Základní věty o dělitelnosti

Části 1-5: Násobek a dělitel. Největší společný dělitel. Nejmenší společný násobek. Vlastnosti čísel nesoudělných. Prvočísla

In: Karel Hruša (author): Základní věty o dělitelnosti. (Czech). Praha: Jednota československých matematiků a fyziků, 1950. pp. 4–31.

Persistent URL: http://dml.cz/dmlcz/402899

I. NÁSOBEK A DĚLITEL

V této knížce se budeme zabývati pouze čísly celými a kladnými. Nejprve si stanovíme tuto úmluvu: Řekneme-li slovo „číslo", budeme vždy míti na mysli pouze číslo celé a kladné, t. j. některé z čísel 1, 2, 3, 4, ... Budeme-li mysliti nějaké jiné číslo (třeba nulu nebo číslo záporné nebo zlomek), po každé to výslovně vytkneme.

Je známo, že sčítáním a násobením dvou čísel celých a kladných dostaneme opět číslo celé a kladné. Výsledek sčítání se jmenuje součet, výsledek násobení se jmenuje součin. Říkáme tedy, že součet a součin čísel celých a kladných je opět číslo celé a kladné. Naproti tomu při odčítání dvou čísel celých a kladných dostaneme číslo celé a kladné jen tehdy, odčítáme-li číslo menší od většího. Podobně při dělení dvou čísel celých a kladných dostaneme číslo celé a kladné jen za určitých podmínek. Jaké jsou to podmínky, tím se v dalších úvahách budeme podrobněji zabývati.

Vezměme si nějaké číslo (podle naší úmluvy myslíme číslo celé a kladné), třeba číslo 12, a tvořme jeho **násobky**. To jsou čísla

$$12, 24, 36, 48, 60, 72, 84, 96, 108, 120, \ldots,$$

která vzniknou tak, že zvolené číslo (t. j. číslo 12) postupně násobíme všemi čísly celými a kladnými, nebo také tak, že ke zvolenému číslu toto zvolené číslo stále postupně přičítáme. Tečky na konci řádku znamenají, že v tvoření násobků můžeme pokračovati libovolně daleko.

V matematice je zvykem čísla označovati písmeny. Každé číslo a, které je násobkem čísla 12, můžeme napsati ve tvaru

$$a = 12c, \tag{1}$$

při čemž c znamená nějaké číslo celé a kladné. Výraz $12c$ nazýváme proto obecným tvarem násobku čísla 12.

Chceme-li rozhodnout, je-li nějaké číslo násobkem čísla 12, stačí je děliti dvanácti. Vyjde-li toto dělení beze zbytku, je dané číslo násobkem čísla 12. Jestliže však dělení beze zbytku nevyjde, pak dané číslo není násobkem čísla 12. Tak na příklad číslo 216 je násobkem čísla 12, neboť dělení $216 : 12 = 18$ vychází beze zbytku. A skutečně

dosadíme-li do rovnice (1) $c = 18$, dostaneme číslo $a = 12 \cdot 18 = 216$, o němž jsme právě rozhodli, že je násobkem čísla 12.

Naproti tomu číslo 320 není násobkem čísla 12, neboť dělení $320 : 12$ dává podíl 26 a zbytek 8. Také nelze do rovnice (1) za c dosaditi žádné číslo celé a kladné, chceme-li, aby vyšlo 320: dosadíme-li $c = 26$, vyjde $a = 12 \cdot 26 = 312$, což je příliš málo, a dosadíme-li $c = 27$, vyjde $a = 12 \cdot 27 = 324$ a to už je příliš mnoho. Říkáme, že číslo 312 je **nejblíže nižší** a číslo 324 je **nejblíže vyšší násobek** dvanácti k číslu 320, ale číslo 320 samo není násobkem čísla 12. Číslo, jež bylo v rovnici (1) označeno písmenem c, je tedy podíl, který vznikne při dělení čísla a dvanácti, vyjde-li toto dělení beze zbytku.

Tyto úvahy můžeme opakovati s tou změnou, že místo čísla 12 zvolíme některé jiné číslo. Označme toto zvolené číslo písmenem b. Pak násobky čísla b jsou

$$b, 2b, 3b, 4b, 5b, 6b, \ldots$$

Je-li tedy číslo a násobkem čísla b, lze nalézti (celé a kladné) číslo c tak, aby

$$a = bc. \tag{2}$$

Nelze-li takové číslo c nalézti, čili, jak říkáme, neexistuje-li takové číslo c, pak číslo a není násobkem čísla b. Jak číslo c nalezneme, to už také víme: stačí číslo a dělit číslem b. Vyjde-li dělení beze zbytku, je číslo a násobkem čísla b a c je podíl tohoto dělení. Jestliže dělení beze zbytku nevyjde, číslo a není násobkem čísla b.

Místo, abychom říkali, že číslo a je násobkem čísla b, říkáme také, že číslo b je **dělitelem** čísla a. Jinak se také říká, že číslo a je číslem b **dělitelné** nebo že číslo b je v čísle a **obsaženo**. Podle toho výrok, že 216 je násobkem čísla 12, znamená přesně totéž jako výroky: 12 je dělitelem čísla 216, 216 je dělitelno číslem 12, 12 je obsaženo v čísle 216. Tato rčení a jejich význam si musíme dobře zapamatovat, neboť jich budeme stále užívat.

Číslo, které je dělitelné dvěma, jmenuje se **sudé**. Na příklad čísla 2, 4, 6, 8, ... jsou sudá. Obecný tvar čísla sudého tedy je $2k$, kde k je libovolné číslo (celé a kladné). Číslo, které není sudé, jmenuje se **liché**.

Cvičení:

1. Rozhodněte, která z čísel 526, 541, 567, 594 jsou dělitelná číslem 27.— [Poslední dvě.]

2. Nalezněte nejblíže a) nižší, b) vyšší násobky čísla 18 k číslům 456, 477, 486. — [a) 450, 468, 468; b) 468, 486, 504.]

3. Rozhodněte, která z čísel 24, 30, 36, 42 jsou děliteli čísla 504. — [24, 36, 42.]

4. Napište všechna čísla větší než 500 a menší než 1000, v nichž je obsaženo číslo 96. — [576, 672, 768, 864, 960.]

5. Doplňte místa označená * takovými číslicemi, aby čísla 572*, 36*4, 4*28, *524 byla dělitelná osmi. — [5720 nebo 5728, 3624 nebo 3664, 4128 nebo 4328 nebo 4528 nebo 4728 nebo 4928, nelze.]

6. Napište obecný tvar čísla dělitelného a) třemi, b) čtyřmi, c) devíti.— [a) $3c$, b) $4c$, c) $9c$.]

O násobcích a dělitelích si odvodíme několik vět, jichž budeme v dalším potřebovat. Pro snazší přehlednost je budeme číslovat.

Především víme, že $12 = 1 \,.\, 12$ a také $12 = 12 \,.\, 1$, t. j. číslo 12 je dělitelné číslem 1 a také číslem 12. Platí

Věta 1. *Každé číslo je dělitelné jednotkou a samo sebou.*

Důkaz: Že je to pravda, nahlédneme okamžitě, neboť vždy lze psát $a = 1 \,.\, a$ a také $a = a \,.\, 1$. Proto při dělení $a : 1$ vyjde podíl a a při dělení $a : a$ vyjde podíl 1.

Každé číslo a má tedy vždy dva dělitele: jednotku a sama sebe. Tyto dva dělitele každého čísla budeme v dalším označovati názvem **samozřejmí dělitelé**. Podle toho každé číslo větší než 1 má dva samozřejmé dělitele: jednotku a sama sebe. Číslo 1 má toliko jednoho (samozřejmého) dělitele: jednotku.

Číslo 12 je dělitelné těmito čísly: 1, 2, 3, 4, 6 a 12. Všecka jsou menší než 12, toliko dělitel 12 je mu roven. Obecně platí

Věta 2. *Žádný dělitel čísla a nemůže být větší než toto číslo.*

Důkaz: Je-li číslo b dělitelem čísla a, znamená to podle rovnice (2), že dovedeme najít číslo c tak, aby $a = bc$. Ale c je číslo celé a kladné; je tedy buď větší než 1 nebo je rovno jedné, t. j. $c \geqq 1$. A nyní víme: Násobíme-li dvě čísla, z nichž jedno je větší a druhé menší, třetím číslem, je součin většího čísla také větší; násobíme-li však dvě stejná čísla číslem třetím, jsou součiny také stejné. Proto z nerovnosti

$c \geqq 1$ plyne nerovnost $bc \geqq b \,.\, 1$, ale místo bc lze psát a a místo $b \,.\, 1$ lze psát b, takže dostaneme $a \geqq b$. Je tedy číslo b buď menší než a nebo je mu nanejvýš rovno, ale zcela jistě není větší než a. To jsme právě chtěli dokázat. Dokázanou větu můžeme vysloviti také ve tvaru: *Žádný násobek čísla b nemůže být menší než toto číslo.*

Z dokázané věty hned vyplývá

VĚTA 3. *Je-li číslo a dělitelné číslem b a současně také číslo b je dělitelné číslem a, pak je* $a = b$.

Důkaz: Je-li číslo a dělitelné číslem b, je podle věty 2 $a \geqq b$. Je-li také naopak číslo b dělitelné číslem a, je podle téže věty $b \geqq a$. Obojímu současně lze vyhověti jen tak, že $a = b$.

Číslo 21 je dělitelné sedmi, neboť $21 = 7 \,.\, 3$. Také číslo $42 = 21 \,.\, 2$ je dělitelné sedmi a vůbec každý násobek čísla 21 je dělitelný sedmi. Touž úvahu můžeme provésti pro kterákoli jiná čísla. Obecně platí

VĚTA 4. *Je-li číslo a dělitelné číslem b, je jím také dělitelný každý násobek čísla a.*

Důkaz: Předpokládejme, že číslo a je dělitelné číslem b, t. j. že existuje takové číslo c, že $a = bc$. Libovolný násobek čísla a lze podle rovnice (2) napsati ve tvaru ak. Dosadíme-li sem $a = bc$, vyjde $ak = bck = b \,.\, ck$. Ježto c a k jsou čísla celá a kladná, je součin ck rovněž číslo celé a kladné. Proto číslo ak je dělitelné číslem b.

