STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor SOČ: 01. Matematika a statistika

p-adická čísla a jejich aplikace v teorii čísel

p-adic numbers and their applications in number theory

Autor: **Vladimír Sedláček**

Škola: **Gymnázium, Brno,**
třída Kapitána Jaroše 14

Konzultant: **Mgr. Petr Pupík**

Brno 2012

Prohlašuji, že jsem svou práci vypracoval samostatně, použil jsem pouze podklady (literaturu, SW atd.) citované v práci a uvedené v přiloženém seznamu a postup při zpracování práce je v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Brně dne 19. března 2012 .....

Poděkování
Rád bych poděkoval Mgr. Petru Pupíkovi za jeho nesmírnou ochotu, trpělivost a cenné nápady při vzniku této práce.

Abstrakt

Hlavním cílem této práce je seznámit čtenáře s tím, co jsou to p-adická čísla a čím jsou zajímavá. Teorie je budována postupně, od p-adické valuace, normy a metriky přes konstrukci p-adických čísel až po jejich aplikaci v teorii čísel, přičemž u všech tvrzení následuje důkaz. Práce se snaží najít kompromis mezi formálností a srozumitelností.

p-adická čísla propojují analýzu, algebru, teorii čísel a diferenciální počet. Dnes prakticky tvoří základ moderní teorie čísel; používají se například k prolomení některých šifrovacích algoritmů postavených na eliptických křivkách nebo k aproximaci Riemannovy zeta funkce. Navzdory vysokoškolské tematice této práce by pro její pochopení měla stačit převážně středoškolská látka, ale předpokládá se, že čtenář je obeznámen s pojmy jako limita posloupnosti, nekonečná řada, třída ekvivalence, kongruence a těleso.

Klíčová slova: p-adická čísla; p-adická valuace; p-adická norma; p-adická metrika; zúplnění racionálních čísel; Henselovo lemma

Abstract

The main goal of this paper is to get the reader introduced to the p-adic numbers and their interesting properties. The theory is being built up gradually, from the p-adic valuation, norm and metric through the construction of the p-adic numbers to their application in number theory; proofs of the statements and theorems are included as well. The paper is trying to find a compromise between formality and comprehensibility.

The p-adic numbers make a connection between the branches of analysis, number theory and differential calculus. Today they practically form the basics of number theory; they are used to break some encryption algorithms based on elliptic curves or to approximate the Riemann zeta function. Despite the academic subject matter of this paper, high school knowledge should suffice to understand it, but it is assumed that the reader is familiar with terms like sequence limit, series, equivalence class, congruence and field.

Keywords: p-adic numbers; p-adic valuation; p-adic norm; p-adic metric; completion of rational numbers; Hensel's lemma

Obsah

Úvod

Tato práce se zabývá p-adickými čísla. Jedná se o relativně málo známou, avšak o to zajímavější oblast matematiky, která propojuje algebru, analýzu a teorii čísel a má v těchto oblastech mnoho využití. Rozšíření racionálních čísel na p-adická je alternativou k rozšíření racionálních čísel na reálná, a funguje na zcela jiných principech.

První myšlenky související s p-adickými čísly se objevily v 19.století. Šlo o myšlenku zobecnit zápisy v číselné soustavě na zápisy s nekonečným rozvojem. Mezi matematiky, kteří se zabývali těmito „p-adickými metodami“, patřili například Kummer, Dedekind a Weber. O objev p-adických čísel se ale zasloužil až Kurt Hensel v roce 1897. Na počátku 20.století se rozvíjí teorie kolem valuací (Kúrschak, Ostrowski, Deuring, Schmidt, Krull) a objevuje se p-adická analýza. Trvalo ještě dlouho, než byla p-adická čísla akceptována matematickou veřejností, ale dnes už prakticky tvoří základ moderní teorie čísel.

V první kapitole této práce se budeme zabývat dělitelností celých čísel a definujeme p-adickou valuaci. Následně zjistíme, co je norma a metrika, jak spolu souvisejí, a co je to nearchimédovská metriká. Také pomocí p-adické valuace zavedeme p-adickou normu a metriku.

Ve druhé kapitole budeme zkoumat, co přesně jsou p-adická čísla a jaké mají vlastnosti. Naučíme se je sčítat, odčítat, násobit a dělit a ukážeme si, že p-adická analýza je v některých směrech jednodušší než reálná.

V poslední kapitole se podíváme na souvislost harmonických sum s p-adickými čísly a dokážeme Wolstenholmovu větu. Nakonec se budeme zabývat Henselovým lemmatem a ukážeme si, jak se s jeho pomocí dají řešit polynomiální kongruence.

Pojďme se tedy podívat, co všechno tato nevšední oblast matematiky skrývá.

1 Valuace, normy a metriky

Pro celý zbytek práce si pevně zvolme prvočíslo p. Pouze v některých speciálních případech budeme pracovat s konkrétním p, které uvedeme.

1.1 *p*-adická valuace

Definice 1.1. Nechť $n \in \mathbb{Z}$ je nenulové číslo. Pak definujeme *p-adickou valuci* $v_p(n)$ jako nejvyšší exponent α takový, že $p^\alpha \mid n$. Ekvivalentně, je-li $n = p^\alpha q$, kde $q \in \mathbb{Z}, p \nmid q$, je $v_p(n) = \alpha$. Navíc dodefinujeme $v_p(0) = \infty$.

Dále p-adickou valuaci $v_p(n)$ rozšíříme na racionální čísla: je-li $q \in \mathbb{Q}$ zlomek ve tvaru $\frac{a}{b}$, pak $v_p(q) = v_p(a) - v_p(b)$.

Nyní se můžeme na p-adickou valuaci na $\mathbb{Q}$ dívat jako na zobrazení $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Ještě než se pustíme do důkazů různých tvrzení, uvedeme si několik příkladů:

$$v_2(24) = v_2(2^3 \cdot 3) = 3,$$

$$v_3\left(\frac{3}{17}\right) = v_3(3) - v_3(17) = 1 - 0 = 1,$$

$$v_7\left(\frac{-156}{49}\right) = v_7(-156) - v_7(49) = 0 - 2 = -2,$$

$$v_{19}\left(\frac{19 \cdot 42}{19^{12345}}\right) = v_3(19 \cdot 42) - v_3(19^{12345}) = 1 - 12345 = -12344.$$

Tvrzení 1.2. *Pro $a \in \mathbb{Q}$ platí $v_p(a) = \infty \Leftrightarrow a = 0$.*

Důkaz. Implikace zprava doleva plyne přímo z definice. Implikaci zleva doprava dokážeme obměnou. Pokud je a nenulové racionální číslo, můžeme ho psát ve tvaru $a = \frac{p^\alpha q}{p^\beta r}$, kde $\alpha, \beta \in \mathbb{Z}$, $q, r \in \mathbb{Q} \setminus \{0\}, v_p(q) = v_p(r) = 0$. Pak $v_p(a) = \alpha - \beta$, což je určitě celé číslo. □

Tvrzení 1.3. *Pro $a, b \in \mathbb{Q} \setminus \{0\}$ platí $v_p(ab) = v_p(a) + v_p(b)$.*

Důkaz. Položme $a = p^\alpha q$, $b = p^\beta r$, $\alpha, \beta \in \mathbb{Z}$, $q, r \in \mathbb{Q} \setminus \{0\}, v_p(q) = v_p(r) = 0$. Ekvivalentně upravujeme:

$$v_p(ab) + v_p(p^\alpha q \cdot p^\beta r) = v_p(p^{\alpha+\beta} qr) = \alpha + \beta = v_p(p^\alpha q) + v_p(p^\beta r) = v_p(a) + v_p(b).$$

□

Důsledek 1.4. *U p-adické valuace nezáleží na tom, zda je zlomek v základním tvaru.*

Důkaz. Mějme $a \in \mathbb{Z}$ a $b, c \in \mathbb{N}$ splňující $\gcd(a, b) = 1$. Pak podle tvrzení 1.3 platí

$$v_p\left(\frac{ac}{bc}\right) = v_p(ac) - v_p(bc) = v_p(a) + v_p(c) - v_p(b) - v_p(c) = v_p\left(\frac{a}{b}\right).$$

□

Tvrzení 1.5. *Pro $a, b \in \mathbb{Q} \setminus \{0\}$ platí $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$, přičemž ostrá nerovnost může nastat pouze pro $v_p(a) = v_p(b)$.*

Důkaz. Položme $a = p^\alpha q, b = p^\beta r$, $\alpha, \beta \in \mathbb{Z}$, kde $q, r \in \mathbb{Q} \setminus \{0\}$, $v_p(q) = v_p(r) = 0$. Bez újmy na obecnosti (dále jen BÚNO) předpokládejme $\alpha \geq \beta$. Ekvivalentně upravujeme:

$$v_p(a+b) = v_p(p^\alpha q + p^\beta r) = v_p(p^\beta(p^{\alpha-\beta}q + r) \geq \beta = \min\{v_p(a) + v_p(b)\}.$$

Aby nastala ostrá nerovnost, musí platit $p \mid p^{\alpha-\beta}q + r$, ale protože $v_p(r) = 0$, musí platit $\alpha = \beta$ (a zároveň $p \mid q + r$), tedy $v_p(a) = v_p(b)$. □

Příklad. Nechť n je přirozené číslo. Spočítejte $v_p((p^n)!)$.

Řešení. Podle tvrzení 1.3 platí $v_p((p^n)!) = \sum_{i=1}^{p^n} v_p(i)$. Pro všechna $a \in \mathbb{N}$ označme $\xi_p(a)$ počet všech čísel menších nebo rovných a, která jsou dělitelná p. Stačí si uvědomit, že každé číslo dělitelné p^k, kde $k \in \mathbb{N}$, zvětší výsledek o k. To nám dává součet $\sum_{i=1}^{n} \xi_p(p^i)$, protože každé číslo dělitelné p^k v něm započítáme právě k-krát. Dostáváme tedy

$$v_p((p^n)!) = \sum_{i=1}^{p^n} v_p(i) = \sum_{i=1}^{n} \xi_p(p^i) = \sum_{i=0}^{n-1} p^i = \frac{p^n - 1}{p-1}.$$

Tvrzení 1.6 (Legendreova formule)**.** *Označme ciferný součet čísla n v soustavě o základu p jako $S_p(n)$. Pak platí*

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - S_p(n)}{p-1}.$$

Důkaz. Podle tvrzení 1.3 platí

$$v_p(n!) = \sum_{i=1}^{n} v_p(i).$$

Nyní si uvědomíme, že z této sumy nás zajímají pouze násobky p, protože všechny ostatní členy budou nulové. Násobků p, které nepřevyšují n, je celkem $\left\lfloor \frac{n}{p} \right\rfloor$. Každý z nich do sumy přispěje jedničkou. Násobky p^2, kterých je $\left\lfloor \frac{n}{p^2} \right\rfloor$ jsme ale započítali pouze jednou, i když do sumy přispívají dvojkou. Stejně tak násobky p^3, kterých je $\left\lfloor \frac{n}{p^3} \right\rfloor$, jsme započítali pouze dvakrát, i když do sumy přispívají trojkou. Takto pokračujeme dále a dostáváme

