

## Seminár 20: Teória čísel IV – prvočísla

### Ciele

Precvičiť so študentmi rôzne úlohy o prvočíslach, pri riešení ktorých sa uplatnia poznatky o deliteľnosti nadobudnuté v seminároch 7 a 8.

### Úlohy a riešenia

**Úloha 20.1.** [63-I-3-N2] Číslo  $n$  je súčinom dvoch rôznych prvočísel. Ak zvážime menšie z nich o 1 a druhé ponecháme, ich súčin sa zväčší o 7. Určte číslo  $n$ .

**Riešenie.** Označme  $p < q$  prvočísla zo zadania. Potom platí  $(p+1)q = pq + 7$ . Po roznásobení ľavej strany a odčítaní výrazu  $pq$  od oboch strán rovnosti dostávame  $q = 7$ . Prvočíсло  $p$  má byť menšie ako  $q$ , preto  $p \in \{2, 3, 5\}$  a hľadaným číslom  $n$  je tak jedno z čísel 14, 21 alebo 35.

**Úloha 20.2.** [63-I-3-N4] Číslo  $n$  je súčinom dvoch prvočísel. Ak zvážime každé z nich o 1, ich súčin sa zväčší o 35. Určte číslo  $n$ .

**Riešenie.** Podobne ako v predchádzajúcom prípade označme  $p \leq q$  (nie nutne rôzne) prvočísla zo zadania a to prepíšme do tvaru rovnosti  $(p+1)(q+1) = pq + 35$ . Po úprave dostávame  $p+q = 34$ . Hľadáme teda dvojice prvočísel, ktorých súčet bude 34. Takými sú jedine 3 a 31, 5 a 29, 11 a 23, 17 a 17. Riešením úlohy je potom  $n \in \{93, 145, 253, 289\}$ .

**Komentár.** Úvodné dve jednoduché úlohy majú prípravný charakter na úlohu nasledujúcu a sú skôr rozcvičkou, než náročnou aplikáciou vedomostí o prvočíslach.

**Úloha 20.3.** [63-I-3] Číslo  $n$  je súčinom troch rôznych prvočísel. Ak zvážime dve menšie z nich o 1 a najväčšie ponecháme nezmenené, zväčší sa ich súčin o 915. Určte číslo  $n$ .

**Riešenie\*.** Nech  $n = pqr$ ,  $p < q < r$ . Rovnosť  $(p+1)(q+1)r = pqr + 915$  ekvivalentne upravíme na tvar  $(p+q+1) \cdot r = 915 = 3 \cdot 5 \cdot 61$ , z ktorého vyplýva, že prvočíсло  $r$  môže nadobudnúť len niektorú z hodnôt 3, 5 a 61. Pre  $r = 3$  ale z poslednej rovnice dostávame  $(p+q+1) \cdot 3 = 3 \cdot 5 \cdot 61$ , čiže  $p+q = 304$ . To je spor s tým, že  $r$  je najväčšie. Analogicky zistíme, že nemôže byť ani  $r = 5$ . Je teda  $r = 61$  a  $p+q = 14$ . Vyskúšaním všetkých možností pre  $p$  a  $q$  vyjde  $p = 3$ ,  $q = 11$ ,  $r = 61$  a  $n = 3 \cdot 11 \cdot 61 = 2013$ .

**Komentár.** Úloha vyžaduje vhodnú manipuláciu rovnosti zo zadania a potom už len dostatočne pozornú analýzu vzniknutých možností.

**Úloha 20.4.** [64-S-3] Nájdite najmenšie prirodzené číslo  $n$  s ciferným súčtom 8, ktoré sa rovná súčinu troch rôznych prvočísel, pričom rozdiel dvoch najmenších z nich je 8.

