VYBRANÉ KAPITOLY Z ELEMENTÁRNEJ TEÓRIE ČÍSEL I

ŠTEFAN ZNÁM, Bratislava

Tento článok je určený profesorom gymnázií ako pomocná literatúra k vyučovaniu výberovej matematiky v 4. ročníku

I. Deliteľnosť čísel

K ľubovoľnej dvojici prirodzených čísel a a b existujú také nezáporné celé čísla q a z, že platí

$$a = bq + z, \qquad \text{pričom} \qquad 0 \leqq z < b \tag{1}$$

Skutočne: ak $\frac{a}{b}$ je pravý zlomok, tak môžeme písať $a = b \,.\, 0 + a$ a žiadané vyjadrenie dostaneme, keď položíme $q = 0$, $z = a$; ak $\frac{a}{b}$ je nepravý zlomok alebo 1, tak ho možno písať v tvare súčtu celého čísla a pravého zlomku

$$\frac{a}{b} = c + \frac{d}{b}, \quad \text{čiže} \quad a = bc + d$$

a žiadané vyjadrenie dostaneme, keď položíme $q = c$, $z = d$ (pretože $0 \leqq d < b$).

Príklad 1. Nech $a = 2$, $b = 3$. Potom $2 = 3 \,.\, 0 + 2$, teda $q = 0$, $z = 2$, a tak z splňuje nerovnice $0 \leqq z < b$.

Príklad 2. Nech $a = 7$, $b = 3$. Potom $a = b \,.\, 2 + 1$, čiže $q = 2$, $z = 1$.

Príklad 3. Ak pracujeme s väčšími číslami, tak q a z nemožno uhádnuť. Vtedy vykonáme čiastočné delenie; q bude čiastočným podielom, z zvyškom. Ak napríklad $a = 187$, $b = 14$, tak

$$\frac{187}{14} = 13 + \frac{5}{14}, \qquad \text{čiže} \qquad q = 13,\ z = 5$$

Ak zvyšok pri delení čísla a číslom b je 0, tak hovoríme, že číslo a je deliteľné číslom b. Označujeme to $b \mid a$. Teda ak a je deliteľné b, tak existuje prirodzené číslo q, pre ktoré platí $a = b \,.\, q$. Fakt, že a nie je, deliteľné b, zapisujeme $b \nmid a$. Keď $b \mid a$ (hovoríme aj b je deliteľom a), potom zrejme $b \leqq a$.

Príklad 4. Číslo 2 je deliteľom čísla 6, lebo $6 = 2 . 3$, a tak môžeme písať $2 \mid 6$. Podobne 33 je deliteľné 11, lebo $33 = 11 . 3$. Naproti tomu $2 \nmid 5$, $3 \nmid 1$, $13 \nmid 2$.

Zoberme teraz pevné prirodzené číslo b. Na základe vyššie povedaného pre každé prirodzené číslo a existujú také čísla q a z, že platí

$$a = bq + z, \qquad \text{kde} \qquad 0 \leqq z < b$$

Teda každé prirodzené číslo sa dá napísať v jednom z tvarov

$$bq, \qquad bq + 1, \ldots, bq + (b - 1)$$

Napríklad ak $b = 4$, tak každé prirodzené číslo možno písať v jednom z tvarov $4q$, $4q + 1$, $4q + 5$, $4q + 3$.

Tento fakt budeme v ďalšom často používať. Teraz na základe uvedených úvah dokážeme jednu vetu, ktorú využijeme v ďalšej časti článku.

Veta 1. Druhá mocnina každého prirodzeného čísla n má tvar $4k$ alebo $4k + 1$.

Dôkaz. Budeme rozlišovať štyri prípady:

a) Nech n má tvar $4q$, tak $n^2 = (4q)^2 = 16q^2 = 4(4q^2)$; položme $4q^2 = k$. Potom $n^2 = 4k$.

b) Nech $n = 4q + 1$, potom $n^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1$. Ak položíme $4q^2 + 2q = k$, dostaneme, že n^2 má tvar $4k + 1$.

c) Nech $n = 4q + 2$, tak $n^2 = 16q^2 + 16q + 4$, teda po vhodnom označení zisťujeme, že má tiež žiadaný tvar.

d) Obdobne by sme postupovali v poslednom prípade, keď n má tvar $4q + 3$.

Teraz sa vrátime k vzťahu deliteľnosti a uvedieme niekoľko jeho vlastností.

Pre ľubovoľné prirodzené číslo a zrejme platí $a \mid a$. Hovoríme tomu, že vzťah deliteľnosti je reflexívny.

Vzťah deliteľnosti je aj tranzitívny, t. j. platí: ak $a \mid b$ a súčasne $b \mid c$, tak $a \mid c$. Skutočne: ak $a \mid b$, tak existuje také prirodzené číslo q, že $b = a . q$; zo vzťahu $b \mid c$ vyplýva existencia prirodzeného čísla p s vlastnosťou $c = b . p$. Z týchto rovností dostávame $c = b . p = (a . q) . p = a . (p . q)$, čiže a je deliteľom c.

Veta 2. Nech $a \mid b$, $a \mid c$, potom pre ľubovoľné celé čísla x a y také, že $bx + cy$ je prirodzené číslo, platí $a \mid bx + cy$.

Dôkaz. Môžeme písať $b = a . p$, $c = a . q$, kde p a q sú prirodzené čísla. Potom $bx + cy = a(px + qy)$. Číslo $px + qy$ je celé (pretože súčet

dvoch celých čísel, ako i súčin dvoch celých čísel je celé číslo) a na základe podmienky vety je kladné (aj a je kladné aj $bx + cy$ je kladné), a preto môžeme vyhlásiť, že číslo $bx + cy$ je deliteľné číslom a.

Dôsledok. ak $a \mid b$, $a \mid c$, tak $a \mid b + c$.

Príklad 4. Súčet dvoch párnych čísel je znova párne číslo. Skutočne: párne číslo je číslo deliteľné dvoma; teda ak $2 \mid a$, $2 \mid b$, tak podľa vety 2 platí $2 \mid a + b$, a tak $a + b$ je párne číslo.

Príklad 5. Možno 40 litrov vody rozliať do 3-litrových a 6-litrových nádob tak, aby každá použitá nádoba bola plná?

Riešenie: Nemožno, lebo podľa vety 2 je číslo $3x + 6y$ deliteľné troma, avšak 40 nie je troma deliteľné.

Cvičenia*)

1. Nájdite neúplný podiel a zvyšok v nasledujúcich prípadoch:
a) $a = 9$, $b = 4$;
b) $a = 7$, $b = 7$;
c) $a = 128$, $b = 31$.

2. Zistite, ktoré z čísel 121, 342, 1001 sú deliteľné číslom 11.

3. Deliteľnosť sa dá úplne analogicky definovať pre všetky celé čísla. Urobte to! Dokážte: ak $a \mid b$, tak $-a \mid b$, $-a \mid -b$, $a \mid -b$.

