# VYBRANÉ KAPITOLY Z ELEMENTÁRNEJ TEÓRIE ČÍSEL II

ŠTEFAN ZNÁM, Bratislava

Tento článok priamo nadväzuje na časť I (pozri [4]) a budeme tu bez ďalšieho vysvetlenia používať tam dokázané vety.

## I. Číselné sústavy

V časti I sme sa zaoberali len deliteľnosťou prirodzených čísel; tu budeme musieť pojem deliteľnosti rozšíriť: hovoríme, že celé číslo $a$ je deliteľné celým číslom $b \neq 0$ ak existuje celé číslo $c$ tak, že platí $a = b \,.\, c$. Možno ukázať (podobne ako v [4] pre prirodzené čísla), že ku každej dvojici celých čísel $a$, $b$ existujú také nezáporné celé čísla $q$ a $z$, že platí

$$a = bq + z, \qquad 0 \leqq z < b.$$

Teraz nás bude zaujímať otázka, či číslami $a$ a $b$ sú už čísla $q$ a $z$ určené jednoznačne. Dokážeme, že áno. Predpokladajme, že platí

$$a = bq_1 + z_1, \qquad 0 \leqq z_1 < b; \tag{1}$$

$$a = bq_2 + z_2, \qquad 0 \leqq z_2 < b. \tag{2}$$

Bez újmy na všeobecnosti môžeme predpokladať, že $z_1 \geqq z_2$. Z (1) a (2) dostaneme

$$bq_1 + z_1 = bq_2 + z_2, \text{ čiže}$$

$$z_1 - z_2 = b(q_2 - q_1). \tag{3}$$

Z toho vyplýva $b \mid (z_1 - z_2)$, a preto $z_1 - z_2 = 0$ (ak by bolo $z_1 - z_2$ prirodzené, tak by platilo $b \leqq z_1 - z_2$, čo je spor s (1) a (2)). Preto $z_1 = z_2$, a tak z (3) vyplýva $b(q_1 - q_2) = 0$, a to je možné len vtedy, keď $q_2 = q_1$. Dokázali sme teda, že čísla $q$ a $z$ sú určené číslami $a$, $b$ jednoznačne.

Teraz sa budeme zaoberať otázkou vyjadriteľnosti prirodzených čísel v rôznych číselných sústavách. Iste nikto z čitateľov nepochybuje o tom, že každé prirodzené číslo $n$ sa dá vyjadriť v desiatkovej sústave, t. j. že sa dá písať v tvare

$$n = a_k \,.\, 10^k + \ldots + a_1 \,.\, 10 + a_0,$$

kde $a_i$ sú nezáporné celé čísla neprevyšujúce 9 (tzv. číslice alebo cifry desiatkovej sústavy).

To, že v matematike sa dnes používa hlavne desiatková sústava, má svoje historické odôvodnenie. Ale to je zároveň jediný argument v prospech desiatkovej sústavy! Ináč by sme takisto dobre pochodili s akoukoľvek inou sústavou (dokonca dvojková sústava by bola z niektorých hľadísk oveľa výhodnejšia). A tak vzniká otázka, či každé prirodzené číslo $n$ možno vyjadriť v ľubovoľnej $g$-adickej sústave ($g$ prirodzené), t. j. vyjadriť v tvare

$$n = a_k \cdot g^k + \ldots + a_1 \cdot g + a_0, \tag{4}$$

kde $a_i$ sú nezáporné celé čísla neprevyšujúce $g - 1$ (pričom $a_k \neq 0$). Čísla $a_i$ nazývame číslicami (ciframi) $g$-adickej sústavy. Možnosť takého vyjadrenia už nie je taká samozrejmá! Ak $g = 1$ tak sa v tvare (4) nedá vyjadriť nijaké prirodzené číslo (lebo číslice neprevyšujú $g - 1$; teda sú nuly). Ináč platí veta:

**Veta 1.** Ak $g > 1$ je prirodzené číslo, tak každé prirodzené číslo možno vyjadriť v $g$-adickej sústave jediným spôsobom.

Dôkaz. Budeme dokazovať v dvoch krokoch.

a) Najprv dokážeme, že každé prirodzené číslo možno vyjadriť v tvare (4). Budeme to dokazovať indukciou. Pre $n = 1$ ($g > 1$) je tvrdenie zrejme pravdivé. Predpokladajme, že tvrdenie je pravdivé pre všetky prirodzené čísla menšie ako $n$ a dokážeme, že je pravdivé aj pre $n$. Existujú nezáporné celé čísla $b$ a $c$ tak, že

$$n = g \cdot b + c, \qquad 0 \leqq c < g.$$

Ak $b = 0$, tak $n = c < g$ a môžeme položiť $k = 0$, $a_0 = c = n$. Nech $b \neq 0$. Číslo $b$ je menšie ako $n$, a tak na základe indukčného predpokladu $b$ sa dá vyjadriť v tvare (4):

$$b = d_s \cdot g^s + \ldots + d_1 \cdot g + d_0,$$

kde $d_i$ sú nezáporné celé čísla neprevyšujúce $g - 1$ a $d_s \neq 0$. Dostávame

$$n = g \cdot b + c = g(d_s \cdot g^s + \ldots + d_1 \cdot g + d_0) + c = d_s \cdot g^{s+1} + \ldots + \\ + d_1 \cdot g^2 + d_0 \cdot g + c.$$

Ak teraz položíme $a_0 = c$, $a_i = d_{i-1}$ pre $i = 1, 2, \ldots, s + 1$, dostaneme vyjadrenie čísla $n$ v žiadanom tvare.

b) Dokážeme, že $n$ sa dá len jedným spôsobom vyjadriť v tvare (4). Budeme to dokazovať znova indukciou. Pre $n = 1$ je tvrdenie pravdivé (pozri cvičenie 3). Predpokladajme, že je pravdivé pre všetky prirodzené čísla menšie ako $n$ a dokážeme, že potom je pravdivé aj pre $n$. Nech by pre $n$ existovali dve vyjadrenie žiadaného tvaru:

$$n = e_r \cdot g^r + \ldots + e_1 \cdot g + e_0,$$

$$n = f_p \cdot g^p + \ldots + f_1 \cdot g + f_0$$

ktorých koeficienty vyhovujú daným podmienkam. Po úprave máme

$$n = g(e_r \,.\, g^{r-1} + \ldots + e_1) + e_0 = g \,.\, E + e_0,$$

$$n = g(f_p \,.\, g^{p-1} + \ldots + f_1) + f_0 = g \,.\, F + f_0.$$

Nakoľko $e_0$ a $f_0$ sú nezáporné celé čísla neprevyšujúce $g - 1$, z úvah na začiatku tohto článku vyplýva, že $e_0 = f_0$ a $E = F$. Avšak $E < n$ a tak na základe indukčného predpokladu $E$ sa dá jediným spôsobom vyjadriť v tvare (4), preto $r = p$, $e_i = f_i$ pre $i = 1, 2, \ldots, r$. Teda aj pre číslo $n$ existuje jediné vyjadrenie v tvare (4), a tým je dôkaz vety ukončený.

