2. kapitola

DOKONALÉ A SPRIATELENÉ ČÍSLA

DOKONOLÉ ČÍSLA (PRVÉHO DRUHU)

Každé číslo $n > 1$ má aspoň dvoch deliteľov, a to čísla 1 a n, preto $\sigma(n) \geqq n + 1$. Ak skúmame veľkosť $\sigma(n)$ v porovnaní s dvojnásobkom čísla n, môžeme všetky prirodzené čísla $n > 1$ rozdeliť do troch množín, z ktorých žiadne dve nemajú spoločné prvky. Prvú množinu tvoria tie čísla $n > 1$, pre ktoré $\sigma(n) < 2n$. Tieto čísla nazývame *číslami deficientnými* (numeri deficientes). Sem patria všetky prvočísla, teda nekonečne veľa čísel patrí do tejto množiny. Druhú množinu tvoria tie čísla $n > 1$, pre ktoré $\sigma(n) > 2n$. Tieto čísla nazývame *číslami abundantnými* (numeri abundantes). Sem patria napr. všetky čísla tvaru $2^k.3$, kde $k > 1$. Naozaj, ak $n = 2^k.3$, $k > 1$, potom na základe $\mathbf{V}_{11}$

$$\sigma(n) = \frac{2^{k+1}-1}{2-1}\,\frac{3^2-1}{3-1} = (2^{k+1}-1).4 > 2.(2^k.3) =$$
$$= 2n.$$

Teda aj táto množina obsahuje nekonečne mnoho čísel. Konečne tretiu množinu tvoria tie čísla $n > 1$, pre ktoré $\sigma(n) = 2n$. Tieto čísla nazývame dokonalými, *perfektnými* (numeri perfecti), niekedy aj podrobnejšie *dokonalými číslami prvého druhu.*

Preskúmajme podrobnejšie podmienku $\sigma(n) = 2n$. Z tejto rovnosti dostávame $\sigma(n) - n = n$. Číslo $\sigma(n) - n$ sa zrejme rovná súčtu všetkých tých prirodzených deliteľov čísla $n > 1$, ktoré sú menšie než n. Takýchto deliteľov nazývame pravými deliteľmi čísla n. Teda ak $n > 1$ je dokonalé, potom sa rovná súčtu všetkých svojich pravých deliteľov. Obrátene, ak $n > 1$ je rovné súčtu všetkých svojich pravých deliteľov, potom $\sigma(n) - n = n$, odtiaľ $\sigma(n) = 2n$, teda n je dokonalé. Tým sme dokázali poučku.

V$_{12}$. Číslo $n > 1$ je dokonalé (prvého druhu) vtedy a len vtedy, keď sa rovná súčtu všetkých svojich pravých deliteľov.

Na základe V$_{12}$ možno teda dokonalé čísla (prvého druhu) definovať aj tak, že sú to tie čísla $n > 1$, ktoré sa rovnajú súčtu všetkých svojich pravých deliteľov.

Videli sme, že aj množina všetkých deficientných, aj množina všetkých abundantných čísel je nekonečná. Podobný výsledok nevieme dokázať o dokonalých číslach a nevieme ani dokázať, že všetkých dokonalých čísel je len konečne mnoho. Hoci pojem dokonalého čísla bol známy už *matematikom Pythagorovej školy* (6. st. pred n. l.) a *Euklidovi* (4. st. pred n. l.), dodnes poznáme len 23 dokonalých čísel. Najmenším z nich je číslo 6 ($= 1 + 2 + 3$). Najväčšie známe dokonalé číslo je $2^{11\,212}.(2^{11\,213} - 1)$. Toto číslo napísané v desiatkovej sústave má 6751 cifier.

Všetky dodnes známe dokonalé čísla sú párne, nepoznáme ani jedno nepárne dokonalé číslo a ani nevieme dokázať existenciu alebo neexistenciu takého čísla. Existuje početná skupina matematických viet, ktoré udávajú nutné podmienky k tomu, aby nepárne číslo bolo dokonalým. Ak ovšem nejaké nepárne číslo tieto podmienky splňa, ešte nemusí byť dokonalým. Už od *L. Eulera* (1707—1783) pochádza nasledujúca veta o nepárnych dokonalých číslach.

