I. Dělitelnost, prvočísla

In: Karel Rychlík (author): Úvod do elementární teorie číselné. (Czech). Praha: Jednota čs. matematiků a fysiků, 1931. pp. 7–29.

Persistent URL: http://dml.cz/dmlcz/402938

I. Dělitelnost, prvočísla.

§ 1. Číslo racionální a je dělitelno racionálním číslem b, jestliže $a = bc$, kdež c je číslo celé. Pak se říká též, že b je dělitelem a neb, že b je obsaženo v a nebo konečně, že a je násobkem b. Pro $b \neq 0$ je patrně a dělitelno b, jestliže a/b je číslo celé.

0 má za dělitele všechna čísla racionální, za násobek jen samu sebe.

Číslo racionální celé je dělitelno ± 1. A také opak platí. Lze dokonce vysloviti větu: Je-li číslo racionální dělitelno číslem celým, je i samo celé.

Dále platí věty:

Každé číslo racionální je dělitelno samo sebou.

Je-li a dělitelno b, $a \neq 0$, $b \neq 0$, je $1/b$ dělitelno $1/a$.

Je-li a dělitelno b, b dělitelno c, je a dělitelno c.

Jsou-li racionální čísla a, b dělitelna racionálním číslem d, je i $a \pm b$ dělitelno d.

Je-li a dělitelno d a m číslo celé, je am dělitelno d.

Z obou posledních vět plyne ihned věta obecnější:

Jsou-li racionální čísla $a_1, a_2, \ldots, a_k$ dělitelna racionálním číslem d a $m_1, m_2, \ldots, m_k$ racionální čísla celá, je i $a_1m_1 + a_2m_2 + \ldots + a_km_k$ dělitelno d.

Konečně platí věta:

Jen čísla ± 1 mají tu vlastnost, že jsou sama i jejich převratné hodnoty celé. Odtud plyne dále: Je-li racionální číslo a dělitelno racionálním číslem b a naopak b dělitelno a, pak jest $a = \pm b$.

§ 2. Budiž x libovolné číslo reální. Uvažujme čísla celá $\leqq x$. Mezi nimi je jisté největší. Označme je $[x]$, takže $[x] \leqq x$, při čemž případ rovnosti může nastati, jen když x je číslo celé.*) $[x]+1$ je již $> x$. I platí o $[x]$:

$$[x] \leqq x < [x] + 1.$$

*) Označení toto pochází od Gausse. Též se užívá označení Legendreova $E(x)$.

Těmi podmínkami je číslo celé $[x]$ jednoznačně určeno. Kdyby existovala dvě celá čísla $n_1, n_2, n_1 \neq n_2$, splňující vztahy

$$n_1 \leqq x < n_1 + 1$$
$$n_2 \leqq x < n_2 + 1,$$

mohli bychom předpokládati, že $n_1 < n_2$, tedy $n_1 + 1 \leq n_2$. Bylo by pak $x < n_1 + 1 \leqq n_2$, tedy $x < x$, což není možné.

Jsou-li x, y čísla reální, je

$$[x] + [y] \leqq [x + y].$$

Je totiž

$$[x] \leqq x, \qquad [y] \leqq y, \qquad x + y < [x + y] + 1,$$

tedy $$[x] + [y] \leqq x + y < [x + y] + 1$$

a, ježto $[x]$, $[y]$ a $[x + y]$ jsou celá čísla, $[x] + [y] \leqq [x + y]$.

Odtud plyne ihned úplnou indukcí pro čísla reální

$$[x_1] + [x_2] + \ldots + [x_n] \leqq [x_1 + x_2 + \ldots + x_n]$$

a pro $$x_1 = x_2 = \ldots = x_n = x$$

$$n\,[x] \leqq [nx].$$

Dále platí věta:

Je-li x číslo reální a k kladné celé, je $\left[\frac{[x]}{k}\right] = \left[\frac{x}{k}\right]$.

Je totiž $$x = [x] + \vartheta, \quad 0 \leqq \vartheta < 1.$$

Dlužno tedy dokázati, že

$$\left[\frac{[x]}{k}\right] = \left[\frac{[x] + \vartheta}{k}\right].$$

To nastane, neexistuje-li žádné číslo celé y hovící nerovnostem

$$\frac{[x]}{k} < y \leqq \frac{[x] + \vartheta}{k}.$$

A takové číslo celé skutečně neexistuje, ježto by pak bylo

$$\frac{[x]}{k} < y < \frac{[x] + 1}{k},$$

t. j. $$[x] < ky < [x] + 1,$$

což je nemožné.

Největší číslo celé $< x$ označíme $[x]'$. I bude $[x]' < x \leqq [x]' + 1$. Není-li x celé, je $[x]' = [x]$, pro x celé je $[x]' = [x] - 1$.

Položme $\{x\} = [x + \frac{1}{2}]$. I bude platiti $[x + \frac{1}{2}] \leqq x + \frac{1}{2} < [x + \frac{1}{2}] + 1$, t. j. $\{x\} - \frac{1}{2} \leqq x < \{x\} + \frac{1}{2}$, takže bude $|\{x\} - x| \leqq \frac{1}{2}$. Jedině v případě, že $x + \frac{1}{2}$ je číslo celé, je $\{x\} = x + \frac{1}{2}$. Jinak bude $\{x\} - \frac{1}{2} < x < \{x\} + \frac{1}{2}$, t. j. $|\{x\} - x| < \frac{1}{2}$.

Buďtež nyní a, b racionální čísla celá, $b > 0$. Položme $\left[\frac{a}{b}\right] = q$, $\frac{a}{b} - q = \frac{r}{b}$. I bude $r = a - qb$ číslo celé a bude platiti $q \leqq \frac{a}{b} < q + 1$, t. j. $0 \leqq r < b$. Lze tedy vždy klásti $a = qb + r$, kdež q, r jsou čísla celá, a platí $0 \leqq r < b$. Případ $r = 0$ nastane, jen když je a dělitelno b. r nazveme nejmenším zbytkem kladným při dělení a číslem b, q je příslušný „částečný podíl".

Podobně položme $\left\{\frac{a}{b}\right\} = q'$, $\frac{a}{b} - q' = \frac{r'}{b}$. $r' = a - q'b$ bude celé číslo. Ježto $q' - \frac{1}{2} \leqq a/b < q' + \frac{1}{2}$, bude o r' platiti $-\frac{1}{2}b \leqq r' < \frac{1}{2}b$. Lze tedy klásti $a = q'b + r'$, kdež q', r' jsou čísla celá a platí $-\frac{1}{2}b \leqq r' < \frac{1}{2}b$, při čemž rovnost nastane, jen když $r' = -\frac{1}{2}b$ je číslo celé. r' se nazývá absolutně nejmenší zbytek při dělení čísla a číslem b, q' pak je příslušný „částečný podíl".

Budiž nyní g celé číslo > 1, x nechť je celé číslo $\geqq 0$. Dokážeme, že *lze x znázorniti ve tvaru* $x = a_0 g^k + a_1 g^{k-1} + \ldots + a_k$, *kde k je číslo celé* $\geqq 0$, *a_i jsou čísla celá hovící nerovnostem*

$$0 \leqq a_i < g, \qquad i = 0, 1, 2, \ldots, k.$$

Tomuto znázornění říká se znázornění čísla x v soustavě g-adické, a_i jsou g-adické číslice, g nazývá se basí soustavy.

Budeme též psáti

$$x = a_0\, a_1\, a_2 \ldots a_k.$$

Pro $g = 10$ máme znázornění čísla v soustavě desítkové (dekadické).

