KAREL RYCHLÍK:

SBÍRKA SPISŮ VYDÁVANÁ JEDNOTOU ČESKOSLOVENSKÝCH MATEMATIKŮ A FYSIKŮ

ÚVOD DO ELEMENTÁRNÍ TEORIE ČÍSELNÉ

KRUH

sv. 7.

Kč 22·—

K R U H

SBÍRKA SPISŮ VYDÁVANÁ

JEDNOTOU ČS. MATEMATIKŮ A FYSIKŮ

za redakce B. Bydžovského, V. Posejpala a M. Valoucha

Svazek 7

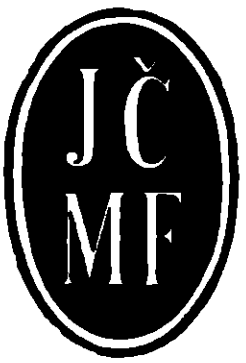
Karel Rychlík:

ÚVOD DO ELEMENTÁRNÍ TEORIE ČÍSELNÉ

ÚVOD DO ELEMENTÁRNÍ TEORIE ČÍSELNÉ

Napsal

Dr. KAREL RYCHLÍK,
profesor vysokého učení technického v Praze



TISKEM A NÁKLADEM

JEDNOTY ČS. MATEMATIKŮ A FYSIKŮ

V PRAZE 1931

ÚVOD.

V úvodu do elementární teorie číselné, který veřejnosti předkládám, vykládám v prvé části pojem dělitelnosti pro čísla racionální a pojem prvočísla, v druhé části kongruence pro čísla celá racionální, řešení lineárních kongruencí o jedné neznámé a lineárních rovnic neurčitých, větu Fermatovu a Wilsonovu, konečně pak pojem primitivních kořenů. V třetí části pojednávám o g-adických zlomcích s užitím na zlomky desetinné, v části čtvrté o kvadratických zbytcích (v oboru čísel racionálních), zákonu reciprocity, uvádím pak některé věty o znázornění čísel speciálními formami kvadratickými a způsob, jak pomocí této nauky zjistiti, zda dané číslo je celé prvočíslem. V části páté se jedná o větě Fermatově (dokázáné Lagrangem), že každé číslo celé kladné je možno znázorniti jako součet nanejvýš čtyř čtverců celých čísel. Konečně v části šesté pojednávám o trojúhelnících Pytagorových, o velké větě Fermatově pro mocnitele čtyři a o trojúhelnicích racionálních.

Předběžné vědomosti, kterých je k studiu předloženého spisku zapotřebí, jsou velmi malé, takže i studující nejvyšších tříd škol středních budou jej moci s prospěchem čísti.

Je mi milou povinností poděkovati panu Dru V. Kořínkovi, asistentu matematického ústavu na vysoké škole strojního a elektrotechnického inženýrství, který četl korektury, sestavil abecední seznam a na několika místech přispěl ke zpřesnění výkladu. Děkuji též Jednotě čsl. matematiků a fysiků, jejímž nákladem kniha vychází a jejíž tiskárna věnovala úpravě knihy velkou péči.

K. Rychlík.

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

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

II. Kongruence.

§ 19. Budiž m číslo racionální celé. Je-li číslo racionální celé a dělitelno m, řekneme také, že a je kongruentní s 0 (mod m) (modulo m, podle modulu m), $a \equiv 0 \pmod{m}$. Je-li též b číslo racionální celé, značí $a \equiv b \pmod{m}$, že $a - b \equiv 0 \pmod{m}$.

Pro $m=0$ přejde kongruence v rovnost.

Je patrno, že kongruence $a \equiv b \pmod{m}$ je splněna tehdy a jen tehdy, platí-li $a \equiv b \pmod{-m}$. Lze tedy též tvrditi, že kongruence $a \equiv b \pmod{m}$ platí tehdy a jen tehdy, platí-li $a \equiv b \pmod{m}$. Bylo by tedy beze všeho možno předpokládati, že $m \geqq 0$, a pro kongruence, které se neredukují na rovnosti, dokonce, že m je celé číslo kladné.

Z definice ihned plyne, že, je-li $a \equiv b \pmod{m}$ a d dělitel čísla m, je též $a \equiv b \pmod{d}$.

Čísla celá a, b nechť jsou spolu kongruentní podle modulů $m_1, m_2, \ldots, m_k$ ($m_1, m_2, \ldots, m_k$ čísla celá $\neq 0$). Pak je též $a \equiv b \pmod{n}$, kdež n je nejmenší společný násobek $m_1, m_2, \ldots, m_k$. Neboť $a - b$, ježto je násobkem každého z čísel $m_1, m_2, \ldots, m_k$, jest též násobkem n. Jsou-li ve speciálním případě $m_1, m_2, \ldots, m_k$ čísla celá po dvou nesoudělná, pak je $a \equiv b \pmod{m_1 m_2 \ldots m_k}$, ježto $n = m_1 m_2 \ldots m_k$. A také opak platí, takže lze vysloviti větu:

Jsou-li $m_1, m_2, \ldots, m_k$ čísla celá po dvou nesoudělná, platí $a \equiv b \pmod{n}$, $n = m_1 m_2 \ldots m_k$, tehdy a jen tehdy, je-li současně

$a \equiv b \pmod{m_1}$, $\pmod{m_2}$, ... a konečně též $\pmod{m_k}$.

§ 20. 1. Jsou-li a, b, c čísla celá, platí:

I $a \equiv a \pmod{m}$.

II Z $a \equiv b \pmod{m}$ plyne $b \equiv a \pmod{m}$.

III Z $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ plyne $a \equiv c \pmod{m}$.

I a II jsou samozřejmé. Důkaz III je zcela jednoduchý. První dvě kongruence značí, že $a - b$ a $b - c$ jsou dělitelny m. Je tedy i $a - c = (a - b) + (b - c)$ dělitelno m.

2. Jsou-li a, b, c, d čísla celá a je-li

$$a \equiv b \pmod m$$
$$c \equiv d \pmod m,$$

je též

$$a + c \equiv b + d \pmod m$$
$$a - c \equiv b - d \pmod m.$$

3. I. Je-li c číslo celé, plyne z kongruence $a \equiv b \pmod m$ též $ac \equiv bc \pmod m$.

II. Je-li pak d číslo celé, a $c \equiv d \pmod m$, je $ac \equiv bd \pmod m$.

Je pak totiž

$$ac \equiv bc \pmod m$$
$$bc \equiv bd \pmod m,$$

tedy i $ac \equiv bd \pmod m$.

Nechť a, b a m jsou čísla racionální celá. Z kongruence $a \equiv b \pmod m$ plyne $a^k \equiv b^k \pmod m$, kdež k je libovolné číslo celé $\geqq 0$.

Je-li $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ mnohočlen s celými koeficienty, pak plyne z $a \equiv b \pmod m$, že $f(a) \equiv f(b) \pmod m$.

Z $a \equiv b \pmod m$ plyne totiž $a^k \equiv b^k \pmod m$, $a_k a^k \equiv a_k b^k \pmod m$ $(k = 0, 1, 2, \ldots, n)$ a tedy i $f(a) \equiv f(b) \pmod m$.

Podobně, je-li $f(x_1, x_2, \ldots, x_n)$ mnohočlen v $x_1, x_2, \ldots, x_n$ s celými koeficienty, plyne z $a_1 \equiv b_1$, $a_2 \equiv b_2, \ldots, a_n \equiv b_n \pmod m$ ($a_1, b_1, a_2, b_2, \ldots, a_n, b_n, m$ čísla celá), že je též

$$f(a_1, a_2, \ldots, a_n) \equiv f(b_1, b_2, \ldots, b_n) \pmod m.$$

4. Z kongruence $ac \equiv bc \pmod m$ (a, b, c, m čísla celá), neplyne obecně $a \equiv b \pmod m$. Kongruence $ac \equiv bc \pmod m$ totiž značí, že $c(a - b)$ je dělitelno m. Je-li c nesoudělné s m, plyne odtud, že $a - b$ je dělitelno m, t. j. $a \equiv b \pmod m$. Obecně označme δ největšího společného dělitele čísel c, m.

Pak $\frac{c}{\delta}(a - b)$ je dělitelno m/δ, a ježto c/δ a m/δ jsou čísla nesoudělná, je $a - b$ dělitelno m/δ, t. j. $a \equiv b \pmod{m/\delta}$. Máme tedy větu:

Z kongruence $ac \equiv bc \pmod m$ *plyne* $a \equiv b \pmod m$, *je-li* c *nesoudělné s* m, *a obecně* $a \equiv b \pmod{m/\delta}$, *je-li* δ *n. s. d. čísel* c *a* m.

Je-li $c \equiv d \pmod m$, t. j. $d = c + qm$, kdež q je číslo celé, je podle věty na konci § 5 $(d, m) = (c + qm, m) = (c, m)$.

Platí-li kongruence $ac \equiv bd \pmod m$, $c \equiv d \pmod m$, je $bd \equiv bc \pmod m$, takže $ac \equiv bc \pmod m$. I platí věta:

Z kongruencí $ac \equiv bd \pmod m$, $c \equiv d \pmod m$ *plyne* $a \equiv b \pmod{m/\delta}$, *kdež* $\delta = (c, m) = (d, m)$.

5. Součin dvou čísel celých může býti kongruentní (mod m) s nulou, ač žádný z činitelů nemá tuto vlastnost. Na př. $6 = 2 \cdot 3 \equiv 0 \pmod 6$, ač ani 2 ani 3 není $\equiv 0 \pmod 6$.

Je-li však modul m prvočíslem p, $m = p$, platí podle § 11 věta:

Je-li součin dvou čísel celých kongruentní (mod p) s nulou, je aspoň jeden z činitelů (mod p) s nulou kongruentní.

§ 21. Množství čísel racionálních celých, která jsou spolu kongruentní (mod m), nazveme třídou (mod m). O dvou číslech téže třídy budeme též říkati, že jedno je zbytkem druhého (mod m). Dvě třídy (mod m) mají buď všechny prvky společné neb žádný. Třída (mod m) bude určena, známe-li jeden její prvek. Prvek ten nazveme také representantem třídy. Všechny prvky třídy (mod m) lze znázorniti ve tvaru $a + mn$, kdež a je libovolný prvek z ní (representant) a n číslo celé. Místo representant třídy (mod m) se též říká zbytek (mod m).