Číslo $14 = 7 \,.\, 2$ je dělitelné sedmi. Číslo $15 = 5 \,.\, 3$ je dělitelné pěti. Číslo $14 \,.\, 15 = 210$ je dělitelné třiceti pěti, neboť $14 \,.\, 15 = 7 \,.\, 2 \,.\, 5 \,.\, 3 = 7 \,.\, 5 \,.\, 2 \,.\, 3 = 35 \,.\, 6$. Touž úvahu můžeme provést i pro kterákoli jiná čísla.

VĚTA 5. *Je-li číslo a dělitelné číslem b a je-li číslo a' dělitelné číslem b', je součin aa' dělitelný součinem bb'.*

Důkaz: Předpokládáme, že a je dělitelné číslem b, t. j. existuje číslo c tak, že $a = bc$. Dále předpokládáme, že a' je dělitelné číslem b', t. j. existuje číslo c' tak, že $a' = b'c'$. Pak $aa' = bc \,.\, b'c' = bb' \,.\, cc'$. Ježto čísla c a c' jsou celá a kladná, je i jejich součin cc' číslo celé a kladné, takže číslo aa' je dělitelné číslem bb'.

Platnost věty 5 lze bez obtíží rozšířiti i na větší počet činitelů.

Cvičení:

7. Aniž provádíte násobení rozhodněte, je-li součin $48 \,.\, 63$ dělitelný těmito čísly: 42, 54, 56, 72. — [Je dělitelný.]

8. Dokažte správnost věty: Součin dvou libovolných čísel sudých je dělitelný čtyřmi. — [Taková čísla jsou $2h$, $2k$.]

9. Dokažte správnost věty: Je-li mezi několika čísly aspoň jedno sudé, je jejich součin také sudý. — [Jde o násobek sudého čísla; užijte věty 4.]

10. Součin dvou po sobě jdoucích čísel (celých) je vždy dělitelný dvěma. Dokažte. — [Užijte výsledku cvič. 9.]

11. Dokažte správnost věty: Součin dvou po sobě jdoucích čísel sudých je vždy dělitelný osmi. — [Taková čísla jsou $2k$, $2k + 2$ a $2k \,.\, (2k + 2) = 4k(k + 1)$; dále viz cvič. 10.]

12. Vyslovte a dokažte větu 5 pro n činitelů. — [Je-li číslo a_1 dělitelné číslem b_1, číslo a_2 číslem b_2, atd. až číslo a_n číslem b_n, je číslo $a_1 a_2 \ldots a_n$ dělitelné číslem $b_1 b_2 \ldots b_n$. Důkaz stejný jako v textu.]

13. Dokažte: Součin čtyř po sobě jdoucích čísel sudých je vždy dělitelný číslem 128. — [Taková čísla jsou $2k$, $2k + 2$, $2k + 4$, $2k + 6$, a $2k(2k + 2) \,.\, (2k + 4)\,(2k + 6) = 16k\,(k + 1)\,(k + 2)\,(k + 3)$; z činitelů k, $k + 1$, $k + 2$, $k + 3$ je jeden dělitelný čtyřmi a jeden dvěma.]

Čísla 56 a 21 jsou obě dělitelná sedmi, neboť $56 = 7 \,.\, 8$, $21 = 7 \,.\, 3$. Také čísla $56 + 21 = 77$, $56 - 21 = 35$, $56 \,.\, 2 - 21 \,.\, 3 = 49$, $56 + 21 \,.\, 2 = 98$ atd. jsou dělitelná sedmi. Dokážeme, že platí

Věta 6. *Jsou-li čísla a, b obě dělitelná číslem c, je jím dělitelné i každé číslo $ah + bk$, kde h, k jsou libovolná čísla celá, jež nemusí být kladná; volíme je však tak, aby $ah + bk$ bylo kladné.*

Důkaz: Předpokládáme, že číslo a je dělitelné číslem c, t. j. existuje takové číslo m, že $a = cm$, a že b je rovněž dělitelné číslem c, t. j. existuje takové číslo n, že $b = cn$. Čísla m, n jsou celá a kladná. Pak je $ah + bk = cmh + cnk = c(mh + nk)$. Ježto h, k, m, n jsou čísla celá, je i $mh + nk$ celé; ježto dále c i $ah + bk$ jsou čísla kladná, je i $mh + nk$ kladné. Je tedy číslo $ah + bk$ dělitelné číslem c.

Z této věty vyplývají dva důležité důsledky:

1. *Jsou-li čísla a, b obě dělitelná číslem c, je jím dělitelný i jejich součet $a + b$.*

2. *Jsou-li čísla a, b, o nichž předpokládáme, že $a > b$, obě dělitelná číslem c, je jím dělitelný i jejich rozdíl $a - b$.*

Prvý z těchto důsledků dostaneme, jestliže ve větě 6 položíme $h = k = 1$; druhý dostaneme, položíme-li v téže větě $h = 1$, $k = -1$.

Platnost věty 6 lze bez obtíží rozšířiti i na větší počet čísel.

Cvičení:

14. Jsou-li čísla a) a, $a + b$, b) a, $a - b$ obě dělitelná číslem c, je také číslo b dělitelné číslem c. Dokažte. — [a) $b = (a + b) - a$, b) $b = a - (a - b)$.]

15. Která celá čísla třeba dosaditi za x, aby výraz $x^2 + x + 6$ byl dělitelný a) dvěma, b) třemi? — [a) Libovolná, b) čísla tvaru $3c$ nebo $3c - 1$.]

16. Jestliže čísla a, b, c splňují rovnici $a + b = c$ a jsou-li kterákoli dvě z nich dělitelná číslem d, je jím dělitelné i třetí číslo. Dokažte. — [Je buď $c = a + b$ nebo $a = c - b$ nebo $b = c - a$.]

17. Vyslovte a dokažte větu 6 pro n čísel. — [Jsou-li čísla $a_1, a_2, \ldots, a_n$ všechna dělitelná číslem b, je i číslo $a_1k_1 + a_2k_2 + \ldots + a_nk_n$ dělitelné číslem b; při tom $k_1, k_2, \ldots, k_n$ jsou libovolná celá čísla volená tak, aby $a_1k_1 + a_2k_2 + \ldots + a_nk_n$ bylo kladné. Důkaz stejný jako v textu.]

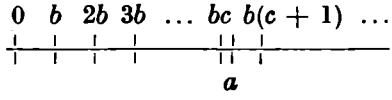
Hned na počátku jsme zjistili, že 320 není dělitelné číslem 12. Lehce se přesvědčíme, že $320 = 12 \cdot 26 + 8$, při čemž $0 < 8 < 12$. Podobný výsledek můžeme napsati i pro kterákoli jiná čísla, z nichž jedno není druhým dělitelné.

VĚTA 7. *Jestliže číslo a není dělitelné číslem b, pak lze jediným způsobem stanoviti čísla c a z tak, aby $a = bc + z$; při tom je c buď nula nebo číslo celé a kladné a z je číslo celé, pro které platí $0 < z < b$.*

Důkaz: Vezměme číslo 0 a všecky násobky čísla b:

$$0, b, 2b, 3b, 4b, 5b, \ldots$$

Číslo a není rovno žádnému z napsaných čísel, neboť o něm předpokládáme, že to není nula a že není násobkem čísla b. Číslo a tedy padne mezi některá dvě sousední napsaná čísla. Dejme tomu, že to jsou třeba čísla bc a $b(c + 1)$; při tom c je buď nula nebo je to některé číslo celé a kladné. Číslo bc je tedy menší než a a číslo $b(c + 1)$ je větší než a (viz obr. 1), takže rozdíl $a - bc$ musí být kladný a menší než rozdíl $b(c + 1) - bc = bc + b - bc = b$. Označíme-li rozdíl $a - bc$ písmenem z, t. j. položíme-li $a - bc = z$, je $a = bc + z$, kde z je číslo kladné, pro které platí $z < b(c + 1) - bc = b$. Tím je dokázána první část naší věty.



Obr. 1.

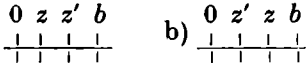
Zbývá ještě dokázat, že čísla c a z jsou čísly a a b určena jednoznačně. Mysleme si, že vedle čísel c a z existují ještě čísla c' a z' tak, že současně platí

$$a = bc + z,\ a = bc' + z',\ \text{kde}\ 0 < z < b,\ 0 < z' < b.$$

Pak musí $bc + z = bc' + z'$. Odtud plyne $bc - bc' = z' - z$ čili

$$b(c - c') = z' - z.$$

Čísla z' a z jsou obě menší než b a obě jsou kladná. Jsou možné tři případy: Buď je $z' > z$; pak je rozdíl $z' - z$ kladný a menší než b (viz obr. 2a). Nebo je $z > z'$; pak je rozdíl $z - z'$ kladný a menší než



Obr. 2.

b (obr. 2b), takže rozdíl $z' - z$ je záporný a větší než $-b$. Třetí možnost je, že $z = z'$; pak je $z' - z = 0$. V každém případě je tedy rozdíl $z' - z$ menší než b a větší než $-b$, t. j. $-b < z' - z < b$. Rozdíl $z' - z$ je roven výrazu $b(c - c')$; proto je také $-b < b(c - c') < b$. Dělíme-li čísla $-b$, $b(c - c')$, b číslem b, dostaneme čísla -1, $c - c'$, 1, o nichž platí $-1 < c - c' < 1$. Rozdíl dvou celých čísel c a c' má tedy být menší než 1 a větší než -1. Tomu lze však vyhovět jen tak, že bude $c = c'$, neboť rozdíl dvou různých celých čísel nemůže být nikdy menší než 1 a zároveň větší než -1. Je tedy nutně $c = c'$, čili $c - c' = 0$. Pak je $z' - z = b(c - c') = 0$, t. j. $z = z'$. Tím je vyslovená věta úplně dokázána.

Poznamenejme k tomu ještě to, že c je podíl, který vznikne při dělení $a : b$, a z je zbytek vzniklý při tomto dělení.

Věta platí i tehdy, když číslo a je dělitelné číslem b; pak ovšem, jak víme, je $a = bc$, t. j. zbytek z při dělení $a : b$ je roven nule.

Cvičení:

18. Dokažte: a) Každé číslo liché je tvaru $2c + 1$; b) každé číslo, které není dělitelné třemi je tvaru $3c + 1$ nebo $3c + 2$. — [Jaký zbytek může vyjít při dělení a) dvěma, b) třemi?]

19. Dokažte správnost vět: a) Součet dvou lichých po sobě jdoucích čísel je vždy dělitelný čtyřmi. b) Součet dvou čísel, z nichž žádné není dělitelné třemi a jejichž rozdíl jsou 2, je vždy dělitelný šesti. — [Taková čísla jsou a) $2c + 1$, $2c + 3$, b) $3c + 2$, $3c + 4$; proč nemůže být prvé číslo tvaru $3c + 1$?]