4. Dokážte: Druhá mocnina každého prirodzeného čísla sa dá napísať buď v tvare $3k$, alebo v tvare $3k + 1$.

5. Dokážte bod d) vety 1.

6. Ak $a \mid c$ a b je ľubovoľné prirodzené číslo, tak $a \mid bc$. Dokážte to!

7. Ak a a b sú prirodzené čísla a ak $a \mid b$, tak $a \leqq b$. Dokážte to!

8. Možno rozliať 50 litrov vody do 4-litrových a 12-litrových nádob tak, aby každá použitá nádoba bola plná?

9. Nájdite všetky prirodzené čísla do 50, ktoré sú deliteľné troma, ale nie sú deliteľné piatimi.

***10.** Vedeli by ste dokázať, že keď $a \mid b$ a súčasne $b \mid a$, tak $a = b$ (hovoríme tomu, že vzťah deliteľnosti je antisymetrický)? Návod: možno písať $b = a \,.\, p$, $a = b \,.\, q$, kde p a q sú prirodzené čísla, čiže $b = (p \,.\, q) \,.\, b$.

II. Najväčší spoločný deliteľ

Majme dané dve prirodzené čísla a a b. Ak o nejakom prirodzenom čísle c platí $c \mid a$, $c \mid b$, tak hovoríme, ze c je spoločným deliteľom čísel a a b.

Číslo 1 je deliteľom každého prirodzeného čísla (lebo pre ľubovoľné a je $a = 1 \,.\, a$) a tak 1 je spoločným deliteľom ľubovoľných dvoch čísel.

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

Na druhej strane, len konečne mnoho prirodzených čísel môže byť spoločným deliteľom daných dvoch čísel (to vyplýva napríklad z *cvičenia 7* v predchádzajúcej časti), a tak spomedzi spoločných deliteľov dvoch čísel možno vybrať najväčšie, a toto číslo budeme nazývať najväčším spoločným deliteľom tých čísel. Najväčšieho spoločného deliteľa čísel a a b budeme označovať (a, b).

Príklad 6. Nájdime najväčšieho spoločného deliteľa (NSD) čísel 36 a 30. Napíšme všetky delitele čísla 36; sú to: 1, 2, 3, 4, 6, 9, 12, 18, 36. Číslo 30 má delitele 1, 2, 3, 5, 6, 10, 15, 30. Vidíme teda, že $(36, 30) = 6$. Neskôr ukážeme rozumnejší spôsob na určenie NSD.

Hneď z definície vyplývajú tieto vlastnosti NSD:

Veta 3. $(a, a) = a$, $(a, 1) = 1$ pre každé prirodzené číslo a.

Veta 4. $(a, b) \mid a$, $(a, b) \mid b$.

Veta 5. Ak a a b sú prirodzené čísla, tak

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$$

Dôkaz. Na základe vety 4 môžeme písať $a = A \,.\, (a, b)$, $b = B \,.\, (a, b)$, kde A a B sú prirodzené čísla. Teda

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = (A, B)$$

Budeme dokazovať nepriamo. Predpokladajme, že $(A, B) = q > 1$. Potom na základe vety 4 možno písať $A = Pq$, $B = Qq$, kde P a Q sú prirodzené čísla. Tak dostávame $a = P \,.\, q \,.\, (a, b)$, $b = Q \,.\, q \,.\, (b, a)$, a preto číslo $q \,.\, (a, b)$ je spoločným deliteľom čísel a a b, pričom $q \,.\, (a, b) > (a, b)$. To je spor s predpokladom, že (a, b) je najväčším spoločným deliteľom a a b. Tým je dôkaz ukončený.

Príklad 7. $(36, 30) = 6$, $\left(\frac{36}{6}, \frac{30}{6}\right) = (6, 5) = 1$.

Veta 6. Ak $(a, b) = n$, tak existujú celé čísla x_0 a y_0 také, že

$$n = ax_0 + by_0$$

Dôkaz. Skúmajme všetky čísla tvaru $ax + by$, kde x a y prebieha všetky celé čísla. Medzi číslami tvaru $ax + by$ budú aj záporné aj kladné celé čísla a bude tam aj 0 ($x = y = 0$). Nech s je najmenšie kladné číslo tohto tvaru. Dokážeme, že $s = n$.

Označme x_0 a y_0 tie celé čísla, pre ktoré platí $ax_0 + by_0 = s$. Dokážeme, že $s \mid a$. Dokazujeme nepriamo. Nech $s \nmid a$ a nech platí $a = s \,.\, q + z$, kde z je prirodzené číslo menšie ako s (vychádzame z predpokladu $s \nmid a$!).

Potom $z = a - s \,.\, q = a - (ax_0 + by_0) \,.\, q = a(1 - qx_0) + b(-qy_0)$. Teda z je prirodzené číslo tvaru $ax + by$ a je menšie ako s, a to je spor. Podobne sa dokáže, že s je deliteľom čísla b. Číslo s je spoločným deliteľom čísel a a b, a tak nemôže prevyšovať ich najväčšieho spoločného deliteľa, čiže $s \leqq n$. Na druhej strane na základe vety 2 je číslo $s = ax_0 + by_0$ deliteľné číslom n (lebo n je spoločným deliteľom a a b), a tak na základe *cvičenia 7* odseku I platí $n \leqq s$. Zhrnutím posledných dvoch nerovníc dostávame $n = s$. Tým je dôkaz vety ukončený, lebo sme ukázali, že $n = ax_0 + by_0$.

Táto veta nám umožňuje dokázať mnoho zaujímavých a dôležitých vzťahov týkajúcich sa najväčšieho spoločného deliteľa.

Veta 7. Ak $c \mid a$, $c \mid b$, tak $c \mid (a, b)$.

Dôkaz. Na základe vety 6 je $(a, b) = ax_0 + by_0$, kde x_0 a y_0 sú celé čísla, a tak na základe vety 2 platí $c \mid ax_0 + by_0 = (a, b)$.

Príklad 8. Vieme už, že $(36, 30) = 6$. Podľa vety 6 sa číslo 6 musí dať vyjadriť v tvare $36x + 30y$. V tomto prípade máme ľahkú úlohu: zrejme $6 = 36 - 30$, teda $x_0 = 1$, $y_0 = -1$.

Najväčší spoločný deliteľ viac ako dvoch čísel sa definuje analogicky: je to najväčšie číslo zo spoločných deliteľov daných čísel.

Príklad 9. Nájdite najväčšieho spoločného deliteľa čísel 36, 30 a 20. Napíšme všetky delitele čísla 20 : 1, 2, 4, 5, 10, 20. Vidíme teda, že $(36, 30, 20) = 2$.

Pre výpočet NSD troch čísel sa dá vhodne použiť aj nasledujúca veta.

