

8. PRVOČÍSLA

Prvočísly sa zaoberali už antickí Gréci. Od nich, presnejšie od Euklida, pochádza prvý dôkaz toho, že existuje nekonečne veľa prvočísel. Ukážeme si ho na nasledujúcich troch úlohách. Dokážeme, že ku každej konečnej množine prvočísel existuje prvočíslo, ktoré do nej nepatrí.

Úloha 170. Nech $p_1, \dots, p_n$ sú prvočísla. Dokážte, že číslo $p_1 \dots p_n + 1$ nie je deliteľné žiadnym z čísel $p_1, \dots, p_n$.

Úloha 171. Ak $p_1, \dots, p_n$ sú prvočísla, potom existuje prvočíslo p_{n+1} rôzne od $p_1, \dots, p_n$.

(Návod: Bude to prvočíselný deliteľ čísla $p_1 \dots p_n + 1$.)

Úloha 172. Dokážte, že existuje nekonečne veľa prvočísel.

Úloha 173. Nech $2 = p_1 < p_2 < \dots < p_n < \dots$ je postupnosť všetkých prvočísel usporiadaná podľa veľkosti. Potom

$$p_{n+1} \leq p_1 \dots p_n + 1.$$

Dokážte.

(Návod: Použite postup z úlohy 170.)

Dnes už poznáme veľmi veľa dôkazov o existencii prvočísel. Uvedieme si ešte jeden, ktorý využíva vlastnosti kongruencií. Je založený na skutočnosti, že postupnosť čísel $2^{2^n} + 1$ nemá spoločných deliteľov.

Úloha A. Nech $p \mid (2^{2^n} + 1, 2^{2^{n+1}} + 1)$. Potom $1 \equiv -1 \pmod{p}$.

Úloha B. Nech $d \mid (2^{2^n} + 1, 2^{2^m} + 1)$ pre $m < n$. Potom $d = 1$.

Úloha C. Pomocou úlohy B dokážte, že existuje nekonečne veľa prvočísel.

Ďalší dôkaz nekonečnosti množiny prvočísel spočíva v divergencii harmonického radu. Nech by $p_1, p_2, \dots, p_k$ boli všetky prvočísla. Potom

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{1}{n} &= \sum_{\alpha_1=0}^{\infty} \sum_{\alpha_2=0}^{\infty} \dots \sum_{\alpha_k=0}^{\infty} \frac{1}{p_1^{\alpha_1} \dots p_k^{\alpha_k}} = \left(\sum_{\alpha_1=0}^{\infty} \frac{1}{p_1^{\alpha_1}} \right) \dots \left(\sum_{\alpha_k=0}^{\infty} \frac{1}{p_k^{\alpha_k}} \right) = \\ &= \frac{p_1}{p_1 - 1} \dots \frac{p_k}{p_k - 1} < \infty. \end{aligned}$$

Dostávame spor s divergenciou harmonického radu. Na tomto dôkaze je zaujímavá skôr táto súvislosť ako nový poznatok.

Teraz si ukážeme, že v postupnosti všetkých prvočísel existujú ľubovoľne veľké medzery. Presnejšie povedané, pre každé n existuje postupnosť po sebe idúcich prirodzených čísel, ktorá má n členov a neobsahuje žiadne prvočíslo.

Úloha 174. Nech $n \geq 2$. Dokážte, že každé z čísel

$$(n+2)! + 2, \dots, (n+2)! + n + 2$$

je zložené číslo.

Analogickým postupom ako pri Euklidovom dôkaze si teraz dokážeme dva špeciálne prípady takzvanej *Dirichletovej vety*.

Dirichletova veta. Ak $a, b \in \mathbb{N}$ a $(a, b) = 1$, potom v aritmetickej postupnosti $\{an + b\}_{n=1}^{\infty}$ existuje nekonečne veľa prvočísel.

Dôkaz tejto vety je veľmi náročný, a preto ho vynecháme.

Úloha 175. Dokážte, že každé prvočíslo $p > 2$ môžeme vyjadriť v tvare $p = 4k + 1, p = 4k + 3$.

(Návod: $4k, 4k + 2$ nie sú prvočísla.)

Úloha 176. Ak $p_1 = 4k_1 + 1, \dots, p_n = 4k_n + 1$ sú prirodzené čísla, potom existuje $K \in \mathbb{N}$ také, že

$$p_1 \dots p_n = 4K + 1.$$

Dokážte.

(Návod: Postupujte matematickou indukciou alebo využite úlohu 108.)

Úloha 177. Ak $p_1, \dots, p_n$ sú prvočísla väčšie ako 3, potom číslo $4p_1 \dots p_n + 3$ nie je deliteľné žiadnym z čísel $p_1, \dots, p_n$. Dokážte.

Úloha 178. Ak $p_1, \dots, p_n$ sú prvočísla väčšie ako 3, ktoré majú tvar $4k + 3$, potom existuje ďalšie prvočíslo p_{n+1} , ktoré má tvar $4k + 3$. Dokážte.