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

To, že suma je nekonečná, nám nevadí, protože od jistého dostatečně velkého $j \in \mathbb{N}$ splňujícího $p^j > n$ budou všechny členy nulové.
Nyní použijeme zápis ve tvaru $n = a_k p^k + a_{k-1}p^{k-1} + \cdots + a_1 p + a_0$, kde $k \in \mathbb{N}$ a $a_i \in \{0, 1, \ldots, p-1\}$ pro všechna $0 \leq i \leq k$. Pak máme $S_p(n) = a_k + a_{k-1} + \cdots + a_1 + a_0$. Pro všechna $0 \leq i \leq k$ zřejmě platí $p^i > a_{i-1}p^{i-1} + \cdots + a_1 p + a_0$, z čehož plyne $\left\lfloor \frac{n}{p^i} \right\rfloor = a_k p^{k-i} + a_{k-1}p^{k-i-1} + \cdots + a_{i+1}p + a_i$. Dosazením do výše dokázané identity dostáváme

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^{k} a_k p^{k-i} + a_{k-1}p^{k-i-1} + \cdots + a_{i+1}p + a_i =$$

$$= \sum_{i=1}^{k} a_i(p^{i-1} + p^{i-2} + \cdots + 1) = \sum_{i=1}^{k} a_i \frac{p^i - 1}{p-1} = \frac{\sum_{i=1}^{k} a_i p^i - \sum_{i=1}^{k} a_i}{p-1} = \frac{n - S_p(n)}{p-1},$$

což jsme chtěli dokázat. □

Důsledek 1.7. *Pro všechna $n, k \in \mathbb{Z}$, $n \geq k$ platí*

$$v_p\left(\binom{n}{k}\right) = \frac{n - S_p(n)}{p-1} - \frac{k - S_p(k)}{p-1} - \frac{(n-k) - S_p(n-k)}{p-1} =$$

$$= \frac{S_p(k) + S_p(n-k) - S_p(n)}{p-1},$$

kde $\binom{n}{k}$ značí kombinační číslo.

Důkaz. Stačí rozepsat $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ a tento výraz upravit podle 1.3 a 1.6. □

1.2 *p*-adická norma

Definice 1.8. Nechť množina $\mathbb{F}$ spolu se sčítáním a násobením tvoří těleso. Zobrazení $\|\cdot\| : \mathbb{F} \to \mathbb{R}_0^+$ nazveme *normou* na $\mathbb{F}$, pokud splňuje tyto vlastnosti:

(i) $\forall x \in \mathbb{F} : \|x\| = 0$ právě tehdy, když $x = 0$,

(ii) $\forall x, y \in \mathbb{F} : \|xy\| = \|x\| \cdot \|y\|$ (linearita),

(iii) $\forall x, y \in \mathbb{F} : \|x + y\| \leq \|x\| + \|y\|$ (trojúhelníková nerovnost).

Pokud navíc platí $\forall x, y \in \mathbb{F} : \|x + y\| \leq \max\{\|x\|, \|y\|\}$ (což je silnější nerovnost než (iii)), nazveme tuto normu *nearchimédovskou*. Všechny ostatní normy se nazývají *archimédovské*.

Standardní norma, se kterou jsme zvyklí pracovat na reálných číslech, je absolutní hodnota. Udává nám, jak je dané číslo vzdálené od počátku. Jedná se o archimédovskou normu. Nyní si pojďme uvést konkrétní příklad nearchimédovské normy.

Definice 1.9. Pro $q \in \mathbb{Q}$ definujeme p-adickou normu $|\cdot|_p$ jako

$$|q|_p := \begin{cases} 0 & \text{pro } q = 0 \\ p^{-v_p(q)} & \text{jinak.} \end{cases}$$

Dále se budeme na p-adickou normu dívat jako na zobrazení $|\cdot|_p : \mathbb{Q} \to \bigcup_{z \in \mathbb{Z}} \{p^z\} \cup \{0\}$. Opět si uvedeme několik příkladů:

$$|24|_2 = 2^{-v_2(2^3 \cdot 3)} = 2^{-3} = \frac{1}{8},$$

$$\left|\frac{3}{17}\right|_3 = 3^{v_3(3) - v_3(17)} = 3^{1-0} = 3,$$

$$\left|\frac{-156}{49}\right|_7 = 7^{v_7(-156) - v_7(49)} = 7^{0-2} = \frac{1}{49},$$

$$\left|\frac{19 \cdot 42}{19^{12345}}\right|_{19} = 19^{v_{19}(19 \cdot 42) - v_{19}(19^{12345})} = 19^{1-12345} = \frac{1}{19^{12344}}.$$

Tvrzení 1.10. *Pro všechna $a \in \mathbb{Q}$ platí $|a|_p \geq 0$, přičemž rovnost $|a|_p = 0$ nastává právě tehdy, když $a = 0$.*

Důkaz. Z definice p-adické valuace plyne $v_p(q) \in \mathbb{Z} \cup \{\infty\}$ pro všechna $q \in \mathbb{Q}$. Pokud $v_p \in \mathbb{Z}$, zřejmě musí být $|q|_p = p^{-v_p(q)} > 0$. Pro $v_p(q) = \infty$ je podle tvrzení 1.2 $q = 0$, takže platí $|q|_p = 0$. Jiné případy zřejmě nastat nemohou. □

Tvrzení 1.11. *Pro všechna $a, b \in \mathbb{Q}$ platí $|ab|_p = |a|_p \cdot |b|_p$.*

Důkaz. Dosadíme a ekvivalentně upravujeme s použitím tvrzení 1.3:

$$|ab|_p = p^{-v_p(ab)} = p^{-v_p(a)-v_p(b)} = p^{-v_p(a)} \cdot p^{-v_p(b)} = |a|_p \cdot |b|_p.$$

□

Nyní ukážeme, že tato norma je opravdu nearchimédovská.

Tvrzení 1.12. *Pro všechna $a, b \in \mathbb{Q}$ platí $|a + b|_p \leq \max\{|a|_p, |b|_p\}$.*

Důkaz. Položme $a = p^\alpha q$, $b = p^\beta r$, $\alpha, \beta \in \mathbb{Z}$, kde $q, r \in \mathbb{Q} \setminus \{0\}, v_p(q) = v_p(r) = 0$; BÚNO předpokládejme $\alpha \geq \beta$. Pak platí $|a|_p = p^{-\alpha} \leq p^{-\beta} = |b|_p$, takže $\max\{|a|_p, |b|_p\} = p^{-\beta}$. Použijeme tvrzení 1.5 a ekvivalentně upravujeme:

$$\begin{aligned} v_p(a+b) &\geq \beta \\ -v_p(a+b) &\leq -\beta \\ p^{-v_p(a+b)} &\leq p^{-\beta} \\ |a+b|_p &\leq \max\{|a|_p, |b|_p\}. \end{aligned}$$

□

Tím jsme dokázali, že $|\cdot|_p$ je nearchimédovská norma na $\mathbb{Q}$. Zároveň každá nearchimédovská norma je v podstatě p-adická, což ukazuje následující věta.

Příklad. Nechť q je racionální číslo. Ukažte, že q je celé, právě když pro všechna prvočísla p platí $|q|_p \leq 1$.

Řešení. Pro $q = 0$ platí $|q|_p = 0$. Dále předpokládejme, že q je celé nenulové číslo. Pak pro pevné p platí $q = p^{v_p(q)} r$, kde $r \in \mathbb{Z}, p \nmid r$, takže $v_p(q) \geq 0$. Pak platí $r \leq q$, z čehož plyne $|q|_p = \frac{1}{p^{v_p(q)}} = \frac{r}{q} \leq 1$.

Nyní naopak předpokládejme $|q|_p \leq 1$ pro všechna p, tedy $p^{-v_p(q)} \leq 1$. Pak je $1 \leq p^{v_p(q)}$, takže $v_p(q) \geq 0$ pro všechna p, což implikuje $q = \frac{r}{s} \cdot p^{v_p(q)}$, kde $r \in \mathbb{Z}, s \in \mathbb{N}, p \nmid r$. Pokud $s \neq 1$, můžeme nyní uvážit takové p, že $p \mid s$, čímž dostaneme $v_p(q) = v_p(p^{v_p(q)} r) - v_p(s) < v_p(q)$, což je spor. Proto musí být $s = 1$, z čehož plyne, že q je celé.

Věta 1.13 (Součinová formule)**.** *Pro každé nenulové racionální číslo q platí*

$$|q| \cdot \prod_p |q|_p = 1,$$

kde $\prod_p$ značí součin přes všechna prvočísla p.

Důkaz. Protože pro absolutní hodnotu, resp. p-adická normu platí $|q| = |-q|$, resp. $|q|_p = |-q|_p$, můžeme se omezit na $q \in \mathbb{Q}^+$. Pak můžeme psát $q = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}}{p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}}$ pro $m, n \in \mathbb{N}$ a $\alpha, \beta \in \mathbb{N}_0$. Pro všechna $i \in \mathbb{N}, i > m$ definujeme $\alpha_i = 0$ a analogicky pro všechna $i \in \mathbb{N}, i > n$ definujeme $\beta_i = 0$. Dosadíme do zadaného výrazu:

$$|q| \cdot \prod_p |q|_p = q \cdot \prod_p p^{-v_p(q)} = q \cdot \prod_p p^{v_p(p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}) - v_p(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m})} = q \cdot \prod_{p_i} \frac{p^{\beta_i}}{p^{\alpha_i}} = q \cdot \frac{1}{q} = 1.$$

□

1.3 *p*-adická metrika

Definice 1.14. Nechť X je neprázdná množina. Binární zobrazení $d(x, y) : X^2 \to \mathbb{R}_0^+$ nazveme *metrikou* na X, pokud splňuje tyto vlastnosti:

(i) $\forall x, y \in X : d(x, y) : d(x, y) = 0$ právě tehdy, když $x = y$,

(ii) $\forall x, y \in X : d(x, y) = d(y, x)$ (symetričnost),

(iii) $\forall x, y, z \in X : d(x, z) \leq d(x, y) + d(y, z)$ (trojúhelníková nerovnost).

Pokud navíc platí $\forall x, y, z \in X : d(x, z) \leq \max\{d(x, y), d(y, z)\}$ (což je silnější nerovnost než (iii)) , nazveme tuto metriku *nearchimédovskou*. Všechny ostatní metriky se nazývají *archimédovské*.
V případě, že platí $d(x, y) = \|x - y\|$, kde $\|\cdot\|$ je norma, říkáme, že metrika d je *indukovaná normou* $\|\cdot\|$. Dvojice (X, d) tvoří *metrický prostor*.

Tvrzení 1.15. *Každá metrika na tělese $\mathbb{F}$, která je indukovaná normou na tomto tělese, skutečně splňuje všechny požadavky kladené na metriku. Pokud je navíc daná norma nearchimédovská, je nearchimédovská i indukovaná metrika.*

Důkaz. Předpokládejme, že $\|\cdot\|$ je norma na $\mathbb{F}$, která na $\mathbb{F}$ indukuje metriku d a mějme $x, y, z \in \mathbb{X}$. Pak podle definice normy platí $d(x, y) = \|x-y\| = 0 \Leftrightarrow x-y = 0 \Leftrightarrow x = y$, což odpodovídá bodu (i) v definici metriky.