**Riešenie\*.** Hľadané číslo  $n$  je súčinom troch rôznych prvočísel, ktoré označíme  $p, q, r$ ,  $p < q < r$ . Číslo  $n = pqr$  má ciferný súčet 8, ktorý nie je deliteľný tromi, preto ani  $n$  nie je deliteľné tromi a teda  $p, q, r \neq 3$ . Napokon hľadané číslo  $n$  nie je deliteľné ani dvoma, pretože by muselo byť  $p = 2$  a  $q = p+8 = 10$ , čo nie je prvočíсло. Musí teda byť  $p = 5$ .

Ak je  $p = 5$ , je  $q = p+8 = 13$ , takže  $r \in \{17, 19, 23, 29, 31, \dots\}$  a  $n \in \{1105, 1235, 1495, 1885, 2015, \dots\}$ . V tejto množine je zrejme najmenšie číslo s ciferným súčtom 8 číslo 2015.

Ak je  $p > 5$ , je  $p = 11$  najmenšie prvočíslo také, že aj  $q = p + 8$  je prvočíslo. Preto  $p = 11$ ,  $q = 19$ , a teda  $r = 23$ , takže pre zodpovedajúce čísla  $n$  platí  $n = 11 \cdot 19 \cdot 23 = 4807 > 2015$ .

**Komentár.** Úloha príjemne spája poznatky o deliteľnosti a prvočíslach a nemala by pre študentov byť neprekonateľnou výzvou.

**Úloha 20.5.** [57-S-1] Nájdite všetky dvojice prirodzených čísel  $a, b$  väčších ako 1 tak, aby ich súčet aj súčin boli mocniny prvočísel.

**Riešenie\*.** Z podmienky pre súčin vyplýva, že  $a$  aj  $b$  sú mocninami toho istého prvočísla  $p$ :  $a = p^r$ ,  $b = p^s$ , pričom  $r, s$  sú celé kladné čísla. Keby bolo  $p$  nepárne, bol by súčet  $a + b$  deliteľný okrem čísla  $p$  aj číslom 2, takže by nebol mocninou prvočísla. Teda  $p = 2$ . Ak  $r < s$ , je súčet  $a + b = 2^r(1 + 2^{s-r})$  opäť číslo párne deliteľné nepárnym číslom väčším ako 1, nie je teda mocninou prvočísla. K rovnakému záveru dôjdeme aj v prípade, keď  $r > s$ . Ostáva preto jediná možnosť:  $a = b = 2^r$ , pričom  $r$  je celé kladné číslo. Skúška  $a + b = 2^r + 2^r = 2^{r+1}$  a  $ab = 2^{2r}$  potvrdzuje, že riešením sú všetky dvojice  $(a, b) = (2^r, 2^r)$ , kde  $r$  je celé kladné číslo.

**Úloha 20.6.** [65-I-1-D2, resp. 55-II-4] Nájdite všetky dvojice prvočísel  $p$  a  $q$ , pre ktoré platí  $p + q^2 = q + 145p^2$ .

**Riešenie\*.** Pre prvočísla  $p, q$  má platiť  $q(q-1) = p(145p-1)$ , takže prvočíslo  $p$  delí  $q(q-1)$ . Prvočíslo  $p$  nemôže deliť prvočíslo  $q$ , pretože to by znamenalo, že  $p = q$ , a teda  $145p = p$ , čo nie je možné. Preto  $p$  delí  $q-1$ , t. j.  $q-1 = kp$  pre nejaké prirodzené  $k$ . Po dosadení do daného vzťahu dostaneme podmienku

$$p = \frac{k+1}{145-k^2}.$$

Vidíme, že menovateľ zlomku na pravej strane je kladný jedine pre  $k \leq 12$ , zároveň však pre  $k \leq 11$  je jeho čitateľ menší ako menovateľ:  $k+1 \leq 12 < 24 \leq 145k^2$ . Iba pre  $k = 12$  tak vyjde  $p$  prirodzené a prvočíslo,  $p = 13$ . Potom  $q = 157$ , čo je tiež prvočíslo. Úloha má jediné riešenie.