(Návod: Použite úlohy 175, 176 a 177. Uvažujte, aké sú prvočíselné delitele čísla $4p_1 \dots p_n + 3$.)

Úloha 179. Dokážte, že existuje nekonečne veľa prvočísel, ktoré majú tvar $4k + 3$.

Úloha 180. Dokážte, že existuje nekonečne veľa prvočísel, ktoré majú tvar $6k + 5$.

Ďalší špeciálny prípad Dirichletovej vety dokážeme v kapitole primitívne korene.

Teraz si ukážeme jednu z metód, pomocou ktorej môžeme zistiť, či nejaké prirodzené číslo je prvočíslo.

Úloha 181. Ak $n \in \mathbb{N}$ je zložené číslo, potom existuje číslo $d \in \mathbb{N}$ také, že $1 < d \leq \sqrt{n}$ a $d|n$. Dokážte.

Úloha 182. Ak $n \in \mathbb{N}$ je zložené číslo, potom existuje prvočíslo $p \leq \sqrt{n}$ a $p|n$. Dokážte.

Úloha 183. Zistite, či čísla 101 a 103 sú prvočísla.

Úloha 184. Dokážte, že najmenší prirodzený deliteľ väčší ako 1 prirodzeného čísla väčšieho ako 1 je prvočíslo.

Úloha 185. Nájdite kanonický rozklad čísla 1977.

Istú charakterizáciu rozloženia prvočísel na číselnej osi nám dáva nasledujúce tvrdenie.

Veta 10. Nech $m, n, r \in \mathbb{N}$. Ak každé z čísel

$$m, m + r, m + 2r, \dots, m + (n - 1)r$$

je nepárne prvočíslo, potom pre každé prvočíslo $p < n$ platí $p|r$.

Voľne povedané, veta 10 nám hovorí, že aritmetická postupnosť, ktorá obsahuje po sebe nasledujúci väčší počet prvočísel, musí mať dostatočne veľkú diferenciu, a preto neexistuje aritmetická postupnosť, ktorá obsahuje ľubovoľne dlhé úseky zložené iba z prvočísel.

Tento výsledok dokázal v roku 1944 francúzsky matematik Thebault. Dôkaz je jednoduchý, a preto si ho ukážeme.

Úloha 186. Ak platia predpoklady vety 10, potom $m \geq n$. Dokážte.

(Návod: Ak $m < n$, potom $m + mr \in \{m, m + r, m + 2r, \dots, m + (n - 1)r\}$.)

Úloha 187. Nech $p, q_1, \dots, q_r$, $r \geq p$ sú rôzne prvočísla. Potom existujú čísla $i \neq j$ také, že $q_i \equiv q_j \pmod{p}$. Dokážte.

(Návod: Zvyšky $q_1 \pmod{p}, \dots, q_r \pmod{p}$ nadobúdajú najviac $p-1$ hodnôt, nakoľko ani jeden sa nerovná 0.)

Úloha 188. Dokážte vetu 10.

(Návod: Ak $p < n$, potom $p, q_1 = m, q_2 = m + r, \dots, q_{p-1} = m + (p-1)r$ sú navzájom rôzne prvočísla. Použite úlohu 187.)

Úloha A.

- a) Koľko po sebe idúcich nepárnych prvočísel môže obsahovať aritmetická postupnosť $\{1 + 8k\}$?
 b) Koľko po sebe idúcich nepárnych prvočísel môže obsahovať aritmetická postupnosť $\{3 + 64k\}$?

Úloha B. Nech q je nepárne číslo. Dokážte, že aritmetická postupnosť $\{a + kq\}_{k=1}^{\infty}$ neobsahuje prvočíselný úsek žiadnej dĺžky väčšej ako 1.

Úloha C. Aká je maximálna možná dĺžka prvočíselného úseku v aritmetickej postupnosti $\{a + 2 \cdot 3 \cdot \dots \cdot q \cdot k\}_{k=1}^{\infty}$, ak $2, 3, \dots, q$ sú za sebou nasledujúce prvočísla?

Úloha D. Dokážte, že neexistuje aritmetická postupnosť, ktorá by obsahovala ľubovoľne dlhé prvočíselné úseky.

Úloha E. Aká je minimálna možná diferenciacia aritmetickej postupnosti, ktorá obsahuje desať nepárnych prvočísel po sebe?

Ak p je prvočíslo a $n \in \mathbb{N}$, potom symbolom $\deg_p(n)$ označujeme exponent, s ktorým p vystupuje v kanonickom rozklade čísla n . Ak p nie je deliteľom čísla n , potom $\deg_p(n) = 0$.

Úloha 189. Nech p je prvočíslo a $n \in \mathbb{N}$. Potom $k = \deg_p(n)$ práve vtedy, keď $p^k | n$ a $p^{k+1} \nmid n$.

