

1. ZÁKLADNÉ POJMY

Symbolom $\mathbb{N}$ budeme označovať množinu prirodzených čísel. Teda

$$\mathbb{N} = \{1, 2, \dots\}.$$

Poznamenajme, že $0 \notin \mathbb{N}$. Symbolom $\mathbb{Z}$ budeme označovať množinu celých čísel. Teda

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}.$$

Budeme využívať dve jednoduché a ľahko pochopiteľné vlastnosti množiny $\mathbb{N}$.

Vlastnosť najmenšieho prvku (V1). Každá neprázdna podmnožina množiny $\mathbb{N}$ má najmenší prvok.

Ak $S \subset \mathbb{N}$ a $S \neq \emptyset$, potom jej najmenší prvok budeme označovať symbolom $\min S$. Uvedomme si, že napríklad množina $\mathbb{Z}$ túto vlastnosť nemá. Nie je náročné dokázať, že vlastnosť (V1) je ekvivalentná s princípom matematickej indukcie.

Vlastnosť najväčšieho prvku (V2): Každá neprázdna konečná podmnožina $\mathbb{N}$ má najväčší prvok.

Ak $S \subset \mathbb{N}$ je konečná podmnožina množiny prirodzených čísel, potom jej najväčší prvok budeme označovať symbolom $\max S$.

Úloha 1. Dokážte, že každá konečná množina reálnych čísel má najväčší prvok. (Návod: Postupujte matematickou indukciou vzhľadom na počet prvkov.) Teraz si pripomenieme už známu reláciu deliteľnosti celých čísel.

Nech $a, b \in \mathbb{Z}$. Hovoríme, že a *delí* b práve vtedy, keď existuje také celé číslo c , že $b = ac$. To, že a delí b , zapisujeme $a|b$. Taktiež hovoríme, že b je *deliteľné* a alebo že a je *deliteľom* b . Každé celé číslo a má *triviálne delitele* ± 1 a $\pm a$. Deliteľov, ktoré nie sú triviálnymi deliteľmi celého čísla a , nazývame *netriviálne delitele*. Prirodzené číslo väčšie ako 1, ktoré nemá netriviálne delitele, nazývame *prvočíslo*. Prirodzené číslo väčšie ako 1, ktoré nie je prvočísлом, nazývame *zložené číslo*. Množina $\mathbb{N}$ sa teda delí na $\{1\}$, množinu prvočísel a množinu zložených čísel.

Teraz sa budeme zaoberať vetou o delení so zvyškom. Dokážeme nasledujúcu vetu.

Veta 1. Nech $m, n \in \mathbb{N}$. Potom existujú také čísla $p \in \mathbb{N} \cup \{0\}$, $r \in \mathbb{Z}$, že platí:

$$0 \leq r < m \tag{1}$$

a

$$n = m \cdot p + r \quad (2).$$

Naviac, čísla p, r sú vzťahmi (1) a (2) určené jednoznačne.

Úloha 2. Nech m a n majú rovnaký význam ako v predchádzajúcej vete. Označme

$$p = \max\{k = 0, 1, 2, \dots; k \cdot m \leq n\}.$$

Dokážte, že hodnota $r = n - p \cdot m$ spĺňa nerovnosť (1).

Úloha 2 nám už ukazuje možnosť delenia so zvyškom, teda existenciu požadovaných čísel p, r . Ešte je potrebné dokázať ich jednoznačnosť.

Úloha 3.

- a) Nech $a, b \in \mathbb{N} \cup \{0\}$, $a < b$ a $b|a$. Potom $a = 0$.
- b) Nech $a, b \in \mathbb{N}$ a $a|b \wedge b|a$. Potom $a = b$. Dokážte.

Úloha 4. Nech $n = m \cdot p_1 + r_1$ a $n = m \cdot p_2 + r_2$. Potom $m|r_1 - r_2$.

Úloha 5. Použitím úloh 3a) a 4 dokážte, že r je vzťahmi (1) a (2) jednoznačne určené, a teda aj p je jednoznačne určené.

