Prvočísla a zložené čísla

Mgr. Jana Králiková

U: Predstav si, že máš 16 jabĺčok a máš ich všetky spravodlivo rozdeliť medzi deti. Koľko detí môžeš obdarovať, aby každé z nich dostalo rovnaký počet jaĺčok?

Ž: *Môžem obdarovať štyri deti. Každé by dostalo po štyri jablká.*

U: Sú aj iné možnosti pre počet detí?

Ž: *Áno. Deti by mohli byť dve, alebo štyri, alebo by ich mohlo byť osem.*

U: Mohlo by ich byť aj šestnásť a mohlo by byť aj jedno samotné dieťa. Zapíš do tabuľky všetky možnosti pre počet detí a pre počet jabĺk, ktoré každý z nich dostane.

Ž: *Takže:*

počet detí	1	2	4	8	16
počet jabĺk pre jedno dieťa	16	8	4	2	1

U: Dobre. A teraz to isté urob pre 17 hrušiek.

Ž: *Hrušky mám spravodlivo rozdeliť medzi deti. Koľkým deťom ich môžem rozdeliť? Môžem to urobiť len pre jedno dieťa alebo pre sedemnásť detí. V tabuľke to bude vyzerať takto:*

počet detí	1	17
počet hrušiek pre jedno dieťa	17	1

U: Vidíš nejaký rozdiel pre čísla 16 a 17?

Ž: *Áno. Číslo* 16 *má viac* **deliteľov** *a číslo* 17 *je deliteľné len jednotkou a samým sebou.*

U: Správne. Prirodzené čísla väčšie ako 1 sa podľa počtu deliteľov rozdeľujú na ***prvočísla*** a ***zložené čísla***. Čo myslíš, ktoré z čísel 16 a 17 je prvočíslo a ktoré je zložené?

Ž: *Číslo* 16 *je určite zložené, pretože sa dá rozložiť na súčin viacerými spôsobmi:* $16 = 2 \cdot 8$, $16 = 4 \cdot 4$, $16 = 1 \cdot 16$. *A* 17 *je potom asi prvočíslo.*

U: Máš pravdu.
Prvočíslo je také prirodzené číslo, ktoré má práve dva rôzne delitele: jednotku a seba samého. Zložené číslo je také prirodzené číslo, ktoré má aspoň tri rôzne delitele.

Ž: *Na číslo* 1 *neviem napasovať ani jednu z tých dvoch definícií.*

U: Číslo 1 nie je totiž ani prvočíslo ani zložené číslo. Ktoré číslo je najmenším prvočíslom?

Ž: *Asi hneď číslo* 2. *Platí pre neho, že má práve dva rôzne delitele: jednotku a dvojku, teda seba.* **Najmenšie prvočíslo je** 2.

U: Áno. Je to párne číslo. Vieš ešte o nejakom inom párnom čísle, ktoré by bolo prvočíslo?

Ž: *Rozmýšľam... Asi žiadne iné párne nebude prvočíslo, pretože párne čísla sú okrem jednotky a seba samého deliteľné aj dvojkou. Všetky párne okrem dvojky sú teda zložené čísla.*

U: Dobre. A vieš, ktoré je najmenšie zložené číslo?

Ž: *Tak počkať. Jednotka je nič, dvojka je prvočíslo, trojka je tiež prvočíslo a štvorka – štvorka je už zložené číslo.* **Najmenšie zložené číslo je 4.**

U: Podľa inej definície je prirodzené číslo n zložené vtedy, ak má aspoň jedného takého deliteľa d, že $1 < d < n$.

Ž: *Veď je to to isté. Zložené číslo n je určite deliteľné jednotkou, sebou a podľa tejto definície ešte aspoň jedným takým déčkom, ktoré sa nerovná ani jednotke ani číslu n. Spolu má teda aspoň tri rôzne delitele.*

U: Áno. Už len poznamenám, že delitele 1 a n sa nazývajú ***samozrejmé delitele*** čísla n, alebo tiež ***nevlastné delitele*** čísla n. Delitele rôzne od 1 a n sa nazývajú ***vlastné delitele*** čísla n.

U: Už si mi povedal, že prvé prvočísla sú 2 a 3. Je dobré poznať prvočísla aspoň do 100.

Ž: *Odkiaľ budem vedieť, ktoré to sú?*

U: Dnes už na vyhľadávanie prvočísel existujú rôzne počítačové programy, ale ja ti ukážem postup, ktorý vymyslel asi 200 rokov pred naším letopočtom grécky matematik ***ERATOSTHENES z Kyrény***.

Ž: *Postup, starý* 2200 *rokov, platný dodnes? To ma zaujíma!*

U: Eratosthenes vytvoril algoritmus, teda postup, ktorým dokážeme vyznačiť všetky prvočísla menšie ako ľubovoľné zvolené číslo. Nech je to číslo 100. Eratosthenes si všetky čísla od 1 do 100 napísal do tabuľky. Ďalej postupoval takto:

- ***najskôr vyčiarkol číslo 1, pretože jednotka sa nepovažuje za prvočíslo,***
- ***zakrúžkoval si číslo 2 ako najmenšie prvočíslo a vyčiarkol všetky násobky čísla 2,***
- ***zakrúžkoval číslo 3, ktoré je ďalším prvočíslom a prečiarkol všetky násobky čísla 3. Niektoré z nich už boli prečiarknuté, pretože sú aj násobky čísla 2,***
- ***číslo 4 už bolo prečiarknuté, pokračoval teda ďalej,***
- ***zakrúžkoval číslo 5 a vyčiarkol všetky násobky čísla 5...***

Takýmto spôsobom postupoval tabuľkou. Ak narazil na neprečiarknuté číslo, tak ho zakrúžkoval a prečiarkol všetky jeho násobky. Nakoniec boli všetky čísla v tabuľke prečiarknuté alebo zakrúžkované.