Je-li m celé $\neq 0$, lze representanty všech čísel celých (mod m) snadno udati. Jsou jimi čísla 0, 1, 2, . . . , $|m| - 1$.

Při $m = 0$, kdy kongruence přejde v rovnost, je každá třída tvořena jediným prvkem.

Libovolné číslo celé a lze totiž podle § 2 str. 9 znázorniti ve tvaru $a = q\,m + r$, kdež q, r jsou čísla celá, $0 \leq r < |m|$. Je tedy $a \equiv r \pmod m$. Každé číslo celé je tudíž (mod m) kongruentní s jedním z čísel $0, 1, 2, \ldots, |m| - 1$ a jen s jedním, ježto žádná dvě z těchto čísel nejsou spolu kongruentní (mod m). Je tedy na počet $|m|$ různých tříd (mod m) a za representanty jejich lze zvoliti čísla $0, 1, 2, \ldots, |m| - 1$.

Jestliže každé číslo celé je (mod m) kongruentní s jedním z čísel $r_1, r_2, \ldots, r_m$ mezi sebou (mod m) nekongruentních, nazveme $r_1, r_2, \ldots, r_m$ úplnou soustavou zbytků celých čísel (mod m). Takovou soustavu tvoří čísla $0, 1, 2, \ldots, |m| - 1$. (Úplná soustava nejmenších kladných zbytků celých čísel (mod m).) Je-li m číslo liché kladné, tvoří úplnou soustavu zbytků (mod m) čísla

$$0, 1, 2, \ldots \frac{m-1}{2}, \frac{m+1}{2} - m, \frac{m+3}{2} - m, \ldots (m-1) - m,$$

t. j. čísla

$$0, \pm 1, \pm 2, \ldots \pm \frac{m-1}{2},$$

(zbytky o nejmenší absolutní hodnotě).

Tvoří-li $r_1, r_2, \ldots, r_m$ *úplnou soustavu zbytků celých čísel (mod* m*), tvoří též*

$$ar_1 + b,\ ar_2 + b,\ \ldots,\ ar_m + b \qquad (1)$$

úplnou soustavu zbytků celých čísel (mod m*), značí-li* a, m *čísla celá nesoudělná.*

Uvedená věta plyne z té okolnosti, že žádná dvě z čísel (1), jichž je na počet m, nejsou spolu kongrueńtní (mod m). Kdyby totiž bylo

$$ar_i + b \equiv ar_j + b \pmod{m},\ i \neq j,$$

i, j jinak libovolná dvě čísla z posloupnosti $1, 2, \ldots, m$, bylo by též $ar_i \equiv ar_j \pmod{m}$, t. j. $r_i \equiv r_j \pmod{m}$, což by bylo proti předpokladu.

§ 22. Jestliže v racionální celé funkci s celými koeficienty $f(x)$ klademe za x hodnoty $0, 1, 2, 3, \ldots$ a vypočteme nejmenší kladné zbytky $f(0), f(1), f(2), f(3), \ldots \pmod{m}$ (m číslo celé $\neq 0$), posloupnost, kterou takto dostaneme, bude periodická, ježto podle § 20 odst. 3

$$f(k + m) \equiv f(k) \pmod{m},\ (k \text{ číslo celé}).$$

Je-li na př. $f(x) = x^3 - 8x + 6$, $m = 5$, bude pro

$n = 0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots$ $f(x) \equiv 1, 4, 3, 4, 3, 1, 4, 3, 4, \ldots \pmod{5}$.

V uvažovaném případě je perioda $1, 4, 3, 4, 3$. Mezi těmito hodnotami se nevyskytuje ani 0 ani 2, takže kongruence

$$x^3 - 8x + 6 \equiv 0 \quad \text{a} \quad x^3 - 8x + 6 \equiv 2 \pmod{5}$$

nejsou řešitelné.

Tím spíše pak rovnice $x^3 - 8x + 6 = 0$ a $x^3 - 8x + 6 = 2$ nemají za kořeny čísla celá racionální.

Mnohočlen s racionálními celými koeficienty $f(x)$ *stupně* $n > 0$ *nemůže pro všechny celé hodnoty* x *představovati prvočísla; pro nekonečně mnoho celých hodnot* x *je* $f(x)$ *číslo složené.*

Nechť pro číslo celé $x = x_0$ je $f(x_0)$ prvočíslo, $f(x_0) = p$. Pro $x = x_0 + kp$, kdež k je celé číslo, t. j. $x \equiv x_0 \pmod{p}$, je $f(x) \equiv f(x_0) \equiv 0 \pmod{p}$, tedy $f(x)$ je dělitelno p. Avšak jen pro konečný počet hodnot k může býti

$$f(x_0 + kp) = 0 \text{ neb } = \pm p.$$

Vyhneme-li se těmto hodnotám, bude $f(x_0 + kp)$ číslo složené.

Existují mnohočleny, které poskytují velký počet prvočísel

$x^2 - x + 41$ je prvočíslo pro $x = 0, 1, 2, 3, \ldots, 40$,
ale též pro $x = -1, -2, -3, \ldots, -39$.
$x^2 + x + 17$ je prvočíslo pro $x = 0, 1, 2, \ldots, 15$.

Fermat se domníval, že $F_n = 2^{2^n} + 1$ je prvočíslo pro n celé $\geqq 0$.

Také skutečně

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

jsou prvočísla.

Naproti tomu

$$F_5 = 641 \cdot 6700417 \text{ (Euler. Viz § 29 konec).}$$

§ 23. a, b, m buďtež celá čísla $m \neq 0$. Budeme hledati kořeny kongruence $ax + b \equiv 0 \pmod m$, t. j. celá čísla x splňující kongruenci onu. Je-li a nesoudělné s m a probíhá-li x úplnou soustavu zbytků (mod m), padne podle věty z § 21 str. 33 $ax + b$ právě jednou do třídy, v níž je číslo 0. Platí tedy věta:

Je-li a nesoudělné s m, jsou všechny kořeny kongruence $ax + b \equiv 0 \pmod m$ spolu kongruentní (mod m), t. j. všechny kořeny oné kongruence tvoří prvky jediné třídy (mod m); říkáme, že řešení kongruence té jsou určena jednoznačně (mod m).

Mají-li a a m za n. s. d. číslo d, tu, má-li býti kongruence $ax + b \equiv 0 \pmod m$ řešitelná, musí platiti též (mod d), a ježto a je dělitelno d, musí býti $b \equiv 0 \pmod d$. Kongruence $ax + b \equiv 0 \pmod m$ je splněna tehdy a jen tehdy, je-li splněna kongruence $\frac{a}{d}x + \frac{b}{d} \equiv 0 \left(\mathrm{mod}\ \frac{m}{d}\right)$. $\frac{a}{d}, \frac{m}{d}$ jsou čísla nesoudělná. Má tedy tato kongruence podle věty předešlé řešení x_0 jednoznačné (mod m/d). Všechna řešení oné kongruence lze psáti ve tvaru $x_0 + \frac{m}{d}y$, kdež y je libovolné číslo celé, a mezi těmito řešeními je jich právě d nekongruentních spolu (mod m). Obdržíme je, probíhá-li y úplnou soustavu zbytků (mod d). Budou to na př. čísla $x_0, x_0 + m/d, x_0 + 2\,m/d, x_0 + 3\,m/d, \ldots, x_0 + (d-1)\,m/d$.

Je-li $(a, m) = d > 1$, je kongruence $ax + b \equiv 0 \pmod m$ řešitelná, jen když b je dělitelno d. Pak má d řešení, z nichž žádná dvě nejsou spolu kongruentní (mod m).

Symbolem $b/a \pmod m$, kdež a, b, m jsou čísla celá, a, m spolu nesoudělná, budeme značiti libovolné číslo celé hovící kongruenci

$$ax \equiv b \pmod{m}.$$

$b/a \pmod{m}$ značí tedy číslo celé, které dostaneme, zvolíme-li ve výraze $(b+km)/a$ celé číslo k tak, aby $b + km$ se stalo násobkem a.

Řešení kongruence $ax \equiv 1 \pmod{m}$, které existuje, jsou-li a a m čísla nesoudělná, bude pak označeno $1/a \pmod{m}$. $1/a \pmod{m}$ nazývá se též číslem k a asociovaným (mod m); naopak je a asociováno k $1/a \pmod{m}$.

§ 24. Převeďme řešení kongruence

$$ax + b \equiv 0 \pmod{m}, \tag{1}$$

kdež $m = m'm''$, m, m', m'' čísla celá, $|m'| > 1$, $|m''| > 1$, na řešení dvou kongruencí (mod m') a (mod m'').

Nechť kongruence

$$ax + b \equiv 0 \pmod{m'} \tag{2}$$

má kořen x', takže $ax' + b \equiv 0 \pmod{m'}$. Je tedy $(ax'+b)/m' = b'$ číslo celé.

x splňující (1) splňuje i (2), takže je $x \equiv x' \pmod{m'}$, t. j. $x = x' + m'y$.

I bude $$ax' + b + am'y \equiv 0 \pmod{m},$$

ježto pak $ax' + b = m'b'$, $m = m'm''$, bude $ay + b' \equiv 0 \pmod{m''}$.

Tento postup by nám umožnil v případě, že m je číslo složené, převésti řešení (1) na řešení kongruencí o modulu prvočíselném.

Měli bychom na př. řešiti kongruenci

$$41x + 9 \equiv 0 \pmod{30}, \text{ t. j. } 11x + 9 \equiv 0 \pmod{30}.$$

Zde $30 = 5 \cdot 6$.

Kongruence

$$11x + 9 \equiv 0 \pmod{5}, \text{ t. j. } x - 1 \equiv 0 \pmod{5}$$

poskytne $$x' = 1.$$

Položme $$x = 1 + 5y.$$

Pak bude

$$55y + 20 \equiv 0 \pmod{30},$$

tedy $$11y + 4 \equiv 0 \pmod{6}, \quad -y + 4 \equiv 0 \pmod{6},$$

t. j. $$y \equiv 4 \pmod{6}.$$

I bude $x \equiv 21 \equiv -9 \pmod{30}$.

