Co víme o přirozených číslech

3. Prvočísla a čísla složená

In: Jiří Sedláček (author): Co víme o přirozených číslech. (Czech). Praha: Mladá fronta, 1961. pp. 16–23.

Persistent URL: http://dml.cz/dmlcz/403439

3.

PRVOČÍSLA A ČÍSLA SLOŽENÁ

●

Číslo 1 je dělitelné jediným přirozeným číslem, totiž právě číslem 1. Zvolíme-li libovolné přirozené číslo $n > 1$, pak vždycky existují alespoň dvě přirozená čísla, která dělí číslo n. Jsou to čísla 1 a n, kterým říkáme *samozřejmí dělitelé* čísla n. Přirozené číslo $p > 1$, které kromě samozřejmých dělitelů není už dělitelné žádným jiným přirozeným číslem, se nazývá *prvočíslo*. Přirozené číslo $s > 1$, které není prvočíslo, se nazývá *složené*. Ze školy jistě znáte příklady prvočísel

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,...

i příklady čísel složených

4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22,...

Studium prvočísel patří mezi nejstarší a také nejobtížnější otázky, jimiž se matematikové zabývají. Vždyť už starořecká matematika znala důkaz tvrzení, že prvočísel je nekonečně mnoho. Tato matematická poučka je totiž obsažena a dokázána ve známém díle starořeckého matematika *Euklida*, který žil v Alexandrii kolem roku 300 před n. l. Euklidův spis „Základy" obsahoval 13 knih a pracovali na něm vedle Euklida už někteří jeho předchůdci (např. *Eudoxos*, *Theaitetos* aj.)*)

*) Snad vás bude zajímat tato malá historka, kterou dějepisec poznamenal o setkání Euklida s faraonem Ptolemaiem I. Farao prý požádal jednou Euklida, aby mu vyložil jednoduchým způsobem základy geometrie. Euklides odpověděl: „Není pro krále soukromé cesty ke geometrii". Na vysvětlenou uveďme, že králové mívali ke svým komnatám v palácích soukromé schodiště, jehož nesměl nikdo jiný používat.

Hledání nepříliš velkých prvočísel se někdy provádí metodou, která se nazývá *Eratosthenovo síto.**) Chceme-li určit všechna prvočísla, která jsou menší nebo nejvýše rovna danému přirozenému číslu a (většímu než 1), postupujeme takto:

Vypíšeme nejprve po řadě všechna přirozená čísla od čísla 1 do čísla a. Číslo 1, které nepočítáme ani mezi prvočísla ani mezi čísla složená, ponecháme stranou, a další číslo, tj. číslo 2, podtrhneme. Nyní budeme v napsané posloupnosti vyškrtávat každé druhé přirozené číslo tak dlouho, dokud všechna napsaná čísla nevyčerpáme. V dalším kroku se vrátíme opět na začátek napsané posloupnosti a vyhledáme to první číslo, které není ani podtrhnuto ani vyškrtnuto; je to zřejmě číslo 3, a toto číslo tedy podtrhneme. Dále budeme vyškrtávat každé třetí číslo v napsané posloupnosti (pokud ovšem toto číslo už nevypadlo při předcházejícím vyškrtávání). Znovu se vrátíme na začátek posloupnosti, podtrhneme číslo 5 a začneme vyškrtávat každé páté (dosud nevyškrtnuté) přirozené číslo. Tyto kroky opakujeme tak dlouho, dokud je to vůbec možné, tj. dokud nejsou všechna napsaná čísla buď podtržena nebo vyškrtnuta. Dá se snadno ukázat, že tímto postupem najdeme všechna prvočísla, která jsou $\leqq a$. Pro $a = 19$ vypadá konečný zápis takto (tučně = vyškrtnuto):

1, $\underline{2}$, $\underline{3}$, **4**, $\underline{5}$, **6**, $\underline{7}$, **8**, **9**, **10**, $\underline{11}$, **12**, $\underline{13}$, **14**, **15**, **16**, $\underline{17}$, **18**, $\underline{19}$.