Ž: *Tie zakrúžkované boli prvočísla a prečiarknuté boli ich násobky, teda zložené čísla.*

U: Áno. Tento algoritmus sa nazýva ***Eratostenovo sito***, pretože funguje na postupnom „preosievaní“ zoznamu čísel. Prvočíslo ostane, zvyšok prepadne sitom preč. Môžeš si skúsiť vyhľadať takýmto spôsobom zopár prvých prvočísel a potvrdiť si, že sú to tieto:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Ž: *Aké najväčšie prvočíslo sa zatiaľ našlo?*

U: So zdokonaľovaním počítačov sa zväčšuje aj dĺžka nájdených prvočísel. V roku 2001 mal zápis najväčšieho nájdeného prvočísla 4 milióny číslic. O dva roky neskôr sa našlo prvočíslo s viac než 6 miliónmi číslic. V roku 2005 malo najdlhšie nájdené prvočíslo 9 miliónov číslic a v roku 2006 bolo tých číslic okolo $9,2$ milióna. Na toho, kto ako prvý objaví desaťmiliónmiestne prvočíslo, čaká odmena 100 000 dolárov.

Ž: *Tak to aby som sa poponáhľal.*

U: Neboj sa, ak by ťa aj niekto predbehol, nejaká odmena bude iste aj za prvočíslo s pätnástimi miliónmi číslic. Ale v tejto chvíli sa takými veľkými prvočíslami nebudeme zaoberať. Pre tvoje potreby zatiaľ úplne postačí, ak budeš poznať prvočísla do 100, prípadne do 200.

Ž: *A načo mi bude dobré poznať tieto prvočísla?*

U: Aj to si povieme.

U: Vedel by si rozložiť zložené číslo 48 na súčin čo najmenších prirodzených činieľov?

Ž: *Určite áno.* $48 = 6 \cdot 8$, *ale to ešte nie sú najmenšie možné činitele. Aj šestka aj osmička sa dajú rozložiť ďalej. Šestka je súčin dvojky a trojky a osmička je súčin dvojky a štvorky.*

U: A to je všetko? Všetky činitele sú už najmenšie možné?

Ž: *To nie. Štvorka sa ešte dá rozložiť na súčin dvoch dvoják.*

U: Zapíšem to takto:

$$48 = 6 \cdot 8 = 2 \cdot 3 \cdot 2 \cdot 4 = 2 \cdot 3 \cdot 2 \cdot 2 \cdot 2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3.$$

Je už teraz číslo 48 rozložené na súčin čo najmenších prirodzených činiteľov?

Ž: *Áno. Číslo* 48 *je vytvorené ako súčin štyroch dvoják a jednej trojky a ani dvojky ani trojka sa už nedajú rozložiť na súčin od nich menších činiteľov.*

U: Pretože sú to prvočísla. Takéto prvočíselné činitele nazývame aj ***prvočinitele***.
Zápis čísla v tvare súčinu, kde každý činiteľ je mocnina prvočísla, nazývame:

– ***rozklad na prvočinitele*** alebo

– ***prvočíselný rozklad*** alebo

– ***rozklad na súčin prvočísel***.

Ž: *Každé prirodzené číslo sa dá rozložiť na súčin mocnín prvočísel?*

U: Áno. Dokonca jediným spôsobom. O tom hovorí nasledujúca veta:
Každé prirodzené číslo n ***väčšie ako jedna sa dá zapísať práve jedným spôsobom v tvare***

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ \ldots \ \cdot p_k^{a_k},$$

kde $p_1 < p_2 < p_3 < \ \ldots \ < p_k$ sú navzájom rôzne prvočísla,
$a_1, \ a_2, \ a_3, \ \ldots \ , a_k$ sú prirodzené čísla.
Táto veta sa nazýva ***Základná veta aritmetiky.***

Ž: *Zdá sa mi, že rozložiť číslo na súčin by pri veľkých hodnotách mohol byť problém.*

U: Preto je dobré poznať ***kritériá deliteľnosti*** niektorými číslami a aj prvočísla do 100 alebo 200, aby si sa nesnažil rozložiť nerozložiteľné.

Ž: *A načo mi je dobrý taký rozklad na súčin prvočísel?*

U: Rozklad na prvočinitele sa využíva napríklad pri určovaní ***najmenšieho spoločného násobku*** a ***najväčšieho spoločného deliteľa*** dvoch alebo viacerých čísel.