Teraz na jednom príklade ukážeme ako možno nájsť vyjadrenie nejakého čísla v $g$-adickej sústave.

*Príklad 1.* Vyjadrite číslo 1973 (je zapísané v desiatkovej sústave) v sedmičkovej sústave.

$$1973 : 7 = 281\ldots$$
$$6$$

Môžeme teda písať: $1973 = 7 \,.\, 281 + 6$. Preto už hneď môžeme vyhlásiť, že $a_0 = 6$ (prečo?). Ďalej:

$$281 : 7 = 40\ldots, \quad \text{čiže} \quad 281 = 7 \,.\, 40 + 1.$$
$$1$$

Dostávame: $1973 = 7 \,.\, 281 + 6 = 7(7 \,.\, 40 + 1) + 6 = 7^2 \,.\, 40 + 7 \,.\, 1 + 6$, a tak $a_1 = 1$. Pokračujme:

$$40 : 7 = 5, \qquad 40 = 7 \,.\, 5 + 5.$$
$$5$$

A tak dostávame konečný výsledok $1973 = 7^2(7 \,.\, 5 + 5) + 7 \,.\, 1 + 6 = 5 \,.\, 7^3 + 5 \,.\, 7^2 + 1 \,.\, 7 + 6$.

My sme zvyknutí v desiatkovej sústave používať skrátený zápis: namiesto

$$a_k \,.\, 10^k + \ldots + a_1 \,.\, 10 + a_0$$

píšeme jednoducho $a_k a_{k-1} \ldots a_1 a_0$ (napríklad namiesto $1 \,.\, 10^3 + 9 \,.\, 10^2 + 7 \,.\, 10 + 3$ píšeme 1973). Podobné možno realizovať aj v iných číselných sústavách. Napríklad naše číslo 1973 by sme v sedmičkovej sústave mohli písať ako 5516. Aby sme vedeli o aké číslo vlastne ide, musíme mať informáciu o tom, v akej sústave je vyjadrené. My to budeme riešiť tak, že vpravo dolu od čísla napíšeme číslo $g$ (ak je to vyjadrenie v $g$-adickej sústave). Napríklad $1973_{10}$ znamená, že to číslo chápeme vyjadrené v desiatkovej sústave a $5516_7$ znamená, že ide o číslo v sedmičkovej sústave. Z dôvodov prehľadnosti používame v každej $g$-adickej sústave číslice (cifry) $0, 1, \ldots, g - 1$. Ak $g > 10$ tak budeme mať aj také číslice, ktorých vyjadre-

nie v desiatkovej sústave je viacciferné — také dávame do zátvoriek. Napríklad číslo $2(11)8_{13}$ znamená $2 \,.\, 13^2 + 11 \,.\, 13 + 8$ (vystupuje tu číslica 11).

Cvičenia*)

**1.** Dokážte, že 0 je deliteľná každým nenulovým celým číslom.

**2.*** Dokážte: nech $a$, $b$ sú ľubovoľné celé čísla, potom existuje dvojica celých čísel $q$ a $r$ tak, že $a = b \,.\, q + r$, kde $0 \leqq r < b$.

**3.** Dokážte, že číslo 1 sa dá jediným spôsobom vyjadriť v tvare (4) pre ľubovoľné $g > 1$.

**4.** Vedeli by ste povedať, prečo číslo 1 nemôžeme voliť za základ číselnej sústavy?

**5.** Vyjadrite číslo $289_{10}$ v dvojkovej sústave.

**6.** Vyjadrite číslo $7\,842_{10}$ v trinástkovej sútave.

**7.** Vedeli by ste postup opísaný v príklade 1 zovšeobecniť na vyjadrenie akéhokoľvek čísla v $g$-adickej sústave, kde $g$ je ľubovoľné prirodzené číslo väčšie ako 1?

**8.** Vyjadrite číslo $23\,057_8$ ($a$) v desiatkovej sústave ($b$) v dvojkovej sústave.

**9.** Vyjadrite číslo $1011011_2$ v desiatkovej sústave a v sedmičkovej sústave.

**10.** Vyjadrite číslo $1(12)1(10)_{13}$ v dvojkovej sústave.

**11.*** Určte číslo $n$, pre ktoré platí:

$$n = (a_1a_0)_9 = (a_0a_1)_{10}.$$

**12.*** Určte číslo $n$, pre ktoré platí:

$$n = (a_1a_0)_{10} = (a_1a_02)_3.$$

## II. Deliteľnosť v rôznych číselných sústavách

Sú dobre známe pravidlá deliteľnosti prirodzených čísel dvoma, troma, štyrmi, piatimi, šiestimi atď. Tieto pravidlá sú zviazané s číslicami daného čísla v desiatkovej sústave, a preto v iných sústavách neplatia. Napríklad číslo $35_9$ je deliteľné dvoma ale nie je deliteľné piatimi (je to číslo $32_{10}$). Naším cieľom v tomto odseku bude odvodiť niektoré pravidlá deliteľnosti, ktoré možno aplikovať v každej číselnej sústave. K tomu budeme používať nasledujúce dve pomocné vety.

**Lema 1.** Pre ľubovoľné prirodzené čísla $m$ a $k$ platí

$$m \mid [(m + 1)^k - 1].$$

Dôkaz. Vychádzajúc zo známeho rozkladu pre $a^k - b^k$ dostaneme (položiac $a = m + 1$, $b = 1$):

$$(m + 1)^k - 1 = m(m^{k-1} + \ldots + m + 1).$$

*) Náročnejšie príklady sú v tejto práci označené hviezdičkou pri čísle príkladu.

**Lema 2.** Pre ľubovoľné prirodzené $m$ platí:

a) ak $k$ je nepárne, tak $m \mid [(m-1)^k + 1]$,

b) ak $k$ je párne, tak $m \mid [(m-1)^k - 1]$.

Dôkaz je veľmi podobný dôkazu lemy 1 (pozri cvičenie 1).

Teraz dokážeme vetu, ktorá je zovšeobecnením známeho pravidla o deliteľnosti deviatimi.

**Veta 2.** Prirodzené číslo

$$n = a_r \ldots a_1 a_{0g} (g > 1)$$

je deliteľné číslom $g - 1$ vtedy a len vtedy, keď (tzv. číslicový súčet — ciferný súčet čísla $n$, t. j.) číslo

$$m = a_r + \ldots + a_1 + a_0$$

je deliteľné číslom $g - 1$.