Je patrné, že v případě, je-li číslo a je dosti veliké, je metoda Eratosthenova síta velmi pracná. Ostatně studium velkých prvočísel patří mezi nejobtížnější otázky jak po stránce teoretické, tak i po stránce praktické. Práci si můžeme mnohdy usnadnit tím, že nahlédneme do některých

*) Tato metoda je nazvána podle řeckého matematika *Eratosthena* z Kyrene (III. stol. př. n. l.).

matematických tabulek, které obsahují též tabulku prvočísel. Tak např. ve školních matematických tabulkách je tabulka všech prvočísel menších než číslo 1000, zatímco Valouchovy Pětimístné tabulky logaritmické uvádějí všechna prvočísla $\leq$ 5 309. Některé cizojazyčné tabulky dávají možnost seznámit se s prvočísly ještě většími. Tak např. *I. G. Popov* vydal r. 1952 v Moskvě knížku s názvem Математические таблицы, kde jsou uvedena všechna prvočísla menší než 10 000.*)

Všechny uvedené tabulky mohou dobře sloužit ke školským účelům, ale pro účely vědecké je někdy potřebí jít ještě dále. V poslední době bylo při sestavování tabulky prvočísel užito nejmodernějších technických metod. Tak švédští matematikové vypočetli roku 1957 na elektronkovém počítači BESK, že číslo $2^{3217} - 1$ je prvočíslo. Tento číselný obr, který má 969 číslic, je největším prvočíslem, které dnes známe. Pokud se týče soustavné tabulky všech prvočísel, tu nejdále sahá tabulka, kterou r. 1959 připravili *C. L. Baker* a *F. J. Gruenberger*. Tabulka těchto autorů je obsažena na mikrofilmu a je v ní systematicky vypsáno šest miliónů prvočísel. Poslední (šestimiliónté) prvočíslo, které je zde uvedeno, je číslo $p_{6\,000\,000} = 104\,395\,301$.

Nemáme-li po ruce tabulky prvočísel, musíme často výpočtem rozhodovat o tom, zda dané přirozené číslo je prvočíslo nebo číslo složené. V příkladě 9 si připomeneme jednu pomocnou metodu, která je při takových výpočtech velmi užitečná.

Příklad 9. Je-li číslo m složené, pak je vždy možno najít prvočíslo $p \leq \sqrt{m}$, které dělí číslo m.

Řešení. Každé složené číslo m můžeme vyjádřit ve tvaru

*) Posledně jmenované tabulky jsou zajímavé také tím, že v nich najdeme rozklad v prvočinitele pro každé přirozené číslo $\leq$ 4850.

$m = xy$, kde $x > 1, y > 1, x \geqq y$. Kdyby bylo $y > \sqrt{m}$, bylo by též $x > \sqrt{m}$ a z těchto dvou nerovností by plynulo $xy > (\sqrt{m})^2 = m$ tedy $xy > m$. To však je spor s předpokladem $xy = m$, takže o čísle y platí $y \leqq \sqrt{m}$. Je-li y prvočíslo, jsme s hledáním hotovi. Je-li y číslo složené, pak je možno (jak víme ze školy) najít prvočíslo p, které dělí y; přitom je $p < y$ a tedy i $p < \sqrt{m}$. Číslo p je tedy tím prvočíslem, jehož existenci jsme měli v dané úloze prokázat.

V dalších dvou příkladech si ukážeme, jak se prakticky využije poznatku, se kterým jsme se seznámili v příkladě 9.

Příklad 10. Rozhodněte, zda číslo 827 je prvočíslo nebo číslo složené.

Řešení. Přesvědčíme se, že číslo 827 je prvočíslo. K tomu je třeba zjistit, že toto číslo není dělitelné žádným prvočíslem menším než 827. Při tomto zkoumání stačí však přezkoušet jen ta prvočísla, která jsou menší než $\sqrt{827}$, jak plyne z předcházejícího příkladu. Platí $\sqrt{827} \doteq 28{,}7$, takže budeme zde zkoušet jen dělitelnost prvočísly 2, 3, 5, 7, 11, 13, 17, 19 a 23.