U: Pri rozklade na prvočinitele a deliteľoch čísla n ešte chvíľu ostaneme.
Ak máme prirodzené číslo $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ \ldots \ \cdot p_k^{a_k}$, tak platí, že:

- ***každý deliteľ*** d ***čísla*** n ***je v tvare*** $d = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \ \ldots \ \cdot p_k^{b_k}$***, pričom pre každé*** $i \in \mathbb{N}$ ***je*** $0 \leqq b_i \leqq a_i$***,***
- ***číslo*** n ***má*** $(a_1 + 1) \cdot (a_2 + 1) \cdot (a_3 + 1) \cdot \ \ldots \ \cdot (a_k + 1)$ ***rôznych kladných deliteľov,***
- ***číslo*** n ***je*** m***-tou mocninou*** $(m \geqq 2)$ ***prirodzeného čísla práve vtedy ak pre každé*** $i \in \mathbb{N}$ ***je exponent*** a_i ***deliteľný číslom*** m***.***

Ž: *Tomu prvému tvrdeniu aj rozumiem. Aby číslo d mohlo byť deliteľom daného čísla n, nemôže mať vo svojom rozklade iné prvočísla než má v rozklade číslo n.*

U: Áno a nemôže mať v rozklade ani vyššiu mocninu niektorého prvočísla než má n.

Ž: *Zato tým zvyšným dvom tvrdeniam nerozumiem vôbec.*

U: Druhé tvrdenie ti vysvetlím na príklade. Uvažujme najprv o čísle, ktoré má vo svojom rozklade len jedno prvočíslo. Napríklad nech $n = 8$. Aký je prvočíselný rozklad čísla 8?

Ž: *Číslo* 8 *je treťou mocninou dvojky, takže* $8 = 2^3$.

U: Aké delitele má osmička?

Ž: *Osmičku delia čísla* 1, 2, 4 *a* 8. *Má teda* 4 *delitele.*

U: Ja to poviem takto: osmička je deliteľná nultou, prvou, druhou a treťou mocninou prvočísla 2, ktoré je v jej rozklade. Tvrdenie hovorí, že tých deliteľov je $a_1 + 1$, čo je pre nás $3 + 1 = 4$.

Ž: *Ak je v rozklade len jedno prvočíslo, tak to sedí. Ale čo tie ďalšie zátvorky?*

U: Buď ešte chvíľu trpezlivý. Nech teraz $n = 25 = 5^2$.

Ž: *Podľa vety by malo mať troch deliteľov, lebo* $a_1 + 1 = 2 + 1 = 3$. *Overím si to. Číslo* 25 *je deliteľné číslami* 1, 5 *a* 25, *teda nultou, prvou a druhou mocninou prvočísla* 5. *Delitele sú tri, sedí to.*

U: A teraz vezmeme za n také číslo, ktoré má v rozklade dve prvočísla, napríklad

$$n = 2^3 \cdot 5^2 = 8 \cdot 25 = 200.$$

Ž: *Prvočíslo* 2 *v tomto rozklade prispieva štyrmi deliteľmi a prvočíslo* 5 *tromi deliteľmi, to sme si ukázali.*

U: Lenže okrem deliteľov 1,2,4,8 a 1,5,25 má číslo 200 aj delitele, ktoré vznikli kombináciou mocnín dvojky a päťky.

Ž: *Napríklad* $2 \cdot 5$, *alebo* $4 \cdot 25$, *alebo aj* $8 \cdot 25$.

U: Ak každý deliteľ čísla 8 skombinuješ s každým deliteľom čísla 25, tak všetkých deliteľov je $4 \cdot 3 = 12$.

Ž: *Aha, a keď sa vrátime k najvyšším mocninám prvočísel* 2 *a* 5*, tak* $4 \cdot 3 = (3 + 1) \cdot (2 + 1)$.

U: Správne. Ak má číslo n v rozklade viac prvočísel, tak každé prvočíslo prispieva toľkými deliteľmi, aká je jeho najvyššia mocnina v rozklade zväčšená o 1. Vzájomnými kombináciami týchto deliteľov dostaneš presne počet uvedený vo vzorci.

Ž: *A čo to posledné tvrdenie?*

U: To hovorí o tom, že v prvočíselnom rozklade čísla n je každý exponent jednotlivých prvočísel deliteľný číslom m práve vtedy ak číslo n je m-tou mocninou nejakého prirodzeného čísla.

Ž: *Prečo?*

U: Vezmeme si ľubovoľné prvočíslo p_i z rozkladu čísla n. Toto prvočíslo je umocnené exponentom a_i. Exponent a_i je deliteľný číslom m práve vtedy, ak existuje také číslo c_i, že $a_i = m \cdot c_i$. Prvočíslo p_i je teda umocnené exponentom $m \cdot c_i$. Využijeme pravidlo pre počítanie s mocninami a dostaneme:

$$p_i^{a_i} = p_i^{m \cdot c_i} = (p_i^{c_i})^m, \text{ pre každé } i \in \mathbb{N}.$$

Ž: *Ak si vieme každý činiteľ v rozklade na súčin prvočísel upraviť takýmto spôsobom, tak dostaneme:*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ \ldots \ \cdot p_k^{a_k} = (p_1^{c_1})^m \cdot (p_2^{c_2})^m \cdot \ \ldots \ \cdot (p_k^{c_k})^m = (p_1^{c_1} \cdot p_2^{c_2} \cdot \ \ldots \ \cdot p_k^{c_k})^m.$$

U: A to je to, k čomu sme chceli dôjsť. Číslo n je m-tou mocninou. Toto tvrdenie má celkom zaujímavý dôsledok:
Ak pre prirodzené čísla a, b, c ***platí:*** $a^2 = b \cdot c^2$, ***tak číslo*** b ***musí byť tiež štvorcom.***

Ž: *Ako môže byť číslo štvorcom?*

U: Ak je číslo druhou mocninou, hovorí sa tomu, že je štvorcom.

