p-adická čísla

Jakub Löwit

Abstrakt. Celá čísla jsou ve skutečnosti pěkně zamotaný objekt a mnoho drsných nástrojů algebry a analýzy se na ně přímočaře použít nedá. V běžném životě si je často představujeme jako podmnožinu racionálních, resp. reálných čísel, čímž se otevírají nové možnosti jejich zkoumání. Nejde je ale vnořit do něčeho exotičtějšího, co by nám o nich prozradilo další věci? Jde!

Značení

$\mathbb{N}$	přirozená čísla
$\mathbb{N}_0$	přirozená čísla s 0
$\mathbb{Z}$	celá čísla
$\mathbb{Q}$	racionální čísla
$\mathbb{Z}_n$	zbytky modulo n
$\mathcal{O}_p$	celá p-adická čísla
$\mathbb{Q}_p$	p-adická čísla

Lepší modulení

Když se člověk dívá na přirozená čísla modulo prvočíslo p, často mu to něco prozradí. Hodně informací se tím ale ztrácí. Možným řešením je modulit vyššími a vyššími mocninami p... ale na rozlišení všech přirozených čísel to nikdy stačit nemůže. Pokud bychom však uměli přirozené číslo vymodulit všemi mocninami p najednou, už by to stačilo...

Definice. Mějme dáno pevné prvočíslo p. Dále mějme nekonečnou posloupnost $(a_i)_{i=1}^{\infty}$, kde $a_i \in \mathbb{Z}_{p^i}$. Tuto posloupnost nazveme *konzistentní*, jestliže pro každé i platí $a_i \equiv a_{i+1} \pmod{p^i}$.

Konzistence tedy znamená, že číslo a_{i+1} dává postupně zbytky $a_1, \ldots, a_{i+1}$ po dělení čísly $p, \ldots, p^{i+1}$.

Definice. Pro prvočíslo p označme $\mathcal{O}_p$ množinu všech konzistentních posloupností vzhledem k p. Na nich definujme sčítání a násobení po složkách, tj.

$$(a_i)_{i=1}^{\infty} + (b_i)_{i=1}^{\infty} = (a_i + b_i)_{i=1}^{\infty},$$

$$(a_i)_{i=1}^{\infty} \cdot (b_i)_{i=1}^{\infty} = (a_i \cdot b_i)_{i=1}^{\infty}.$$

Množinu $\mathcal{O}_p$ s těmito operacemi nazýváme *celými p-adickými čísly*.

Cvičení 1. Rozmyslete si, že součet i součin konzistentních posloupností je opět konzistentní posloupnost, tedy definice $\mathcal{O}_p$ skutečně dává smysl.

Všimněme si, že $\mathcal{O}_p$ v sobě ukrývá celá čísla $\mathbb{Z}$. Každému celému číslu totiž můžeme přiřadit posloupnost jeho zbytků modulo $p, p^2, p^3, \ldots$, což samozřejmě dává konzistentní posloupnost. Sčítání a násobení takových posloupností skutečně odpovídá sčítání a násobení přirozených čísel.

Tvrzení. (Obor integrity) *Součin libovolných dvou nenulových prvků $\mathcal{O}_p$ je opět nenulový.*

Důkaz. Mějme dvě taková nenulová $a, b \in \mathcal{O}_p$. To znamená, že pro nějaká $i, j \in \mathbb{N}_0$ platí $a_i \neq 0, b_j \neq 0$. Z konzistence vyplývá, že každý vyšší člen posloupnosti $(a_i)_{i=1}^{\infty}$ je dělitelný p^i, ale již nemůže být dělitelný p^{i+1}. Podobně každý vyšší člen posloupnosti $(b_i)_{i=1}^{\infty}$ je dělitelný p^j, ale nemůže být dělitelný p^{j+1}. Součin členů $a_{i+j+1} \cdot b_{i+j+1}$ proto není dělitelný p^{i+j+1}, tedy číslo $a + b$ má na této pozici nenulový koeficient a proto je nenulové.

Prvky $\mathcal{O}_p$ si ale můžeme představit i jiným způsobem jako *mocninné řady*, tj. jako „nekonečné“ zápisy čísel v soustavě o základu p. Sčítání a násobení takových řad pak ale nestačí provést „po členech“, je potřeba „převádět přes desítky“ a roznásobovat „nekonečné závorky“ (tj. provádět ho jako sčítání a násobení „pod sebou jako ve škole“).