Prvočísly 2, 3, 5 a 11 není naše číslo dělitelné, jak plyne ze znaků dělitelnosti probíraných na střední škole. Zbývají nám prvočísla 7, 13, 17, 19 a 23, u nichž musíme dělitelnost prověřit tím, že provedeme příslušné dělení. Tak dělení 827 : 7 vychází se zbytkem 1, dělení 827 : 13 dává zbytek 8 a také zbývající tři případy ukazují, že číslo 827 není dělitelné prvočísly 17, 19, 23.

Odpověď. Číslo 827 je prvočíslo.

Příklad 11. Určete nejmenší čtyřciferné číslo, které je prvočíslem.

Řešení. Nejmenší čtyřciferné číslo vůbec je číslo 1000; je to zřejmě číslo složené. V dalších úvahách si pochopitelně nemusíme všímat čísel sudých. Číslo 1001 je dělitelné jedenácti, takže je složené. Dále platí $1003 = 17 . 59$, číslo 1005 je dělitelné pěti a $1007 = 19 . 53$. Ve všech těchto případech šlo tedy o čísla složená. Snadno se přesvědčíme, že číslo 1009 je prvočíslo. Přitom budeme postupovat obdobným způsobem, s kterým jsme se seznámili při řešení příkladu 10.

Odpověď. Nejmenší čtyřciferné prvočíslo je číslo 1009.

Ze školy jistě víte, že každé složené číslo je možno napsat jako součin několika prvočísel, a to až na pořadí činitelů jediným způsobem. Prvočísla, jejichž součinem je dané složené číslo, jsou tzv. *prvočinitelé.* Vyjádříme-li dané složené číslo jako součin mocnin prvočinitelů, říkáme, že jsme provedli jeho *rozklad v prvočinitele.*

Při řešení některých úloh je třeba nejprve provést rozklad složeného čísla v prvočinitele, jak uvidíme v dalším příkladě.

Příklad 12. Určete nejmenší přirozené číslo, kterým je třeba znásobit číslo 1224, abychom dostali druhou mocninu přirozeného čísla.

Řešení. Nejprve rozložíme číslo 1224 v prvočinitele; platí $1224 = 2^3 . 3^2 . 17$. Prvočísla 2 a 17 jsou zde umocněna lichým exponentem, proto musíme číslo 1224 znásobit alespoň součinem $2 . 17$, abychom dostali druhou mocninu přirozeného čísla. Tato mocnina je pak rovna $2^4 . 3^2 . 17^2 = (2^2 . 3 . 17)^2 = 204^2$.

Odpověď. Nejmenší přirozené číslo, kterým musíme násobit, je číslo 34.

Prvočísla jsou v posloupnosti přirozených čísel rozložena velmi nepravidelně. V některých intervalech pozorujeme, že je tu nakupeno velmi mnoho prvočísel, jinde můžeme opět najít velikou skupinu vytvořenou výhradně z čísel složených. O této otázce nás trochu poučí další příklad.

Příklad 13. Ukažte, že je možno najít tisíc po sobě jdoucích přirozených čísel, jež jsou vesměs složená.

Řešení. Příkladem takové skupiny tisíce po sobě jdoucích složených čísel je skupina*)
$1001! + 2, 1001! + 3, 1001! + 4, 1001! + 5, \ldots,$
$1001! + 1000, 1001! + 1001.$

Číslo $1001! + 2$ je zřejmě dělitelné dvěma, číslo $1001! + $ $+ 3$ třemi a konečně číslo $1001! + 1001$ je dělitelné číslem 1001; všechna tato čísla jsou tedy složená.

Poznamenejme, že z naší úvahy nijak nevyplývá, že v posloupnosti všech přirozených čísel existuje mezi prvočísly mezera obsahující právě 1000 čísel složených. V předcházející úvaze jsme totiž nezkoumali, zda číslo $1001! + 1$ je složené nebo není, a na první pohled je patrno, že číslo $1001! + 1002$ je složené (je totiž sudé).

Závěrem tohoto paragrafu si všimněme jedné aritmetické posloupnosti, v níž po sobě následuje pět prvočísel.

Příklad 14. Pět prvočísel tvoří pět po sobě jdoucích členů aritmetické posloupnosti s diferencí $d = 6$. Určete tato prvočísla.