20. Dokažte větu: Dělíme-li číslo, které je aspoň trojciferné, čtyřmi, dostaneme týž zbytek, jako dělíme-li čtyřmi jeho poslední dvojčíslí. — [Každé číslo a, které je aspoň trojciferné, lze psát ve tvaru $a = 100A + B$.]

21. Dokažte větu: Dělíme-li číslo, které je aspoň čtyrciferné, osmi, dostaneme týž zbytek, jako dělíme-li osmi jeho poslední trojčíslí. — [Číslo a, které je aspoň čtyrciferné, lze psát $a = 1000A + B$.]

22. Dokažte větu: Dělíme-li číslo devíti (třemi) dostaneme týž zbytek, jako dělíme-li devíti (třemi) jeho ciferný součet. — [Je vždy $10^k = 9c + 1$ a každé číslo lze psát $a = b_0 + b_1 . 10 + b_2 . 10^2 + \ldots + b_n . 10^n$, při čemž $b_0, b_1, b_2, \ldots, b_n$ značí číslice, jimiž je psáno číslo a.]

23. Dokažte větu: Součin dvou lichých čísel je číslo liché. — [$(2h + 1) . (2k + 1) = 2(2hk + h + k) + 1$.]

24. Dokažte: a) Součet dvou sudých čísel je číslo sudé. b) Součet dvou lichých čísel je číslo sudé. c) Součet dvou čísel, z nichž jedno je sudé a druhé liché, je číslo liché.

25. Dokažte: Druhá mocnina každého lichého čísla zmenšená o 1 je dělitelná osmi. — [$(2k + 1)^2 - 1 = 4k(k + 1)$.]

26. Nejsou-li čísla a, b dělitelná třemi, je vždy jedno z čísel $a + b$, $a - b$ dělitelné třemi. Dokažte. — [Je-li $a = 3h + z_1$, $b = 3k + z_2$ (při tom z_1, z_2 je buď 1 nebo 2, viz cvič. 18), potom $a \pm b = 3(h \pm k) + z_1 \pm z_2$; jaké může býti $z_1 \pm z_2$?]

27. Je-li n libovolné číslo celé větší než 1, je vždy jedno z čísel $n^2 - 1$, n^2, $n^2 + 1$ dělitelné pěti. Dokažte. — [$n = 5c + z$, kde z je některé z čísel 0, 1, 2, 3, 4; $n^2 = 5(5c^2 + 2cz) + z^2$.]

28. Napíšeme-li n libovolných po sobě jdoucích čísel celých a kladných, je právě jedno z nich dělitelné číslem n. Dokažte. — [První z čísel je $a = nc + z$, kde $0 \leqq z < n$, poslední je $a + n - 1 = nc + z + n - 1$, kde $n - 1 \leqq z + n - 1 < 2n - 1$. Buď je $z = 0$ nebo mezi čísly z, $z + 1$, $z + 2, \ldots, z + n - 1$ je právě jedno, které je rovno n.]

29. Dělíme-li číslo 4754 devíti (jedenácti), dostaneme zbytek 2; týž zbytek dostaneme, dělíme-li devíti (jedenácti) číslo 47 + 54. Dokažte, že tuto vlastnost mají všecka čtyrciferná čísla. — [Čtyrciferné číslo lze psát ve tvaru $100A + B$ a $100 = 9 . 11 + 1$.]

30. Dělíme-li libovolné šesticiferné číslo dvaceti sedmi (třiceti sedmi), dostaneme týž zbytek, jako dělíme-li dvaceti sedmi (třiceti sedmi) součet jeho trojčíslí. Dokažte. — [Číslo můžeme psát ve tvaru $1000A + B$ a $1000 = 27 . 37 + 1$.]

31. Jestliže čísla a, b dělena číslem c dávají zbytky z_1, z_2, pak čísla a) $a + b$, b) $a - b$, c) ab dělena číslem c dávají zbytky, které se liší od výrazů a) $z_1 + z_2$, b) $z_1 - z_2$, c) $z_1 z_2$ o násobek čísla c. Dokažte. — [Je-li $a = ch + z_1$, $b = ck + z_2$ a $a + b = cm + z$, je $z = c(h + k - m) + z_1 + z_2$; je-li dále $a - b = cn + z'$, je $z' = c(h - k - n) + z_1 - z_2$; je-li konečně $ab = cp + z''$, je $z'' = c(chk + hz_2 + kz_1 - p) + z_1 z_2$.]

2. NEJVĚTŠÍ SPOLEČNÝ DĚLITEL

Zvolme si nějaká dvě čísla, třeba 36 a 60. Snadno se přesvědčíme, že číslo 36 je dělitelné čísly

1, 2, 3, 4, 6, 9, 12, 18, 36

a že číslo 60 je dělitelné čísly

1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

V obou skupinách se vyskytují čísla společná: 1, 2, 3, 4, 6 a 12. Tato čísla se nazývají společní dělitelé čísel 36 a 60. Číslo 12 je z nich největší. Proto říkáme, že 12 je největším společným dělitelem čísel 36 a 60. Zapisujeme to takto: $D(36, 60) = 12$.

Každé číslo, jímž jsou dvě daná čísla dělitelná, nazýváme jejich **společným dělitelem** a největší ze všech čísel, jimiž jsou obě daná čísla dělitelná, nazýváme jejich **největším společným dělitelem**. Pojmy společný dělitel a největší společný dělitel jsou ústřední pojmy, jimiž se budeme v této knížce zabývat. Že číslo D je největším společným dělitelem čísel a, b, zapisujeme $D(a, b) = D$.

VĚTA 8. *Číslo* 1 *je společným dělitelem kterýchkoli dvou čísel.*

Důkaz: Je to samozřejmý důsledek věty 1, podle níž je číslo 1 dělitelem každého čísla.

Tohoto společného dělitele kterýchkoli dvou čísel budeme v dalším nazývati jejich **samozřejmým společným dělitelem**.

Odtud a z věty 2 především plyne, že každá dvě (celá a kladná) čísla a, b mají největšího společného dělitele. Podle věty 8 mají totiž vždy aspoň jednoho společného dělitele, a to číslo 1. Podle věty 2 žádný dělitel čísla a nemůže být větší než a a žádný dělitel čísla b nemůže být větší než b; proto společný dělitel obou čísel a, b nemůže být větší, než je menší z čísel a, b. Mezi číslem 1 a menším z čísel a, b je konečný počet čísel, z nichž aspoň jedno, totiž číslo 1, je zcela jistě společným dělitelem čísel a, b. Je tedy také společných dělitelů čísel a, b konečný počet a jeden z nich je zcela jistě největší.

O společných dělitelích si nejprve odvodíme několik vět.

Největším společným dělitelem čísel 18 a 6 je číslo 6, neboť $18 = 6 \cdot 3$ a $6 = 6 \cdot 1$ a číslo 6 již většího dělitele mít nemůže.

Věta 9. *Je-li číslo a násobkem čísla b, je číslo b největším společným dělitelem obou čísel.*

Důkaz: Číslo a je dělitelné číslem b podle předpokladu a číslo b je dělitelné samo sebou podle věty 1; je tedy b společným dělitelem obou čísel. Zároveň je to jejich největší společný dělitel, neboť číslo b nemá žádného většího dělitele podle věty 2.

Obráceně z podmínky $D(a, b) = b$ ovšem plyne, že číslo a je dělitelné číslem b.

Před chvílí jsme zjistili, že $D(60, 36) = 12$. Dělíme-li číslo 60 číslem 36, vyjde podíl 1 a zbytek 24, t. j. podle věty 7 platí $60 = 36 \cdot 1 + 24$. Ale ihned vidíme, že také čísla 36 a 24 mají největšího společného dělitele 12, t. j. $D(36, 24) = 12$. Tento výsledek platí pro kterákoli dvě čísla. To praví

Věta 10. *Není-li číslo a násobkem čísla b a je-li $a > b$, pak největší společný dělitel čísel a, b je zároveň největším společným dělitelem čísel b, z, kde z je zbytek vzniklý při dělení $a : b$.*

Důkaz: Dělíme-li číslo a číslem b, dostaneme podíl c a zbytek z. Tato čísla vyhovují podle věty 7 rovnici $a = bc + z$. Odtud vypočteme $z = a - bc$. Důkaz má dvě části:

a) Nejprve dokážeme, že největší společný dělitel D čísel a, b je také dělitelem čísla z. To však vyplývá z věty 6. Je-li D (největším) společným dělitelem čísel a, b, existují čísla r, s tak, že $a = Dr$, $b = Ds$; potom je $z = a - bc = Dr - Dsc = D(r - sc)$. To však značí, že číslo D je také dělitelem čísla z. Číslo D je tedy společným dělitelem čísel b, z. Ještě ovšem nevíme, je-li to jejich největší společný dělitel. Označme největšího společného dělitele čísel b, z znakem D'. Musí tedy platit $D \leqq D'$, neboť D' je největší společný dělitel čísel b, z a žádný jiný jejich společný dělitel nemůže být větší.

b) Druhá část důkazu spočívá v tom, že dokážeme, že největší společný dělitel čísel b, z je také dělitelem čísla a. To však opět vyplývá z věty 6. Je-li D' (největším) společným dělitelem čísel b, z, existují čísla t, u tak, že $b = D't$, $z = D'u$; potom je $a = bc + z = D'tc + D'u = D'(tc + u)$. To však značí, že číslo D' je také dělitelem čísla a. Je to tedy společný dělitel čísel a, b. Poněvadž D je největší společný dělitel čísel a, b, musí být $D \geqq D'$.

Podle a) je $D \leqq D'$ a zároveň podle b) je $D \geqq D'$. Obojímu současně lze vyhovět jen tak, když je $D = D'$, a to jsme měli dokázat.

Cvičení:

32. Určete a) $D(a, 1)$, b) $D(a, a)$, c) $D(a, ab + 1)$. — [a) 1, b) a, c) 1, neboť žádný dělitel čísla a větší než 1 není dělitelem čísla $ab + 1$.]

33. Mají-li čísla a, b největšího společného dělitele D a je-li $a = Dr$, $b = Ds$, je největší společný dělitel čísel r, s roven jedné. Dokažte. — [Je-li $r = hm$, $s = km$, je $a = Dhm$, $b = Dkm$ a tedy také číslo Dm je společným dělitelem čísel a, b, ale to nesmí být větší než D. Je tedy $m = 1$.]