Číslo r z vety 1 nazývame *zvyškom* čísla n po delení číslom m a označujeme ho

$$r = n \bmod m.$$

Hodnota p sa nazýva *neúplný podiel*. V tejto súvislosti upozorníme na jednu zaujímavú funkciu.

Nech α je kladné reálne číslo. Označme symbolom $[\alpha]$ najväčšie celé číslo, ktoré nie je väčšie ako α . Napríklad $[5, 3] = 5$, $[0, 1] = 0$, $[-1, 2] = -1$. Hodnotu $[\alpha]$ nazývame *celá časť čísla α* .

Úloha 6. Nech $m, n \in \mathbb{N}$ a p je neúplný podiel čísel n, m . Dokážte, že

$$p = \left\lfloor \frac{n}{m} \right\rfloor.$$

Hodnotu $\{\alpha\} = \alpha - [\alpha]$ nazývame *necelou časťou α* . Niekedy ju nie úplne presne nazývame *zlomkovou časťou*.

Úloha 7. Nech $m, n \in \mathbb{N}$. Potom

$$n \bmod m = m \cdot \left\{ \frac{n}{m} \right\}.$$

Je zrejmé, že $a|b$ práve vtedy, keď $b \bmod a = 0$. Nech $m, n \in \mathbb{N}$. Potom číslo $d \in \mathbb{N}$ nazývame spoločným deliteľom m a n , ak $d|m$ a $d|n$. Je zrejmé, že množina týchto spoločných deliteľov je konečná. Jej najväčší prvok nazývame *najväčší spoločný deliteľ* čísel m, n a označujeme ho symbolom (m, n) . Ak $(m, n) = 1$, potom čísla m, n nazývame nesúdeliteľné.

Veta 2. Nech $m, n \in \mathbb{N}$. Potom existujú čísla $a, b \in \mathbb{Z}$ také, že

$$(m, n) = a \cdot m + b \cdot n.$$

Pri dôkaze vety 2 využijeme vlastnosť najmenšieho prvku (V1).

Úloha 8. Dokážte, že najmenší prvok množiny

$$L = \{a \cdot m + b \cdot n; a, b \in \mathbb{Z} \wedge a \cdot m + b \cdot n > 0\} \quad (3)$$

je spoločným deliteľom čísel m, n .

(Návod: Nech $d = \min L$. Použite vetu 1: ak $m \bmod d, n \bmod d > 0$, potom $m \bmod d, n \bmod d \in L$ a to je spor.)

Úloha 9. Dokážte, že žiadny spoločný deliteľ m, n nie je väčší ako $\min L$, kde L je množina určená vzťahom (3).

Je zrejmé, že úloha 8 a úloha 9 tvoria dôkaz vety 2. To nám umožňuje inak charakterizovať najväčší spoločný deliteľ.

Úloha 10. Nech $m, n \in \mathbb{N}$ a $d \in \mathbb{N}$. Potom $d = (m, n)$ práve vtedy, keď

$$\begin{aligned} & d|m \wedge d|n, \\ \forall d' \in \mathbb{N} : & \quad d'|m \wedge d'|n \Rightarrow d'|d. \end{aligned}$$

Úloha 10 nám vlastne hovorí, že (m, n) je násobkom všetkých ostatných spoločných deliteľov.

Veta 2 nám však nedáva praktický návod na výpočet (m, n) . Ak m a n sú veľké čísla, potom je náročné hľadať najmenší prvok množiny L . Metódu na určovanie (m, n) nazývame Euklidov algoritmus alebo metóda postupného delenia. Je založená na nasledujúcich faktoch.

Úloha 11. Nech $m, n \in \mathbb{N}$ a $m < n$. Potom $(m, n) = (m, n \bmod m)$.

Úloha 12. Ak $m, n \in \mathbb{N}$ a $m|n$, potom

$$(m, n) = m.$$

Čitateľ si iste všimol, že (m, n) ľahko určíme vtedy, keď m, n sú malé čísla. Tvrdenie úlohy 11 nám umožňuje postupne znižovať hodnotu argumentov m a n , aby sme mohli použiť úlohu 12.