Veta 8. Pre ľubovoľné prirodzené čísla a, b a c platí

$$(a, b, c) = \big((a, b), c\big)$$

(Slovami: najväčšieho spoločného deliteľa troch čísel vypočítame tak, že vypočítame NSD prvých dvoch — označíme to d — a potom NSD tretieho čísla a čísla d.)

Dôkaz. (a, b, c) je deliteľom čísel a a b, a tak podľa vety 7 $(a, b, c) \mid (a, b)$; pritom (a, b, c) je deliteľom aj čísla c, a tak je spoločným deliteľom čísel (a, b) a c. Z toho vyplýva, že (a, b, c) je menšie alebo rovnaké ako NSD čísel (a, b) a c, čiže $(a, b, c) \leqq ((a, b), c)$. Podobne sa dokáže nerovnica $(a, b, c) \geqq ((a, b), c)$ a z týchto dvoch nerovníc už vyplýva tvrdenie našej vety.

Príklad 10. Vypočítajme ešte raz $(36, 30, 20)$. Podľa poslednej vety $(36, 30, 20) = ((36, 30), 20) = (6, 20) = 2$.

Poznámka. Dá sa dokázať tvrdenie: nech $n \geqq 3$ je prirodzené číslo a nech $x_1, \ldots, x_n$ sú tiež prirodzené čísla. Potom

$$(x_1, \ldots, x_{n-1}, x_n) = \big((x_1, \ldots, x_{n-1}), x_n\big)$$

Nech $a_1, \ldots, a_n$ sú prirodzené čísla. Hovoríme, že sú nesúdeliteľné, ak $(a_1, \ldots, a_n) = 1$. Ináč hovoríme, že sú súdeliteľné. Hovoríme, že tie čísla sú po dvoch nesúdeliteľné, ak pre všetky $i, j = 1, \ldots, n$ platí $(a_i, a_j) = 1$.

Príklad 11. Čísla 5, 6, 12 sú nesúdeliteľné, lebo $(5, 6, 12) = 1$, ale nie sú po dvoch nesúdeliteľné, lebo $(6, 12) = 2$. Naproti tomu čísla 2, 3, 5 sú po dvoch nesúdeliteľné (a preto aj nesúdeliteľné!), lebo $(2, 3) = (2, 5) = (3, 5) = 1$.

Veta 9. Ak $a \mid bc$, pričom a a b sú nesúdeliteľné, tak $a \mid c$.

Dôkaz. $(a, b) = 1$, teda podľa vety 6 existujú celé čísla x_0 a y_0 tak, že $1 = ax_0 + by_0$. Vynásobme túto rovnosť číslom c: $c = acx_0 + bcy_0$. Z vety 2 a z predpokladu $a \mid bc$ vyplýva, že pravá strana je deliteľná číslom a, preto je číslom a deliteľná aj ľavá strana, čiže c. Tým je dôkaz ukončený.

Cvičenia

1. Nájdite všetky spoločné delitele čísel 28 a 72.

2. Nájdite $(32, 48)$ a $(32, 48, 40)$.

3. Dokážte: Pre ľubovoľné a, b a m je $(ma, mb) = m(a, b)$.

4. Nech b a s sú symboly vystupujúce v dôkaze vety 6. Dokážte $s \mid b$.

5. Dokážte: $(a, b, c) \geqq ((a, b), c)$.

***6.** Dokážte nasledujúce tvrdenie (ktoré je zovšeobecnením vety 3): ak d je ľubovoľný spoločný deliteľ čísel a a b, tak

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$$

7. Dokážte: Ak $(a, b) = 1$, tak $(a^2, b^3) = 1$.

8. Dokážte: $a^2 \mid b^2$ vtedy a len vtedy, keď $a \mid b$.

***9.** Nech $xy = z^2$, pričom $(x, y) = 1$. Potom $x = (x, z)^2$, $y = (y, z)^2$.
Návod: $(x, z)^2 \mid z^2 = xy$, pričom $((x, z)^2, y) = 1$, a tak $(x, z)^2 \mid x$ atď.

***10.** Dokážte: Ak číslo a je deliteľné dvoma nesúdeliteľnými číslami, tak je deliteľné aj ich súčinom.

11. Na príklade ukážte, že keď $p \mid a$ a súčasne $q \mid a$, potom ešte nemusí platiť $pq \mid a$. Porovnajte to s predchádzajúcim príkladom.

12. Je pravdivé tvrdenie: ak $ab \mid c^2$, tak aspoň jedno z čísel a a b je deliteľom čísla c?

13. Nájdite takú trojicu nesúdeliteľných čísel, aby každé dva z nich boli súdeliteľné.

14. Z vety 6 vyplýva existencia takých celých čísel x_0 a y_0, že platí $9x_0 + 12y_0 = 3$ (pretože $(9, 12) = 3$). Pokúste sa nájsť také čísla x_0 a y_0.

15. Dokážte: Ak $a \mid b$, tak $(a, b) = a$.

III. Euklidov algoritmus

V predchádzajúcich odsekoch sme sa niekoľkokrát stretli s výpočtom najväčšieho spoločného deliteľa dvoch čísel. Počítali sme ho primitívnou metódou tak, že sme vymenovali všetky deliteľe obidvoch čísel a našli sme najväčší zo spoločných prvkov. Je všeobecne známa iná — rozumnejšia — metóda na výpočet NSD pomocou rozkladu daných čísel na prvočinitele. Achilovou pätou tejto metódy je, že rozložiť väčšie čísla na koreňové činitele nie je taká jednoduchá vec. Ukážeme tu na výpočet NSD ďalší spôsob, ktorý je veľmi mechanický.

Majme dané dve prirodzené čísla a a b a dajme si za úlohu nájsť (a, b).

Predpokladajme, že $a > b$. Na základe úvah prvého odseku existujú také nezáporné celé čísla q_1 a r_1, že

$$a = bq_1 + r_1, \qquad 0 \leqq r_1 < b$$

Ak $r_1 = 0$, tak $b \mid a$ a $(a, b) = b$ (pozri *cvičenie 15* odseku II). Predpokladajme, že $r_1 > 0$. Aplikujme hore uvedenú úvahu na dvojicu čísel b a r_1: existujú nezáporné celé čísla q_2 a r_2 tak, že $b = r_1q_2 + r_2$, kde $0 \leqq r_2 < r_1$. Ak $r_2 = 0$, tak sa proces končí, lebo (podobnými úvahami ako vo vete 10) sa dá dokázať, že potom $(a, b) = r_1$. Ak $r_2 > 0$, tak pokračujeme ďalej a dostávame rovnosť

$$r_1 = r_2q_3 + r_3, \qquad \text{kde} \qquad 0 \leqq r_3 < r_2 \text{ atď.}$$

Čísla $b, r, r_2, r_3, \ldots$ tvoria klesajúcu postupnosť nezáporných celých čísel, a preto po konečnom počte krokov dospejeme k takému i, že $r_i = 0$. Vtedy náš proces končí.

