Rozhledy matematicko-fyzikální

Adéla Heroudková

p-adická čísla

Rozhledy matematicko-fyzikální, Vol. 97 (2022), No. 3, 19–31

Persistent URL: http://dml.cz/dmlcz/151280

p-adická čísla

Adéla Heroudková, Gymnázium Brno, třída Kapitána Jaroše

Úvod

Když na přelomu 19. a 20. století přišel německý matematik Kurt Hensel s myšlenkou p-adických čísel, netušil, jak velkou roli budou hrát v matematice o pár desetiletí později.

V dnešní době patří mezi jeden z hlavních předmětů zkoumání v teorii čísel a mají využití i v jiných oborech, jako je kryptografie, fyzika, biologie a dokonce i geologie [4]. Minulý rok se dokonce přišlo na to, že by se mohla dát používat při modelování šíření viru Covid-19 [5].

Bohužel i přesto stále nepatří ani mezi základní vysokoškolské učivo. Já si ovšem myslím, že by spoustu nejen vysokoškolských studentů mohla p-adická čísla nadchnout. Proto se nyní pokusím nastínit základní myšlenku p-adických čísel a jejich vlastností.

Reálná čísla a nekonečné řady

Než se podíváme na to, co jsou to čísla p-adická, zamysleme se nad tím, co jsou to čísla reálná.

Reálná čísla se skládají z čísel racionálních a iracionálních. Racionální jsou ta, která mají konečný nebo periodický desetinný rozvoj, a iracionální jsou ta, která mají nekonečný neperiodický desetinný rozvoj – například číslo π nebo $\sqrt{2}$.

Též můžeme říct, že reálná čísla jsou množina všech nekonečných řad následujícího tvaru:

$$\pm \sum_{k=0}^{\infty} a_k \cdot 10^{m-k} = \pm(a_0 \cdot 10^{m-0} + a_1 \cdot 10^{m-1} + a_2 \cdot 10^{m-2} \dots),$$

kde m je celé číslo a $a_n \in \{0, 1, 2, \dots, 9\}$.

Každé reálné číslo umíme napsat jako tuto řadu alespoň jedním způsobem. Součet každé této řady je roven nějakému reálnému číslu. Pro ujasnění si pojďme ukázat dva konkrétní příklady:

Příklad 1. Pokusme se napsat číslo 320,78 jako zmíněnou nekonečnou řadu:

$$320{,}78 = 3\cdot 10^2 + 2\cdot 10^1 + 0\cdot 10^0 + 7\cdot 10^{-1} + 8\cdot 10^{-2} + 0\cdot 10^{-3} + 0\cdot 10^{-4} \ldots$$

Podívejme se na řadu, která se bude rovnat π:

$$\pi = 3\cdot 10^0 + 1\cdot 10^{-1} + 4\cdot 10^{-2} + 1\cdot 10^{-3} + 5\cdot 10^{-4} + 9\cdot 10^{-5} + \ldots$$

Jak vidíme, umíme tak napsat čísla s konečným i nekonečným desetinným rozvojem.

Je zřejmé, že se dané nekonečné řady musí rovnat daným číslům. Nicméně s čísly s nekonečným rozvojem je to přeci jen trochu trikovější, protože u nich sčítáme nekonečně mnoho čísel (při konečném desetinném rozvoji od jistého momentu přičítáme jen nuly) a obecně nemusí platit, že když sečteme nekonečně mnoho čísel, dostaneme reálné číslo – v mnoha případech bychom dostali plus, nebo minus nekonečno, anebo součet nemusí existovat vůbec. Na rozpoznání, zda je nekonečná řada rovna reálnému číslu nebo nekonečnu, nám slouží cauchyovské posloupnosti.

Abychom později mohli pracovat s cauchyovskými posloupnostmi p-adických čísel, zadefinujeme si je obecně pro metrické prostory.

Definice 1. Metrický prostor je neprázdná množina M spolu s metrikou ρ (vzdáleností), funkcí $\rho\colon M \times M \to \mathbb{R}^0_+$, kde pro libovolná $x, y, z \in M$ platí:

- $\rho(x, y) = 0$ právě tehdy, když $x = y$,
- $\rho(x, y) = \rho(y, x)$,
- trojúhelníková nerovnost: $\rho(x, z) \leq \rho(x, y) + \rho(y, z)$.