Určiti celé číslo x, které hoví kongruencím

$$\begin{aligned} ax + b &\equiv 0 \pmod{m_1} \\ ax + b &\equiv 0 \pmod{m_2} \\ &\dots\dots\dots\dots \\ ax + b &\equiv 0 \pmod{m_k} \end{aligned}$$

(a, b čísla celá, $m_1, m_2, \dots, m_k$ čísla celá $\neq 0$), je patrně podle § 19 str. 30 úkol ekvivalentní s řešením kongruence

$$ax + b \equiv 0 \pmod{m},$$

kdež m je nejmenší společný násobek čísel $m_1, m_2, \dots, m_k$. Jsou-li $m_1, m_2, \dots, m_k$ čísla po dvou spolu nesoudělná, je $m = m_1 m_2 \dots m_k$.

Je-li $m = p_1^{\mu_1} p_2^{\mu_2} \dots p_k^{\mu_k}$, kdež $p_1, p_2, \dots, p_k$ jsou od sebe různá prvočísla a $\mu_1, \mu_2, \dots, \mu_k$ čísla celá kladná, je řešení kongruence $ax + b \equiv 0 \pmod{m}$ patrně podle věty na konci § 19 ekvivalentní s řešením soustavy kongruencí

$$\begin{aligned} ax + b &\equiv 0 \pmod{p_1^{\mu_1}} \\ ax + b &\equiv 0 \pmod{p_2^{\mu_2}} \\ &\dots\dots\dots\dots \\ ax + b &\equiv 0 \pmod{p_k^{\mu_k}}. \end{aligned}$$

Dejme tomu, že by se jednalo o určení celého čísla x, hovícího současně kongruencím

$$\begin{aligned} a_1 x + b_1 &\equiv 0 \pmod{m_1} \\ a_2 x + b_2 &\equiv 0 \pmod{m_2} \\ &\dots\dots\dots\dots \\ a_k x + b_k &\equiv 0 \pmod{m_k}, \end{aligned} \tag{1}$$

kdež a_i, b_i, m_i jsou čísla celá, $m_i > 1$ a a_i je nesoudělné s m_i ($i = 1, 2, \dots, k$).

Kongruenci (mod m_i), kdež m_i není mocninou prvočísla, lze nahraditi kongruencemi o modulech $m'_i, m''_i, \dots$, jejichž moduly jsou mocniny prvočísel. Tak dostaneme soustavu

$$\begin{aligned} &a_1 x + b_1 \equiv 0 \pmod{m'_1}, \quad a_1 x + b_1 \equiv 0 \pmod{m''_1}, \dots \\ &a_2 x + b_2 \equiv 0 \pmod{m'_2}, \quad a_2 x + b_2 \equiv 0 \pmod{m''_2}, \dots \\ &\dots\dots\dots\dots\dots\dots \quad \dots\dots\dots\dots\dots\dots \end{aligned} \tag{2}$$

Řešme každou z těchto kongruencí. I dostaneme

$$\begin{aligned} &x \equiv r'_1 \pmod{m'_1}, \quad x \equiv r''_1 \pmod{m''_1}, \dots \\ &x \equiv r'_2 \pmod{m'_2}, \quad x \equiv r''_2 \pmod{m''_2}, \dots \\ &\dots\dots\dots\dots\dots \quad \dots\dots\dots\dots\dots \end{aligned} \tag{3}$$

Je-li některý modul rovný jinému, $m_i^{(j)} = m_s^{(t)}$, je nutno, aby

$$r_i^{(j)} \equiv r_s^{(t)} \pmod{m_i^{(j)} = m_s^{(t)}}.$$

Není-li tomu tak, je systém neřešitelný.

Vyskytnou-li se v systému (2) moduly, které jsou mocniny téhož prvočísla, pak příslušné kongruence z (3) buď si odporují (systém je pak neřešitelný), nebo jsou důsledkem jedné z nich. V tomto případě ponecháme kongruenci s modulem, který jest nejvyšší mocninou prvočísla, ostatní vynecháme.

I vidíme, že soustava kongruencí (1) dá se vždy převésti na soustavu

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv r_k \pmod{m_k}, \end{aligned} \tag{4}$$

kdež $m_1, m_2, \ldots, m_k$ jsou čísla celá po dvou spolu nesoudělná.

Dokážeme, že soustava ta je vždy řešitelná a to jednoznačně (mod m), kdež $m = m_1 m_2 \ldots m_k$.

Určeme čísla $e_1, e_2, \ldots, e_k$ hovící kongruencím

$$e_i \equiv 1 \pmod{m_i}, \quad e_i \equiv 0 \pmod{m_j}, \quad i \neq j, \quad i, j = 1, 2, 3, \ldots, k.$$

e_i určíme, klademe-li $e_i = e_i m/m_i$ a najdeme $\overline{e_i}$ z kongruence

$$\overline{e_i} \frac{m}{m_i} \equiv 1 \pmod{m_i}.$$

Pak je řešení soustavy (4)

$$x \equiv r_1 e_1 + r_2 e_2 + \ldots + r_k e_k \pmod{m_i} \quad i = 1, 2, 3, \ldots, k. \tag{5}$$

Neboť pak je též

$$x \equiv r_1 e_1 + r_2 e_2 + \ldots + r_k e_k \pmod{m},$$

t. j.

$$x \equiv r_i \pmod{m_i}.$$

Jestliže též x' splňuje kongruence (4), je

$$x' \equiv x \pmod{m_i},$$

t. j.

$$x' \equiv x \pmod{m},$$

ježto čísla $m_1, m_2, \ldots, m_k$ jsou po dvou spolu nesoudělná.

Probíhají-li čísla $r_1, r_2, \ldots, r_k$ úplné soustavy zbytků podle modulů resp. $m_1, m_2, \ldots, m_k$, poskytne nám výraz

$$r_1 e_1 + r_2 e_2 + \ldots + r_k e_k$$

$m_1 m_2 \ldots m_k = m$ hodnot, které tvoří též úplnou soustavu zbytků (mod m). Skutečně jsou tyto hodnoty (mod m) nekongruentní. Kdyby bylo

$$r_1 e_1 + r_2 e_2 + \ldots + r_k e_k \equiv r'_1 e_1 + r'_2 e_2 + \ldots + r'_k e_1 \pmod{m},$$

platila by tato kongruence též (mod m_i), takže by bylo

$$r_i \equiv r'_i \pmod{m_i}, \quad i = 1, 2, \ldots, k.$$

Má-li býti současně

$$x \equiv 9 \pmod{1400}, \quad x \equiv 37 \pmod{252}, \quad x \equiv 64 \pmod{135},$$

lze tyto kongruence, ježto

$$1400 = 2^3 \cdot 5^2 \cdot 7, \quad 252 = 2^2 \cdot 3^2 \cdot 7, \quad 135 = 3^3 \cdot 5,$$

nahraditi systémem

$$\begin{array}{lll} x \equiv 9 \pmod{2^3}, & x \equiv 9 \pmod{5^2}, & x \equiv 9 \pmod{7}, \\ x \equiv 37 \pmod{2^2}, & x \equiv 37 \pmod{3^2}, & x \equiv 37 \pmod{7}, \\ x \equiv 64 \pmod{3^3}, & x \equiv 64 \pmod{5}. & \end{array}$$

Srovnáním dostaneme, že podmínka nutná a postačující pro řešitelnost je splnění těchto kongruencí

$$\begin{aligned} 37 &\equiv 9 \pmod{2^2} \\ 64 &\equiv 37 \pmod{3^2} \\ 64 &\equiv 9 \pmod{5} \\ 37 &\equiv 9 \pmod{7}. \end{aligned}$$

Tyto jsou skutečně splněny a systém se redukuje na jednodušší

$$x \equiv 9 \pmod{2^3}, \quad x \equiv 64 \pmod{3^3}, \quad x \equiv 9 \pmod{5^2}, \quad x \equiv 9 \pmod{7}$$

neboli

$$x \equiv 9 \pmod{1400}, \quad x \equiv 64 \pmod{27},$$

t. j.

$$x \equiv 9 \pmod{1400}, \quad x \equiv 10 \pmod{27}.$$

Určeme čísla e_1, e_2 splňující kongruence

$$\begin{aligned} e_1 &\equiv 1 \pmod{1400}, \quad e_1 \equiv 0 \pmod{27} \\ e_2 &\equiv 0 \pmod{1400}, \quad e_2 \equiv 1 \pmod{27}. \end{aligned}$$

Ta jsou

$$e_1 \equiv 9801 \pmod{37800}, \quad e_2 \equiv 28000 \pmod{37800}.$$

I dostaneme

$$x \equiv 28009 \pmod{37800}, \quad 37800 = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7.$$

Také bychom mohli postupovati takto:
Kongruenci

$$x \equiv 9 \pmod{1400}$$

hoví číslo $x = 9 + 1400y$, kdež y je číslo celé. y dlužno voliti tak, aby byla splněna kongruence $x \equiv 10 \pmod{27}$, t. j.

$$1400y \equiv 1 \pmod{27},$$

tedy

$$23y \equiv 1 \pmod{27}.$$

Odtud dostaneme $y \equiv 20 \pmod{27}$

a tedy $x \equiv 28009 \pmod{37800}$.

Řešení soustavy (4) můžeme užíti ke zjednodušení řešení kongruence

$$ax + b \equiv 0 \pmod{m}, \tag{1'}$$

kdež a, m jsou čísla celá nesoudělná, $m = m_1 m_2 \ldots m_k$ rozklad v činitele po dvou spolu nesoudělné.

Kongruence (1') je patrně splněna tehdy a jen tehdy, je-li splněn souhrn kongruencí

$$ax + b \equiv 0 \pmod{m_1}, \quad ax + b \equiv 0 \pmod{m_2}, \ldots, \quad ax + b \equiv 0 \pmod{m_k}. \tag{2'}$$

Buďtež $r_1, r_2, \ldots, r_k$ jejich řešení.