Tvrzení. (Mocninné řady) *Prvky $\mathcal{O}_p$ si lze představit jako mocninné řady $\sum_{i=0}^{\infty} d_i p^i$, pro $d_i \in \mathbb{Z}_p$, které se sčítají a násobí „jako ve škole“.*

Důkaz. K jednoznačnému zakódovaní konzistentní posloupnosti nám stačí nekonečná posloupnost $(d_i)_{i=1}^{\infty}$, kde $d_i \in \mathbb{Z}_p$. Pokud totiž známe prvních i členů, máme přesně p možností na volbu členu a_{i+1}, při kterých bude výsledná posloupnost konzistentní – a_{i+1} je zbytek modulo p^{i+1}, přitom už známe jeho zbytek modulo p^i. Mocninné řadě $\sum_{i=0}^{\infty} d_i p^i$ naopak v této korespondenci odpovídá konzistentní posloupnost jejích částečných součtů. Že sčítání a násobení funguje správně, je dost jasné.

Pro $a \in \mathbb{Z} \subset \mathcal{O}_p$ jsou koeficienty d_i od nějakého členu dál všechny nulové a daná řada odpovídá dobře známému zápisu přirozených čísel v soustavě o základu p. Každé celé p-adické číslo má také jednoznačně určený zápis a každý zápis definuje nějaké celé p-adické číslo.

Cvičení 2. Pokud by p nebylo prvočíslo, musel by být pořád součin dvou nenulových prvků $\mathcal{O}_p$ nenulový?

Henselovo lemma

Dostáváme se k tvrzení, které z velké části motivovalo zkoumání p-adických čísel. Rádi bychom totiž uměli řešit polynomiální rovnice modulo mocnina prvočísla p. Pokud se nám povede vyřešit takovou rovnici nad $\mathcal{O}_p$, vyřešíme ji tím vlastně modulo

všechny mocniny prvočísla p najednou. Henselovo lemma (a jeho různé varianty) mluví právě o takovém řešení.

Definice. Mějme polynom $f = \sum_{i=0}^{n} a_i x^i$ v proměnné x. Jeho *derivací* rozumíme polynom $f' = \sum_{i=0}^{n} i \cdot a_i x^{i-1}$.

Pro reálné polynomy naše definice odpovídá skutečnému derivování, to nám ale může být jedno. Derivace je pro nás prostě operace, která z jednoho polynomu vyrobí jiný. Pojďme si nyní formulovat základní verzi Henselova lemmatu.

Tvrzení. (Henselovo lemma) *Ať f je celočíselný polynom, $m \in \mathbb{Z}$. Je-li $f(m) \equiv 0 \pmod p$ a zároveň $f'(m) \not\equiv 0 \pmod p$, potom existuje jednoznačně určené $a \in \mathcal{O}_p$ splňující $f(a) = 0$ takové, že $a \equiv m \pmod p$.*

Důkaz. Důkaz provedeme indukcí, tj. postupně zkonstruujeme členy konzistentní posloupnosti odpovídající číslu a. Budeme chtít, aby pro každé i platilo $f(a_i) \equiv 0 \pmod p$, $f'(a_i) \not\equiv 0 \pmod p$. Volme $a_1 = m$.

Máme-li už a_i, uvažme čísla $a_i, a_i + p^i, a_i + 2p^i, \dots, a_i + (p-1)p^i$. Vezměme dvě sousední z nich a označme je $x < y$. Protože $y - x = p^i$, platí kongruence $f(y) - f(x) \equiv f'(a_i) \cdot p^i \pmod{p^{i+1}}$. Díky podmínce $f'(a_i) \not\equiv 0 \pmod p$ pak kongruenci $f(z) \equiv 0 \pmod{p^{i+1}}$ splňuje právě jedno z uvažovaných p čísel. Toto číslo označme a_{i+1}. Z jeho tvaru vidíme, že $a_i \equiv a_{i+1} \pmod{p^i}$. Potom také $f'(a_{i+1}) \equiv f'(a_1) \not\equiv 0 \pmod p$. Tím je indukční krok dokončen. Zároveň je z postupu jasné, že číslo a_{i+1} bylo určené jednoznačně.

Cvičení 3. Rozhodněte, zda v $\mathcal{O}_7$ existuje $\sqrt{3}$.

Cvičení 4. Rozhodněte, zda v $\mathcal{O}_7$ existuje $\sqrt{-3}$.

Cvičení 5. Existuje přirozené číslo, jehož třetí mocnina dává po dělení 5^{2018} zbytek 2?

Cvičení 6. Existuje přirozené číslo, jehož sedmá mocnina dává po dělení 30^{2018} zbytek 31?

Cvičení 7. Ať $p \geq 3$ je prvočíslo a přirozené číslo n dává náhodný nenulový zbytek po dělení p. Jaká je šance, že v $\mathcal{O}_p$ existuje $\sqrt{n}$?