Nech $m < n$. Potom

$$n = m \cdot p_1 + r_1, 0 \leq r_1 < m$$

a

$$(m, n) = (r_1, m).$$

Potom ale

$$m = r_1 \cdot p_2 + r_2, 0 \leq r_2 < r_1$$

a

$$(m, n) = (r_1, m) = (r_1, r_2).$$

Ďalej

$$r_1 = r_2 \cdot p_3 + r_3, 0 \leq r_3 < r_2$$

a

$$(m, n) = (r_1, m) = (r_1, r_2) = (r_2, r_3).$$

Podobným spôsobom postupne delíme

$$r_2 = r_3 \cdot p_4 + r_4, 0 \leq r_4 < r_3$$

...

$$r_{k-1} = r_k \cdot p_{k+1} + r_{k+1}, 0 \leq r_{k+1} < r_k$$

a

$$(m, n) = (r_k, r_{k+1}).$$

Postupnosť nezáporných čísel $r_1, r_2, \dots$ stále klesá a preto raz musí nastať prípad, že $r_{n+1} = 0$.

Použitím úlohy 12 dokážte tvrdenie v nasledujúcej úlohe.

Úloha 13. Ak v predchádzajúcom postupe platí, že $r_{n+1} = 0$, potom $(m, n) = r_n$.

Euklidov algoritmus nám po spätnom dosadení umožní nájsť koeficienty a, b z vety 2.

Úloha 14. Vypočítajte $(46, 58)$ a vyjadrite ho v tvare

$$(46, 58) = a \cdot 46 + b \cdot 58.$$

Hľadanie koeficientov a, b z vety 2 má význam najmä pri riešení lineárnych diofantických rovníc, ako zistíme neskôr.

Podobne ako definujeme najväčší spoločný deliteľ dvoch prirodzených čísel, môžeme definovať aj najväčší spoločný deliteľ viacerých čísel. Nech $m_1, \dots, m_k \in \mathbb{N}$. Potom najväčším spoločným deliteľom čísel $m_1, \dots, m_k$ nazývame najväčšie prirodzené číslo d také, že $d|m_1, \dots, d|m_k$. Toto číslo analogicky označujeme

$$d = (m_1, \dots, m_k).$$

Úloha 15. Nech $m_1, \dots, m_k \in \mathbb{N}$. Potom

$$(m_1, \dots, m_k) = ((m_1, \dots, m_{k-1}), m_k).$$

Dokážte.

Úloha 16. Nech $m_1, \dots, m_k \in \mathbb{N}$. Potom existujú také celé čísla $a_1, \dots, a_k$, že

$$(m_1, \dots, m_k) = a_1 \cdot m_1 + \dots + a_k \cdot m_k.$$

Dokážte.

(Návod: Postupujte podobne ako pri riešení úloh 8 a 9. Uvažujte množinu kladných hodnôt tvaru $a_1 \cdot m_1 + \dots + a_k \cdot m_k$, $a_i \in \mathbb{Z}$ a jej minimum. Môžete postupovať aj matematickou indukciou podľa postupu z úlohy 15.)

Teraz sa budeme zaoberať vlastnosťami nesúdeliteľných čísel.

Úloha 17. Nech $m, n \in \mathbb{N}$ a nech existujú čísla $a, b \in \mathbb{Z}$ také, že

$$am + bn = 1.$$

Potom $(m, n) = 1$.

Použitie tvrdenia z úlohy 17 si teraz ukážeme na nasledujúcich dvoch úlohách.

Úloha A. Ak $x, y, d \in \mathbb{N}$, $d|x \wedge d|y$ a $(\frac{x}{d}, \frac{y}{d}) = 1$, potom $(x, y) = d$. Dokážte.

Úloha B. Nech $x, y, d \in \mathbb{N}$. Dokážte, že $(dx, dy) = d(x, y)$.

Úloha 18. Na príklade ilustrujte, že ak pre $a, b \in \mathbb{Z}$ platí

$$am + bn = d > 1,$$

potom ešte nemusí platiť, že $d = (a, b)$.