Vzdálenost (metriku) dvou reálných čísel definujeme jako absolutní hodnotu jejich rozdílu. Nyní není těžké si rozmyslet, že reálná čísla s touto metrikou skutečně splňují definici metrického prostoru. Nulovou vzdálenost dostaneme skutečně právě tehdy, když budeme dělat absolutní hodnotu rozdílu dvou stejných čísel. Je jedno, zda budeme brát vzdálenost čísla x od čísla y nebo obráceně. Ze školy známe trojúhelníkovou nerovnost, takže není těžké si rozmyslet, že reálná čísla s touto metrikou splňují i třetí bod z definice.

Definice 2. (*Cauchyovská posloupnost*) Uvažujme posloupnost prvků metrického prostoru M $(a_0, a_1, a_2, \dots)$ takovou, že pro jakékoli kladné pevně dané $\varepsilon > 0$ existuje index N tak, že následující nerovnost platí pro všechna $i > N$, $j > N$:

$$\rho(a_i, a_j) < \varepsilon.$$

Tedy pro libovolně malé kladné reálné číslo existuje hranice, za kterou je již vzdálenost libovolných dvou členů posloupnosti menší než toto číslo. Takovou posloupnost nazveme cauchyovskou.

Pro každou nekonečnou řadu máme definovanou posloupnost částečných součtů – například pro π je touto posloupností $(3; 3{,}1; 3{,}14; 3{,}141; 3{,}1415; 3{,}14159; \dots)$, tedy postupně přičítáme jednotlivé sčítance v nekonečné řadě. Platí, že pokud je posloupnost částečných součtů nekonečné řady cauchyovská, nekonečná řada takzvaně konverguje (její součet není roven $\pm\infty$). A v tomto případě je skutečně posloupnost $(3; 3{,}1; 3{,}14; 3{,}141; 3{,}1415; 3{,}14159; \dots)$ cauchyovská a součtem této řady je proto π.

Posloupnosti částečných součtů řad, pomocí kterých jsme vyjadřovali reálná čísla, jsou vždy cauchyovské. Pro libovolně malé nezáporné epsilon platí, že od jistého členu jsou od sebe částečné součty vzdáleny o méně, než je hodnota tohoto čísla. Například si vezměme $\varepsilon = 10^{-10}$ – pro toto malé číslo je hranicí částečný součet $a_0 \cdot 10^0 + \dots + a_{-10} \cdot 10^{-10}$, protože když si vezmeme libovolný větší částečný součet, jejich vzdálenost bude určitě menší než 10^{-10}:

$$\begin{aligned} |(a_0 \cdot 10^0 + \dots + a_{-10} \cdot 10^{-10}) - \\ - (a_0 \cdot 10^0 + \dots + a_{-10} \cdot 10^{-10} + a_{-11} \cdot 10^{-11} + \dots)| = \\ = |-(a_{-11} \cdot 10^{-11} + \dots)| < 10^{-10}, \end{aligned}$$

protože $a_n \in \{0, 1, \dots, 9\}$ pro všechna $n \in \mathbb{N}$. A vzhledem k tomu, že tato hranice existuje pro libovolně malou mocninu 10, existuje pro všechna libovolně malá ε.

Pokud je to čtenáři trochu nejasné, doporučuji si to promyslet pro zmiňovanou posloupnost $(3; 3{,}1; 3{,}14; 3{,}141; 3{,}1415; 3{,}14159; \dots)$.

Všechny tyto znalosti nyní budeme potřebovat při popisování p-adických čísel, ale přišlo mi jednodušší je vysvětlit na reálných číslech. Ona jsou totiž p-adická čísla těm reálným hodně podobná.

p-adická čísla a p-adická absolutní hodnota

Existuje více způsobů, jak p-adická čísla definovat (pro zájemce odkazuji na [2] do sekce o p-adických číslech). Já bych vám zde ráda představila ten dle mého názoru nejjednodušší na pochopení pro středoškolské studenty.