V$_{13}$. Ak $n > 1$ je nepárne dokonalé číslo, potom n musí mať tvar: $n = p^{4k+1}.N^2$, kde k je celé, $k \geqq 0$, p je prvočíslo tvaru $4s + 1$ ($s \geqq 1$) a N nie je deliteľné číslom p.

Dôkaz. Nech n je nepárne číslo > 1, nech n je dokonalé. Ak $n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_r^{\alpha_r}$ je kanonický rozklad čísla n, potom v dôsledku $\mathbf{V}_{3c}$ sú všetky prvočísla p_i ($i = 1, 2, \dots r$) nepárne. Keďže n je dokonalé, dostávame na základe vety $\mathbf{V}_{11}$

$$(14') \quad \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1} = 2n.$$

Uvážme, že čísla $\dfrac{p_i^{\alpha_i+1} - 1}{p_i - 1}$ ($i = 1, 2, \dots r$) sú celé. Keďže $2n$ je párne číslo, je aj súčin vľavo v (14′) párnym číslom a tak v dôsledku $\mathbf{V}_9$ existuje j tak, že $2 \mid \dfrac{p_j^{\alpha_j+1} - 1}{p_j - 1}$. Bez ujmy na všeobecnosti môžeme predpokladať, že $j = 1$. Ak by $2n$ bolo deliteľné číslom 4, vyplývala by odtiaľ deliteľnosť čísla n číslom 2. Preto $2n$ nie je deliteľné číslom 4 a tak ani ľavá strana v (14′) nie je deliteľná číslom 4. Z toho ľahko vyplýva, že čísla $\dfrac{p_i^{\alpha_i+1} - 1}{p_i - 1}$ ($i = 2, 3, \dots r$) musia byť nepárne. Uvážme, že $\dfrac{p_i^{\alpha_i+1} - 1}{p_i - 1} = 1 + p_i + p_i^2 + \dots + p_i^{\alpha_i}$.

Pretože p_i ($i = 2, 3, \dots r$) je nepárne, je aj každé z čísel p_i^n (n je prirodzené) nepárne a tak vpravo máme súčet $\alpha_i + 1$ nepárnych čísel. Pretože tento súčet je nepárnym číslom, musí byť počet sčítancov v ňom nepárny (pozri $\mathbf{V}_{3b}$) a tak $\alpha_i + 1 = 2l_i + 1$, odtiaľ $\alpha_i = 2l_i$($i = 2, 3, \dots r$). Položme $N = p_2^{l_2}.p_3^{l_3} \dots p_r^{l_r}$, potom N je zrejme nesúdeliteľné s $p_1^{\alpha_1}$ a $n = p_1^{\alpha_1}.N^2$.

Keďže $\dfrac{p_1^{\alpha_1+1}-1}{p_1-1} = 1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1}$ je párne, podobnou úvahou predošlej zistíme, že α_1 musí byť nepárne. Položme $\alpha_1 = 2l + 1$. Potom na základe známej už použitej identity $x^n - 1 = (x-1).(1 + x + x^2 + \ldots$ $\ldots + x^{n-1})$ dostaneme $\dfrac{p_1^{\alpha_1+1}-1}{p_1-1} = \dfrac{p_1^{2(l+1)}-1}{p_1-1} =$

$$= \frac{(p_1^2)^{l+1}-1}{p_1-1} = \frac{(p_1^2-1).(1+p_1^2+p_1^4+\ldots+p_1^{2l})}{p_1-1} =$$

$= (p_1+1).(1+p_1^2+p_1^4+\ldots+p_1^{2l})$.

Keďže p_1 je nepárne, vyplýva z V_3 ľahko, že p_1 musí mať tvar $4s + 1$ alebo $4s + 3$. Ak $p_1 = 4s + 3$ ($s \geq 0$), potom $p_1 + 1 = 4.(s + 1)$ je deliteľné číslom 4 a tak na základe (14″) aj $\dfrac{p_1^{\alpha_1+1}-1}{p_1-1}$ a potom aj $2n$ je deliteľné číslom 4. Musí teda p_1 mať tvar $p_1 = 4s + 1 (s \geq 1)$.

Ďalej

$$(14''') \qquad 1 + p_1^2 + p_1^4 + \ldots + p_1^{2l}$$

musí byť nepárne (inak by pravá a potom aj ľavá strana v (14″) bola deliteľná číslom 4). Keďže každý zpomedzi sčítancov v (14‴) je nepárny, musí byť počet sčítancov v (14‴) nepárne číslo (pozri V_{3b}). Teda $l + 1 = 2k + 1$, $1 + \dfrac{\alpha_1 - 1}{2} = 2k + 1$, $\alpha_1 = 4k + 1$, $k \geqq 0$. Tým je dôkaz vety skončený.

