1.5.4 Prvočísla a složená čísla

Předpoklady: 1502, 1503

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.

$D(1)=\{1\}$
$D(3)=\{1,3\}$
$D(4)=\{1,2,4\}$
$D(6)=\{1,2,3,6\}$
$D(7)=\{1,7\}$
$D(9)=\{1,3,9\}$
$D(14)=\{1,2,7,14\}$
$D(18)=\{1,2,3,6,9,18\}$

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?
$48=1\cdot 48$
$48=2\cdot 24$
$48=3\cdot 16$
$48=4\cdot 12$
$48=6\cdot 8$
víc možností, jak jej rozložit na dělitele

Zkusím pokračovat v rozkládání složených čísel v rozkladech, dokud nebudu mít pouze prvočísla:
$48=2\cdot 24=2\cdot 4\cdot 6=2\cdot 2\cdot 2\cdot 2\cdot 3=2^4\cdot 3$

$48 = 3 \cdot 16 = 4 \cdot 4 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$
$48 = 4 \cdot 12 = 2 \cdot 2 \cdot 4 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$
$48 = 6 \cdot 8 = 2 \cdot 3 \cdot 4 \cdot 2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$
získal jsem **prvočíselný rozklad**, zdá se, že pokud prvočísla seřadím podle velikosti je jednoznačný (nezáleží jak začnu,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 jednoznačný výsledek

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*, $p_1, p_2, ..., p_k$, $r_1, r_2, ..., r_k$.

$60 = 2^2 \cdot 3 \cdot 5$
$k = 3$ - v rozkladu jsou 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 bohužel sami nemají snahu větě porozumět tak, aby věděli co jednotlivé koeficienty znamenají. Bohužel nemají žádnou tendenci se na to 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: $p_1 = 3; p_2 = 5; p_3 = 7$, $r_1 = 2;\ r_2 = 1;\ r_3 = 1$.

Napíšu rozklad podle zadaných hodnot a vynásobím ho: $3^2 \cdot 5 \cdot 7 = 315$

Chci vyrobit prvočíselný rozklad $\Rightarrow$ důležité znát prvočísla (abych věděl, kde už zastavit).

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. 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.

Neexistuje největší prvočíslo. Například 9945656597 je také prvočíslo (možno **doma** ověřit na kalkulačce).

Pedagogická poznámka: Že číslo 9945656597 je prvočíslem není na většině běžných kalkulaček možné ověřit pouhým dělením, protože výsledek po dělení třemi přesahuje počet míst na displeji. U prvočísel menších než deset je nutné ověřovat pomocí zpětného násobení nebo pomocí znaků dělitelnosti.
Každopádně diskuse je většinou příliš dlouhá. Já osobně se příště budu snažit zadat příklad domů a neztrácet s ním čas ve škole, kde jenom ukáži pomocí násobení, že číslo není dělitelné třemi.

Jak úsporně zjistit zda je 943 prvočíslo?

Zkouším dělit:
1. jen prvočísly (v prvočíselném rozkladu jsou jen prvočísla)
2. která jsou menší než odmocnina z 943 (každý rozklad odhalí 2 dělitele viz rozklad 48 z nichž jedno je menší než odmocnina a druhé větší než odmocnina)

$\sqrt{943} < 31$ - poslední číslo, které vyzkouším je 29
2,3,5,7,11,13,17,19, - nejde
Číslo 943 není prvočíslo, protože $943 = 23 \cdot 41$

Př. 8: Rozhodni, zda čísla 899 a 907 jsou prvočísla.

$\sqrt{899} < 30$ - poslední číslo, které vyzkouším je 29
2,3,5,7,11,13,17,19, 23, - nejde
Číslo 899 není prvočíslo, protože $899 = 29 \cdot 31$

$\sqrt{907} < 30$ - poslední číslo, které vyzkouším je 29
2,3,5,7,11,13,17,19, 23, 29 - nejde
Číslo 907 je prvočíslo.

Př. 9: 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:
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

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

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