Zhrnutím dostávame sústavu

$$\begin{aligned} a &= bq_1 + r_1 & 0 &< r_1 < b \\ b &= r_1q_2 + r_2 & 0 &< r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 & 0 &< r_3 < r_2 \\ &\vdots \\ r_{i-3} &= r_{i-2}q_{i-1} + r_{i-1} \\ r_{i-2} &= r_{i-1}q_i & 0 &< r_{i-1} < r_{i-2} \end{aligned} \tag{2}$$

Tento proces sa nazýva Euklidov algoritmus. Ako to v ďalšom uvidíme, je veľmi užitočný nielen pri výpočte NSD dvoch čísel, ale aj pri riešení iných úloh teórie čísel.

Príklad 11. Aplikujme Euklidov algoritmus na čísla 46 a 18.

$$46 = 18 \,.\, 2 + 10 \qquad q_1 = 2, r_1 = 10 < 18$$

$$18 = 10 \,.\, 1 + 8 \qquad q_2 = 1, r_2 = 8 < 10$$

$$10 = 8 \,.\, 1 + 2 \qquad q_3 = 1, r_3 = 2 < 8$$

$$8 = 2 \,.\, 4 + 0 \qquad q_4 = 4, r_4 = 0$$

Veta 10. $(a, b) = r_{i-1}$.
(Slovami: Najväčší spoločný deliteľ dvoch čísel a a b sa rovná poslednému deliteľu v Euklidovom algoritme aplikovanom na čísla a a b).

Dôkaz. Najskôr dokážeme

$$(a, b) = (b, r_1) \tag{3}$$

Nech $(b, r_1) = d$. Z prvej rovnosti (2) a z vety 2 a vety 4 vyplýva $d \mid a$; zrejme $d \mid b$, a tak d je spoločným deliteľom čísel a a b, a preto d je menšie alebo rovnaké ako NSD čísel a a b, čiže

$$(b, r_1) \leqq (a, b)$$

Prvú rovnosť (2) možno upraviť takto: $r_1 = a - bq_1$. Označme $D = (a, b)$. Potom na základe viet 2 a 4 je D deliteľom r_1 a nakoľko je deliteľom aj b, nemôže prevyšovať NSD čísel b a r_1, a tak $(a, b) \leqq (b, r_1)$.
Z posledných dvoch nerovníc dostávame rovnosť (3).
Teraz by sme úplne analogicky dokázali rovnosti

$$(b, r_1) = (r_1, r_2) = \ldots = (r_{i-2}, r_{i-1}) \tag{4}$$

Pomocou poslednej rovnosti z (2) (*cvičenie 15* odseku II), sa môžeme presvedčiť, že

$$(r_{i-2}, r_{i-1}) = r_{i-1} \tag{5}$$

Zhrnutím (3), (4) a (6) máme

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{i-1}, r_{i-2}) = r_{i-1} \tag{6}$$

Tým je dôkaz vety 10 ukončený.
Vráťme sa k *príkladu 11*. Môžeme teraz konštatovať, že $(46, 18) = 2$. Vidíme, že pri výpočte sme nepoužili rozklad na prvočinitele. Euklidovým algoritmom možno vypočítať len NSD dvoch čísel; pri väčšom počte čísel musíme použiť úvahy uvedené v predchádzajúcich odsekoch.

Príklad 12. Vypočítajte najväčšieho spoločného deliteľa čísel 342 a 180 (za a volíme vždy to väčšie číslo).

Postup:

$$342 : 180 = 1 \ldots \qquad 342 = 180 \,.\, 1 + 162, r_1 = 162$$
162

$$180 : 162 = 1 \ldots \qquad 180 = 162 \,.\, 1 + 18, r_2 = 18$$
18

$$162 : 18 = 9 \qquad 162 = 18 \,.\, 9 + 0,\ r_3 = 0$$
$$0$$

Teda (342, 180) = 18.

Príklad 13. Vypočítajte (342, 180, 600). Použijeme tu rovnosť (342, 600, 180) = ((342, 180), 600) = (18, 600).

$$600 : 18 = 33\ldots \qquad r_1 = 6$$
$$60$$
$$6$$
$$18 : 6 = 3 \qquad r_2 = 0$$
$$0$$

Posledným deliteľom je 6, a to je najväčším spoločným deliteľom všetkých troch čísel.

Príklad 14. Doteraz sme uviedli len príklady, keď Euklidov algoritmus „prebehol" rychlo. Nie je tomu vždy tak a niekedy potrebujeme mnoho „krokov", kým nájdeme NSD.

Vypočítajme teraz (13 740, 6 945).

$$13\,740 : 6\,945 = 1\ldots \qquad r_1 = 6\,795$$
$$6\,793$$
$$6\,945 : 6\,795 = 1\ldots \qquad r_2 = 150$$
$$150$$
$$6\,795 : 150 = 44\ldots \qquad r_3 = 45$$
$$795$$
$$45$$
$$150 : 45 = 3\ldots \qquad r_4 = 15$$
$$15$$
$$15 : 3 = 5 \qquad r_5 = 0$$

Teda (13 740, 6 945) = 3.

Euklidov algoritmus nám umožňuje riešiť ešte jednu ďalšiu úlohu z teórie čísel (o závažnosti ktorej sa presvedčíme v nasledujúcom odseku). Veta 6 pre každé dve prirodzené čísla a a b zaručuje existenciu takých celých čísel x_0 a y_0, že platí $(a, b) = ax_0 + by_0$; použitím Euklidovho algoritmu vieme nájsť tieto čísla. Teraz ukážeme, ako sa to robí. Ak $b \mid a$, tak $(a, b) = b = b \,.\, 1 + a \,.\, 0$. Preto môžeme predpokladať, že $b \nmid a$. Zoberme predposlednú rovnosť zo sústavy (2) (pozri vetu 10)

$$r_{i-3} = r_{i-2}q_{i-1} + r_{i-1} = r_{i-2}q_{i-1} + (a, b)$$

Po úprave z nej dostaneme

$$(a, b) = r_{i-3} - r_{i-2}q_{i-1} \tag{7}$$

Teda (a, b) sme vyjadrili v tvare $Ar_{i-3} + Br_{i-2}$. Z predchádzajúcej rovnosti (2) možno r_{i-2} vyjadriť pomocou r_{i-3} a r_{i-4}. Ak to dosadíme do (7), dostaneme (a, b) vyjadrené v tvare $Cr_{i-3} + Dr_{i-4}$, atď. Ak takto budeme postupovať, dostaneme nakoniec (a, b) vyjadrené v tvare $aF + bG$, kde F a G sú celé čísla.

Príklad 15. Vráťme sa k *príkladu 12.* Ukázali sme, že $(342, 180) = 18$. Vyjadrime 18 v tvare $342x + 180y$. Budeme vychádzať z rovností

$$342 = 180 \,.\, 1 + 162$$

$$180 = 162 \,.\, 1 + 18$$

Z druhej rovnosti vyplýva: $18 = 180 - 162 \,.\, 1$. Dosaďme namiesto 162 výraz $342 - 180 \,.\, 1$ (čo sme získali úpravou prvej rovnosti). Výsledok je $18 = 180 - (342 - 180 \,.\, 1) = 180 \,.\, 2 + 342 \,.\, (-1)$. V tomto prípade $x_0 = 2$, $y_0 = -1$.