Dnes je už známe, že nepárne dokonalé čísla, ak vôbec existujú, majú tvar $12k + 1$ alebo $36k + 9$ ($k \geq 1$) a žiadne nepárne číslo menšie než 10^{20} nie je dokonalé.

Vráťme sa k párnym dokonalým číslam. Medzi klasické výsledky teorie čísel patrí nasledujúca veta, podľa ktorej možno rozhodovať, či dané párne číslo je dokonalé alebo nie.

V₁₄. Párne číslo $n > 1$ je dokonalé vtedy a len vtedy, keď má tvar $n = 2^{s-1}.(2^s - 1)$, kde s je prirodzené, $s > 1$ a $2^s - 1$ je prvočíslo.

Dôkaz. Nech n má uvedený tvar. Označme $p = 2^s - 1$. Potom $n = 2^{s-1}.p$ je kanonický rozklad čísla n a tak na základe V_{11} $\sigma(n) = \dfrac{2^s - 1}{2 - 1} \dfrac{p^2 - 1}{p - 1} =$

$$= (2^s - 1) \frac{(p-1)(p+1)}{p-1} = (2^s - 1).(p + 1) =$$

$= 2^s.p - p + 2^s - 1 = 2^s.p$, teda $\sigma(n) = 2(2^{s-1}.p) = 2n$, n je dokonalé.

Nech teraz obrátene, $n > 1$ je párne dokonalé číslo. Napred ľahko nahliadneme, že v kanonickom rozklade čísla n musí okrem prvočísla 2 vystupovať aj nejaké iné (teda nepárne) prvočíslo. Ak by tomu tak nebolo, potom by n malo tvar $n = 2^\alpha$, $\alpha \geqq 1$ a z predpokladu, že n je dokonalé, dostávame na základe V_{11}

$$\sigma(n) = \frac{2^{\alpha+1} - 1}{2 - 1} = 2n = 2^{\alpha+1},$$

odtiaľ $2^{\alpha+1} - 1 = 2^{\alpha+1}$ a to je zrejme nesprávna rovnosť. Teda kanonický rozklad čísla n musí mať tvar $n = 2^\alpha.p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \geqq 1$, α, $\alpha_i (i = 1, 2, \dots k)$ sú prirodzené čísla, $p_i (i = 1, 2, \dots k)$ sú nepárne prvočísla.

Položme $l = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k}$, potom $l > 1$, l je nepárne číslo. Ďalej položme $\alpha = s - 1$, potom $s = \alpha + 1 > 1$. Keďže n je dokonalé, pomocou V_{11} dostávame

$$\sigma(n) = \frac{2^s - 1}{2 - 1} \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} =$$
$$= (2^s - 1).\sigma(l) = 2^s.l,$$

keďže $\sigma(l) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$. Rovnosť

$$(17) \qquad (2^s - 1).\sigma(l) = 2^s.l$$

ukazuje, že 2^s delí súčin $(2^s - 1).\sigma(l)$. Z vety $\mathbf{V}_1$ vyplýva, že číslo 2^s je deliteľné len číslami $1, -1, \pm 2^r, 1 \leqq r \leqq s$. Pretože $2^s - 1$ je nepárne, ľahko odtiaľ vyplýva, že čísla 2^s a $2^s - 1$ sú nesúdeliteľné. Z fundamentálnej vety aritmetiky $\mathbf{V}_6$ vyplýva, že $2^s \mid \sigma(l)$. Preto existuje $q \geqq 1$ tak, že $\sigma(l) = 2^s . q$. Dosaďme za $\sigma(l)$ z poslednej rovnosti do (17), dostaneme po vykrátení číslom 2^s

