 \equiv (p-y)^2 \pmod{p}$) па како $|A| + |B| = p+1 > p = |\{0, 1, \ldots, p-1\}|$ онда постоје неки $x_0, y_0 \in \{0, 1, \ldots, p-1\}$ такви да $y_0^2 \equiv t' - x_0^2 \pmod{p}$ па је $t' \equiv x_0^2 + y_0^2 \pmod{p}$ и бар један од x_0, y_0 није 0 по модулу p, нека је то без умањења

општости x_0. Дефинишимо онда $F(X) = X^2 + (y_0^2 - t')$. Како је $F(x_0) \equiv 0 \pmod{p}$ и $F'(x_0) = 2x_0 \not\equiv 0 \pmod{p}$ по Хенселовој леми постоји $x \in \mathbb{Z}_p$ такво да је $F(x_0) = 0$, односно $x^2 + y_0^2 = t'$.
Ако је v парно, то јест $v = 2k$, онда $t = p^{2k}t' = p^{2k}(x^2 + y^2) = (p^k x)^2 + (p^k y)^2$.
Ако је v непарно, претпоставимо да постоје $x, y \in \mathbb{Q}_p$ такви да је $t = x^2 + y^2$. Пошто је v непарно, ниједан од x, y не може бити 0 (јер би онда по **Теореми 3.4.3.** v био паран). Такође, мора бити $v_p(x) = v_p(y)$ (јер би у супротном било $v_p(t) = \max\{2v_p(x), 2v_p(y)\}$ што је парно). Ставимо $x = p^n z$ и $y = p^n w$ где $n \geq 0$ и $z, w \in \mathbb{Z}_p^\times$. Онда

$$t = x^2 + y^2 = p^{2n}(z^2 + w^2).$$

Пошто је $v_p(t)$ непарно, $z^2 + w^2 \notin \mathbb{Z}_p^\times$ па $z^2 + w^2 \equiv 0 \pmod{p}$. Следи $(z/w)^2 \equiv -1 \pmod{p}$. Другим речима, -1 је квадратни остатак модуло p, али то је могуће ако и само ако $p \equiv 1 \pmod{4}$, контрадикција. □

Теорема 5.10. *Ненула* $2-$*адски цео број* $t = 2^v t'$ *са* $t' \in \mathbb{Z}_2^\times$ *је збир два квадрата из* $\mathbb{Q}_2$ *ако и само ако* $t' \equiv 1 \pmod{4}$.

Доказ. Ако је $t' \equiv 1 \pmod{4}$, онда је или $t' \equiv 1 \pmod{8}$ или $t' \equiv 5 \pmod{8}$.
Ако $t' \equiv 1 \pmod{8}$, онда је по **Теореми 3.4.4.** $t' = s^2 = s^2 + 0^2$ за неко $s \in \mathbb{Q}_2$.
Ако $t' \equiv 5 \pmod{8}$, онда је $(t'/5) \equiv 1 \pmod{8}$ па по **Теореми 3.4.4.** $t'/5 = s^2$, онда $t' = 5s^2 = s^2 + (2s)^2$.
Ако је $t' \equiv 3 \pmod{4}$, претпоставимо да је t збир два квадрата у $\mathbb{Q}_2$. Пошто је $1/2 = (1/2)^2 + (1/2)^2$ збир два квадрата у $\mathbb{Q}$, $t' = t(1/2)^v$ је такође збир два квадрата у $\mathbb{Q}_2$. (јер се производ два броја која се могу написати као збир два квадрата такође може написати као збир два квадрата). Ставимо $t' = x^2 + y^2$. Ако су x и y $2-$адски цели, онда $t' \equiv x^2 + y^2 \pmod{4}$. Квадратни остаци модуло 4 су 0 и 1, па је збир два квадрата модуло 4 или 0 или 1 или 2, али смо претпоставили да је $t' \equiv 3 \pmod{4}$, контрадикција. Следи да неки од x и y није у $\mathbb{Z}_2$, на пример x. Онда $|x^2|_2 = |x|_2^2 > 1 = |t'|_2$ па је $|y^2|_2 = |t' - x^2|_2 = |x^2|_2 > 1$ по ултраметричкој неједнакости. Ставимо $|x|_2 = 2^n$, одакле и $|y|_2 = 2^n$. Нека је онда $x = z/2^n$ и $y = w/2^n$ где $z, w \in \mathbb{Z}_2^\times$. Имамо $z^2 + w^2 = 4^n t' \equiv 0 \pmod{4}$. Али пошто су z, w $2-$адске јединице имамо $z^2, w^2 \equiv 1 \pmod{4}$ што значи $z^2 + w^2 \equiv 2 \pmod{4}$, контрадикција. □