34. Mají-li čísla a, b největšího společného dělitele D, při čemž $a > b$, mají téhož největšího společného dělitele i čísla b, $a - b$. Dokažte. — [Třeba dokázat dvě věci: a) Největší společný dělitel čísel a, b je dělitelem čísla $a - b$, a tedy také společným dělitelem čísel b, $a - b$. b) Největší společný dělitel čísel b, $a - b$ je dělitelem čísla a, a tedy také společným dělitelem čísel a, b. Závěr jako v důkazu věty 10.]

35. Mají-li čísla a, b největšího společného dělitele D, mají téhož největšího společného dělitele i čísla $a + kb$, b, kde k je libovolné číslo celé. Dokažte. — [a) Největší společný dělitel čísel a, b je dělitelem čísla $a + kb$. b) Největší společný dělitel čísel $a + kb$, b je dělitelem čísla a.]

Věty 9 a 10 nám umožní stanoviti největšího společného dělitele kterýchkoli dvou čísel. Vezměme třeba čísla 684 a 252. Proveďme dělení 684 : 252. Vyjde podíl 2 a zbytek 180. Proto podle věty 10 je $D(684, 252) = D(252, 180)$. Opakujeme-li tento postup s čísly 252 a 180, shledáme, že 252 : 180 dává podíl 1 a zbytek 72, takže opět podle věty 10 je $D(252, 180) = D(180, 72)$. Postup opakujeme ještě jednou. Dělení 180 : 72 dává podíl 2 a zbytek 36; proto $D(180, 72) = D(72, 36)$. Při dalším dělení 72 : 36 vyjde podíl 2 beze zbytku. Je tedy číslo 72 dělitelné číslem 36, a proto podle věty 9 je $D(72, 36) = 36$. Celkem tedy je $D(684, 252) = 36$.

Tento způsob výpočtu se zpravidla označuje názvem **Eukleidův algoritmus postupného dělení.***) Abychom při něm nemuseli mnoho psát, lze výpočet uspořádati třeba takto:

*) Eukleides byl jedním z nejslavnějších matematiků starověku. Žil ve IV. stol. př. Kr. v Alexandrii v Egyptě a napsal spis nazvaný Stoicheia (česky Základy), který se stal jednou z nejrozšířenějších a nejznámějších knih na světě. Obsahuje 13 částí (knih), z nichž 5 jedná o rovinné geometrii, 3 o vlastnostech celých čísel, 2 o poměrech úseček a 3 o geometrii v prostoru. Názvem algoritmus označujeme početní předpis, podle něhož lze nějaké číslo vypočítat. Název vznikl zkomolením jména arabského matematika Mohameda al Chovarismi (žil v IX. stol. a pocházel z provincie Chorazan, nynější Chivy v Uzbecké SSR) a řeckého slova arithmos — číslo.

684	252	180	72	36	0
	2	1	2	2	

Do prvého řádku napíšeme daná dvě čísla (větší napřed), dělíme je mezi sebou, při čemž podíl píšeme do druhého řádku a zbytek do prvého řádku o jedno místo dále. Tak pokračujeme tak dlouho, až vyjde dělení beze zbytku. Poslední zbytek, který není roven nule, je největším společným dělitelem daných dvou čísel.

Ještě by bylo třeba ukázat, že tento postup vždy vede k cíli, t. j. že skončí po určitém počtu kroků. To však nahlédneme velice snadno, uvědomíme-li si, že zbytek při dělení je vždy číslo celé a kladné a menší než dělitel (viz větu 7). Proto se velikost zbytků při každém kroku zmenšuje. Ježto nemůže vyjít zbytek záporný, musí po určitém počtu kroků vyjít zbytek rovný nule.

Řadu dělení, která jsme právě provedli, lze zapsati takto:

$$\begin{aligned} 684 &= 252 \,.\, 2 + 180, \\ 252 &= 180 \,.\, 1 + 72, \\ 180 &= 72 \,.\, 2 + 36, \\ 72 &= 36 \,.\, 2. \end{aligned}$$

Z těchto rovnic postupně vyplývá

$$\begin{aligned} 180 &= 684 - 252 \,.\, 2, \\ 72 &= 252 - 180 \,.\, 1 = 252 - (684 - 252 \,.\, 2) \,.\, 1 = 252 \,.\, 3 - 684 \,.\, 1, \\ 36 &= 180 - 72 \,.\, 2 = 684 - 252 \,.\, 2 - (252 \,.\, 3 - 684) \,.\, 2 = \\ &= 684 \,.\, 3 - 252 \,.\, 8. \end{aligned}$$

Tím se nám podařilo vyjádřit největšího společného dělitele (36) pomocí obou daných čísel (684 a 252).

Týž výpočet lze provésti i pro kterákoli jiná dvě čísla. Je ovšem možné, že pro jiná čísla povede k jinému počtu kroků; výsledek však bude vždy týž, t. j. *největšího společného dělitele libovolných dvou čísel a, b, z nichž žádné není dělitelné druhým, dostaneme vždy jako rozdíl dvou vhodných násobků těchto čísel.*

Čísla 60 a 36 mají největšího společného dělitele 12. Vedle toho mají ještě další společné dělitele: 1, 2, 3, 4, 6, jak jsme zjistili na str. 12. Všichni tito dělitelé jsou děliteli čísla 12. Platí

Věta 11. *Každý společný dělitel čísel a, b je dělitelem jejich největšího společného dělitele.*

Důkaz: Označme některého společného dělitele čísel a, b písmenem d. Ježto d je dělitelem obou čísel a, b, lze nalézti dvě čísla u, v tak, že $a = du$, $b = dv$. Předpokládejme třeba, že $a > b$. Kdyby tomu bylo naopak, stačí čísla a, b spolu vyměnit. Dělíme-li číslo a číslem b, dostaneme podíl c a zbytek z, t. j. platí $a = bc + z$ čili $z = a - bc$. Dosadíme-li sem $a = du$, $b = dv$, vyjde $z = du - dvc = d(u - vc)$, takže číslo d je také dělitelem čísla z a je tedy také společným dělitelem čísel b, z. Pokračujeme-li dále v provádění Eukleidova algoritmu, dostáváme další zbytky a všecky tyto zbytky mají podle toho, co bylo právě dokázáno, číslo d za dělitele. Má jej tedy také za dělitele i poslední zbytek, který není roven nule a který je, jak víme, největším společným dělitelem čísel a, b. Tím je věta dokázána.

Cvičení:

36. Postupným dělením určete a) $D(455, 273)$, b) $D(945, 729)$, c) $D(903, 221)$. — [a) 91, b) 27, c) 1.]

37. Je-li d společný dělitel čísel a, b, t. j. je-li $a = du$, $b = dv$, a je-li největší společný dělitel čísel u, v roven jedné, je $d = D(a, b)$. Dokažte a porovnejte s větou ve cvič. 33. — [$D(a, b) = dm$ (věta 11); je-li $a = Dr$, $b = Ds$, je $a = dmr$, $b = dms$, takže $u = mr$, $v = ms$. Je-li $D(u, v) = 1$, musí $m = 1$.]

38. Mají-li čísla a, b největšího společného dělitele D, mají čísla ma, mb největšího společného dělitele mD. Dokažte. — [Označme $D(ma, mb) = D'$. a) mD je společným dělitelem čísel ma, mb, proto $mD \leqq D'$. b) m je dělitelem čísla D' (věta 11). Je-li $ma = D'r$, $mb = D's$, je $a = \frac{D'}{m} . r$, $b = \frac{D'}{m} . s$, proto $\frac{D'}{m}$ je společným dělitelem čísel a, b, takže $\frac{D'}{m} \leqq D$.]

39. Větu uvedenou ve cvič. 33 lze dokázati také tak, že porovnáme Eukleidův algoritmus prováděný s čísly a, b s týmž postupem prováděným s čísly r, s. Proveďte to. — [Všecky zbytky se zmenší Dkrát.]

40. Větu uvedenou ve cvič. 38 dokažte tak, že porovnáte Eukleidův algoritmus prováděný s čísly a, b s týmž postupem prováděným s čísly ma, mb. — [Všecky zbytky se zvětší $m$krát.]

Lze také hovořiti o společných dělitelích většího počtu čísel. Jsou to čísla, jimiž jsou všecka daná čísla dělitelná. Největší z nich se nazývá největší společný dělitel daných čísel. Jsou-li daná čísla označena písmeny a, b, c, ..., užíváme pro jejich největšího společného dělitele znaku $D(a, b, c, \ldots)$.

Hledáme-li $D(90, 60, 36)$, nalezneme nejprve třeba $D(90, 60) = 30$. Číslo 30 je dělitelem čísel 90 a 60. Utvoříme-li nyní $D(30, 36) = 6$, jsou jím dělitelná i čísla 90 a 60, proto $D(90, 60, 36) = D(30, 36) = 6$. O tom, jak se vypočte největší společný dělitel tří čísel, nás poučuje

VĚTA 12. *Největší společný dělitel tří čísel a, b, c je roven největšímu společnému děliteli čísel D, c, kde $D = D(a, b)$.*

Důkaz: Označme největšího společného dělitele čísel a, b, c znakem Δ, největšího společného dělitele čísel a, b znakem D a největšího společného dělitele čísel D, c znakem D'.

a) Číslo Δ je společným dělitelem čísel a, b, a proto je podle věty 11 také dělitelem jejich největšího společného dělitele D. Vedle toho je také dělitelem čísla c, takže je také společným dělitelem čísel D, c. To je možné jen tak, že $\Delta \leqq D'$, neboť D' je největší společný dělitel čísel D, c.

b) Číslo D' je dělitelem čísla D, proto je také společným dělitelem čísel a, b. Vedle toho je také dělitelem čísla c, takže je společným dělitelem čísel a, b, c. To je možné jen tak, že $D' \leqq \Delta$, neboť Δ je největším společným dělitelem čísel a, b, c.

Podle a) je $\Delta \leqq D'$ a zároveň podle b) je $D' \leqq \Delta$. Obojímu současně lze vyhověti jen tak, že $D' = \Delta$, a to jsme měli dokázat.

Při hledání největšího společného dělitele tří čísel lze vyjíti od kterýchkoli dvou z nich. Označíme-li třeba největšího společného dělitele čísel b, c znakem D_1 a největšího společného dělitele čísel a, D_1 znakem D_1', dokážeme zcela stejně, že $D_1' = \Delta$, takže $D_1' = D'$, čímž je vyslovené tvrzení dokázáno.

