# Dokonalé a spriatelené čísla

## 1. kapitola. Niektoré poznatky z teorie čísel

In: Tibor Šalát (author): Dokonalé a spriatelené čísla. (Slovak). Praha: Mladá fronta, 1969. pp. 5–17.

Persistent URL: http://dml.cz/dmlcz/403668

1. kapitola

# NIEKTORÉ POZNATKY Z TEORIE ČÍSEL

## DELITEĽNOSŤ V OBORE CELÝCH ČÍSEL

V tejto knižke slovo „číslo", uvedené samostatne, bez prídavného mena, značí celé číslo, teda prvok množiny

$$\{0, 1, -1, 2, -2, \ldots n, -n, \ldots\}.$$

Často budeme hovoriť o prirodzených číslach, teda o prvkoch množiny

$$\{1, 2, 3, \ldots n, \ldots\}.$$

V ďalšom budeme používať túto, čitateľovi iste známu vlastnosť celých čísel:

Nech $M$ je nejaká neprázdna množina celých čísel. Ak existuje také reálne číslo $a$, že všetky prvky množiny $M$ sú nie väčšie než $a$, potom v množine $M$ existuje najväčší (maximálny) prvok (tj. existuje také číslo $b$, že $b \in M$*) a pre každý prvok $x \in M$ platí $x \leqq b$).

Podobne platí:

Nech $M$ je nejaká neprázdna množina celých čísel. Ak existuje také reálne číslo $a'$, že všetky prvky množiny $M$ sú nie menšie než $a'$, potom v množine $M$ existuje najmenší (minimálny) prvok (tj. existuje teké číslo $b'$, že $b' \in M$ a pre každý prvok $x \in M$ platí $x \geqq b'$).

*) $x \in \mathbf{A}$ značí: $x$ patrí do množiny $\mathbf{A}$.

Pripomeňme ešte pojem absolutnej hodnoty celého čísla. Ak $a$ je celé číslo, potom absolutnou hodnotou $|a|$ čísla $a$ rozumieme číslo $a$, ak $a \geq 0$ a číslo $-a$, ak $a < 0$. Tak napríklad $|6| = 6$, $|-5| = -(-5) = 5$ a pod.

Iste je čitateľovi známe, že absolutná hodnota súčinu dvoch čísel sa rovná súčinu absolutných hodnôt tých čísel a absolutná hodnota súčtu dvoch čísel nepresahuje súčet absolutných hodnôt tých čísel. Tak napr. $|(-3).8| = |-3|.8 = 3.8 = 24$, $|-3+8| \leqq |-3| + |8| = 11$.

**D1.** Hovoríme, že číslo $a$ delí číslo $b$, ak existuje číslo $q$ tak, že $b = aq$.

Namiesto „$a$ delí $b$" hovoríme aj „$a$ je deliteľom čísla $b$", „$b$ je násobkom čísla $a$", „$b$ je deliteľné číslom $a$". Ak $a$ delí $b$, píšeme $a \mid b$. Ak $a$ nedelí $b$, píšeme $a \nmid b$.

Celé čísla, ktoré sú deliteľné číslom 2 nazývame párnymi, ostatné celé čísla nazývame nepárnymi.

**P1.** $3 \mid 18$, $3 \nmid (-101)$, $0 \mid 0$, $0 \nmid 6$.

**P2.** Ako vyzerá množina všetkých násobkov čísla 7?

**P3.** Ak $a \mid b$, potom aj $(-a) \mid b$, $a \mid (-b)$, $(-a) \mid (-b)$.

Tie prirodzené čísla, ktoré sú deliteľmi čísla $a$, nazývame prirodzenými deliteľmi čísla $a$. Tak napr. čísla 1, 2, 3, 4, 6, 12 sú prirodzenými deliteľmi čísla $-12$ a číslo $-12$ už iných prirodzených deliteľov nemá.