Пређимо сада на природне бројеве:

Теорема 5.11. *Број* $n \in \mathbb{N}$ *је збир два квадрата из* $\mathbb{Z}$ *ако и само ако је за сваки прост број* $p \mid n$, *за који је* $p \equiv 3 \pmod{4}$, *број* $v_p(n)$ *паран.*

Доказ. Ако број n можемо представити као збир два квадрата у $\mathbb{Q}_p$ и $\mathbb{R}$, онда је по **Теореми 5.1.** n збир два квадрата у $\mathbb{Q}$. Сада у Давенпорт-Каселсовој теореми, за квадратну форму $F(X_1, X_2) = X_1^2 + X_2^2$ важи хипотеза (јер за дато (x_1, x_2) постоје цели (y_1, y_2) за које $|x_1 - y_1| \leq 1/2$ и $|x_2 - y_2| \leq 1/2$, па $F(x_1 - y_1, x_2 - y_2) \leq 1/2$), па је n збир два квадрата у $\mathbb{Z}$. Свуда заправо важи и други смер, односно ако је број збир два квадрата из $\mathbb{Z}$ онда је и збир два квадрата у $\mathbb{Q}_p$ и $\mathbb{R}$.

Комбинујући претходне три теореме, видимо да су бројеви описани теоремом тачно бројеви који се могу представити као збир квадрата у сваком $\mathbb{Q}_p$, док нам услов за $\mathbb{R}$ даје $n > 0$. □

Слично ћемо приступити и проблему збира три квадрата. Видели смо да је сваки број у $\mathbb{Z}_p$ са $p \equiv 1 \pmod 4$ збир два квадрата из $\mathbb{Q}_p$, а самим тим и збир три квадрата.

Теорема 5.12. *За прост $p \equiv 3 \pmod 4$, свако $t \in \mathbb{Z}_p$ је збир три квадрата из $\mathbb{Q}_p$.*

Доказ. Нека $t = p^v t'$ где $v_p(t') = 0$. По **Теореми 5.9.** ако $2 \mid v$ онда је t збир два квадрата. Ако је v непарно, онда је бар 1, следи да $p \mid t$. Циљ је да остваримо услове за Хенселову лему, зато је потребно да нађемо једну тројку (x_0, y_0, z_0) такву да је $x_0^2 + y_0^2 + z_0^2 - t \equiv 0 \pmod p$, а онда применимо Хенселову лему на $F(X) = X^2 + y_0^2 + z_0^2 - t$. Служимо се истим триком као када смо у **Теореми 5.9.** доказали да v мора бити парно. Фиксирамо $x_0 = 1$ и посматрамо скупове

$$A = \{y^2 \pmod p : 0 \leq y \leq p-1\}, \quad B = \{-1 - z^2 \pmod p : 0 \leq z \leq p-1\}.$$

Важи да је $|A| = |B| = (p+1)/2$ па постоје y_0, z_0 тако да је $y_0^2 \equiv -1 - z_0^2 \pmod p$, па је $F(1) = F(x_0) = x_0^2 + y_0^2 + z_0^2 - t \equiv 0 \pmod p$ и $F'(1) = 2 \not\equiv 0 \pmod p$ па по Хенселовој леми постоји x тако да је $F(x) = 0$, одакле је t збир три квадрата. □

Теорема 5.13. *Број $t \in \mathbb{Z}_2$ је збир три квадрата из $\mathbb{Q}_2$ ако и само ако $-t$ није квадрат у $\mathbb{Q}_2$.*