Dôkaz. Na základe lemy 1 pre všetky $i = 1, \ldots, r$ platí $g - 1 \mid g^i - 1$, čiže $g^i = 1 + x_i(g-1)$ (kde $x_i$ sú prirodzené čísla), a tak môžeme písať:

$$n = a_r \cdot g^r + \ldots + a_1 \cdot g + a_0 = a_r[1 + x_r(g-1)] + \ldots + a_1[1 + x_1(g-1)] + a_0 = (g-1)(a_r x_r + \ldots + a_1 x_1) + a_r + \ldots + a_1 + a_0 = K(g-1) + m.$$

Máme teda rovnosť $n = K(g-1) + m$. Z tejto rovnosti na základe vety 2 časti I vyplýva: ak $g - 1 \mid m$, tak $g - 1 \mid n$. Podobne sa dá dokázať: ak $g - 1 \mid n$, tak $g - 1 \mid m$ (pozri cvičenie 2). Tým je dôkaz vety ukončený.

*Poznámka.* Ak zoberieme $g = 10$, tak dostaneme známe pravidlo: v desiatkovej sústave zapísané číslo je deliteľné deviatimi vtedy a len vtedy, keď je deviatimi deliteľný súčet jeho číslic.

*Príklad 2.* Zistite, či je šiestimi deliteľné číslo $54063_7$.

Podľa vety 2 je toto číslo deliteľné šiestimi (teda číslom $g - 1$) vtedy a len vtedy, keď je šiestimi deliteľný súčet číslic $5_7 + 4_7 + 0_7 + 6_7 + 3_7 = 24_7$. Ešte raz aplikujeme vetu 2: $24_7$ je deliteľné šiestimi pretože $2_7 + 4_7 = 6_7$. Môžeme teda vyhlásiť, že aj číslo $54063_7$ je deliteľné šiestimi.

**Veta 3.** Prirodzené číslo

$$n = a_r \ldots a_1 a_{0\,g}$$

je deliteľné číslom $g + 1$ práve vtedy, keď číslo

$$m = (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots)$$

je deliteľné číslom $g + 1$.

Dôkaz. Na základe lemy 2 pre párne čísla $i$ platí $g + 1 \mid g^i - 1$, čiže môžeme písať $g^i = 1 + s_i(g+1)$ a pre nepárne $i$ je $g + 1 \mid g^i + 1$, a tak možno písať $g^i = -1 + s_i(g+1)$. Tak dostávame:

$$n = a_r \cdot g^r + \ldots + a_1 \cdot g + a_0 = a_0 + a_1[-1 + s_1(g + 1)] +$$
$$+ a_2[1 + s_2(g + 1)] + \ldots = (g + 1)(a_1 s_1 + a_2 s_2 + \ldots + a_r s_r) +$$
$$+ (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) = K(g + 1) + m.$$

Ďalej môžeme postupovať podobne ako v dôkaze vety 2.

*Príklad 3.* Zistite, ktoré z čísel 56 742, 89 441, 345 180 je deliteľné jedenástimi (čísla sú zapísané v desiatkovej sústave, a preto — tak ako sme to zvykli robiť — označenie sústavy neuvádzame).

Číslo 56 742 nie je deliteľné jedenástimi, lebo $(2 + 7 + 5) - (4 + 6) = 4$ nie je deliteľné jedenástimi. Číslo 89 441 je deliteľné 11, lebo $1 + 4 + 8 - 4 - 9 = 0$. Ľahko sa možno presvedčiť, že môžeme vždy postupovať tak, ako to teraz ukážeme (z počtárskeho hľadiska je to najrýchlejší spôsob): $0 - 8 + 1 - 5 + 4 - 3 = -11$, a tak číslo 345 180 je deliteľné jedenástimi.

Cvičenia

1. Dokážte lemu 2.
2. Dokážte: ak $g - 1 | n$ tak $g - 1 | m$ (pozri dôkaz vety 2).
3. Dokážte vetu 3.
4. Zistite či je deliteľné šiestimi a ôsmimi číslo $121243_7$.
5. Zistite, či je ôsmimi a desiatimi deliteľné číslo $7736_9$.
6. Ako zistíme o nejakom čísle zapísanom v $g$-adickej sústave, či je deliteľné číslom $g$?
7. Nech $p|g$. Nájdite pravidlo, kedy nejaké číslo zapísané v $g$-adickej sústave je deliteľné číslom $p$ (špeciálnym prípadom tohto pravidla sú pravidlá deliteľnosti dvoma a piatimi v desiatkovej sústave).
8. Vedeli by ste nájsť nejaké ďalšie pravidlo platné v každej číselnej sústave?

## 3. Úloha o minimálnom počte závaží

Je dobre známa nasledujúca úloha: aký minimálny počet závaží postačí na odváženie každej (celistvej) váhy od 1 do $K$ kilogramov, pričom závažia možno klásť len na jednu misku (ak je dovolené klásť závažie aj na druhú misku, vzniká iná — trocha ťažšia — varianta úlohy). Pri riešení našej úlohy teraz uplatníme naše znalosti o vyjadriteľnosti celých čísel v dvojkovej sústave.

**Veta 4.** Závažiami váhy 1, 2, ..., $2^{n-1}$ kilogramov možno odvážiť každú váhu do $2^n - 1$ kilogramov. Menej ako $n$ závaží na túto úlohu nestačí.

Dôkaz. Najprv dokážeme prvé tvrdenie. Každé prirodzené číslo $m$ sa dá vyjadriť v dvojkovej sústave (veta 1) takto

$$m = a_s \cdot 2^s + \ldots + a_1 \cdot 2 + a_0.$$

Ak $m \leqq 2^n - 1$ tak zrejme $s < n$ (pozri cvičenie 1). Každá číslica sa môže rovnať 0 alebo 1 (to sú jediné číslice v dvojkovej sústave). Teda $m$ sa dá vlastne vyjadriť ako súčet nejakých rôznych čísel tvaru $2^i (0 \leqq i \leq n - 1)$, a to znamená, že váha $m$ kilogramov sa dá vyjadriť ako súčet nejakých závaží váhy $2^i (0 \leqq i \leqq n - 1)$ kilogramov. Tým je tvrdenie (prvé) dokázané.

Pomocou $t$ závaží však možno vyjadriť najviac $2^t - 1$ rôznych váh (pozri cvičenie 2), a tak je správne aj druhé tvrdenie.

Táto veta rieši nastolenú úlohu len pre $K$ tvaru $2^t - 1$. Pomocou nej však ľahko možno dokázať nasledujúcu vetu, dávajúcu úplnú odpoveď na položenú otázku.

**Veta 5.** Ak $2^{n-1} \leqq K < 2^n$, tak na odváženie všetkých váh od 1 do $K$ kilogramov je potrebné (a stačí) $n$ závaží.

Dá sa dokázať aj to, že v prípade $N = 2^n - 1$ úlohe vyhovuje jediná sada závaží: $1, 2, 2^2, \ldots, 2^{n-1}$. V prípade $K < 2^n - 1$ však sada nie je jednoznačne určená.