Príklad 16. Pokúsme sa vyjadriť číslo 6 v tvare $372x + 150y$. Urobme Euklidov algoritmus pre dvojicu čísel 372 a 150:

$$372 = 150 \,.\, 2 + 72$$

$$150 = 72 \,.\, 2 + 6$$

(ďalej už nemusíme pokračovať!)
Máme preto $6 = 150 - 2 \,.\, (372 - 150 \,.\, 2) = 373 \,.\, (-2) + 150 \,.\, 5$, čiže $x = -2$, $x = 5$.

Cvičenia

1. Riešte *príklady 12, 13* a *14* známou metódou (rozkladom na prvočiniteľov) a porovnajte obťažnosť tých dvoch metód.

2. Použitím Euklidovho algoritmu vypočítajte: a) (324, 160), b) (7536, 8000), c) (345, 500, 1210), d) (240, 150, 85, 325).

3. Najmenším spoločným násobkom dvoch prirodzených čísel a a b nazývame najmenšie prirodzené číslo D s vlastnosťou $a \mid D$, $b \mid D$. Pre výpočet najmenšieho spoločného násobku čísel a a b — označujeme ho $[a, b]$ — dá sa odvodiť nasledujúci vzťah

$$[a, b] = \frac{ab}{(a, b)} \tag{8}$$

Vidíme teda, že prostredníctvom tohto vzťahu možno využiť Euklidov algoritmus aj pri výpočte najmenšieho spoločného násobku dvoch čísel.

Použitím vzťahu (8) vypočítajte najmenší spoločný násobok čísel 24 a 32. Vypočítajte ho aj inou metódou a porovnajte stupeň obťažnosti.

4. Vypočítajte [17, 19], [125, 350].

5. Vyjadrite číslo 15 v tvare $450x + 105y$.

6. Vedeli by ste číslo 30 vyjadriť v tvare $450x + 105y$.

7. Dá sa číslo 15 vyjadriť v tvare $450x + 315y$.

8. Dokážte: Ak $(a, b) = 1$, tak číslo 2 sa dá vyjadriť v tvare $ax + by$. Nevedeli by ste tento fakt zovšeobecniť?

9. Vyjadrenie (a, b) v tvare $ax + by$ nie je jednoznačné. Vedeli by ste nájsť aj iné vyjadrenie v *príklade 15*? Koľko rôznych vyjadrení asi existuje?

10. Vyjadrite číslo 100 v tvare $625x + 1000y$.

IV. Lineárne diofantické rovnice

Už v prvom odseku sme sa pýtali, či možno 40 litrov tekutiny rozliať do 3-litrových a 6-litrových nádob. Pri riešení sme prišli do styku s rovnicou $3x + 6y = 40$ a hľadali sme jej riešenie v celých číslach (pretože x a y predstavujú počty nádob určitého druhu, a tak nemôžu byť necelé čísla!). Mnoho matematických problémov, ale aj hádaniek vedie na hľadanie celočíselných riešení nejakej rovnice alebo rovníc tohto druhu. Takéto rovnice nazývame diofantickými rovnicami (grécky matematik Diofantos sa v 3. storočí pred naším letopočtom prvý zaoberal riešením takýchto rovníc).

My sa obmedzíme len na riešenie niekoľko málo typov diofantických rovníc. V tomto odseku sa budeme zaoberať len riešením tzv. lineárnych diofantických rovníc s dvoma neznámymi, ktoré sa dajú zapísať v tvare

$$ax + by = c \tag{9}$$

kde a, b, c sú nenulové celé čísla. Vždy možno dosiahnuť (a my to v ďalšom budeme predpokladať) $c > 0$.

Riešením rovnice (9) nazývame takú dvojicu celých čísel x_0 a y_0, že platí $ax_0 + by_0 = c$. Napríklad dvojica (2, 1) je riešením diofantickej rovnice $2x + 3y = 7$, pretože $2 \,.\, 2 + 3 \,.\, 1 = 7$ a pritom 2 a 1 sú celé čísla. Rovnica (9) sa nazýva riešiteľná, ak existuje aspoň jedno riešenie; riešiť rovnicu znamená nájsť všetky jej riešenia.

Veta 11. Diofantická rovnica (9) je riešiteľná vtedy a len vtedy, keď

$$d = (|a|, |b|) \mid c \tag{10}$$

(symbolom $|a|$ označujeme absolútnu hodnotu čísla a).

Dôkaz. Budeme dokazovať v dvoch krokoch.

a) Najprv dokážeme, že keď je rovnica (9) riešiteľná, tak platí (10). Predpokladajme, že existujú celé čísla x_0 a y_0 také, že $c = ax_0 + by_0$. Na základe vety 4 platí $d \mid |a|$, $d \mid |b|$, a preto na základe vety 2: $d \mid ax_0 + by_0 = c$.

b) Dokážeme, že keď platí (10), tak rovnica (9) je riešiteľná. Z (10) vyplýva

$$c = e\,(|\,a\,|, |\,b\,|) = e\,.\,d$$

Skúmajme teraz diofantickú rovnicu

$$ax + by = d \tag{11}$$

Podľa vety 6 existujú také celé čísla x_0 a y_0, že platí

$$|\,a\,|\,x_0 + |\,b\,|\,y_0 = d$$

(pretože d je najväčším spoločným deliteľom čísel $|\,a\,|$ a $|\,b\,|$).

Ak $a > 0 (a < 0)$, tak položme $x_1 = x_0 (x_1 = -x_0)$; ak $b > 0$ $(b < 0)$, tak položme $y_1 = y_0 (y_1 = -y_0)$. Potom zrejme platí

$$ax_1 + by_1 = d$$

Teda diofantická rovnica (11) je riešiteľná.

Položme $x_2 = ex_1$, $y_2 = ey_1$. Potom

$$ax_2 + by_2 = a(ex_1) + b(ey_1) = e(ax_1 + by_1) = ed = c$$

To znamená, že dvojica (x_2, y_2) je riešením diofantickej rovnice (9), a tým je dôkaz vety 11 ukončený.

Príklad 17. Zistite, či je riešiteľná diofantická rovnica

$$6x - 9y = 32$$

Nie je riešiteľná, pretože $(6, 9) = 3$ a $3 \nmid 32$.

Príklad 18. Nájdite nejaké riešenie diofantickej rovnice

$$6x - 9y = 3$$

Poznámka. Dá sa dokázať, že riešenie tejto rovnice sa nezmení, ak všetky koeficienty delíme nejakým ich spoločným deliteľom. To isté platí aj v ďalších príkladoch.