$$(18) \qquad (2^s - 1) . q = l.$$

Odtiaľ ľahkou úpravou dostaneme

$$(19) \qquad 2^s . q = l + q,$$

teda

$$(20) \qquad \sigma(l) = l + q.$$

Číslo $l > 1$ je deliteľné číslom l a na základe (18) aj číslom q. Z rovnosti (19) vyplýva ($s > 1$!) $l \neq q$. (20) ukazuje, že číslo l nemôže mať iných prirodzených deliteľov, než sú l a q. Ak by totiž nejaké $d \geqq 1$, $d \neq l, q$, delilo l, potom by súčet všetkých prirodzených deliteľov čísla l bol aspoň rovný súčtu $l + q + d$ a to by viedlo ku sporu s (20). Teda l, q sú jedinými prirodzenými deliteľmi čísla l a tak l má práve dvoch rôznych prirodzených deliteľov. Preto l musí byť prvočíslo a $q = 1$. Z (18) potom dostávame $l = 2^s - 1$ a $n = 2^{s-1}.l = 2^{s-1}.(2^s - 1)$, kde $l = 2^s - 1$

je prvočíslo. Tým sme dokázali, že ak n je párne dokonalé číslo, potom n má tvar $2^{s-1}.(2^s - 1)$, kde $s > 1$ a $2^s - 1$ je prvočíslo. Tým je dôkaz vety skončený.

Na prvý pohľad sa zdá, že V_{14} nám umožňuje pohodlne hľadať párne dokonalé čísla. No nie je tomu tak, celá ťažkosť spočíva v tom, že v poučke V_{14} sa vyžaduje, aby $2^s - 1$ bolo prvočíslo. Použiteľnosť vety V_{14} vyžaduje riešiť túto otázku: Pre aké hodnoty $s > 1$ je $2^s - 1$ prvočíslo? Riešenie tejto otázky je veľmi ťažké, dodnes neuskutočnené. Čísla $M_s = 2^s - 1$ $(s = 1, 2, \ldots)$ nazývame *Mersennovými číslami* (M. Mersenne (1588—1648) bol francúzskym matematikom). Prvočísla tohoto tvaru nazývame Mersennovými prvočíslami. Ak s je zložené a napr. $s = k.l$, $1 < k < s$, $1 < l < s$, potom $2^s - 1 = 2^{kl} - 1 = (2^k)^l - 1$ odtiaľ vidieť, že $M_s = 2^s - 1$ je deliteľné číslom $a = 2^k - 1$, $1 < a < M_s$, takže M_s je zložené.

Teda M_s môže byť prvočíslom, len ak s je prvočíslo. Ale ani skutočnosť, že s je prvočíslo, nezaručuje, že M_s je prvočíslo. Tak pre $s = 2, 3, 5, 7$ je M_s prvočíslo (o tom sa čitateľ ľahko presvedčí), no $M_{11} = 2^{11} - 1 = 2047$ je zložené číslo, ako ukazuje rovnosť $2047 = 23.89$.

Teda problém hľadania párnych dokonalých čísel je v dôsledku V_{14} prevedený na veľmi ťažký problém hľadania Mersennových prvočísel. Dodnes poznáme len 23 Mersennových prvočísel a teda aj práve toľko párnych dokonalých čísel. Najväčšie známe Mersennovo prvočíslo je $M_{11\,213} = 2^{11\,213} - 1$ a to je aj súčasne najväčšie známe prvočíslo vôbec.

Existujú viaceré matematické postupy, ktoré slúžia k overovaniu toho, či $M_p = 2^p - 1$ (p je prvočíslo) je prvočíslo. Tieto postupy kladú obyčajne veľké nároky na zdĺhavé výpočty a preto predtým, než boli skonštruované moderné matematické počítacie stroje, nenachádzali väčšie uplatnenie. Pomocou niektorých týchto postupov možno vypracovať pre elektronkové počítacie stroje programy na overovanie prvočíselnosti čísel M_p, p je prvočíslo. Medzi takéto postupy patrí aj postup na overovanie prvočíselnosti Mersennových čísel, založený na tejto poučke, ktorú uvedieme bez dôkazu.

V15. Nech p je nepárne prvočíslo. Potom M_p je prvočíslom vtedy a len vtedy, keď M_p je deliteľom čísla μ_{p-1}, ktoré vypočítame pomocou tohoto (rekurentného) postupu: klademe $\mu_1 = 4$,

$$\mu_2 = \mu_1^2 - 2, \mu_3 = \mu_2^2 - 2, \ldots \mu_{p-1}^2 = \mu_{p-2} - 2.$$

Použitím matematických počítacích strojov bolo pomocou V_{15} zistené, že zpomedzi čísel M_p (p prvočíslo), $p < 12\,000$ sú prvočíslami tie a len tie čísla M_p, kde $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11\,213$. To je spolu 23 Mersennových prvočísel.