Dále si všimněme, že z linearity normy plyne $\|x\| = \|x \cdot 1\| = \|x\| \cdot \| 1\|$. Pro všechna $x \neq 0$ je ale $\|x\| \neq 0$, takže musí platit $\|1\| = 1$. To můžeme upravit na $\|(-1)^2\| = (\| - 1\|)^2 = 1$, a protože oborem hodnot normy jsou nezáporná čísla, dostáváme po odmocnění $\| - 1\| = 1$. Z toho už plyne symetričnost metriky: $d(x, y) = \|x - y\| = \| - 1\| \cdot \|y - x\| = d(y, x)$.

Využitím trojúhelníkové nerovnosti normy dostáváme trojúhelníkovou nerovnost metriky: $d(x, z) = \|x - z\| = \|x - y + y - z\| \leq \|x - y\| + \|y - z\| = d(x, y) + d(y, z)$.

Nakonec předpokládejme, že daná norma je nearchimédovská. Pak platí $d(x, z) = \|x - z\| = \|x - y + y - z\| \leq \max\{\|x - y\|, \|y - z\|\} = \max\{d(x, y), d(y, z)\}$, takže indukovaná metrika je také nearchimédovská. □

Metrika nám umožňuje měřit vzdálenost mezi dvěma prvky množiny. Na reálných číslech se v drtivé většině případů používá euklidovská metrika, která je indukována absolutní hodnotou a udává, jaká je vzdálenost mezi dvěma čísly na číselné ose. Tato archimédovská metrika má v životě široké využití, protože odpovídá intuitivní představě vzdálenosti. Nás teď ale bude zajímat spíše nearchimédovská metrika, přesněji p-adická.

Definice 1.16. Zobrazení $d_p(x,y) : \mathbb{Q}^2 \to \bigcup_{z\in\mathbb{Z}}\{p^z\}\cup\{0\}$ nazveme p-adickou metrikou, pokud platí

$$d_p(x,y) = |x-y|_p.$$

Tato metrika je indukována p-adickou normou, takže podle 1.15 je nearchimédovská.

Poznámka. Předpokládejme, že dvě celá čísla x, y jsou od sebe v p-adické metrice vzdálena nejvýše $\frac{1}{p^n}$ pro nějaké $n \in \mathbb{N}$, tedy $|x-y|_p \leq \frac{1}{p^n}$. Pak $p^n \leq v_p(x-y)$, takže $p^n \mid x-y$. Protože jsme celou dobu postupovali ekvivalentně, dostáváme

$$x \equiv y \pmod{p^n} \Leftrightarrow d_p(x,y) \leq \frac{1}{p^n}.$$

Všimněme si, že zavedením metriky v závislosti na dělitelnosti jsme učinili první krok k propojení p-adické analýzy a teorie čísel. U euklidovské metriky nic podobného není možné.

Tvrzení 1.17 (Princip rovnoramenného trojúhelníku)**.** *V každé nearchimédovské metrice na tělese $\mathbb{F}$ je každý trojúhelník rovnoramenný, tedy pro všechna $x, y, z \in \mathbb{F}$ platí, že alespoň dvě z hodnot $\|x-y\|, \|y-z\|, \|z-x\|$ jsou si rovny.*

Důkaz. Mějme body $x, y, z \in \mathbb{F}$. BÚNO přepokládejme $\|x-y\| \leq \|y-z\| \leq \|z-x\|$. Podle symetričnosti a trojúhelníkové nerovnosti platí

$$\|z-x\| = \|x-z\| = \|x-y+y-z\| \geq \max\{\|x-y\|, \|y-z\|\} = \|y-z\|,$$

z čehož plyne $\|z-x\| = \|y-z\|$. □

Tvrzení 1.18. *V každé nearchimédovské metrice na tělese $\mathbb{F}$ má každý kruh střed v libovolném vnitřním bodě, tedy pro každou množinu $K(S,r) = \{x \in \mathbb{F} \mid \|S-x\| \leq r\}$, kde $S \in \mathbb{F}$ a $r \in \mathbb{R}^+$, platí $a \in K(S,r) \Rightarrow K(S,r) = K(a,r)$.*

Důkaz. Mějme $a \in K(S,r)$, takže $\|S-a\| \leq r$. Pak pro všechna $x \in K(S,r)$ platí $\|S-x\| \leq r$ a podle trojúhelníkové nerovnosti také $\|a-x\| = \|a-S+S-x\| \leq \max\{\|S-a\|, \|S-x\|\} \leq r$, z čehož plyne $x \in K(S,r) \Rightarrow x \in K(a,r)$.

Naopak pro všechna $x \in K(a,r)$ platí $\|a-x\| \leq r$ a podle trojúhelníkové nerovnosti také $\|S-x\| = \|S-a+a-x\| \leq \max\{\|S-a\|, \|a-x\|\} \leq r$, z čehož plyne $x \in K(a,r) \Rightarrow x \in K(S,r)$.

Složením těchto dvou implikací dostáváme $x \in K(a,r) \Leftrightarrow x \in K(S,r)$, takže a je skutečně středem kruhu $K(S,r)$ a důkaz je hotov. □

2 *p*-adická čísla

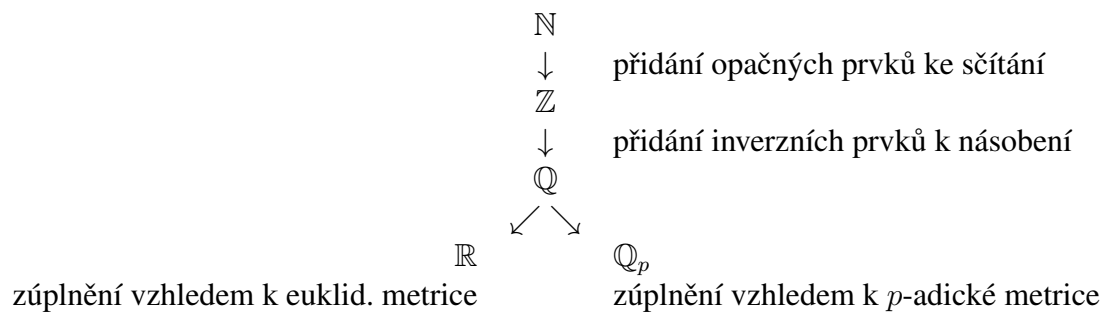
2.1 Zavedení *p*-adických čísel

Než zkonstruujeme p-adická čísla, budeme ještě potřebovat dva pojmy.

Definice 2.1. Posloupnost $\{a_i\}_{i=0}^{\infty}$ je vzhledem k metrice d *cauchyovská* právě tehdy, když platí $\forall \varepsilon \in \mathbb{R}^+ \; \exists N \in \mathbb{N} : \forall m, n \in \mathbb{N} \mid m, n \geq N : d(a_m, a_n) < \varepsilon$. Neformálně řečeno, členy cauchyovské posloupnosti se k sobě blíží libovolně blízko. Např. každá konvergentní posloupnost je zřejmě cauchyovská.

Definice 2.2. Metrický prostor (X, d) nazveme *úplný*, pokud v něm každá cauchyovská posloupnost vzhledem k metrice d konverguje vzhledem k metrice d.

Všimněme si, že množina reálných čísel vznikla zúplněním racionálních čísel vzhledem k euklidovské metrice, tj. přidáním limit všech cauchyovských posloupností racionálních čísel (vzhledem k euklidovské metrice) do množin racionálních čísel. Podobně budeme chtít vytvořit množinu p-adických čísel: zúplníme množinu racionálních čísel vzhledem k p-adické metrice. Budování číselných oborů rekapituluje následující diagram:



Definice 2.3. Množinu všech p-adických čísel $\mathbb{Q}_p$ definujeme takto: $\mathbb{Q}_p$ je množina všech nekonečných řad tvaru

$$\sum_{i=-m}^{\infty} a_i p^i = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \ldots,$$

kde $m \in \mathbb{Z}, a_{-m} \neq 0$ a $a_i \in \{0, 1, \ldots, p-1\} \; \forall i \in \mathbb{Z} \mid i \geq -m$. Čísla a_i nazýváme p-adické číslice. Dosazením za p dostáváme 3-adická čísla, 5-adická čísla, atd.

Poznámka. Narozdíl od reálných čísel nepoužívají p-adická čísla znaménko a místo nekonečného zápisu doprava mají nekonečný zápis doleva. Je to proto, že zatímco v reálných číslech řada $\sum_{i=0}^{\infty} p^i$ diverguje a řada $\sum_{i=0}^{\infty} \frac{1}{p^i}$ konverguje, v p-adické metrice je tomu přesně naopak. Další zajímavou vlastností, kterou reálná čísla nemají, je jednoznačnost zápisu (dvě p-adická čísla jsou stejná právě tehdy, když mají shodné posloupnosti p-adických číslic.)

Dohoda. Pro $a \in \mathbb{Q}_p$, $a = \sum_{i=m}^{\infty} a_i p^i$ budeme někdy pro větší přehlednost používat zápis

$$a = (\ldots a_1 a_0, a_{-1} \ldots a_{m+3} a_{m+2} a_{m+1} a_m)_p \,,$$

případně

$$a = (\ldots \{a_1\}\{a_0\}, \{a_{-1}\} \ldots \{a_{m+3}\}\{a_{m+2}\}\{a_{m+1}\}\{a_m\})_p \,,$$

pokud budou mít cifry složitější tvar.

2.2 Operace sčítání a násobení na *p*-adických číslech

Definice 2.4 („+“)**.** Neutrálním prvkem k operaci $+$ je $0 \in \mathbb{Q}_p$, tedy pro všechna $q \in \mathbb{Q}_p$ platí $q + 0 = q$. Dále mějme $\sum_{i=m}^{\infty} a_i p^i, \sum_{j=n}^{\infty} b_j p^j \in \mathbb{Q}_p \setminus \{0\}$. BÚNO předpokládejme $m \leq n$, pak můžeme dodefinovat $b_m = b_{m+1} = \cdots = b_{n-1} = 0$, takže místo prvku $\sum_{j=n}^{\infty} b_j p^j$ můžeme uvažovat prvek $\sum_{j=m}^{\infty} b_j p^j$. Nyní uvažme nekonečnou řadu $\sum_{k=m}^{\infty} c_k p^k$, kde pro všechna $l \geq m, l \in \mathbb{Z}$ platí $c_l \in \{0, 1, \ldots, p-1\}$, přičemž koeficienty c_k se určí induktivně tímto způsobem:

$$c_m \equiv a_m + b_m \pmod{p}$$

a pro všechna $l \in \mathbb{N}$ je

$$c_{m+l} \equiv \varphi(l) + a_{m+l} + b_{m+l} \pmod{p},$$

kde funkce $\varphi : \mathbb{N}_0 \to \{0, 1\}$ je definována takto:

$$\varphi(l) = \begin{cases} 0 & \text{pro } l = 0 \\ \dfrac{\varphi(l-1) + a_{m+l-1} + b_{m+l-1} - c_{m+l-1}}{p} & \text{pro } l \geq 1. \end{cases}$$