Veta 3. Nech $a, b, c \in \mathbb{N}$, $a|b \cdot c$ a $(a, b) = 1$. Potom $a|c$.

Dôsledok. Ak $a, b, c \in \mathbb{N}$, $(a, b) = 1$, $a|c$ a $b|c$, tak $ab|c$.

Úloha 19. Dokážte vetu 3 a jej dôsledok.

(Návod: Môžeme si vyjadriť $1 = ax + by$, $x, y \in \mathbb{Z}$. Potom $c = acx + bcy$. Uvedomme si, že posledný sčítanec je deliteľný a .)

Veta 3 má fundamentálny význam pri mnohých úvahách v elementárnej teórii čísel a jej rôzne zovšeobecnenia hrajú dôležitú úlohu aj v abstraktnejších oblastiach matematiky.

Použitie vety 3 teraz ukážeme pri dôkaze vety, ktorá je známa aj pod označením hlavná veta aritmetiky. Táto veta hovorí o možnosti jednoznačného rozkladu prirodzeného čísla na súčin prvočísel. Pripomeňme si, že číslo $p \in \mathbb{N}$, $p \neq 1$ nazývame prvočíslom, ak pre každé $d \in \mathbb{N}$ platí

$$d|p \Rightarrow d = 1 \vee d = p.$$

Sú to teda tie prirodzené čísla, ktoré majú práve dva delitele, a to 1 a samé seba.

Úloha 20. Nech $p \neq q$ sú prvočísla. Potom $(p, q) = 1$.

Úloha 21. Nech $p \neq q$ sú prvočísla a $p|a \cdot q$. Potom $p|a$.

Veta 4. Nech $n \in \mathbb{N}$ a $n \neq 1$. Potom n môžeme vyjadriť v tvare

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \quad (4)$$

kde $p_i, i = 1, 2, \dots, k$ sú rôzne prvočísla a $\alpha_i, i = 1, 2, \dots, k$ sú prirodzené čísla. Uvedený rozklad je jednoznačný až na poradie činiteľov.

Dôkaz. Najskôr metódou matematickej indukcie dokážeme existenciu rozkladu. Ak $n = 2$, tak veta platí, nakoľko 2 je prvočíslo. Nech veta platí pre všetky $n < N$. Ak N je prvočíslo, veta platí. Ak N nie je prvočíslo, potom $N = N_1 \cdot N_2$, kde $N_1, N_2 < N$, a preto rozklad (4) pre N_1 a N_2 existuje. Z rovnosti $N = N_1 \cdot N_2$ dostávame, že existuje rozklad taktiež pre N .

Dôkaz jednoznačnosti rozdelíme do niekoľkých úloh.

Úloha 22. Nech p je prvočíslo a $a \in \mathbb{N}$. Potom buď $(a, p) = 1$ alebo $p|a$.

Úloha 23. Nech p je prvočíslo a $p|a_1 \cdot \dots \cdot a_k$, $a_i \in \mathbb{N}$, $i = 1, \dots, k$. Potom existuje také číslo i , pre ktoré platí, že $p|a_i$, $0 < i \leq k$.

(Návod: Použite vetu 3, úlohu 22 a matematickú indukciu.)

Úloha 24. Nech p je prvočíslo, $p|a^n$, $a \in \mathbb{N}, n \in \mathbb{N}$. Potom aj $p^n|a^n$.

Úloha 25. Nech $a, b \in \mathbb{N}$ a $(a, b) = 1$. Ak $\alpha \in \mathbb{N}$, potom aj $(a^\alpha, b) = 1$.

(Návod: Podľa vety 2 existujú $k_1, k_2 \in \mathbb{Z}$ také, že $k_1 a + k_2 b = 1$. Teda $k_1 a = 1 - k_2 b$. Umocnením poslednej rovnosti na α a úpravami dokážte, že $\exists k'_1, k'_2$ také, že $k'_1 a^\alpha + k'_2 b = 1$.)