**P4.** Číslo 0 je deliteľné každým číslom.

**P5.** Číslo 0 nie je deliteľom žiadneho celého čísla $b \neq 0$.

**V1.** Ak $a \mid b$, $b \neq 0$, potom $|a| \leqq |b|$.

**Dôkaz.** Na základe predpokladu existuje celé $q$ tak, že

$$b = aq. \tag{1}$$

Keďže $b \neq 0$, je aj $q \neq 0$ a tak $|q| \geq 1$. Z (1) dostávame potom $|b| = |a|.|q| \geq |a|$, teda $|b| \geq |a|$.

**P6.** Nech $a \mid b$ a súčasne $b \mid a$. Potom $|a| = |b|$.

Návod: Použite $\mathbf{V}_1$. a $\mathbf{P}_5$!

Vzťah $a \mid b$ nie je symetrický, to značí, že z $a \mid b$ nevyplýva ešte $b \mid a$. Tak napr. $2 \mid 4$, ale $4 \nmid 2$. No tento vzťah má nasledujúcu vlastnosť, tzv. vlastnosť tranzitívnosti.

**V₂.** Ak $a \mid b$, $b \mid c$, potom $a \mid c$.

**Dôkaz.** Na základe predpokladu existujú čísla $q_1$, $q_2$ tak, že $b = aq_1$, $c = bq_2$. Ak do druhej rovnosti dosadíme z prvej za $b$, dostaneme $c = (aq_1) \cdot q_2 = a(q_1 \cdot q_2)$. Pretože $q_1$, $q_2$ sú celé čísla, je aj $q_1 \cdot q_2$ celé a $c = a(q_1 \cdot q_2)$, teda $a \mid c$.

**V₃.** Nech $a$ je celé, $m$ prirodzené. Potom existujú čísla $q$, $r$, $0 \leqq r < m$ tak, že

$$a = mq + r. \tag{2}$$

Čísla $q$, $r$, $0 \leqq r < m$ sú číslami $a$, $m$ jednoznačne určené.

**Dôkaz.** Zostrojme racionálne číslo $\frac{a}{m}$. V množine všetkých celých čísel nie väčších než $\frac{a}{m}$ existuje najväčší prvok. Označme ho znakom $q$. Teda na základe definície čísla $q$ platí: $q \leqq \frac{a}{m} < q + 1$. Vynásobením týchto nerovností číslom $m$ dostaneme $mq \leqq a < mq + m$. Položme

$$r = a - mq. \tag{3}$$

Z predošlého vyplýva, že $r$ je celé a $0 \leqq r < m$. Z (3) dostávame potom $a = mq + r$.

Nech čísla $q'$, $r'$, $0 \leqq r' < m$ spĺňajú rovnosť

$$a = mq' + r' \tag{4}$$

a nech napr. $r \geqq r'$. Potom ak od (2) odčítame (4), dostaneme

$$r - r' = m(q - q'). \tag{5}$$

Odtiaľ vyplýva, že $m$ delí rozdiel $r - r'$. No z podmienok $r \geq r', 0 \leqq r < m, 0 \leqq r' < m$ vyplýva $0 \leqq r - r' < m$ a odtiaľ v dôsledku $\mathbf{V}_1$ $r - r' = 0, r = r'$ a z (5) $q = q'$. Teda dvojica čísel $q, r, 0 \leqq r < m$ je číslami $a, m$ jednoznačne určená.

**P7.** Nájdite $q, r, 0 \leqq r < m$, ak

1. $a = -58, m = 10.$
2. $a = 74, m = 13.$

Uvedieme teraz niektoré vlastnosti párnych a nepárnych čísel. Ak $a$ je celé číslo, potom na základe vety $\mathbf{V}_3$ existujú celé $k, r$ tak, že $a = 2k + r$, pričom $0 \leqq r < 2$. Ak $r = 0$, potom $a$ je deliteľné číslom 2, teda $a$ je párne. Ak $r = 1$, potom $a$ nemôže byť deliteľne číslom 2. Ak by totiž $a$ bolo deliteľné číslom 2, potom na základe $\mathbf{V}_4$ a $\mathbf{P}_3$ aj číslo $1 = a - 2k$ by bolo deliteľné číslom 2, a to nie je možné (pozri $\mathbf{V}_1$). Tým sme dokázali vetu

**$\mathbf{V}_{3a}$.** Celé číslo $a$ je párne vtedy a len vtedy, keď má tvar $a = 2k$ ($k$ celé) a nepárne vtedy a len vtedy, keď má tvar $a = 2k + 1$ ($k$ celé).