Pokud je $c_l = 0$ pro všechna $l \geq m$, klademe

$$\sum_{i=m}^{\infty} a_i p^i + \sum_{j=n}^{\infty} b_j p^j = 0.$$

V opačném případě označíme m_0 nejmenší index, pro který je $c_{m_0} \neq 0$. Pak klademe

$$\sum_{i=m}^{\infty} a_i p^i + \sum_{j=n}^{\infty} b_j p^j = \sum_{k=m_0}^{\infty} c_k p^k.$$

Definice 2.5 („·“)**.** Součin libovolného prvku s nulou je roven nule, tedy $q \cdot 0 = 0$ pro všechna $q \in \mathbb{Q}_p$. Dále opět mějme $\sum_{i=m}^{\infty} a_i p^i, \sum_{j=n}^{\infty} b_j p^j \in \mathbb{Q}_p \setminus \{0\}$. Pak klademe

$$\left(\sum_{i=m}^{\infty} a_i p^i \cdot \sum_{j=n}^{\infty} b_j p^j \right) = \sum_{k=m+n}^{\infty} c_k p^k,$$

kde pro všechna $l \geq m + n, l \in \mathbb{Z}$ platí $a_l \in \{0, 1, \ldots, p-1\}$, přičemž koeficienty c_k se opět určí induktivně:

$$c_{m+n} \equiv a_m b_n \pmod{p}$$

a pro všechna $l \in \mathbb{N}$ je

$$c_{m+n+l} \equiv \varepsilon(l) + \textstyle\sum_{s=0}^{l} a_{m+s} + b_{n+l-s} \pmod{p},$$

kde funkce $\varepsilon : \mathbb{N}_0 \to \mathbb{N}_0$ je definována takto:

$$\varepsilon(l) = \begin{cases} 0 & \text{pro l=0} \\ \dfrac{\varepsilon(l-1) + \left(\sum_{s=0}^{l-1} a_{m+s} b_{n+l-1-s} \right) - c_{m+n+l-1}}{p} & \text{pro } l \geq 1. \end{cases}$$

Poznámka. Snadno si ověříme, že pro racionální čísla jsou tyto operace konzistentní se sčítáním a násobením racionálních čísel. Tyto definice sčítání a násobení navíc odpovídají intuitivní představě písemného sčítání a násobení, při kterém postupujeme zprava doleva. Nesmíme ale zapomenout, že nepracujeme v desítkové soustavě, ale v soustavě o základu p.

Ukážeme si sčítání a násobení na příkladech. Všimněme si, že výsledek umíme určit s libovolnou přesností, ale pokud se číslice nezačnou periodicky opakovat, nikdy nebude výsledek zcela přesný.

Příklad. Sečtěte $\ldots(42356)_7$ a $\ldots(60243)_7$.

$$\begin{array}{cccccccc} & \ldots & 4 & 2 & 3 & 5 & 6 \\ + & \ldots & 6 & 0 & 2 & 4 & 3 \\ \hline & & & & & & 2 \end{array}$$

Protože $6 + 3 = 1 \cdot 7 + 2$, zapíšeme dvojku a „držíme si“ jedničku.

$$\begin{array}{cccccccc} & \ldots & 4 & 2 & 3 & 5 & 6 \\ + & \ldots & 6 & 0 & 2 & 4 & 3 \\ \hline & & & & & 3 & 2 \end{array}$$

Protože $5 + 4 + 1 = 1 \cdot 7 + 3$, zapíšeme trojku a „držíme si“ jedničku.

$$\begin{array}{cccccccc} & \ldots & 4 & 2 & 3 & 5 & 6 \\ + & \ldots & 6 & 0 & 2 & 4 & 3 \\ \hline & & & & 6 & 3 & 2 \end{array}$$

Protože $3 + 2 + 1 = 0 \cdot 7 + 6$, zapíšeme šestku a nic „si nedržíme“.

$$\begin{array}{cccccccc} & \ldots & 4 & 2 & 3 & 5 & 6 \\ + & \ldots & 6 & 0 & 2 & 4 & 3 \\ \hline & & & 2 & 6 & 3 & 2 \end{array}$$

Protože $2 + 0 = 0 \cdot 7 + 2$, zapíšeme dvojku a nic „si nedržíme“.

$$\begin{array}{cccccccc} & \ldots & 4 & 2 & 3 & 5 & 6 \\ + & \ldots & 6 & 0 & 2 & 4 & 3 \\ \hline & \ldots & 3 & 2 & 6 & 3 & 2 \end{array}$$

Protože $4 + 6 = 1 \cdot 7 + 3$, zapíšeme trojku a „držíme si“ jedničku.

Stejným způsobem bychom mohli pokračovat dále.

Příklad. Vynásobte $(\ldots 20431)_5$ a $(\ldots 31324)_5$.

$$\begin{array}{cccccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & & & & & & 4 \end{array}$$

Protože $4 \cdot 1 = 0 \cdot 5 + 4$, zapíšeme čtyřku a nic „si nedržíme“.

$$\begin{array}{cccccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & & & & & 2 & 4 \end{array}$$

Protože $4 \cdot 3 = 2 \cdot 5 + 2$, zapíšeme dvojku a „držíme si“ dvojku.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & & & & 3 & 2 & 4 \end{array}$$

Protože $4 \cdot 4 + 2 = 3 \cdot 5 + 3$, zapíšeme trojku a „držíme si“ trojku.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & & & 3 & 3 & 2 & 4 \end{array}$$

Protože $4 \cdot 0 + 3 = 0 \cdot 5 + 3$, zapíšeme trojku a nic „si nedržíme“.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \end{array}$$

Protože $4 \cdot 2 = 1 \cdot 5 + 3$, zapíšeme trojku a „držíme si“ jedničku. Přesuneme se na další řádek.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & & & & & 2 & \end{array}$$

Protože $2 \cdot 1 = 0 \cdot 5 + 2$, zapíšeme dvojku a nic „si nedržíme“.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & & & & 1 & 2 & \end{array}$$

Protože $2 \cdot 3 = 1 \cdot 5 + 1$, zapíšeme jedničku a „držíme si“ jedničku.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & & & 4 & 1 & 2 & \end{array}$$

Protože $2 \cdot 4 + 1 = 1 \cdot 5 + 4$, zapíšeme čtyřku a „držíme si“ jedničku.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & \ldots & 1 & 4 & 1 & 2 & \end{array}$$

Protože $2 \cdot 0 + 1 = 0 \cdot 5 + 1$, zapíšeme jedničku a nic „si nedržíme“. Přesuneme se na další řádek.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & \ldots & 1 & 4 & 1 & 2 & \\ & & & & 3 & & \end{array}$$

Protože $3 \cdot 1 = 0 \cdot 5 + 3$, zapíšeme trojku a nic „si nedržíme“.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & \ldots & 1 & 4 & 1 & 2 & \\ & & & 4 & 3 & & \end{array}$$

Protože $3 \cdot 3 = 1 \cdot 5 + 4$, zapíšeme čtyřku a „držíme si“ jedničku.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & \ldots & 1 & 4 & 1 & 2 & \\ & \ldots & 3 & 4 & 3 & & \end{array}$$

Protože $3 \cdot 4 + 1 = 2 \cdot 5 + 3$, zapíšeme trojku a „držíme si“ dvojku. Přesuneme se na další řádek.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & \ldots & 1 & 4 & 1 & 2 & \\ & \ldots & 3 & 4 & 3 & & \\ & & & 1 & & & \end{array}$$

Protože $1 \cdot 1 = 0 \cdot 5 + 1$, zapíšeme jedničku a nic „si nedržíme“.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & \ldots & 1 & 4 & 1 & 2 & \\ & \ldots & 3 & 4 & 3 & & \\ & \ldots & 3 & 1 & & & \end{array}$$

Protože $1 \cdot 3 = 0 \cdot 5 + 3$, zapíšeme trojku a nic „si nedržíme“. Přesuneme se na poslední řádek.

$$\begin{array}{cccccc} & \ldots & 2 & 0 & 4 & 3 & 1 \\ \cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\ \hline & \ldots & 3 & 3 & 3 & 2 & 4 \\ & \ldots & 1 & 4 & 1 & 2 & \\ & \ldots & 3 & 4 & 3 & & \\ & \ldots & 3 & 1 & & & \\ & \ldots & 3 & & & & \end{array}$$

Protože $3 \cdot 1 = 0 \cdot 5 + 3$, zapíšeme trojku a nic „si nedržíme“. Nyní sečteme všechny mezisoučty.

$$
\begin{array}{cccccc}
 & \ldots & 2 & 0 & 4 & 3 & 1 \\
\cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\
\hline
 & \ldots & 3 & 3 & 3 & 2 & 4 \\
 & \ldots & 1 & 4 & 1 & 2 & \\
 & \ldots & 3 & 4 & 3 & & \\
 & \ldots & 3 & 1 & & & \\
 & \ldots & 3 & & & & \\
\hline
 & & & & & & 4
\end{array}
$$

Protože $4 + 0 = 0 \cdot 5 + 4$, zapíšeme čtyřku a nic „si nedržíme“.

$$
\begin{array}{cccccc}
 & \ldots & 2 & 0 & 4 & 3 & 1 \\
\cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\
\hline
 & \ldots & 3 & 3 & 3 & 2 & 4 \\
 & \ldots & 1 & 4 & 1 & 2 & \\
 & \ldots & 3 & 4 & 3 & & \\
 & \ldots & 3 & 1 & & & \\
 & \ldots & 3 & & & & \\
\hline
 & & & & & 4 & 4
\end{array}
$$

Protože $2 + 2 = 0 \cdot 5 + 4$, zapíšeme čtyřku a nic „si nedržíme“.

$$
\begin{array}{cccccc}
 & \ldots & 2 & 0 & 4 & 3 & 1 \\
\cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\
\hline
 & \ldots & 3 & 3 & 3 & 2 & 4 \\
 & \ldots & 1 & 4 & 1 & 2 & \\
 & \ldots & 3 & 4 & 3 & & \\
 & \ldots & 3 & 1 & & & \\
 & \ldots & 3 & & & & \\
\hline
 & & & & 2 & 4 & 4
\end{array}
$$

Protože $3 + 1 + 3 = 1 \cdot 5 + 2$, zapíšeme dvojku a „držíme si“ jedničku.

$$
\begin{array}{cccccc}
 & \ldots & 2 & 0 & 4 & 3 & 1 \\
\cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\
\hline
 & \ldots & 3 & 3 & 3 & 2 & 4 \\
 & \ldots & 1 & 4 & 1 & 2 & \\
 & \ldots & 3 & 4 & 3 & & \\
 & \ldots & 3 & 1 & & & \\
 & \ldots & 3 & & & & \\
\hline
 & & & 3 & 2 & 4 & 4
\end{array}
$$

Protože $3 + 4 + 4 + 1 + 1 = 2 \cdot 5 + 3$, zapíšeme trojku a „držíme si“ dvojku.

$$
\begin{array}{cccccc}
 & \ldots & 2 & 0 & 4 & 3 & 1 \\
\cdot & \ldots & 3 & 1 & 3 & 2 & 4 \\
\hline
 & \ldots & 3 & 3 & 3 & 2 & 4 \\
 & \ldots & 1 & 4 & 1 & 2 & \\
 & \ldots & 3 & 4 & 3 & & \\
 & \ldots & 3 & 1 & & & \\
 & \ldots & 3 & & & & \\
\hline
 & \ldots & 0 & 3 & 2 & 4 & 4
\end{array}
$$

Protože $3+1+3+3+3+2 = 3\cdot 5+0$, zapíšeme nulu a „držíme si“ trojku.