Existuje veľa hypotéz, ktoré sa týkajú dokonalých čísel. Väčšina z nich je doteraz nerozriešená. Tak napr. nie je ani dokázaná ani vyvrátená hypotéza, podľa ktorej existuje nekonečne mnoho dokonalých čísel. Iná taká hypotéza tvrdí, že ak $M_p = 2^p - 1$ je prvočíslo, potom aj $M_{M_p} = 2^{M_p} - 1 = 2^{2^p - 1} - 1$ je tiež prvočíslo. Bolo dokázané, že táto hypotéza je nesprávna. Číslo $M_{13} = 8191$ je totiž prvočíslo, no $M_{M_{13}} = 2^{8191} - 1$ je zložené. Dôkaz uvedeného tvrdenia o čísle $M_{M_{13}}$ bol uskutočnený na matematickom počítacom stroji pomocou poučky V_{15} a celý výpočet na stroji trval vyše 100 hodín. Poznamenajme, že i keď vieme, že $2^{8191} - 1$ je zložené číslo, nepoznáme doteraz žiadneho jeho netriviálneho deliteľa.

Pojem dokonalého čísla možno zovšeobecniť, ako ukazuje nasledujúca definícia.

D5. Nech $m > 1$. Hovoríme, že číslo $n > 1$ je m-násobne dokonalé, ak $\sigma(n) = mn$.

Teda dokonalé čísla sú práve tie čísla $n > 1$, ktoré sú dvojnásobne dokonalé.

Označme v ďalšom znakom Q_m množinu všetkých m-násobne dokonalých čísel. Je už známe, že ku každému m, $1 < m \leqq 8$ existuje aspoň jedno m-násobne dokonalé číslo. Teda každá z množín Q_m, $1 < m \leqq 8$ je neprázdna. Nie je známe, či podobné platí aj o množinách Q_m, $m > 8$.

K pojmu dokonalého čísla sa primyká aj pojem kvazi-dokonalého čísla.

D6. Číslo $n > 1$ sa nazýva kvazi-dokonalým, ak $\sigma(n) = 2n + 1$.

Poznamenajme, že dodnes nepoznáme ani jedno kvazi-dokonalé číslo.

P23. Dokážte, že $n > 1$ je kvazi-dokonalé vtedy a len vtedy, keď sa rovná súčtu všetkých svojich netriviálnych deliteľov.

P24. Nech $d_1, d_2, \dots d_s$ sú všetky delitele čísla $n > 1$, väčšie než 1. Dokážte, že n je dokonalé vtedy a len vtedy, keď

$$1 = \frac{1}{d_1} + \frac{1}{d_2} + \dots + \frac{1}{d_s}.$$

Návod. Uvážte, že ak d delí n, potom aj prirodzené číslo $\frac{n}{d}$ delí n.

P25. Dokážte: ak $n \in Q_3$ a $3 \nmid n$, potom $3n \in Q_4$.

Návod. Použite **P18**!

P26. Nech n, k sú prirodzené čísla. Nech $3n \in Q_{4k}$, $3 \nmid n$. Potom $n \in Q_{3k}$. Dokažte to!

Návod. Ako v **P25**.

P27. Dokažte: $120 \in Q_3$, $2^5 . 3^2 . 5 . 7 \in Q_4$.

P28. Ak $n \in Q_5$, potom n musí mať viac než päť roznych prvočíselných deliteľov. Dokážte to!

Riešenie. Ak $n = p_1^{\alpha_1} . p_2^{\alpha_2} \dots p_k^{\alpha_k}$ (kanonický rozklad), potom

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} < \frac{p_1^{\alpha_1+1}}{p_1 - 1} \cdots$$

(21) $$\cdots \frac{p_k^{\alpha_k+1}}{p_k - 1} = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \frac{p_1}{p_1 - 1} \cdots \frac{p_k}{p_k - 1}.$$

Nech $p_1 < p_2 < \dots < p_k$. Pretože $\frac{a}{a-1}$ sa zmenší, ak zväčšíme a a pretože $p_1 \geqq 2$, $p_2 \geqq 3$, $p_3 \geqq 5$, $p_4 \geqq 7$, $p_5 \geqq 11$, dostávame pri $k \geqq 5$ z (21)

$$\sigma(n) \leqq n \frac{2}{2-1} \frac{3}{3-1} \frac{5}{5-1} \frac{7}{7-1} \frac{11}{11-1} = \frac{77}{16} n < 5n.$$

DOKONALÉ ČÍSLA DRUHÉHO DRUHU

Dokonalými číslami (prvého druhu) sme nazvali tie čísla $n > 1$, ktoré sa rovnajú súčtu všetkých svojich pravých deliteľov. Nahradením slova „súčet" slovom „súčin" dochádzame k pojmu dokonalého čísla druhého druhu.