Lze vždy určiti celé číslo kladné k tak, že

$$\frac{x}{g^{k+1}} < 1,^*) \quad \text{t. j.} \quad \left[\frac{x}{g^{k+1}}\right] = 0.$$

---

*) Je důsledkem té okolnosti, že $\lim_{n\to\infty} \frac{x}{g^n} = 0$. Bez užití pojmu limity lze to dokázati, užijeme-li pomocné věty, která slouží k důkazu, že $\lim_{n\to\infty} g^n = \infty$:

Pro $a > 0$ totiž platí, jak lze snadno dokázati úplnou indukcí (neb jak plyne ihned z binomické poučky) $(1 + a)^n > 1 + na$,

Položme

$$\left[\frac{x}{g^k}\right] = a_0.$$

Pak

$$\left[\frac{a_0}{g}\right] = \left[\frac{\left[\frac{x}{g^k}\right]}{g}\right] = \left[\frac{x}{g^{k+1}}\right] = 0,$$

tedy

$$0 \leqq \frac{a_0}{g} < 1, \text{ t. j. } 0 \leqq a_0 < g.$$

Klaďme

$$x - a_0 g^k = x_1;$$

i bude

$$\frac{x_1}{g^k} = \frac{x}{g^k} - a_0 = \frac{x}{g^k} - \left[\frac{x}{g^k}\right], \text{ t. j. } 0 \leqq \frac{x_1}{g^k} < 1, \left[\frac{x_1}{g^k}\right] = 0.$$

Označme $\left[\frac{x_1}{g^{k-1}}\right] = a_1$, i bude $\left[\frac{a_1}{g}\right] = \left[\frac{\left[\frac{x_1}{g^{k-1}}\right]}{g}\right] = \left[\frac{x_1}{g^k}\right] = 0,$

tedy $0 \leqq a_1 < g$.

Postupujme podobně dále. Klaďme

$$x_{i-1} - a_{i-1} g^{k+1-i} = x_i, \left[\frac{x_i}{g^{k-i}}\right] = a_i, \; i = 1, 2, 3, \ldots, \; x_0 = x.$$

Dokážeme, že bude $\left[\frac{x_i}{g^{k+1-i}}\right] = 0$. Je totiž

$$\frac{x_i}{g^{k+1-i}} = \frac{x_{i-1}}{g^{k+1-i}} - a_{i-1} = \frac{x_{i-1}}{g^{k+1-i}} - \left[\frac{x_{i-1}}{g^{k+1-i}}\right],$$

tedy číslo $\geqq 0$ a < 1, takže je skutečně $\left[\frac{x_i}{g^{k+1-i}}\right] = 0$.

Dále bude

$$\left[\frac{a_i}{g}\right] = \left[\frac{\left[\frac{x_i}{g^{k-i}}\right]}{g}\right] = \left[\frac{x_i}{g^{k+1-i}}\right] = 0$$

---

n číslo celé kladné, t. j. $g^n > 1 + n(g-1)$. Zvolíme-li tedy k tak, aby $1 + (k+1)(g-1) > x$, t. j. $k > \frac{x-1}{g-1} - 1 = \frac{x-g}{g-1}$, bude $g^{k+1} > x$, neboli $\frac{x}{g^{k+1}} < 1$.

a tedy

$$0 \leqq \frac{a_i}{g} < 1, \text{ t. j. } 0 \leqq a_i < g.$$

I bude

$$a_k = [x_k] = x_k,$$

ježto x_k je celé. Dále

$$x_{k+1} = x_k - a_k = 0 \text{ a } x_i = 0 \text{ pro } i > k.$$

Je tedy

$$\begin{aligned} x - a_0 g^k &= x_1 \\ x_1 - a_1 g^{k-1} &= x_2 \\ &\ldots\ldots\ldots\ldots \\ x_k &= a_k \end{aligned}$$

a sečtením dostaneme

$$x = a_0 g^k + a_1 g^{k-1} + \ldots + a_k.$$

Tak dostali jsme jedno znázornění v soustavě g-adické. Je-li x kladné, je možno beze všeho předpokládati, že $a_0 \neq 0$. *V tomto případě je znázornění to možné jen jediným způsobem, t. j. je-li též*

$$x = a'_0 g^{k'} + a'_1 g^{k'-1} + \ldots + a'_{k'},$$

kdež k' je číslo celé $\geqq 0$ a a'_i jsou čísla celá, o nichž platí $0 \leqq a'_i < g$, je $k = k'$, $a_i = a'_i$ pro $i = 0, 1, 2, \ldots, k$.

Kdyby to nebylo pravda, dostali bychom odečtením

$$0 = b_0 g^l + b_1 g^{l-1} + \ldots + b_l,$$

kdež $b_0, b_1, \ldots, b_l$ jsou čísla celá, $b_0 \neq 0$, $-g < b_i < g$ pro $i = 1, 2, \ldots, l$.

Bylo by tedy

$$g^l \leqq |b_0 g^l| = |b_l + b_{l-1} g + \ldots + b_1 g^{l-1}| \leqq (g-1)(1 + g + \ldots + g^{l-1}),$$

t. j.

$$g^l \leqq g^l - 1,$$

což není možné.

§ 3. Nazveme modul I množství čísel racionálních, které má tyto vlastnosti:

1. Patří-li do I čísla a, b, patří tam i $a \pm b$.*)

2. Existuje číslo racionální celé g (o němž lze beze všeho

*) Místo 1. lze předpokládati, že platí pouze

1′. Patří-li a, b do I, patří tam i $a - b$. Pak patří do I i $0 = a - a$; patří-li pak b do I, patří tam i $-b = 0 - b$. Patří-li konečně do I čísla a i b, patří tam i $a + b = a - (-b)$.

předpokládati, že je > 0) té vlastnosti, že ag je celé pro každé číslo a z I.

Podmínka 2. je jistě splněna, jsou-li všechna čísla z I celá.

Jako příklad modulu uveďme souhrn všech čísel celých.

0 je patrně prvkem každého modulu a tvoří sama o sobě modul, který označíme 0.

Je-li a libovolný prvek z modulu I a c pevné číslo racionální, tvoří čísla ac zase modul. Označíme jej cI. Modul gI má za prvky patrně čísla celá.

Je ihned patrno, že, patří-li a do I, patří tam i všechny násobky a.

Je-li totiž a číslo z I a víme-li, že do I patří na, kdež n je číslo racionální celé > 0, bude tam patřiti i $na + a = (n + 1)a$. Na základě úplné indukce je tedy v I zároveň s a i na pro n celé kladné. Je-li pak a v I, je tam i $-a$, 0 je pak v I samozřejmě, čímž důkaz proveden.

Uveďme důležitý případ modulu. Budiž $L = L(x_1, x_2, \ldots, x_k) = a_1x_1 + a_2x_2 + \ldots + a_kx_k$ lineární homogenní funkce s racionálními koeficienty $a_1, a_2, \ldots, a_k$. Probíhají-li proměnné $x_1, x_2, \ldots, x_k$ všechna čísla racionální celá, tvoří hodnoty této funkce množství číselné, které je modulem.

Je-li totiž

$$a = L(x'_1, x'_2, \ldots, x'_k),\ b = L(x''_1, x''_2, \ldots, x''_k),$$

je

$$a \pm b = L(x'_1 \pm x''_2,\ x'_2 \pm x''_2, \ldots, x'_k \pm x''_k),$$

takže je splněna vlastnost 1.

Racionální čísla $a_1, a_2, \ldots, a_k$ lze psáti ve tvaru

$$a_1 = \frac{a'_1}{g},\quad a_2 = \frac{a'_2}{g}, \ldots, a_k = \frac{a'_k}{g},$$

kdež $a'_1, a'_2, \ldots, a'_k, g$ jsou čísla racionální celá, $g > 0$. Racionální číslo a_i lze totiž vždy znázorniti ve tvaru $a_i = r_i/s_i$, kdež r_i, s_i jsou celá čísla, $s_i \neq 0$. Ježto je též $a_i = -r_i/-s_i$, je možno vždy docíliti, aby bylo $s_i > 0$. Za g možno pak třeba zvoliti součin $s_1s_2s_3 \ldots s_k$. $gL(x_1, x_2, \ldots, x_k)$ je pak číslo racionální celé, ať jsou $x_1, x_2, \ldots, x_k$ jakákoliv čísla celá, takže i vlastnost 2. je splněna.

Modul právě uvažovaný nazveme modulem k-členným a označíme jej $I(a_1, a_2, \ldots, a_k)$.

Násobky libovolného čísla racionálního d tvoří modul jednočlenný, $I(d)$.

Skládají-li se dva moduly z týchž čísel racionálních, řekneme

o nich, že jsou si rovny. Dva moduly jednočlenné $I(d)$, $I(d')$ budou si rovny, $I(d) = I(d')$, bude-li $d = \pm d'$, t. j. $|d| = |d'|$. Pak totiž každý násobek d bude i násobkem d' a naopak, jak plyne z konce § 1.

O modulech platí věta:

Každý modul I možno znázorniti jako modul jednočlenný, t. j. existuje číslo racionální d té vlastnosti, že I pozůstává z násobků jeho, tedy $I = I(d)$. d je určeno pomocí I až na znaménko; je též $I = I(-d)$.