Riešenie. Táto diofantická rovnica je riešiteľná, pretože $(6, 9) = 3 = c$. Vieme nájsť riešenie rovnice $6z + 9t = 3$ (pozri odsek III) pomocou Euklidovho algoritmu: $9 = 6\,.\,1 + 3$, čiže $3 = 6.\ (-1) + 9\,.\,1$. Preto $x_0 = -1$, $y_0 = 1$. Položme $x_1 = x_0 = -1$, $y_1 = -y_0 = -1$(pozri časť b) dôkazu vety 11). Dvojica $(-1, -1)$ je riešením našej rovnice, pretože $6\,.\,(-1) - 9\,.\,(-1) = 3$.

Príklad 19. Nájdite nejaké riešenie rovnice

$$6x + 10y = 8$$

Riešenie. Urobme Euklidov algoritmus pre dvojicu 6, 10

$$10 = 6 \,.\, 1 + 4$$
$$6 = 4 \,.\, 1 + 2$$
$$4 = 2 \,.\, 2$$

Platí $(6, 10) = 2 \mid 8$, a preto naša rovnica je riešiteľná. Skúmajme teraz rovnicu $6x + 10y = 2$. Na základe Euklidovho algoritmu môžeme nájsť $2 = 6 \,.\, 1 - 4 \,.\, 1 = 6 \,.\, 1 - (10 \,.\, 1 - 6 \,.\, 1) = 6 \,.\, 2 + 10 \,.\, (-1)$. Preto dvojica $(2, -1)$ je riešením rovnice $6x + 10y = 2$. Položme teraz $x_2 = 4 \,.\, x_1 = 8$, $y_2 = 4 \,.\, (-1) = -4$ (pozri časť b) dôkazu vety 11). Dvojica $(8, -4)$ je riešením našej rovnice, lebo $6 \,.\, 8 + 10 \,.\, (-4) = 48 - 40 = 8$.

Pre každú riešiteľnú diofantickú rovnicu už vieme nájsť nejaké riešenie. Ostáva ešte nevyriešená otázka nájdenia všetkých riešení. Teraz sa sústredíme na tento problém.

Nech (x_0, y_0) je nejaké pevné riešenie rovnice (9). Nech dvojica (r, s) je ľubovoľné riešenia rovnice (9). Potom platí

$$ar + bs = c = ax_0 + by_0$$

z toho po úprave máme

$$a(r - x_0) = -b(s - y_0)$$

Nech $(|a|, |b|) = d$. Deľme poslednú rovnosť číslom d

$$\frac{a}{d}(r - x_0) = -\frac{b}{d}(s - y_0) \tag{12}$$

Na základe vety 5 je $\left(\left|\frac{a}{d}\right|, \left|\frac{b}{d}\right|\right) = 1$ a na základe vety 9 potom z rovnosti (12) vyplýva, že $\frac{a}{d}$ je deliteľom čísla $s - y_0$ (pozri *cvičenie 3* odseku I). Možno preto písať (znovu na základe *cvičenia 3* odseku I) $s - y_0 = u \,.\, \frac{a}{d}$. Podobnými úvahami dostaneme $r - x_0 = t \,.\, \frac{b}{d}$ (u a t sú celé čísla). Dosaďme to do (12)

$$\frac{a}{d}\left(\frac{b}{d}t\right) = -\frac{b}{d}\left(\frac{a}{d}u\right)$$

čiže $u = -t$. Zhrňme tieto výsledky do vety:

Veta 12. Nech (x_0, y_0) je jedno pevné riešenie rovnice (9). Potom dvojica (r, s) je riešením rovnice (9) vtedy a len vtedy, keď má tvar

$$r = x_0 + \frac{b}{d} t$$

$$s = y_0 - \frac{a}{d} t$$

kde t je ľubovoľné celé číslo.

Dôkaz. Dokázali sme už, že dvojica, ktorá je riešením rovnice (9), musí mať tento tvar. Zostáva ešte dokázať, že každá dvojica spomínaného tvaru je skutočne riešením rovnice (9).

$$a\left(x_0 + \frac{b}{d} t\right) + b\left(y_0 - \frac{a}{d} t\right) = ax_0 + a\frac{b}{d} t + by_0 - b\frac{a}{d} t = ax_0 + by_0 = c$$

Tým je dôkaz vety ukončený.

Príklad 20. Nájdite všetky riešenia diofantickej rovnice

$$6x + 10y = 8$$

Riešenie. V *príklade 19* sme už našli jedno riešenie: $x_0 = 8$, $y_0 = -4$. Na základe vety 12 teda všetky riešenia našej rovnice majú tvar

$$r = 8 + \frac{10}{2} t = 8 + 5t$$

$$s = -4 - \frac{6}{2} t = -4 - 3t$$

Skutočne, každá taká dvojica je riešením, pretože

$$6(8 + 5t) + 10(-4 - 3t) = 48 + 30t - 40 - 30t = 8$$

Nájdime niekoľko ďalších riešení: ak položíme $t = 0$, dostaneme už známe riešenie (8, —4); ak položíme $t = -1$, dostaneme riešenie (3, —1); ak položíme $t = -2$, máme riešenie (—2, 2) atď.

Príklad 21. Teraz pri riešení diofantickej rovnice

$$18x - 30y = 60$$

ukážeme celkový postup pri riešení diofantických rovníc (lineárnych s dvoma neznámymi).

Riešenie. Aplikujme Euklidov algoritmus na dvojicu 30, 18.

$$30 = 18 \,.\, 1 + 12$$

$$18 = 12 \,.\, 1 + 6$$

$$12 = 6 \,.\, 2$$

Teda $(18, 30) = 6 \mid 60$, a preto rovnica je riešiteľná. Z Euklidovho algoritmu dostaneme: $6 = 18 - 12 = 18 - (30 - 18) = 18 \,.\, 2 + 30 \,.\, (-1)$, čiže $6 = 18 \,.\, 2 - 30 \,.\, 1$. Ďalej, $60 = (18, 30) \,.\, 10$, a tak $x_2 = x_1 \,.\, 10 = 20$, $y_2 = y_1 \,.\, 10 = 10$. Toto je jedno riešenie našej rovnice. Preto všetky riešenia majú tvar

$$r = 20 + \frac{30}{6} \,.\, t = 20 + 5t$$

$$s = 10 - \frac{18}{6} \,.\, t = 10 - 3t$$

kde t je ľubovoľné celé číslo. Skutočne: $18(20 + 5t) - 30(10 - 3t) = 60$. Ďalšie riešenia:

$$t = 1, \quad r = 25, s = 13;$$

$$t = -3, r = 5, \quad s = 1;$$

$$t = -4, r = 0, \quad s = -2$$

Pri matematických úlohách a hádankách sa však (okrem celočíselnosti) kladú ďalšie podmienky na riešenie diofantických rovníc. Napríklad v spomínanej úlohe o rozliatí M litrov tekutiny do 3-litrových a 6-litrových nádob (vedie to na diofantickú rovnicu $3x + 6y = M$) sa predpokladá, že x a y sú nezáporné čísla. Táto podmienka nezápornosti je veľmi častá.