Stejně jako můžeme reálná čísla definovat jako množinu konvergentních nekonečných řad, můžeme podobně definovat i p-adická čísla. Množinu p-adických čísel definujeme pro každé prvočíslo p následovně:

$$\mathbb{Q}_p = \left\{ \sum_{n=k}^{\infty} a_n p^n, k \in \mathbb{Z}, a_n \in \{0, 1, \ldots, p-1\} \right\}.$$

Je vidět, že tato množina obsahuje všechna kladná celá čísla. Též je vidět, že každá konečná řada nám opět zadá racionální číslo (protože sčítáme konečně mnoho racionálních čísel).

Jak je to ale s těmi nekonečnými? Přeci přičítáme pořád větší mocniny p, tudíž bychom měli dostat nekonečno, protože posloupnost částečných součtů takovéto řady přeci nemůže být cauchyovská.

Trik je v tom, že na p-adických definujeme jinak vzdálenost než na reálných číslech.

Než se ale do této vzdálenosti pustíme, musíme definovat, co je to p-valuace:

Věta 1. *Pro každé prvočíslo p a každé celé nenulové n existuje právě jedno celé nezáporné $v_p(n)$ tak, že*

$$n = p^{v_p(n)} m, \quad m \in \mathbb{Z}, \quad p \nmid m.$$

Důkaz. Tato věta plyne z toho, že pro každé celé nenulové n máme jednoznačný rozklad na součin prvočinitelů (až na násobení ± 1). Následně $v_p(n)$ je rovno exponentu p v tomto rozkladu.

Definice 3. Číslo $v_p(n)$ z předchozí věty 1 nazýváme p-valuací čísla n. Valuaci rozšíříme na racionální čísla následovně: jestliže $x = \frac{a}{b} \in \mathbb{Q} \setminus \{0\}$, $a, b \in \mathbb{Z}$, $\mathrm{nsd}(a, b) = 1$, potom

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

Pro nulu zavedeme

$$v_p(0) = \infty.$$

Příklad 1. Pro ujasnění si uveďme příklad:

- $9 = 3^2 \implies v_3(9) = 2$,
- $4 = 2^2(3^0),\ \ 54 = 2^1 3^3 \implies v_3(\frac{4}{54}) = 0 - 3 = -3$,
- $3 = 3^1(5^0),\ \ 22 = 2^1 11^1(5^0) \implies v_5(\frac{3}{22}) = 0 - 0 = 0$.

Pojďme se podívat na nějaké užitečné vlastnosti p-valuace:

Věta 2. *Pro všechna $x, y \in \mathbb{Q}$, platí:*

1. $v_p(xy) = v_p(x) + v_p(y)$,
2. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Důkaz. Nejprve si vezměme případ, kdy je jedno z čísel nulové. Součtem celého čísla a nekonečna rozumíme nekonečno a nekonečno považujeme za větší než libovolné celé číslo. Potom je pro tento případ jasné, že tvrzení platí.

Čísla $x \neq 0, y \neq 0$ si zapíšeme jako: $x = p^a \frac{x'}{x''}, y = p^b \frac{y'}{y''}$, $p \nmid x'x''y'y''$ a $x', x'', y', y'' \in \mathbb{Z}$.

První vlastnost dokážeme následovně:

$$v_p(xy) = v_p\left(p^a \frac{x'}{x''} p^b \frac{y'}{y''}\right) = v_p\left(p^{a+b} \frac{x'}{x''} \frac{y'}{y''}\right) = a + b = v_p(x) + v_p(y).$$

Nyní se podívejme na druhou vlastnost a řekněme bez újmy na obecnosti, že platí, že $\min\{v_p(x), v_p(y)\} = \min\{a, b\} = a$:

$$v_p(x + y) = v_p\left(p^a \frac{x'}{x''} + p^b \frac{y'}{y''}\right) = v_p\left(p^a \left(\frac{x'}{x''} + p^{b-a} \frac{y'}{y''}\right)\right) =$$
$$= a + v_p\left(\frac{x'}{x''} + p^{b-a} \frac{y'}{y''}\right) \geq \min\{a, b\}.$$

Poslední nerovnost musí platit, protože když si převedeme zlomek na stejného jmenovatele, dostaneme

$$v_p\left(\frac{x'y'' + p^{b-a}y'x''}{x''y''}\right) \geq 0,$$

neboť p může dělit $x'y'' + p^{b-a}y'x''$, ale nemůže dělit $x''y''$. Levá strana je tudíž rovna a, pokud je $b > a$, protože pak $p \nmid (x'y'' + p^{b-a}y'x'')$.