Větu 12 lze bez obtíží rozšířiti i na větší počet čísel.

Cvičení:

41. Stanovte a) $D(568, 426, 355)$, b) $D(468, 819, 1092)$. — [a) 71, b) 39.]

42. Určete $D(ac, bc, c)$. — [c.]

43. Co značí podmínka $D(a, b, c) = c$? — [$a = ch$, $b = ck$.]

44. Je-li $D(a, c) = 1$, $D(b, c) = 1$, je také $D(ab, c) = 1$. Dokažte. — [Vypočtěte $D(ab, ac, c)$ dvojím způsobem, při čemž užijete výsledku cvič. 38.]

45. Dokažte větu: Každý společný dělitel čísel a, b, c je dělitelem jejich největšího společného dělitele. — [Označme $D(a, b) = D$. Každý společný dělitel d čísel a, b, c je dělitelem čísla D (proč?) a je také dělitelem největšího společného dělitele čísel D a c.]

46. Je-li $D(a, b) = D_1$, $D(c, d) = D_2$, je $D(a, b, c, d) = D(D_1, D_2)$. Dokažte. — [Označme $D(a, b, c, d) = \Delta$, $D(D_1, D_2) = D$. a) Δ je dělitelem čísel D_1 i D_2, proto $\Delta \leqq D$. b) D je dělitelem čísel $a, b; c, d$, proto $D \leqq \Delta$.]

47. Je-li $D(a, b) = D$, $D(a', b') = D'$, určete $D(aa', ab', ba', bb')$. — [Užijte výsledků cvič. 46 a cvič. 38. Výsledek DD'.]

3. NEJMENŠÍ SPOLEČNÝ NÁSOBEK

Vyjděme opět ze dvou libovolně zvolených čísel, třeba z čísel 36 a 60. Utvořme všecky jejich násobky. Dostaneme dvě řady násobků:

36, 72, 108, 144, **180**, 216, 252, 288, 324, **360**, 396, 432, ...,

60, 120, **180**, 240, 300, **360**, 420, 480, **540**, 600, 660, **720**, ...

V obou skupinách se vyskytují čísla společná: 180, 360, 540, 720, ... Tato čísla se nazývají společné násobky čísel 36 a 60. Číslo 180 je z nich nejmenší. Proto říkáme, že 180 je nejmenší společný násobek čísle 136 a 60. Zapisujeme to takto: $n(36, 60) = 180$.

Každé číslo, v němž jsou dvě daná čísla obsažena, nazýváme jejich **společným násobkem**. Nejmenší ze všech čísel, v němž jsou obě daná čísla obsažena, nazýváme jejich **nejmenším společným násobkem**. Že číslo n je nejmenším společným násobkem čísel a, b, zapisujeme $n(a, b) = n$.

Snadno zjistíme, že každá dvě (celá a kladná) čísla a, b mají nejmenší společný násobek. Součin ab obou čísel je jistě jejich společným násobkem. Podle věty 2 žádný násobek čísla a nemůže být menší než a a žádný násobek čísla b nemůže být menší než b; proto společný násobek čísel a, b nemůže být menší, než je větší z čísel a, b. Mezi větším z čísel a, b a jejich součinem ab je konečný počet čísel, z nichž aspoň jedno, totiž číslo ab, je zcela jistě společným násobkem čísel a, b. Mezi větším z čísel a, b a součinem ab je tedy také konečný počet jejich společných násobků a jeden z nich je zcela jistě nejmenší.

Mezi společnými děliteli dvou čísel a jejich společnými násobky je však jeden zásadní rozdíl: Každá dvě čísla mají vždy jen konečný počet společných dělitelů, ale nekonečný počet společných násobků.

Nejmenším společným násobkem čísel 18 a 6 je číslo 18, neboť $18 = 18 . 1$ a $18 = 6 . 3$ a číslo 18 již menší násobek míti nemůže.

Věta 13. *Je-li číslo a násobkem čísla b, je číslo a nejmenším společným násobkem čísel a, b.*

Důkaz: Číslo a je násobkem sama sebe podle věty 1 a je také násobkem čísla b podle předpokladu. Je tedy společným násobkem obou čísel. Zároveň je také nejmenším společným násobkem obou čísel, neboť žádný násobek čísla a nemůže být podle věty 2 menší než a.

Obráceně z podmínky $n(a, b) = a$ ovšem plyne, že číslo a je násobkem čísla b.

Čísla 36 a 60 mají společné násobky 180, 360, 540, 720, ..., při čemž $360 = 180 . 2$, $540 = 180 . 3$, $720 = 180 . 4$ atd.; všechny tyto násobky jsou násobky čísla 180, které je nejmenším společným násobkem čísel 36 a 60. Dokážeme, že platí

Věta 14. *Každý společný násobek čísel a, b je násobkem jejich nejmenšího společného násobku.*

Důkaz: Označme některý společný násobek čísel a, b písmenem N, jejich nejmenší společný násobek písmenem n. Ježto N je společným násobkem čísel a, b, lze nalézti dvě čísla u, v tak, že $N = au = bv$. Ježto dále n je nejmenším společným násobkem čísel a, b, lze nalézti dvě čísla r, s tak, že $n = ar = bs$. Dělíme-li číslo N číslem n, dostaneme podle věty 7 podíl k a zbytek z, t. j. $N = nk + z$, při čemž k a z jsou čísla celá a buď $z = 0$ nebo $0 < z < n$. Odtud plyne, že $z = N - nk$. Dosadíme-li sem $N = au$, $n = ar$, je $z = au - ark = a(u - rk)$. Podobně dosadíme-li $N = bv$, $n = bs$, je $z = bv - bsk = b(v - sk)$. Čísla $u - rk$, $v - sk$ jsou buď obě rovna nule (to nastane, když $z = 0$) nebo jsou obě celá a kladná (když $z > 0$). V tomto druhém případě z je společným násobkem čísel a, b, který je menší než n. To však není možné, neboť jsme předpokládali, že n je nejmenší společný násobek čísel a, b. Proto tato druhá možnost nenastane a obě uvažovaná čísla $u - rk$, $v - sk$, jakož i číslo z, musí být rovna nule a číslo N je tedy násobkem čísla n. To jsme chtěli dokázat.

Cvičení:

48. Určete a) $n(a, 1)$, b) $n(a, a)$. — [a) a, b) a.]

49. Je možné, aby největší společný dělitel dvou čísel byl roven jejich

nejmenšímu společnému násobku? — [Je-li x společná hodnota největšího společného dělitele i nejmenšího společného násobku čísel a, b, musí $a \leqq x$ a současně $x \leqq a$; podobně pro b.]

50. Napište všechna čísla, která dělena čísly a, b dávají po každé zbytek z. — [Čísla tvaru $k \,.\, n(a, b) + z$.]

51. Je-li n nejmenší společný násobek čísel a, b a je-li $n = ar = bs$, je největší společný dělitel čísel r a s roven jedné. Dokažte. — [Je-li $r = km$, $s = hm$, je také $\frac{n}{m} = ak = bh$, takže číslo $\frac{n}{m}$ je společným násobkem čísel a, b, ale to nemůže být menší než n. Je tedy $m = 1$.]

52. Je-li N společným násobkem čísel a, b, t. j. je-li $N = ar = bs$, a je-li největší společný dělitel čísel r, s roven jedné, je $N = n(a, b)$. Dokažte. — [$N = nm$ (věta 14); je-li $n = au = bv$, je $N = aum = bvm$, takže $r = um$, $s = vm$. Ježto má být $D(r, s) = 1$, musí $m = 1$.]

53. Mají-li čísla a, b nejmenší společný násobek n, mají čísla ma, mb nejmenší společný násobek mn. Dokažte. — [Označme $n(ma, mb) = n'$. a) mn je společný násobek čísel ma, mb, proto $mn \geqq n'$. b) $n' = mar = mbs$, n' je dělitelné číslem m a $\frac{n'}{m}$ je společný násobek čísel a, b; proto $\frac{n'}{m} \geqq n$.]

Vypočítali jsme, že $D(36, 60) = 12$, $n(36, 60) = 180$. Snadno shledáme, že $12 \,.\, 180 = 36 \,.\, 60 = 2160$. Dokážeme, že tuto vlastnost má největší společný dělitel a nejmenší společný násobek každých dvou čísel.

Věta 15. *Je-li D největší společný dělitel a n nejmenší společný násobek čísel a, b, je $ab = Dn$.*

Důkaz: Je-li D největší společný dělitel a n nejmenší společný násobek čísel a, b, lze nalézti čísla r, s, u, v tak, že $a = Dr$, $b = Ds$, $n = au = bv$.

a) Utvořme číslo $\frac{ab}{D}$. Toto číslo je ovšem celé, neboť kterékoli z čísel a, b je dělitelné číslem D. Protože $b = Ds$, proto $\frac{ab}{D} = as$. Protože dále $a = Dr$, proto $\frac{ab}{D} = br$, takže $\frac{ab}{D}$ je společným násobkem čísel a, b. Podle věty 14 je to tedy násobek jejich nejmenšího společného násobku, a proto $\frac{ab}{D} \geqq n$ čili $ab \geqq Dn$.

b) Utvořme nyní číslo $\frac{ab}{n}$. To je také celé vzhledem k větě 14,

neboť ab je společný násobek daných čísel. Protože $n = bv$, proto $\frac{ab}{n} = \frac{a}{v}$ čili $a = \frac{ab}{n} . v$. Protože dále $n = au$, proto $\frac{ab}{n} = \frac{b}{u}$ čili $b = \frac{ab}{n} . u$, takže $\frac{ab}{n}$ je společným dělitelem čísel a, b. Podle věty 11 je to tedy dělitel jejich největšího společného dělitele, a proto $\frac{ab}{n} \leqq D$ čili $ab \leqq Dn$.

Podle a) je $ab \geqq Dn$ a zároveň podle b) je $ab \leqq Dn$. Tomu lze vyhověti jen tak, že $ab = Dn$.

Věta 15 nám umožní výpočet nejmenšího společného násobku dvou čísel. Nejprve vypočteme Eukleidovým algoritmem jejich největšího společného dělitele D a pak podle právě dokázané věty jejich nejmenší společný násobek je $n = \frac{ab}{D}$.

Cvičení:

54. Vypočtěte a) $n(135, 144)$, b) $n(238, 357)$, c) $n(1071, 882)$. — [a) 2160, b) 714, c) 14 994.]

55. Největší společný dělitel dvou čísel je 24, jejich nejmenší společný násobek je 5040. Jedno číslo je 240. Určete druhé. — [504.]

