Celá čísla p-naruby

Jakub „šnEk“ Opršal

Abstrakt. Příspěvek obsahuje základy teorie p-adických čísel, ukazuje jeden z intuitivnějších a méně formálních způsobů zavedení. Obsahuje také mnohá cvičení na osvětlení struktury p-adických celých čísel.

Prvočísla vždy hrála velkou roli v teorii čísel, už jen z toho důvodu, že když počítáme modulo prvočíslo, můžeme všemi nenulovými zbytky dělit. Na vlastnostech prvočísel také velmi stojí koncept p-adické valuace, která počítá nejvyšší mocninu prvočísla p, která dělí dané číslo. Tato myšlenka sama o sobě umí řešit mnohé diofantické rovnice.

p-adická čísla jen posouvají valuaci dále, definují pomocí ní normu a tak převádějí otázky (jako dělitelnost) dříve řešené jen algebraickou teorií čísel do analýzy a diferenciálního počtu. Dnes jsou p-adická čísla prakticky základem moderní teorie čísel, používají se například pro zlomení některých šifrovacích algoritmů postavených na eliptických křivkách či k aproximaci Riemannovy zeta funkce.

p-adická valuace a norma

Nechť p je prvočíslo. Definujeme *p-adickou valuaci* $v_p(n)$ nenulového celého čísla n jako nejvyšší exponent x takový, že $p^x \mid n$. Definujeme navíc $v_p(0) = \infty$. Ekvivalentně je-li $n = p^\alpha q$, kde $p \nmid q$, pak $v_p(n) = \alpha$.

p-adickou valuaci můžeme rozšířit i na racionální čísla, je-li $q = a/b$ zlomek (v základním tvaru), pak $v_p(q) = v_p(a) - v_p(b)$.

Cvičení. Ukažte, že v definici p-adické valuace na racionálních číslech nezáleží na tom, jestli je zlomek a/b v základním tvaru.

Tvrzení. *p-adická valuace na $\mathbb{Q}$ je zobrazení $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ a splňuje pro všechna racionální čísla a a b*

(i) $v_p(a) = \infty$, *právě když* $a = 0$,
(ii) $v_p(ab) = v_p(a) + v_p(b)$,
(iii) $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$.

Klíčová slova. p-adická čísla, valuace, celá čísla, dělitelnost, teorie čísel

Přitom v poslední situaci může ostrá nerovnost nastat pouze pro $v_p(a) = v_p(b)$.

Cvičení. Buď p prvočíslo a n přirozené. Ukažte, že platí

$$v_p\big((p^n)!\big) = 1 + p + p^2 + \cdots + p^{n-1}.$$

Cvičení. Nechť $S(n)$ značí ciferný součet čísla n v soustavě o základu p. Dokažte, že

$$v_p(n!) = \frac{n - S(n)}{p - 1}.$$

Z p-adické valuace je odvozena tzv. *p-adická norma* racionálního čísla q jako

$$|q|_p = \frac{1}{p^{v_p(q)}},$$

speciálně $|0|_p = 0$.

Tvrzení. *p-adická norma* $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}_0^+$ *je zobrazení splňující*

(i) $|q|_p \geq 0$ *a přitom* $|q|_p = 0$, *právě když* $q = 0$,
(ii) $|ab|_p = |a|_p \cdot |b|_p$,
(iii) $|a + b|_p \leq \max\{|a|_p, |b|_p\}$.

Metrika na množině (prostoru) X je binární zobrazení $\rho : X^2 \to \mathbb{R}_0^+$, které dvěma bodům přiřadí jejich vzdálenost. Po metrice chceme, aby měla nějaké docela intuitivní vlastnosti, například aby splňovala trojúhelníkovou nerovnost. Nás přesná definice moc zajímat nebude, stačit bude představa, že metrika nám dovoluje měřit vzdálenosti.