Skutočnosť, že $\deg_p(n) = k$, budeme označovať taktiež symbolom $p^k || n$.

Úloha 190. Nech p je prvočíslo a $n_1, n_2 \in \mathbb{N}$. Potom

$$\deg_p(n_1 n_2) = \deg_p(n_1) + \deg_p(n_2).$$

Dokážte.

Úloha 191. Nech p je prvočíslo a $n \in \mathbb{N}$. Potom

$$\deg_p(n!) = \sum_{k=1}^n \deg_p(k).$$

Dokážte.

Úloha 192. Nech $m, n \in \mathbb{N}$. Potom v množine $\{1, \dots, n\}$ existuje práve $\left\lfloor \frac{n}{m} \right\rfloor$ čísel deliteľných číslom m . Dokážte.

Úloha 193. Nech p je prvočíslo a $n \in \mathbb{N}$, $k \in \mathbb{Z}$, $k \geq 0$. Potom množina $\{1, \dots, n\}$ obsahuje práve

$$\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$$

prírodných čísel m takých, že $\deg_p(m) = k$. Dokážte.

(Návod: Použite úlohy 189, 192.)

Úloha 194. Nech p je prvočíslo a $n \in \mathbb{N}$ a r je také celé číslo, že $p^r \leq n < p^{r+1}$. Potom

$$\deg_p(n!) = \sum_{k=0}^r k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right).$$

Dokážte.

(Návod: Použite úlohy 191, 193.)

Úloha 195. Nech p je prvočíslo, $n \in \mathbb{N}$ a r je také celé číslo, že $p^r \leq n < p^{r+1}$. Potom

$$\deg_p(n!) = \sum_{k=1}^r \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Dokážte.

(Návod: Upravte výraz z úlohy 194 na rozdiel dvoch súm a v druhej sume zmeníte sumačný index.)

Úloha 196. Nech p je prvočíslo a $n \in \mathbb{N}$. Potom

$$\deg_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Dokážte.

(Návod: Úloha sa iba formálne odlišuje od úlohy 195, nakoľko pre $k > r$ je $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$.)

Úloha 197. Nech p je prvočíslo, $n \in \mathbb{N}$ a r je také celé číslo, pre ktoré $p^r \leq n < p^{r+1}$. Potom

$$r \leq \frac{\log n}{\log p}.$$

Dokážte.

Úloha 198. Nech p je prvočíslo a $n \in \mathbb{N}$. Potom

$$\deg_p(n!) = \frac{n}{p-1} + h(p, n),$$

kde $|h(p, n)| \leq \frac{\log n}{\log p}$. Dokážte.

(Návod: Použite úlohy 195, 196, 197 a vzorec pre súčet geometrickej postupnosti.)

Úloha 199. Nech p je prvočíslo. Potom

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \deg_p(n) = \frac{1}{p-1}.$$

Dokážte.

(Návod: Použite úlohy 191, 198.)

Poznamenajme, že ak g je aritmetická funkcia, potom hodnota

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N g(n),$$

sa nazýva *stredný rád aritmetickej funkcie* g , ak táto limita existuje.

Aj dnes existuje veľa nevyriešených otázok týkajúcich sa prvočísel, hoci prvočísla sú objektom pozornosti matematikov počas celej histórie ľudského myslenia. Neexistuje žiadny explicitný vzorec, pomocou ktorého by sme mohli vyjadriť všetky prvočísla. Taktiež doteraz nevieme, či dvojčlen $x^2 + 1$ nadobúda nekonečne veľa prvočíselných hodnôt atď.

Zaujímavú vlastnosť prvočísel obsahuje tvrdenie, ktoré poznáme pod názvom: **Bertrandov postulát**. Ak $n \in \mathbb{N}$ a $n > 1$, potom existuje také prvočíslo p , pre ktoré platí, že $n < p < 2n$.

Dôkaz tohto tvrdenia uvedieme neskôr. Zatiaľ poznamenajme, že je elementárny a je z veľkej miery založený na úlohe 196. Ukážeme si však zaujímavý dôsledok Bertrandovho postulátu.

Úloha 200. Ak $n \in \mathbb{N}$ a $n > 1$, potom číslo $(2n)!$ nie je druhou mocninou žiadneho prirodzeného čísla. Dokážte.

(Návod: Ak p je prvočíslo a $n < p < 2n$, potom $p \mid (2n)!$.)

Úloha 201. Ak $n, k \in \mathbb{N}$ a $n, k > 1$, potom číslo $(n!)^{\frac{1}{k}}$ je iracionálne. Dokážte.

Úloha 202.

- Ak $n, k \in \mathbb{N}$ a $n, k > 1$, potom číslo $[1, \dots, n]^{\frac{1}{k}}$ je iracionálne. Dokážte.
- Dokážte, že čiastočný súčet harmonického radu pre $n > 1$

nie je celé číslo.

$$1 + \frac{1}{2} + \cdots + \frac{1}{n}$$