Naopak pokud je $a = b$, pak součet $x + y$ může mít jinou valuaci než $\min\{a, b\}$. Prvočíslo p totiž může dělit $x'y'' + y'x''$.

Za pomoci p-valuace můžeme zavést slibovanou p-adickou vzdálenost. Použijeme na to takzvanou p-adickou absolutní hodnotu.

Definice 4. Pro každé nenulové $x \in \mathbb{Q}$ definujeme jeho p-adickou absolutní hodnotu jako:

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

Pokud $x = 0$, pak $|x|_p = 0$.

Nyní se pojďme zamyslet, v čem se podobá a v čem se liší od klasické absolutní hodnoty, jak jsme si ji představili před chvilkou.

Platí, že $|x|_p = 0$ právě tehdy, když $x = 0$, stejně jako u klasické absolutní hodnoty. Stejně tak platí $|xy|_p = |x|_p \cdot |y|_p$, což plyne z první části věty 2. Z druhé části této věty plyne i další vlastnost stejná s klasickou absolutní hodnotou: $|x + y|_p \leq |x|_p + |y|_p$ – tedy trojúhelníková nerovnost.

Druhá část této věty nám též umožňuje říct ještě silnější tvrzení, a to, že $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ – jedná se o takzvanou nearchimédovskou vlastnost, a proto p-adické absolutní hodnotě říkáme nearchimédovská. Klasická absolutní hodnota tuto vlastnost nemá a říká se jí tudíž archimédovská.

Když si opět definujeme vzdálenost dvou čísel jako absolutní hodnotu (v tomto případě p-adickou absolutní hodnotu) jejich rozdílu, dostaneme, že stejně jako reálná čísla i p-adická čísla tvoří metrický prostor.

Díky nearchimédovské vlastnosti p-adické absolutní hodnoty platí následující věta.

Věta 3. *Posloupnost (x_n) racionálních čísel je cauchyovská vzhledem k nearchimédovské absolutní hodnotě $|\ |_p$ právě tehdy, když pro libovolně malé ε platí, že existuje index $N \in \mathbb{N}$ takový, že:*

$$|x_N - x_{N+1}|_p < \varepsilon.$$

Důkaz můžete opět nalézt v [3] v druhé kapitole nebo si ho zkusit rozmyslet.

Díky této větě platí, že p-adická čísla, jakožto nekonečné řady, mají vždy konečný součet. Posloupnosti jejich částečných součtů jsou totiž určitě cauchyovské.

Uveďme si dva konkrétní příklady nekonečných p-adických řad.

Příklad 2. Zkusme najít 3-adické vyjádření pro $\frac{1}{5}$. Pro tento zlomek platí, že pokud ho vynásobíme pětkou, dostaneme jedničku. Tento vztah

musí splňovat i jejich 3-adické vyjádření. Nekonečnou řadu pro jedničku a pětku známe a tu pro $\frac{1}{5}$ si pojďme prozatím napsat pomocí neurčitých koeficientů:

$$1 = (2 + 1 \cdot 3)(a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + \dots).$$