V triviálním případě, kdy I pozůstává pouze z čísla 0, je věta samozřejmá. Předpokládejme tedy, že v I jsou čísla $\neq 0$.

Mezi kladnými čísly z I je číslo nejmenší. Jsou-li všechna čísla z I celá, je existence tohoto čísla patrná. V obecném případě stačí uvažovati modul gI (g dáno podmínkou 2.), jehož čísla jsou celá, takže mezi nimi je jistě jisté nejmenší d'. $d = d'/g$ je pak nejmenší z kladných čísel z I.

Snadno lze pak dokázati, že každé číslo z I je dělitelno d. Kdyby totiž číslo a z I nebylo dělitelno d, takže by a/d nebylo celé, platilo by pro $\left[\frac{a}{d}\right]$

$$\left[\frac{a}{d}\right] < \frac{a}{d} < \left[\frac{a}{d}\right] + 1,$$

tedy pro číslo $b = a - d\left[\frac{a}{d}\right]$ by platilo podle § 2 str. 9

$$0 < b < d. \tag{1}$$

Avšak b je číslo z I, ježto a i d jsou čísla z I a $\left[\frac{a}{d}\right]$ je číslo celé. Podle (1) by pak d nebylo nejmenší kladné číslo z I. Je tedy $I = I(d)$. Z $I = I(d')$ by plynulo $I(d) = I(d')$, tedy $d = \pm d'$.

§ 4. Budeme se nyní zabývati úlohou, určiti společné dělitele čísel racionálních $a_1, a_2, \ldots, a_k$.

Je-li m společný dělitel čísel $a_1, a_2, \ldots, a_k$, je také číslo tvaru $a_1x_1 + a_2x_2 + \ldots + a_kx_k$, kdež $x_1, x_2, \ldots, x_k$ jsou racionální čísla celá, dělitelno m, t. j. každé číslo modulu $I = I(a_1, a_2, \ldots, a_k)$ je m dělitelno. Avšak podle předešlého § $I = I(d)$, takže společní dělitelé čísel $a_1, a_2, \ldots, a_k$ jsou děliteli čísel modulu $I(d)$, t. j. děliteli čísla d. Nejsou-li všechna čísla $a_1, a_2, \ldots, a_k = 0$, je $d \neq 0$, takže pro společného dělitele m čísel $a_1, a_2, \ldots, a_k$ platí $|m| \leqq |d|$. Má tedy d mezi společnými děliteli čísel $a_1, a_2, \ldots, a_k$ největší abso-

lutní hodnotu. Z toho důvodu nazveme d největším společným dělitelem (n. s. d., největší společnou mírou) čísel $a_1, a_2, \ldots, a_k$.

Největší společný dělitel jest určen pouze svou absolutní hodnotou, ježto je $I(d) = I(-d) = I(|d|)$.

Označíme $|d| = (a_1, a_2, \ldots, a_k)$.

Je patrně $(a_1, a_2, \ldots, a_k)=0$ tehdy a jen tehdy, když $a_1 = a_2 = \ldots = a_k = 0$.

Máme tedy větu:

Jsou-li $a_1, a_2, \ldots, a_k$ čísla racionální, existuje číslo racionální d, jejich největší společný dělitel (n. s. d.), těchto vlastností:

1. *d je společný dělitel čísel $a_1, a_2, \ldots, a_k$;*
2. *každý společný dělitel čísel $a_1, a_2, \ldots, a_k$ je dělitelem d.*

Vlastnostmi 1. a 2. je absolutní hodnota n. s. d. určena jednoznačně. Má-li totiž též d' vlastnosti ty, pak d' jako společný dělitel čísel $a_1, a_2, \ldots, a_k$ musí býti dělitelno d a též naopak, d musí býti dělitelno d', tedy podle konce § 1 $d' = \pm d$, $|d'| = |d|$.

Ježto je d číslo z $I(a_1, a_2, \ldots, a_k)$, lze d znázorniti ve tvaru $d = a_1m_1 + a_2m_2 + \ldots + a_km_k$, při čemž $m_1, \ldots, m_k$ jsou čísla celá.

$d=0$, jen když je $a_1=a_2=\ldots=a_k=0$. Nejsou-li všechna tato čísla rovna 0, je $|d|$ nejmenší kladné číslo z modulu $I(a_1, a_2, \ldots, a_k)$; $|d|$ je největší ze společných dělitelů čísel $a_1, a_2, \ldots, a_k$.

Čísla, jejichž n. s. d. je ± 1, nazveme nesoudělná. Ježto taková čísla musí býti dělitelna ± 1, jsou podle § 1 str. 7 celá. I lze pak určiti čísla celá $m_1, m_2, \ldots, m_k$, takže platí $a_1m_1 + a_2m_2 + \ldots + a_km_k = +1$ nebo -1. Platí-li obráceně tato rovnice pro celá čísla $a_1, a_2, \ldots, a_k$, jsou tato čísla zřejmě nesoudělná.

Z té vlastností, že $I(a_1, a_2, \ldots, a_k) = I(d)$, plyne ihned věta:

Rovnici $a_1x_1 + a_2x_2 + \ldots + a_kx_k = c$, kdež $a_1, a_2, \ldots, a_k$, c jsou čísla racionální, lze řešiti celými hodnotami $x_1, x_2, \ldots, x_k$ tehdy a jen tehdy, jestliže c je dělitelno n. s. d. čísel $a_1, a_2, \ldots, a_k$. Jsou-li čísla $a_1, a_2, \ldots, a_k$ nesoudělná, lze rovnici tu řešiti celými čísly $x_1, x_2, \ldots, x_k$ tehdy a jen tehdy, když c je číslo celé.

§ 5. Uveďme některé vlastnosti n. s. d.

1. $(a_1, a_2, \ldots, a_k) = (|a_1|, |a_2|, \ldots, |a_k|)$.
2. $(a, a, \ldots, a) = |a|$.
3. $(a, 0) = |a|$, $(a_1, a_2, \ldots, a_k, 0) = (a_1, a_2, \ldots, a_k)$.
4. $(a, m) = |m|$, je-li a násobek m, a obecněji

$(a_1, a_2, \ldots a_k, m) = |m|$, jsou-li $a_1, a_2, \ldots, a_k$ násobky m.

5. $(a, 1) = 1$, je-li a celé; $(a_1, a_2, \ldots, a_k, 1) = 1$, jsou-li $a_1, a_2, \ldots, a_k$ celá.

6. $(ma_1, ma_2, \ldots, ma_k) = |m| (a_1, a_2, \ldots, a_k)$.

Odtud plyne, je-li $(a_1, a_2, \ldots, a_k) = |d| \neq 0$ a zvolíme-li $m = 1/d$, věta:

Čísla racionální $a_1, a_2, \ldots, a_k$ mají n. s. d. $d \neq 0$ tehdy a jen tehdy, jsou-li čísla $a_1/d, a_2/d, \ldots, a_k/d$ nesoudělná.

Důkaz vlastností 1.—6. je zcela jednoduchý, uvažujeme-li příslušné moduly. Stejně lze dokázati komutativní zákon pro operaci, vyznačenou závorkou ( ):

7. $(a, b) = (b, a)$.

Dále platí zákon asociativní

8. $((a, b), c) = (a, (b, c)) = (a, b, c)$.

Z 6. a 8. plyne obecněji

9. $(a_1, a_2, \ldots, a_k)\,(b_1, b_2, \ldots, b_l) =$
$= (a_1b_1, a_2b_1, \ldots a_kb_1, a_1b_2, a_2b_2, \ldots a_kb_2, \ldots a_1b_l, a_2b_l, \ldots a_kb_l)$.

Konečně lze snadno dokázati větu, která nám bude sloužiti při výpočtu n. s. d.:

$$(a_1, a_2, \ldots . a_k) = (a'_1, a_2, \ldots, a_k), \text{ kdež } a'_1 = a_1 + ma_2$$

a m je číslo celé.