*Príklad 4.* Ak $K = 40$, tak (nijakých 5 závaží nestačí!) závažiami 1, 2, 4, 8, 16, 32 možno odvážiť všetky váhy od 1 do 40 kilogramov (to vyplýva z vety 5), ale možno to urobiť aj pomocou závaží 1, 2, 4, 8, 16, 9. Skutočne (po 31 je to zrejme pravda: pozri vetu 4): $32 = 16 + 9 + 4 + 2 + 1$, $33 = 16 + 9 + 8, \ldots, 40 = 16 + 9 + 8 + 4 + 2 + 1$.

Ak zoberieme sadu $t$ závaží, v ktorej sa vyskytujú aj rovnaké závažia (v praxi je to častý jav; mnohokrát sa stretávame napríklad so sadou 1, 1, 2, 5), tak pomocou nich možno odvážiť len menší počet rôznych váh ako $2^t - 1$ (napríklad pomocou vyššie uvedenej sady 1, 1, 2, 5 možno odvážiť len váhy $1, 2, \ldots, 9$).

Ak zase zoberieme nejakú sadu $h$ rôznych závaží, ale líšiacu sa od sady $1, 2, \ldots, 2^{h-1}$, tak sa môže stať, že pomocou nich možno odvážiť $2^h - 1$ rôznych váh, ale nebudú to za sebou nasledujúce váhy $1, 2, 3, \ldots, 2^h - 1$. Napríklad, pomocou sady 1, 2, 5 možno odvážiť $2^3 - 1 = 7$ rôznych váh 1, 2, 3, 5, 6, 7, 8, ale chýba tam 4.

Cvičenia

**1.** Dokážte (dôkaz vety 4): ak $m \leqq 2^n - 1$, tak $s < n$.

**2.** Indukciou dokážte: Pomocou $h$ závaží možno odvážiť najviac $2^h - 1$ rôznych váh.

**3.** Dokážte vetu 5.

**4.** Pomocou závaží $1, 2, \ldots 2^{n-1}$ sa dá každá váha od 1 do $2^n - 1$ odvážiť jedinou skupinou závaží. (Návod: ku každej skupine závaží možno priradiť vyjadrenie nejakého prirodzeného čísla v dvojkovej sústave; ďalej použi vetu 1).

## 4. Kanonický rozklad prirodzených čísel

Každé prirodzené číslo $n > 1$ je deliteľné aspoň dvoma rôznymi prirodzenými číslami — jednotkou a sebou samým. Čísla, ktoré okrem spomínaných nemajú ďalšie prirodzené delitele, nazývame prvočíslami. Prvočíslami sú napríklad čísla 2, 3, 37, 97, ... Prirodzené číslo $n > 1$, ktoré nie je prvočíslom, nazývame zloženým číslom. Zložené čísla sú napríklad 4, 6, 100, ... Číslo 1 nepovažujeme ani za zložené číslo, ani za prvočíslo.

**Veta 6.** Nech $p$ je prvočíslo a nech $p \mid ab$. Potom buď $p \mid a$, buď $p \mid b$.

Dôkaz. Pretože $p$ je prvočíslo, môžu nastať len dva prípady: $p \mid a$ — vtedy nemáme čo dokazovať, alebo $(p, a) = 1$. V druhom prípade na základe vety 9 časti I platí $p \mid b$.

**Veta 7.** Každé zložené číslo sa dá písať v tvare súčinu prvočísel.

Dôkaz. Budeme dokazovať indukciou. Najmenšie zložené číslo je 4, pre ktoré platí $4 = 2 \,.\, 2$ — čiže tvrdenie je správne. Predpokladajme, že tvrdenie je pravdivé pre všetky zložené čísla menšie ako $n$. Keď $n$ je zložené číslo, možno ho napísať v tvare $n = a \,.\, b$, kde $1 < a < n$, $1 < b < n$. Číslo $a$ je buď prvočíslo, buď zložené číslo menšie ako $n$, a tak podľa indukčného predpokladu ho možno napísať vo tvare súčinu prvočísel. To isté platí aj o $b$, a tak aj $n$ možno písať v tvare súčinu prvočísel (lebo je súčinom $a$ a $b$).

Veta 7 tvrdí, že každé zložené číslo možno napísať v tvare $n = p_1 p_2 \dots p_k$, kde $p_i$ sú prvočísla; nie je však povedané, že $p_i$ sú rôzne prvočísla. Ony sa v skutočnosti aj môžu navzájom rovnať. Ak prvočísla $p_i$ usporiadame podľa veľkosti a rovnaké zhrnieme do jedného činiteľa, dostaneme vyjadrenie

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

kde $p_i$ sú rôzne prvočísla a $\alpha_i$ sú prirodzené čísla. Takéto vyjadrenie nazývame kanonickým rozkladom prirodzeného čísla $n$ na prvočinitele.

**Veta 8.** (Základná veta aritmetiky). Každé prirodzené číslo $n > 1$ sa dá jediným spôsobom vyjadriť v tvare

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \tag{5}$$

kde $p_1 < p_2 < \dots < p_k$ sú prvočísla a $\alpha_1, \dots, \alpha_k$ sú prirodzené čísla.

Dôkaz. Možnosť takého vyjadrenie pre zložené čísla sme ukázali vyššie. Ak $n$ je prvočíslo, tak stačí položiť $k = 1$, $p_1 = n$, $\alpha_1 = 1$.

Musíme ešte ukázať, že pre každé prirodzené číslo existuje jediné také vyjadrenie. Predpokladajme, že pre nejaké $n$ existujú dve vyjadrenia v kanonickom tvare:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

$$n = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s},$$

kde $p_1 < p_2 < \dots < p_k$, $q_1 < q_2 < \dots < q_s$ sú prvočísla a $\alpha_1, \dots, \alpha_k$ a $\beta_1, \dots, \beta_s$ sú prirodzené čísla. Potom

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}.$$

Pre každé $i$ je teda

$$p_i \mid q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}. \tag{6}$$

Z toho už na základe vety 6 (pozri cvičenie 2) vyplýva, že existuje také $j$, že $p_i \mid q_j$, a teda (pretože $p_i$ a $q_j$ sú prvočísla) $p_i = q_j$. To je ale možné len vtedy, keď $s \geqq k$. Podobne: pre všetky $q_j$ existuje také $p_i$, že $q_j = p_i$, a preto $k \geqq s$. Z tých dvoch nerovníc potom vyplýva $s = k$. Pretože $p_i$ a $q_j$ sú usporiadané podľa veľkosti, môžeme vyhlásiť, že

$$p_1 = q_1, \dots, p_k = q_k.$$

Musíme ešte ukázať, že $\alpha_i = \beta_i$ pre $i = 1, 2, \dots, k$. To dokážeme nepriamo. Predpokladajme napríklad, že $\alpha_i > \beta_i$. Potom z rovnosti (6) (a z rovnosti $s = k$) po vydelení číslom $p_i^{\beta_i}$ dostaneme

$$p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_i^{\alpha_i - \beta_i} p_{i+1}^{\alpha_{i+1}} \dots p_k^{\alpha_k} = p_1^{\beta_1} \dots p_{i-1}^{\beta_{i-1}} p_{i+1}^{\beta_{i+1}} \dots p_k^{\beta_k}.$$

Číslo $\alpha_i - \beta_i > 0$, a preto ľavá strana poslednej rovnosti je deliteľná prvočíslom $p_i$, ale pravá nie (pozri cvičenie 2), a to je spor.