Ľahkým dôsledkom uvedenej poučky sú tieto vety.

**$\mathbf{V}_{3b}$.** Súčet dvoch párnych čísel je párny, súčet dvoch nepárnych čísel je párny. Súčet $k$ ($k \geqq 2$) nepárnych čísel je párne číslo vtedy a len vtedy, keď $k$ je párne číslo.

**$\mathbf{V}_{3c}$.** Súčin dvoch párnych čísel je párny, súčin dvoch nepárnych čísel je nepárny a súčin nepárneho a párneho čísla je párny.

Ak $a, b$ sú celé čísla, potom existujú (celé) čísla, ktoré sú súčasne deliteľmi aj čísla $a$ aj čísla $b$. Takými číslami sú 1, — 1.

**$\mathbf{D}_2$.** Číslo $d$ nazývame spoločným deliteľom čísel $a, b$, ak $d \mid a, d \mid b$.

**$\mathbf{D}_3$.** Čísla $a, b$ nazývame nesúdeliteľnými, ak nemajú

iných spoločných deliteľov než 1, — 1. Ak $a$, $b$ nie sú nesúdeliteľné, nazývajú sa súdeliteľné.

Príkladom nesúdeliteľných čísel sú čísla 12, — 35, príkladom súdeliteľných čísel sú čísla 24, 60.

**P₃.** Nájdite množinu všetkých spoločných deliteľov čísel 1. 24, 60 2. — 50, 17 3. — 18, 48.

**V₄.** Ak $a \mid b$, a $a \mid c$, potom $a \mid (b + c)$.

**Dôkaz.** Podľa predpokladu existujú celé $q_1$, $q_2$ tak, že $b = aq_1$, $c = aq_2$. Potom $b + c = a(q_1 + q_2)$. Pretože $q_1 + q_2$ je celé, vyplýva tvrdenie vety z rovnosti $b + c = a(q_1 + q_2)$.

**V₅.** Ak $a \mid b$ a $c$ je celé číslo, potom $a \mid b.c$.

**Dôkaz.** Podľa predpokladu existuje celé $q$ tak, že $b = aq$. Potom z rovnosti $bc = a(q.c)$ vyplýva tvrdenie vety.

Naskytá sa otázka, či predošlé vety $\mathbf{V}_4$, $\mathbf{V}_5$ možno v istom zmysle obrátiť, presne rečeno, či platia tieto poučky:

Ak $a \mid bc$, potom buď $a \mid b$ alebo $a \mid c$.

Ak $a \mid (b + c)$, potom buď $a \mid b$ alebo $a \mid c$.

Ľahko sa možno presvedčiť, že posledne uvedené výroky sú nepravdivé. Stačí napr. voliť $b = 6$, $c = 8$, $a = 14$. Potom $a \mid (b + c)$, a súčasne $a \mid b.c$, no pritom $a \nmid b$, $a \nmid c$.

Teda deliteľ súčinu dvoch čísel nemusí byť deliteľom niektorého z činiteľov súčinu. Pri istom dodatočnom predpoklade vyplýva z deliteľnosti súčinu dvoch čísel daným číslom deliteľnosť aspoň jedného z činiteľov daným číslom. O tom pojednáva nasledujúca veta, nazývaná pre jej veľký význam aj fundamentálnou vetou aritmetiky. Originálny dôkaz tejto vety, ktorý tu podáme, pochádza od maďarského matematika *J. Surányiho*.

**V₆.** Nech $a \mid b.c$ a nech $a$ je nesúdeliteľné s $b$. Potom $a \mid c$.

**Dôkaz.** Označme znakom $C$, množinu všetkých tých

čísel $x$, pre ktoré $a \mid bx$. Teda $c \in C$. Na základe $\mathbf{V}_5$ do $C$ patria všetky násobky čísla $a$. Ukážeme (a to k dokončeniu dôkazu stačí), že $C$ pozostáva práve zo všetkých násobkov čísla $a$.