Opět bychom mohli stejným způsobem pokračovat dále. Při odčítání a dělení postupujeme analogicky.

Nyní se pojďme podívat, jak lze nalézt opačné prvky ke sčítání a inverzní prvky k násobení.

Tvrzení 2.6. *Nechť číslo a má v $\mathbb{Q}_p$ rozvoj $(\dots a_{m+3}a_{m+2}a_{m+1}a_m)_p$, kde $m \in \mathbb{Z}$. Potom číslo $-a$ má v $\mathbb{Q}_p$ rozvoj $(\dots\{p-a_{m+3}-1\}\{p-a_{m+2}-1\}\{p-a_{m+1}-1\}\{p-a_m\})_p$.*

Důkaz. Stačí obě čísla sečíst:

$$\begin{array}{cccccc} & \dots & a_{m+3} & a_{m+2} & a_{m+1} & a_m \\ + & \dots & p-a_{m+3}-1 & p-a_{m+2}-1 & p-a_{m+1}-1 & p-a_m \\ \hline & \dots & 0 & 0 & 0 & 0 \end{array}$$

Přenesením jedniček dostáváme

$$a+(\dots\{p-a_{m+3}-1\}\{p-a_{m+2}-1\}\{p-a_{m+1}-1\}\{p-a_m\})_p = \dots 0000_p = 0,$$

z čehož plyne

$$-a = (\dots\{p-a_{m+3}-1\}\{p-a_{m+2}-1\}\{p-a_{m+1}-1\}\{p-a_m\})_p\,.$$

□

Tvrzení 2.7. *Nechť číslo $a \neq 0$ má v $\mathbb{Q}_p$ rozvoj $(\dots a_{m+3}a_{m+2}a_{m+1}a_m)_p$, kde $m \in \mathbb{Z}$ a $a_m \neq 0$. Pak existuje právě jedno $b \in \mathbb{Q}_p$ splňující $a\cdot b = 1$.*

Důkaz. Položme $b = (\dots a_{-m+3}a_{-m+2}a_{-m+1}a_{-m})_p$. Pak z definice násobení platí

$$a_m b_{-m} \equiv 1 \pmod{p}$$

Protože $\gcd(a_m, p) = 1$, má tato kongruence právě jedno řešení a jednoznačně určí $\varepsilon(1)$. Pak dostáváme kongruenci

$$a_m b_{-m+1} + a_{m+1}b_{-m} + \varepsilon(1) \equiv 0 \pmod{p},$$

která má jedinou neznámou b_{-m+1}, a ta je opět jednoznačně určena, čímž dostáváme i jednoznačné $\varepsilon(1)$. Stejným způsobem můžeme pokračovat dále a určit libovolný počet dalších cifer. □

Příklad. Nalezněte inverzní prvek vzhledem k násobení k číslu 6 v $\mathbb{Q}_3$.

Důkaz. Máme $a = 6 = 2\cdot 3+0 = (\dots 0020)_3$ a chceme najít $b \in \mathbb{Q}_p$ splňující $ab = 1$. Dostáváme kongruenci

$$2b_{-1} \equiv 1 \pmod{3},$$

jejímž jediným řešením je $b_{-1} = 2$. Pak máme

$$\varepsilon(1) = \frac{\varepsilon(0)+2\cdot 2-1}{3} = 1.$$

Dále dostáváme kongruenci

$$2b_0 + 0\cdot 1 + 1 \equiv 0 \pmod{3},$$

jejímž jediným řešením je $b_0 = 1$. Pak máme

$$\varepsilon(2) = \frac{\varepsilon(1) + 2 \cdot 1 + 0 \cdot 2 - 0}{3} = 1.$$

Nyní dostáváme kongruenci

$$2b_1 + 0 \cdot 1 + 0 \cdot 2 + 1 \equiv 0 \pmod 3,$$

jejímž jediným řešením je $b_1 = 1$. Pak máme

$$\varepsilon(3) = \frac{\varepsilon(1) + 2 \cdot 1 + 0 \cdot 1 + 0 \cdot 2 - 0}{3} = 1.$$

Nyní už si můžeme všimnout, že pro všechna $i \geq 2$ platí $b_i = 1$, protože pro všechna $j \geq 2$ je $a_j = 0$. Ověříme, že číslo $b = (\ldots 1111, 2)$ je skutečně inverzní k číslu a:

$$\begin{array}{cccccccc}
 & \ldots & 0 & 0 & 0 & 2 & 0, & 0 \\
\cdot & \ldots & 1 & 1 & 1 & 1 & 1, & 2 \\
\hline
 & \ldots & 0 & 0 & 1 & 1, & 0 & 0 \\
 & \ldots & 0 & 0 & 2 & 0, & 0 & \\
 & \ldots & 0 & 2 & 0 & 0, & & \\
 & \ldots & 2 & 0 & 0 & & & \\
 & \ldots & 0 & 0 & & & & \\
 & \ldots & 0 & & & & & \\
\hline
 & \ldots & 0 & 0 & 0 & 1, & 0 & 0.
\end{array}$$

Tvrzení 2.8. *Trojice $(\mathbb{Q}_p, +, \cdot)$ tvoří těleso.*

Důkaz. Uzavřenost, asociativita a komutativita obou operací plynou z jejich definice. Je vidět, že neutrálním prvek ke sčítání je číslo 1 a neutrálním prvkem k násobení je číslo 0. Existenci opačných a inverzních prvků jsme dokázali výše. Ověření distributivního zákona je ovšem kvůli pracnosti vynecháno. □

Definice 2.9. Mějme čísla $a, b \in \mathbb{Q}_p$ a $c \in \mathbb{Z}$ taková, že $a^c = b$. Pak říkáme, že a je c-tou odmocninou z b a píšeme $a = \sqrt[c]{b}$.

Poznámka. Všimněme si, že zadaný vztah může splňovat více čísel. Odmocnina v oboru $\mathbb{Q}_p$ proto není funkce, ale relace (podobně jako v komplexních číslech). Problematice odmocnin se budeme více věnovat v kapitole o Henselově lemmatu.

Tvrzení 2.10. *Vynásobení, resp. vydělení p-adického čísla číslem p^n je ekvivalentní s posunutím všech číslic daného čísla o n míst doleva, resp. doprava pro všechna $n \in \mathbb{Z}$.*

Důkaz. Mějme $a = (\ldots a_{m+3}a_{m+2}a_{m+1}a_m)_p$, kde $m \in \mathbb{Z}$ a . Pak platí

$$p^n \cdot a = p^n \cdot \sum_{i=0} a_i p^i = \sum_{i=0} a_i p^{i+n} = \left(\ldots a_{m+3}a_{m+2}a_{m+1}a_m \underbrace{0 \ldots 0}_{n} \right)_p .$$

Protože vynásobení p-adického čísla nenulovým číslem a následné vydělení tím stejným číslem dané p-adické číslo nezmění, dostáváme i druhou část tvrzení.

□

2.3 Rozšíření *p*-adické valuace, normy a metriky

Definice 2.11. Rozšířenou p-adickou valuaci $v_p(q) : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ definujeme jako

$$v_p(q) = \begin{cases} \infty & \text{pro } q = 0 \\ -m & \text{pro } q = \sum_{i=m}^{\infty} a_i p^i, \end{cases}$$

rozšířenou p-adickou normu $|\cdot| : \mathbb{Q}_p \to \bigcup_{z\in\mathbb{Z}}\{p^z\} \cup \{0\}$ jako

$$|q|_p = \begin{cases} 0 & \text{pro } q = 0 \\ p^{-m} & \text{pro } q = \sum_{i=m}^{\infty} a_i p^i \end{cases}$$

a rozšířenou p-adickou metriku jako $d_p(x, y) : \mathbb{Q}_p^2 \to \bigcup_{z\in\mathbb{Z}}\{p^z\} \cup \{0\}$ jako

$$d_p(x, y) = |x - y|_p.$$

Snadno se ověří, že i po rozšíření je skutečně p-adická norma normou a p-adická metrika metrikou.

Poznámka. Všimněme si, že zatímco při rozšíření $\mathbb{Q}$ na $\mathbb{R}$ se obor hodnot euklidovské normy rozšířil, při rozšíření $\mathbb{Q}$ na $\mathbb{Q}_p$ zůstal obor hodnot p-adické normy stejný.

Rozšířená p-adická valuace udává, na které pozici je poslední nenulová cifra daného p-adického čísla. Pro $a, b \in \mathbb{Q}_p$ a $k \in \mathbb{N}$ také můžeme psát $a \equiv b \pmod{p^k}$, což znamená, že platí $|a - b|_p \leq \frac{1}{p^k}$, což je vlastně ekvivalentní s tím, že p-adické rozvoje čísel a a b se zprava shodují až do koeficientu na k-tém místě.

Dohoda. V následujícím textu budeme slovo *rozšířená* vynechávat.

Následující důležité tvrzení je jedním z hlavních důvodů pro zavedení p-adických čísel:

Tvrzení 2.12. *Metrický prostor $(\mathbb{Q}_p, d_p)$ je úplný.*

Důkaz. Mějme cauchyovskou posloupnost $\{a_i\}_{i=0}^{\infty}$ vzhledem k p-adické metrice, kde $a_i \in \mathbb{Q}_p$ pro všechna $i \in \mathbb{N}_0$. Pak pro všechna $k \in \mathbb{N}$ existují $M, N \in \mathbb{N}, M > N$, která splňují $|a_M - a_N|_p < \frac{1}{p^k}$. To je ale podle poznámky výše ekvivalentní s tím, že p-adické rozvoje čísel a_M a a_N se zprava shodují až do koeficientu na k-tém místě. Odtud už je vidět, že posloupnost $\{a_i\}_{i=0}^{\infty}$ vzhledem k p-adické metrice konverguje v $\mathbb{Q}_p$. □

Jednou z výhod p-adické analýzy oproti reálné je toto tvrzení:

Tvrzení 2.13. *Mějme nekonečnou řadu $\sum_{i=0}^{\infty} a_n$, kde $a_n \in \mathbb{Q}_p$ pro všechna $n \in \mathbb{N}_0$. Tato řada je v p-adické metrice konvergentní právě tehdy, když $\lim_{n\to\infty} |a_n|_p = 0$.*

Důkaz. Mějme $M, N \in \mathbb{N}, M > N$.
Využijeme trojúhelníkové nerovnosti nearchimédovské metriky:

$$\left|\sum_{i=0}^{M} a_n - \sum_{i=0}^{N} a_n\right|_p = |a_{N+1} + a_{N+2} + \cdots + a_M|_p \leq \max\{|a_{N+1}|_p, |a_{N+2}|_p, \ldots, |a_M|_p\}.$$

Odtud už je vidět, že pokud platí $\lim_{n\to\infty} |a_n|_p = 0$, je posloupnost částečných součtů cauchyovská, a protože prostor $(\mathbb{Q}_p, d_p)$ je úplný, musí být konvergentní.