Podobne by sme postupovali v prípade $\beta_i > \alpha_i$, takže pre všetky $i = 1, \dots, k$ platí $\alpha_i = \beta_i$. To ale znamená, že každé dve vyjadrenia čísla $n$ v kanonickom tvare sú totožné, a tak ľubovoľné $n$ sa dá vyjadriť v tvare (5) jediným spôsobom. Tým je dôkaz vety ukončený.

Cvičenia

1. Vymenujte všetky párne prvočísla.

2. Na základe vety 6 dokážte: nech $p, q_1, \dots, q_k$ sú prvočísla, $\alpha_1, \dots, \alpha_k$ prirodzené čísla; potom zo vzťahu $p \mid q_1^{\alpha_1} \dots q_k^{\alpha_k}$ vyplýva, že existuje také $i$ pre ktoré platí $p = q_i$.

3. Napíšte číslo 6000 v tvare súčinu prvočísel.

4. Nájdite kanonický rozklad čísla 6000.

5. Nech $n$ je prirodzené číslo väčšie ako 1 a nech $p$ je jeho najmenší deliteľ rôzny od 1. Potom $p$ je prvočíslo. Dokážte!

6. Ak $p$ a $g$ sú prvočísla, potom buď $p = q$, buď $(p, q) = 1$.

## 5. Aritmetické funkcie

Nech kanonický rozklad prirodzeného čísla $n$ je

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Skúmajme čísla tvaru

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \tag{7}$$

kde $\beta_i$ sú celé čísla vyhovujúce nerovnostiam

$$0 \leqq \beta_i \leqq \alpha_i .$$

Každé číslo tvaru (7) je deliteľom čísla $n$. Skutočne:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = (p_1^{\beta_1} p_2^{\beta_3} \dots p_k^{\beta_k})\, p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \dots p_k^{\alpha_k-\beta_k} =$$
$$= d(p_1^{\alpha_1-\beta_2} p_2^{\alpha_2-\beta_2} \dots p_k^{\alpha_k-\beta_k}),$$

pričom $p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \dots p_k^{\alpha_k-\beta_k}$ je prirodzené číslo, a tak $d \mid n$.

Podobnými úvahami ako v dôkaze vety 8 možno ukázať, že každý deliteľ čísla $n$ má tvar (7) (pozri cvičenie 1).

*Príklad 3.* Nájdite všetky delitele čísla 72.

Kanonický rozklad je $72 = 2^3 3^2$. Teda delitele čísla 72 budú práve čísla tvaru

$$2^\alpha \,.\, 3^\beta,$$

kde $\alpha = 0, 1, 2, 3$, $\beta = 0, 1, 2$. Delitele zhrnieme v tabuľke

| $\alpha$ | 0 | 1 | 2 | 3 | 0 | 1 | 2 | 3 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\beta$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 |
| $d$ | 1 | 2 | 4 | 8 | 3 | 6 | 12 | 24 | 9 | 18 | 36 | 72 |

Nech $n$ je prirodzené číslo. Označme symbolom $D(n)$ počet všetkých deliteľov čísla $n$. Napríklad $D(6) = 4$ (deliteľmi sú 1, 2, 3, 6), $D(72) = 12$.

**Veta 9.** Ak $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ (kanonický rozklad), tak

$$D(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1).$$

Dôkaz. Všetky delitele čísla $n$ sú tvaru (7), pričom $0 \leqq \beta_i \leqq \alpha_i$ pre všetky $i = 1, 2, \dots, k$. Teda exponent $\beta_1$ môžeme voliť $\alpha_i + 1$ spôsobmi (sú to: $0, 1, \dots, \alpha_1$). Nezávisle od výberu $\beta_1$, exponent $\beta_2$ možno voliť $\alpha_2 + 1$ spôsobmi ($0, 1, \dots \alpha_2$) atď., exponent $\beta_k$ (nezávisle od voľby predchádzajúcich) možno voliť $\alpha_k + 1$ spôsobmi. Dá sa vybrať teda celkove

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

rôznych $k$-tíc exponentov $(\beta_1, \beta_2, \dots, \beta_k)$. Podobnou úvahou ako v dôkaze vety 8 možno ukázať, že dvom rôznym $k$-ticiam exponentov zodpovedajú rôzne delitele čísla $n$. Takto dostaneme zrejme všetky delitele.

*Príklad 4.* Určte počet všetkých deliteľov čísla 1 000.

Kanonický rozklad je $1\,000 = 2^3 5^3$, čiže $\alpha_1 = \alpha_2 = 3$, a tak počet deliteľov je $(3 + 1)(3 + 1) = 16$.

Nech $S(n)$ označuje súčet všetkých deliteľov prirodzeného čísla $n$. Napríklad $S(6) = 1 + 2 + 3 + 6 = 12$.

**Veta 10.** Ak $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ (kanonický rozklad) tak

$$S(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Dôkaz. Skúmajme výraz

$$(1 + p_1 + \dots + p_1^{\alpha_1})(1 + p_2 + \dots + p_2^{\alpha_2}) \dots (1 + p_k + \dots + p_k^{\alpha_k}). \qquad (8)$$

Keď vykonáme naznačené násobenia, dostanem súčet výrazov tvaru (7). Možno sa presvedčiť, že každý výraz tvaru (7) sa objaví v spomínanom súčte práve raz. Preto súčin (8) sa rovná súčtu všetkých deliteľov čísla $n$, čiže $S(n)$. Musíme ešte upraviť výraz (8). Zoberme si $i$-teho činiteľa

$$P_i = 1 + p_i + \dots + p_i^{\alpha_i}.$$

Je to súčet prvých $\alpha_i + 1$ členov geometrickej postupnosti s kvocientom $p_i$, a tak na základe dobre známeho vzorca dostaneme

$$P_i = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Ak dosadíme za $P_i$ do (8), obdržíme dokazovanú rovnosť pre $S(n)$.

*Príklad 6.* Nájdite $S(72)$.

Kanonický rozklad je $72 = 2^3 3^2$, čiže $p_1 = 2$, $p_2 = 3$, $\alpha_1 = 3$, $\alpha_2 = 2$, a tak

$$S(72) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} = 15 \,.\, 13 = 195.$$

Skutočne: $1 + 2 + 3 + 4 + 6 + 8 + 9 + 12 + 18 + 24 + 36 + 72 = 195$.