Je totiž $a_1 = a'_1 - ma_2$, takže $I(a_1, a_2, \ldots, a_k) = I(a'_1, a_2, \ldots \ldots, a_k)$, tedy i

$$(a_1, a_2, \ldots, a_k) = (a'_1, a_2, \ldots, a_k).$$

§ 6. Výpočet n. s. d. čísel racionálních lze převésti na výpočet n. s. d. čísel celých. Lze totiž vždy vyjádřiti $a_1, a_2, \ldots, a_k$ ve tvaru

$$a_1 = \frac{a'_1}{g}, \quad a_2 = \frac{a'_2}{g}, \ldots, a_k = \frac{a'_k}{g},$$

kdež $a'_1, a'_2, \ldots, a'_k, g$ jsou čísla celá a $g > 0$, jak bylo podotčeno v § 3. Pak je podle 6.

$$(a_1, a_2, \ldots, a_k) = \frac{(a'_1, a'_2, \ldots, a'_k)}{g}.$$

Na základě asociativního zákona lze pak převésti počítání n. s. d. více čísel na počítání n. s. d. dvou čísel. Bude se tedy konečně jednati o výpočet (a_1, a_2), kdež a_1, a_2 jsou čísla celá kladná, a $a_1 > a_2$. K výpočtu (a_1, a_2) lze užíti tak zvaného Euklidova algoritmu. (Základy, 10. kniha, III, Servítův překlad str. 161.) Dělme a_1 číslem a_2. Budiž při tom a_3 nejmenší kladný zbytek a q_1 částečný podíl, takže je

$$a_1 = a_2 q_1 + a_3, \qquad (1)$$

kdež q_1, a_3 jsou čísla celá a $0 \leqq a_3 < a_2$. Z věty uvedené na konci předešlého paragrafu pak plyne $(a_1, a_2) = (a_2, a_3)$. Obecně, je-li $a_{k+1} > 0$, dělme a_k číslem a_{k+1}. Nejmenší kladný zbytek při tom nechť jest a_{k+2}, částečný podíl q_k, takže $a_k = a_{k+1} q_k + a_{k+2}$, $0 \leqq a_{k+2} < a_{k+1}$. a_k jsou pro $k \geqq 1$ čísla celá $\geqq 0$ stále klesající. Takových je jen konečný počet. Nechť je na př. $a_{l+2} = 0$.

Ježto je $(a_1, a_2) = (a_2, a_3) = \ldots = (a_{l+1}, a_{l+2}) = (a_{l+1}, 0) = a_{l+1}$, je poslední nemizící zbytek a_{l+1} hledaným n. s. d. čísel a_1, a_2. Je-li tento zbytek 1, jsou čísla a_1, a_2 nesoudělná.

Určení n. s. d. více čísel lze vždy převésti na případ určení n. s. d. čísel celých kladných mezi sebou různých $a_1 < a_2 < a_3 < \ldots < a_k$. Je-li a_1 společným dělitelem čísel $a_2, a_3, \ldots, a_k$, je a_1 hledaným n. s. d. (Viz § 5, větu 4.) Není-li tomu tak, dělme $a_2, a_3, \ldots, a_k$ číslem a_1. Nejmenší kladné zbytky při tom označme $a'_2, a'_3, \ldots, a'_k$. Vyskytuje-li se 0 mezi čísly $a_1, a'_2, \ldots, a'_k$, vynechme ji, z čísel sobě rovných vezměme každé jen jednou a uspořádejme podle velikosti. Tak dostaneme čísla $b_1 < b_2 < \ldots < b_l = a_1$, $l \leqq k$. I bude podle věty na konci § 5 $(a_1, a_2, \ldots, a_k) = (b_1, b_2, \ldots, b_l)$. S $b_1, b_2, \ldots, b_l$ naložme podobně. Je patrno, že postup ten po konečném počtu kroků skončí a povede k určení n. s. d. čísel $a_1, a_2, \ldots, a_k$.

Jak v tomto obecnějším případě, tak při Euklidově algoritmu bylo by možno bráti místo nejmenších zbytků kladných absolutně nejmenší zbytky.

§ 7. Uvedeme nyní několik vět o číslech spolu nesoudělných.

1. *Je-li a číslo racionální celé, m, b čísla racionální nesoudělná (tedy též celá), pak je*

$$(am, b) = (a, b).$$

Položme $d = (a, b)$, $\bar{d} = (am, b)$. a, b tedy i am, b mají společného dělitele d; je tedy $\bar{d}$ násobkem d. Z nesoudělnosti m, b plyne, že lze určiti čísla celá k, l tak, že je $mk + bl = 1$. (§ 4 str. 14) Bude tedy $a = amk + bla$, t. j. $d = (a, b) = (amk + bla, b) = (amk, b)$. am, b tedy i amk, b mají společného dělitele $\bar{d}$. Je tedy též d násobkem $\bar{d}$, takže skutečně $d = \bar{d}$, j. b. d.

Ve speciálním případě, kdy $(a, b) = 1$, $(m, b) = 1$, dostaneme větu:

2. *Jsou-li a, m nesoudělná s b, je také jejich součin nesoudělný s b.*

A odtud plyne obecněji (úplnou indukcí):

3. *Je-li každé z čísel* $a_1, a_2, \ldots, a_k$ *nesoudělné s* b, *je i jejich součin* $a_1 a_2 \ldots a_k$ *nesoudělný s* b.

4. *Je-li každé z čísel* $a_1, a_2, \ldots, a_k$ *nesoudělné s každým z čísel* $b_1, b_2, \ldots, b_l$, *jsou též součiny* $a_1 a_2 \ldots a_k$, $b_1 b_2 \ldots b_l$ *spolu nesoudělné.*

5. *Je-li* a *nesoudělné s* b, *je i* a^k *nesoudělné s* b^l (k, l *čísla celá* $\geqq 0$).

6. *Je-li* c *číslo celé,* a, b *čísla nesoudělná a* ac *dělitelno* b, *pak je* c *dělitelno* b.

Ježto a, b jsou nesoudělná, lze určiti čísla celá k, l taková, že $ak + bl = 1$; pak je $c = ack + bcl = b\left(\frac{ac}{b}k + cl\right)$; ac/b je však celé, z čehož tvrzení ihned vyplývá.

Konečně platí věta:

7. *Je-li* a' *celý dělitel čísla* a *a jsou-li* a, b *nesoudělná, jsou i* a', b *nesoudělná.*

Zase lze určiti celá čísla k, l taková, že platí $ak + bl = 1$. Avšak $a = a'c$, kdež c je celé, takže je též $a'ck + bl = 1$, z čehož plyne ihned (podle § 4) tvrzení.

§ 8. Každé číslo racionální lze znázorniti ve tvaru a_1/a_2, kdež a_1, a_2 jsou čísla celá, $a_2 \neq 0$. Je-li d n. s. d. čísel a_1, a_2, bude $a_1 = da'$, $a_2 = da''$, takže $a = a'/a''$ a a', a'' jsou čísla celá nesoudělná, $a'' \neq 0$. Lze tedy každé číslo racionální znázorniti zlomkem, jehož čitatel a jmenovatel jsou čísla nesoudělná. Takový zlomek nazývá se **redukovaný**. Ježto pak $a = a'/a'' = -a'/-a''$, $a'' \neq 0$, lze o jmenovateli předpokládati, že je kladný.

Lze snadno nahlédnouti, že rovnost dvou redukovaných zlomků a'/a'', b'/b'' vyžaduje, buď aby $a' = b'$, $a'' = b''$ neb $a' = -b'$, $a'' = -b''$, takže znázornění racionálního čísla redukovaným zlomkem o kladném jmenovateli je jednoznačné.

Redukovaný zlomek znázorňuje číslo celé, jen když jmenovatel je ± 1. Z toho plyne ihned věta:

m-tá odmocnina z čísla celého a kladného (m *číslo celé kladné*) *není nikdy číslo racionální necelé; je vždy buď zase číslo celé nebo číslo iracionální.*

Nechť je $\sqrt[m]{a} = a'/b'$, kdež a'/b' je zlomek redukovaný. Pak $a = a'^m/b'^m$, kteryžto zlomek je zase redukovaný (podle § 7 věty 5). Z toho ihned plyne $b'^m = \pm 1$, tedy $b' = \pm 1$, jak bylo tvrzeno.

Redukovaný zlomek a'/a'' je dělitelný redukovaným zlomkem b'/b'', jestliže a' je dělitelno b' a b'' dělitelno a''.

Má-li býti a'/a'' dělitelno b'/b'', musí býti $a'b''$ dělitelno $a''b'$, tedy $a'b''$ dělitelno a'' i b'. Ježto pak b', b'' jsou nesoudělná, musí býti (podle § 7, vlastnosti 6.) a' dělitelno b'. Podobně z nesoudělnosti a' a a'' plyne, že b'' je dělitelno a''.