**Komentár.** Úloha opäť ukazuje, že upravenie podmienok zo zadania do vhodného tvaru, o ktorom môžeme ďalej diskutovať, je často kľúčovým krokom v riešení. V tomto prípade ide o podmienku  $q = kp + 1$  a následný rozbor hodnôt v čitateli a menovateli zlomku. To by v študentoch malo umocniť dojem, že zručné narábanie s algebraickými výrazmi nájde svoje široké uplatnenie.

**Úloha 20.7.** [62-I-5] Určte všetky celé čísla  $n$ , pre ktoré  $2n^3 - 3n^2 + n + 3$  je prvočíslo.

**Riešenie\*.** Ukážeme, že jedinými celými číslami, ktoré vyhovujú úlohe, sú  $n = 0$  a  $n = 1$ .

Upravme najskôr výraz  $V = 2n^3 - 3n^2 + n + 3$  nasledujúcim spôsobom:

$$V = (n^3 - 3n^2 + 2n) + (n^3 - n) + 3 = (n-2)(n-1)n + (n-1)n(n+1) + 3.$$

Oba súčiny  $(n-2)(n-1)n$  a  $(n-1)n(n+1)$  v upravenom výraze  $V$  sú deliteľné tromi pre každé celé číslo  $n$  (v oboch prípadoch sa jedná o súčin troch po sebe idúcich celých čísel), takže výraz  $V$  je pre všetky celé čísla  $n$  deliteľný tromi. Hodnota výrazu  $V$  je preto prvočíslom práve vtedy, keď  $V = 3$ , teda práve vtedy, keď súčet oboch spomenutých súčinov je rovný nule:

$$0 = (n-2)(n-1)n + (n-1)n(n+1) = n(n-1)[(n-2) + (n+1)] = n(n-1)(2n-1).$$

Poslednú podmienku však spĺňajú iba dve celé čísla  $n$ , a to  $n = 0$  a  $n = 1$ . Tým je úloha vyriešená.

*Poznámka.* Fakt, že výraz  $V$  je deliteľný tromi pre ľubovoľné celé  $n$ , môžeme odvodiť aj tak, že doňho postupne dosadíme  $n = 3k$ ,  $n = 3k + 1$  a  $n = 3k + 2$ , pričom  $k$  je celé číslo, rozdelíme teda všetky celé čísla  $n$  na tri skupiny podľa toho, aký dávajú zvyšok po delení tromi.

**Komentár.** Aj keď vzorové riešenie môže vyzeráť trikovo, po vyskúšaní niekoľko málo hodnôt  $n$  je vždy hodnota zo zadania deliteľná 3, čo by študentov mohlo priviesť na myšlienku skúsiť dokázať deliteľnosť čísla zo zadania tromi.

**Úloha 20.8.** [[?], príklad 2.3, str. 174] Nájdite všetky prvočísla, ktoré sú súčasne súčtom a rozdielom dvoch vhodných prvočísel.

**Riešenie\*.** Predpokladajme, že prvočíslo  $p$  je súčasne súčtom aj rozdielom dvoch prvočísel. Potom je však  $p > 2$  a teda je  $p$  nepárne. Pretože je  $p$  zároveň súčet aj rozdiel dvoch prvočísel, jedno z nich musí byť vždy párne, teda 2. Takže hľadáme prvočísla  $p, p_1, p_2$  tak, že  $p = p_1 + 2 = p_2 - 2$ , teda  $p_1, p, p - 2$  sú tri po sebe idúce nepárne čísla a teda práve jedno z nich je deliteľné tromi (študenti by si mali rozmyslieť prečo). Avšak tromi je deliteľné jediné prvočíslo 3, odkiaľ vzhľadom na to, že  $p_1 \geq 1$  vyplýva  $p_1 = 3$ ,  $p = 5$  a  $p_2 = 7$ . Jediné prvočíslo vyhovujúce zadaniu je teda  $p = 5$ .