Ž: *Aha, čiže ak je druhou mocninou, tak to znamená, že existuje nejaké prirodzené číslo* x *také, že* $b = x^2$.

U: Áno. V našom prípade má x hodnotu $\frac{a}{c}$, lebo:

$$b = \frac{a^2}{c^2} = \left(\frac{a}{c}\right)^2 = x^2.$$

U: Zopár zaujímavých viet platí aj pre prvočísla. Napríklad:

- ***každé prvočíslo väčšie ako*** 3 ***sa dá napísať v tvare*** $6k + 1$ ***alebo*** $6k - 1$***, kde*** k ***je prirodzené číslo,***
- ***každé prvočíslo väčšie ako*** 2 ***sa dá napísať v tvare*** $4k + 1$ ***alebo*** $4k - 1$***, kde*** k ***je prirodzené číslo.***

Ž: *Overím si na niekoľkých prvočíslach, či platí prvá veta. Prvočíslo* 53 *sa dá napísať ako* $6{\cdot}9-1$*, prvočíslo* $37=6{\cdot}6+1$*, prvočíslo* $97=6{\cdot}16+1$*. Super. Takto ľahko nájdem hocijaké prvočíslo. Vezmem si ľubovoľný násobok čísla* 6 *a pripočítam alebo odpočítam jednotku.*

U: Myslíš? Vezmi si napríklad tridsiatyprvý násobok čísla 6.

Ž: *Vypočítam si jeho hodnotu:* $6\cdot 31=186$ *a odpočítam alebo pripočítam jednotku:*
$186-1=185$*, to nie je prvočíslo, lebo toto číslo je deliteľné číslom* 5*.*
$186+1=187$*, takže toto číslo je prvočíslo.*

U: Nie je. Číslo $187=11\cdot 17$, takže nie je prvočíslo.

Ž: *Tak kde je chyba?*

U: Veta tvrdí toto: ak je číslo p prvočíslom, tak je určite tesným susedom niektorého násobku šestky. Veta však neplatí obrátene. Nie každý sused násobku šestky je prvočíslom.

Ž: *Druhá veta je asi podobná, len hovorí o násobku štvorky.*

U: Áno. Ďalšia veta by ti mohla pomôcť pri rozklade čísla na súčin prvočísel:

- ***každé zložené číslo*** n ***je deliteľné aspoň jedným prvočíslom menším alebo rovným ako*** $\sqrt{n}$**.**

Ak rozkladáš na súčin veľké číslo, pomôžu ti ***kritéria deliteľnost*** ale aj to, že nejaký prvočíselný deliteľ je určite z intervalu $\langle 2;\sqrt{n}\rangle$.

Ž: *Nemusím teda prehľadávať strašne veľa čísel, len po tú odmocninu. Aspoň nejaká úľava.*

U: Teraz niečo o deliteľnosti súčinu prvočíslom:

- ***ak*** p ***je prvočíslo, ktoré delí súčin celých čísel*** a ***a*** b***, potom*** p ***delí*** a ***alebo*** p ***delí*** b**.**

Ž: *To je celkom jasné. Ak súčin* $a{\cdot}b$ *rozložím na súčin prvočísel, tak tam to prvočíslo* p *bude, ale to znamená, že bude v rozklade aspoň jedného z činiteľov* a*,* b*.*

U: Dobre. Ak sa prvočíslo p vyskytne v rozklade viackrát, tak môže byť deliteľom aj oboch činiteľov. Táto veta sa často využíva pri dôkazových úlohách.

U: Nasledujúca veta súvisí s tým, že ***prvočísel je nekonečne veľa***. Hľadanie stále väčších a väčších prvočísel je však ťažká úloha, pretože sa doposiaľ nezistilo, akým spôsobom sú rozmiestnené medzi ostatnými – zloženými číslami. Prvočísla totiž nenasledujú po sebe podľa žiadneho známeho pravidla a neexistuje vzorec, podľa ktorého sa dajú vyrátať. Platí ale:

- ***ak*** n ***je prirodzené číslo, tak existuje prvočíslo*** p ***také, že platí*** $n \leqq p \leqq 2n$**.**

Ž: *Aha. Táto veta hovorí, že ak si zvolím ľubovoľne veľké prirodzené číslo, tak niekde medzi ním a jeho dvojnásobkom sa určite nájde nejaké prvočíslo.*

U: Správne. Táto veta sa nazýva aj Bertrandov postulát, podľa svojho objaviteľa.

U: Ďalšie dve vety nesú tiež meno podľa človeka, ktorý ich vyslovil a dokázal:

- ***Malá Fermatova veta: ak*** p ***je prvočíslo a*** a ***je celé číslo, tak každé číslo v tvare*** $a^p - a$ ***je násobkom čísla*** p***,***
- ***Wilsonova veta: ak*** p ***je prirodzené číslo väčšie ako*** 1***, tak číslo*** $(p-1)! + 1$ ***je deliteľné číslom*** p ***práve vtedy, ak číslo*** p ***je prvočíslom.***

Všimni si, že Malá Fermatova veta už nehovorí len o deliteľnosti prirodzených čísel, ale zaoberá sa deliteľnosťou v množine celých čísel.