„Olympiádní" úlohy

Pojďme se nyní podívat na několik celkem těžkých olympiádních úloh, kde lze výhodně použít některé, právě nabyté, znalosti. Z teorie p-adických čísel pro nás bude stěžejní Henselovo lemma. Z elementární teorie čísel je dobré znát Čínskou zbytkovou větu a Bezoutovu větu. K duhu nám také přijde následující Schurovo lemma:

Lemma 8. (Schurovo) *Ať f je celočíselný nekonstantní polynom. Potom existuje nekonečně mnoho prvočísel p, která dělí nějaké nenulové číslo z množiny $\{f(1), f(2), f(3), \dots\}$.*

Úloha 9. Ať f je nekonstantní celočíselný polynom. Ukažte, že pro libovolné $k \in \mathbb{N}$ existuje nekonečně mnoho prvočísel p takových, že p^k dělí nějaké nenulové číslo z množiny $\{f(1), f(2), f(3), \dots\}$.

Úloha 10. Najděte všechny celočíselné polynomy f, které pro všechna $m, n \in \mathbb{N}$ splňují implikaci $f(m)|f(n) \implies m|n$.

(Irán TST)

Úloha 11. Existuje celočíselný polynom, který nemá žádný racionální kořen, ale má kořen modulo libovolné přirozené číslo?

(Kömal)

Valuace

Mějme přirozené číslo n. Jeho p–valuací myslíme nejvyšší mocninu prvočísla p, která ho dělí. Pro celá p-adická čísla lze tento koncept rozumně dodefinovat, což se vyplatí.

Definice. Prvek $u \in O_p$ nazveme *jednotkou*, jestliže existuje nějaké $v \in O_p$ splňující $uv = 1$.

Všimněme si, že součin jednotek je vždy jednotka.

Tvrzení. (Popis jednotek) *Prvek $a = (a_i)_{i=1}^{\infty} \in O_p$ je jednotka právě tehdy, když $a_1 \neq 0$ v $\mathbb{Z}_p$.*

Důkaz. Pokud je a_1 rovno nule, žádným přenásobením z něj 1 vyrobit nelze. Pokud je naopak a_1 nenulové, žádné a_i není dělitelné p, tedy má inverz modulo p^i. Seřazení těchto inverzů do posloupnosti dá konzistentní posloupnost, čímž jsme hotovi.

Tvrzení. (Rozklad na mocninu a jednotku) *Každý nenulový prvek $a \in \mathcal{O}_p$ lze jednoznačně zapsat ve tvaru $a = p^k u$, pro $k \in \mathbb{N}_0$ a jednotku $u \in O_p$.*

Důkaz. Pro $a \in \mathcal{O}_p$ označme $k+1$ index prvního nenulového prvku příslušné konzistentní posloupnosti. Potom platí $a = \sum_{i=0}^{\infty} d_i p^i = p^k \cdot \sum_{i=k}^{\infty} d_i p^{i-k}$, což je hledaný rozklad.

Tento rozklad je navíc skutečně jednoznačný – jsou-li $p^k u$, $p^l v$ dva takové rozklady, pro přirozená $k \geq l$, můžeme upravovat $p^k u = p^l v$ na $p^l \cdot (p^{k-l} u - v) = 0$. Přitom $p^l \neq 0$ a součin dvou nenulových prvků je vždy nenulový – dostáváme tedy $p^{k-l} u = v$. Protože jsou u, v jednotky, lze rovnost přepsat na $p^{k-l} w = 1$ pro nějakou jednotku w. Tím pádem je ale p^{k-l} také jednotka, takže dle předešlého tvrzení dostáváme $k = l$; dosazením do rovnosti $p^{k-l} u = v$ pak dostáváme také $u = v$.

Předchozí tvrzení nám umožňuje definovat p-adickou valuaci, která rozšiřuje běžnou valuaci na celých číslech.

Definice. Pro $0 \neq a \in \mathcal{O}_p$ definujeme *p-adickou valuaci* $v_p(a)$ jako to jednoznačně určené $k \in \mathbb{N}_0$, pro které lze psát $a = p^k u$ pro nějakou jednotku u. Navíc bereme $v_p(0) = \infty$.

Je vidět, že na celých číslech se tato valuace chová jako běžná prvočíselná valuace, tj. $v_p(a)$ odpovídá nejvyššímu exponentu k, pro který ještě p^k dělí a. Hned si

všimněme dvou základních vlastností valuace, které platí pro libovolná celá p-adická čísla.

Tvrzení. (Vlastnosti valuace) *Pro libovolná $a, b \in \mathcal{O}_p$ platí*

(1) $v_p(a \cdot b) = v_p(a) + v_p(b)$,
(2) $v_p(a + b) \geq min(v_p(a), v_p(b))$, *přičemž pokud $v_p(a) \neq v_p(b)$, tak už nutně nastává rovnost.*

Důkaz. První vlastnost je jasná, $p^k u \cdot p^l v = p^{k+l} uv$, kde uv je jednotka. Nerovnost z druhé vlastnosti je také jednoduchá: pokud jsou konzistentní posloupnosti příslušné číslům a, b na nějaké pozici obě nulové, je na této pozici nulová i posloupnost příslušející jejich součtu. Pokud je navíc jedna ze sčítaných posloupností na nějaké pozici nulová a druhá nenulová, jejich součet je na této pozici opět nenulový.