56. Mají-li čísla a, b největšího společného dělitele D a nejmenší společný násobek n, je $a = Dr$, $b = Ds$, $n = au = bv$. Dokažte, že $r = v$, $s = u$. — [Z rovnice $ab = Dn$ plyne $\frac{a}{D} = \frac{n}{b}$, $\frac{b}{D} = \frac{n}{a}$.]

57. Větu ze cvič. 53 dokažte pomocí věty 15 užívajíce výsledku cvič. 38. — [Označme $D(a, b) = D$, $D(ma, mb) = D'$, $n(ma, mb) = n'$; při tom $D' = mD$. Pak $ma . mb = D'n'$, $n' = \frac{ma . mb}{mD} = mn$.]

Lze také hovořiti o společných násobcích většího počtu čísel. Jsou to čísla, která jsou všemi danými čísly dělitelná. Nejmenší z nich se nazývá nejmenší společný násobek daných čísel. Jsou-li daná čísla označena písmeny a, b, c, ..., užíváme pro jejich nejmenší společný násobek znaku $n(a, b, c, \ldots)$.

Hledáme-li na příklad $n(24, 36, 60)$, nalezneme nejprve $n(24, 36) = 72$. V čísle 72 jsou obsažena čísla 24 i 36. Utvoříme-li $n(72, 60) = 360$, jsou v něm obsažena také čísla 24 a 36; proto $n(24, 36, 60) = 360$.

Věta 16. *Nejmenší společný násobek tří čísel a, b, c, je roven nejmenšímu společnému násobku čísel n, c, kde $n = n(a, b)$.*

Důkaz: Označme nejmenší společný násobek čísel a, b, c znakem v, nejmenší společný násobek čísel a, b znakem n a nejmenší společný násobek čísel n, c znakem n'.

a) Číslo v je společným násobkem čísel a, b, a proto je podle věty 14 násobkem jejich nejmenšího společného násobku n. Ježto v je také násobkem čísla c, je zároveň společným násobkem čísel n, c. To je možné jen tak, že $v \geqq n'$, neboť n' je nejmenším společným násobkem čísel n, c.

b) Číslo n' je společným násobkem čísel n, c, avšak n je násobkem čísla a a zároveň také násobkem čísla b; proto n' je společným násobkem čísel a, b, c. To je možné jen tak, že $n' \geqq v$, neboť v je nejmenším společným násobkem čísel a, b, c.

Podle a) je $v \geqq n'$ a zároveň podle b) je $n' \geqq v$. Obojímu současně lze vyhověti jen tak, když je $n' = v$, a to jsme chtěli dokázat.

Při hledání nejmenšího společného násobku tří čísel lze vyjíti od kterýchkoli dvou z nich. Označíme-li třeba nejmenší společný násobek čísel b, c znakem n_1 a nejmenší společný násobek čísel a, n_1 znakem n_1', dokážeme zcela stejně, že $n_1' = v$, takže $n_1' = n'$, čímž je vyslovené tvrzení dokázáno.

Dokázanou větu lze bez obtíží rozšířiti i na větší počet čísel.

Cvičení:

58. Stanovte a) $n(58, 87, 145)$, b) $n(296, 222, 185)$. — [a) 870, b) 4440.]

59. Co značí $n(a, b, c) = c$? — [$c = ar$, $c = bs$.]

60. Každý společný násobek čísel a, b, c je násobkem jejich nejmenšího společného násobku. Dokažte. — [Označíme-li $n(a, b) = n$, je každý společný násobek N čísel a, b, c násobkem čísla n (proč?). Je tedy N společným násobkem čísel n, c.]

61. Je-li $n(a, b) = n_1$, $n(c, d) = n_2$, je $n(a, b, c, d) = n(n_1, n_2)$. Dokažte. — [Označíme $n(a, b, c, d) = v$, $n(n_1, n_2) = n$. a) v je násobkem čísel n_1, n_2, proto $v \geqq n$. b) n je násobkem čísel a, b; c, d, proto $n \geqq v$.]

62. Je-li $n(a, b) = n$, $n(a', b') = n'$, určete $n(aa', ab', ba', bb')$. — [Užijte výsledku cvič. 61 a cvič. 53; výsledek nn'.]

63. Dokažte, že $n(ab, ac, bc) = \frac{abc}{D(a, b, c)}$. — [Označme $D(a, b) = D$,

$D(a, b, c) = \Delta$. Pak $n(ab, ac, bc) = n\left(ab, c \cdot \frac{ab}{D}\right) = \frac{ab}{D} \cdot n(D, c) = \frac{ab}{D} \cdot \frac{Dc}{D(D, c)} = \frac{abc}{\Delta}$.]

64. Dokažte, že $D(ab, ac, bc) = \frac{abc}{n(a, b, c)}$. — [Označme $n(a, b) = n$, $n(a, b, c) = \nu$. Pak $D(ab, ac, bc) = D\left(ab, c \cdot \frac{ab}{n}\right) = \frac{ab}{n} \cdot D(n, c) = \frac{ab}{n} \cdot \frac{nc}{n(n, c)} = \frac{abc}{\nu}$.]

4. VLASTNOSTI ČÍSEL NESOUDĚLNÝCH

Taková dvě čísla, jejichž největší společný dělitel je roven jedné, se nazývají navzájem nesoudělná. Jestliže největší společný dělitel dvou čísel je větší než 1, nazýváme tato čísla navzájem soudělnými.

Na příklad čísla 4 a 9 jsou navzájem nesoudělná, neboť $D(4, 9) = 1$. Také čísla 1, a třeba považovati za čísla navzájem nesoudělná, neboť $D(1, a) = 1$.

Snadno shledáme, že $n(9, 4) = 9 \cdot 4 = 36$. To platí pro každou dvojici čísel navzájem nesoudělných.

Věta 17. *Nejmenší společný násobek dvou čísel a, b navzájem nesoudělných je roven jejich součinu. Obráceně, je-li nejmenší společný násobek dvou čísel roven jejich součinu, jsou to čísla navzájem nesoudělná.*

Důkaz: Věta je bezprostředním důsledkem věty 15. Jestliže do rovnice $ab = Dn$ dosadíme $D = 1$, vyjde $n = ab$. Dosadíme-li do téže rovnice $n = ab$, vyjde $D = 1$.

Čísla 4 a 9 jsou navzájem nesoudělná. Číslo 252 je dělitelné čtyřmi i devíti, neboť $252 = 4 \cdot 63 = 9 \cdot 28$, a je také dělitelné třiceti šesti ($= 9 \cdot 4$), neboť $252 = 36 \cdot 7$. To platí obecně.

Věta 18. *Je-li číslo c dělitelné dvěma čísly a, b, jež jsou navzájem nesoudělná, je dělitelné také jejich součinem.*

Důkaz: Předpokládejme, že c je dělitelné číslem a i číslem b. Je tedy c společným násobkem obou těchto čísel a podle věty 14 je násobkem jejich nejmenšího společného násobku n, t. j. $c = nk$. Ale

a, b jsou čísla navzájem nesoudělná, proto podle věty 17 je $n = ab$, takže $c = ab \,.\, k$. Je tedy číslo c dělitelné součinem ab.

Víme, že číslo 252 je dělitelné devíti. Dále víme, že 252 se dá psát jako součin $4 \,.\, 63$ a že čísla 4 a 9 jsou navzájem nesoudělná. Z toho můžeme soudit, že číslo 63 je dělitelné devíti.

Věta 19. *Je-li součin am dvou čísel a, m dělitelný třetím číslem b, jež je nesoudělné s činitelem a, je číslem b dělitelný druhý činitel m.*

Důkaz: Předpokládejme, že součin am je dělitelný číslem b, které je s číslem a nesoudělné. Vedle toho je součin am také dělitelný číslem a, takže am je dělitelné dvěma čísly a, b, jež jsou navzájem nesoudělná. Proto je podle věty 18 číslo am dělitelné součinem ab, t. j. $am = ab \,.\, k$. Dělíme-li obě strany této rovnice číslem a, vyjde $m = bk$, takže číslo m je dělitelné číslem b.

Cvičení:

65. Ze dvou čísel navzájem nesoudělných je aspoň jedno liché. Dokažte. — [Co by se stalo, kdyby byla obě sudá?]

66. Každá dvě bezprostředně po sobě následující čísla celá kladná a, b jsou navzájem nesoudělná. Dokažte. — [Čím musí být dělitelné číslo $b - a$?]

67. Každá dvě lichá čísla lišící se o libovolnou mocninu čísla 2 jsou navzájem nesoudělná. Dokažte. — [Čím musí být dělitelno $b - a$?]

68. Součin tří po sobě následujících čísel celých kladných, z nichž prostřední je liché, je vždy dělitelný dvaceti čtyřmi. Dokažte. — [Z těchto čísel je vždy jedno dělitelné třemi, jedno krajní dvěma a druhé krajní čtyřmi.]

69. Součin pěti po sobě následujících čísel celých kladných, z nichž prostřední je sudé, je vždy dělitelný číslem 240. Dokažte. — [Z těchto čísel je vždy jedno dělitelné pěti, aspoň jedno třemi a buď jedno čtyřmi a dvě dvěma nebo dvě čtyřmi a jedno dvěma.]

70. Je-li n libovolné číslo celé větší než 1, dokažte, že číslo $(n^3 - 1)\, n^2(n^3 + 1)$ je dělitelné šedesáti. — [Z uvedených činitelů je jeden dělitelný třemi, jeden čtyřmi a jeden pěti (viz cvič. 27).]

71. Větu 17 lze dokázati přímo z věty 14 bez použití věty 15 (a tedy také bez použití věty 11). Proveďte to. — [1. Z věty 14 plyne $ab = nh$, při čemž h je společný dělitel čísel a, b. Ježto a, b jsou čísla navzájem nesoudělná, je $h = 1$. 2. Je-li $n = ab$ a je-li $a = Dr$, $b = Ds$, je $\frac{n}{D} = br = as$ také společný násobek čísel a, b, který však nemůže být menší než n. Proto musí $D = 1$.]

72. Jsou-li a, b dvě čísla navzájem nesoudělná, je $D(am, b) = D(m, b)$; při tom m je libovolné číslo. Dokažte. — [Vypočtěte dvojím způsobem $D(am, bm, b)$.]

