Teorie čísel: Cvičení 1 – výsledky, nápovědy, vzorová řešení

Simona Hlavinková, e-mail: simonkahlavinkova@gmail.com

Výsledky:

1. 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 $v_2(1 + 1) = 1$). Obecně lze brát $a = p - 1$, $b = 1$.

5. a) $\left\lfloor \frac{x}{n} \right\rfloor$; c) 24

6. 1 a 0

7. Ne. Dokonce téměř nikdy. Pro každé prvočíslo jsou jednoznačně určené obě hodnoty valuace, ale není jasné, která patří k a a která k b. Proto, pokud se nsn a NSD liší v mocninách více než jednoho prvočísla, není dvojice $\{a, b\}$ určena jednoznačně.

11. Ne.

12. Funguje například $(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + (n + 1)$.

18. Ano.

Nápovědy:

5. b) Použijte vzorec pro valuaci součinu a vzniklou sumu místo „po sloupcích“ sečtěte „po řádcích“.

8. Dokonce platí pro každé x, že $\lfloor 2x \rfloor - 2 \lfloor x \rfloor \in \{0, 1\}$.

9. Použijte Legendreův vzorec (příklad 5b).

10. Vzorec pro valuaci podílu použijte jako definici. Všechny důležité vlastnosti by měly být zachovány.

13., 17. Příklady lze dokázat chytrým použitím p-valuací.

14.–16. Vyjděte z Legendreova vzorce (příklad 5b). 15 je důsledkem 16, ale samostatně ho lze dokázat o něco snáz.

18. Použijte Čínskou zbytkovou větu. Pokud ji neznáte, příkladem se netrapte.

19. Tento náročný a netypický příklad je ilustrací Prvočíselné věty. Vyjděte z toho, že Prvočíselná věta je ekvivalentní tvrzení $\vartheta(x) \sim x$ (což předpokládejte bez důkazu – lze si to zhruba rozmyslet, ale přesný důkaz je technicky náročný a není pointou příkladu). Jak souvisí délka knihy s funkcí $\vartheta(x)$?

Vybraná vzorová řešení:

Vzorová řešení příkladů 0 a 5 byla předvedena na cviku.

2. a) Buďte $a = \pm \prod_{i=1}^{n} p_i^{\alpha_i}$, $b = \pm \prod_{i=1}^{m} q_i^{\beta_i}$ 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 nebo q_j. Pokud $p = p_i$ pro některé i, pak zjevně dělí a; jestliže $p = q_j$ pro některé j, pak dělí b.

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 („Když prvočíslo dělí součin, pak dělí i některý z činitelů.“) používá. Přísně vzato jsme proto právě provedli důkaz kruhem. Na přednášce z Algebry si ukážete důkaz, který jednoznačný prvočíselný rozklad nevyužívá. Cílem tohoto cvičení bylo uvědomit si, že daná toto tvrzení platí, a osvěžit si práci s prvočísly, ne budovat teorii dělitelnosti od nuly.*

2. 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 $a \mid b$.
2. 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 $a = \pm\prod_{p\in\mathbb{P}} p^{v_p(a)}$, $b = \pm\prod_{p\in\mathbb{P}} p^{v_p(b)}$ a $ab = \pm\prod_{p\in\mathbb{P}} p^{v_p(ab)}$. Pronásobením prvních dvou vztahů dostaneme $ab = \pm\prod_{p\in\mathbb{P}} p^{v_p(a)v_p(b)}$. Z jednoznačnosti prvočíselných rozkladů už dostaneme kýženou rovnost.
3. b) Protože je $\frac{m}{n}$ celé číslo, tak n dělí m a můžeme psát $m = nk$. Potom už je jen o přeuspořádání vzorce z předchozího bodu:

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

3. c) Potřebujeme dokázat, že když p^k dělí m i n, pak dělí i jejich součet. To je ale známá vlastnost dělitelnosti.

Ve druhé části BÚNO předpokládejme, že $v_p(m) > v_p(n)$. Pak lze psát $n = p^k n_0$, kde $p \nmid n_0$, a $m = p^{k+1}m'$ (o m' nic nepředpokládáme). Dostáváme $m + n = p^k(pm' + n_0)$, a protože $pm' + n_0$ není dělitelné p, tvrzení je dokázáno.