Označme znakom $m$ najmenšie kladné číslo patriace do $C$. Zrejme stačí dokázať platnosť týchto dvoch výrokov:
(i) Každý prvok z $C$ je deliteľný číslom $m$.
(ii) $m = |a|$.

Nech $x \in C$. Na základe $\mathbf{V}_3$ existujú celé $q, r$, $0 \leqq r < m$ tak, že $x = mq + r$. Odtiaľ $r = x - mq$ a tak $br = bx - bmq$. Pretože $x, m \in C$, delí číslo $a$ súčin $bx$ i $bm$ a teda aj čísla $bx$ a $-bmq$ (pozri $\mathbf{V}_5$). Na základe $\mathbf{V}_4$ potom $a \mid (bx - bmq)$, teda $a \mid br$, $r \in C$. Keby bolo $0 < r < m$, potom by $r$ bolo kladným prvkom množiny $C$ menším než $m$ a to by viedlo ku sporu s definíciou čísla $m$. Musí teda byť $r = 0$, potom $x = mq$, $m \mid x$. Tým je platnosť výroku (i) dokázaná.

Dokážeme (ii). Pretože $a \in C$, $m \mid a$ na základe (i). Teda existuje číslo $q_1$ tak, že

$$a = mq_1. \tag{6}$$

Keďže $m \in C$, $a \mid bm$, existuje číslo $q_2$ tak, že $bm = aq_2$. Dosaďme za $a$ do poslednej rovnosti zo (6), dostaneme $bm = mq_1 . q_2$, odtiaľ

$$b = q_1 . q_2. \tag{7}$$

Teda $q_1$ delí $a$ (pozri (6)) a na základe (7) aj $b$. Pretože však $a$, $b$ sú nesúdeliteľné, je $q_1 = 1$ alebo $q_1 = -1$ (pozri $\mathbf{D}_3$). Zo (6) potom dostávame $m = |a|$.

Každé prirodzené číslo $n > 1$ má aspoň dvoch prirodzených deliteľov, sú nimi čísla 1 a $n$. Ak $d \mid n$ a $1 < d < n$, potom $d$ nazývame netriviálnym deliteľom čísla $n$. Čísla 1 a $n$ nazývame triviálnymi deliteľmi čísla $n$.

**D4.** Číslo $n > 1$ sa nazýva prvočíslom, ak nemá netriviálnych deliteľov. Číslo $n > 1$ sa nazýva zloženým číslom, ak nie je prvočíslom.

Ak teda číslo $n$ je zložené, má aspoň jedného netriviálneho deliteľa.

Už *Euklidovi* (4. st. pred n. l.) bol známy pojem prvočísla. Od Euklida pochádza aj prvý dôkaz nekonečnosti počtu prvočísel. I keď vieme, že všetkých prvočísel je nekonečne mnoho, predsa ich konkrétne všetky nepoznáme. Nevieme napríklad, aké je vyjadrenie všetkých prvočísel v desiatkovej sústave. Ba vieme toho hodne menej. Nepoznáme dokonca ani žiadne prvočíslo väčšie než $2^{11^{213}}$. Najväčšie známe prvočíslo je $2^{11^{213}} - 1$. Pre hľadanie prvočísel sa v poslednom čase s výhodou používajú najnovšie matematické počítacie stroje.

**P9.** Dokážte, že každé párne číslo $a > 2$ je zložené!

**P10.** Ak $p$, $q$ sú dve prvočísla, potom buď $p = q$ alebo $p$, $q$ sú nesúdeliteľné. Dokážte to!

**V7.** Nech $n$ je zložené číslo, nech $p$ je najmenší netriviálny deliteľ čísla $n$. Potom $p$ je prvočíslo.

**Dôkaz.** Z definície netriviálneho deliteľa vyplýva, že $p > 1$. Ak $p$ nie je prvočíslo, potom existuje $d$, $1 < d < p$ tak, že $d \mid p$. Z $d \mid p$, $p \mid n$ vyplýva na základe $\mathbf{V}_2$ $d \mid n$. To je však vo spore s definíciou čísla $p$.