U: No a na záver:

- ***ak*** p ***je prvočíslo rôzne od*** 2 ***a*** 5***, potom racionálne číslo*** $\frac{1}{p}$ ***má v desiatkovej číselnej sústave nekonečný periodický desatinný rozvoj.***

Ž: *Zlomky* $\dfrac{1}{2}$ *a* $\dfrac{1}{5}$ *majú konečné desatinné rozvoje, lebo* $\dfrac{1}{2} = 0,5$ *a* $\dfrac{1}{5} = 0,2$*. Ich sa táto veta naozaj netýka. A tie ostatné prevrátené hodnoty prvočísel majú nekonečne veľa desatinných miest?*

U: Áno. Ich desatinný rozvoj je nekonečný a periodický. O prvočíslach ešte existuje mnoho ďalších viet, ale zatiaľ ich nebudem spomínať.

Príklad D: *Dokážte, že prvočísel je nekonečne veľa.*

U: Dokazovať budeme sporom.

Ž: *Potrebujem teda* **negáciu** *nášho tvrdenia. Mohla by byť v tvare:*
Prvočísel je iba konečný počet *alebo* **existuje iba konečne veľa prvočísel**.

U: Dobre. Nech ich bude napríklad n, pričom n je prirodzené číslo. Označme si teraz prvočísla takto: $p_1, p_2, p_3, \dots, p_n$.

Ž: *A čo teraz? Všetky sú pomenované, ale kde je tu nejaký spor?*

U: Vytvorme súčin týchto prvočísel zväčšený o 1:

$$p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1.$$

Ktorým z prvočísel $p_1, p_2, p_3, \dots, p_n$ je toto číslo deliteľné?

Ž: *Predsa žiadnym. Pri delení hociktorým z týchto prvočísel dostaneme vždy zvyšok* 1.

U: Správne. Číslo $p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$ musí byť teda buď prvočíslo, alebo musí byť deliteľné nejakým iným prvočíslom.

Ž: *V oboch prípadoch je to spor s tým, že žiadne iné prvočíslo než prvočísla* $p_1, p_2, p_3, \dots, p_n$ *neexistuje.*

U: Presne tak. Množina prvočísel zo začiatku dôkazu nie je úplná, čo je spor s predpokladom.

Ž: *Dokázali sme, že* **prvočísel je nekonečne veľa.**

Príklad 1: *Rozložte na súčin prvočísel zložené číslo* 2604.

U: Ak máš rozložiť väčšie číslo – ako je napríklad toto, premysli si aké ***kritériá deliteľnosti*** poznáš a ktoré z nich využiješ.

Ž: *Číslo je párne, takže využijem, že je deliteľné dvojkou.*

U: Posledné dvojčíslie je 04, môžeš teda rovno využiť deliteľnosť štvorkou.

Ž: *Dobre:*

$$2604 : 4 = 651.$$

U: Číslo 2604 sa zatiaľ dá rozložiť na súčin čísel 4 a 651.

Ž: *Štvorku môžem rovno rozložiť na súčin dvoch dvoják. Rozklad čísla* 2604 *bude zatiaľ vyzerať takto:*

$$2604 = 2 \cdot 2 \cdot 651.$$

U: Teraz potrebujeme rozložiť číslo 651.

Ž: *Párne už nie je, takže nemôžem využiť deliteľnosť dvojkou ani štvorkou ani žiadnym iným párnym číslom. Skúsim, či nie je deliteľné trojkou. Ciferný súčet čísla* 651 *je* $6+5+1 = 12$, *dvanástka je deliteľná trojkou, teda aj číslo* 651 *je deliteľné trojkou:*

$$651 : 3 = 217.$$

U: Rozklad čísla 2604 je zatiaľ takýto:

$$2604 = 2 \cdot 2 \cdot 3 \cdot 217.$$

Ž: *A teraz som trošku nahratý. Svoje obľúbené kritériá som už vystrieľal, číslo* 217 *nie je párne, jeho ciferný súčet nie je násobkom ani čísla* 3 *ani čísla* 9, *nekončí na nulu ani na päťku, tak čo s tým?*

U: Ak rozkladáš na súčin prvočísel zložené číslo, môže ti pomôcť aj to, že nejaký jeho prvočíselný deliteľ je určite z intervalu $\langle 2; \sqrt{n}\rangle$.

Ž: *Aha. Potrebujem teda odmocninu z čísla* 217*:*

$$\sqrt{217} \doteq 14,73.$$

Prvočísla menšie ako táto odmocnina sú: 2, 3, 5, 7, 11 *a* 13.

U: Niektoré môžeš hneď vylúčiť.

Ž: *Dvojku, trojku a päťku vylúčim. Ostane mi preveriť deliteľnosť sedmičkou, jedenástkou a trinástkou.*

U: No, môžeš to skúsiť.

Ž: *Keďže kritériá pre deliteľnosť týmito číslami nepoznám, budem rovno deliť:*

$$217 : 7 = 31.$$

Hops a mám rovno pekný výsledok. Ďalej už skúšať nemusím, lebo 31 *je tiež prvočíslo.*

Ž: *Zapíš ešte výsledný rozklad čísla* 2604 *tak, že prvočísla v ňom budú usporiadané podľa veľkosti a viacnásobný výskyt prvočísla* 2 *zapíš pomocou mocniny.*

Ž: *Tu je:*

$$2604 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 31 = 2^2 \cdot 3 \cdot 7 \cdot 31.$$

Úloha : *Rozložte na súčin prvočísel zložené čísla* 1836 *a* $21\,420$*.*

Výsledok*:*

$1836 = 2^2 \cdot 3^3 \cdot 17,$

$21\,420 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17.$

Príklad 2: *Nájdite najväčšie prvočíslo, ktorým je deliteľné číslo* 2652.