**Komentár.** Úloha, ktorá vyžaduje viac uvažovania, než tvrdého počítania, je zaujímavá práve jediným výsledkom.

**Úloha 20.9.** [[?], príklad 3, str. 95] Nájdite celočíselné riešenia rovnice

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{p},$$

kde  $p$  je pevne dané prvočíslo.

**Riešenie\*.** Ak existujú vôbec nejaké riešenia vyšetrovanej rovnice, potom sú nenulové. Preto môžeme rovnicu upraviť na ekvivalentný tvar  $yx - px - py = 0$ , resp.  $(x - p)(y - p) - p^2 = 0$ , a teda

$$(x - p)(y - p) = p^2.$$

Odtiaľ je vidieť, že celočíselné riešenia môžeme dostať len vtedy, ak  $x - p$  prebehne všetkých deliteľov čísla  $p^2$ , pričom  $y - p$  prebehne doplnkové delitele. Pretože je  $p$  prvočíslo, musí byť nutne

$$x - p \in \{1, p, p^2, -1, -p, -p^2\}.$$

Pretože  $x \neq 0$ , odpadá  $x - p = -p$ . Ostáva teda

$$x \in \{1 + p, 2p, p + p^2, p - 1, p - p^2\} \quad \text{a teda} \quad y \in \{p + p^2, 2p, 1 + p, p - p^2, p - 1\}.$$

Tieto hodnoty sú skutočne riešením, o čom sa môžeme presvedčiť skúškou.

**Komentár.** Úloha, v ktorej opäť predtým, než uplatníme znalosti o deliteľnosti, príp. prvočíslach, musíme umne upraviť východiskový tvar rovnice.

## Domáca práca

**Úloha 20.10.** [65-I-1] Nájdite všetky možné hodnoty súčinu prvočísel  $p, q, r$ , pre ktoré platí

$$p^2 - (q + r)^2 = 637.$$

**Riešenie\*.** Ľavú stranu danej rovnice rozložíme na súčin podľa vzorca pre  $A^2 - B^2$ . V takto upravenej rovnici

$$(p + q + r)(p - q - r) = 637$$

už ľahko rozoberieme všetky možnosti pre dva celočíselné činitele naľavo. Prvý z nich je väčší a kladný, preto aj druhý musí byť kladný (lebo taký je ich súčin), takže podľa rozkladu na súčin prvočísel čísla  $637 = 7^2 \cdot 13$  ide o jednu z dvojíc  $(637, 1)$ ,  $(91, 7)$  alebo  $(49, 13)$ . Prvočíslo  $p$  je zrejme aritmetickým priemerom oboch činiteľov, takže sa musí rovnať jednému z čísel  $\frac{1}{2}(637 + 1) = 319$ ,  $\frac{1}{2}(91 + 7) = 49$ ,  $\frac{1}{2}(49 + 13) = 31$ . Prvé dve z nich však prvočísla nie sú ( $319 = 11 \cdot 29$  a  $49 = 7^2$ ), tretie áno. Takže nutne  $p = 31$  a prislúchajúce rovnosti  $31 + q + r = 49$  a  $31 - q - r = 13$  platia práve vtedy, keď  $q + r = 18$ . Také dvojice prvočísel  $\{q, r\}$  sú iba  $\{5, 13\}$  a  $\{7, 11\}$  (stačí prebrať všetky možnosti, alebo si uvedomiť, že jedno z prvočísel  $q, r$  musí byť aspoň  $18 : 2 = 9$ , nanaľvýš však  $18 - 2 = 16$ ). Súčin  $pqr$  tak má práve dve možné hodnoty, a to  $31 \cdot 5 \cdot 13 = 2015$  a  $31 \cdot 7 \cdot 11 = 2387$ .

## Doplňujúce zdroje a materiály

Ďalšie zaujímavé príklady je možné nájsť v [?], paragraf 2 a taktiež v [?].