Pak x hovící kongruencím

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \ldots, x \equiv r_k \pmod{m_k} \tag{3'}$$

splňuje i kongruenci (1').

§ 25. Kongruence

$$ax + b \equiv 0 \pmod{m} \tag{1}$$

vyžaduje, aby $ax + b$ bylo násobkem m a naopak, je splněna, je-li tomu tak. Je tedy řešení kongruence (1) ekvivalentní s řešením rovnice

$$ax + b = my, \tag{2}$$

v níž a, b, m jsou čísla celá, čísly celými x, y.

Aby tedy rovnice (2) byla řešitelná čísly celými, je nutno a postačí, aby n. s. d. čísel a, m byl obsažen v b.

Pišme rovnici (2) ve tvaru více symetrickém

$$ax + by = c. \tag{3}$$

Aby rovnice ta byla řešitelná čísly celými x, y, je nutno a postačí, aby c bylo dělitelno d, kdež $d = (a, b)$.

Řešení rovnice (3) čísly celými x, y je pak ekvivalentní s řešením kongruence

$$ax \equiv c \pmod{b}.$$

Je-li jedno její řešení x_0, jsou všechna její řešení dána výrazem

$$x = x_0 + \frac{b}{d} z,$$

kdež z je číslo celé.

$ax_0 - c$ je dělitelno b. Klaďme tedy
$ax_0 - c = -by_0$, t. j.
$ax_0 + by_0 = c$,

takže (x_0, y_0) je řešení rovnice (3) čísly celými.

I bude podle (3)

$$by = c - ax = c - ax_0 - \frac{ab}{d} z = by_0 - b\,\frac{a}{d}\,z,$$

t. j.

$$y = y_0 - \frac{a}{d} z.$$

Obecné řešení rovnice (3) celými čísly je tedy

$$x = x_0 + \frac{b}{d} z, \quad y = y_0 - \frac{a}{d} z$$

a ve speciálním případě, kdy a, b jsou čísla spolu nesoudělná, tedy $d = 1$,

$$x = x_0 + bz, \quad y = y_0 - az.$$

§ 26. Eulerovo (Bachetovo) řešení rovnice

$$a_1 x - a x_1 = b \tag{1}$$

čísly celými.

Předpokládejme, že a, a_1 jsou čísla celá nesoudělná, $a_1 > 0$. Kdyby $a_1 < 0$, pak bychom uvažovali místo (1) rovnici $-a_1 x + ax_1 = -b$, která jest splněna stejnými páry čísel (x, y).

Z rovnice (1) plyne

$$x = \frac{ax_1 + b}{a_1} = A_1 x_1 + B_1 + \frac{a_2 x_1 - b_1}{a_1},$$

kdež A_1, B_1, a_2, b_1 jsou čísla celá. Jest pak

$$\begin{matrix} a = A_1 a_1 + a_2 \\ b = B_1 a_1 - b_1 \end{matrix} \text{ t. j. } \begin{matrix} a \equiv a_2 \\ b \equiv -b_1 \end{matrix} \pmod{a_1};$$

za a_2 zvolme nejmenší kladný zbytek čísla $a \pmod{a_1}$, tedy

$$0 < a_2 < a_1.$$

Má-li býti x celé číslo, musí býti $(a_2x_1 - b_1)/a_1$ číslo celé, rovnající se x_2. Čísla x_1 a x_2 splňují pak rovnici

$$a_2x_1 - a_1x_2 = b_1 \qquad (2)$$

stejného tvaru jako (1), v níž a_1, a_2 jsou čísla celá nesoudělná $0 < a_2 < a_1$.

Z (2) bychom dostali

$$x_1 = \frac{a_1x_2 + b_1}{a_2} = A_2x_2 + B_2 + \frac{a_3x_2 - b_2}{a_2}$$

$$\begin{matrix} a_1 = A_2a_2 + a_3 \\ b_1 = B_2a_2 - b_2 \end{matrix} \text{ t. j. } \begin{matrix} a_1 \equiv a_3 \\ b_1 \equiv -b_2 \end{matrix} \pmod{a_2}.$$

Za a_3 bychom opět volili nejmenší kladný zbytek čísla $a_1 \pmod{a_2}$, takže by bylo $0 < a_3 < a_2$; a_3 by bylo opět nesoudělné s a_2. Kladli bychom $(a_3x_2 - b_2)/a_2 = x_3$ a x_3 by bylo číslo celé. Čísla x_2, x_3 by tedy splňovala rovnici $a_3x_2 - a_2x_3 = b_2$. Takovýmto postupem bychom po konečném počtu kroků došli k rovnici

$$a_kx_{k-1} - a_{k-1}x_k = b_{k-1},$$

v níž $a_k = 1$. Z ní by plynulo $x_{k-1} = a_{k-1}x_k + b_{k-1}$. Číslo x_{k-1} by bylo číslo celé, ať je x_k jakékoliv číslo celé.

Postupně bychom dostali x_{k-2}, x_{k-3}, ... x_1, x jako lineární funkce s celými koeficienty v x_k.

Jako příklad uveďme řešení rovnice

$$39x - 56y = 11$$

celými čísly x, y. Jest

$$x = \frac{56y + 11}{39} = y + \frac{17y + 11}{39} = y + r,$$

klademe-li

$$\frac{17y + 11}{39} = r.$$

Dále máme:

$$y = \frac{39r - 11}{17} = 2r - 1 + \frac{5r + 6}{17} = 2r - 1 + s$$

$$\frac{5r + 6}{17} = s$$

$$r = \frac{17s - 6}{5} = 3s - 1 + \frac{2s - 1}{5} = 3s - 1 + t$$

$$\frac{2s-1}{5} = t$$

$$s = \frac{5t+1}{2} = 2t + \frac{t+1}{2} = 2t + u$$

$$\frac{t+1}{2} = u$$

$$t = 2u - 1.$$

Nyní výpočtem postupně dostaneme

$$s = 5u - 2,\ r = 17u - 8,\ y = 39u - 19,\ x = 56u - 27.$$

Celé kladné hodnoty x, y dostaneme pro $u \geqq 1$.
Postup bychom mohli zkrátiti takto:

$$y = \frac{39z - 11}{17} = 2r - 3 + \frac{5(r+8)}{17}.$$

Ježto 5 a 17 jsou čísla nesoudělná, musí býti, aby y bylo celé, $\frac{1}{17}(r+8)$ číslo celé, rovnající se s'. Tak dostaneme $r = 17s' - 8$, $y = 2s' - 3 + 5r = 39s' - 19$, $x = 56s' - 27$.

§ 27. Řešení rovnice

$$ax + by = c, \tag{1}$$

kdež a, b, c jsou čísla celá kladná, a, b spolu nesoudělná, celými kladnými čísly x, y.

x bude probíhati všechna čísla celá $\geqq 0$, položíme-li

$$x = b\xi + u,$$

kdež ξ probíhá čísla celá $\geqq 0$ a u probíhá množství U, skládající se z čísel

$$0,\ 1,\ 2,\ \ldots,\ b - 1.$$

Podobně bude y probíhati všechna čísla celá $\geqq 0$, klademe-li

$$y = a\eta + v,$$

kdež η probíhá čísla celá $\geqq 0$ a v probíhá množství V, skládající se z čísel

$$0, 1, 2, \ldots, a - 1.$$

Budiž r nejmenší zbytek $\geqq 0$ čísla c (mod ab), tedy

$$c = qab + r,$$

kdež

$$q = \left[\frac{c}{ab}\right], \quad 0 \leqq r < ab.$$

Z (1) tak dostaneme

$$qab + r = ab\,(\xi + \eta) + au + bv. \qquad (2)$$

Probíhá-li u úplnou soustavu nejmenších kladných zbytků (mod b), t. j. množství U, a v úplnou soustavu nejmenších kladných zbytků (mod a), t. j. množství V, probíhá $au + bv$ podle § 24 str. 35 úplnou soustavu zbytků (mod ab) a je

$$0 \leqq au + bv < 2ab.$$

Bude tedy buď $au + bv$ neb $au + bv - ab$ číslo z úplné soustavy nejmenších kladných zbytků (mod ab).

V prvém případě bude existovati u z U a v z V té vlastnosti, že

$$au + bv = r, \quad \text{tedy } \xi + \eta = q;$$

lze pak klásti

$$\xi = 0,\ 1,\ 2, \ldots, q,$$
$$\eta = q,\ q - 1,\ q - 2, \ldots, 0,$$

takže (1) má v tomto případě $q + 1$ řešení celých kladných.

V druhém případě bude existovati u z U a v z V té vlastnosti, že

$$au + bv - ab = r, \qquad \text{tedy } \xi + \eta = q - 1;$$

lze pak klásti

$$\xi = 0,\ 1,\ 2, \ldots, q - 1,$$
$$\eta = q - 1,\ q - 2,\ q - 3, \ldots, 0,$$

takže (1) má v tomto případě q řešení celých kladných.

V prvém případě rovnice $au + bv = r$ je řešitelná, v druhém není řešitelná čísly celými $\geqq 0$.

Máme tedy větu:

Rovnice (1) má

$$\left[\frac{c}{ab}\right] + 1$$

řešení čísly celými kladnými, je-li rovnice $au + bv = r$ řešitelná čísly celými $\geqq 0$,

$$\left[\frac{c}{ab}\right]$$

řešení čísly celými kladnými, není-li rovnice $au + bv = r$ řešitelná čísly celými $\geqq 0$.*)

*) Je-li N počet řešení rovnice (1) čísly celými kladnými, je $\lim_{c \to \infty} \frac{N}{\frac{c}{ab}} = 1$.

§ 28. Kriteria dělitelnosti. Budiž číslo celé $a \geqq 0$ vyjádřeno v soustavě desítkové (viz § 2 str. 9)

$$a = a_0 + 10a_1 + 10^2a_2 + \ldots + 10^ka_k, \tag{1}$$

kdež

$a_0, a_1, \ldots, a_k$ jsou čísla celá, $0 \leqq a_i \leqq 9$, $i = 0, 1, 2, \ldots, k$.