D7. Číslo $n > 1$ sa nazýva dokonalým číslom druhého druhu, ak sa rovná súčinu všetkých svojich pravých deliteľov.

Príkladom dokonalého čísla druhého druhu je číslo 6 (= 1. 2. 3.). Teda 6 je dokonalé číslo prvého i druhého druhu.

Zatiaľ čo dodnes nevieme, či množina všetkých dokonalých čísel prvého druhu je konečná a či nekonečná, je podobná otázka pre dokonalé čísla druhého druhu úplne zodpovedaná v nasledujúcej poučke.

V_{16}. Číslo $n > 1$ je dokonalé číslo druhého druhu vtedy a len vtedy, keď je buď treťou mocninou prvočísla alebo súčinom dvoch rôznych prvočísel.

Dôkaz. Ak $n = p^3$ alebo $n = p_1 . p_2$ (p, p_1, p_2 sú prvočísla, $p_1 \neq p_2$), potom v prípade $n = p^3$ sú pravými deliteľmi n čísla $1, p, p^2$, v prípade $n = p_1 . p_2$ čísla $1, p_1, p_2$, v oboch prípadoch vidieť, že n sa rovná súčinu všetkých svojich pravých deliteľov, teda n je dokonalé druhého druhu.

Nech obrátene $n > 1$ je dokonalé číslo druhého druhu. Ukážeme, že potom $n = p_1^3$ alebo $n = p_1 . p_2$, p_1, p_2 sú prvočísla, $p_1 \neq p_2$. Nech $n = p_1^{\alpha_1} . p_2^{\alpha_2} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla n. Položme $s = \tau(n)$, nech $d_1, d_2, \dots d_s$ sú všetky prirodzené delitele čísla n, nech $1 = d_1 < d_2 < \dots \dots < d_s = n$. Pretože n je dokonalé druhého druhu, je $n = d_1 . d_2 \dots d_{s-1}$. Ak násobíme túto rovnosť na oboch stranách číslom $n = d_s$, dostaneme

$$n^2 = d_1 . d_2 \dots d_s. \tag{22}$$

Uvážme, že spolu s číslom d, $d \mid n$ aj číslo $\frac{n}{d}$ delí n, preto $n = \frac{n}{d_1}, \frac{n}{d_2}, \dots \frac{n}{d_s} = 1$ sú (všetky) prirodzené delitele čísla n. Preto

$$n^2 = \frac{n}{d_1} \cdot \frac{n}{d_2} \dots \frac{n}{d_s}. \tag{23}$$

Ak vynásobíme (22), (23) dostaneme $n^4 = n^s$, odtiaľ $s = 4$. Teda ak n je dokonalé číslo druhého druhu, potom $\tau(n) = 4$. Vieme, že $\tau(n) = (\alpha_1 + 1) \dots (\alpha_k + 1)$ (pozri V_{11}). V každej zátvorke vpravo sa nachádza číslo ≥ 2. Ak by bolo $k > 2$, potom z predošlého by vyplývalo $\tau(n) \geq 2^3 = 8$. Keďže je $\tau(n) = 4 < 8$, musí byť $k \leq 2$, takže kanonickým rozkladom čísla n je buď $n = p_1^{\alpha_1} . p_2^{\alpha_2}$ alebo $n = p_1^{\alpha_1}$. Ak $n = p_1^{\alpha_1}$, potom z $\tau(n) = \alpha_1 + 1 = 4$ vyplýva $\alpha_1 = 3$, teda $n = p_1^3$. Ak $n = p_1^{\alpha_1} . p_2^{\alpha_2}$, potom z rovnosti $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) = 4$ vyplýva $\alpha_1 + 1 = 2$, $\alpha_2 + 1 = 2$, $\alpha_1 = \alpha_2 = 1$, teda $n = p_1 . p_2$, Tým je dôkaz vety skončený.