Diofantická rovnica je buď neriešiteľná, alebo má v obore celých čísel nekonečne mnoho riešení (t prebieha všetky celé čísla). Naproti tomu počet riešení nejakej úlohy — pod vplyvom ďalších podmienok — býva obyčajne konečné číslo.

Príklad 22. Zistite, koľkými spôsobmi možno 45 litrov vody rozliať do 3-litrových a 6-litrových nádob.

Riešenie. Úloha vedie k diofantickej rovnici

$$3x + 6y = 45$$

Pretože $(3, 6) = 3 \mid 45$, rovnica je riešiteľná. Ďalej: $3 \,.\, 1 + 6 \,.\, 0 = 3$, a tak $3 \,.\, 15 + 6 \,.\, 0 = 45$. Všetky riešenia našej rovnice sú dvojice tvaru

$$r = 15 + 2t, \qquad s = -t$$

Diofantická rovnica má teda nekonečne mnoho riešení, našej úlohe však vyhovujú len tie dvojice, pre ktoré platí $r \geqq 0$, $s \geqq 0$, čiže

$$15 + 2t \geqq 0, \qquad -t \geqq 0; \qquad -\frac{15}{2} \leqq t \leqq 0$$

Ľahko sa možno presvedčiť, že obidvom nerovnostiam vyhovujú len celé čísla $t = -7$ $-6, -5, -4, -3, -2, -1, 0$. Úloha má sedem riešení; sú to:

t	-7	-6	-5	-4	-3	-2	-1	0
x	1	3	5	7	9	11	13	15
y	7	6	5	4	3	2	1	0

Cvičenia

1. Zistite, ktoré z nasledujúcich diofantických rovníc sú riešiteľné:

a) $2x - 3y = 1$,
b) $16x + 48y = 40$,
c) $42x - 72y = 32$,
d) $10x + 4y = 16$.

2. Dokážte: Ak $(a, b) = 1$, tak diofantická rovnica $ax + by = c$ je riešiteľná pre ľubovoľné celé číslo c.

3. Riešte diofantickú rovnicu $15x - 20y = 100$.

4. Určte všetky čísla x, pre ktoré je výraz $\frac{17x - 2}{15}$ celým číslom.

5. Nájdite všetky také riešenia diofantickej rovnice $24x - 30y = 12$, pre ktoré platí $x > 0$, $y \geqq 1$.

6. Zistite, akými spôsobmi sa dá 100-korunová bankovka rozmeniť na 10-koruny a 3-koruny.

7. Vedeli by ste nájsť všetky riešenia diofantickej rovnice $ax + by = 0$?

8. Dokážte: Lineárna diofantická rovnica s troma neznámymi $ax + by + cz = d$ je riešiteľná len vtedy, ak $(|a|, |b|, |c|) \mid d$.

9. Dokážte: Ak diofantická rovnica $ax + by = c$ je riešiteľná, potom má jedno také riešenie (x_0, y_0) že platí $x_0 \leqq b$.

10. Dokážte: Rovnica $ax + by = c$ je riešiteľná vtedy a len vtedy, keď $(a, b) = (a, b, c)$.

V. Pytagorejské trojuholníky a Fermatov problém

V tomto odseku sa budeme zaoberať ďalšou zaujímavou diofantickou rovnicou

$$x^2 + y^2 = z^2 \tag{13}$$

ktorú poznáme z geometrie: ak x, y a z sú stranami pravouhlého trojuholníka, potom sú zviazané vzťahom (13) (Pytagorova veta). Trojicu prirodzených čísel $T = (x, y, z)$, pre ktoré platí (13), budeme nazývať pytagorejským trojuholníkom.

Dajme si teraz za úlohu nájsť všetky pytagorejské trojuholníky.

Predovšetkým si musíme uvedomiť, že keď $(x, y) = d > 1$, tak $d^2 \mid x^2$, $d^2 \mid y^2$ (pozri *cvičenie 8* odseku II), a tak na základe vety 6 $d^2 \mid z^2$, a preto $d \mid z$ (znova *cvičenie 8* odseku II). Nech $x = dx_1$, $y = dy_1$, $z = dz_1$. Dosaďme to do (13), a potom celú rovnicu deľme číslom d^2; dostaneme

$$x_1^2 + y_1^2 = z_1^2 \tag{14}$$

Podľa vety 5 je $(x_1, y_1) = 1$ a dá sa ľahko dokázať, že potom aj $(y_1, z_1) = (x_1, z_1) = 1$. Pytagorejský trojuholník, ktorého čísla sú po dvoch nesúdeliteľné, sa nazýva primitívny.

Napríklad $T = (3, 4, 5)$ je primitívny, ale $T' = (6, 8, 10)$ nie je primitívny pytagorejský trojuholník.

Vychádzajúc z týchto úvah už ľahko možno dokázať vety:

Veta 13. Ak $T = (x, y, z)$ je pytagorejský trojuholník, tak trojica (cx, cy, cz) je pre každé prirodzené číslo c tiež pytagorejským trojuholníkom.

Veta 14. Každý pytagorejský trojuholník (x, y, z) sa dá napísať v tvare $(x, y, z) = (cx_1, cy_1, cz_1)$, kde c je prirodzené číslo a (x_1, y_1, z_1) je primitívny pytagorejský trojuholník.

Napríklad $(3, 4, 5)$ je pytagorejský trojuholník, a preto pre ľubovoľné prirodzené číslo c je aj trojica $(3c, 4c, 5c)$ pytagorejským trojuholníkom. Skutočne: $(3c)^2 + (4c)^2 = 25c^2 = (5c)^2$.

Trojica $(10, 24, 26)$ je pytagorejský trojuholník, ale nie primitívny, lebo $(10, 24) = 2 > 1$. Možno ho však dostať z primitívneho pytagorejského trojuholníka $(5, 12, 13)$ tak, že všetky čísla vynásobíme dvoma.

Aby sme vyriešili vytýčenú úlohu, stačí nájsť všetky primítívne pytagorejské trojuholníky.