73. Nechť čísla a, b jsou navzájem nesoudělná a nechť b je násobkem čísla c. Pak čísla a, c jsou také navzájem nesoudělná. Dokažte. — [Označme $D(a, c) = D$. Pak $a = Dr$, $c = Dt$. Ježto $b = ck = Dtk$, je D společným dělitelem čísel a, b, t. j. $D \leqq D(a, b)$.]

74. Čísla a, b jsou navzájem nesoudělná a čísla am, b jsou obě dělitelná číslem c. Pak je číslo m dělitelné číslem c. Dokažte. — [Podle cvič. 73 je $D(a, c) = 1$. Číslo am je dělitelné číslem c, které je s a nesoudělné; proto $m = ch$. — Jiný důkaz: Hledejte $D(am, bm, c)$ dvěma způsoby.]

5. PRVOČÍSLA

Mezi všemi čísly hrají důležitou úlohu čísla zvaná **prvočísla**. To jsou ta čísla, která nemají jiných dělitelů kromě dělitelů samozřejmých. Čísla, která nejsou prvočísly, se nazývají **čísla složená**. Na příklad čísla 2, 3, 5, 7, ..., jsou prvočísla, čísla 4, 6, 8, 9, ... jsou čísla složená. Číslo 1 se zpravidla za prvočíslo nepovažuje.

Prvočíslo 3 je dělitelné pouze čísly 1 a 3. Prvočíslo 7 je dělitelné pouze čísly 1 a 7. Prvočísla 3 a 7 mají tedy pouze samozřejmého společného dělitele, jímž je číslo 1.

VĚTA 20. *Každá dvě různá prvočísla p, q jsou navzájem nesoudělná.*

Důkaz: Poněvadž p je prvočíslo, má pouze dva dělitele: 1 a p. Z téhož důvodu má q pouze dva dělitele: 1 a q. Ježto p je různé od q, čísla p, q mají jediného společného dělitele: jednotku. Jsou to tedy čísla navzájem nesoudělná.

Číslo 60 je dělitelné dvěma, t. j. $60 = 2 \cdot 30$. Číslo 30 je rovněž dělitelné dvěma, t. j. $30 = 2 \cdot 15$, takže $60 = 2 \cdot 2 \cdot 15$. Číslo 15 je dělitelné třemi, t. j. $15 = 3 \cdot 5$, takže $60 = 2 \cdot 2 \cdot 3 \cdot 5$. Tak jsme číslo 60, které je složené, vyjádřili ve tvaru součinu prvočísel.

VĚTA 21. *Každé číslo složené lze napsati ve tvaru součinu několika prvočísel.*

Důkaz: Není-li a prvočíslem, má (kromě jednotky a sama sebe) ještě další dělitele. Budiž p_1 nejmenší z nich. Číslo p_1 je jistě prvočíslem. To dokážeme takto: Kdyby p_1 nebylo prvočíslem, bylo by dělitelné nějakým číslem $m < p_1$ různým od jedné a podle věty 4 by také číslo a bylo dělitelné číslem m. Pak by p_1 nebyl nejmenší dělitel

čísla a různý od jedné, nýbrž dělitelem m by byl menší. Není tedy možné, aby p_1 nebylo prvočíslo. Tak dostáváme $a = p_1 b$, kde p_1 je prvočíslo a $b < a$. Je-li b také prvočíslo, jsme hotovi; je-li však b číslo složené, lze postup opakovati pro číslo b a dostaneme $b = p_2 c$, kde p_2 je opět prvočíslo a $c < b$. Tak můžeme postupovati dále. Poněvadž podíly b, c, ..., které takto dostaneme, se stále zmenšují, při čemž to jsou čísla kladná, postup určitě jednou skončí a nakonec dospějeme k součinu samých prvočísel: $a = p_1 p_2 p_3 \ldots p_r$. Prvočísla, jež takto dostaneme, nemusí být ovšem všecka navzájem různá.

Nyní si odvodíme větu, podle níž můžeme poznat, je-li nějaké číslo prvočíslem. Abychom rozhodli, je-li třeba číslo 149 prvočíslem, musíme dokázat, že nemá jiných dělitelů kromě dělitelů samozřejmých. Měli bychom je tedy děliti všemi čísly celými a kladnými a menšími než 149. To však není třeba; bude stačit, najdeme-li jeho nejmenšího dělitele různého od jedné. Tento nejmenší dělitel však je prvočíslo, jak víme z důkazu věty 21. Stačí tedy číslo 149 dělit všemi prvočísly menšími než 149, ale i to je zbytečně mnoho. Uvidíme, že stačí se omezit jen na taková prvočísla, jejichž druhá mocnina je menší než 149. To jsou prvočísla: 2, 3, 5, 7, 11. Snadno se přesvědčíme, že číslo 149 není dělitelné žádným z nich. Z toho usoudíme, že 149 je prvočíslo, neboť platí

Věta 22. *Dané číslo a je prvočíslem, není-li dělitelné žádným prvočíslem p, které má tu vlastnost, že $p^2 \leqq a$, t. j. jehož druhá mocnina je menší než dané číslo nebo je mu nanejvýš rovna.*

Důkaz: Z důkazu věty 21 je patrno, že úloha rozložiti dané číslo a v součin prvočísel je totožná s úlohou nalézti nejmenšího dělitele daného čísla, který je různý od jedné. Tento dělitel p je prvočíslem. Platí-li $a = pb$, je druhý činitel b také dělitelem čísla a. Ježto p je nejmenší dělitel, je vždy $p \leqq b$, neboť b nemůže být menší než p. Násobíme-li tuto nerovnost kladným číslem p, dostaneme $p^2 \leqq pb$. Ale $pb = a$, takže $p^2 \leqq a$. Je-li číslo a složené, je tedy dělitelné aspoň jedním prvočíslem p, pro něž platí $p^2 \leqq a$. Neexistuje-li žádné prvočíslo této vlastnosti, je číslo a prvočíslem.

Odtud je vidno, že lze konečným počtem pokusů rozhodnout, je-li dané číslo prvočíslem; ovšem je-li to číslo dosti veliké, může býti

těchto pokusů veliké množství. Proto dosud není o mnohých velkých číslech známo, jsou-li prvočísly, či jsou-li čísly složenými.

Na větě 22 spočívá způsob, jak lze vyhledati všecka prvočísla menší než libovolné číslo. Napíšeme řadu všech čísel celých a kladných (bez čísla 1) a vynecháme v nich postupně násobky všech prvočísel. Číslo 2 ponecháme a vyškrtáme všecky jeho vyšší násobky. To, co zbude, jsou (vedle čísla 2) čísla, jež nejsou dělitelná dvěma. Prvé další zbylé číslo je číslo 3. To ponecháme a vyškrtáme všecky jeho vyšší násobky. Vedle čísel 2 a 3 zbudou čísla, jež nejsou dělitelná dvěma ani třemi. Nejmenší další číslo, které zbylo, je číslo 5. Vynecháme všecky jeho vyšší násobky a tak pokračujeme dále. Vždy první další zbylé číslo p je prvočíslo, neboť není dělitelné žádným číslem menším (mimo číslo 1). Lze však tvrditi ještě více: Také všecka nepřeškrtnutá čísla menší než p^2 jsou prvočísla, neboť nejsou dělitelná žádným prvočíslem menším než p (věta 22). Provedeme-li tento postup pro násobky čísel 2, 3, 5, obdržíme všecka prvočísla menší než $7^2 = 49$, t. j. prvočísla

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

Popsaný způsob vyhledávání prvočísel je známý pod jménem Eratosthenovo síto.*)

Snadno se přesvědčíme, že číslo 364 je dělitelné sedmi, neboť $364 = 7 \cdot 52$. Ale $364 = 4 \cdot 91$. Odtud můžeme usoudit, že alespoň jedno z čísel 4, 91 je dělitelné sedmi. A skutečně je $91 = 7 \cdot 13$.

Věta 23. *Je-li součin ab dvou činitelů a, b dělitelný prvočíslem p, je jím dělitelný aspoň jeden z činitelů a, b.*

Důkaz: Předpokládejme, že součin ab je dělitelný prvočíslem p. Jsou dvě možnosti:

1. Buď je číslo a dělitelné prvočíslem p. Pak je věta správná a nemáme co dokazovat.

2. Nebo číslo a není dělitelné prvočíslem p. Prvočíslo p má pouze dva dělitele: 1 a p. Ježto a není dělitelné prvočíslem p, mají čísla a a p jediného společného dělitele: jednotku. Jsou to tedy čísla navzájem

*) Eratosthenes byl řecký matematik z III. stol. př. Kr. V jeho dobách se psalo na voskové tabulky a místo přeškrtávání vynechaných čísel se do tabulky dělaly otvory; odtud název síto.

nesoudělná. Součin ab je dělitelný číslem p, které je s číslem a nesoudělné. Proto podle věty 21 číslo b je dělitelné číslem p. Věta je tedy správná i v tomto případě.

Větu 23 lze rozšířiti na libovolný počet činitelů:

VĚTA 24. *Je-li součin jakéhokoli počtu činitelů dělitelný prvočíslem p, je jím dělitelný aspoň jeden činitel.*

Důkaz: Budiž r nejmenší počet činitelů, o němž nevíme, zda pro něj naše tvrzení platí, a předpokládejme, že máme zjištěno, že platí pro každý počet činitelů, který je menší než r. Mějme součin $c_1c_2c_3 \dots c_r$, který obsahuje r činitelů $c_1, c_2, c_3, \dots, c_r$ a rozdělme tyto činitele ve dvě skupiny: do prvé skupiny zařadíme třeba prvních $k < r$ činitelů $c_1, c_2, c_3, \dots, c_k$ a jejich součin označíme a, t. j. $a = c_1c_2c_3 \dots c_k$. Do druhé skupiny pak zařadíme zbývajících $r - k$ činitelů c_{k+1}, $c_{k+2}, \dots, c_r$ a jejich součin označíme b, t. j. $b = c_{k+1}c_{k+2} \dots c_r$. V každé skupině je tedy méně činitelů než r a součin daných čísel lze napsati jako součin našich dvou činitelů a, b, t. j. $c_1c_2c_3 \dots c_r = ab$. Ten je podle předpokladu dělitelný prvočíslem p. Proto podle věty 23 musí prvočíslem p být dělitelný aspoň jeden činitel, t. j. buď číslo a nebo číslo b. Ale každé z čísel a, b má méně než r činitelů; je-li tedy číslo a dělitelné prvočíslem p, je jím dělitelný aspoň jeden z jeho činitelů $c_1, c_2, c_3, \dots, c_k$, a je-li číslo b dělitelné prvočíslem p, je jím dělitelný aspoň jeden ze zbývajících činitelů $c_{k+1}, c_{k+2}, \dots, c_r$. V každém případě je tedy aspoň jeden z činitelů $c_1, c_2, c_3, \dots, c_r$ dělitelný prvočíslem p. Platí-li tedy naše tvrzení pro každý menší počet činitelů než r, platí také pro r činitelů.