Opačná implikace je zřejmá, protože pokud řada konverguje, musí být posloupnost jejích částečných součtů cauchyovská, z čehož plyne $\lim_{n\to\infty} |a_n|_p = 0$. □

Definice 2.14. Číslo $z \in \mathbb{Q}_p$ nazýveme p-adickým celým číslem, pokud platí $|z|_p \leq 1$. Ekvivalentní definice je taková, že p-adické celé číslo nemá žádné cifry za p-tinnou čárkou ($a_i = 0 \; \forall i < 0$). Množinu p-adických celých čísel značíme $\mathbb{Z}_p$.

Tvrzení 2.15. *Každé celé číslo je p-adické celé a všechna racionální čísla $\frac{a}{b}$ taková, že $p \nmid b$ jsou p-adická celá.*

Důkaz. Pro všechna $q \in \mathbb{Q}$, jejichž jmenovatel není násobkem p, platí $v_p(q) \geq 0$. Tato podmínka je ale ekvivalentní s podmínkou $|q|_p \leq 1$, protože z definice je $|q|_p = p^{-v_p(q)}$. □

Příklad. Určete p-adický rozvoj čísla $\frac{2}{3}$ v $\mathbb{Q}_5$.

Řešení. Zřejmě platí $\gcd(3,5) = 1$, z čehož plyne $\frac{2}{3} \in \mathbb{Z}_5$. Označme $\frac{2}{3} = (\dots a_3 a_2 a_1 a_0)_p$. Dostáváme několik kongruencí:

$$\begin{aligned} 3a_0 &\equiv 2 \pmod 5 \Rightarrow a_0 = 4 \\ 3a_1 + 2 &\equiv 0 \pmod 5 \Rightarrow a_1 = 1 \\ 3a_2 + 1 &\equiv 0 \pmod 5 \Rightarrow a_2 = 3 \\ 3a_3 + 2 &\equiv 0 \pmod 5 \Rightarrow a_3 = 1. \end{aligned}$$

Nyní si můžeme všimnout, že pro všechna $i \geq 1$ platí $a_{i+2} = a_i$. Provedeme zkoušku:

$$\begin{array}{cccccccc} & \dots & 3 & 1 & 3 & 1 & 4 \\ \cdot & & & & & & 3 \\ \hline & \dots & 0 & 0 & 0 & 0 & 2. \end{array}$$

Příklad. Určete v p-adické metrice součet $1 + p + p^2 + p^3 + \dots$.

Řešení. Položme $1 + p + p^2 + p^3 + \dots = a \in \mathbb{Z}_p$ a uvažme součin $a \cdot (p-1)$:

$$\begin{array}{cccccccc} & \dots & 1 & 1 & 1 & 1 & 1 \\ \cdot & \dots & 0 & 0 & 0 & 0 & p-1 \\ \hline & \dots & p-1 & p-1 & p-1 & p-1 & p-1 \end{array}.$$

Odtud už je vidět, že

$$a \cdot (p-1) + 1 = 0,$$

tedy

$$a = \frac{1}{1-p}.$$

Příklad. Určete v p-adické metrice součet $1 - p + p^2 - p^3 + p^4 - p^5 + \dots$.

Řešení. Položme $-(1 - p + p^2 - p^3 + p^4 - p^5 + \dots) = (p-1) \cdot 1 + (p-1) \cdot p^2 + (p-1) \cdot p^4 + \dots = a \in \mathbb{Z}_p$ a uvažme součet $a + a \cdot p$:

$$\begin{array}{cccccccc} & \dots & p-1 & 0 & p-1 & 0 & p-1 \\ + & \dots & 0 & p-1 & 0 & p-1 & 0 \\ \hline & \dots & p-1 & p-1 & p-1 & p-1 & p-1 \end{array}.$$

Odtud už je vidět, že

$$p + a \cdot p + 1 = 0,$$

tedy

$$a = -\frac{1}{p+1},$$

z čehož plyne

$$1 - p + p^2 - p^3 + p^4 - p^5 + \cdots = \frac{1}{1+p}.$$

Příklad. Určete v p-adické metrice součet $1+(p-1)p+p^2+(p-1)p^3+p^4+(p-1)p^5+\ldots$.

Řešení. Položme $1+(p-1)p+p^2+(p-1)p^3+p^4+(p-1)p^5+\cdots = a \in \mathbb{Z}_p$ a uvažme součet $a + a \cdot p$:

$$\begin{array}{cccccccc} & \ldots & 1 & p-1 & 1 & p-1 & 1 \\ \cdot & \ldots & p-1 & 1 & p-1 & 1 & 0 \\ \hline & \ldots & 1 & 1 & 1 & 0 & 1 \end{array}$$

Díky výsledku předminulého příkladu je vidět, že platí

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

což dále ekvivalentně upravujeme:

$$a(p+1) - 1 = \frac{p^2}{1-p}$$

$$a(p+1) = \frac{p^2 - p + 1}{1-p}$$

$$a = \frac{p^2 - p + 1}{1-p^2}.$$

3 Aplikace *p*-adických čísel

Poznámka. V této kapitole budeme pracovat s kongruencemi, které obsahují racionální čísla. Aby tyto úvahy měly smysl, musí být jmenovatel zlomku nesoudělný s modulem. Pak je totiž zápis $\frac{a}{b} \equiv c \pmod{p}$ ekvivalentní se zápisem $a \equiv bc \pmod{p}$ pro všechna $a, b, c \in \mathbb{Z}$.

3.1 Harmonické řady a Wolstenholmova věta

Definice 3.1. Harmonickým n-tým součtem rozumíme číslo H_n, definované jako

$$H_n := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{i=1}^{n} \frac{1}{i}$$

pro všechna $n \in \mathbb{N}$.

Věta 3.2. *Mějme $m, n \in \mathbb{N}$, $m < n$. Pak platí $H_n - H_m \notin \mathbb{Z}$. Speciálně pro $m = 1$ dostáváme $H_n \notin \mathbb{Z}$, protože $H_1 = 1$.*

Důkaz. Upravme zadaný výraz:

$$H_n - H_m = \sum_{i=1}^{n} \frac{1}{i} - \sum_{i=1}^{m} \frac{1}{i} = \sum_{i=m+1}^{n} \frac{1}{i}.$$

Pro $n - m = 1$ máme $H_n - H_m = \frac{1}{n} \notin \mathbb{Z}$. Předpokládejme tedy $m - n \geq 2$. Nyní položme $r = \max\{v_2(k) \mid m + 1 \leq k \leq n\}$. Protože v této množině jsou alespoň dvě po sobě jdoucí čísla, je alespoň jedno z nich sudé, takže musí platit $r \geq 1$. Nyní předpokládejme, že existují dvě různá čísla i, j splňující $m + 1 \leq i < j \leq n$ a zároveň $v_2(i) = v_2(j) = r$. Pak můžeme psát $i = 2^r a$, $j = 2^r b$ pro nějaká lichá a, b, $a < b$. Pak ale platí $m + 1 \leq 2^r a < 2^r(a + 1) < 2^r b \leq n$, a protože je $a + 1$ sudé, musí být $v_2(2^r(a + 1)) > r$, což je spor s maximalitou r. Z čísel $v_2(m + 1), v_2(m + 2), \ldots v_2(n)$ je tedy právě jedno rovno r, z čehož plyne $v_2(H_n - H_m) = v_2(\frac{1}{r}) = -r$. Pak je ale $|H_n - H_m|_2 = 2^r > 1$, což implikuje $H_n - H_m \notin \mathbb{Z}_2$, tedy speciálně $H_n - H_m \notin \mathbb{Z}$. □

Věta 3.3. *Pro každé prvočíslo p platí, že množina $\{n \in \mathbb{N}, n \geq 1 : H_n \in \mathbb{Z}_p\}$ je konečná právě tehdy, když $\lim_{n\to\infty} |H_n|_p = \infty$.*

Důkaz. Pokud platí $\lim_{n\to\infty} |H_n|_p = \infty$, je zřejmě množina $\{n \in \mathbb{N}, n \geq 1 : H_n \in \mathbb{Z}_p\}$ konečná, protože podle definice $x \in \mathbb{Z} \Leftrightarrow |x|_p \leq 1$. Zajímavější je druhá implikace.

Mějme $n \in \mathbb{N}$ a pišme ho jako $n = pq + r$ pro nějaké $q \in \mathbb{N}$ a $r \in \{1, 2, \ldots, p - 1\}$. Množina $\mathbb{Z}_p$ je zřejmě uzavřená na sčítání. Navíc pro všechna $k \in \mathbb{N}$ splňující $\gcd(p, k) = 1$ platí $\frac{1}{k} \in \mathbb{Z}_p$. Z toho plyne

$$H_n \in \mathbb{Z}_p \Leftrightarrow \frac{1}{p} + \frac{1}{2p} + \cdots + \frac{1}{pq} = \frac{1}{p} H_q \in \mathbb{Z}_p,$$

protože všechny ostatní členy v H_n mají jmenovatel nesoudělný s p.

Protože předpokládáme, že množina $\{n \in \mathbb{N}, n \geq 1 : H_n \in \mathbb{Z}_p\}$ je konečná, musí existovat $N_0 \in \mathbb{N}$, splňující $|H_n|_p > 1$ pro všechna $n \in \mathbb{N}, n \geq N_0$. Nyní indukcí ukážeme, že pro všechna $k \in \mathbb{N}_0$ platí

$$n \geq p^k N_0 \Rightarrow |H_n|_p > p^k.$$

Pro $k = 0$ tvrzení platí podle definice N_0. Nyní předpokládejme, že tvrzení platí pro k a mějme $n = pq + r \geq p^{k+1}N_0$. Pak musí platit $q \geq p^k N_0$, z čehož plyne $|H_q|_p > p^k$. Pak je $|\frac{1}{p}H_q|_p > p^{k+1}$. Navíc $H_n - \frac{1}{p}H_q \in \mathbb{Z}_p$, takže dostáváme

$$\left|H_n - \frac{1}{p}H_q\right|_p \leq 1 < p^{k+1} < \left|\frac{1}{p}H_q\right|_p .$$

Z trojúhelníkové nerovnosti nearchimédovské normy pak dostáváme

$$\left|\frac{1}{p}H_q\right|_p = \left|\left(\frac{1}{p}H_q - H_n\right) + H_n\right|_p \leq \max\left\{\left|H_n - \frac{1}{p}H_q\right|_p, |H_n|_p\right\} = |H_n|_p .$$

Zároveň ale platí

$$|H_n|_p = \left|\left(H_n - \frac{1}{p}H_q\right) + \frac{1}{p}H_q\right|_p \leq \max\left\{\left|H_n - \frac{1}{p}H_q\right|_p, \left|\frac{1}{p}H_q\right|_p\right\} = \left|\frac{1}{p}H_q\right|_p .$$

Složením těchto dvou nerovností získáme

$$|H_n|_p = \left|\frac{1}{p}H_q\right|_p > p^{k+1},$$

takže tvrzení platí i pro $k + 1$, čímž je indukce dokončena. Posloupnost $|H_n|_p$ tedy roste nade všechny meze, z čehož plyne $\lim_{n\to\infty} |H_n|_p = \infty$. Tím je důkaz dokončen.