Nyní musí platit, že $2a_0$ dává zbytek 1 po dělení třemi, tudíž $a_0 = 2$. Odtud dostaneme

$$-3^2 = (2 + 1 \cdot 3)(a_1 \cdot 3 + a_2 \cdot 3^2 + \dots),$$

tudíž $0 = 2a_1 \cdot 3 \mod 9$, což je ekvivalentní $0 = 2a_1 \mod 3$. Máme tak $a_1 = 0$. Odtud dále plyne

$$-3^2 = (2 + 1 \cdot 3)(a_2 \cdot 3^2 + a_3 \cdot 3^3 + \dots),$$

tedy $-3^2 = 2a_2 \cdot 3^2 \mod 3^3$, což je ekvivalentní $-1 = 2a_2 \mod 3$. Platí proto $a_2 = 1$. Odtud nyní dostaneme

$$-2 \cdot 3^3 = (2 + 1 \cdot 3)(a_3 \cdot 3^3 + a_4 \cdot 3^4 + \dots),$$

tudíž $-2 \cdot 3^3 = 2a_3 \cdot 3^3 \mod 3^4$, což je ekvivalentní $-2 = 2a_3 \mod 3$. Máme tak $a_3 = 2$. Podobným uvažováním bychom postupně spočítali i zbytek koeficientů pro $\frac{1}{5}$ a dostali, že $\frac{1}{5} = \dots 1012\ 1012\ 1012\ 102|_3$. Pro přehlednost píšeme 3-adické vyjádření pouze pomocí koeficientů (jako bychom psali číslo v trojkové soustavě).

Dalším příkladem nekonečných p-adických řad jsou vyjádření pro záporná racionální čísla. My se podíváme na vyjádření záporných celých čísel, protože se s nimi lépe počítá.

Příklad 3. Podívejme se na 3-adické vyjádření čísel 1, 2, 3, 4, 5:

$$1 = 1|_3, \quad 2 = 2|_3, \quad 3 = 10|_3, \quad 4 = 11|_3, \quad 5 = 12|_3.$$

Nyní hledáme vyjádření pro čísla -1, -2, -3, -4 a -5. Když tato čísla přičteme k jejich číslům opačným, dostaneme nulu.

Podívejme se na -1, jako koeficient a_0 musí mít 2, protože po sečtení s $1|_3$ dostaneme na pozici jednotek 0. Nicméně nám přeteče jednička na další pozici, tudíž $a_1 = 2$, abychom opět dostali nulu. A znovu nám přetekla jednička, takže též přidáme dvojku a když budeme pokračovat dál dostaneme: $-1 = \dots 2222|_3$. Stejným uvažováním dostaneme i vyjádření pro ostatní záporná čísla:

$$-2 = \dots 2221|_3, \ -3 = \dots 22220|_3, \ -4 = \dots 22212|_3, \ -5 = \dots 22211|_3.$$

Příklad 4. Stejně bychom pracovali i s jinými prvočísly než je 3. Můžeme se zamyslet, jak by obecně vypadala -1 v p-adickém vyjádření. Platí, že 1 vypadá ve všech p soustavách následovně: $1 = 1|_p$. Tudíž $-1 = \ldots(p-1)(p-1)(p-1)(p-1)|_p$.

Díky nearchimédovské vlastnosti p-adické absolutní hodnoty též platí, že v p-adickém prostoru jsou všechny trojúhelníky rovnoramenné. Což znamená, že když si vezmeme libovolná tři p-adická čísla a spočítáme jejich vzdálenosti, vždy se budou alespoň dvě z těchto tří hodnot rovnat.

Věta 4. *V p-adickém prostoru jsou všechny trojúhelníky rovnoramenné.*

Důkaz. Mějme tři p-adická čísla x, y, z. Ukážeme, že pokud

$$|x-y|_p \neq |y-z|_p,$$

tak platí:

$$|x-z|_p = \max\{|x-y|_p, |y-z|_p\}.$$

Díky symetrii mezi x a z můžeme bez újmy na obecnosti předpokládat, že $|x-y|_p < |y-z|_p$. Z nearchimédovské vlastnosti plyne

$$|x-z|_p \leq \max\{|x-y|_p, |y-z|_p\} = |y-z|_p.$$

Podobně

$$|y-z|_p \leq \max\{|y-x|_p, |x-z|_p\} = \max\{|x-y|_p, |x-z|_p\}.$$

Maximum vpravo nemůže být $|x-y|_p$, protože $|x-y|_p < |y-z|_p$. Je to tedy $|x-z|_p$. Z čehož dostaneme $|x-z|_p = |y-z|_p$, což jsme chtěli dokázat.