Ve větě 23 jsme dokázali, že vyslovené tvrzení platí pro dva činitele. Chceme zjistit, platí-li také pro tři. Poněvadž platí pro každý počet činitelů menší než tři, t. j. pro dva činitele, platí podle toho, co bylo právě dokázáno, i pro tři činitele. Z toho můžeme týmž postupem usoudit, že naše tvrzení platí také pro čtyři činitele, a tak lze pokračovati libovolně daleko. Tím je dokázáno, že věta 24 platí pro každý počet činitelů.

Nyní máme všechno připraveno, abychom dokázali, že platí

VĚTA 25. *Každé číslo lze rozložiti v součin prvočísel jen jedním způsobem.*

Důkaz: Dejme tomu, že by byl možný dvojí rozklad: jednak $a = p_1 p_2 p_3 \dots p_r$ a jednak $a = q_1 q_2 q_3 \dots q_s$, kde znaky $p_1, p_2, p_3, \dots, p_r$ znamenají prvočísla v počtu r, která nemusí být navzájem různá, a znaky $q_1, q_2, q_3, \dots, q_s$ znamenají jiná prvočísla v počtu s, která opět nemusí být navzájem různá. Musí ovšem platit

$$p_1 p_2 p_3 \dots p_r = q_1 q_2 q_3 \dots q_s, \qquad (*)$$

t. j. součin $p_1 p_2 p_3 \dots p_r$ musí být dělitelný číslem q_1. Podle věty 24 je to možné jen tak, že aspoň jedno z prvočísel $p_1, p_2, p_3, \dots, p_r$ je dělitelné prvočíslem q_1. Ale podle věty 20 každá dvě různá prvočísla jsou navzájem nesoudělná, proto některé z prvočísel $p_1, p_2, p_3, \dots, p_r$ se musí rovnat prvočíslu q_1. Dejme tomu, že je to třeba p_1, takže $p_1 = q_1$. Dělíme-li rovnici (*) tímto číslem, vyjde

$$p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

Odtud usoudíme, zcela stejně, že prvočíslo q_2 se musí rovnat některému z ostatních prvočísel $p_2, p_3, \dots, p_r$. Je-li to třeba p_2, musí platit $p_2 = q_2$. V postupu lze pokračovat tak dlouho, až všecka prvočísla z pravé strany rovnice (*) vyčerpáme. Každé prvočíslo z pravé strany musí tedy být rovno některému prvočíslu z levé strany; musí tedy na levé straně být všecka prvočísla, která jsou na pravé straně. Ale na levé straně jich více být nemůže, protože při dělení rovnice (*) všemi prvočísly z pravé strany zbude na pravé straně číslo 1. Musí tedy na levé straně vyjít také číslo 1, a proto není možné, aby na levé straně bylo více prvočísel než na pravé. Tím je dokázáno, že oba rozklady jsou totožné a mohou se lišiti nejvýše jen v pořadí činitelů, ale je známo, že hodnota součinu na pořadí činitelů nezávisí.

Věta 25 je vrcholem, k němuž směřovaly úvahy této knížky. Poznamenejme k ní ještě to, že není nikterak samozřejmá, ač se zdá zcela přirozená. Lze totiž snadno udati příklad, kdy věta o jednoznačnosti rozkladu čísla v součin prvočísel neplatí. Stačí v oboru celých kladných čísel vynechati jedno prvočíslo, třeba prvočíslo 2. V číselném oboru skládajícím se z čísel

$$1, 3, 4, 5, 6, 7, 8, 9, 10, \dots$$

lze bez omezení provádět sčítání a násobení, kterýchkoli čísel z tohoto oboru, při čemž dostaneme opět čísla z tohoto oboru. Při odčítání a

dělení dvou čísel z tohoto oboru vyjdou čísla z tohoto oboru jen za určitých omezení. Vedle omezení, jež platí v úplném oboru čísel celých a kladných, třeba se ještě vyvarovati odčítání a dělení, jejichž rozdílem, podílem nebo zbytkem by mělo být číslo 2, které v našem oboru neexistuje. Jinak tu lze provádět úvahy o dělitelnosti zcela obdobně, jako jsme je prováděli dříve. V tomto oboru jsou čísla 3, 4, 5, 6, 7, 8, 10, ... „prvočísly", neboť žádné z nich nemá jiného dělitele mimo jednotku a sama sebe (nesmíme zapomenout, že číslo 2 pro nás nyní neexistuje). Lehko zjistíme, že platí $3 \cdot 8 = 4 \cdot 6$; to značí, že součin $3 \cdot 8$ je dělitelný prvočíslem 4, ale žádný z jeho činitelů jím není dělitelný. Je to tedy obor, v němž neplatí věta 23 a také ne věta 25, neboť právě uvedené součiny jsou dva navzájem různé rozklady čísla 24 v součin prvočísel.

Bylo by tedy přirozené domnívati se, že v oboru všech čísel celých a kladných by mohl nastati podobný případ. To, že jsme dosud ještě nikdy při rozkladu žádného čísla dvojí rozklad nedostali, nemůžeme považovati za důkaz toho, že čísla s dvojím rozkladem neexistují, neboť je myslitelné, že by tento zjev mohl nastati u některého čísla neobvykle velikého, jehož rozklad v součin prvočísel dosud ještě nebyl proveden. Věta 25 však všecky naše pochybnosti předem vyvrací.

Cvičení:

75. Dokažte větu: Každé prvočíslo (s výjimkou prvočísla 2) je číslo liché. — [Jaký tvar mají čísla sudá?]

76. Dokažte větu: Číslo $n^2 - 1$ není prvočíslem pro žádné celé n větší než 2. — [Platí $n^2 - 1 = (n + 1)(n - 1)$.]

77. Je-li p prvočíslo větší než 3, je vždy jedno z čísel $p - 1$, $p + 1$ dělitelné šesti. Dokažte. — [Obě čísla jsou dělitelná dvěma a jedno z nich třemi.]

78. Je-li p prvočíslo větší než 3, je číslo $p^2 - 1$ dělitelné dvaceti čtyřmi. Dokažte. — [Viz cvič. 76 a 77.]

79. Kolik je čísel menších než 100, jež se dají vyjádřiti jako součin dvou prvočísel? — [Celkem 34 čísel.]

80. Rozložte v součin prvočísel čísla a) 648, b) 343; c) 1156, d) 2431. — [a) $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3$, b) $7 \cdot 7 \cdot 7$, c) $2 \cdot 2 \cdot 17 \cdot 17$, d) $11 \cdot 13 \cdot 17$.]

81. Kterými prvočísly je třeba dělit, abychom zjistili, jsou-li prvočísly čísla a) 331, b) 593; c) 997? Dokažte, že to jsou prvočísla. — [Prvočísly menšími než a) 19, b) 29, c) 37.]

82. Jak daleko třeba prováděti Eratosthenovo síto, chceme-li stanovit všecka prvočísla menší než a) 100, b) 1000, c) 10 000? — [Stačí vynechat všecky násobky prvočísel nejvýše rovných číslu a) 7, b) 31, c) 97.]

83. Jestliže číslo a lze rozložiti v součin dvou činitelů b, c, je druhá mocnina jednoho činitele nejvýše rovna a druhá mocnina druhého činitele aspoň rovna číslu a. Dokažte. — [Je-li $b \leqq c$, je $b^2 \leqq bc$, $bc \leqq c^2$.]

84. Je-li třetí mocnina nejmenšího prvočísla, jímž je složené číslo a dělitelné, větší než a, je číslo a součinem dvou prvočísel (různých nebo stejných). Dokažte. — [Kdyby bylo $a = pqr \ldots$, kde $p \leqq q \leqq r \leqq \ldots$ jsou prvočísla v počtu $k \geqq 3$, bylo by $p^3 \leqq p^k \leqq pqr \ldots = a$.]

85. Jsou-li a, b čísla navzájem nesoudělná, jsou i čísla $a + b$, ab navzájem nesoudělná. Dokažte. — [Kdyby bylo $a + b = pk$, $ab = ph$, kde p je prvočíslo, bylo by buď a (a proto i b) nebo b (a proto i a) dělitelné číslem p.]

86. Co lze říci o dvou číslech, jejichž nejmenší společný násobek je p-násobkem jejich největšího společného dělitele, při čemž p je prvočíslo? — [Podle věty 15 je $ab = D \,.\, pD$. Je-li $a = Dr$, $b = Ds$, je $rs = p$. Buď je $a = pb$ nebo je $b = pa$.]

87. Rozložíme-li některého dělitele čísla a v součin prvočísel, dostaneme jen taková prvočísla, jež se vyskytují v rozkladu čísla a v součin prvočísel. Dokažte. — [$a = bc$; každé prvočíslo z rozkladu čísla b musí být rovno některému prvočíslu z rozkladu čísla a.]

88. Jestliže žádné z prvočísel $p_1, p_2, \ldots, p_r$ není rovno některému z prvočísel $q_1, q_2, \ldots, q_s$, jsou čísla $a = p_1 p_2 \ldots p_r$ a $b = q_1 q_2 \ldots q_s$ navzájem nesoudělná. Dokažte. — [Kdyby byla navzájem soudělná, muselo by aspoň jedno z prvočísel $p_1, p_2, \ldots, p_r$ být rovno některému z prvočísel $q_1, q_2, \ldots, q_s$.]

89. Každé číslo větší než 1 a menší než 30, jež je s číslem 30 nesoudělné, je prvočíslem. Odůvodněte. — [Číslo nesoudělné s číslem 30 nesmí být dělitelné žádným z prvočísel 2, 3, 5. Ale všechna čísla menší než 30, jež nejsou dělitelná žádným z prvočísel 2, 3, 5, jsou prvočísla.]

90. Nalezněte všecka čísla a, která mají tuto vlastnost: každé číslo větší než 1 a menší než a, jež je s číslem a nesoudělné, je prvočíslo. — [Je-li p prvočíslo, pak a musí být složeno ze všech prvočísel menších než p tak, aby $a < p^2$. Pro $p = 3$ je $a = 4$ nebo 8; pro $p = 5$ je $a = 6$ nebo 12 nebo 18 nebo 24; pro $p = 7$ je $a = 30$.]