1.5.7 Prvočísla a složená čísla

Předpoklady: 1503, 1506

Dnes bez kalkulačky.

Číslo 12 je dělitelné čísly 1, 2, 3, 4, 6 a 12. Množinu, kterou tvoří právě tato čísla, nazýváme množina dělitelů čísla 12, značíme $D(12)$.

Platí: $D(12)=\{1,2,3,4,6,12\}$

Př. 1: Najdi množiny dělitelů čísel 1, 3, 4, 6, 7, 9, 14 a 18. Podle počtu dělitelů se přirozená čísla dělí do tří skupin. Navrhni rozdělení uvedených čísel.

$D(1)=\{1\}$

$D(3)=\{1,3\}$

$D(4)=\{1,2,4\}$

$D(6)=\{1,2,3,6\}$

$D(7)=\{1,7\}$

$D(9)=\{1,3,9\}$

$D(14)=\{1,2,7,14\}$

$D(18)=\{1,2,3,6,9,18\}$

Dělení do skupin: počet dělitelů se liší od 1 do 6 $\Rightarrow$ tři skupiny nestačí na to, abychom v jedné skupině měli čísla se stejným počtem dělitelů.

Postřehy:

- Všechna čísla jsou dělitelná jedničkou $\Rightarrow$ první samozřejmý dělitel.
- Všechna čísla jsou dělitelná sama sebou $\Rightarrow$ druhý samozřejmý dělitel.
- Některá čísla mají další dělitele.

$\Rightarrow$ tři skupiny:

- Čísla s jedním dělitelem (jen jednička, u které oba samozřejmí dělitelé splývají v jednoho).
- Čísla se dvěma děliteli (čísla, která mají pouze samozřejmé dělitele).
- Čísla s více než dvěma děliteli (čísla, která mají i nesamozřejmé dělitele).

Přirozená čísla můžeme rozdělit do tří skupin:

- **Prvočísla**: všechna přirozená čísla, která mají právě 2 různé dělitele, jedničku a sami sebe (2,3,5,7,11,13,17,19....).
- **Složená čísla:** všechna přirozená čísla, která mají alespoň 3 různé dělitele (6, 9, 12 ….).
- **Jednička:** má pouze jednoho dělitele, skupina sama o sobě, není ani prvočíslo ani složené číslo.

Př. 2: Najdi množinu dělitelů čísla 48 a rozhodni, do jaké skupiny čísel patří.

$D(48)=\{1,2,3,4,6,8,12,16,24,48\} \Rightarrow$ číslo 48 je složené.

Jak je číslo 48 složené?

- $48=1\cdot 48$,
- $48=2\cdot 24$,
- $48=3\cdot 16$,
- $48=4\cdot 12$,
- $48=6\cdot 8$,

$\Rightarrow$ více možností, jak jej rozložit na dělitele.

Zkusíme pokračovat v rozkládání složených čísel v rozkladech, dokud nezískáme pouze prvočísla.

- $48=2\cdot 24=2\cdot 4\cdot 6=2\cdot 2\cdot 2\cdot 2\cdot 3=2^4\cdot 3$
- $48=3\cdot 16=4\cdot 4\cdot 3=2\cdot 2\cdot 2\cdot 2\cdot 3=2^4\cdot 3$
- $48=4\cdot 12=2\cdot 2\cdot 4\cdot 3=2\cdot 2\cdot 2\cdot 2\cdot 3=2^4\cdot 3$
- $48=6\cdot 8=2\cdot 3\cdot 4\cdot 2=2\cdot 2\cdot 2\cdot 2\cdot 3=2^4\cdot 3$

Získali jsme **prvočíselný rozklad**. Zdá se, že pokud prvočísla seřadíme podle velikosti, je jednoznačný (nezáleží jak začneme, výsledek je vždy stejný).

Př. 3: Najdi prvočíselný rozklad čísla 60.

- $60=2\cdot 30=2\cdot 2\cdot 15=2\cdot 2\cdot 3\cdot 5$
- $60=4\cdot 15=2\cdot 2\cdot 3\cdot 5$
- $60=6\cdot 10=2\cdot 3\cdot 2\cdot 5=2\cdot 2\cdot 3\cdot 5$

Opět všechny cesty vedou ke stejnému výsledku.