**V8.** Ak $a$ je celé a $p$ prvočíslo, potom buď $p \mid a$ alebo $p$, $a$ sú nesúdeliteľné.

**Dôkaz.** Ak $p$, $a$ sú súdeliteľné, potom existuje celé číslo $d \neq 1, -1$ tak, že $d \mid p$ a súčasne $d \mid a$. Z $d \mid p$ vyplýva na základe $\mathbf{P}_3$ $|d| \mid p$ a keďže $d \neq 1, -1$, je $q = |d| > 1$. Keďže $q \mid p$, je $q = p$ a tak $p \mid a$.

**V9.** Nech $a$, $b$ sú celé a $p$ prvočíslo. Ak $p \mid a.b$, potom buď $p \mid a$ alebo $p \mid b$.

**Dôkaz.** Ak $p \nmid a$, potom na základe $\mathbf{V}_8$ sú $a$, $p$ nesúdeliteľné. Z $\mathbf{V}_6$ vyplýva $p \mid b$.

Nasledujúca veta má veľmi názorný význam. Ukazuje, populárne rečeno, že prvočísla sú stavebnými kameňmi, z ktorých sú vybudované všetky prirodzené čísla $> 1$.

Poznamenajme, že v ďalšom výraz $a_1.a_2 \dots a_s$, kde $a_i$ sú celé a $s \geqq 1$, nazývame súčinom (o $s$ činiteľoch). Teda v prípade $s = 1$ máme súčin o jedinom činiteli.

**V$_{10}$.** Každé prirodzené číslo $n > 1$ sa dá vyjadriť ako súčin prvočísel a to až na poradie činiteľov jednoznačne.

**Dôkaz.** Napred ukážeme, že každé $n > 1$ sa dá písať vo tvare súčinu prvočísel. Dôkaz tohoto faktu uskutočníme matematickou indukciou. Tvrdenie je zrejme správne pre $n = 2$ (2 je prvočíslo!). Predpokladajme, že tvrdenie je správne pre všetky prirodzené čísla $> 1$, ktoré sú nie väčšie než $n (n > 1)$. Dokážeme, že tvrdenie platí aj pre $n + 1$. Keďže $n + 1 > 1$, je $n + 1$ buď prvočíslo alebo zložené číslo. Ak $n + 1$ je prvočíslo, potom tvrdenie platí zrejme. Ak $n + 1$ je zložené, potom na základe V$_7$ existuje prvočíslo $p$ tak, že $p \mid (n + 1)$. V dôsledku toho existuje prirodzené $a$ tak, že

$$n + 1 = p.a. \tag{8}$$

Keďže $p \geqq 2$, je $a \leqq n$ a keďže $n + 1$ je zložené, musí byť $a > 1$. Podľa indukčného predpokladu $a = p_1.p_2 \dots p_s$, kde $p_i (i = 1, 2, \dots s)$ sú prvočísla, $s \geqq 1$. Z (8) potom vyplýva $n + 1 = p.p_1.p_2 \dots p_s$, teda aj $n + 1$ je súčinom prvočísel.

Dokážeme teraz jednoznačnosť takého vyjadrenia. Treba dokázať, že ak

$$n = p_1.p_2 \dots p_s \tag{9}$$

a súčasne

$$n = q_1.q_2 \dots q_r \tag{10}$$

($p_i, i = 1, 2, \dots s$; $q_j, j = 1, 2, \dots r$, sú prvočísla, $s$, $r$ sú

prirodzené čísla), potom $s = r$ a každé $p_i$ je totožné s nejakým $q_j$ a obrátene. Z (9) a (10) dostávame

$$p_1 . p_2 \ldots p_s = q_1 . q_2 \ldots q_r. \tag{11}$$

Nech $s < r$. Potom z (11) vyplýva $q_1 \mid p_1 . p_2 \ldots p_s$. Na základe $\mathbf{V_9}$ odtiaľ vyplýva $q_1 \mid p_1$ alebo $q_1 \mid p_2 . p_3 \ldots p_s$. Ak $q_1 \nmid p_1$ opätovným použitím $\mathbf{V_9}$ dostaneme: $q_1 \mid p_2$ alebo $q_1 \mid p_3 \ldots p_s$. Po konečnom počte týchto úvah nájdeme také $i$, $1 \leqq i \leqq s$, že $q_1 \mid p_i$. Pretože pri formulácii jednoznačnosti neberieme ohľad na poradie činiteľov, môžeme už predpokladať, že $i = 1$ (keby tomu tak nebolo, zamenili by sme očíslovanie čísel $p_1$ a $p_i$). Potom teda $q_1 \mid p_1$ a z $\mathbf{P_{10}}$ vyplýva $q_1 = p_1$. Ak $s > 1$, dostaneme z (11)