Nech $T = (x, y, z)$ je primitívny pytagorejský trojuholník, potom jedno z čísel x a y je párne, druhé nepárne. Skutočne: obidve tieto čísla nemôžu byť párne, lebo sú nesúdeliteľné; keby boli obidve nepárne, zasa ich druhá mocnina by mala tvar $4k + 1$ (pozri dôkaz vety 1) a súčet ich druhých mocnín by mal tvar $4s + 2$; na základe vety 1 však z^2 nemôže mať tento tvar. Bez újmy na všeobecnosti možno predpokladať, že x je nepárne, y párne (pretože x a y vystupujú v tejto úlohe symetricky). Rovnicu (13) možno napísať v tvare

$$x^2 = z^2 - y^2 = (z + y)(z - y) \tag{15}$$

Z vyššie urobeného predpokladu (x je nepárne, y párne) vyplýva, že z je nepárne, a tak $y + z$ a $z - y$ sú nepárne čísla (súčet párneho čísla s nepárnym číslom je nepárne číslo). Nech $(z + y, z - y) = d > 1$. Potom na základe vety 2 je $d \mid 2z = (z + y) + (z - y)$ a $d \mid 2y = (z + y) - (z - y)$. Na základe vety 9 potom $d \mid z$, $d \mid y$ (pretože d je

nepárne číslo, a tak $(2, d) = 1$), ale to je spor s predpokladom, že T je primitívny pytagorejský trojuholník. Teda $(z + y, z - y) = 1$. Na základe *cvičenia 9* odseku II možno písať

$$\begin{aligned} z + y &= r^2 \\ z - y &= s^2 \end{aligned} \tag{16}$$

kde r a s sú (nesúdeliteľné a nepárne) celé čísla.

Teraz, z rovnice (15), dostávame

$$x^2 = r^2 s^2, \qquad \text{čiže} \qquad x = rs$$

Z rovností (16) zase môžeme vyjadriť y a z

$$y = \frac{r^2 - s^2}{2}$$

$$z = \frac{r^2 + s^2}{2}$$

Naopak, zoberme dve nesúdeliteľné a nepárne prirodzené čísla r a s $(r > s)$. Položme

$$x = rs, \qquad y = \frac{r^2 - s^2}{2}, \qquad z = \frac{r^2 . s^2}{2}$$

Potom

$$x^2 + y^2 = (rs)^2 + \left(\frac{r^2 - s^2}{2}\right)^2 = r^2 s^2 + \frac{r^4 - 2r^2 s^2 + s^4}{4} =$$

$$= \frac{r^4 + 2r^2 s^2 + s^4}{4} = \left(\frac{r^2 + s^2}{2}\right)^2 = z^2$$

čiže trojica (x, y, z) tvorí pytagorejský trojuholník. Ľahko sa možno presvedčiť, že je to primitívny pytagorejský trojuholník, t. j. že platí $(x, y) = 1$ (vyplýva to z podmienky $(r, s) = 1$).

Zhrnutím dostávame vetu:

Veta 15. Trojica (x, y, z) je primitívnym pytagorejským trojuholníkom s párnym y vtedy a len vtedy, keď

$$x = rs, \qquad y = \frac{r^2 - s^2}{2}, \qquad z = \frac{r^2 + s^2}{2}$$

kde r a s sú nesúdeliteľné prirodzené nepárne čísla, pričom $r > s$.

Poznámka. Ak by sme skúmali prípad, keď x je párne a y nepárne, nedostali by sme nijaké ďalšie primitívne pytagorejské trojuholníky (iba označenie odvesien by bolo zamenené).

Nájdime niekoľko pytagorejských trojuholníkov. Ak položíme $r = 3$, $s = 1$, tak $x = 3$, $y = 4$, $z = 5$. To je tá dobre známa trojica. Ak $r = 5$, $s = 1$, tak $x = 5$, $y = 12$, $z = 13$, čiže trojica, s ktorou sme sa už tiež stretli vyššie. Novú trojicu dostaneme, ak položíme $r = 5$, $s = 3$: $x = 15$, $y = 8$, $z = 17$. Skutočne: $x^2 + y^2 = 225 + 64 = 289 = 17^2 = z^2$.

Rovnica (13) má teda nekonečne mnoho riešení a našli sme ich pomerne ľahko. Práve preto nás prekvapuje nasledujúca veta a ťažkosti vyskytnuvšie sa pri jej dôkaze.

Veta 16. Nech n je prirodzené číslo väčšie ako 2. Neexistujú také prirodzené čísla x, y a z, aby platilo

$$x^n + y^n = z^n$$

Veta 16 — ktorá je vlastne iba domnienkou — sa nazýva veľkou Fermatovou vetou a má túto históriu. Francúzsky matematik P. Fermat (1601—1665) napísal na okraj jednej knihy, že našiel dôkaz (vety 16), ale pre nedostatok miesta ho, vraj, tam neuvádza. Po Fermatovej smrti niekto našiel túto poznámku a pokúsil sa Fermatovu vetu dokázať. Od tej doby sa mnohí slávni matematici (ale aj nematematici) pokúsili nájsť dôkaz tejto vety, ale nikomu sa to nepodarilo. Bolo vypísaných viac vysokých cien na nájdenie dôkazu, ale nikto ich doteraz nezískal, lebo dodnes nie je známy úplný dôkaz (je známe, že pre niektoré prirodzené čísla n je Fermatova veta správna). Pritom spomínaná veta zohrala v teórii čísel (ale aj v celej matematike) mimoriadnu úlohu, lebo mnohí matematici v snahe o dôkaz vymysleli veľa užitočných matematických výsledkov.

Cvičenia

1. Dokážte: Nech prirodzené čísla x_1, y_1, z_1 splňujú rovnosť $x_1^2 + y_1^2 = z_1^2$, potom z podmienky $(x_1, y_1) = 1$ vyplýva $(x_1, z_1) = (y_1, z_1) = 1$.

2. Dokážte vetu 13.

3. Dokážte vetu 14.

4. Dokážte: Ak $z = r^2 + s^2$ a z je nepárne, tak r a s sú opačnej parity.

5. Dokážte: Nech $x = r^2 - s^2$, $y = 2rs$, potom ak $(r, s) = 1$, tak aj $(x, y) = 1$.

6. Dokážte: Rovnica $x^2 + y^2 = 3z^2$ nemá riešenie v prirodzených číslach.

7. Nájdite všetky primitívne pytagorejské trojuholníky, pre ktoré je $z < 30$.

8. Dokážte: Neexistujú prirodzené čísla x, y a $n > 1$ tak, aby platilo $x^n + y^n = 3^n$.

9. Dokážte: Ak platí (13) tak a) aspoň jedno z čísel x a y je deliteľné troma, b) aspoň jedno z čísel x, y a z je deliteľné piatimi.

10. Dokážte, že existuje viac ako 1 000 000 primitívnych pytagorejských trojuholníkov.

Možno sa čitateľ domnieva, že obmedziť sa na začiatku článku len na deliteľnosť prirodzených čísel nebolo správne (ďalej sme aj tak museli niekde pracovať aj s deliteľnosťou celých čísel!). Vychádzali sme však z myšlienky uviesť neskúseného čitateľa do teórie čísel čím jednoduchšími pojmami.

Vedome sme tu nikde nepoužili pojem prvočísel a rozkladu prirodzených čísel na prvočinitele (hoci by sa tým mnohé úvahy podstatne zjednodušili).

Literatúra

[1] Schwarz, Š.: Algebraické čísla. SPN.

[2] Davydov, U. S.—Znám, Š.: Teória čísel. SPN, Bratislava 1966.

[3] Niven, I.—Zuckerman, H. S.: An introduction to the theory of numbers. John Wiley, 1966.