Teorie čísel: Cvičení 1 – výsledky a vybraná vzorová řešení

14. února 2022

Web: https://www2.karlin.mff.cuni.cz/~raskam/vyuka/tc.html
Email: raska.martin@gmail.com

Výsledky:

2. a) $v_3(63) = 2$, $v_7(63) = 1$, $v_p(63) = 0$ pro ostatní prvočísla p,
   b) $v_2(170) = 1$, $v_5(170) = 1$, $v_{17}(170) = 1$, $v_p(170) = 0$ pro ostatní prvočísla p,
   c) $v_2(360) = 3$, $v_3(360) = 2$, $v_5(360) = 1$, $v_p(170) = 0$ pro ostatní prvočísla p.
4. Například $a = b = 1$ a $p = 2$ ($v_2(1) = 0$ a $v_2(1 + 1) = 1$).
6. 24
7. 1 a 0
8. Ne
9. Funguje například $(n + 1)! + 2, (n + 1)! + 3, \ldots$.
10. Ne

V příklady 11, 15 lze dokázat chytrým použitím p-valuací.
Příklady 12, 13, 14 jsou na aplikaci Legendreova vzorce z příkladu 5.

Vybraná vzorová řešení:

Vzorová řešení příkladů 0 a 5 byla předvedena na cviku.

1. a) Buď $a = \pm\prod_{i=1}^{n} p_i^{\alpha_i}$, $b = \pm\prod_{i=1}^{m} q_i^{\beta_i}$ jednoznačné prvočíselné rozklady čísel a, b (předpokládejme, že jsou tato čísla nenulová, pro nulu je příklad triviální). Číslo ab pak ve svém prvočíselném rozkladu obsahuje právě prvočísla $p_1, \cdots, p_n, q_1, \cdots, q_m$. Protože $p \mid ab$, tak se v tomto prvočíselném rozkladu nachází, a tedy je rovno některému z prvočísel p_i, q_j. BÚNO $p = p_i$ pro vhodné i. Tedy se ale p nachází v prvočíselném rozkladu a a nutně dělí a.

Alternativně lze toto nahlédnout pomocí p-valuací za použití $v_p(ab) = v_p(a) + v_p(b)$ (viz příklad 3). Protože je z předpokladu číslo nalevo v rovnosti větší než 0, tak alespoň jeden z členů napravo musí být větší než 0.

POZNÁMKA: Oba tyto důkazy (druhý nepřímo) používají tvrzení o jednoznačném prvočíselném rozkladu a závislost dělitelnosti a tohoto rozkladu. To je netriviální tvrzení, které ve svém důkazu naopak toto tvrzení o prvočíslech ($p \mid ab \to p \mid a \vee p \mid b$) používá. Tedy se správně vzato jedná o důkaz kruhem. Na přednášce z Algebry si ukážete důkaz, který jednoznačný prvočíselný rozklad nevyužívá. Cílem tohoto cvičení bylo uvědomit si, že daná věc platí a osvěžit si práci s prvočísly :)

1. b) Opět předpokládejme nenulovost obou čísel, jinak je příklad triviální. Uvažme prvočíselný rozklad $a = \pm\prod_{i=1}^{n} p_i^{\alpha_i}$. Podobně jako v příkladu 0 si rozmysleme, že $v_{p_i}(a) = \alpha_i$ pro prvočísla z rozkladu a pro ostatní je to rovno 0, tedy p-valuace je v podstatě rovna exponentu v prvočíselném rozkladu. (Skutečně $p_i^{\alpha_i} \mid a$ a pokud by naopak $p_i^{\alpha_i+1} \mid a$, tak by p_i muselo dělit součin ostatních prvočísel v prvočíselném rozkladu, tedy jako důlsedek 1a) by muselo dělit nějaké jiné prvočíslo, což by byl spor.) Můžeme tedy psát $a = \pm\prod_{p \text{ prvočíslo}} p^{v_p(a)}$, a tedy $a^2 = \prod_{p \text{ prvočíslo}} p^{2v_p(a)}$ – z jednoznačnosti prvočíselného rozkladu pak $v_p(a^2) = 2v_p(a)$. Podobně pro b. Podle příkladu 0 pak $a^2 \mid b^2$ právě tehdy když $2v_p(a) = v_p(a^2) \leq v_p(b^2) = 2v_p(b)$ pro všechna prvočísla p. To je ale očividně ekvivalentní s $v_p(a) \leq v_p(b)$, což opět podle 0 nastává právě tehdy když $a \mid b$.

1. c) Pro spor předpokládejme, že nějaké přirozené číslo dělí zároveň a^n a b^m, BÚNO je to prvočíslo p. Poté ale p dělí i a a b, neboť jejich mocniny mají ve svém prvočíselném rozkladu stejná prvočísla. To je chtěný spor.

3. a) Podobně jako v příkladu 1.b) si uvědomíme, že p-valuace odpovídají exponentům v prvočíselném rozkladu. Tedy$a = \pm \prod_{p \text{ prvočíslo}} p^{v_p(a)}$, $b = \pm \prod_{p \text{ prvočíslo}} p^{v_p(b)}$ a $ab = \pm \prod_{p \text{ prvočíslo}} p^{v_p(ab)}$. Pronásobením prvních dvou vztahů dostaneme $ab = \pm \prod_{p \text{ prvočíslo}} p^{v_p(a)v_p(b)}$. Z jednoznačnosti prvočíselných rozkladů už dostaneme chtěnou rovnost.

3. b) Protože je $\frac{m}{n}$ celé číslo, tak n dělí m a můžeme psát $m = nk$. Potom

$$v_p\left(\frac{m}{n}\right) = v_p(k) = v_p(k) + v_p(n) - v_p(n) = v_p(nk) - v_p(n) = v_p(m) - v_p(n).$$