Úloha 26. Nech $a, b \in \mathbb{N}$ a $\alpha, \beta \in \mathbb{N}$. Ak $(a, b) = 1$, potom aj $(a^\alpha, b^\beta) = 1$.

Úloha 27. Nech p_1, p_2 sú rôzne prvočísla a $\alpha_1, \alpha_2 \in \mathbb{N}$. Potom $(p_1^{\alpha_1}, p_2^{\alpha_2}) = 1$.

Teraz už môžeme dokazovať jednoznačnosť rozkladu prirodzeného čísla na súčin prvočísel. Budeme postupovať matematickou indukciou. Pretože jednoznačnosť požadujeme až na poradie jednotlivých činiteľov, môžeme v (4) predpokladať, že

$$p_1 < p_2 < \dots < p_k.$$

Úloha 28. Nech $p_1 < \dots < p_k$ a $q_1 < \dots < q_l$ sú prvočísla. Nech

$$p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot \dots \cdot q_l^{\beta_l}. \quad (5)$$

Potom $p_1 = q_1$ a $\alpha_1 = \beta_1$.

(Návod: Uvedomte si, že p_1 je najmenší prvočíselný deliteľ čísla $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ a podobne aj q_1 .)

Úloha 29. Matematickou indukciou vzhľadom na k dokážte, že z (5) vyplýva $k = l$, $p_i = q_i$, $\alpha_i = \beta_i$, $i = 1, \dots, k$.

Vidíme, že úlohou 29 sme ukončili dôkaz vety 4.

Úloha 30. Nech $a, a_1, b, b_1 \in \mathbb{N}$ a $(a, b_1) = 1 = (a_1, b)$ a $ab = a_1b_1$. Potom $a = a_1 \wedge b = b_1$. Dokážte.

(Návod: Použite úlohu 3 b) a vetu 3.)

Keď máme dve prirodzené čísla n_1, n_2 , ktoré majú rozklady

$$n_1 = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}, n_2 = q_1^{\beta_1} \cdot \dots \cdot q_r^{\beta_r},$$

môžeme si ich vyjadriť v tvare

$$n_1 = r_1^{\gamma_1} \cdot \dots \cdot r_s^{\gamma_s}, \quad n_2 = r_1^{\gamma'_1} \cdot \dots \cdot r_s^{\gamma'_s}$$

tak, že $r_1, \dots, r_s$ sú všetky prvočísla $p_1, \dots, p_k, q_1, \dots, q_r$ a ako exponenty $\gamma_1, \dots, \gamma_s, \gamma'_1, \dots, \gamma'_s$ pripúšťame aj 0. Takéto vyjadrenie prirodzených čísel teraz použijeme na vyjadrenie ich najväčšieho spoločného deliteľa pomocou kanonického rozkladu.

Úloha 31. Nech $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ a $m = p_1^{\beta_1} \cdot \dots \cdot p_k^{\beta_k}$. Označme

$$\gamma_i = \min\{\alpha_i, \beta_i\}, \quad i = 1, \dots, k.$$

Potom

$$(m, n) = p_1^{\gamma_1} \cdot \dots \cdot p_k^{\gamma_k}.$$

Dokážte.

(Návod: Ak p je prvočíslo a $p^\alpha | m \wedge p^\alpha | n$, potom $p = p_i$ a $\alpha \leq \alpha_i \wedge \alpha \leq \beta_i$.)

Pripomeňme si teraz pojem najmenšieho spoločného násobku čísel $m, n \in \mathbb{N}$. Je to

$$\min\{k > 0; \quad m|k \wedge n|k\}.$$

Musíme si uvedomiť, že vďaka vlastnosti (V1) uvedené minimum existuje, pretože $m \cdot n \in \{k > 0; \quad m|k \wedge n|k\}$ a teda táto množina je neprázdna. Najmenší spoločný násobok čísel m, n budeme označovať symbolom $[m, n]$.