S pomocí valuace není problém mluvit o kongruenci modulo p^i na celých p-adických číslech. Dvě čísla budou kongruentní, pokud má jejich rozdíl dostatečně velkou valuaci. Na celých číslech se definice opět shoduje s tou dobře známou.

Definice. Pro $a, b \in \mathcal{O}_p$ budeme psát $a \equiv b \pmod{p^i}$ právě když $v_p(a - b) \geq i$.

Zlomky

Racionální čísla vzniknou z celých tak, že si dovolíme dělit nenulovými prvky. Podobně můžeme z celých p-adických čísel $\mathcal{O}_p$ vyrobit „racionální“ p-adická čísla $\mathbb{Q}_p$. Těm se pro jednoduchost říká prostě *p-adická čísla*.

Definice. Pro prvočíslo p definujeme *p-adická čísla* $\mathbb{Q}_p$ jako všechny zlomky tvaru $\frac{a}{b}$ pro $a, b \in \mathcal{O}_p$, kde navíc $b \neq 0$. Dva takové zlomky $\frac{a}{b}$, $\frac{c}{d}$ považujeme ze stejné právě když $ad = cb$.

S trochou práce není těžké ukázat, že tato definice $\mathbb{Q}_p$ skutečně dává smysl a že pro počítání s p-adickými čísly platí v zásadě stejná „pravidla“ jako pro počítání s racionálními. Důležitou ingrediencí je (nám už dobře známý) fakt, že dva nenulové prvky $a, b \in \mathcal{O}_p$ se opět vynásobí na nenulový prvek. Pojďme si ale nyní právě vzniklé $\mathbb{Q}_p$ prohlédnout podrobněji.

Tvrzení. (Mocninné řady v $\mathbb{Q}_p$) *Každé $a \in \mathbb{Q}_p$ lze jednoznačně vyjádřit ve tvaru $p^k u$, pro $k \in \mathbb{Z}$ a jednotku $u \in \mathcal{O}_p$.*

Důkaz. Číslo $\frac{a}{b}$ lze přepsat do tvaru $\frac{p^k u}{p^l v}$ pro $k, l \in \mathbb{N}$, u, v jednotky. Pronásobením čitatele i jmenovatele číslem inverzním k v s označením $w = uv$ dostáváme $\frac{p^k w}{p^l} = p^{k-l} w$.

Celkem tedy můžeme popsat $\mathbb{Q}_p$ jako všechny mocninné řady od $-\infty$ do ∞ s koeficienty ze $\mathbb{Z}_p$, které mají od nějakého indexu níže všechny koeficienty nulové. Naše p-adická čísla si tedy lze představovat jako „čísla s nekonečným zápisem doleva“. (Na rozdíl od běžných racionálních čísel $\mathbb{Q}$, která umíme zapisovat v soustavě o základu

p, až na znaménko, jako ty řady od $-\infty$ do ∞ s koeficienty ze $\mathbb{Z}_p$, které mají od nějakého indexu výše všechny koeficienty nulové.)

Definice. Pro $a, b \in \mathcal{O}_p$ definujme $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.

Přitom je zřejmé, že tato definice nezáleží na konkrétním zlomku, kterým dané p-adické číslo reprezentujeme. Na celých (a tedy i na racionálních) číslech se právě definovaná valuace shoduje s tou běžnou. Valuace na $\mathbb{Q}_p$ navíc stále splňuje vlastnosti (1) a (2), které má na $\mathcal{O}_p$. Stejně jako dříve můžeme definovat kongruenci modulo p:

Definice. Pro $a, b \in \mathbb{Q}_p$ budeme psát $a \equiv b \pmod{p^i}$ právě když $v_p(a-b) \geq i$.

Raději si nyní pojďme na vlastní kůži vyzkoušet, jak se p-adická čísla chovají. Mocninnou řadu příslušnou některému p-adickému číslu si přitom skutečně chceme představovat jako jakýsi jeho „zápis v soustavě o základu p“. Ten se často pro přehlednost zapisuje zleva doprava, tedy naopak, než jsme zvyklí – číslu $6 = 2 + 2^2$ bychom tak přiřadili zápis 011, číslu $\frac{13}{2} = 6 + \frac{1}{2}$ zápis $1,011$ atd.

Cvičení 12. Rozhodněte, zda rovnice $x^2 = p$ má řešení v $\mathbb{Q}_p$.

Cvičení 13. Je-li $a = d_j p^j + d_{j+1} p^{j+1} + d_{j+2} p^{j+2} + \dots$ mocninná řada příslušná číslu $a \in \mathbb{Q}_p$, potom číslo $-a$ odpovídá mocninné řadě:

$$(p - d_j)p^j + (p - 1 - d_{j+1})p^{j+1} + (p - 1 - d_{j+2})p^{j+2} + \dots$$

Cvičení 14. Upravte číslo $1 + 2 + 2^2 + 2^3 + \dots$ v $\mathbb{Q}_2$ na co nejhezčí tvar.