□

Věta 3.4 (Wolstenholmova věta)**.** *Pro všechna prvočísla $p \geq 5$ platí $H_{p-1} \equiv 0 \pmod{p^2}$.*

Důkaz. Využijeme toho, že $p - 1$ je sudé, takže můžeme členy spárovat po dvou podle „vzdálenosti od středu součtu“:

$$\begin{aligned}
H_{p-1} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-2} + \frac{1}{p-1} \\
H_{p-1} &= \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \cdots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{\frac{p+1}{2}}\right) \\
H_{p-1} &= \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{1}{i} + \frac{1}{p-i}\right) \\
H_{p-1} &\equiv \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{p}{i(p-i)}\right) \pmod{p^2} \\
\frac{1}{p}H_p &\equiv \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{1}{pi - i^2}\right) \pmod{p} \\
\frac{1}{p}H_p &\equiv -\sum_{i=1}^{\frac{p-1}{2}} \left(\frac{1}{i^2}\right) \pmod{p}
\end{aligned}$$

Nyní si všimněme, že platí

$$\left(\frac{p-1}{2}\right)^2 \equiv \left(-\frac{p-1}{2}\right)^2 \equiv \left(\frac{p+1}{2}\right)^2 \pmod{p}.$$

Navíc každé z čísel

$$1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$$

má zřejmě jinou hodnotu modulo p, takže tvoří množinu všech kvadratických zbytků. Pak musí tvořit množinu všech kvadratických zbytků i čísla

$$\frac{1}{1^2}, \frac{1}{2^2}, \ldots, \left(\frac{1}{\frac{p-1}{2}}\right)^2.$$

Kdyby totiž platilo

$$\left(\frac{1}{i^2}\right)^2 \equiv 0 \pmod{p},$$

pro nějaká $1 \leq i < j \leq \frac{p-1}{2}$, dostali bychom

$$\begin{aligned} i^2 &\equiv j^2 \pmod{p} \\ (i+j)(i-j) &\equiv \pmod{p} \\ i &\equiv \pm j \pmod{p}, \end{aligned}$$

což je spor. Dostáváme tedy

$$\begin{aligned} \frac{1}{p} H_{p-1} &\equiv -\sum_{i=1}^{\frac{p-1}{2}} \left(\frac{1}{i^2}\right) \pmod{p} \\ \frac{1}{p} H_{p-1} &\equiv -\sum_{i=1}^{\frac{p-1}{2}} i^2 \pmod{p}. \end{aligned}$$

Využijeme známý vzorec $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$:

$$\begin{aligned} \frac{1}{p} H_{p-1} &\equiv -\frac{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)p}{6} \pmod{p} \\ \frac{1}{p} H_{p-1} &\equiv -\frac{p(p^2-1)}{24} \pmod{p} \end{aligned}$$

Protože $p \geq 5$, dostáváme

$$-\frac{p(p^2-1)}{24} \equiv 0 \pmod{p},$$

tedy

$$H_{p-1} \equiv 0 \pmod{p^2},$$

což jsme chtěli dokázat.

□

3.2 Henselovo lemma

Věta 3.5 (Henselovo lemma)**.** *Nechť* $F(x) = \sum_{i=0}^{n} c_i x^i$ *je polynom s koeficienty ze* $\mathbb{Z}_p$ *a* $F'(x) = \sum_{i=1}^{n} i \cdot c_i x^{i-1}$*. Je-li* $a_0 \in \mathbb{Z}_p$ *takové, že* $F(a_0) \equiv 0 \pmod{p}$ *a zároveň* $F'(a_0) \not\equiv 0 \pmod{p}$*, pak existuje jednoznačné* $a \in \mathbb{Z}_p$ *takové, že* $F(a) = 0$ *a zároveň* $a \equiv a_0 \pmod{p}$.

Důkaz. Použitím indukce vzhledem k n ukážeme, že existuje jednoznačně zadaná posloupnost p-adických celých čísel $a_1, a_2, \ldots$, splňující tyto podmínky pro všechna $n \geq 1$:

(i) $F(a_n) \equiv 0 \pmod{p^{n+1}}$

(ii) $a_n \equiv a_{n-1} \pmod{p^n}$

(iii) $0 \leq a_n < p^{n+1}$.

Nejprve provedeme bázový krok. Mějme $n = 1$ a definujme b_0 jako číslo z množiny $\{0, 1, \ldots, p-1\}$, které je kongruentní s a_0 modulo p (zřejmě je takové právě jedno). Každé a_1, které splňuje (i) a (iii) musí být tvaru $b_0 + b_1 p$, kde b_1 je celé číslo splňující $0 \leq b_1 \leq p-1$. Rozepíšeme $F(a_1)$ podle binomické věty a využijeme přitom, že všechny členy kromě prvních dvou budou dělitelné p^2:

$$\begin{aligned}
F(a_1) &= F(b_0 + b_1 p) \\
F(a_1) &= \sum_{i=0}^{n} c_i (b_0 + b_1 p)^i \\
F(a_1) &= \sum_{i=0}^{n} \left(c_i b_0^i + i c_i b_0^{i-1} b_1 p + \binom{i}{2} c_i b_0^{i-2} b_1^2 p^2 + \cdots + c_i b^i p^i \right) \\
F(a_1) &\equiv \sum_{i=0}^{n} \left(c_i b_0^i \right) + \sum_{i=0}^{n} \left(i c_i b_0^{i-1} \right) b_1 p \pmod{p^2} \\
F(a_1) &\equiv F(b_0) + F'(b_0) b_1 p \pmod{p^2}.
\end{aligned}$$

Chceme, aby platilo $F(a_1) \equiv 0 \pmod{p^2}$. Z předpokladu $F(a_0) \equiv 0 \pmod{p}$ plyne $F(a_0) \equiv \alpha p \pmod{p^2}$, kde $\alpha \in \{0, 1, \ldots, p-1\}$. Dosadíme:

$$\begin{aligned}
\alpha p + F'(b_0) b_1 p &\equiv 0 \pmod{p^2} \\
\alpha + F'(b_0) b_1 &\equiv 0 \pmod{p}.
\end{aligned}$$

Díky předpokladu $F'(a_0) \not\equiv 0 \pmod{p}$ platí také $F'(b_0) \not\equiv 0 \pmod{p}$, takže můžeme kongruenci vydělit $F'(b_0)$:

$$b_1 \equiv -\frac{\alpha}{F'(b_0)} \pmod{p}.$$

Tím je b_1 jednoznačně určeno a po dosazení dostáváme také jednoznačné a_1:

$$\begin{aligned}
b_1 p &\equiv -\frac{\alpha p}{F'(a_0)} \pmod{p^2} \\
b_0 + b_1 p &\equiv b_0 - \frac{F(a_0)}{F'(a_0)} \pmod{p^2} \\
a_1 &\equiv b_0 - \frac{F(a_0)}{F'(a_0)} \pmod{p^2}.
\end{aligned}$$

Z podmínky $F'(b_0) \not\equiv 0 \pmod{p}$ plyne, že a_1 je p-adické celé číslo. Navíc zřejmě splňuje podmínky (i)-(iii), takže bázový krok je hotov.

Zbývá provést indukční krok. Bude velmi podobný bázovému. Předpokládejme, že už máme prvky $a_1, a_2, \ldots, a_{n-1}$ hledané posloupnosti, která splňuje podmínky (i)-(iii). Chceme najít a_n. Podle (ii) a (iii) platí $a_n = a_{n-1} + b_n p^n$, kde $b_n \in \{0, 1, \ldots, p-1\}$. Rozepíšeme $F(a_n)$ podobně jako v bázovém kroku, ale tentokrát nás nebudou zajímat členy dělitelné p^{n+1}:

$$\begin{aligned}
F(a_n) &= F(a_{n-1} + b_n p^n) \\
F(a_n) &= \sum_{i=0}^{n} c_i (a_{n-1} + b_n p^n)^i \\
F(a_n) &= \sum_{i=0}^{n} \left(c_i a_{n-1}^i + i c_i a_{n-1}^{i-1} b_n p^n + \binom{i}{2} c_i a_{n-1}^{i-2} b_n^2 p^{2n} + \cdots + c_i b_n^i p^{in} \right) \\
F(a_n) &\equiv \sum_{i=0}^{n} \left(c_i a_{n-1}^i \right) + \sum_{i=0}^{n} \left(i c_i a_{n-1}^{i-1} \right) b_n p^n \pmod{p^{n+1}} \\
F(a_n) &\equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^n \pmod{p^{n+1}}.
\end{aligned}$$

Chceme, aby platilo $F(a_n) \equiv 0 \pmod{p^{n+1}}$. Z indukčního předpokladu $F(a_{n-1}) \equiv 0 \pmod{p^n}$ plyne $F(a_{n-1}) \equiv \alpha' p^n \pmod{p^{n+1}}$, kde $\alpha' \in \{0, 1, \ldots, p-1\}$. Dosadíme:

$$\begin{aligned}
\alpha' p^n + F'(a_{n-1}) b_n p^n &\equiv 0 \pmod{p^{n+1}} \\
\alpha' + F'(a_{n-1}) b_n &\equiv 0 \pmod{p}.
\end{aligned}$$

Díky předpokladu $a_{n-1} \equiv a_n \pmod{p^n}$ platí $F'(a_{n-1}) \equiv F'(a_{n-2}) \equiv \cdots \equiv F'(a_0) \not\equiv 0 \pmod{p}$, takže můžeme kongruenci vydělit $F'(a_{n-1})$:

$$b_n \equiv -\frac{\alpha}{F'(a_{n-1})} \pmod{p}.$$

Tím je b_n jednoznačně určeno a po dosazení dostáváme také jednoznačné a_n:

$$\begin{aligned}
b_n p^n &\equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}} \\
a_n &\equiv a_{n-1} - \frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.
\end{aligned}$$

Z podmínky $F'(a_{n-1}) \not\equiv 0 \pmod{p}$ plyne, že a_n je p-adické celé číslo. Navíc zřejmě splňuje podmínky (i)-(iii), takže indukční krok je hotov. Dokázali jsme tak, že existuje právě jedna posloupnost p-adických celých čísel $a_1, a_2, \ldots$, která splňují podmínky (i)-(iii).

Důkaz Henselova lemmatu je už teď velmi jednoduchý. Stačí položit $a = b_0 + b_1 p + b_2 p^2 + \cdots = \lim_{n\to\infty} a_n$ (vzhledem k p-adické metrice). Protože pro všechna $n \in \mathbb{N}$ platí $a \equiv a_n \pmod{p^{n+1}}$, podle podmínky (i) dostáváme $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$ pro všechna $n \in \mathbb{N}$, z čehož plyne $F(a) = 0$. Naopak pro každé $a = b_0 + a_1 + a_2 + \cdots = b_0 + b_1 p + b_2 p^2 + \cdots = \lim_{n\to\infty} a_n$ dostáváme posloupnost a_n splňující podmínky (i)-iii), a z jednoznačnosti této posloupnosti plyne jednoznačnost a. Tím je Henselovo lemma dokázáno. □

Poznámka. Všimněme si, že Henselovo lemma pro p-adická čísla je velmi podobné Newtonově metodě tečen pro reálná čísla. Henselovo lemma má ale jednu velkou výhodu. Zjišťováním dalších členů posloupnosti získáváme stále více p-adických číslic hledaného kořenu, takže tento kořen musí být limitou vytvořené posloupnosti. Naopak Newtonova metoda v reálných číslech nemusí vždy konvergovat (i když tomu tak většinou je).