Úloha 32. Nech $d, m, n \in \mathbb{N}$. Dokážte, že $d = [m, n]$ práve vtedy, keď

$$m|d \wedge n|d, \tag{a}$$

$$\forall d' \in \mathbb{N} : \quad m|d' \wedge n|d' \Rightarrow d|d'. \quad (b)$$

Pomocou tvrdenia v úlohe 32 dokážeme, že platí podobné vyjadrenie $[m, n]$ ako v prípade (m, n) v úlohe 31.

Úloha 33. Nech $m = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, $n = p_1^{\beta_1} \cdot \dots \cdot p_k^{\beta_k}$, $p_i, i = 1, \dots, k$ sú prvočísla. Nech

$$\gamma_i = \max\{\alpha_i, \beta_i\}, \quad i = 1, \dots, k.$$

Potom

$$[m, n] = p_1^{\gamma_1} \cdot \dots \cdot p_k^{\gamma_k}.$$

Dokážte.

(Návod: Ak $m|d \wedge n|d$, potom $p_i^{\gamma_i}|d$, $i=1, \dots, k$.)

Úloha 33 nám dáva taktiež návod na výpočet hodnoty $[m, n]$. Problém je však v tom, že musíme nájsť rozklad čísel m, n na súčin prvočísel, čo je veľmi náročná úloha. Ak si spomenieme na úlohu 13, teda na Euklidov algoritmus na hľadanie najväčšieho spoločného deliteľa dvoch prirodzených čísel, vidíme, že máme k dispozícii omnoho efektívnejší postup na výpočet (m, n) , ako keby sme ho počítali pomocou úlohy 31, teda rozkladom na súčin prvočísel. Nasledujúca úloha nám ukáže, ako možno $[m, n]$ vypočítať pomocou (m, n) .

Úloha 34. Nech $m, n \in \mathbb{N}$. Potom

$$[m, n] = \frac{m \cdot n}{(m, n)}.$$

Dokážte.

(Návod: Použite úlohu 31 a 33.)

Úloha 35. Ak m, n sú nesúdeliteľné prirodzené čísla, potom

$$[m, n] = m \cdot n.$$

(Návod: Použite dôsledok vety 3.)

Tvrdenie úlohy 34 môžeme dokázať aj iným spôsobom, ktorý teraz uvedieme, aby sme si precvičili príslušné pojmy.

Úloha A. Dokážte, že pre $m, n \in \mathbb{N}$ platí

$$\left(\frac{m}{(m, n)}, \frac{n}{(m, n)} \right) = 1.$$

Úloha B. Nech $a, m, n \in \mathbb{N}$. Dokážte, že $a[m, n] = [am, an]$.

Úloha C. Dokážte tvrdenie v úlohe 34 pomocou úloh A, B a úlohy 35.

Úloha D. Nech $m, n \in \mathbb{N}$. Pomocou tvrdenia v úlohe 34 a úlohe A dokážte, že

$$\left(\frac{[m, n]}{m}, \frac{[m, n]}{n} \right) = 1.$$

Rozklad prirodzeného čísla n v tvare

$$n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k},$$

kde $p_1, \dots, p_k$ sú navzájom rôzne prvočísla, nazývame kanonickým rozkladom. Čísla $\alpha_1, \dots, \alpha_k$ nazývame exponenty kanonického rozkladu čísla n .

Úloha 36. Nech $(m, n) = 1$ a $m = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, $n = q_1^{\beta_1} \cdot \dots \cdot q_l^{\beta_l}$ sú kanonické rozklady čísel m a n . Potom $m \cdot n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdot \dots \cdot q_l^{\beta_l}$ je kanonický rozklad čísla $m \cdot n$.

Úloha 37. Nech m je druhou mocninou prirodzeného čísla. Potom všetky exponenty jeho kanonického rozkladu sú párne.

Úloha 38. Nech $(m, n) = 1$ a $m \cdot n = r^2$, $r \in \mathbb{N}$. Potom $m = (m, r)^2$, $n = (n, r)^2$. Dokážte, že predpoklad $(m, n) = 1$ nemožno vynechať.

(Návod: Môžete postupovať podľa úlohy 37, ale aj bez použitia kanonického rozkladu podľa vety 2 a časti b) úlohy 3.)