Доказ. Ако је $-t$ квадрат у $\mathbb{Q}_2$, онда је $-t = 2^{2k}t'$ где $t' \equiv 1 \pmod 8$. Ако би било $t = x^2 + y^2 + z^2$, онда је и $-t' = (x/2^k)^2 + (y/2^k)^2 + (z/2^k)^2$. Такође, бројеви x, y, z морају бити 2-адски цели (ако на пример $x \notin \mathbb{Z}_2$, онда је именилац x^2 бар 4, па y^2, z^2 не могу да скрате тај именилац). Међутим, квадратни остаци модуло 8 су $0, 1, 4$, па збир 3 квадрата даје све могуће остатке модуло 8, осим 7, али $-t' \equiv 7 \pmod 8$, контрадикција. Нека сада $-t$ није квадрат у $\mathbb{Q}_2$. Видели смо да ако је t збир 3 квадрата, онда је то и $t/4^k$, па можемо претпоставити да $v_2(t) \in \{0, 1\}$. Овде припремамо услове да искористимо јачу Хенселову лему на полином $F(X) = X^2 + y_0^2 + z_0^2 - t$, за погодно изабране y_0, z_0. Како t даје неки од остатака $1, 2, 3, 5, 6$ модуло 8, који редом одговарају збировима 3 квадрата $0+0+1, 0+1+1, 1+1+1, 4+1+0, 4+1+1$, узмимо за дато t из одговарајућег збира оно x_0 за које је $v_p(x_0) = 0$, а друга два обележимо са y_0, z_0. Овако је $|F(x_0)|_2 = |x_0^2 + y_0^2 + z_0^2 - t|_2 \leq 2^{-3}$ и $|F'(x_0)|_2^2 = |4x_0^2|_2 = 2^{-2}$, па применом Хенселове леме постоји x за које $F(x) = 0$. □

Теорема 5.14. *Број $n \in \mathbb{N}$ се може записати као збир три квадрата ако и само ако $n \neq 4^a(8k+7)$ за неке $a, k \in \mathbb{N}$.*

Доказ. Применимо прво **Теорему 5.1.** да бисмо видели да је довољно да разматрамо n у пољима $\mathbb{Q}_p$ и $\mathbb{R}$. Видели смо да је n збир 3 квадрата у $\mathbb{Q}_p$ за све непарне p, а у $\mathbb{Q}_2$ ако $-n$ није квадрат у $\mathbb{Q}_2$. Али, $-n$ је квадрат у $\mathbb{Q}_2$ ако и само ако је $n = 2^{2b}(8c-1)$, што је тачно услов из теореме. Сада, служећи се сличним аргументом као у случају

збира два квадрата можемо применити и Давенпорт-Каселсову теорему на квадратну форму $F(X_1, X_2, X_3) = X_1^2 + X_2^2 + X_3^2$ (за дато (x_1, x_2, x_3), узмимо (y_1, y_2, y_3) тако да $|x_i - y_i| \leq 1/2$, одакле $F(x_1 - y_1, x_2 - y_2, x_3 - y_3) \leq 3/4$), па како имамо решење у $\mathbb{Q}$, имамо решење и у $\mathbb{Z}$. □

Последица 5.14.1. *Сваки природан број је збир* 4 *квадрата из* $\mathbb{Z}$.

Доказ. Ако је $n \neq 4^a(8k-1)$, онда је n збир 3 квадрата, па самим тим и 4. Ако $n = 4^a(8k-1)$, онда је $n = 4^a \cdot (8k-2) + (2^a)^2$ а број $4^a(8k-2)$ је збир 3 квадрата по претходној теореми. □

Последица 5.14.2. *Сваки природан број је збир* 3 *троугаона броја.*

Доказ. Нека је n позитиван цео број. Применом теореме на $8n+3$, постоје x_1, x_2, x_3 такви да је

$$x_1^2 + x_2^2 + x_3^2 = 8n + 3.$$

По модулу 4 следи да су сви x_1, x_2, x_3 непарни, нека $x_i = 2m_i + 1$. Дакле,

$$\sum_{i=1}^{3} \frac{m_i(m_i+1)}{2} = \frac{1}{8}(\sum_{i=1}^{3}(2m_i+1)^2 - 3) = \frac{1}{8}(8n+3-3) = n.$$

□

Наведимо сада пример где хипотеза Давенпорт-Каселсове теореме не важи.

Пример 11. Размотримо једначину $x^2 + 11y^2 = 3$. Она очигледно нема решења у $\mathbb{Z}$, и има решење у $\mathbb{R}$. Ако је $p \neq 2, 11$, конгруенција $x^2 \equiv 3 - 11y^2 \pmod{p}$ има решење (које се налази слично као у доказу **Теореме 5.9.**), а онда применом Хенселове леме и полазна једначина има решење у $\mathbb{Z}_p$. За $p = 2$, имамо да је $3/11 \equiv 1 \pmod{8}$ квадратни остатак модуло 2 па можемо да решимо $11y^2 = 3$ у $\mathbb{Z}_2$. За $p = 11$, имамо $5^2 \equiv 3 \pmod{11}$, па можемо решити $x^2 = 3$ у $\mathbb{Z}_{11}$.