Věta (Základní věta aritmetiky)
Každé přirozené číslo *n* větší než 1, lze zapsat jediným způsobem ve tvaru $n=p_1^{r_1}\cdot p_2^{r_2}\cdot .....\cdot p_k^{r_k}$ **, kde** $p_1<p_2<....<p_k$ **jsou prvočísla a** $r_1,r_2,....,r_k$ **jsou přirozená čísla.**

Př. 4: Zapiš prvočíselný rozklad čísla 48 ve tvaru udávaném v základní větě aritmetiky a zapiš hodnoty proměnných k, $p_1,p_2,....,p_k$, $r_1,r_2,....,r_k$.

$48=2^4\cdot 3^1$
$k=2$; $p_2=p_k$ (rozklad obsahuje dvě prvočísla)
$p_1=2; r_1=4; p_2=3=p_k; r_2=1=r_k$

Př. 5: Zapiš prvočíselný rozklad čísla 60 ve tvaru udáveném z základní větě aritmetiky a zapiš hodnoty proměnných k, $p_1,p_2,....,p_k$, $r_1,r_2,....,r_k$.

$60=2^2\cdot 3\cdot 5$
$k=3$ (rozklad obsahuje tři prvočísla)

$p_1 = 2; p_2 = 3; p_3 = 5 = p_k$
$r_1 = 2;\ r_2 = 1;\ r_3 = 1 = r_k$

Pedagogická poznámka: Předchozí dva příklady se možná zdají zbytečné, není to pravda. Celý příklad 4 nevyřeší bez rady většinou vůbec nikdo, asi třetina studentů najde koeficienty p_1, p_2, r_1, r_2. Další najdou tyto koeficienty pokud na tabuli napíšete pod sebe: $48 = 2^4 \cdot 3^1$ / $n = p_1^{r_1} \cdot p_2^{r_2} \cdot ..... \cdot p_k^{r_k}$.
Význam koeficientu *k* je pro ně zcela neprůhledný.
Studenti nejsou zvyklí na matematické vyjadřování v učebnicích a sami nemají snahu větě porozumět tak, aby věděli co jednotlivé koeficienty znamenají. Navíc nemají ani žádnou tendenci se zeptat (protože je prý ve škole normální, učit se věci, které jim nic neříkají). Tento smutný fakt je podle mě jedním ze základních limitů jakéhokoliv vysvětlování ve škole, na které je nutné brát ohled.

Př. 6: Urči číslo, pro jehož prvočíselný rozklad platí: $p_1 = 3; p_2 = 5; p_3 = 7$, $r_1 = 2;\ r_2 = 1;\ r_3 = 1$.

Napíšeme rozklad podle zadaných hodnot a vynásobíme ho: $3^2 \cdot 5 \cdot 7 = 315$.

Chceme najít prvočíselný rozklad $\Rightarrow$ důležité znát prvočísla (abychom věděli, kde se zastavit s dělením).

Př. 7: Najdi všechna prvočísla menší než 50.

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$

Pedagogická poznámka: Je zajímavé, že ačkoliv studenti odkývají rozdělení čísel na prvočísla, složená čísla a jedničku jako bezproblémové, do seznamu prvočísel přidá polovina z nich i jedničku (a značné množství jich vynechá dvojku). Ačkoliv je možné studenty „donutit“ k tomu, aby věci chápali (tím, že je musí počítat sami a nic jiného jim nezbývá), nenašel jsem zatím způsob, jak je přesvědčit, aby si něco pamatovali.
Každopádně je dobré jim připomenout, že pokud se setkají s něčím, co odporuje jejich zažitým představám (jedničku většinou považují za prvočíslo), je dobré si to zkusit zapamatovat.

Je dokázáno, že neexistuje největší prvočíslo. V současnosti je největším nalezeným prvočíslem číslo $2^{57885161} - 1$. Vyjádření v desítkové soustavě má 17 452 170 číslic.

Jak úsporně zjistit, zda je 221 prvočíslo?
Nejtupější a nejpomalejší postup: Zkoušíme číslo 221 dělit postupně všemi čísly, která jsou menší (2, 3, 4, 5, 6, ..., 220). Pokud všechna dělení vyjdou se zbytkem, je číslo 221 prvočíslem.

Př. 8: Najdi vylepšení algoritmu pro ověřování prvočíselnosti.