Ž: *Ja by som urobil jeho* **rozklad na súčin prvočísel** *a z tohot rozkladu by som určil to najväčšie prvočíslo.*

U: Dobre.

Ž: *Číslo* 2652 *je párne a jeho ciferný súčet je deliteľný trojkou, takže môžem povedať, že číslo* 2652 *je deliteľné šestkou.*

U: Správne. Vydeľ číslo 2652 šestkou a potom uvidíme čo ďalej.

Ž: *Idem na to:*

$$2652 : 6 = 442,$$

$$2652 = 6 \cdot 442 = 2 \cdot 3 \cdot 442.$$

V rozklade na súčin mi vyšlo znova párne číslo, takže ešte raz vydelím dvojkou.

$$442 : 2 = 221,$$

$$2652 = 6 \cdot 442 = 2 \cdot 3 \cdot 2 \cdot 221 = 2^2 \cdot 3 \cdot 221.$$

U: Ostáva ešte preveriť, čím a či vôbec je číslo 221 deliteľné. Ak je to zložené číslo, tak je deliteľné aspoň jedným prvočíslom menším alebo rovným ako $\sqrt{221}$.

Ž: *Odmocním číslo* 221*:*

$$\sqrt{221} \doteq 14,87.$$

U: Dobre. Prvočísla menšie ako 14 sú 13, 11, 7, 5, 3 a 2. Začni tými najväčšími.

Ž: *Preverím teda, ktorým z týchto čísel je číslo* 221 *deliteľné:*

$$221 : 13 = 17.$$

A mám to:

$$2652 = 2^2 \cdot 3 \cdot 13 \cdot 17.$$

Najväčšie prvočíslo, ktorým je číslo 2652 deliteľné, je prvočíslo 17.

Úloha : *Nájdite najväčšie prvočíslo, ktorým je deliteľné číslo* 4812.

Výsledok: *prvočíslo* 401.

Príklad 3: *Upravte na základný tvar zlomky*

$$\frac{165}{728} \quad a \quad \frac{165}{462}.$$

Ž: *Zlomok je v základnom tvare vtedy, ak čitateľ a menovateľ sú* **nesúdeliteľné** *čísla.*

U: A kedy sú čitateľ a menovateľ nesudeliteľné čísla?

Ž: *No predsa, ak sa už ďalej nedajú deliť tým istým číslom.*

U: A ako zistíš, či sa čitateľ a menovateľ dajú alebo nedajú deliť?

Ž: *Zistím, či majú nejaké spoločné delitele.*

U: A ako to zistíš?

Ž: *Mohol by som vypísať všetky delitele čitateľa a všetky delitele menovateľa a hľadať medzi nimi spoločnú hodnotu.*

U: Aj to by šlo. Ale môžeš si aj urobiť rozklad na súčin prvočísel pre číslo z čitateľa zlomku aj pre číslo z menovateľa. Všetky spoločné prvočísla z oboch rozkladov potom vykrátiš.

Ž: a) *Dobre. Najprv rozklad čísla* 165. *Je deliteľné päťkou, lebo končí na päťku a aj trojkou, lebo jeho ciferný súčet je dvanásť:*

$$165 = 5 \cdot 33 = 5 \cdot 3 \cdot 11.$$

U: Zvykni si usporiadať prvočísla podľa veľkosti. Budeš v nich mať lepší prehľad.

Ž: *Tak teda:*

$$165 = 3 \cdot 5 \cdot 11.$$

U: A teraz rozklad čísla 728.

Ž: *Je párne, teda deliteľné dvojkou. Vlastne je deliteľné aj štvorkou, lebo jeho posledné dvojčíslie je štvorkou deliteľné:*

$$728 = 4 \cdot 182 = 2 \cdot 2 \cdot 182,$$

číslo 182 *je tiež párne, tak ho ešte vydelím dvojkou:*

$$728 = 2 \cdot 2 \cdot 2 \cdot 91.$$

U: To ešte nie je celý rozklad. Číslo 91 je násobok sedmičky.

Ž: *Aha. Trinásty násobok. Takže rozklad bude:*

$$728 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 13.$$

U: Prezri si oba rozklady. Akým spoločným prvočíslom môžeš vykrátiť čitateľa a menovateľa?

Ž: *Zdá sa, že žiadnym.* **Čísla 165 a 728 sú nesúdeliteľné, zlomok $\frac{165}{728}$ je už v základnom tvare.**

Ž: b) *Druhý zlomok má v čitateli tiež číslo* 165, *využijem jeho rozklad z prvého príkladu:*

$$165 = 3 \cdot 5 \cdot 11.$$

U: A teraz rozklad menovateľa.