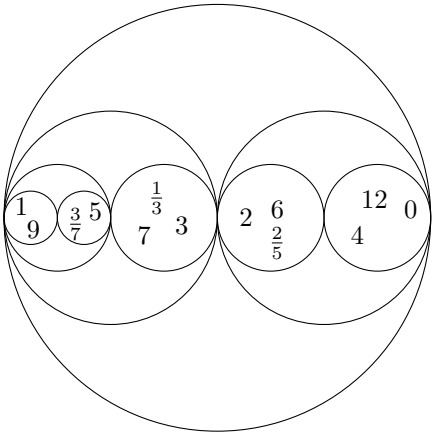
Z p-adické valuace můžeme definovat p-adickou metriku následovně

$$\rho_p(x, y) = |x - y|_p.$$

Tvrzení. *V p-adické metrice je každý trojúhelník rovnoramenný a každý kruh má střed v libovolném vnitřním bodě.*

Následující obrázek ukazuje topologii 2-adických čísel. Největší kružnice vyjadřuje kružnici s poloměrem 1, dvě menší pak mají každá poloměr $1/2$, ty ještě menší mají poloměr $1/4$ a nejmenší kružnice má poloměr $1/8$. Všechna celá čísla leží v tomto největším kruhu, spolu s některými racionálními čísly. Ostatní racionální čísla, jako

například $1/2$, $1/6$, $1/100$, leží vně tohoto největšího kruhu.



Cvičení. Buď x racionální číslo. Ukažte, že x je celé, právě když pro všechna prvočísla p platí $|x|_p \leq 1$.

Ještě se na chvíli zamyslíme, co znamená, že dvě čísla jsou od sebe vzdálena $1/p^n$ v p-adické metrice. Nechť a a b jsou dvě taková čísla, pak

$$|a-b|_p = \frac{1}{p^n} \quad \longleftrightarrow \quad v_p(a-b) = n.$$

Tedy existuje q nesoudělné s p, že $a - b = p^n q$. Stejnou úvahou můžeme odvodit, že

$$|a-b|_p \leq \frac{1}{p^n} \quad \longleftrightarrow \quad a \equiv b \pmod{p^n}.$$

Zápis racionálních čísel v p-adické soustavě a p-adická čísla

Zopakujeme si nejdříve, co znamená zápis celého čísla k v soustavě o základu p. Je to zápis ve tvaru

$$(k)_p = (a_n \cdots a_1 a_0)_p,$$

kde a_0, a_1, … , a_n jsou cifry, tj. celá čísla od 0 do $p-1$, který vyjadřuje rovnost

$$k = a_n p^n + \cdots + a_1 p + a_0.$$

Podobně chápeme i zápis s desetinnou[1] čárkou

$$(a_n \cdots a_0, a_{-1} a_{-2} \cdots a_{-m})_p = a_n p^n + \cdots + a_0 + a_{-1}\frac{1}{p} + a_{-2}\frac{1}{p^2} + \cdots + a_{-m}\frac{1}{p^m}.$$

[1] Pojmenování „desetinná čárka“ je dost zavádějící, když je to vlastně p-tinná čárka.

Normálně je zvykem racionální čísla zapisovat s nekonečným zápisem doprava, za desetinnou čárku. V p-adických číslech je tomu však naopak, tedy zajímají nás čísla s nekonečným zápisem doleva. Důvod k tomu je ten, že $1/p^\alpha$ mají čím dál větší p-adickou absolutní hodnotu, tedy například součet $1+1/p+1/p^2+\dots$ nedává smysl, protože když sčítáme postupně, tak každým dalším číslem uděláme větší a větší skok. Je to podobná situace jako kdybychom chtěli sečíst $1+p+p^2+\dots$ v reálných číslech. Na druhou stranu tento druhý součet má velmi dobrý smysl v p-adických číslech.

Množinu všech *p-adických čísel* definujeme následovně: p-adická čísla jsou množinou všech řad tvaru

$$a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + \cdots,$$

kde $a_i = 0, 1, \dots, p-1$. Tedy všech čísel, která mají v p-kové soustavě nekonečný (nebo i konečný) zápis

$$\dots a_2 a_1 a_0, a_{-1} \dots a_{-m}.$$

Všimni si, že p-adická čísla nemají, na rozdíl od reálných čísel, znaménko. To proto, že ho prostě nepotřebujeme, „záporná čísla“ umíme vyjádřit i bez něj.

Cvičení. Spočtěte $1 + 2 + 2^2 + \dots$ a $1 - 2 + 2^2 - 2^3 + \dots$ v $\mathbb{Q}_2$.

Cvičení. Máme-li dané p-adické číslo a s rozvojem

$$\dots a_1 a_0, a_{-1} \dots a_{-m},$$

jak vypadá p-adický rozvoj čísla $-a$?

Cvičení. Vyjádřete rozvoj $1/5$ v 2-adických číslech.

Cvičení. Spočtěte rozvoj $1/3!$ v $\mathbb{Q}_3$.