Možné vylepšení:

- U čísla 221 nemusíme dělit až do 220, největší dělitel může být maximálně polovinou čísla (pro 221 konkrétně maximálně 110).
- Nemusíme dělit složenými čísly, dělitelnost stačí ověřit na prvočíslech (pokud je číslo například dělitelné 6, je určitě dělitelné i 3 a 2, při rozdělování čísel se dostaneme až k prvočíselnému rozkladu, který se skládá pouze z prvočísel).
- Dělitelé se ukazují v párech (viz. rozklady čísel 18 a 60 z počátku hodiny). Čím je jedno číslo v páru větší, tím je druhé menší $\Rightarrow$ největší dělitel se ukáže v páru, kde jsou číslo "co nejstejnější", v ideálním případě jsou čísla stejná (jako v rozkladu $64 = 8 \cdot 8$) a rovnají se druhé odmocnině z čísla ($\sqrt{64} = 8$). $\Rightarrow$ Zkoušíme dělit pouze čísly, která jsou menší než druhá odmocnina z čísla, které prověřujeme.

Při ověřování prvočíselnosti zkoušíme dělit:

- jen prvočísly (v prvočíselném rozkladu jsou jen prvočísla),
- která jsou menší než odmocnina z prověřovaného čísla.

Ověřujeme prvočíselnosti čísla 221:

$\sqrt{221} < 15 \Rightarrow$ Nemá cenu zkoušet prvočísla větší než 13.

2, 3, 5 $\Rightarrow$ není dělitelné podle znaků dělitelnosti.

$221 : 7 = 3...$ (11) $\Rightarrow$ není dělitelné 7, $221 : 11 = 2...$ (01) $\Rightarrow$ není dělitelné 11,

$221 : 13 = 17$ (91, 0) $\Rightarrow$ číslo $221 = 13 \cdot 17$ není prvočíslo.

Dodatek: Tři tečky u výpočtů s dělením naznačují, že dělení by mělo pokračovat, ale dopočítávat výsledek dělení je zbytečné, od chvíle, kdy je jasné, že nevyjde beze zbytku.

Pedagogická poznámka: Žákům zdůrazňuji, že dopočítávat dělení je zbytečné a koukám v průběhu následujícího příkladu, zda tuto radu dodržují.

Př. 9: Rozhodni, zda uvedená čísla patří mezi prvočísla.
a) 323 b) 397 c) 899 d) 943

a) 323

$\sqrt{323} < \sqrt{400} < 20 \Rightarrow$ Nemá cenu zkoušet prvočísla větší než 19.

2, 3, 5 $\Rightarrow$ není dělitelné podle znaků dělitelnosti.

$323 : 7 = 4...$ (43) $\Rightarrow$ není dělitelné 7, $323 : 11 = 2...$ (103) $\Rightarrow$ není dělitelné 11,

$323 : 13 = 2...$ (83) $\Rightarrow$ není dělitelné 13, $323 : 17 = 19...$ (153, 0) $\Rightarrow$ číslo $323 = 17 \cdot 19$ není prvočíslo.

b) 397
$\sqrt{397} < 20 \Rightarrow$ Nemá cenu zkoušet prvočísla větší než 19.
2,3,5,7,11,13,17,19 - nejde $\Rightarrow$ číslo 397 je prvočíslo.

c) 899
$\sqrt{899} < 30 \Rightarrow$ Nemá cenu zkoušet prvočísla větší než 29.
2,3,5,7,11,13,17,19, 23, - nejde
Číslo 899 není prvočíslo, protože $899 = 29 \cdot 31$.

d) 943
$\sqrt{943} < 31 \Rightarrow$ Nemá cenu zkoušet prvočísla větší než 29.
2,3,5,7,11,13,17,19, - nejde
Číslo 943 není prvočíslo, protože $943 = 23 \cdot 41$.

Př. 10: Mezi prvočísly se vyskytují dvojice „prvočíselných dvojčat“ – prvočísel $p, p+2$ lišících se o 2. Jaký je společný dělitel čísel $p+1$ ležících mezi nimi?

Mezi prvočísly do 50 jsou to dvojice:
5, 7 11, 13 17, 19 29, 31 41, 43
Číslo mezi nimi je dělitelné 6.
$p, p+1, p+2$ - trojice čísel jdoucích po sobě.

- krajní jsou lichá $\Rightarrow$ $p+1$ je sudé,
- krajní nejsou dělitelná 3 $\Rightarrow$ $p+1$ je dělitelné třemi,

$\Rightarrow$ $p+1$ je dělitelné šesti.

Prvočísla mají velký význam pro šifrování, například asymetrická šifra RSA je založena na tom, že:

- součin prvočísel jde spočítat snadno (šifrování),
- rozklad součinu na prvočísla je pomalý (rozšifrování).

Př. 11: Rozhodni s pomocí kalkulačky, zda je číslo 9945656597 prvočíslo.

Řešení v následující hodině.

Shrnutí: Složená čísla jsou jednoznačně rozložitelná na prvočíselný rozklad. Jednička mezi prvočísla nepatří.