Cvičení 15. Vyjádřete $\frac{1}{5}$ v $\mathbb{Q}_2$ jako mocninnou řadu.

Cvičení 16. Vyjádřete $\frac{1}{6}$ v $\mathbb{Q}_3$ jako mocninnou řadu.

Cvičení 17. Dokažte, že v $\mathbb{Q}_p$ platí vzorec pro součet geometrické řady:

$$\frac{1}{1 - p^k} = 1 + p^k + p^{2k} + \dots$$

Všimněme si, jak pěkně předchozích pár cvičení vyšlo. To není náhoda – existuje totiž elegantní charakterizace skutečných racionálních čísel v rámci těch p-adických. K obecnému hledání rozvojů p-adických čísel nám velmi pomůže znalost Malé Fermatovy věty a vzorec pro součet geometrické řady.

Tvrzení. ($\mathbb{Q}$ uvnitř $\mathbb{Q}_p$) *Mějme číslo $a \in \mathbb{Q}_p$. Potom $a \in \mathbb{Q}$ právě tehdy, když je jemu příslušná mocninná řada od jistého členu periodická.*

Dále umíme rozumně popsat ta racionální čísla s nulovou valuací, jejichž řada je periodická hned od začátku (tj. od prvního nenulového členu, který se nachází na pozici jednotek).

Tvrzení. (Čistě periodické řady) *Ať $a \in \mathbb{Q}$ splňuje $v_p(a) = 0$. Potom je řada $a = d_0 + d_1 p + d_2 p^2 + \dots$ čistě periodická právě když $-1 \leq a < 0$.*

Nakonec této části si ukážeme jednu úlohu ilustrující použití počítání v $\mathbb{Q}_p$ na běžnou úlohu o dělitelnosti.

Úloha 18. Ať $p > 5$ je prvočíslo. Ukažte, že p^4 dělí čitatel čísla

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

Vzdálenost

Abychom na problémy z teorie čísel uměli efektivně vypustit monstra matematické analýzy, potřebujeme jenom jediné – definovat vzdálenost mezi prvky $\mathbb{Q}_p$. K tomu nám poslouží dříve definovaná valuace.

Definice. *Normou* p-adického čísla $0 \neq a \in \mathbb{Q}_p$ myslíme číslo $|a|_p = p^{-v_p(a)}$. Speciálně klademe $|0|_p = 0$.

Z vlastností valuace hned vyplývají analogické vlastnosti normy.

Tvrzení. (Vlastnosti normy)

(1) $|a|_p \geq 0$, *přičemž rovnost nastává pouze pro* $a = 0$,
(2) $|(a \cdot b)|_p = |a|_p \cdot |b|_p$,
(3) $|(a+b)|_p \leq max(|a|_p, |b|_p)$, *přičemž pro* $|a|_p \neq |b|_p$ *už nutně nastává rovnost.*

Definice. Vzdálenost dvou p-adických čísel $a, b \in \mathbb{Q}_p$ definujeme jako normu jejich rozdílu, tedy jako číslo $|a-b|_p$.

Speciálně si všimněme, že vzdálenost každých dvou různých čísel je kladná. Navíc je díky třetímu bodu předchozího tvrzení pro libovolná $a, b, c \in \mathbb{Q}_p$ splněna trojúhelníková nerovnost $|a-c|_p \leq |a-b|_p + |b-c|_p$.

Tato vzdálenost funguje na první pohled trochu neintuitivně. Dvě čísla jsou k sobě tím blíže, čím větší mocnina prvočísla p dělí jejich rozdíl. Třeba čísla 1000 a 2000 jsou v 2-adické vzdálenosti mnohem blíž, než čísla 1 a 2.

Dovolme si nyní krátkou analýznickou odbočku. Definujme si dva základní pojmy, které lze zavést s použitím pojmu vzdálenosti – limitu posloupnosti a součet řady. Následně se můžeme chvíli kochat, jak hezky se tyto pojmy na p-adických číslech chovají.

Definice. Nekonečná posloupnost čísel $(q_i)_{i=0}^{\infty} \in \mathbb{Q}_p$ *konverguje* k číslu $q \in \mathbb{Q}_p$, jestliže pro libovolně malé $\varepsilon > 0$ už od nějakého indexu dál platí $|q - q_i| < \varepsilon$. Číslo q nazýváme *limitou* této posloupnosti.

Definice. Nekonečná řada čísel $\sum_{i=1}^{\infty} r_i$, kde $r_i \in \mathbb{Q}_p$, *konverguje* k číslu $r \in \mathbb{Q}_p$, jestliže k tomuto číslu konverguje nekonečná posloupnost $q_m = \sum_{i=0}^{m}$. Číslo r nazýváme *součtem* této řady.