Je-li $10 \equiv r \pmod m$, bude

$$a \equiv a_0 + ra_1 + r^2a_2 + \ldots + r^ka_k \pmod m, \tag{2}$$

a obecněji, je-li $10^i \equiv r_i \pmod m$, pak

$$a \equiv a_0 + r_1a_1 + r_2a_2 + \ldots + r_ka_k \pmod m, \tag{3}$$

takže a bude dělitelno m, bude-li výraz na pravé straně kongruence (2) neb (3) dělitelný m. (Úvaha tato ovšem platí, jsou-li a_0, $a_1, \ldots, a_k$ libovolná čísla celá splňující rovnost (1)).

Pro $m = 2$ a 5 je

$$10 \equiv 0, \ 10^2 \equiv 0, \ldots,$$

tedy $$a \equiv a_0 \pmod 2 \text{ i } \pmod 5,$$

takže číslo celé je dělitelno 2 neb 5, jsou-li jeho jednotky v desítkové soustavě dělitelny 2 resp. 5.

$$10 \equiv 1 \pmod 9, \quad a \equiv a_0 + a_1 + \ldots + a_k \pmod 9,$$

tedy i

$$a \equiv a_0 + a_1 + \ldots + a_k \pmod 3.$$

Je tedy číslo celé kongruentní mod 9 i mod 3 se součtem svých číslic v soustavě desítkové.

Pro modul 11 platí $10 \equiv -1 \pmod{11}$, takže bude

$$10^i \equiv (-1)^i \pmod{11} \quad \text{pro } i \geqq 1.$$

Pro modul 7 je

$$10 \equiv 3, \ 10^2 \equiv 2, \ 10^3 \equiv -1, \ 10^4 \equiv -3, \ 10^5 \equiv -2, \ 10^6 \equiv 1, \ 10^7 \equiv 3, \ldots \pmod 3,$$

tedy

$$a \equiv (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - (a_9 + 3a_{10} + 2a_{11}) + \ldots \pmod 7.$$

Mějme pro číslo celé a znázornění

$$a = A_0 + 100A_1 + 100^2A_2 + \ldots + 100^kA_k,$$

kdež

$$A_0, \ A_1, \ldots, A_k$$

jsou čísla celá.

(Případ, kdy $a \geqq 0$, $0 \leqq A_i \leqq 99$, $i = 0, 1, 2, \ldots, k$, odpovídá rozdělení čísla psaného v soustavě desítkové na skupiny po dvou číslicích.)

Ježto $100 - 1 = 99 = 9 \cdot 11$, bude $100 \equiv 1 \pmod{11}$, tedy $100^i \equiv 1 \pmod{11}$ pro i celé $\geqq 0$, z čehož plyne konečně

$$a \equiv A_0 + A_1 + \ldots + A_k \pmod{11}.$$

Podobně je-li

$$a = B_0 + 1000\, B_1 + 1000^2 B_2 + \ldots + 1000^L B_L,$$

kdež $B_0, B_1, \ldots, B_L$ jsou čísla celá (případ $0 \leqq B_i \leqq 999$, $i = 0, 1, 2, \ldots, L$, $a \geqq 0$ odpovídá rozdělení čísla psaného v soustavě desítkové na skupiny po třech číslicích), pak z $1000 + 1 = 1001 \equiv 7 \cdot 11 \cdot 13$ plyne $1000 \equiv -1 \pmod{7, 11, 13}$, t. j. $1000^i \equiv (-1)^i$ (i číslo celé kladné), podle týchž modulů, takže bude

$$a \equiv B_0 - B_1 + B_2 - B_3 + \ldots + (-1)^L B_L \pmod{7, 11, 13}.$$

Budiž číslo celé $a = a_0 + 10A$, kdež a_0, A jsou zase čísla celá. Nechť m je číslo celé nedělitelné ani 2 ani 5. Pak lze určiti číslo celé μ tak, že $10\mu \equiv 1 \pmod{m}$. μ je pak nesoudělné s m.

I bude

$$a\mu = a_0\mu + 10\mu A \equiv a_0\mu + A \pmod{m}.$$

Klaďme $a' = a_0\mu + A$, takže $a\mu \equiv a' \pmod{m}$. I bude a dělitelno číslem m tehdy a jen tehdy, bude-li a' dělitelno číslem m.

Pro $m = 3, 9$ je $\mu = 1$, pro $m = 11$ je $\mu = -1$. Dostaneme tak pravidla již dříve odvozená.

Pro $m = 7$ je $\mu = -2$, $a' = A - 2a_0$;
pro $m = 13$ je $\mu = 4$ neb -9, $a' = A + 4a_0$ neb $a' = A - 9a_0$;
pro $m = 17$ je $\mu = -5$, $a' = A - 5a_0$;
pro $m = 19$ je $\mu = 2$, $a' = A + 2a_0$;
pro $m = 37$ je $\mu = -11$, $a' = A - 11a_0$.

$a = 3192 = 2 + 10 \cdot 319$ bude dělitelno sedmi, je-li sedmi dělitelno $a' = 319 - 2 \cdot 2 = 315$, avšak $315 = 5 + 10 \cdot 31$ bude dělitelno sedmi, je-li sedmi dělitelno $31 - 2 \cdot 5 = 21$. Ježto 21 je sedmi dělitelno, je sedmi dělitelno i 315 a 3192.

§ 29. Z vlastností kongruencí plyne možnost užíti jich k verifikaci početních úkonů.

Dejme tomu, že $f(x_1, x_2, \ldots, x_n)$ je racionální celá funkce v $x_1, x_2, \ldots, x_n$ s celými koeficienty a že jsme vypočetli

$$A = f(A_1, A_2, \ldots, A_n), \tag{1}$$

kdež $A_1, A_2, \ldots, A_n$ jsou čísla celá.

Je-li

$$A \equiv a,\ A_1 \equiv a_1,\ A_2 \equiv a_2, \ldots, A_n \equiv a_m \pmod m,$$

musí býti

$$a \equiv F(a_1, a_2, \ldots, a_m) \pmod m. \tag{2}$$

Platnost kongruence (2) je podmínka nutná (nikoliv však postačující) pro platnost rovnice (1).

Za m lze užíti s výhodou 9 neb 11, ježto podle předešlého u čísla psaného v soustavě desítkové lze velmi snadno určiti zbytky (mod 9) resp. (mod 11). Na tom založena je tak zvaná zkouška devítková resp. jedenáctková

Abychom na př. zjistili, zda $(15 + 54) \cdot 13 - 325 = 572$, nahraďme na levé straně každé číslo jeho zbytkem (mod 9). Dostaneme

$$(6 + 0) \cdot 4 - 1 = 23 \equiv 5 \pmod 9.$$

Avšak $572 \equiv 5 \pmod 9$, takže „zkouška vyšla" a lze, ovšem jen s jistou pravděpodobností, souditi, že výpočet je správný.

Podobně ke zjištění, zda $(15^2 - 21) \cdot 326 = 66504$, vypočtěme zbytky (mod 11).

Obdržíme $(4^2 - 10) \cdot 7 = 6 \cdot 7 = 42 \equiv 9 \pmod{11}$ a stejně $66504 \equiv 9 \pmod{11}$.

Mnohdy lze pomocí kongruencí výpočet značně zjednodušiti. Dokažme, že $2^{32} + 1$ je dělitelno 641. (Viz § 22 konec.)

$$2^2 = 4,\ 2^4 = 16,\ 2^8 = 256,$$
$$2^{16} = 65536 \equiv 154,$$
$$2^{32} \equiv 154^2 \equiv 23716 \equiv -1$$

vesměs (mod 641).

Neb jednodušeji

$$641 = 1 + 5 \cdot 2^7 = 2^4 + 5^4,$$

takže $$2^7 \equiv -\tfrac{1}{5},\quad (\tfrac{2}{5})^4 \equiv -1 \pmod{641}.$$

Je tedy

$$2^8 \equiv -\tfrac{2}{5},$$
$$2^{32} \equiv (-\tfrac{2}{5})^4 \equiv (\tfrac{2}{5})^4 \equiv -1 \pmod{641}.$$

§ 30. Budiž m číslo celé $\neq 0$. Označíme $\varphi(m)$ počet čísel celých nesoudělných s m, obsažených mezi čísly $0, 1, 2, 3, \ldots, |m| - 1$, neb též mezi čísly $1, 2, 3, \ldots, |m|$.

Je-li $b \equiv a \pmod m$, je podle § 20 str. 31 $(a, m) = (b, m)$, takže všechna čísla téže třídy mají s m téhož n. s. d. I vidíme,

že můžeme $\varphi(m)$ definovati též takto: $\varphi(m)$ je počet čísel celých nesoudělných s m, která jsou obsažena v úplné soustavě zbytků celých čísel (mod m). Čísla celá nesoudělná s m z úplné soustavy zbytků (mod m) tvoří tak zvanou redukovanou soustavu zbytků (mod m).

Určíme nejprve $\varphi(m)$ pro případ, že m je mocnina kladného prvočísla p, $m = p^a$, a číslo celé kladné. Z čísel 0, 1, 2, 3, ..., $p^a - 1$ musíme vyloučiti čísla, která nejsou nesoudělná s p^k, což jsou násobky p, t. j. čísla p, $2p$, $3p$, ..., $p^a = p^{a-1} \cdot p$.

Bude tedy $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a \left(1 - \frac{1}{p}\right)$.

Obraťme se nyní k případu, kdy m je dělitelno více různými prvočísly.

Budiž $m = m_1 m_2 \ldots m_k$, kdež $m_1, m_2, \ldots, m_k$ jsou čísla celá po dvou spolu nesoudělná. Nechť je $e_i \equiv 1 \pmod{m_i}$, $e_j \equiv 0 \pmod{m_i}$, $i \neq j$, $i, j = 1, 2, 3, \ldots, k$. Dokázali jsme v § 25 str. 37, že, probíhají-li r_i úplné soustavy zbytků (mod m_i), probíhá

$$r = r_1 e_1 + r_2 e_2 + \ldots + r_k e_k \qquad (*)$$

úplnou soustavu zbytků (mod m).