Poznámka. Existuje také varianta Henselova lemmatu, ve které je vypuštěn předpoklad $F'(a_0) \not\equiv 0 \pmod{p}$. Pak je kořen také jednoznačně určen, ale jeho nalezení je mnohem složitější.

Henselovo lemma nám poskytuje jednoduché kritérium pro existenci odmocnin z celých čísel v $\mathbb{Z}_p$:

Důsledek 3.6. *Mějme $q \in \mathbb{Z}$ a $n \in \mathbb{N}$, přičemž $p \nmid q$ a $p \nmid n$. Pak $\sqrt[n]{q} \in \mathbb{Z}_p$ právě tehdy, když kongruence*

$$r^n \equiv q \pmod{p}$$

má celočíselná řešení pro r.

Důkaz. Předpokládejme, že existuje $a_0 \in \mathbb{N}$ splňující $a_0^n \equiv q \pmod{p}$. Uvažme polynom $F(x) = x^n - q$. Pak platí $F(a_0) = a_0^n - q \equiv 0 \pmod{p}$ a $F'(a_0) = n a_0^{n-1} \not\equiv 0 \pmod{p}$ (protože $p \nmid q$ spolu s $a_0^n - q \equiv 0 \pmod{p}$ implikuje $p \nmid a_0$ a ze zadání $p \nmid n$). Pak podle Henselova lemmatu existuje $a \in \mathbb{Z}_p$, které splňuje $a \equiv a_0 \pmod{p}$ a zároveň $F(a) = 0$, tedy $a^n = q$, z čehož plyne $a = \sqrt[n]{q}$. Důkaz Henselova lemmatu nám navíc dává návod, jak toto a najít.

Naopak pokud $a = \sqrt[n]{q} \in \mathbb{Z}_p$, máme $a = \sum_{i=0}^{\infty} a_i p^i$, kde $a_i \in \{1, 2, \ldots, p-1\}$ pro všechna $i \in \mathbb{N}_0$. Pak musí platit $q = a^n = \left(\sum_{i=0}^{\infty} a_i p^i\right)^n$, tedy speciálně $q \equiv a_0^n \pmod{p}$, což jsme chtěli dokázat.

□

Příklad. Nalezněte rozvoj čísla $\sqrt{-3}$ v $\mathbb{Z}_7$ s přesností na 4 místa.

Řešení. Mějme $F(x) = x^2 + 3$ (z čehož plyne $F'(x) = 2x$) a $a_0 = b_0 = 2$. Postupným dosazováním čísel $1, 2, \ldots, 6$ za x zjistíme, že kogruence $F(x) \equiv 0 \pmod{7}$ má dvě řešení: $x = 2$ a $x = 5$. Položme tedy $a_0 = 2 = b_0$. Pak platí $F(a_0) \equiv 0 \pmod{7}$ a zároveň $F'(a_0) \equiv 4 \pmod{7}$. Podle Henselova lemmatu proto můžeme dopočítat další členy posloupnosti:

$$a_1 = b_0 - \frac{F(a_0)}{F'(a_0)} = 2 - \frac{7}{4} = \frac{1}{4} \equiv 37 = 2 + 5 \cdot 7 \pmod{7^2}$$

$$a_2 = a_1 - \frac{F(a_1)}{F'(a_1)} = 37 - \frac{37^2 + 3}{2 \cdot 37} = \frac{683}{37} \equiv 37 = 2 + 5 \cdot 7 + 0 \cdot 7^2 \pmod{7^3}$$

$$a_3 = a_2 - \frac{F(a_2)}{F'(a_2)} = 37 - \frac{37^2 + 3}{2 \cdot 37} = \frac{683}{37} \equiv 2095 = 2 + 5 \cdot 7 + 0 \cdot 7^2 + 6 \cdot 7^3 \pmod{7^4}$$

Odtud dostáváme

$$\sqrt{-3}_1 \doteq 2 + 5 \cdot 7 + 0 \cdot 7^2 + 6 \cdot 7^3 = 6052_7.$$

(Číslo 1 v indexu odmocniny značí, že se jedná pouze o jedno z možných řešení, zatímco číslo 7 v indexu čísla napravo značí, že se pohybujeme v 7-adických celých číslech.)

Zatím jsme ale použili pouze jedno řešení kogruence $F(x) \equiv 0 \pmod 7$. Nyní naopak zvolme $a_0 = 5 = b_0$. Pak platí $F(a_0) \equiv 0 \pmod 7$ a zároveň $F'(a_0) \equiv 3 \pmod 7$. Podle Henselova lemmatu proto opět můžeme dopočítat další členy posloupnosti:

$$a_1 = b_0 - \frac{F(a_0)}{F'(a_0)} = 5 - \frac{28}{3} = -\frac{13}{3} \equiv 12 = 5 + 1 \cdot 7 \pmod{7^2}$$

$$a_2 = a_1 - \frac{F(a_1)}{F'(a_1)} = 12 - \frac{12^2 + 3}{2 \cdot 12} = \frac{47}{8} \equiv 306 = 5 + 1 \cdot 7 + 6 \cdot 7^2 \pmod{7^3}$$

$$a_3 = a_2 - \frac{F(a_2)}{F'(a_2)} = 306 - \frac{306^2 + 3}{2 \cdot 306} = \frac{31211}{204} \equiv 306 = 5 + 1 \cdot 7 + 6 \cdot 7^2 + 0 \cdot 7^3 \pmod{7^4}$$

Odtud dostáváme

$$\sqrt{-3}_2 \doteq 5 + 1 \cdot 7 + 6 \cdot 7^2 + 0 \cdot 7^3 = 0615_7.$$

Všimněme si, že jsme dostali dva různé výsledky, což odpovídá tomu, co bychom očekávali v reálných, resp. komplexních číslech. Navíc platí

$$\sqrt{-3}_1 + \sqrt{-3}_2 = 6052_7 + 0615_7 = 0,$$

tedy

$$\sqrt{-3}_1 = -\sqrt{-3}_2.$$

To je v souladu s kongruencí

$$\sqrt{-3}_1 \equiv 2 \equiv -5 \equiv \sqrt{-3}_2 \pmod 7.$$

Na závěr si ještě ověřme, že nalezené odmocniny jsou skutečně přibližnými kořeny rovnice $x^2 + 3 = 0$:

$$0615_7^2 = 6052_7^2 = \ldots 6664_7$$

$$0615_7^2 + 3 = 6052_7^2 + 3 = \ldots 6664_7 + \ldots 0003_7$$

$$0615_7^2 + 3 = 6052_7^2 + 3 = \ldots 0000_7 = 0.$$

Hlavní význam Henselova lemmatu ovšem nespočívá ve hledání p-adických rozvojů odmocnin z celých čísel, nýbrž v řešení polynomiálních kongruencí. Jak už víme, posloupnost $a_1, a_2, \ldots$, kterou jsme v důkazu konstruovali, splňuje $F(a_n) \equiv 0 \pmod{p^{n+1}}$ pro všechna $n \in \mathbb{N}$. To znamená, že kdykoliv umíme polynomiální kongruenci vyřešit pro modulo p, umíme ji vyřešit i pro modulo p^n pro všechna $n \in \mathbb{N}$, což nám velice usnadňuje práci (pro vyřešení kongruence modulo p zřejmě stačí pouze postupně dosazovat hodnoty $\{0, 1, \ldots, p-1\}$). Ukážeme si to na příkladu.

Příklad. Nalezněte všechna celočíselná řešení kongruence $x^4 + 7x + 4 = 0 \pmod{27}$.

Řešení. Položme $F(x) = x^4 + 7x + 4$. Pak dostáváme $F'(x) = 4x^3 + 7$. Zřejmě platí $F(0) \equiv 1 \pmod 3$, $F(2) \equiv 1 \pmod 3$, $F(1) \equiv 0 \pmod 3$ a $F'(1) \equiv 2 \pmod 3$. Můžeme tedy použít Henselovo lemma pro $a_0 = b_0 = 1$. Dopočítáme další členy posloupnosti:

$$\begin{aligned}
a_1 &\equiv 1 - \frac{F(1)}{F'(1)} \pmod{3^2} \\
a_1 &\equiv 1 - \frac{12}{11} \pmod{3^2} \\
11a_1 &\equiv -1 \pmod{3^2} \\
a_1 &= 4 \\
a_1 &= 1 + 1 \cdot 3 \\
a_2 &\equiv 4 - \frac{F(4)}{F'(4)} \pmod{3^3} \\
a_2 &\equiv 4 - \frac{288}{263} \pmod{3^3} \\
263a_2 &\equiv 764 \pmod{3^3} \\
a_2 &= 22 \\
a_2 &= 1 + 1 \cdot 3 + 2 \cdot 9
\end{aligned}$$

Odtud vidíme, že číslo 22 je řešením zadané kongruence. Všechna řešení zadané kongruence jsou proto ve tvaru $x = 27k + 22$ pro nějaké $k \in \mathbb{Z}$. (Žádná další řešení neexistují, protože podmínce pro Henselovo lemma na začátku vyhovovalo právě jedno číslo.)

Závěr

Přestože p-adická čísla nepatří k běžným vysokoškolským znalostem, skrývá se v nich neobyčejný potenciál. Umožňují nečekaná propojení analýzy, algebry a teorie čísel. Zejména v teorii čísel mají řadu zajímavých aplikací, z nichž jsme si některé ukázali. Existuje velice málo prací psaných v českém jazyce, které se tímto tématem zabývají; proto lze na tuto práci nahlížet jako na úvod do této problematiky, který by měl být dost podrobný na to, aby mu mohl porozumět i český středoškolský student se zájmem o matematiku.

Použitá literatura a zdroje

[1] KOBLITZ, N.: *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics 58, Springer-Verlag New York, 1984. ISBN 0-387-96017-1.

[2] WERL, M.: *Aplikace p-adické analýzy v teorii čísel*, Diplomová práce, Přírodovědecká fakulta Masarykovy univerzity, Brno 2008

[3] BOREVICH, Z. I.,SHAFAREVICH, I .R.: *Number theory*, New York: Academic Press, 1966. 439 s. ISBN 012117851X.

[4] SORENSON, J.: *Exploring p-adic numbers and Dirichlet characters*, MTH 391W, University of Rochester, Spring 2009

[5] CONRAD, K.: *The p-adic growth of harmonic sums* [online], URL <http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/padicharmonicsum.pdf> [quote on 18-3-2012]

[6] BULANT, M.: *Algebra 2 - Teorie čísel*, Skripta k předmětu Algebra 2 na Přírodovědecké fakultě Masarykovy univerzity

[7] GOUVÊA, Q.F. [online], URL <http://www.math.uwo.ca/~srankin/courses/403/2004/hensel2.pdf> [quote on 18-3-2012]