За крај, бавићемо се квадратним формама реда бар 5. Знамо из нумеричке анализе да сваку квадратну форму можемо свести на дијагонализовану њој еквивалентну квадратну форму, то јест ону код које су ненула коефицијенти само уз чланове X_i^2.

Теорема 5.15. *Нека је* $F(X_1, X_2, \ldots, X_n)$ *квадратна форма у* $\mathbb{Z}_p$ *са* $n \geq 5$. *Тада постоји* $(x_1, x_2, \ldots, x_n) \in \mathbb{Q}_p$, *где је бар један* $x_i \neq 0$, *тако да је* $F(x_1, x_2, \ldots, x_n) = 0$.

Доказ. Видели смо да можемо претпоставити да је $F = a_1X_1^2 + \cdots + a_nX_n^2$. Заменама $X_i \mapsto p^kX_i$ можемо извући све факторе p из броја a_i, осим највише једног. Такође, можемо претпоставити да бар 3 међу a_i није дељиво са p (у супротном помножимо целу једначину са p и урадимо поново оно што смо урадили на почетку). Онда резултат за $p \neq 2$ следи по **Последици 5.3.1.**. Нека је сада $p = 2$. Онда је довољно размотрити следећа два случаја, у свакој другој квадратној форми, прво урадимо оно што смо урадили на почетку, а затим ставимо одговарајуће $X_i = 0$.

1. Ако $F = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + 2a_4X_4^2$, где су a_i непарни, имамо да се F анулира по модулу 8 за $(x_1, x_2, x_3, x_4) = (1, 1, 2, 1)$. Посматрајмо онда F као полином по X_1, заменивши $X_i = x_i$ за $i > 1$, онда је $F'(x_1) = 2x_1 \not\equiv 0 \pmod 4$, па по јачој Хенселовој леми постоји x тако да $F(x) = 0$.

2. Ако $F = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2 + a_5X_5^2$, где су a_i непарни, имамо да се F анулира по модулу 8 за $(x_1, x_2, x_3, x_4, x_5) = (1, 1, 1, 1, 2)$. Посматрајмо онда F као полином по X_1, заменивши $X_i = x_i$ за $i > 1$, онда је $F'(x_1) = 2x_1 \not\equiv 0 \pmod 4$, па по јачој Хенселовој леми постоји x тако да $F(x) = 0$. □

Пример 12. Једначина $2014x_1^2 + 2015x_2^2 + 2016x_3^2 + 2017x_4^2 = 2018x_5^2$ по претходној теореми има решење у сваком $\mathbb{Q}_p$, у $\mathbb{R}$ тривијално има решење, па по **Теореми 5.1** има решења и у $\mathbb{Q}$.

6 Закључак

У овом раду смо начели p-адске бројеве, и видели да у великом броју задатака из теорије бројева у којима тражимо целобројна или рационална решења неке једначине, има смисла трагати прво за решењима у $\mathbb{Q}_p$ и $\mathbb{R}$, и у њима је често лакше решити једначину него у $\mathbb{Q}$. И још, пажљивије коришћење Хенселове леме нам даје универзалан начин да нађемо експлицитно решење у сваком $\mathbb{Q}_p$, док поступак налажења решења у $\mathbb{Q}$ углавном зависи од једначине.

Желео бих да се захвалим менторима Стевану Гајовићу и Милошу Ђорићу на пруженој великој помоћи у избору литератури и приказаном стрпљењу и подршци приликом израде рада.

7 Литература

[1] Fernando Q. Gouvêa, *p-adic Numbers: An introduction*, Springer-Verlag, Berlin, Heidelberg, 1993.

[2] Горан Ђанковић, *Алгебра 3*, `http://poincare.matf.bg.ac.rs/~djankovic/Alg3_2018_dodatni.pdf`.

[3] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1977, 1984.

[4] Keith Conrad, *The local-global principle*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/localglobal.pdf`.

[5] Jean-Pierre Serre, *Local Fields*, Springer Verlag, Berlin, Heidelberg, New York, 1974.