P29. Dokážte: Číslo $n > 1$ sa rovná súčinu všetkých svojich prirodzených deliteľov vtedy a len vtedy, keď n je prvočíslo.

P30. Ak n je zložené, potom súčin všetkých jeho prirodzených deliteľov je $\geq n^{\frac{3}{2}}$. Dokážte to!

Návod. Použite $\mathbf{P}_{20}$!

P31a). Nájdite také dokonalé číslo druhého druhu, ktoré je deliteľné číslom 7 a pre ktoré $\sigma(n) = 32$!

b) Dokážte, že 6 je jediné párne číslo, ktoré je dokonalým číslom prvého i druhého druhu!

Návod. Použite $\mathbf{V}_{14}$ a $\mathbf{V}_{16}$!

c) Dokážte, že neexistujú nepárne čísla, ktoré by boli súčasne dokonalé prvého i druhého druhu!

Návod. Použite $\mathbf{V}_{13}$ a $\mathbf{V}_{16}$!

SPRIATELENÉ ČÍSLA

D8. Dve prirodzené čísla a, b, $a \neq b$ nazývame spriatelenými, ak súčet všetkých pravých deliteľov čísla a sa rovná číslu b a súčet všetkých pravých deliteľov čísla b sa rovná číslu a.

Keďže súčet všetkých pravých deliteľov čísla $m > 0$

je $\sigma(m) - m$, sú a, b spriatelené, vtedy a len vtedy, keď $\sigma(a) - a = b$, $\sigma(b) - b = a$, teda vtedy a len vtedy, keď $\sigma(a) = \sigma(b) = a + b$.

Ak a, b sú spriatelené, potom množinu $\{a, b\}$ nazývame *dvojicou spriatelených čísel* a čísla a, b nazývame členmi tejto dvojice.

Už *Pythagorovi* (6. st. pred n. l.) bola známa dvojica $\{220, 284\}$ spriatelených čísel. Všetkými pravými deliteľmi čísla 220 sú čísla 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110 — ich súčet je 284 a všetkými pravými deliteľmi čísla 284 sú čísla 1, 2, 4, 7, 142 — ich súčet je 220.

Ďalšiu dvojicu spriatelených čísel objavil *P. Fermat* (1601—1665). Bola to dvojica $\{2^4.23.47, 2^4.1151\}$. Dvojicu $\{2^7.191.383, 2^7.73727\}$ spriatelených čísel objavil *R. Descartes* (1596—1650). Viac než 59 dvojíc spriatelených čísel našiel *L. Euler*. V 19. storočí bolo známych 66 dvojíc spriatelených čísel. Dnes poznáme už asi 390 takých dvojíc. Z najmenších členov pozostáva už uvedená dvojica $\{220, 284\}$.

Dodnes nevieme, či všetkých dvojíc spriatelených čísel je konečne a či nekonečne mnoho. Dodnes nepoznáme ani jednu takú dvojicu spriatelených čísel, ktorej jedným členom by bolo párne a druhým nepárne číslo. Doteraz uvedené príklady dvojíc spriatelených čísel sú také, že oba ich členy sú párne čísla. Poznáme dnes aj takú dvojicu spriatelených čísel, ktorej oba členy sú nepárne. Je to napr. dvojica $\{3^3.5.7.11, 3.5.7.139\}$. Dodnes nie je známa dvojica spriatelených čísel, ktorej členy by boli nesúdeliteľné. Bolo dokázané, že ak taká dvojica existuje, potom každý jej člen musí byť väčší než 10^{23} a súčin jej členov musí byť deliteľný viac než dvadsiatimi rôznymi prvočíslami.

V 9 st. n. l. udal arabský matematik *Thâbit ben Korrah* túto formulu pre hľadanie dvojíc spriatelených čísel.

V17. Ak $p = 3.2^{n-1} - 1$, $q = 3.2^n - 1$, $r = 9.2^{2n-1} - 1$

$(n > 1)$ sú prvočísla, potom $2^n.pq$ a $2^n.r$ sú spriatelené čísla.