$$p_2 \ldots p_s = q_2 \ldots q_r. \tag{12}$$

Ak predošlú úvahu zopakujeme ešte $s - 1$ -krát, dostaneme z (12) $1 = q_{s+1} \ldots q_r$. Táto rovnosť je zrejme nesprávna, pretože súčin na jej pravej strane má hodnotu $\geqq 2$. Musí teda byť $s \geqq r$. Analogicky sa dá ukázať, že $r \geqq s$, teda $s = r$. Z priebehu dôkazu vidieť, že pri eventuálnom prečíslovaní čísel $p_1, \ldots p_s$ dostávame $p_i = q_i$ $(i = 1, 2, \ldots s)$.

Pri vyjadrení čísla $n > 1$ vo tvare súčinu prvočísel

$$n = p_1 . p_2 \ldots p_s, s \geqq 1, \tag{13}$$

nemusia byť prvočísla $p_1, p_2, \ldots p_s$ navzájom rôzne. Ak na základe známeho komutatívneho a asociatívneho zákona pre násobenie zgrupujeme rovnakých činiteľov, dostaneme z (13) tzv. kanonický rozklad čísla

$$n = q_1^{\alpha_1} . q_2^{\alpha_2} \ldots q_k^{\alpha_k}, \tag{14}$$

$q_1, q_2, \ldots q_k$ sú navzájom rôzne prvočísla, $\alpha_1, \alpha_2, \ldots \alpha_k$ sú prirodzené čísla.

**P11.** Nájdite kanonické rozklady čísel 32, 54, 300.

**P12.** Dokážte, že ak $n > 2$, potom medzi $n$ a $n! = 1.2 \ldots n$ leží aspoň jedno prvočíslo.

**Riešenie.** Pretože $n \geq 3$, je $n! - 1 \geq 2$. Preto v dôsledku $\mathbf{V}_{10}$ existuje prvočíslo $p$ tak, že $p \mid (n! - 1)$, teda $p \leq n! - 1 < n!$. Ak by $p \leq n$, potom by $p$ delilo $n!$ a tak v dôsledku $\mathbf{V}_1$ by $p$ delilo aj $1 = n! - (n! - 1)$. Musí teda byť $p > n$, teda vcelku $n < p < n!$.

**P13.** Dokážte na základe **P12**, že všetkých prvočísel je nekonečne veľa.

**Riešenie.** Medzi 3 a 3! leží $p_1$, medzi 3! a (3!)! leží $p_2$ atď. Takto možno (indukciou) konštruovať nekonečnú postupnosť navzájom rôznych prvočísel.

## ARITMETICKÉ FUNKCIE $\sigma$ a $\tau$

Aritmetickými funkciami nazývame funkcie definované na množine všetkých prirodzených čísel s hodnotami v množine komplexných čísel. Aritmetické funkcie sú teda vlastne postupnosti s komplexnými členmi, špeciálne teda môžu ich členy byť celými resp. prirodzenými číslami.

Nám pôjde v ďalšom len o dve také funkcie, a to $\sigma$ a $\tau$. Funkcia $\sigma$ ($\tau$) je definovaná takto:
ak $n$ je prirodzené číslo, potom $\sigma(n)$ ($\tau(n)$) značí súčet (počet) prirodzených deliteľov čísla $n$.
Tak napr. $\sigma(1) = 1$, $\sigma(2) = 1 + 2 = 3$, $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$, $\tau(1) = 1$, $\tau(2) = 2$, $\tau(3) = 2$, $\tau(4) = 3$, $\tau(12) = 6$.