§ 9. Buďtež $a_1, a_2, \ldots, a_k$ racionální čísla různá od nuly. Uvažujme jejich společné násobky. Dokážeme, že mezi nimi je takový, n, že každý jiný společný násobek m je jím dělitelný. $|n|$ je určeno jednoznačně, má pak mezi kladnými násobky čísel $a_1, a_2, \ldots, a_k$ nejmenší hodnotu. Proto nazývá se n nejmenší společný násobek čísel $a_1, a_2, \ldots, a_k$. Zavedeme označení $|n| = [a_1, a_2, \ldots, a_k]$. I platí

$$[a_1, a_2, \ldots, a_k] = \frac{1}{\left(\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}\right)}.$$

$\left(\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}\right)$ jako n. s. d. čísel $\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}$ je obsažen ve všech číslech $\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}$. Je tedy $\frac{1}{a_i\left(\frac{1}{a_1}, \ldots, \frac{1}{a_k}\right)}$ $(i = 1, 2, \ldots, k)$ číslo celé, t. j. $\frac{1}{\left(\frac{1}{a_1}, \ldots, \frac{1}{a_k}\right)}$ je dělitelno a_i, takže $\frac{1}{\left(\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}\right)}$ je společný násobek čísel $a_1, a_2, \ldots, a_k$. Předpokládejme dále, že $m \neq 0$ je společný násobek čísel $a_1, a_2, \ldots, a_k$. Pak je $\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}$ dělitelno $\frac{1}{m}$, tedy též $\left(\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}\right)$ dělitelno $\frac{1}{m}$, t. j. m dělitelno $\frac{1}{\left(\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}\right)}$. Je tedy $\frac{1}{\left(\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_k}\right)}$ skutečně společný násobek čísel $a_1, a_2, \ldots, a_k$ té vlastnosti, že každý společný násobek čísel těch je jím dělitelný. Takové číslo je však určeno jednoznačně až na znamení. Kdyby totiž též n' mělo tu vlastnost, bylo by n dělitelno n' a též n' dělitelno n, tedy $n' = \pm n$, t. j. $|n'| = |n|$.

Snadno lze dokázati, že platí

$$[a, b] = \frac{1}{\left(\frac{1}{a}, \frac{1}{b}\right)} = \frac{|ab|}{(a, b)}.$$

Jest totiž podle § 5, 6.

$$\left(\frac{1}{a}, \frac{1}{b}\right) = \frac{1}{|ab|}(a, b).$$

Položíme-li $M = a_1 a_2 \ldots a_k$, $A_i = \frac{M}{a_i}$, $i = 1, 2, \ldots, k$, bude

$$\frac{1}{a_i} = \frac{A_i}{M}, \quad \frac{1}{\left(\frac{A_1}{M}, \frac{A_2}{M}, \ldots, \frac{A_k}{M}\right)} = \frac{1}{\frac{1}{M}(A_1, A_2, \ldots, A_k)} =$$

$$= \frac{M}{(A_1, A_2, \ldots, A_k)}.$$

Odtud plyne

$$[a_1, a_2, \ldots, a_k] = \frac{M}{(A_1, A_2, \ldots, A_k)}.$$

Jsou-li a, b nesoudělná, je $(a, b) = 1$, tedy $[a, b] = |ab|$.

Jsou-li každá dvě z čísel $a_1, a_2, \ldots, a_k$ nesoudělná, platí $[a_1, a_2, \ldots, a_k] = |a_1 a_2 \ldots a_k|$. Důkaz lze provésti úplnou indukcí na základě věty předešlé.

Pro n. s. n. platí podobné věty jako pro n. s. d. Při tom [ ] se vztahuje na racionální čísla $\neq 0$.

1. $[a_1, a_2, \ldots, a_k] = [|a_1|, |a_2|, \ldots, |a_k|]$.
2. $[a, a, \ldots, a] = |a|$.
3. $[a, m] = |m|$, je-li m dělitelno a a obecněji,

$$[a_1, a_2, \ldots, a_k, m] = |m|,$$

je-li m dělitelno čísly $a_1, a_2, \ldots, a_k$.

4. $[a, 1] = |a|$, je-li a celé.
5. $[ma_1, ma_2, \ldots, ma_k] = |m|\,[a_1, a_2, \ldots, a_k]$.
6. $[a, b] = [b, a]$.
7. $[[a, b], c] = [a, [b, c]] = [a, b, c]$.

Konečně platí vzorec, který dostaneme ze vzorce 9 § 5, nahradíme-li závorky ( ) závorkami [ ].

§ 10. Čísla ± 1 mají jediné celé dělitele $+1$ a -1. Číslo racionální celé $a \neq 1$ a $\neq -1$ má samozřejmě celé dělitele $\pm a$, ± 1. Jestliže číslo celé $p > 1$, nemá jiných dělitelů celých než

$\pm p, \pm 1$, nazývá se prvočíslo. Taková čísla existují, na př. 2, 3, 5, . . .

Je ihned patrno, že číslo racionální celé a, jehož absolutní hodnota je >1 a které není prvočíslem, lze znázorniti ve tvaru $a=bc$, kdež b a c jsou čísla celá $\neq \pm 1$.

Snadno lze dokázati, že *počet prvočísel není konečný*. Důkaz tvrzení tohoto je již v Euklidových Základech (9. kniha; XX, Servítův překlad str. 149).

Dejme tomu, že prvočísel by byl jen konečný počet 2, 3, 5, . . . , p, takže by p bylo největší existující prvočíslo. Číslo $P_p = 2 \cdot 3 \cdot 5 \ldots p + 1$ dává při dělení prvočísly 2, 3, 5, . . ., p zbytek 1, není tedy žádným z nich dělitelno. Je tedy P_p buď samo prvočíslo nebo je dělitelno prvočíslem $> p$.

$P_2 = 3$, $P_3 = 7$, $P_5 = 11$, $P_7 = 211$, $P_{11} = 2311$ jsou prvočísla, naproti tomu je $P_{13} = 59 \cdot 509$, $P_{17} = 19 \cdot 97 \cdot 277$.

Tento Euklidův důkaz mimo to nám poskytuje konečné intervaly, v nichž musí ležeti aspoň jedno prvočíslo. Plyne z něho: Je-li p libovolné prvočíslo (> 0), leží v intervalu od $p + 1$ do $2 \cdot 3 \cdot 5 \ldots p + 1$ (inkl.) aspoň jedno prvočíslo, t. j. existuje prvočíslo q takové, že $p + 1 < q \leqq 2 \cdot 3 \cdot 5 \ldots p + 1$.

Na druhé straně lze snadno udati intervaly libovolně velké, v nichž neleží žádné prvočíslo.

Je-li n celé číslo $\geqq 2$, není z $n - 1$ po sobě jdoucích čísel

$$n! + 2,\ n! + 3,\ n! + 4, \ldots, n! + n$$

žádné prvočíslem, ježto pro každé $k = 2, 3, \ldots, n$ je $n! + k$ dělitelno k.

Podobně jako Euklid dokázal, že existuje nekonečně mnoho prvočísel, lze dokázati:

Existuje nekonečně mnoho prvočísel tvaru $4n - 1$ (n celé > 0).

K tomu stačí uvažovati čísla $4(3 \cdot 7 \cdot 11 \ldots p) - 1$.

Existuje nekonečně mnoho prvočísel tvaru $6n - 1$ (n celé > 0).

Zde třeba uvažovati čísla $6(5 \cdot 11 \cdot 17 \cdot 23 \ldots p) - 1$.

Dirichlet (Werke, I, 307—312, 313—342) pomocí metod analytické teorie číselné dokázal větu:

V aritmetické posloupnosti $a + bn$, kdež a, b jsou čísla celá nesoudělná a n probíhá čísla celá, je nekonečně mnoho prvočísel.

O této otázce viz Landau, Handbuch I, 432—435, kdež podán důkaz věty Dirichletovy v zjednodušeném tvaru.

§ 11. Dříve než přistoupím k důkazu věty o znázornění čísel racionálních pomocí prvočísel, uvedeme si několik vět pomocných.

Je-li a celé číslo nedělitelné prvočíslem p, jsou čísla a a p nesoudělná. Je-li pak q též prvočíslo $\neq p$, jsou p, q nesoudělná.

O prvočísle p platí dále věta: Součin dvou čísel celých ab je dělitelný prvočíslem p jen tehdy, je-li aspoň jeden z činitelů prvočíslem p dělitelný.

Důkaz plyne snadno z 2. věty § 7. Není-li na př. a dělitelno p, jsou čísla a a p nesoudělná. Kdyby ani b nebylo p dělitelno, bylo by i b nesoudělné s p, tedy i ab nesoudělné s p, proti předpokladu. Odtud tedy plyne, že b je dělitelno p.

