BRněnský KOrespondenční Seminář

XXIX. ročník
2022/2023

Studijní text ke 3. sérii

p-VALUACE

autor: *Adéla Heroudková*

Jedním ze zásadních a základních výsledků v teorii čísel je základní věta aritmetiky, která říká, že každé přirozené číslo můžeme jednoznačně rozložit na součin prvočísel. Z tohoto rozkladu vychází i pojem p-valuace, kterému je věnována tato série. Jedná se o velice užitečný koncept, který můžete využít nejen při řešení úloh z Brkosu a matematické olympiády, ale jsou pomocí něj také zavedena p-adická čísla, která byla sice objevena teprve na začátku 20. století, ale dnes již patří k jedněm z nejdůležitějších částí moderní teorie čísel. Jedná se o množinu čísel, na které pomocí p-valuace umíme zavést něco jako „vzdálenost" a tím získáme prostor se spoustou zajímavých vlastností. Díky těmto vlastnostem se ukázalo, že p-adická čísla můžeme využít dokonce i ve fyzice, biologii a geologii. Máme za sebou reklamu, tak vzhůru k definici!

Definice 1. Máme-li $z \in \mathbb{Z}$ a prvočíslo p, pak p-valuací čísla z rozumíme nejvyšší nezáporné celé k takové, že platí $p^k | z$. Toto k značíme $v_p(z)$.

Ekvivalentně by p-valuace také šly definovat jako exponent v rozkladu na prvočísla. Tedy pokud $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ je rozklad přirozeného čísla n na součin mocnin různých prvočísel, tak pak $v_{p_i}(n) = \alpha_i$. Rozmyslete si ekvivalenci obou definic!

Pro zájemce dodáváme, že p-valuaci můžeme rozšířit na racionální čísla následovně: jestliže $x = \frac{a}{b} \in \mathbb{Q} \setminus \{0\}$, $a, b \in \mathbb{Z}$, potom $v_p(x) = v_p(a) - v_p(b)$. My však budeme uvažovat p-valuace pouze pro celá čísla. Pro nulu zavedeme $v_p(0) = \infty$.

Příklad. Pro ujasnění si uveďme příklad:

- $9 = 3^2 \implies v_3(9) = 2$,
- $-54 = -2^1 3^3 \implies v_2(-54) = 1, v_3(-54) = 3$ a $v_p(-54) = 0$ pro všechna ostatní p,
- $3 = 3^1 11^0$, $22 = 2^1 11^1 \implies v_{11}(\frac{3}{22}) = 0 - 1 = -1$.

Pojďme se podívat na nějaké užitečné vlastnosti p-valuace:

Věta 1. Pro všechna $x, y \in \mathbb{Z}$, platí:

1. $v_p(xy) = v_p(x) + v_p(y)$,
2. $v_p(a^b) = b \cdot v_p(a)$,
3. $x \mid y \iff$ pro každé prvočíslo p platí $v_p(x) \leq v_p(y)$,
4. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$,
5. $v_p((a, b)) = \min\{v_p(a), v_p(b)\}$,
6. $v_p([a, b]) = \max\{v_p(a), v_p(b)\}$

((a,b), resp. $[a,b]$, značí největší společný dělitel, resp. nejmenší společný násobek).

Důkaz. Ukážeme pouze důkaz třetí vlastnosti. Ostatní důkazy doporučujeme čtenářům jako užitečné cvičení.
„$\Longrightarrow$“ (Dokažme nejprve implikaci zleva doprava): Pokud $x|y$, tak existuje $k \in \mathbb{N}$ takové, že $y = kx$. Potom podle první vlastnosti víme, že pro libovolné prvočíslo p platí $v_p(y) = v_p(x) + v_p(k)$. Jelikož p-valuace jsou vždy nezáporné, tak tím dostáváme, že $v_p(y) \geq v_p(x)$.
„$\Longleftarrow$“: Nechť $x = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, y = p_1^{\beta_1} \cdots p_k^{\beta_k}$ jsou rozklady čísel x, y na součin mocnin různých prvočísel. Pak podle poznámky za definicí p-valuace na předchozí straně a podle předpokladu platí $\alpha_i = v_{p_i}(x) \leq v_{p_i}(y) = \beta_i$. Uvažme číslo $k = p_1^{\beta_1 - \alpha_1} \cdots p_k^{\beta_k - \alpha_k}$, pak podle předchozích nerovností víme, že k je celé. Navíc zřejmě platí, že $kx = y$, což dokazuje druhou implikaci. □

Ještě než se pustíme dál, tak okomentujme vlastnosti pět a šest, protože čtenář je ve skutečnosti už dávno zná! Tyto vlastnosti totiž odpovídají tomu, jak se učí počítat největší společný dělitel a nejmenší společný násobek na základní škole. Podívejme se na příklad. Jak spočítáme největšího společného dělitele čísel 18 a 30? Rozložíme obě čísla na součin prvočísel $18 = 2^1 3^2, 30 = 2^1 3^1 5^1$, porovnáme exponenty u stejných prvočísel a vždy vybereme ten menší. Tedy exponent u trojky v rozkladu čísla $(18, 30) = 6$ je 1, což je minimum čísel 2 a 1. Tento postup ale přesně odpovídá tvrzení pět!