Pri štúdiu rozmanitých otázok v teórii čísel je veľmi dôležité vedieť na základe znalosti kanonického rozkladu čísla $n > 1$ určiť hodnoty $\sigma(n)$ a $\tau(n)$. O tom pojednáva nasledujúca poučka.

**V**$_{11}$. Nech $n = q_1^{\alpha_1} . q_2^{\alpha_2} \dots q_k^{\alpha_k}$ je kanonický rozklad čísla $n > 1$. Potom

$$\sigma(n) = \frac{q_1^{\alpha_1+1} - 1}{q_1 - 1} \cdot \frac{q_2^{\alpha_2+1} - 1}{q_2 - 1} \dots \frac{q_k^{\alpha_k+1} - 1}{q_k - 1},$$
$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1).$$

**Dôkaz.** Napred ukážeme, že prirodzené číslo $d$ je deliteľom čísla $n$ vtedy a len vtedy, keď má tvar

$$d = q_1^{\beta_1} . q_2^{\beta_2} \dots q_k^{\beta_k}, \tag{15}$$

kde $0 \leqq \beta_i \leqq \alpha_i$ $(i = 1, 2, \dots k)$. Ak $d$ má tvar (15), potom je zrejme deliteľom čísla $n$, vyplýva to ihneď zo zrejmej rovnosti

$$q_1^{\alpha_1} . q_2^{\alpha_2} \dots q_k^{\alpha_k} = (q_1^{\beta_1} . q_2^{\beta_2} \dots q_k^{\beta_k}) . (q_1^{\alpha_1 - \beta_1} . q_2^{\alpha_2 - \beta_2} \dots q_k^{\alpha_k - \beta_k}).$$

Obrátene, ak $d \mid n$, potom existuje prirodzené $n'$ tak, že $n = dn'$, teda $dn' = q_1^{\alpha_1} . q_2^{\alpha_2} \dots q_k^{\alpha_k}$. Z tejto rovnosti na základe **V**$_{10}$ vyplýva, že v prípade $d > 1$ v kanonickom rozklade čísla $d$ môžu vystupovať len prvočísla $q_i$ a to s exponentami nie väčšími než $\alpha_i$ $(i = 1, 2, \dots k)$. Teda $d > 1$ musí mať tvar (15). Ak $d = 1$, dostaneme ho z (15) pri $\beta_1 = \beta_2 = \dots = \beta_k = 0$.

Z vety **V**$_{10}$ vyplýva, že dve čísla

$$d = q_1^{\beta_1} . q_2^{\beta_2} \dots q_k^{\beta_k}, \; d' = q_1^{\beta'_1} . q_2^{\beta'_2} \dots q_k^{\beta'_k}$$

sú rôzne, ak existuje $i$ tak, že $\beta_i \neq \beta'_i$. Odtiaľ vyplýva, že všetkých prirodzených deliteľov čísla $n$ je práve toľko, koľko je rôznych $k$ — tic $(\beta_1, \beta_2, \dots \beta_k)$, $0 \leqq \beta_i \leqq \alpha_i$ $(i = 1, 2, \dots, k)$. Týchto $k$-tic je zrejme $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$, teda $\tau(n) = (\alpha_1 + 1).(\alpha_2 + 1) \dots (\alpha_k + 1)$.

Ďalej $\sigma(n)$ je rovno súčtu všetkých čísel (15) a tento súčet možno napísať vo tvare
$(1 + q_1 + q_1^2 + \ldots + q_1^{\alpha_1}).(1 + q_2 + q_2^2 + \ldots + q_2^{\alpha_2}) \ldots$
$(16) \ldots (1 + q_k + q_k^2 + \ldots + q_k^{\alpha_k})$.
Skutočne, ak v (16) vykonáme naznačené násobenie, objaví sa tam každé z čísel $d$ práve raz. Na základe vzorca pre geometrický súčet dostávame odtiaľ

$$\sigma(n) = \frac{q_1^{\alpha_1+1} - 1}{q_1 - 1} \cdot \frac{q_2^{\alpha_2+1} - 1}{q_2 - 1} \cdots \frac{q_k^{\alpha_k+1} - 1}{q_k - 1}$$