Lze snadno nahlédnouti, že, probíhají-li r_i redukované soustavy zbytků (mod m_i), probíhají r redukovanou soustavu zbytků (mod m), takže

$$\varphi(m) = \varphi(m_1)\,\varphi(m_2) \ldots \varphi(m_k).$$

Probíhají-li r_i redukované soustavy zbytků (mod m_i), nabude r v (*) $\varphi(m_1)\,\varphi(m_2) \ldots \varphi(m_k)$ hodnot spolu (mod m) nekongruentních. Stačí tedy dokázati, že každé z těchto čísel r je nesoudělné s m, a že, je-li některý z n. s. d. (r_1, m_1), (r_2, m_2), ..., $(r_k, m_k) > 1$, je i $(r, m) > 1$, t. j. není ani r nesoudělné s m. Jest totiž

$$r \equiv r_i \pmod{m_i},$$

z čehož tvrzení ihned vyplývá.

Budiž $|m| = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, kdež $p_1, p_2, \ldots, p_k$ jsou mezi sebou různá prvočísla, $a_1, a_2, \ldots, a_k$ čísla celá kladná. Pak z čísel $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$ každá dvě jsou spolu nesoudělná, takže

$$\varphi(m) = \varphi(p_1^{a_1})\,\varphi(p_2^{a_2}) \ldots \varphi(p_k^{a_k}),$$

t. j. $$\varphi(m) = |m| \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right).$$

§ 31. Zajímavou vlastnost funkce $\varphi(m)$ poskytne tato úvaha. Označme d celého kladného dělitele čísla m. Hledejme počet čísel z řady

$$1, 2, 3, \ldots, m,$$

která mají s m největšího společného dělitele d. Nalézají se ovšem mezi násobky d z oné řady, t. j. mezi čísly

$$d, 2d, 3d, \ldots, \frac{|m|}{d} . d.$$

Číslo takové hd má s $|m| = \frac{|m|}{d} . d$ tehdy a jen tehdy n. s. d. d, jsou-li h a $\frac{|m|}{d}$ nesoudělná. Je tedy hledaný počet roven počtu čísel z řady $1, 2, 3, \ldots, \frac{|m|}{d}$, která jsou nesoudělná s $\frac{|m|}{d}$, t. j. $\varphi\left(\frac{m}{d}\right)$.

Jsou-li $d_1 = 1, d_2, d_3, \ldots, d_\nu = |m|$ všichni celí kladní dělitelé čísla m, má každé z čísel $1, 2, 3, \ldots, |m|$ jednoho z těchto dělitelů za n. s. d. s m. Dáme-li do jedné skupiny čísla, jež mají téhož n. s. d. s m, dostaneme v těchto skupinách resp. $\varphi\left(\frac{m}{d_1}\right)$, $\varphi\left(\frac{m}{d_2}\right), \ldots, \varphi\left(\frac{m}{d_\nu}\right)$ čísel, která dohromady musí poskytnouti všechna čísla z řady $1, 2, 3, \ldots, m$, takže musí platiti

$$|m| = \varphi\left(\frac{m}{d_1}\right) + \varphi\left(\frac{m}{d_2}\right) + \varphi\left(\frac{m}{d_3}\right) + \ldots + \varphi\left(\frac{m}{d_\nu}\right).$$

§ 32. Je-li $\varrho_1, \varrho_2, \ldots, \varrho_h$, $h = \varphi(m)$, redukovaná soustava zbytků celých čísel (mod m), je též $a\varrho_1, a\varrho_2, \ldots, a\varrho_h$ takovou soustavou, je-li a nesoudělné s m. Z $(a, m) = 1$, $(\varrho_i, m) = 1$ $(i = 1, 2, 3, \ldots, h)$ plyne totiž ihned $(a\varrho_i, m) = 1$. Dále je $a\varrho_i \equiv a\varrho_j \pmod m$. jen když $i = j$. Ježto pak každé z čísel $a\varrho_1, a\varrho_2, \ldots, a\varrho_h$ je (mod m) kongruentní s jedním z čísel $\varrho_1, \varrho_2, \ldots, \varrho_h$, je též součin čísel $a\varrho_1, a\varrho_2, \ldots, a\varrho_h$ kongruentní (mod m) se součinem $\varrho_1, \varrho_2, \ldots, \varrho_h$, t. j.

$$a^h \varrho_1 \varrho_2 \ldots \varrho_h \equiv \varrho_1 \varrho_2 \ldots \varrho_h \pmod m.$$

Ježto pak každé ϱ_i je nesoudělné s m, takže i $\varrho_1 \varrho_2 \ldots \varrho_h$ je nesoudělné s m, bude, dělíme-li $\varrho_1 \varrho_2 \ldots \varrho_h$, $a^h \equiv 1 \pmod m$.

I platí věta, zvaná větou Fermatovou:

Je-li a číslo celé nesoudělné s m, je $a^{\varphi(m)} \equiv 1$ (mod m). Je-li $m = p$ prvočíslo, pak je $\varphi(m) = p - 1$. I platí pro každé číslo celé nedělitelné p: $a^{p-1} \equiv 1 \pmod p$, a násobíme-li a, dostaneme $a^p \equiv a \pmod p$. Tato kongruence platí pro každé číslo celé a.

Z věty Fermatovy plyne, že pro a nesoudělné s m je $1/a \equiv$

$\equiv a^{(\varphi m)-1} \pmod m$. Je tedy každá kongruence $ax + b \equiv 0 \pmod m$ pro a nesoudělné s m, splněna číslem

$$x \equiv -ba^{\varphi(m)-1} \pmod m.$$

§ 33. Dva mnohočleny s celými koeficienty

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$
$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$$

nazývají se **identicky kongruentní podle modulu** m, (mod m) (m celé číslo), $f(x) \equiv g(x) \pmod m$, platí-li

$$a_i \equiv b_i \pmod m \text{ pro } i = 0, 1, 2, \ldots, n.$$

Pro konstanty, t. j. mnohočleny stupně 0, kryje se tento pojem s pojmem kongruence dříve podaným.

Všimněme si, že z platnosti kongruencí $f(x_0) \equiv g(x_0) \pmod m$ pro všechna x_0 celá neplyne, že mnohočleny $f(x)$ a $g(x)$ jsou spolu identicky kongruentní (mod m).

Ukazují to mnohočleny x^p a x (mod p), p prvočíslo. Podle věty Fermatovy je $x^p \equiv x \pmod p$, ať je x jakékoliv číslo celé. Kongruence $x^p \equiv x \pmod p$ neplatí však identicky.

Pro kongruence mnohočlenů platí podobná pravidla početní jako pro kongruence číselné. Důkaz byl by zcela jednoduchý.

Je-li α celé číslo té vlastnosti, že $f(\alpha) \equiv 0 \pmod m$, nazývá se α **kořenem kongruence** $f(x) \equiv 0 \pmod m$.

Je-li α kořen kongruence $f(x) \equiv 0 \pmod m$ a platí-li $\beta \equiv \alpha \pmod m$, je patrně též β kořenem oné kongruence.

Mnohočlen s celými koeficienty stupně nanejvýš n, $f(x)$, má podle modulu prvočíselného p nanejvýše n spolu nekongruentních kořenů, není-li $f(x) \equiv 0 \pmod p$ identicky. Je-li $f(x) \equiv 0 \pmod p$ identicky, t. j. jsou-li všechny koeficienty $f(x)$ dělitelny p, má kongruence za kořeny všechna čísla celá.

Věta platí patrně pro mnohočleny stupně 0, t. j. pro konstanty. Pro $f(x) = a_0$ nemá $f(x) \equiv 0 \pmod p$ řešení, není-li a_0 dělitelno p. neb má za řešení všechna čísla celá, je-li $a_0 \equiv 0 \pmod p$, t. j. $f(x) \equiv 0 \pmod p$ identicky.

Předpokládejme, že věta je dokázána pro mnohočleny stupně $\leq n - 1$, dokažme pak, že platí i pro mnohočleny stupně $\leq n$.

Dejme tomu, že by kongruence $f(x) \equiv 0 \pmod p$ měla aspoň $n + 1$ spolu nekongruentních celých kořenů. Označme je $\alpha, \alpha_1, \ldots, \alpha_n$. Položme

$$g(x) = a_n (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

Bude to mnohočlen s celými koeficienty a s koeficientem a_n u x^n.

$f(x) - g(x)$ bude mnohočlen stupně nanejvýš $n - 1$. Kongruence $f(x) - g(x) \equiv 0 \pmod{p}$ měla by n spolu nekongruentních kořenů $\alpha_1, \alpha_2, \ldots, \alpha_n$, platilo by tedy podle předpokladu o mnohočlenu $f(x) - g(x)$, že je kongruentní s 0 (mod p) identicky, t. j. že všechny jeho koeficienty jsou $\equiv 0 \pmod{p}$.

Musilo by tedy platiti pro α: $f(\alpha) - g(\alpha) \equiv 0 \pmod{p}$. Ježto však α je kořenem kongruence $f(x) \equiv 0 \pmod{p}$, takže $f(\alpha) \equiv 0 \pmod{p}$, bylo by i $g(\alpha) \equiv 0 \pmod{p}$, t. j. $a_n (\alpha - \alpha_1)(\alpha - \alpha_2) \ldots (\alpha - \alpha_n) \equiv 0 \pmod{p}$. Podle předpokladu $\alpha \not\equiv \alpha_i \pmod{p}$ $(i = 1, 2, \ldots, n)$ bylo by tedy $a_n \equiv 0 \pmod{p}$. Pak by však mnohočlen $f(x)$ byl (mod p) kongruentní s mnohočlenem stupně nanejvýše $n-1$, pro který věta platí. Platí tedy i pro mnohočlen $f(x)$ stupně nanejvýš n.

Věta neplatí pro případ, že modul je číslo složené. Stačí uvažovati kongruenci $x^2 - 1 \equiv 0 \pmod{8}$. Mnohočlen 2. stupně $x^2 - 1$ má čtyři (mod 8) nekongruentní kořeny 1, 3, 5, 7.