Platí však též věta: Číslo celé kladné $p \neq 0$ a $+1$ je prvočíslem, jestliže z předpokladu, že součin ab dvou čísel racionálních celých a, b je dělitelný p, a však není dělitelno p, plyne, že b je dělitelno p.

Kdyby p nebylo prvočíslo, bylo by $p = ab$, kdež a a b jsou celá čísla > 1; a ani b by nebylo dělitelno p, ač jejich součin $ab = p$ by byl p dělitelný.

Z věty 4. § 7 plyne ihned:

Jsou-li $p_1, p_2, \ldots, p_k$, $q_1, q_2, \ldots, q_l$ prvočísla vesměs mezi sebou různá, jsou čísla $p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$ a $q_1^{n_1} q_2^{n_2} \ldots q_l^{n_l}$, kdež $m_1, m_2, \ldots, m_k$, $n_1, n_2, \ldots, n_l$ značí čísla celá $\geqq 0$, nesoudělná.

Z toho plyne dále, že zlomek $\dfrac{p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}}{q_1^{n_1} q_2^{n_2} \ldots q_l^{n_l}}$ je redukovaný (§ 8, str. 17). Může pak výraz ten představovati celé číslo, jen když jmenovatel $= 1$, což nastane jen při $n_1 = n_2 = \ldots = n_l = 0$. Výraz ten může býti $= 1$, jen když čitatel i jmenovatel bude $= 1$, t. j. při $m_1 = m_2 = \ldots = m_k = n_1 = n_2 = \ldots = n_l = 0$.

I můžeme vysloviti větu:

Výraz $p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, *kdež* $n_1, n_2, \ldots, n_k$ jsou *čísla celá, představuje číslo celé, jen když* $n_1, n_2, \ldots, n_k$ *jsou čísla celá* $\geqq 0$. *Výraz ten je roven* 1, *jen když* $n_1 = n_2 = \ldots = n_k = 0$.

§ 12. Uvažujme celé číslo $a > 1$. To je jistě dělitelno aspoň jedním kladným prvočíslem, ježto nejmenší dělitel čísla a, celý a > 1, jakožto číslo mající za celé kladné dělitele jen 1 a samo sebe, je jistě prvočíslem. Klademe-li $a = p_1 a_1$, kdež p_1 je prvočíslo, a je-li $a_1 > 1$, zase $a_1 = p_2 a_2$, kdež p_2 je zase prvočíslo, atd., musíme po konečném počtu kroků, ježto $a_1, a_2, a_3, \ldots$ jsou racionální čísla celá kladná stále klesající, přijíti k případu $a_k = 1$. Tak je a znázorněno jako součin prvočísel $p_1 p_2 \ldots p_k$. Píšeme-li součiny sobě rovných prvočísel ve tvaru mocniny, vidíme, že možno každé číslo celé > 1 znázorniti ve tvaru $a = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$,

kdež prvočísla $p_1, p_2, \ldots, p_r$ jsou mezi sebou různá a mocnitelé $a_1, a_2, \ldots, a_r$ čísla celá kladná.

Budiž nyní $p_1, p_2, \ldots$ množství všech mezi sebou různých prvočísel (v pořádku libovolném).

Ježto číslo racionální kladné a lze znázorniti jako podíl dvou čísel celých kladných, dostaneme pro číslo takové znázornění

$$a = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}, \tag{1}$$

kdež r je číslo celé kladné a mocnitelé $a_1, a_2, \ldots, a_r$ jsou čísla celá. Znázornění toto je jednoznačné v tom smyslu, že, je-li též

$$a = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r}, \tag{2}$$

platí $a_1 = b_1$, $a_2 = b_2, \ldots, a_r = b_r$. (Máme-li součiny $q_1^{c_1} q_2^{c_2} \ldots q_s^{c_s}$ $r_1^{d_1} r_2^{d_2} \ldots r_t^{d_t}$, kdež $q_1, q_2, \ldots, q_s$, $r_1, r_2, \ldots, r_t$ jsou prvočísla a $c_1, c_2, \ldots, c_s$, $d_1, d_2, \ldots, d_t$ čísla celá, lze tyto součiny psáti ve tvaru (1) a (2), připustíme-li mocnitele 0 u těch prvočísel, které se nevyskytují v jednom součinu a vyskytují v druhém.)

Důkaz je zcela jednoduchý. Z (1) a (2) plyne

$$p_1^{a_1 - b_1} p_2^{a_2 - b_2} \ldots p_r^{a_r - b_r} = 1,$$

kterážto rovnice nemůže býti podle § 11 jinak splněna, než když je $a_1 - b_1 = a_2 - b_2 = \ldots = a_r - b_r = 0$, t. j. $a_1 = b_1$, $a_2 = b_2, \ldots, a_r = b_r$.

Libovolné číslo racionální $a \neq 0$ *lze pak znázorniti ve tvaru* $a = \pm 1 \cdot p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, kdež $p_1, p_2, \ldots, p_r$ jsou prvočísla mezi sebou různá a $a_1, a_2, \ldots, a_r$ jsou čísla celá.

Říká se, že a obsahuje p_k právě v mocnině a_k, a je-li a celé, že a je dělitelno právě $p_k^{a_k}$ (a je dělitelno p_k^n pro $n \leqq a_k$, není však dělitelno p_k^n pro $n > a_k$).

Je-li $a_k \neq 0$, nazveme p_k prvočinitelem čísla a.

§ 13. Máme-li dána dvě čísla racionální kladná $a = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r}$, při čemž $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_r$ jsou čísla celá, bude a dělitelno b, bude-li $a_1 \geqq b_1$, $a_2 \geqq b_2, \ldots, a_r \geqq b_r$.

Konečný počet čísel racionálních kladných $a, b, \ldots, c$ lze znázorniti ve tvaru

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} \\ b &= p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r} \\ &\ldots\ldots\ldots\ldots \\ c &= p_1^{c_1} p_2^{c_2} \ldots p_r^{c_r}, \end{aligned}$$

při čemž $a_i, b_i, \ldots, c_i$ $(i = 1, 2, \ldots, r)$ jsou čísla celá a r jest ve všech výrazech totéž celé číslo kladné. (Viz poznámku v § 12) Pak lze největší společnou míru a nejmenší společný násobek čísel těch zcela snadno vyjádřiti.

Je totiž $(a, b, \ldots, c) = p_1^{d_1} p_2^{d_2} \ldots p_r^{d_r}$, $[a, b, \ldots, c] = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$, kdež $d_i = \min(a_i, b_i, \ldots c_i)$, $n_i = \max(a_i, b_i, \ldots, c_i)$.*)

Dokažme to pro $(a, b, \ldots, c)$.

Kladní společní dělitelé čísel $a, b, \ldots, c$ jsou čísla m tvaru

$$m = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r} p_{r+1}^{m_{r+1}} \ldots p_s^{m_s},$$

kdež $m_1, m_2, \ldots, m_s$ jsou celá čísla hovící podmínkám

$$m_i \leqq a_i,\ m_i \leqq b_i, \ldots, m_i \leqq c_i \ (i = 1, 2, \ldots, r) \tag{1}$$

$$m_{r+1} \leqq 0, \ldots, m_s \leqq 0. \tag{2}$$

Podmínky (1) lze nahraditi podmínkami

$$m_i \leqq d_i.$$

Největšího společného kladného dělitele dostaneme pro

$$m_i = d_i,\ i = 1, 2, \ldots, r;\quad m_j = 0,\ j = r+1,\ r+2, \ldots, s.$$

Je tedy d skutečně n. s. d.

§ 14. Konečným počtem pokusů lze vždy rozhodnouti, zda dané číslo celé kladné a je prvočíslem. Číslo a nebude totiž prvočíslem, je-li dělitelno některým z čísel $2, 3, \ldots, a - 1$. Stačí však zkoušeti dělitelnost pro čísla celá > 1 a $\leqq \sqrt{a}$. Je-li totiž d celý dělitel čísla a, > 1 a $< a$, tedy $a = dd'$, kdež celá čísla kladná d, d' jsou > 1, lze beze všeho předpokládati $d \leqq d'$, neboť bychom v opačném případě mohli spolu d a d' zaměniti; z $d \leqq d'$ plyne však $a = dd' \geqq d^2$, tedy $d \leqq \sqrt{a}$. Bude-li $d \leqq [\sqrt{a}]$, bude též $d \leqq \sqrt{a}$, ježto $[\sqrt{a}] \leqq \sqrt{a}$. Nemá-li a žádného dělitele mezi čísly celými $\geqq 2$ a $\leqq [\sqrt{a}]$, je prvočíslem. Při tom stačí však zkoumati pouze dělitelnost prvočísly, takže lze vysloviti větu: *Číslo celé kladné a je prvočíslem, není-li dělitelno žádným prvočíslem $\leqq [\sqrt{a}]$.*

Na tom založen jest postup, jak z přirozené řady čísel 1, 2, 3, 4,... vyloučiti všechna prvočísla. Je to tak zvané síto Eratostenovo.