**P14.** Aký je počet všetkých prirodzených deliteľov čísla 100?

**P15.** Nájdite všetky tie prirodzené čísla $n$, pre ktoré je $\tau(n) = 2$, $\tau(n + 1) = 3$.

**Riešenie.** Z $\tau(n) = 2$ vyplýva, že $n$ je prvočíslo. Z $\tau(n + 1) = 3$ vyplýva zase, že $n + 1$ musí mať tvar $n + 1 = q^2$, $q$ je prvočíslo. Odtiaľ $n = (q - 1).(q + 1)$. Ak $q - 1 > 1$, potom $n$ nie je prvočíslo. Musí teda byť $q - 1 = 1$, $q = 2$, $n + 1 = 4$, $n = 3$. Obrátene $\tau(3) = 2$, $\tau(3 + 1) = \tau(4) = 3$.

**P16.** Nájdite prirodzené $n$, ak viete, že $3 \mid n$, $4 \mid n$, $\tau(n) = 14$.

**Riešenie.** Keďže $4 \mid n$, aj $2 \mid n$. Preto ak $n =$

$$q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_k^{\alpha_k}$$

je kanonický rozklad čísla $n$, musí byť $k \geq 2$. Ďalej $\tau(n) = 14 = 2.7 = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$. Pretože 2, 7 sú prvočísla, musí byť $k \leq 2$, teda $k = 2$, $n = q_1^{\alpha_1} \cdot q_2^{\alpha_2}$, $q_1 = 2$, $q_2 = 3$. Potom je buď $\alpha_1 + 1 = 2$, $\alpha_2 + 1 = 7$ alebo $\alpha_1 + 1 = 7$, $\alpha_2 + 1 = 2$. V prvom prípade $\alpha_1 = 1$, $n = 2.3^6$ a $n$ nie je deliteľné číslom 4. Musí teda byť $\alpha_1 + 1 = 7$, $\alpha_2 + 1 = 2$, $n = 2^6.3 = 192$. Obrátene pre $n = 192$ platí $3 \mid n$, $4 \mid n$, $\tau(n) = 14$.

**P17.** Vypočítajte $\sigma(100)$, $\sigma(128)$, $\sigma(45)$.

**P18.** Ak $a$, $b$ sú nesúdeliteľné prirodzené čísla, potom $\sigma(a.b) = \sigma(a).\sigma(b)$, $\tau(a.b) = \tau(a).\tau(b)$. Dokážte to!

Návod. Použite $\mathbf{V}_{11}$.

**P19.** Dokážte, že $\sigma(n) = n + 1$ vtedy a len vtedy, keď $n$ je prvočíslo!

**P20.** Dokážte, že pre každé zložené $n$ je $\sigma(n) \geqq \geqq 1 + \sqrt{n} + n$; pre nekonečne mnoho $n$ je $\sigma(n) = 1 + \sqrt{n} + n$ a tiež pre nekonečne mnoho $n$ je $\sigma(n) > 1 + \sqrt{n} + n$.

Návod. Nech $p$ je najmenší netriviálny deliteľ čísla $n$. Potom $n = pn_1, n > n_1 > 1$ a tak aj $n_1$ je netriviálny deliteľ čísla $n$. Z definície $p$ vyplýva $n_1^2 \geqq pn_1 = n$, $n_1 \geqq \sqrt{n}$. Pre $n = p^2$ ($p$ je prvočíslo) je $\sigma(n) = 1 + p + p^2 = 1 + \sqrt{n} + n$.

Pre $n = p^3$ ($p$ je prvočíslo) dostanete $\sigma(n) > 1 + \sqrt{n} + n$.

**P21.** Nájdite všetky tie prvočísla $p$, pre ktoré $\sigma(p)$ je druhou mocninou prirodzeného čísla!

**P22.** Dokážte, že rovnica s neznámou $x$ : $\sigma(x) = x + 1$ má nekonečne mnoho riešení a rovnica $\sigma(x) = x + k$ ($k$ je pevne zvolené prirodzené číslo $> 1$) má len konečný počet riešení v prirodzených $x$.

Návod. Použite $\mathbf{P}_{19}$, $\mathbf{P}_{20}$.