Je-li $f(x) \equiv g(x)\, h(x) \pmod{p}$, *kdež* $f(x)$, $g(x)$, $h(x)$ *jsou mnohočleny s celými koeficienty, pak je každý kořen* $f(x)$ (*mod* p) *kořenem aspoň jednoho z mnohočlenů* $g(x)$ *a* $h(x)$.

Platí-li pro celé číslo α: $f(\alpha) \equiv 0 \pmod{p}$, je $g(\alpha)\, h(\alpha) \equiv f(\alpha) \equiv 0 \pmod{p}$, tedy buď $g(\alpha) \equiv 0 \pmod{p}$ neb $h(\alpha) \equiv 0 \pmod{p}$ neb obojí (§ 20, 5., str. 32), jak bylo dokázati.

Je-li modul číslo složené, tu věta opět neplatí.

Tak je na př. $x^2 \equiv (x-2)(x-2) \pmod{4}$. 4 je kořenem mnohočlenu x^2 (mod 4), nikoliv však kořenem $x - 2 \pmod{4}$.

Platí-li pro mnohočleny s celými koeficienty $g(x)$, $h(x)$ *identicky* $g(x)\, h(x) \equiv 0$ (*mod* p), *pak je identicky buď* $g(x) \equiv 0$ (*mod* p) *neb* $h(x) \equiv 0$ (*mod* p) *neb obojí.*

Dejme tomu, že by věta neplatila. Že by tedy nebylo ani $g(x)$ ani $h(x) \equiv 0 \pmod{p}$ identicky. Vynechme v $g(x)$ a $h(x)$ členy dělitelné p. Dostaneme tak mnohočleny $g_1(x)$, $h_1(x)$,

$$g_1(x) = b_0 + b_1 x + \ldots + b_k x^k, \quad k \geqq 0,$$
$$h_1(x) = c_0 + c_1 x + \ldots + c_l x^l, \quad l \geqq 0,$$

kdež b_k, c_l jsou čísla nedělitelná p. I bylo by $g(x) \equiv g_1(x)$, $h(x) \equiv h_1(x) \pmod{p}$ identicky. Ježto pak $g(x)\, h(x) \equiv 0 \pmod{p}$, bylo by i $g_1(x)\, h_1(x) \equiv 0 \pmod{p}$, v obojím případě identicky. Z této kongruence by plynulo $b_k c_l \equiv 0 \pmod{p}$, což není možno. Je tedy předpoklad, že věta neplatí, nemožný, a tudíž věta uvedená správná.

Mnohočlen s celými koeficienty nazývá se **primitivní**, jsou-li jeho koeficienty nesoudělné, platí-li tedy $f(x) \not\equiv 0 \pmod{p}$ identicky, ať je p jakékoliv prvočíslo.

I platí věta:

Součin dvou mnohočlenů primitivních je zase mnohočlen primitivní.

§ 34. Věta Wilsonova.

Je-li p prvočíslo je $(p-1)! + 1 \equiv 0 \pmod{p}$.

Uvažujme mnohočlen $f(x) = (x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1}-1)$. Ten má, jak plyne z věty Fermatovy, $p-1$ kořenů spolu nekongruentních

$$1, 2, 3, \ldots, p-1.$$

Člen stupně $p-1$ se ruší, je to tedy mnohočlen stupně $< p-1$. Platí tedy $f(x) \equiv 0 \pmod{p}$ identicky, t. j. všechny jeho koeficienty jsou $\equiv 0 \pmod{p}$. Prostý člen poskytuje

$$1 \cdot 2 \cdot 3 \ldots (p-1) + 1 \equiv 0 \pmod{p},$$
$$\text{t. j. } (p-1)! + 1 \equiv 0 \pmod{p},$$

jak bylo dokázati.

$(p-1)! + 1 \equiv 0 \pmod{p}$ je však pro celá čísla kladná p také podmínkou nutnou, má-li býti p prvočíslem. Je-li totiž p dělitelno celým prvočíslem $q < p$, je $(p-1)!$ dělitelno q, takže $(p-1)! + 1$ není dělitelno q, tedy ani p.

Větu Wilsonovu možno dokázati též takto: Je-li x číslo se soustavy $1, 2, 3, \ldots p-1$, lze najíti k x jediné číslo z téže soustavy té vlastnosti, že $xy \equiv 1 \pmod{p}$. (Viz § 23.)

x může býti $= y$ jen v případě $x = 1$ neb $x = p-1$, ježto pak x nutně hoví kongruenci $x^2 \equiv 1 \pmod{p}$. Viz větu v § 33 str. 49. Vidíme tedy, že pro $p > 3$ čísla $2, 3, \ldots p-2$ rozpadají se na $P = \frac{1}{2}(p-3)$ dvojic

$$x_1, y_1;\ x_2, y_2;\ \ldots x_P, y_P,$$

pro které platí

$$x_1 y_1 \equiv 1,\ x_2 y_2 \equiv 1, \ldots, x_P y_P \equiv 1 \pmod{p}$$

$x_1, y_1, x_2, y_2, \ldots, x_P, y_P$ jsou tedy až snad na pořádek čísla $2, 3, \ldots, p-2$.

Je pak $x_1 y_1 x_2 y_2 \ldots x_P p_P \equiv 1 \pmod{p}$, t. j. $2, 3, \ldots (p-2) \equiv 1 \pmod{p}$ a násobíme-li $p-1 \equiv -1 \pmod{p}$, dostaneme

$$(p-1)! \equiv -1 \pmod{p}.$$

Pro $p = 2$ a $p = 3$ platí tato kongruence samozřejmě.

§ 35. Budiž m číslo celé $\neq 0$, a nesoudělné s m. Pak existují čísla celá kladná f té vlastnosti, že $a^f \equiv 1 \pmod{m}$.

Takovým číslem je na př. $f = \varphi(m)$. Mezi těmito čísly celými kladnými je jisté nejmenší. Je-li f nejmenší číslo celé kladné té

vlastnosti, že platí $a^f \equiv 1 \pmod m$, říká se, že a **přísluší (patří)** (mod m) k **mocniteli** f.

Je-li q číslo celé $\geqq 0$, je $a^{qf} \equiv 1 \pmod m$. Platí však věta:

Mocnitel celý kladný k, té vlastnosti, že platí $a^k \equiv 1 \pmod m$, je násobkem mocnitele f, k němuž přísluší a (mod m).

Jistě je $k \geqq f$, sice by a nepatřilo k f (mod m). Lze tedy klásti $k = qf + f'$, kdež q, f' jsou čísla celá, $0 \leqq f' < f$. Pak $a^k = a^{qf}a^{f'} \equiv 1$ (mod m) a tedy $a^{f'} \equiv 1 \pmod m$. Kdyby bylo $f' \neq 0$, nepatřilo by a k f (mod m). Je tedy nutně $f' = 0$, $k = qf$, j. b. d.

Ježto je $a^{\varphi(m)} \equiv 1 \pmod m$, je $\varphi(m)$ *násobkem mocnitele f, k němuž a přísluší (mod m).*

Předpokládejme dále, že m je liché prvočíslo $= p$. Pak je $\varphi(p) = p - 1$. Mocnitel f, k němuž přísluší číslo celé a neděliteln é p, je dělitelem $p - 1$.

Dokážeme, že skutečně *ke každému děliteli $d > 0$ čísla $p - 1$ přísluší jisté číslo celé (mod p), a určíme, že počet těchto čísel je $\varphi(d)$.*

Každé číslo příslušné (mod p) k mocniteli d vyhovuje kongruenci

$$x^d - 1 \equiv 0 \pmod p. \tag{1}$$

Předpokládejme, že takové číslo a příslušné k d (mod p) existuje. Pak čísla

$$1, a, a^2, a^3, \ldots, a^{d-1} \tag{2}$$

vyhovují kongruenci (1) a jsou mezi sebou nekongruentní mod p.

Kdyby totiž bylo $a^k \equiv a^h \pmod p$, kdež h, k značí čísla celá $0 \leqq h < k < d$, platilo by $a^{k-h}(a^h - 1) \equiv 0 \pmod p$. Avšak a^{k-h} jest nesoudělné s p a $a^h \not\equiv 1 \pmod p$, protože a patří k exponentu d. Představují tedy (2) všechna řešení nekongruentní mod p kongruence (1), která má totiž nanejvýš d spolu nekongruentních řešení. Viz § 33 str. 49.

Platí tedy věta:

Každé číslo, které patří k mocniteli d (mod p), je kongruentní (mod p) s některým z čísel (2).

Dále platí věta:

Je-li $\delta > 0$ n. s. d. čísel m a d (m celé číslo kladné), patří a^m k mocniteli d/δ (mod p).

Nechť je $m = \delta m'$, $d = \delta d'$; m', d' jsou nesoudělná; pak je

$$(a^m)^{d'} = a^{\delta m' d'} = a^{dm'} \equiv 1 \pmod p, \text{ t. j. } (a^m)^{d/\delta} \equiv 1 \pmod p.$$

Je tedy mocnitel d_0, k němuž patří a^m (mod p), dělitelem čísla $d/\delta = d'$. Položme tedy

$$d' = kd_0 \quad (k \text{ celé kladné}). \tag{3}$$

I bude $d = k\delta d_0$. Na druhé straně plyne z $(a^m)^{d_0} \equiv 1 \pmod p$, t. j. $a^{md_0} \equiv a^{m'\delta d_0} \equiv 1 \pmod p$, že $m'\delta d_0$ je násobek $d = k\delta d_0$, tedy m' je násobek k,

$$m' = kl \ (l \text{ celé kladné}). \tag{4}$$

Z (3) a (4) plyne, ježto d' a m' jsou čísla spolu nesoudělná, že $k = 1$. Je tedy skutečně mocnitel d_0, k němuž patří $a^m \pmod p$, $d_0 = d' = d/\delta$. Pro $\delta = 1$, $d_0 = d$ dostáváme větu:

Je-li a číslo příslušné (mod p) k mocniteli d, obdržíme všechna čísla mezi sebou nekongruentní (mod p), která též přísluší (mod p) k mocniteli d ve tvaru a^m, kdež je m číslo celé nesoudělné s d.