V p-adickém prostoru se též velice zajímavě chovají koule. Pojďme si nejprve zadefinovat, co to taková koule je:

Definice 5. Otevřenou p-adickou kouli o poloměru r a středu $a \in \mathbb{Q}_p$ definujeme následovně:

$$B(a,r) = \{x \in \mathbb{Q}_p, |x-a|_p < r\}.$$

A uzavřenou p-adickou kouli o poloměru $r \in \mathbb{R}$ a středu $a \in \mathbb{Q}_p$ definujeme následovně:

$$\bar{B}(a,r) = \{x \in \mathbb{Q}_p, |x-a|_p \leq r\}.$$

Pro p-adické koule platí následující tvrzení:

Věta 5.

1. *Pokud $b \in B(a,r)$, pak*

$$B(a,r) = B(b,r).$$

Jinými slovy, každý bod ležící v otevřené kouli je jejím středem.

2. *Mějme $a, b \in \mathbb{Q}_p$, $r, s \in \mathbb{R}$, pro která platí*

$$B(a,r) \cap B(b,s) \neq \emptyset,$$

potom platí, že

$$B(a,r) \subset B(b,s) \quad \textit{nebo} \quad B(b,s) \subset B(a,r).$$

Tedy každé dvě otevřené koule se buď neprotínají, nebo jedna leží v té druhé.

Důkaz. Vzhledem k tomu, že $b \in B(a,r)$, platí, že $|b-a|_p < r$. Vezměme si libovolné $x \in B(a,r)$, $x \neq b$. Tudíž opět platí $|x-a|_p < r$. Z nearchimédovské vlastnosti plyne:

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

Tedy $x \in B(b,r)$, z čehož plyne

$$B(a,r) \subset B(b,r).$$

Když prohodíme a a b, dostaneme opačnou inkluzi, z čehož plyne, že jsou tyto dvě koule shodné.

Nyní se podívejme na druhé tvrzení. Bez újmy na obecnosti řekněme, že $r \leq s$. Podle zadání musí existovat $c \in B(a,r) \cap B(b,s)$. Potom podle prvního tvrzení víme, že

$$B(a,r) = B(c,r) \quad \text{a} \quad B(b,s) = B(c,s).$$

Z toho dostaneme:

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

což je to, co jsme chtěli dokázat.

Toto tvrzení platí i pro uzavřené koule a dokazuje se stejně.

Důležitou uzavřenou koulí v p-adických číslech je koule se středem v nule a poloměrem jedna, nazýváme ji množinou celých p-adických čísel:

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

Též se dá zapsat následovně:

$$\mathbb{Z}_p = \left\{ \sum_{n=0}^{\infty} a_n p^n, a_n \in \{0,1,\ldots,p-1\} \right\}.$$

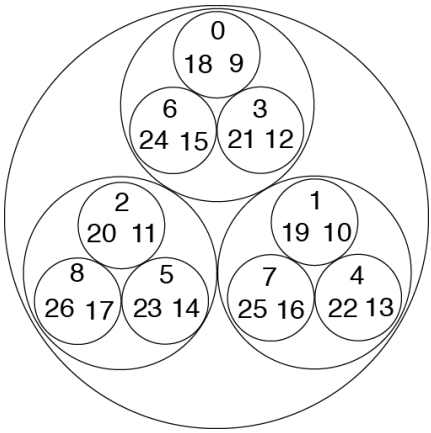
Je vidět, že její podmnožinou jsou celá čísla, protože všechna celá čísla mají p-adickou absolutní hodnotu menší nebo rovnu jedné.

Celá p-adická čísla mají spoustu užitečných vlastností, o kterých se můžete dozvědět v [3, kapitola 3].

p-adická čísla v prostoru

Další zvláštností p-adických čísel je, že není jednoduché si je představit v prostoru. Netvoří totiž souvislý prostor jako reálná čísla.