Prirodzené čísla, pre ktoré platí $S(n) = 2n$, sa nazývajú dokonalé (majú túto vlastnosť: súčet deliteľov menších ako $n$ sa rovná číslu $n$). Dokonalým číslom je napríklad 6, pretože $1 + 2 + 3 = 6$. Matematikom sa dodnes nepodarilo dokázať, či dokonalých čísel je nekonečne mnoho. Nie je známe nijaké nepárne dokonalé číslo. Existuje nekonečne mnoho čísel, pre ktoré platí $S(n) < 2n$ (napríklad všetky prvočísla — pozri vetu 12) aj nekonečne mnoho takých, pre ktoré je $S(n) > 2n$ (sú to napríklad všetky čísla tvaru $3 \,.\, 2^k$).

Cvičenia

1. Dokážte, že každý deliteľ čísla $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ je tvaru (7).

2. Nájdite všetky delitele čísla 120.

3. Nájdite všetky párne delitele čísla 1200.

4. Aký je počet deliteľov čísel 72 a 120? (Vypočítajte použitím vzorca a porovnajte s príkladom 5 a cvičením 3).

5. Vypočítajte $D$ (1200), D(83), D(500).

6. Nech $p$ je prvočíslo. Určte $D(p)$.

7. Určte $D(2p^3)$, keď $p$ je nepárne prvočíslo.

8. R ôznym $k$-ticiam exponentov $(\beta_1, \beta_2, \dots, \beta_k)$ zodpovedajú rôzne delitele čísla $n$ (pozri dôkaz vety 9).

9*. Dokážte, že po roznásobení (8) sa každý deliteľ čísla $n$ objaví práve raz ako sčítanec.

10. Vypočítajte $S$ (120). Porovnajte s cvičením 2.

11. Vypočítajte $S$ (144) a $S$ (250).

12. Vypočítajte $S(p)$, ak $p$ je prvočíslo.

13. Vypočítajte $S(2p^3)$, ak $p$ je nepárne prvočíslo.

14.* Dokážte: pre všetky čísla tvaru $n = 3 \,.\, 2^k$ platí $S(n) > 2n$.

15.* Nech $n = p^\alpha q^\beta$, kde $p$ a $q$ sú rôzne prvočísla. Nech číslo $n^2$ má 21 rôznych deliteľov. Koľko deliteľov má $n^3$?

16.* Nájdite číslo tvaru $2^\alpha 3^\beta$, keď viete, že súčet jeho deliteľov je 403.

## 6. Pojednanie o prvočíslach

Ak $n$ je zložené číslo, tak ho možno zapísať v tvare $n = a \,.\, b$, kde $1 < a < n$, $1 < b < n$. Zrejme nemôže platiť súčasne $a > \sqrt{n}$, $b > \sqrt{n}$, lebo potom by bolo $a \,.\, b > n$. To znamená, že každé zložené číslo má aspoň jedného deliteľa, ktorý neprevyšuje $\sqrt{n}$. Z cvičenia 5 odseku 4 vyplýva, že najmenší nejednotkový deliteľ každého čísla $n$ je prvočíslo. Dokázali sme vlastne vetu:

**Veta 11.** Každé zložené číslo $n$ je deliteľné aspoň jedným prvočíslom $p$ neprevyšujúcim $\sqrt{n}$.

Na tejto vete je postavená metóda na hľadanie všetkých prvočísel v nejakom intervale od 1 do $N$. Napíšeme čísla od 1 do $N$ v rastúcom poradí. O čísle 1 vieme, že nie je prvočíslom — preto ho vyčiarkneme. Dvojka je najmenšie prvočíslo — zakrúžkujeme ju; vyčiarkneme všetky čísla od 3 do N, ktoré sú deliteľné dvoma (párne), lebo tie nie sú prvočísla. Prvé nevyčiarknuté číslo je teraz 3, a to je prvočíslo (zakrúžkujeme ho). Vyčiarkneme všetky čísla od 4 do N, ktoré sú deliteľné troma. Najmenšie nevyčiarknuté číslo 5 je znova prvočíslo; dáme ho do krúžku, a potom vyčiarkneme všetky násobky piatich medzi 6 a $N$... Takto postupujeme

dovtedy, kým najmenšie nevyčiarknuté číslo bude väčšie ako $\sqrt{n}$ (to znamená, že sme vyčiarkli násobky všetkých prvočísel neprevyšujúcich $\sqrt{n}$). Čísla, ktoré potom ostali nevyčiarknuté, všetky zakrúžkujeme, lebo musia byť prvočíslami (pozri vetu 11). Táto metóda sa nazýva Eratostenovo sito (Eratostenes — grécky matematik v treťom storočí pred naším letopočtom).

Ukážeme teraz Eratostenovo sito po $N = 100$ (postup: vyčiarkneme všetky násobky prvočísel neprevyšujúcich $\sqrt{100} = 10$; sú to prvočísla 2, 3, 5 a 7; zvyšné čísla zakrúžkujeme, lebo musia byť prvočíslami).*)

*1*, **2**, **3**, *4*, **5**, *6*, **7**, *8*, *9*, *10*, **11**, *12*, **13**, *14*, *15*, *16*, **17**, *18*, **19**, *20*, *21*, *22*, **23**, *24*, *25*, *26*, *27*, *28*, **29**, *30*, **31**, *32*, *33*, *34*, *35*, *36*, **37**, *38*, *39*, *40*, **41**, *42*, **43**, *44*, *45*, *46*, **47**, *48*, *49*, *50*, *51*, *52*, **53**, *54*, *55*, *56*, *57*, *58*, **59**, *60*, **61**, *62*, *63*, *64*, *65*, *66*, **67**, *68*, *69*, *70*, **71**, *72*, **73**, *74*, *75*, *76*, *77*, *78*, **79**, *80*, *81*, *82*, **83**, *84*, *85*, *86*, *87*, *88*, **89**, *90*, *91*, *92*, *93*, *94*, *95*, *96*, **97**, *98*, *99*, *100*

V rozložení prvočísel sa matematikom dodnes nepodarilo nájsť nijakú rozumnú pravidelnosť. Napríklad súdiac podľa prvej „stovky" (v prvej desiatke sú štyri prvočísla — 2, 3, 5, 7, kým v poslednej jediné — 97) by sme sa mohli domnievať, že prvočísel medzi veľkými číslami je vždy menej a menej a nakoniec úplne zmiznú (čiže ich počet by bol konečný). Toto pozorovanie je však nesprávne, pretože už 300 rokov pred naším letopočtom grécky matematik Euklides dokázal:

**Veta 12.** Prvočísel je nekonečne mnoho.

Dôkaz. Teraz už existuje veľké množstvo dôkazov tejto vety; my uvedieme ten, ktorý našiel Euklides.