Můžeme velmi snadno definovat p-adickou valuaci na p-adických číslech. Důležité je, že p z indexu valuace se shoduje s prvočíslem p v p-adické soustavě. Definujeme

$$v_p(\dots a_1 a_0, a_{-1} \dots a_{-m}) = -m,$$

pro a_{-m} nenulové, tedy $v_p(a)$ udává, na které pozici je poslední nenulová cifra čísla a. Všimni si, že toto rozšiřuje p-adickou valuaci definovanou na celých číslech. Z toho už snadno rozšíříme i p-adickou normu – zadefinujeme ji stejně, jako v racionálních číslech, tj. $|a|_p = p^{-v_p(a)}$.

Můžeme také psát

$$a \equiv b \pmod{p^k}$$

pro $a, b \in \mathbb{Q}_p$ a $k \in \mathbb{N}$, což znamená, že $|a-b|_p \leq 1/p^k$. Jinými slovy že zápisy a a b se shodují zprava až do cifry na místě p^k.

Celým p-adickým číslem rozumíme každé takové číslo z, že z nemá žádné cifry za desetinnou čárkou. Jinými slovy jsou to právě taková p-adická čísla z, že $|z|_p \leq 1$.

Například každé celé číslo je p-adické celé a racionální čísla a/b taková, že $p \nmid b$ jsou p-adická celá. Kromě těchto čísel i všechna s nekonečným neperiodickým zápisem.

Cvičení. Ukažte, že je-li p prvočíslo a q libovolné celé číslo takové, že $p \nmid q$, pak $1/q \in Z_p$, a ukažte, jak lze nalézt p-adický rozvoj takových čísel.

Cvičení. Ukažte, že pro libovolné číslo $a \in \mathbb{Q}_p$, $|a|_p = 1$, existuje $b \in \mathbb{Z}_p$, že platí $ba = 1$, neboli pro taková a platí $1/a \in \mathbb{Z}_p$. Jaká je pak p-adická norma čísla $1/a$?

Cvičení. Spočtěte $\sqrt{-3}$ a $\sqrt{2}$ v $\mathbb{Q}_7$ s přesností na 4 cifry. Existuje v $\mathbb{Q}_7$ odmocnina z 3?

Cvičení. Nalezněte rozvoj $\sqrt{7}$ v $\mathbb{Q}_2$ s přesností na 5 cifer.

Cvičení. Jak poznáme, že v $\mathbb{Q}_p$ existuje odmocnina z n, kde $p \nmid n$?

Věta. (Henzelovo lemma) *Nechť $F(x) = c_0 + c_1x + \cdots + c_nx^n$ je polynom, jehož koeficienty jsou p-adická celá čísla, a buď $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1}$. Je-li $a_0 \in \mathbb{Z}_p$ takové, že $F(a_0) \equiv 0 \pmod p$ a $F'(a_0) \not\equiv 0 \pmod p$, pak existuje jednoznačné p-adické číslo a takové, že*

$$F(a) = 0 \quad \text{a} \quad a \equiv a_0 \pmod p.$$

Drsná teorie čísel

Nearchimédovskou normou na $\mathbb{Q}$ myslíme zobrazení $||\cdot||\colon \mathbb{Q} \to \mathbb{R}$ takové, které splňuje

(i) $||a|| \geq 0$ a $||a|| = 0$, právě když $a = 0$,
(ii) $||ab|| = ||a|| \cdot ||b||$,
(iii) $||a + b|| \leq \max\{||a||, ||b||\}$.

Příkladem takových norem jsou všechny p-adické normy. To, že žádné jiné příklady fakticky neexistují, nám říká Ostrovského věta.

Věta. (Ostrovski) *Pro každou nearchimédovskou normu $||\cdot||\colon \mathbb{Q} \to \mathbb{R}_0^+$ existuje prvočíslo p a reálné číslo α, že platí*

$$||q|| = |q|_p^\alpha$$

pro každé racionální $\mathbb{Q}$.

V teorii kolem valuací a norem je docela důležité následující tvrzení, které nám jinými slovy také říká, že jsme na žádnou normu nezapomněli a že se kruh do sebe uzavírá. Toto tvrzení si můžeš zkusit dokázat, je to docela jednoduché.

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

$$|q| \cdot \prod\nolimits_p |q|_p = 1,$$

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

Literatura

[K] Neal Koblitz, *p-adic Numbers, p-adic analysis, and Zeta-Functions*, Springer-Verlag, New York, 1984.

[KHŠ] R. Kučera, J. Herman, J. Šimša, *Metody řešení matematických úloh I.*, Masarykova Univerzita, Brno, 2002.