Vzdálenost na p-adických číslech má následující hezké vlastnosti, které vzdálenost na běžných reálných číslech obecně nemá.

Tvrzení. (Konvergence řad) *Řada $\sum_{i=0}^{\infty} r_i$, kde $r_i \in \mathbb{Q}_p$, konverguje k nějakému $r \in \mathbb{Q}_p$ právě tehdy, když posloupnost čísel r_i konverguje k 0.*

Tvrzení. (Přerovnávání řad) *Součet konvergentní řady čísel $r_i \in \mathbb{Q}_p$ nezávisí na jejich pořadí.*

Tvrzení. (Kompaktnost $\mathcal{O}_p$) *Každá posloupnost $(q_i)_{i=0}^{\infty}$ prvků $\mathcal{O}_p$ obsahuje podposloupnost, která konverguje k nějakému $q \in \mathcal{O}_p$.*

Z předchozího tvrzení mimo jiné vyplývá, že pokud posloupnost prvků $\mathcal{O}_p$ konverguje v rámci $\mathbb{Q}_p$, konverguje k nějakému prvku $\mathcal{O}_p$.

Tvrzení. (Návrat mocninných řad) *Pro každé $r \in \mathcal{O}_p$ existují jednoznačně určená čísla $r_i \in \{0, 1, \ldots, p-1\}$ taková, že $\sum_{i=0}^{\infty} r_i p^i$ konverguje k r.*

To už jsme tu jednou měli – hned na začátku jsme si uvědomili, že celá p-adická čísla odpovídají takovýmto řadám. Tenkrát jsme ale vůbec nepřemýšleli o nějaké konvergenci – prostě se nám tak jednotlivá čísla hodilo zapisovat. Oba přístupy naštěstí splývají.

Analogický výsledek platí obecněji pro čísla $r \in \mathbb{Q}_p$. Pro každé takové r existuje jednoznačně určené číslo $m \in \mathbb{Z}$ a čísla $r_i \in \{0, 1, \ldots, p-1\}$ taková, že $r_m \neq 0$ a $\sum_{i=m}^{\infty} r_i p^i$ konverguje k r.

Nyní si ale raději pojďme procvičit, jak se pracuje s vzdálenostmi mezi p-adickými čísly. Tato vzdálenost je totiž na první pohled celkem divná.

Cvičení 19. Každá trojice různých čísel $a, b, c \in \mathbb{Q}_p$ určuje rovnoramenný trojúhelník.

Cvičení 20. Každý kruh v $\mathbb{Q}_p$ má střed v libovolném svém vnitřním bodě.

Cvičení 21. Spočtěte součet řady $1 - 2 + 2^2 - 2^3 + \ldots$ v $\mathbb{Q}_2$.

Dovolme si ještě předvést jeden zdánlivě nesouvisející problém, který několik vysokoškolských triků společně se znalostí p-adických čísel snadno vyřeší.

Definice. Pro $r \in \mathbb{Q}$, $k \in \mathbb{N}$ definujeme binomický koeficient

$$\binom{r}{k} = \frac{r \cdot (r-1) \cdots (r-k+1)}{1 \cdot 2 \cdots k}.$$

Úloha 22. Ukažte, že každé prvočíslo, které dělí jmenovatel čísla $\binom{r}{k}$, musí dělit i jmenovatel čísla r.

Úloha 23. Každé prvočíslo, které dělí jmenovatel čísla r, dělí i jmenovatel čísla $\binom{r}{k}$.

Drsnější verze Henselova lemmatu

Zformulujeme si nyní Henselovo lemma v mírně silnější podobě a jinými slovy. Oproti předchozímu zde dovolujeme, aby koeficienty zadaného polynomu byla libovolná čísla z $\mathcal{O}_p$, jinak je tvrzení do puntíku stejné.

Tvrzení. (Henselovo lemma) *Ať f je polynom nad $\mathcal{O}_p$, $a \in \mathcal{O}_p$ splňující $f(a) \equiv 0 \pmod{p}$, $f'(a) \not\equiv 0 \pmod{p}$. Potom existuje právě jedno $b \in \mathcal{O}_p$ splňující $f(b) = 0$, $a - b \equiv 0 \pmod{p}$.*

Poznamenejme ještě, že z definice kongruence a normy lze lemma ekvivalentně zformulovat takto: „Ať f je polynom nad $\mathcal{O}_p$, $a \in \mathcal{O}_p$ splňující $|f(a)|_p < 1$, $|f'(a)|_p = 1$. Potom existuje právě jedno $b \in \mathcal{O}_p$ splňující $f(b) = 0$, $|a - b|_p < 1$.“ Dříve než půjdeme dál zobecňovat toto tvrzení, podíváme se, co umí už teď.

Cvičení 24. Ať $n \in \mathbb{N}$ a p je prvočíslo, které nedělí n. Dále ať $u \in \mathcal{O}_p$ splňuje $u \equiv 1 \pmod{p}$. Ukažte, že u je n-tá mocnina nějakého prvku z $\mathcal{O}_p$.