Ž: *V menovateli je číslo párne s ciferným súčtom deliteľným trojkou, takže celé číslo je deliteľné šestkou:*

$$462 = 6 \cdot 77 = 2 \cdot 3 \cdot 77.$$

Číslo 77 *v tomto rozklade je súčinom sedmičky a jedenástky, takže celý rozklad bude:*

$$462 = 2 \cdot 3 \cdot 7 \cdot 11.$$

U: Môžeš si teraz oba rozklady dosadiť do čitateľa a menovateľa zlomku.

Ž: *Keď rozklady dosadím, dostanem:*

$$\frac{165}{462} = \frac{3 \cdot 5 \cdot 11}{2 \cdot 3 \cdot 7 \cdot 11}.$$

Vidím, že v oboch rozkladoch sú prvočísla 3 *a* 11*. Vykrátim ich:*

$$\frac{165}{462} = \frac{5}{2 \cdot 7} = \frac{5}{14}.$$

Najväčším spoločným deliteľom čísel 165 *a* 462 *je číslo* 33*,* **zlomok $\frac{165}{462}$ má základný tvar $\frac{5}{14}$.**

Úloha : *Upravte na základný tvar zlomky*

$$\frac{84}{405}, \quad \frac{108}{225} \quad a \quad \frac{1800}{3780}.$$

Výsledok: $\frac{84}{405} = \frac{28}{135}, \ \frac{108}{189} = \frac{4}{7}, \ \frac{1800}{3780} = \frac{10}{21}.$

Príklad 4: *Určte najmenšie prirodzené číslo, ktorým treba vynásobiť číslo* 2008 *tak, aby sme dostali druhú mocninu prirodzeného čísla.*

Ž: *Samotné číslo* 2008 *nie je druhou mocninou žiadneho prirodzeného čísla, to som si overil.*

U: Keby bolo druhou mocninou prirodzeného čísla, tak by tvoja úloha bola veľmi jednoduchá.

Ž: *To áno, lebo najmenšie prirodzené číslo, ktorým by som mal násobiť by bola jednotka.*

U: Rozlož si číslo 2008 na ***súčin prvočísel***.

Ž: *Číslo* 2008 *je deliteľné osmičkou, takže:*

$$2008 = 8 \cdot 251 = 2^3 \cdot 251.$$

Potrebujem ešte zistiť, či 251 *je prvočíslo alebo zložené číslo.*

U: Ak je to zložené číslo, tak v intervale $\langle 2, \sqrt{251}\rangle$ je určite jeho prvočíselný deliteľ.

Ž: *Keď odmocním číslo* 251, *dostanem približnú hodnotu* 15,84. *Prvočísla menšie ako* 15 *sú:* 2, 3, 5, 7, 11 *a* 13.

U: Vyskúšaš deliteľnosť všetkými?

Ž: *Nie. Prvé tri prvočísla môžem hneď vylúčiť, pretože číslo* 251 *nie je ani párne, ani nemá ciferný súčet deliteľný trojkou a ani nekončí na nulu alebo päťku. Ostáva mi preveriť prvočísla* 7, 11 *a* 13*:*

$$251 : 7 \doteq 35{,}857, \quad 251 : 11 \doteq 22{,}818, \quad 251 : 13 \doteq 19{,}307.$$

U: Číslo 251 nie je deliteľné žiadnym z prvočísel z intervalu $\langle 2, \sqrt{251}\rangle$, takže je prvočíslom.

Ž: *Rozklad čísla* 2008 *na súčin prvočísel je:*

$$2008 = 2^3 \cdot 251.$$

U: Pomocou tohto rozkladu zisti, čím máš vynásobiť číslo 2008, aby si dostal druhú mocninu prirodzeného čísla.

Ž: *Ak je číslo druhou mocninou nejakého prirodzeného čísla, tak všetky prvočísla v jeho prvočíselnom rozklade majú mocninu, ktorá je násobkom dvojky.*

U: Správne. Musíš teda do súčinu $2^3 \cdot 251$ pridať také prvočíselné činitele, aby si dostal $2^4 \cdot 251^2$.

Ž: *Aha. Musím teda násobiť číslom* $2 \cdot 251 = 502$.

U: A ako by si urobil skúšku, či si došiel k správnemu číslu?

Ž: *Ak vynásobím číslo* 2008 *číslom* 502 *dostanem:*

$$2008 \cdot 502 = 1\,008\,016 \qquad a \qquad \sqrt{1\,008\,016} = 1004,$$

1004 *je prirodzené číslo.* **Hľadané číslo je 502.**

Úloha : *Určte najmenšie prirodzené číslo, ktorým treba vynásobiť číslo* 60 *tak, aby sme dostali tretiu mocninu prirodzeného čísla.*

Výsledok*: Hľadané číslo je* $2 \cdot 3^2 \cdot 5^2 = 450$.

Príklad 5: *Určte počet deliteľov čísla* 5940.

U: Ak máme prirodzené číslo n, ktorého ***prvočíselný rozklad*** je

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ \ldots \ \cdot p_k^{a_k},$$

kde $p_1 < p_2 < p_3 < \ \ldots \ < p_k$ sú navzájom rôzne prvočísla
a $a_1, \ a_2, \ a_3, \ \ldots \ , a_k$ sú prirodzené čísla,
tak počet rôznych deliteľov čísla n je:

$$(a_1 + 1) \cdot (a_2 + 1) \cdot (a_3 + 1) \cdot \ \ldots \ \cdot (a_k + 1).$$

Ž: *Najprv teda urobím prvočíselný rozklad čísla* 5940. *Číslo je deliteľné desiatkou, pretože končí na nulu a aj deviatkou, pretože jeho číselný súčet je deviatkou deliteľný:*

$$5940 = 10 \cdot 594 = 10 \cdot 9 \cdot 66 = \cdots$$

Desiatka je súčin dvojky a päťky, deviatka je súčin dvoch trojek. Zatiaľ teda rozklad vyzerá takto:

$$\cdots = 2 \cdot 5 \cdot 3 \cdot 3 \cdot 66.$$

U: Dobre. Ostáva ti rozložiť zložené číslo 66.