Řešení. Nejprve ukážeme toto: Je-li a libovolné celé nezáporné číslo, pak alespoň jedno z čísel

$$a, \quad a + 6, \quad a + 12, \quad a + 18, \quad a + 24 \qquad (1)$$

*) Připomeňme, že zápis $n!$ (čti n faktoriál) znamená součin všech přirozených čísel počínaje číslem 1 a konče číslem n; je tedy např. $4! =$ $= 1 . 2 . 3 . 4 = 24$.

je dělitelné pěti. Podle cvičení 9 je možno vyjádřit číslo a v právě jednom ze tvarů $5k$, $5k + 1$, $5k + 2$, $5k + 3$, $5k + 4$. Je-li $a = 5k$, pak první z čísel v řádku (1) je dělitelné pěti. Je-li $a = 5k + 1$, pak $a + 24 = 5k + 25 = 5(k + 5)$, takže poslední z čísel v (1) je pěti dělitelné. Obdobně pro $a = 5k + 2$ vychází $a + 18 = 5(k + 4)$, pro $a = 5k + 3$ je $a + 12 = 5(k + 3)$ a konečně pro $a = 5k + 4$ máme $a + 6 = 5(k + 2)$.

Ukázali jsme tedy, že v řádku (1) je jedno z čísel dělitelné pěti. Podle podmínek uvedených v textu příkladu chceme, aby všechna čísla v řádku (1) byla prvočísla. Z toho vyplývá, že číslo, pro něž jsme před chvílí prokázali dělitelnost pěti, je rovno právě číslu 5. Vzhledem k tomu, že $d = 6$, stojí číslo 5 nutně na prvním místě mezi uvažovanými prvočísly, takže $a = 5$, $a + 6 = 11$, $a + 12 = 17$, $a + 18 = 23$, $a + 24 = 29$.

Zkouška ukazuje, že všech pět nalezených čísel jsou prvočísla.

Odpověď. Úloze vyhovuje jediná pětice prvočísel, totiž 5, 11, 17, 23, 29.*)

Úlohy

15. Pomocí Eratosthenova síta určete všechna prvočísla menší než číslo 100.

16. Rozhodněte zda číslo 2437 je prvočíslo nebo číslo složené. Obdobnou otázku zodpovězte též pro číslo 2771.

17. Rozložte v prvočinitele a) 3248; b) 2418; c) 3819.

*) Čtenář se snadno přesvědčí, že šestý člen uvažované aritmetické posloupnosti již není prvočíslo.

18. Vyhledejte největší prvočíslo, jímž je dělitelné číslo 4812.

19. Určete nejmenší přirozené číslo, kterým je třeba znásobit číslo 600, abychom dostali třetí mocninu přirozeného čísla.

20. Rozhodněte, zda číslo $10! + 1$ je prvočíslo nebo číslo složené.

21. Určete největší trojciferné prvočíslo.

22. *Prvočíselnými dvojčaty* nazýváme takovou dvojici prvočísel (p, q), o nichž platí $q = p + 2$. Vyhledejte všechna prvočíselná dvojčata menší než 100.

23. V posloupnosti přirozených čísel není možno najít mezeru mezi prvočísly obsahující právě tisíc čísel složených. Dokažte.

24. Pět prvočísel tvoří pět po sobě jdoucích členů aritmetické posloupnosti s diferencí $d = 12$. Určete tato prvočísla.

25. Je možno najít pět prvočísel, která tvoří pět po sobě jdoucích členů aritmetické posloupnosti s diferencí $d = 8$?

26. Každé prvočíslo větší než 3 je možno vyjádřit buď ve tvaru $6k + 1$ nebo ve tvaru $6k + 5$, kde k je vhodné celé nezáporné číslo. Dokažte.

27. a) Rozhodněte, zda každé přirozené číslo větší než 3, které je tvaru $6k + 1$, je prvočíslem. b) Obdobnou otázku zodpovězte též pro tvar $6k + 5$.

28. Určete nejmenší složené číslo, které není možno vyjádřit jako součet dvou prvočísel.