Cvičení 25. Je dáno prvočíslo $p \geq 3$ a jednotka $u \in \mathcal{O}_p$. Dokažte, že u je čtverec právě tehdy, když je první složka jeho konzistentní posloupnosti u_1 čtverec modulo p.

Cvičení 26. Mějme prvočíslo p. Ukažte, že se polynom $x^p - x$ rozkládá na lineární činitele v $\mathbb{Q}_p$.

Definice. Číslo $a \in \mathcal{O}_p$ nazveme odmocninou z jedné, jestliže existuje $n \in \mathbb{N}$, pro které je $a^n = 1$.

V racionálních číslech jsou tedy odmocniny z jedné dvě, 1 a -1. Naproti tomu v komplexních číslech už jich je nekonečně. Kolik jich bude v našem $\mathbb{Q}_p$?

Tvrzení. (Odmocniny z jedné) *Pro prvočíslo $p \geq 3$ existuje v $\mathbb{Q}_p$ právě $p - 1$ různých odmocnin z jedné. V $\mathbb{Q}_2$ existují právě dvě odmocniny z jedné.*

Nyní si zformulujeme slíbenou drsnější verzi Henselova lemmatu. Podmínka na $f'(a)$ je v ní mnohem slabší – i když má polynom f v nějakém čísle „násobný kořen“, pořád se něco dovíme.

Tvrzení. (drsnější Henselovo lemma) *Ať f je polynom nad $\mathcal{O}_p$, $a \in \mathcal{O}_p$ splňující*

$$|f(a)|p < |f'(a)|_p^2.$$

Potom existuje jednoznačně určené $b \in \mathcal{O}_p$ splňující $|a - b|_p < |f'(a)|_p$. Dokonce platí

(1) $|a - b|_p = |\frac{f(a)}{f'(a)}|_p < |f'(a)|_p$,
(2) $|f(a)|_p = |f'(a)|_p$.

Něco na závěr

Teorie p-adických čísel je samozřejmě mnohem hlubší a bohatší, my jsme do ní jen rychle nahlédli. Důležitým výsledkem je například známá Ostrowského věta, která říká, že běžná vzdálenost a p-adické vzdálenosti jsou v podstatě jediné rozumné vzdálenosti na racionálních číslech.

Pojem p-adické vzdálenosti jde jednoznačně rozšiřovat dokonce ještě dál. Krásným důsledkem související teorie je například velmi překvapivá Monskyho věta: „Čtverec

nelze rozřezat na lichý počet trojúhelníků se stejným obsahem.“ Pro sudé počty trojúhelníků je konstrukce jednoduchá, pro liché ale neexistuje – a není znám žádný elementárnější důkaz!

Návody

1. Přímočaré.

2. Ne, stačí rozložit p na netriviální součin dvou nesoudělných čísel a z nich induktivně vyrobit dvě nenulové řady s nulovým součinem.

3. Ne, tato rovnice nemá řešení ani modulo 7.

4. Ano, rovnice $x^2 + 3 = 0$ má modulo 7 řešení například $x = 2$, které splňuje předpoklady Henselova lemmatu.

5. Ano, polynom $f = x^3 - 2$ splňuje $f(3) \equiv 0 \pmod 5$ a $f'(3) \equiv 2 \not\equiv 0 \pmod 5$.

6. Ano, použijte Henselovo lemma zvlášť pro $p = 2, 3, 5$ a zakončete Čínskou zbytkovou větou.

7. Přesně $\frac{1}{2}$. Jde jen o to, zda je n kvadratický zbytek modulo p.

8. Pro $f(0) = 1$ to není těžké, případ $f(0) = 0$ se dá zvesela ignorovat. Je-li $f(0) = m \neq 0$, uvažte polynom $g(x) = \frac{f(0) \cdot x}{f(0)}$.

9. Na Schurovo lemma použijte Henselovo lemma. Aby šlo použít, je potřeba vzít f ireducibilní nad $\mathbb{Z}$ a dostatečně velká prvočísla p.

10. Fungují právě polynomy tvaru ax^k pro $a \in \mathbb{Z}$, $k \in \mathbb{N}_0$. Použijte předchozí úlohu.

11. Volte $f = (x^2 + 3)(x^2 - 13)(x^2 + 39)$. Z Čínské zbytkové věty stačí tvrzení dokazovat pro mocniny prvočísel, z Henselova lemmatu v podstatě jen pro prvočísla.

12. Nemá. Levá strana má sudou valuaci, zatímco valuace pravé strany je 1.

13. Koeficienty výsledné řady jsou čísla ze $\mathbb{Z}_p$ a obě řady se sečtou na 0.

14. Vyjde -1.

15. Začněte zápisem čísla 5 a postupně hledejte inverz; nakonec vyjde $1 + 2^2 + 2^3 + 2^6 + 2^7 + \dots$, tj. číslo s periodickým zápisem $1\overline{1100}$.