Budeme dokazovať nepriamo. Predpokladajme, že existuje len konečne mnoho prvočísel a označme ich

$$p_1, p_2, \ldots, p_k. \tag{9}$$

Skúmajme číslo $P = p_1 p_2 \ldots p_k + 1$. $P$ je väčšie ako 1, a tak je buď prvočíslo, buď zložené číslo. Keď $P$ je prvočíslo, tak dochádzame k sporu s predpokladom, že v (9) sú vymenované všetky prvočísla (pretože $P > p_i$ pre všetky $i = 1, 2, \ldots, k$). Ak $P$ je zložené číslo, tak podľa cvičenia 5 odseku 4 jeho najmenší nejednotkový deliteľ je prvočíslo. Teda $P$ je deliteľné nejakým prvočíslom. Na základe vety 2 časti I však $P$ nie je deliteľné ani

*) Čísla, ktoré by mali byť vyčiarknuté, sú vysádzané *kurzívou*. Čísla, ktoré by mali byť zakrúžkované, sú vysádzané polotučne.

jedným z prvočísel (9) (pozri cvičenie 3), teda musí existovať ešte nejaké ďalšie prvočíslo neobsiahnuté v (9). To je znova spor. Teda predpoklad, že provočísel je len konečne mnoho, vedie vždy k sporu. Musí ich byť preto nekonečne mnoho.

Jediné párne prvočíslo je 2. Všetky zvyšné prvočísla sú teda buď tvaru $4k + 1$, buď tvaru $4k + 3$. Tvrdenie vety 12 sa dá takto zosilniť:

**Veta 13.** Existuje nekonečne mnoho prvočísel tvaru $4k + 3$.

Dôkaz. Nepriamo: predpokladajme, že prvočísel tvaru $4k + 3$ je len konečne mnoho, a teda že všetky prvočísla väčšie ako nejaké prvočíslo $p$ sú už tvaru $4k + 1$. Skúmajme teraz výraz

$$Q = 2^2 . 3 . 5 . 7 . 11 \ldots p - 1.$$

Toto číslo je zrejme tvaru $4s + 3$ (presvedčte sa o tom!), preto nemôže byť prvočíslom (pretože $Q > p$), ale ani súčinom prvočísel tvaru $4k + 1$ (pretože súčin ľubovoľného počtu čísel tvaru $4s + 1$ je znova číslo tohto tvaru). Teda $Q$ je deliteľné aspoň jedným prvočíslom tvaru $4s + 3$. Na základe vety 2 časti I však $Q$ nie je deliteľné ani jedným z prvočísel 3, 5, 7, ..., $p$ (pozri cvičenie 5), a tak musí byť deliteľné prvočíslom tvaru $4s + 3$ väčším ako $p$. To je spor s predpokladom, že všetky prvočísla tvaru $4s + 3$ sú menšie alebo sa rovnajú $p$.

**Poznámka.** Dá sa dokázať ešte silnejšie a všeobecnejšie tvrdenie (tzv. Dirichletova veta): ak $(a, b) = 1$, tak existuje nekonečne mnoho prvočísel tvaru $an + b$.

Dve za sebou nasledujúce čísla môžu byť prvočíslami jedine v prípade 2 a 3 (inač jedno z nich je párne a väčšie ako 2). Naproti tomu dve čísla tvaru $a$, $a + 2$ môžu byť prvočíslami vo viacerých príkladoch: 3, 5; 5, 7; 11,13; 17, 19; 29, 31; ... Takéto dve čísla sa nazývajú prvočíselné dvojčatá. Nie je známe, či prvočíselných dvojčiat je nekonečne veľa.

Z troch čísel tvaru $a$, $a + 2$, $a + 4$ je vždy práve jedno deliteľné troma, a tak môžu byť prvočíslami súčasne jedine v prípade 3, 5, 7.

Naproti tomu ľubovoľný počet za sebou nasledujúcich čísel môže byť zložených. Napríklad čísla 120, 121, 122, 123, 124, 125, 126 sú všetky zložené. Na druhej strane však podľa známeho Bertrandovho postulátu pre ľubovoľné prirodzené $n \geqq 2$ sa medzi $n$ a $2n$ nachádza aspoň jedno prvočíslo.

Matematici sa už veľmi dávno pokúšali nájsť nejaký vhodný predpis na tvorenie prvočísel. Francúzsky matematik P. Fermat (o ktorom sme už hovorili v časti I) sa domnieval, že všetky čísla tvaru $2^{2^n} + 1$ (tzv. Fermatove čísla) sú prvočíslami. Jeho domnienka bola veľmi unáhlená, lebo čoskoro sa ukázalo, že už pre $n = 5$ je to zložené číslo! Pravda, pre $n = 1$,

2, 3 a 4 dostávame skutočne prvočísla. Ďalšie známe čísla sú tzv. Mersennove čísla; sú to čísla tvaru $2^n - 1$. Takéto číslo môže byť prvočíslom len vtedy, ak $n$ je prvočíslo. Avšak ani to nie je postačujúca podmienka, pretože $2^{11} - 1 = 2047$ je deliteľné číslom 23.

Cvičenia

**1.** Rozšírte Eratostenovo sito po $N = 300$.

**2.** Ak $n$ je zložené číslo a $n = xy$, tak $x$ a $y$ sa nazývajú združené delitele čísla $n$. Podľa vety 11 vždy práve jeden z navzájom združených deliteľov je $\leqq \sqrt{n}$ (a druhý $\geqq \sqrt{n}$). Z toho vyplýva, že pri hľadaní všetkých deliteľov čísla $n$ môžeme postupovať takto: nájdeme všetky delitele neprevyšujúce $\sqrt{n}$ a k nim združené delitele. Opísanou metódou nájdite všetky delitele čísla 640.

**3.** Dokážte, že $P$ nie je deliteľné ani jedným z čísel $p_i$, (pozri dôkaz vety 12).

**4.** Dokážte: súčin ľubovoľného počtu čísel tvaru $4s + 1$ je tiež číslo toho tvaru.

**5.** Dokážte: $Q$ nie je deliteľné ani jedným z čísel $2, 3, 5, \ldots, p$ (pozri dôkaz vety 13).

**6.** Dokážte, že existuje nekonečne mnoho prvočísel tvaru $6k + 5$ (návod: všetky prvočísla okrem 2 a 3 sú tvaru $6k + 1$ alebo $6k + 5$; súčin ľubovoľného počtu čísel tvaru $6k + 1$ je znova číslo tohto tvaru).

**7.** Z $k$ prirodzených čísel $a, a + 1, a + 2, \ldots, a + k - 1$ je vždy aspoň jedno deliteľné číslom $k$. Dokážte!

**8.** Nech $n > 1$ je ľubovoľné prirodzené číslo. Dokážte, že čísla $x_1 = n! + 2$, $x_2 = n! + 3, \ldots x_{n-1} = n! + n$ sú zložené.