Ale díky tomu, že je máme vyjádřené jako dané nekonečné řady, můžeme si je představit následovně: máme p koleček, v každém z nich p menších koleček, a tak to pokračuje dál. Na obr. 1 vidíme případ, kdy $p = 3$. Pro zjednodušení jsou na obrázku jenom celá p-adická čísla. Největší koule je tedy $\bar{B}(0,1)$ a v ní jsou postupně koule o poloměru $\frac{1}{p}$, $\frac{1}{p^2}$ atd.

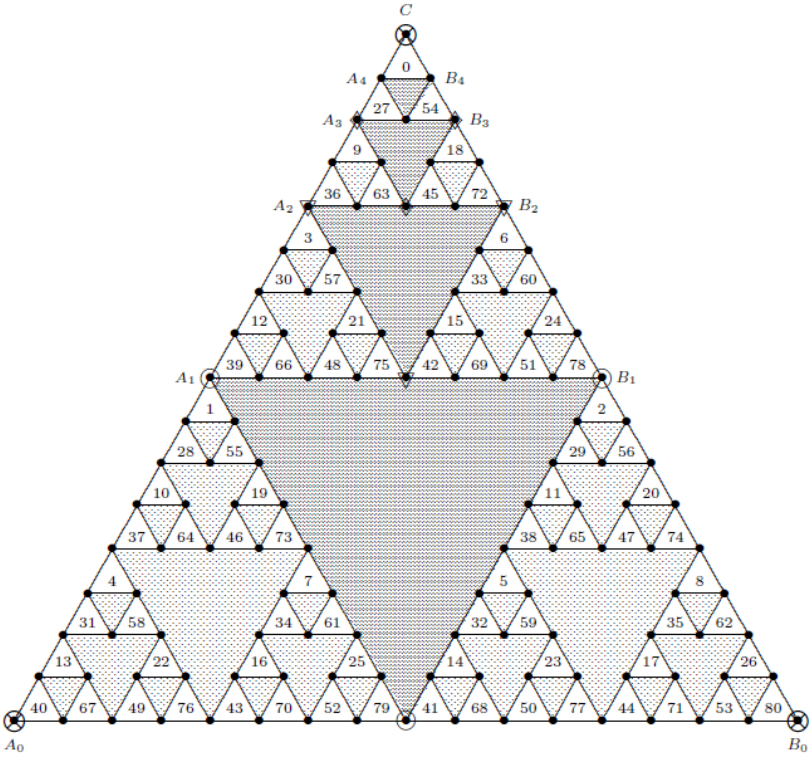


Obr. 1 [8]

A jak se umisťují čísla do koleček? Čísla se stejným koeficientem u p^0 umístíme do stejného kolečka. Následně v tomto kolečku roztřídíme čísla do p menších koleček podle koeficientu u p^1 atd. Pro p-adická čísla platí, že čím menší kolečko spolu sdílejí, tím jsou si p-adicky blíže.

Příklad 5. Například 26 napíšeme 3-adicky jako $2+2\cdot3+2\cdot3^2$. Následně 17 napíšeme 3-adicky jako $2+2\cdot3+3^2$ a 23 napíšeme jako $2+3+2\cdot3^2$. Všechna tato čísla mají koeficient u p^0 dva, proto spolu sdílejí větší kolečko. Koeficient u p^1 mají 26 a 17 opět dva, proto spolu sdílejí i menší kolečko, ale 23 má tento koeficient roven jedné, proto je v jiném kolečku. A kdyby se do koleček rozdělovaly dál, tak 17 a 26 spolu už menší kolečko sdílet nebudou, protože koeficient u p^2 už mají různý.

Hezky se dají celá 3-adická čísla znázornit pomocí doplnění do Sierpińského trojúhelníku (obr. 2).



Obr. 2

Vidíme zde čísla ve vzdálenosti 0, $\frac{1}{27}$, $\frac{1}{9}$, $\frac{1}{3}$ a 1 od nuly. Nahoře vidíme nulu a pod ní jsou čísla, co jsou jí nejblíže, 27 a 54, ve vzdálenosti $\frac{1}{27}$. Dva trochu větší trojúhelníčky pod body A_3 a B_3 obsahují čísla ve vzdálenosti $\frac{1}{9}$ od nuly. Dva ještě větší trojúhelníky pod body A_2 a B_2 obsahují čísla ve vzdálenosti $\frac{1}{3}$ od nuly a ty největší trojúhelníky pod body A_1 a B_1 obsahují čísla ve vzdálenosti 1 od nuly.