16. Násobení mocninou trojky jenom posouvá řády, vyjde $2 \cdot 3^{-1} + 1 + 3 + 3^2 + \dots$, tj. číslo s periodickým zápisem $2, \overline{1}$.

17. Součin závorek $(1 + (p-1)p^k + (p-1)p^{2k} + \dots) \cdot (1 + p^k + p^{2k} + \dots)$ je 1.

18. Upravujte, využijte p-adické identity $\frac{1}{k(p-k)} = -\frac{1}{k^2}\left(1 + \frac{p}{k} + \frac{p}{k^2} + \dots\right)$.

19. Zkoumejte čísla $(a - b)$, $(b - c)$, $(c - a)$. Mohou se tři čísla s různými normami sečíst na 0?

20. K číslu $a \in \mathbb{Q}_p$ jsou blízko ta čísla, jejichž mocninné řady mají od jisté pozice ty samé koeficienty.

21. Součty geometrických řad, vyjde $\frac{1}{3}$.

22. Chceme ukázat, že $|r|_p \leq 1$ implikuje $\left|\binom{r}{k}\right|_p \leq 1$. K číslu r jde dokonvergovat čísly z $\mathcal{O}_p$, funkce $\binom{x}{k}$ je spojitá funkce $\mathbb{Q}_p \to \mathbb{Q}_p$.

23. Dokazujte, že $|r|_p > 1$ implikuje $\left|\binom{r}{k}\right|_p > 1$.

24. Henselovo lemma na polynom $f = x^n - u$ s počáteční hodnotou 1.

25. Vezměte polynom $f = x^2 - u$, začněte dosazením u_1. Druhá implikace je jasná.

26. Použijte Malou Fermatovu větu.

Zdroje

[1] Titu Andreescu, Gabriel Dospinescu: *Problems from the Book*
[2] Titu Andreescu, Gabriel Dospinescu: *Straight from the Book*
[3] Keith Conrad: *Hensel's Lemma*
[4] Keith Conrad: *The p-adic expansion of Rational Numbers*
[5] Keith Conrad: *Binomial Coefficients and p-adic Limits*
[6] Jakub Opršal: *Celá čísla p-naruby*, PraSe
[7] Radovan Švarc: *Monskyho věta*, PraSe

Náboj

Úloha. Může být hodnota polynomu $f(x) = x^{11} + x^2 + 11x + 3$ v nějakém přirozeném čísle dělitelná 11^{2018}?

Řešení. S pomocí Malé Fermatovy věty máme $f(5) \equiv 0 \pmod{11}$, přitom $f'(5) \not\equiv 0 \pmod{11}$. Z Henselova lemmatu tedy takové číslo existuje.

Úloha. Může být hodnota polynomu $f(x) = x^{11} + x^2 + 11x + 1$ v nějakém přirozeném čísle dělitelná 11^{2018}?

Řešení. Ne, tento polynom nemá kořen dokonce ani modulo 11 (neboť polynom $x^{11} + x^2 + 11x \equiv x(x+1) \pmod{11}$ dává pouze zbytky 0, 1 2, 6, 8, 9).

Úloha. Kolik existuje přirozených čísel n menších než 100^{100}, že $10^{10} \mid n^5 + n^2 + 4$?

Řešení. Označme $f(n) = n^5 + n^2 + 4$. Platí $f(1) \equiv 0 \pmod{2}$ a $f'(1) \equiv 1 \pmod{2}$, z Henselova lemmatu proto existuje právě jeden (nutně nenlový) kořen f modulo 2^{10}. Obdobně $f(2) \equiv 0 \pmod{5}$ a $f'(1) \equiv 4 \pmod{5}$, tedy existuje právě jeden (nenulový) kořen modulo 5^{10}. Z čínské zbytkové věty pak existuje jednoznačný kořen modulo 10^{10}. Vyjde proto $\frac{100^{100}}{10^{10}} = 10^{190}$.

Úloha. Rozepište $\frac{1}{5}$ v $\mathcal{O}_3$ jako mocninnou řadu. *(Zlomkem $\frac{1}{5}$ myslíme takový prvek, který splňuje rovnost $\frac{1}{5} \cdot 5 = 1$)*

Řešení. V soustavě o základu 3 rozepíšeme $5 = 2 + 3$. Postupně dopočítáme

$$\frac{1}{5} = 2 + 2 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 + 0 \cdot 3^5 + 1 \cdot 3^3 + 2 \cdot 3^4 + 0 \cdot 3^5 + \ldots,$$

tj. koeficienty tvoří periodickou posloupnost $2\overline{201}$. (Obecněji na to jde trikově přijít pomocí Malé Fermatovy věty a sčítání geometrických řad v $\mathcal{O}_p$.)