Když už známe spoustu vlastností, které p-valuace mají, tak si pojďme demonstrovat jejich užitečnost na příkladu z americké matematické olympiády:

Příklad (USAMO 1972**):** Nechť a, b, c jsou přirozená. Ukažte, že platí

$$\frac{(a,b,c)^2}{(a,b)(a,c)(b,c)} = \frac{[a,b,c]^2}{[a,b][a,c][b,c]}.$$

Řešení: Rovnost ze zadání je zřejmě ekvivalentní rovnosti

$$(a,b,c)^2[a,b][a,c][b,c] = [a,b,c]^2(a,b)(a,c)(b,c).$$

Označme L levou stranu dokazované rovnosti a P pravou. Ukážeme, že pro všechna prvočísla p platí $v_p(L) = v_p(P)$. Díky třetímu tvrzení věty 1 tak dostaneme, že levá strana dělí pravou a pravá levou, jsou si tedy rovny.

Jelikož zadání je symetrické, tak bez újmy na obecnosti můžeme předpokládat, že $v_p(a) \leq v_p(b) \leq v_p(c)$. Díky tomu vidíme (podle páté a šesté vlastnosti):

$$\begin{aligned} v_p((a,b,c)) = v_p((a,b)) = v_p((a,c)) &= v_p(a), \\ v_p([a,b,c]) = v_p([a,c]) = v_p([b,c]) &= v_p(c), \\ v_p((b,c)) = v_p([a,b]) &= v_p(b). \end{aligned}$$

Nyní už jen stačí spočítat p-valuaci levé a pravé strany. Budeme u toho využívat první

část předchozího tvrzení:

$$\begin{aligned} v_p(L) &= 2v_p((a,b,c)) + v_p([a,b]) + v_p([a,c]) + v_p([b,c]) \\ &= 2v_p(a) + v_p(b) + 2v_p(c). \end{aligned}$$

$$\begin{aligned} v_p(P) &= 2v_p([a,b,c]) + v_p((a,b)) + v_p((a,c)) + v_p((b,c)) \\ &= 2v_p(c) + 2v_p(a) + v_p(b). \end{aligned}$$

Dostáváme tedy, že pro libovolné prvočíslo platí, že $v_p(L) = v_p(P)$, tak $L = P$, čímž je tvrzení dokázáno.

Na závěr ještě uveďme pár tvrzení pro opravdové fajnšmekry! Pokud chcete víc informací o p-valuacích, tak zkuste pořádně prozkoumat následující trojici tvrzení známou jako Lifting the exponent lemma.

Věta 2. LTE-lemma 1: Nechť p je liché prvočíslo a $a, b \in \mathbb{N}$ taková, že $p \nmid a, p \nmid b$ a $p|a-b$. Pak pro všechna $n \in \mathbb{N}$ platí:

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n).$$

Věta 3. LTE-lemma 2: Nechť p je liché prvočíslo a $a, b \in \mathbb{N}$ taková, že $p \nmid a, p \nmid b$ a $p|a+b$. Pak pro všechna lichá $n \in \mathbb{N}$ platí:

$$v_p(a^n + b^n) = v_p(a+b) + v_p(n).$$

Věta 4. LTE-lemma 3: Buď $a, b \in \mathbb{N}$ taková, že $2|a-b$. Pak pro všechna $n \in \mathbb{N}$ platí:

$$v_2(a^n - b^n) = v_2(a-b) + v_2(a+b) + v_2(n) - 1.$$

LTE lemma je už opravdový kanón, který často zabije jinak velice náročnou úlohu. Můžete to zkusit na úloze, která byla v BrKoSu kdysi dávno nejtěžší úloha v poslední sérii. Vzorové řešení je elementární a LTE lemma nepoužívá. Pokud ho ale použijete, tak si ho můžete hodně zkrátit.

Příklad (BRKOS 24. ročník, 6. série, příklad 4): Najděte všechna přirozená a, n taková, že existuje prvočíslo p splňující

$$2a^p p + a^p + np^n = anp^n + 2p + 1.$$