Metoda pozůstává v tom, že postupně vynecháme všechny násobky určitého prvočísla. Začneme tak, že vynecháme všechna čísla sudá, t. j. škrtneme každé druhé. První číslo, které nám zbude, je prvočíslo 3. I škrtneme každé číslo dělitelné 3. První číslo, které nám v řadě číselné zbude, je prvočíslo 5. Nyní vyškrtne-

*) Jsou-li $a_1, a_2, \ldots, a_k$ čísla reálná, je $m = \min(a_1, a_2, \ldots, a_k)$ nejmenší z čísel $a_1, a_2, \ldots, a_k$ a $M = \max(a_1, a_2, \ldots, a_k)$ největší z čísel $a_1, a_2, \ldots, a_k$. Na př. $\min(-3, 0, -3) = -3$, $\max(-3, 0, -3) = 0$.

me každé číslo dělitelné 5, atd. Je-li po několika krocích p první číslo přirozené řady číselné, které zůstalo nepřeškrtnuto, je p prvočíslo. Vyškrtáme-li nyní násobky p, tedy každé číslo p-té, budou čísla q hovící vztahu $p \leq q < p^2$ prvočísly. Chceme-li určiti všechna prvočísla $\leq x$, kdež x je libovolné číslo reální kladné, stačí z přirozené řady číselné vyloučiti násobky všech prvočísel $\leq [\sqrt{x}]$. Tak kdybychom chtěli určiti prvočísla kladná ≤ 30, stačí vyškrtati násobky 2, 3, 5, ježto $[\sqrt{30}] = 5$, a zbudou nám další prvočísla 7, 11, 13, 17, 19, 23, 29.

Existují tabulky udávající, zda dané číslo celé kladné je prvočíslo. Největší tištěné tabulky toho druhu jsou od Lehmera (Factor table for the first ten millions) udávající nejmenšího kladného celého dělitele každého čísla nedělitelného 2, 3, 5, 7 mezi 0 a 10 017 000. (Washington 1909.)

Největší rukopisné tabulky jsou však Kulikovy (Jakub Filip Kulik, 1773—1863, prof. matematiky na praž. universitě). chované v knihovně vídeňské akademie, udávající nejmenšího kladného celého dělitele každého čísla nedělitelného 2, 3, 5 v prvních sto milionech. Podle mínění Lehmerova, který jich užil při své práci, by se k publikaci nehodily, ježto obsahují dosti chyb, ač ovšem by při publikaci dalších tabulek mohly úkol značně usnadniti.

Malé tabulky prvočísel jsou:

Luigi Poletti, Tavole di Numeri Primi, Manuali Hoepli, Milán 1920, obsahující prvočísla mezi 1 a 200000, rozklad prvních 50000 čísel celých kladných a jiné podobné tabulky.

§ 15. Budiž a číslo celé $\neq 0$. Nechť je $|a| = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, kdež $p_1, p_2, \ldots, p_k$ jsou různá prvočísla a $a_1, a_2, \ldots, a_k$ čísla celá ≥ 0. Číslo celé kladné d bude dělitelem a, lze-li je psáti ve tvaru $d = p_1^{d_1} p_2^{d_2} \ldots p_k^{d_k}$, kdež pro čísla celá $d_1, d_2, \ldots, d_k$ platí nerovnosti $0 \leq d_1 \leq a_1, 0 \leq d_2 \leq a_2, \ldots, 0 \leq d_r \leq a_r$. Z toho plyne, že každý člen součinu

$$(1 + p_1 + p_1^2 + \ldots + p_1^{a_1})(1 + p_2 + p_2^2 + \ldots + p_2^{a_2}) \ldots \\ \ldots (1 + p_k + p_k^2 + \ldots + p_k^{a_k})$$

bude celým kladným dělitelem čísla a a naopak všechny celé kladné dělitele čísla a lze takto obdržeti. Počet dělitelů celých kladných čísla a, $\sigma_0(a)$, je tedy roven počtu členů tohoto součinu, t. j.

$$\sigma_0(a) = (a_1 + 1)(a_2 + 1) \ldots (a_k + 1).$$

Součet celých kladných dělitelů čísla a, $\sigma_1(a)$, je roven onomu součinu, t. j.

$$\sigma_1(a) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

Snadno lze také určiti součet r-tých mocnin celých kladných dělitelů čísla a, $\sigma_r(a)$ (r celé číslo kladné). Tento součet je roven součinu

$$(1 + p_1^r + p_1^{2r} + \ldots + p_1^{a_1 r})(1 + p_2^r + p_2^{2r} + \ldots + p_2^{a_2 r}) \ldots \\ \ldots (1 + p_r^r + p_r^{2r} + \ldots + p_r^{a_r r}),$$

takže

$$\sigma_r(a) = \frac{p_1^{(a_1+1)r} - 1}{p_1^r - 1} \cdot \frac{p_2^{(a_2+1)r} - 1}{p_2^r - 1} \cdots \frac{p_k^{(a_k+1)r} - 1}{p_k^r - 1}.$$

Snadno lze nahlédnouti, že $\sigma_r(PQ) = \sigma_r(P)\,\sigma_r(Q)$, jsou-li P, Q čísla celá nesoudělná $\neq 0$, $r \geqq 0$.

§ 16. Pro $a = 2^{n-1}(2^n - 1)$ (n číslo celé kladné) bychom za předpokladu, že $2^n - 1$ je prvočíslo, našli

$$\sigma_1(a) = \frac{2^n - 1}{2 - 1} \cdot \frac{(2^n - 1)^2 - 1}{(2^n - 1) - 1} = 2^n(2^n - 1) = 2a.$$

Číslo a právě uvedené je tak zvané číslo dokonalé (perfektní). Tak nazývají se čísla, pro něž platí $\sigma_1(a) = 2a$, $\sigma_1(a) - a = a$, t. j. jež rovnají se součtu svých dělitelů celých kladných menších než dané číslo samo. Čísla dokonalá lichá nejsou známa (také však nebyl proveden důkaz, že neexistují).

Ukažme, že není jiných čísel dokonalých sudých mimo čísla tvaru $2^{n-1}(2^n - 1)$, kdež n je číslo celé kladné, $2^n - 1$ prvočíslo (čísla dokonalá Euklidova typu, Základy, 9. kniha, XXXVI, Servítův překlad str. 154).

Nechť číslo $a = 2^n q$ je dokonalé (n číslo celé kladné, q číslo liché > 0).

Pak je $\sigma_1(a) = \sigma_1(2^n)\,\sigma_1(q) = (2^{n+1} - 1)\,s$, označíme-li $\sigma_1(q) = s$. Z dokonalosti čísla a plyne $\sigma_1(a) = 2a$, t. j. $(2^{n+1} - 1)\,s = 2^{n+1}q$, tedy $s = \frac{2^{n+1}q}{2^{n+1} - 1} = q + \frac{q}{2^{n+1} - 1}$, neboli $s = q + d$, kdež $d = \frac{q}{2^{n+1} - 1}$. Číslo d je tedy celým kladným dělitelem čísla q; ježto pak $s = q + d$ a s značí součet celých kladných dělitelů čísla q, má q za dělitele celé kladné pouze q a d. To není jinak

možno, než když $d = 1$ a $q = 2^{n+1} - 1$ je prvočíslo. Pak skutečně $a = 2^n (2^{n+1} - 1)$.

Má-li býti $2^n - 1$ prvočíslo, musí býti n prvočíslo. $2^{pq} - 1$ jest totiž dělitelno $2^p - 1$ i $2^q - 1$. Tato podmínka je nutná, nikoliv však dostačující. $2^n - 1$ je prvočíslo pro tyto hodnoty n:

$$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127.$$

Naproti tomu

$$2^{23} - 1 = 47 \cdot 178481.$$

Viz Kraitschik, *1* I. 9, 218; *2* 19.