Doufám, že je z obrázků jasné, že i když se p-adická čísla v něčem podobají těm reálným, v mnoha případech se chovají odlišně, protože nejsou uspořádaná lineárně.[1)]

Využití p-adických čísel v matematice

Významné využití v matematice má například p-adická analýza, kde sice existuje spousta zajímavých tvrzení, která neplatí v reálné analýze, ale zase se zde daleko hůř pracuje s derivacemi.

Jeden z důvodů, proč jsou p-adická čísla tak užitečná, je, že kromě reálných a p-adických čísel neexistují žádné další množiny obsahující racionální čísla s takovými vlastnostmi, jako mají tyto množiny. V matematice je někdy těžké rozhodnout, zda tvrzení platí pro racionální čísla, a využívá se toho, že se tato tvrzení prvně zkoumají pro reálná a p-adická čísla. Například platí, že kvadratická forma má řešení nad racionálními čísly, právě když má řešení v reálných číslech a ve všech p-adických.

Jako důkaz, jak moc aktuálním tématem v matematice p-adická čísla jsou, může posloužit fakt, že je využil Andrew Wiles při svém důkazu Velké Fermatovy věty a můžeme je nalézt i ve dvou Problémech tisíciletí.

Kdybyste se chtěli podívat na nějaké trochu pochopitelnější využití p-adických čísel, doporučuji se podívat na důkaz, že čtverec není možné rozdělit na lichý počet trojúhelníků stejného obsahu, který využívá 2-adických čísel. Podrobný důkaz můžete nalézt v [1] a [6].

Poděkování

Závěrem bych chtěla poděkovat svému recenzentovi za spoustu dobrých rad a připomínek.

[1)] Mějme relaci $\mathcal{R}$ na množině X a tři prvky $a, b, c \in X$. Potom tuto relaci nazveme lineárním uspořádáním, pokud splňuje, že je
– tranzitivní ($a\mathcal{R}b \wedge b\mathcal{R}c \implies a\mathcal{R}c$),
– slabě asymetrická ($a\mathcal{R}b \wedge b\mathcal{R}a \implies a = b$) a
– trichotomická ($a\mathcal{R}b \vee b\mathcal{R}a \vee a = b$). [7]

Literatura

[1] Dlab, V., Bečvář, J.: *Od aritmetiky k abstraktní algebře*. 2. vydání, ČVUT, Praha, 2022.

[2] Kato, K., Saitō, T., Kurokawa, N.: *Fermat's Dream*. Number theory, 186, Amer. Math. Soc., Providence, R.I., 2000.

[3] Heroudková, A.: *p-adická čísla*. Masarykova univerzita, Brno, 2021, https://socv2.nidv.cz/archiv43/getWork/hash/e2ad1406-9303-11eb-acaf-005056bd6e49.

[4] Khrennikov, A., Lopéz, M. C., Oleschko, K.: *Applications of p-adic numbers: from physics to geology*. In: *Advances in Non-Archimedean Analysis*, Contemporary mathematics, 665,2016, https://www.researchgate.net/publication/303480790_Applications_of_-adic_numbers_from_physics_to_geology.

[5] Khrennikov, A.: Ultrametric diffusion equation on energy landscape to model disease spread in hierarchic socially clustered population. *Physica A*, 583 (2021), č. 126284, s. 1–14. https://doi.org/10.1016/j.physa.2021.126284

[6] Verrill, H. A.: *Dissecting a square into triangles*. Louisiana State University, 2004, https://web.archive.org/web/20100818142143/http://www.math.lsu.edu/~verrill/teaching/math7280/triangles.pdf.

[7] Wikipedia: Lineární uspořádání. https://cs.wikipedia.org/wiki/Line%C3%A1rn%C3%AD_uspo%C5%99%C3%A1d%C3%A1n%C3%AD

[8] https://static.scientificamerican.com/blogs/assets/Image/3adic3.png