Dôkaz. Za predpokladov vety na základe V_{11} dostávame

$$\sigma(2^n.pq) = (2^{n+1} - 1).(p + 1)(q + 1) = (2^{n+1} - 1).$$
$$.3.2^{n-1}.3.2^n = (2^{n+1} - 1).9.2^{2n-1}, \sigma(2^n.r) =$$
$$= (2^{n+1} - 1).(r + 1) = (2^{n+1} - 1).9.2^{2n-1},$$

$$\text{teda } \sigma(2^n.pq) = \sigma(2^n.r).$$

Ďalej

$$2^n.pq + 2^n.r = 2^n.(pq + r) = 9.2^{2n-1}.(2^{n+1} - 1),$$

teda

$$\sigma(2^n.pq) = \sigma(2^n.r) = 2^n.pq + 2^n.r.$$

Pre $n = 2$ dostávame z predošlej vety dvojicu $\{220, 284\}$ spriatelených čísel, podobne dostaneme aj pre $n = 4$ a $n = 7$ dvojice spriatelených čísel. Pre žiadne iné $n < 200$ nie je splnený predpoklad prvočíselnosti čísel p, q, r a pre žiadne $n < 200$, $n \neq 2, 4, 7$ predošlá formula nedáva dvojicu spriatelených čísel.

P_{32}. Dokážte: Ak $p \neq q$, p, q sú prvočísla, potom p^3, q^3 nie sú spriatelené čísla.

P_{33}. Pokúste sa zovšeobecniť tvrdenie z P_{32}. Na ostatné mocniny p^k, q^k $(k \neq 3)$ prvočísel p, q!

Návod. Postupujte v dôkaze nepriamo!

P_{34}. Dokážte, že dve rôzne dokonalé čísla druhého druhu, obe tvaru $p.q$, $p \neq q$, p, q nepárne prvočísla, nie sú spriatelené.

Riešenie. Nech $p_1 . q_1$, $p_2 . q_2$ sú dve dokonalé čísla druhého druhu, uvedeného tvaru. Nech napr.

$$q_2 = \max(p_1, q_1, p_2, q_2).$$

Z predpokladu $\sigma(p_1 . q_1) = \sigma(p_2 . q_2) = p_1 . q_1 + p_2 . q_2$ vyplýva $(p_1 + 1)(q_1 + 1) = p_1 . q_1 + p_2 . q_2$, odtiaľ dostaneme

(25) $$p_2q_2 = p_1 + q_1 + 1.$$

Na základe predpokladu vety je $p_1 \neq q_1$. Nech napr. $q_1 > p_1$, teda $q_1 \geq p_1 + 2$ a tak $p_2q_2 \geq 3q_2 > 2q_2 \geq 2q_1 \geq \geq p_1 + q_1 + 2$, teda $p_2q_2 > p_1 + q_1 + 2$ a to je vo spore s (25).

P35. Nech $a \in Q_m$, $b \in Q_k$, $a \neq b$. Nech b, m sú nesúdeliteľné. Dokážte, že potom a, b nie sú spriatelené!

Návod. Postupujte podobne ako v riešení **P34**.

Už z toho, čo sme doteraz povedali o dokonalých a spriatelených číslach sa dá vytušiť, že dokonalé a spriatelené čísla sú číslami veľmi vzácnymi. Túto domnienku potvrdzuje aj nasledujúci výsledok, ktorý podáme v trochu populárnej forme: Nech A značí ktorúkoľvek z nasledujúcich troch množín: množina všetkých dokonalých čísel prvého druhu, množina všetkých dokonalých čísel druhého druhu, množina všetkých spriatelených čísel. Potom A má túto vlastnosť: ak $\{1, 2, 3, \ldots n\}$ nazveme úsekom množiny všetkých prirodzených čísel a číslo n dĺžkou tohoto úseku, potom ku každému prirodzenému číslu m existuje také prirodzené číslo n_0, že všetky úseky, ktorých dĺžka n je väčšia než n_0 obsahujú menej než $\frac{n}{m}$ čísel patriacich do A. Tak teda napr. aj k číslu $m = 10^6$ existuje také n_0, že zpomedzi čísel $\{1, 2, \ldots n\}$, $n > n_0$ patrí do množiny A menej než $\frac{n}{10^6}$, teda menej než miliontina počtu týchto čísel. Stručne rečeno, všetky dosť dlhé úseky prirodzených čísel obsahujú menej čísel z množiny A než činí miliontina počtu ich prvkov. Podrobnejšie o týchto otázkach pohovoríme v tretej kapitole.