Ž: *Číslo* 66 *je súčin šestky a jedenástky, šestka je súčin dvojky a trojky, takže:*

$$5940 = 2 \cdot 5 \cdot 3 \cdot 3 \cdot 2 \cdot 3 \cdot 11.$$

U: Zvykni si písať prvočísla v rozklade usporiadané podľa veľkosti a využi aj mocninový zápis.

Ž: *Poupratujem a dostanem:*

$$5940 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 11 = 2^2 \cdot 3^3 \cdot 5 \cdot 11.$$

U: Podľa vety o počte deliteľov si potrebuješ uvedomiť len exponenty prvočísel v rozklade.

Ž: *Exponenty prvočísel sú* 2 *a* 3.

U: Nielen tie. Prvočísla 5 a 11 sú umocnené na prvú, aj o tých musíš uvažovať. Teda:

$$5940 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 11 = 2^2 \cdot 3^3 \cdot 5^1 \cdot 11^1.$$

Ž: *Takže* 2, 3, 1 *a* 1. *Každý z týchto exponentov zväčším o* 1 *a potom ich vynásobím:*

$$(2 + 1) \cdot (3 + 1) \cdot (1 + 1) \cdot (1 + 1) = 3 \cdot 4 \cdot 2 \cdot 2 = 48.$$

Počet deliteľov čísla 5940 je 48.

Úloha : *Určte počet deliteľov čísel* 2010 *a* 2652.

Výsledok: *Počet deliteľov čísla* 2010 *je* 16, *počet deliteľov čísla* 2652 *je* 24.

Príklad 6: *Určte všetky prvočísla p, pre ktoré aj čísla $p+10$ a $p+20$ sú prvočísla.*

U: Každé prvočíslo p väčšie ako 3 má jeden z uvedených tvarov:

$$p = 6k+1 \qquad \textit{alebo} \qquad p = 6k-1,$$

kde k je vhodné prirodzené číslo.

Ž: *Ako to využijem?*

U: Pre každé prvočíslo $p > 3$ vyjadri $p+10$ a $p+20$ v oboch uvedených tvaroch a zisti, či výsledný výraz predstavuje prvočíslo.

Ž: *Použijem najprv tvar:*

$$p = 6k+1.$$

$$p+10 = (6k+1)+10 = 6k+11,$$

$$p+20 = (6k+1)+20 = 6k+21 = 3\cdot(2k+7)\,.$$

Ž: *Číslo p+20 je určite zložené číslo, lebo je to násobok trojky. O čísle p+10 neviem rozhodnúť, či je prvočíslo alebo zložené.*

U: V tomto prípade už nie je dôležité, či je prvočíslo alebo zložené, pretože v trojici čísel p, $p+10$, $p+20$ sme našli jedno číslo, ktoré určite nie je prvočíslom.

Ž: *Jasné. Číslo $p+20$ určite nie je prvočíslom, takže $p+10$ už môže byť hocijaké.*

U: Poďme teda preveriť druhý možný tvar prvočísla.

Ž: *Nech sa teda prvočíslo p dá zapísať v tvare:*

$$p = 6k-1.$$

$$p+10 = (6k-1)+10 = 6k+9 = 3\cdot(2k+3)\,,$$

$$p+20 = (6k-1)+20 = 6k+19.$$

U: Čo mi vieš teraz povedať o trojici čísel p, $p+10$, $p+20$?

Ž: *Číslo $p+10$ je násobkom trojky, takže je to zložené číslo. A číslo $p+20$ už nie je dôležité. Zdá sa, že ani jeden z tvarov $6k\pm1$ neviedol k riešeniu.*

U: Máš pravdu. Pre žiadne prvočíslo $p > 3$ neexistujú prvočíselné hodnoty $p+10$ a $p+20$.

Ž: *Ale ešte existujú aj prvočísla, ktoré sú menšie alebo rovné ako 3.*

U: Výborne. Veta o nich nehovorí nič. Musíš preveriť, či pre prvočísla 2 a 3 sú čísla, ktoré sú o 10 a 20 väčšie, tiež prvočíslami.

Ž: *Dobre:*
ak $p=2$, tak $p+10=12$ *a to nie je prvočíslo,*
$p+20=22$ *ani to nie je prvočíslo.*

U: Ostáva posledná možnosť.

Ž: *ak* $p = 3$, *tak* $p + 10 = 13$ *to je prvočíslo,*
$p + 20 = 23$ *aj to je prvočíslo.*
Super. **Hľadaným prvočíslom je prvočíslo 3, pretože čísla 13 a 23 sú tiež prvočísla.**

Úloha : *Nájdite tri také prvočísla, že druhé je o* 14 *väčšie ako prvé a tretie je o* 14 *väčšie ako druhé.*

Výsledok: *Prvočísla* 3, 17, 31.