Platí-li pro čísla celá kladná a, b

$$\sigma_1(a) = \sigma_1(b) = a + b,$$

nazývají se čísla ta spřátelená. Pak je patrně $\sigma_1(a) - a = b$, $\sigma_1(b) - b = a$. Takovými čísly jsou na př. $a = 220$, $b = 284$.

§ 17. Každému celému děliteli d čísla celého kladného a odpovídá dělitel celý kladný a/d, tak zvaný **dělitel komplementární**. Uvažujme všechny celé kladné dělitele čísla celého kladného a, seřazené třeba podle velikosti $d_1 = 1, d_2, d_3, \ldots, d_\nu = a$, kdež $\nu = \sigma_0(a)$. Pak dělitelé komplementární $a/d_1 = a, a/d_2, a/d_3, \ldots, a/d_\nu = 1$ dávají řadu předešlou, psanou v obráceném pořádku. Označme P součin celých kladných dělitelů čísla a. I bude

$$P = d_1 d_2 \ldots d_\nu$$

a též

$$P = \frac{a}{d_1} \cdot \frac{a}{d_2} \cdots \frac{a}{d_\nu}$$

Bude tedy $P^2 = a^\nu$, a tudíž $P = a^{\frac{1}{2}\nu}$, $\nu = \sigma_0(a)$.

Lze snadno nahlédnouti, že ν je sudé vyjímaje případ, kdy a je úplný čtverec, t. j. kdy a je čtvercem čísla celého. Dělitelé celí kladní čísla a se rozpadají na dvojice dělitelů spolu komplementárních, vyjímaje případ, kdy existuje dělitel rovný svému děliteli komplementárnímu, což nastane patrně, jen když a je úplný čtverec.

§ 18. Budeme hledati rozklad $[x]!$ $(x > 0)$ v prvočinitele.

Předpokládejme nejprve x celé. V $x!$ mohou se vyskytovati jen kladní prvočinitelé $p \leqq x$. Je otázka, v jaké mocnině se p vyskytuje. Počet násobků p z řady $1, 2, 3, \ldots, x$ je $\left[\frac{x}{p}\right]$, podobně počet násobků p^2 je $\left[\frac{x}{p^2}\right]$, počet násobků p^3 je $\left[\frac{x}{p^3}\right]$ atd. Kdyby

součin $x!$ neobsahoval žádného činitele dělitelného p^2, obsahovalo by $x!$ prvočinitele p právě $\left[\frac{x}{p}\right]$-krát. Vyskytují-li se však také členy dělitelné p^2, přidává každý z nich k $\left[\frac{x}{p}\right]$ jeden nový činitel p. Bude tedy počet činitelů pocházejících od členů dělitelných p a p^2 roven $\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right]$. Stejně poskytne každý člen součinu dělitelný p^3 k uvedeným dalšího činitele p, takže členy řady $1, 2, 3, \ldots, x$ dělitelné p, p^2, p^3 dávají v $x!$ p na mocninu $\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \left[\frac{x}{p^3}\right]$. Tak můžeme pokračovati. Bude tedy $x!$ dělitelno p právě v mocnině

$$\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \left[\frac{x}{p^3}\right] + \ldots$$

Řada ta sama se ukončí, ježto je $\frac{x}{p^m} \geqq 1$ jen pro $m \leqq \frac{\log x}{\log p}$; pro $\frac{x}{p^m} < 1$, tedy $m > \frac{\log x}{\log p}$, je $\left[\frac{x}{p^m}\right] = 0$. Je tudíž

$$x! = \prod_{p \leqq x} p^{\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \left[\frac{x}{p^3}\right] + \ldots},$$

kdež součin se vztahuje na prvočísla $\leqq x$.

Jest však pro každé reální $x > 0$ $[x]! = \prod_{p \leqq x} p^{\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \ldots}$.

Důkaz bude snadno plynouti z věty pomocné z § 2: Je-li x kladné číslo reální a k kladné číslo celé, je

$$\left[\frac{[x]}{k}\right] = \left[\frac{x}{k}\right].$$

Podle předešlého je

$$[x]! = \prod_{p \leqq [x]} p^{\left[\frac{[x]}{p}\right] + \left[\frac{[x]}{p^2}\right] + \left[\frac{[x]}{p^3}\right] + \ldots}.$$

Podle oné věty pomocné však $\left[\frac{[x]}{p^m}\right] = \left[\frac{x}{p^m}\right]$. Dále množství prvočísel, hovících nerovnosti $p \leqq [x]$, je totožné s množstvím prvočísel hovících nerovnosti $p \leqq x$. Z toho pak vyplývá ihned tvrzení.

Je-li x číslo celé $\geqq 0$, lze je znázorniti v soustavě p-adické ve tvaru

$$x = a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k,$$

kdež k je číslo celé $\geqq 0$, a_i jsou p-adické číslice, t. j. čísla celá splňující nerovnosti: $0 \leqq a_i < p$; $i = 1, 2, 3, \ldots, k$. (Viz § 2 str. 9).

Pak je

$$\left[\frac{x}{p}\right] = a_1 + a_2 p + a_3 p^2 + \ldots + a_k p^{k-1}$$

$$\left[\frac{x}{p^2}\right] = a_2 + a_3 p + \ldots + a_k p^{k-2},$$

$$\left[\frac{x}{p^k}\right] = a_k$$

$$\left[\frac{x}{p^{k+1}}\right] = \left[\frac{x}{p^{k+2}}\right] = \ldots = 0$$

$$\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \ldots = a_1 + a_2(1 + p) + a_3(1 + p + p^2) + \ldots$$

$$\ldots + a_k(1 + p + p^2 + \ldots + p^{k-1})$$

$$= a_1 \frac{p-1}{p-1} + a_2 \frac{p^2-1}{p-1} + a_3 \frac{p^3-1}{p-1} + \ldots$$

$$\ldots + a_k \frac{p^k - 1}{p-1}$$

$$= \frac{x - (a_0 + a_1 + a_2 + \ldots + a_k)}{p-1}.$$

Pro $p = 2$ bude $\left[\frac{x}{2}\right] + \left[\frac{x}{2^2}\right] + \ldots = x - h$. h udává, kolik je mezi číslicemi $a_0, a_1, a_2, \ldots, a_k$ jedniček.

Dokažme si větu:

Jsou-li $n_1, n_2, \ldots, n_k$ čísla celá kladná hovící podmínce $n = n_1 + n_2 + \ldots + n_k$, pak je $n_0!/n_1!n_2! \ldots n_k!$ číslo celé.

Budiž p libovolné prvočíslo. $n!$ obsahuje p právě v mocniteli

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots = \left[\frac{n_1 + n_2 + \ldots + n_k}{p}\right] +$$

$$+ \left[\frac{n_1 + n_2 + \ldots + n_k}{p^2}\right] + \ldots$$

Součin $n_1!\, n_2! \ldots n_k!$ obsahuje pak p právě v mocniteli

$$\left[\frac{n_1}{p}\right]+\left[\frac{n_1}{p^2}\right]+\ldots+\left[\frac{n_2}{p}\right]+\left[\frac{n_2}{p^2}\right]+\ldots+\ldots+\left[\frac{n_k}{p}\right]+\left[\frac{n_k}{p^2}\right]+\ldots$$

Jest však podle § 2 str. 8

$$\left[\frac{n_1+n_2+\ldots+n_k}{p}\right] \geqq \left[\frac{n_1}{p}\right]+\left[\frac{n_2}{p}\right]+\ldots+\left[\frac{n_k}{p}\right]$$

$$\left[\frac{n_1+n_2+\ldots+n_k}{p^2}\right] \geqq \left[\frac{n_1}{p^2}\right]+\left[\frac{n_2}{p^2}\right]+\ldots+\left[\frac{n_k}{p^2}\right]$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

z čehož tvrzení ihned plyne. $n!/n_1!n_2!\ldots n_k!$ je počet permutací n prvků, z nichž je resp. $n_1, n_2, \ldots, n_k$ stejných. Je to koeficient u $x_1^{n_1}x_2^{n_2}\ldots x_k^{n_k}$ v rozvoji $(x_1+x_2+\ldots,+x_k)^n$. Ve speciálním případě je tak dokázána celost binomického koeficientu

$$\binom{n}{n_1}=\binom{n}{n_2}=\frac{n!}{n_1!\, n_2!},\quad n=n_1+n_2.$$