**9.** Overte platnosť Bertrandovho postulátu pre $n = 1, \ldots, 15$.

**10.** Overte, že pre $n = 1, 2, 3, 4$ je Fermatovo číslo prvočíslom.

**11.** Dokážte: $a^n - 1$ môže byť prvočíslom len pre $a = 2$.

**12.** Číslo $2^n - 1$ môže byť prvočíslom len vtedy, ak $n$ je prvočíslo.

**13.** Zistite, ktoré z Mersennových čísel $M_1, \ldots M_{10}$ sú prvočíslami.

**14.** Nájdite ešte ďalšie prvočíselné dvojčatá.

**15.** Číslo $n^2 - n + 41$ je prvočíslom pre $n = 1, 2, \ldots, 40$, ale pre 41 je už zloženým číslom. Pokúste sa nájsť podobný polynóm, aby jeho hodnotami boli prvočísla pre mnoho čísel $n$.

## 7. O iracionálnosti niektorých čísel*)

Racionálnymi číslami nazývame také reálne čísla, ktoré sa dajú vyjadriť v tvare zlomku s prirodzeným menovateľom a celým čitateľom. Iracionálnymi nazývame také reálne čísla, ktoré nie sú racionálne.

Už antickí grécki matematici vedeli, že $\sqrt{2}$ nie je racionálne číslo (je to dĺžka uhlopriečky štvorca so stranou 1). Ukážeme teraz metódu dôkazu, ktorá sa málo líši od tej, ktorú použili Gréci.

*) Touto problematikou sa hlbšie zaoberá článok: Šalát, T.: O iracionálnych číslach. Matematické obzory, 1 (1972), 37—51.

Dokazujeme nepriamo: Predpokladajme, že $\sqrt{2}$ je racionálne číslo, a tak sa dá písať v tvare

$$\sqrt{2} = \frac{A}{B},$$

kde $A$ a $B$ sú prirodzené čísla. Nech $(A, B) = d$ a nech $A = ad$, $B = bd$. Po krátení zlomku číslom $d$ dostaneme

$$\sqrt{2} = \frac{a}{b},$$

pričom zlomok $\frac{a}{b}$ je v základnom tvare, t. j. $(a, b) = 1$ (pozri vetu 5 časti I). Umocnením poslednej rovnosti dostaneme

$$2 = \frac{a^2}{b^2}, \qquad \text{čiže} \qquad 2b^2 = a^2.$$

Z vety 6 vyplýva, že potom $2 \mid a$, a tak $2^2 \mid a^2$, čiže môžeme písať $a^2 = 2^2c$, kde $c$ je prirodzené číslo. Po vsadení do poslednej rovnosti dostaneme:

$$2b^2 = 4c.$$

Z toho po vydelení dvoma máme

$$b^2 = 2c.$$

Teda $2 \mid b^2$, a tak podľa vety 6: $2 \mid b$. To je ale spor s predpokladom $(a, b) = 1$, lebo sme dostali $2 \mid a$, $2 \mid b$, a tak $(a, b)$ je aspoň 2.

Predpoklad, že $\sqrt{2}$ je racionálne číslo, viedol k sporu, a tak to musí byť iracionálne číslo.

Presne touto úvahou možno dokázať, že $\sqrt{p}$ je iracionálne číslo pre každé prvočíslo $p$. My namiesto toho dokážeme oveľa všeobecnejšie tvrdenie:

**Veta 14.** Číslo $\sqrt[k]{n}$ je prirodzeným číslom vtedy a len vtedy, keď v kanonickom rozklade

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

sú všetky exponenty $\alpha_1, \alpha_2, \dots, \alpha_s$ deliteľné číslom $k$.

Dôkaz. Ak pre všetky $i = 1, 2, \dots, s$ platí $k \mid \alpha_i$, tak môžeme písať $\alpha_i = k\beta_i$, kde $\beta_i$ je prirodzené číslo. Preto $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = (p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s})^k = m^k$, kde $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, a tak $\sqrt[k]{n} = \sqrt[k]{m^k} = m$, a to je prirodzené číslo.

Naopak, nech teraz $\sqrt[k]{n} = m$ je prirodzené číslo a nech

$$m = p_1^{\omega_1} p_2^{\omega_2} \dots p_s^{\omega_s}.$$

Potom

$$n = m^k = (p_1^{\omega_1} p_2^{\omega_2} \dots p_s^{\omega_s})^k = p_1^{k\omega_1} p_2^{k\omega_2} \dots p_s^{k\omega_s}.$$

Na základe vety 8 však posledný výraz je (jediným) kanonickým rozkladom čísla $n$, a tým je dôkaz vety ukončený.

**Poznámka 1.** Ak $k$-tá odmocnina z celého čísla je racionálne číslo, tak musí byť celým číslom. Skutočne, nech

$$\sqrt[k]{n} = \frac{a}{b},$$

kde $\frac{a}{b}$ je zlomok v základnom tvare. Úpravou poslednej rovnosti dostaneme $a^k = nb^k$. Nech teraz $p$ je nejaký prvočíselný deliteľ čísla $b$. Potom $p \mid a^k$, a tak na základe vety 6 $p \mid a$. To je ale spor s predpokladom, že $\frac{a}{b}$ je zlomok v základnom tvare. To znamená, že $b$ nemôže byť deliteľné nijakým prvočíslom, a to je možné len vtedy, keď $b = 1$, čiže $\sqrt[k]{n} = a$ (celé číslo).

**Poznámka 2.** Iracionálnosť $\sqrt{p}$ ($p$ prvočíslo) je dôsledkom vety 14, lebo v kanonickom rozklade prvočísla $p$ je $s = 1$, $p_1 = p$, $\alpha_1 = 1$ (teda nepárne číslo!).

Cvičenia

**1.** Metódou použitia pri dôkaze iracionálnosti čísla $\sqrt{2}$ dokážte: $\sqrt{p}$ je iracionálne pre každé prvočíslo $p$.

**2.** Zistite, či tretia odmocnina z 5400 je celé číslo.

**3.** Nájdite druhú odmocninu z čísla $n = 2^8 3^6 7^2$.

**4.** Nech $\frac{a}{b}$ je zlomok v základnom tvare. Potom $k$-tá odmocnina z $\frac{a}{b}$ je racionálne číslo vtedy a len vtedy, keď $\sqrt[k]{a}$ aj $\sqrt[k]{b}$ sú celé čísla.

**5.** Zistite, či je racionálnym číslom tretia odmocnina z $\frac{64}{27}$.

## Literatúra

[1] Davydov, U. S.—Znám, Š.: Teória čísel, SPN 1972.

[2] Hardy, G. H.—Wright, E. M.: An introduction to the theory of numbers, Oxford 1954.

[3] Šalát, T.: Vybrané kapitoly z teórie čísel, SPN 1966.

[4] Znám, Š.: Vybrané kapitoly z elementárnej teórie čísel, I. Matematické obzory, 3 (1973).