Existují-li tedy k dělitelům $d > 0$ čísla $p - 1$ vůbec čísla a, která k nim patří (mod p), je jich na počet $\varphi(d)$. Mohou tedy nastati jen dvě možnosti: Buď není žádné číslo příslušné k d (mod p) nebo je jich na počet $\varphi(d)$. Označíme-li $\psi(d)$ počet čísel příslušných k mocniteli d (mod p), je $\psi(d) = \varphi(d)$, neb $= 0$.

Buďtež $d_1, d_2, \ldots, d_\nu$ všichni celí kladní dělitelé čísla $p-1$. Každé z čísel mezi sebou nesoudělných $1, 2, \ldots, p-1$ přísluší (mod p) k některému z čísel d_i jako mocniteli, takže

$$\psi(d_1) + \psi(d_2) + \ldots + \psi(d_\nu) = p - 1.$$

Na druhé straně víme z § 31, že platí

$$\varphi(d_1) + \varphi(d_2) + \ldots + \varphi(d_\nu) = p - 1,$$

tedy $(\varphi(d_1) - \psi(d_1)) + \varphi(d_2) - \psi(d_2) + \ldots + \varphi(d_\nu) - \psi(d_\nu) = 0.$

Ježto $\varphi(d_\nu) - \psi(d_\nu) \geqq 0$, musí býti $\varphi(d_\nu) - \psi(d_\nu) = 0$, t. j. $\psi(d) = \varphi(d)$. I máme větu:

Ke každému celému kladnému děliteli d čísla $p - 1$ existuje $\varphi(d)$ čísel, k nimž tento dělitel patří (mod p).

Zvláštní význam mají čísla příslušná (mod p) k mocniteli $p-1$. Nazývají se primitivní kořeny (mod p). Je jich na počet $\varphi(p-1)$ mezi sebou nekongruentních.

Značí-li g libovolný primitivní kořen (mod p), jsou mocniny

$$g^0 = 1, \ g, g^2, \ldots, g^{p-2}$$

spolu nekongruentní (mod p) a představují tudíž redukovanou soustavu zbytků mod p. Z toho plyne, že pro číslo celé r nedělitelné p platí $r \equiv g^i \pmod p$, kdež i je číslo celé $0 \leqq i \leqq p - 2$.

i nazývá se indexem čísla r při basi g, $i = \mathrm{ind}_g r$, neb stručněji $i = \mathrm{ind}\, r$, budeme-li uvažovati indexy o téže basi.

Patrně je $\mathrm{ind}_g 1 = 0$ pro každý primitivní kořen g.

Z $g^{p-1}-1=(g^{\frac{1}{2}(p-1)}-1)(g^{\frac{1}{2}(p-1)}+1)\equiv 0 \pmod p$ plyne, ježto není $g^{\frac{1}{2}(p-1)}\equiv 1 \pmod p$, že $g^{\frac{1}{2}(p-1)}\equiv -1 \pmod p$, tedy

$$\operatorname{ind}(-1)=\operatorname{ind}(p-1)=\tfrac{1}{2}(p-1).$$

Pro indexy platí věty analogické větám o logaritmech.

Značí-li r, r' dvě čísla celá nedělitelná p, je

$$\operatorname{ind} rr' \equiv \operatorname{ind} r + \operatorname{ind} r' \pmod{p-1}.$$

Je totiž $r\equiv g^{\operatorname{ind} r}$, $r'\equiv g^{\operatorname{ind} r'} \pmod p$, tedy $rr'\equiv g^{\operatorname{ind} r+\operatorname{ind} r'} \pmod p$. Je však též $rr'\equiv g^{\operatorname{ind} rr'} \pmod p$, takže

$$g^{\operatorname{ind} rr'}\equiv g^{\operatorname{ind} r+\operatorname{ind} r'} \pmod p. \qquad (*)$$

Z kongruence $g^m\equiv g^n \pmod p$ plyne, je-li na př. $m\geqq n$, $g^{m-n}\equiv 1 \pmod p$, tedy je $m-n$ dělitelno $p-1$, t. j. $m\equiv n \pmod{p-1}$.

Plyne tedy z (*) vztah, který jsme chtěli dokázati.

Zcela podobně je $\operatorname{ind} r^n \equiv n \operatorname{ind} r \pmod{p-1}$, n číslo celé $\geqq 0$.

Uveďme ještě vztah mezi indexy pro různé base.

Nechť je $r\equiv g^i \pmod p$ a též $r\equiv \gamma^{i'} \pmod p$, kdež γ je opět primitivní kořen (mod p), $0\leqq i'\leqq p-1$, $i=\operatorname{ind}_g r$, $i'=\operatorname{ind}_\gamma r$. γ, ježto není dělitelno p, má index (mod p) vzhledem ke g, $c=\operatorname{ind}_g \gamma$, takže $\gamma\equiv g^c \pmod p$. I bude $r\equiv g^{ci'} \pmod p$, tedy $g^i\equiv g^{ci'} \pmod p$, t. j. $i\equiv ci' \pmod{p-1}$, $\operatorname{ind}_g r\equiv \operatorname{ind}_g \gamma \operatorname{ind}_\gamma r \pmod{p-1}$. Zvolíme-li $r=g$, dostaneme $\operatorname{ind}_g \gamma \,.\, \operatorname{ind}_\gamma g\equiv 1 \pmod{p-1}$.

Primitivní kořen v případě, že modul m je číslo složené, je číslo příslušné (mod m) k mocniteli $\varphi(m)$.

Pro každé m neexistuje primitivní kořen.

Podle věty Fermatovy platí pro číslo celé a nesoudělné s 3 a 7 kongruence $a^6\equiv 1$ (mod 3) i (mod 7), tedy též (mod 21). Pro $m=21$ je tudíž 6 největší mocnitel, k němuž může a (mod 21) příslušeti; naproti tomu je $\varphi(21)=12$.

K vůli úplnosti podotýkám, že primitivní kořeny existují pro $m=p^n$ a $m=2p^n$, kdež p je liché prvočíslo, n číslo celé kladné a pro $m=2$, $m=4$.

K určení indexu čísla při daném p (pro určité g) a k určení čísla k indexu lze užíti tabulek.*)

Pomocí takových tabulek lze snadno řešiti kongruenci

$$ax\equiv b \pmod p.$$

*) Tabulku indexů pro prvočísla <1000 podal Jacobi, Canon arithmeticus, Berlin 1839 (errata Cunningham, Mess. of Math. 46, 1916, str. 57—59, 67, 68). Kraitchik *2.* I str. 131—145 udává primitivní kořen pro prvočíslo $\leqq 27457$; tamtéž řada tabulek podobného obsahu. Menší tabulky obsahuje Wertheim *2.*

Tak na př. pro $p = 17$ je primitivní kořen 3. Volme za basi $g = 3$.

I odpovídají

číslům	indexům	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
indexy		16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
	čísla	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Z kongruence

$$8x \equiv 13 \pmod{17}$$

by plynulo

$$\begin{aligned} \text{ind } 8 + \text{ind } x &\equiv \text{ind } 13 \pmod{16} \\ 10 + \text{ind } x &\equiv 4 \pmod{16} \\ \text{ind } x &\equiv -6 \equiv 10 \pmod{16} \\ x &\equiv 8 \pmod{17}. \end{aligned}$$

III. g-adické zlomky.

§ 36. Budiž g číslo celé > 1. Zlomkem g-adickým (zlomkem systematickým o základu g) nazývá se řada

$$a_0 + \frac{a_1}{g} + \frac{a_2}{g^2} + \ldots + \frac{a_n}{g^n} + \ldots, \qquad (1)$$

kdež $a_0, a_1, a_2, \ldots, a_n, \ldots$ jsou čísla celá, a_0 libovolné, $0 \leqq a_n < g$ pro $n \geqq 1$; a_n je pro $n \geqq 1$ „g-adická číslice".

Zlomek (1) bude konečný, budou-li všechna $a_n = 0$ jistým n počínajíc, nekonečný, bude-li pro nekonečně mnoho ν platiti $a_\nu \neq 0$. Zlomek g-adický budeme též psáti $a_0 + 0, a_1 a_2 a_3, \ldots$, neb, je-li $a_0 > 0$, $a_0, a_1 a_2 a_3 \ldots$ a g-adický zlomek konečný

$$a_0 + 0, a_1 a_2 a_3 \ldots a_h \text{ resp. } a_0, a_1 a_2 a_3 \ldots a_h.$$

Zlomek g-adický

$$a_0 + 0, a_1 a_2 \ldots a_h a_{h+1} \ldots a_{h+f} a_{h+1} \ldots a_{h+f} \ldots a_{h+1} \ldots a_{h+f} \ldots,$$

v němž tedy od jistého místa počínajíc se stále opakuje skupina číslic

$$a_{h+1}\, a_{h+2} \ldots a_{h+f},$$

nazývá se periodický. Platí tedy pro číslice zlomku periodického $a_l = a_k$ pro $l \equiv k \pmod{f}$; k, l, f jsou čísla celá kladná, pro něž platí $k, l > h$. Skupina číslic, které se opakují, $a_{h+1}, a_{h+2}, \ldots \ldots, a_{h+f}$, nazývá se perioda. Při $h = 0$ zlomek

$$a_0 + 0, a_1 a_2 \ldots a_f a_1 a_2 \ldots a_f \ldots a_1 a_2 \ldots a_f \ldots$$

nazývá se ryze periodický, při $h > 0$ neryze periodický. Zlomek konečný můžeme považovati za nekonečný zlomek o periodě 0.

Zlomek g-adický periodický $a_0 + 0, a_1 a_2 \ldots a_h a_{h+1} \ldots \ldots a_{h+f} a_{h+1} \ldots a_{h+f} \ldots$ se také kratčeji psává ve tvaru $a_0 + 0, a_1 a_2 \ldots a_h \dot{a}_{h+1} \ldots \dot{a}_{h+f}$.

Řada (1) konverguje a její součet α nazývá se hodnotou zlomku g-adického (1). Konvergence ta je jednoduchým důsledkem té okolnosti, že lze určiti dvě posloupnosti, jednu neklesající,

druhou nestoupající, které mají α za společnou limitu. Položme totiž

$$A_n = a_0 + \frac{a_1}{g} + \frac{a_2}{g^2} + \ldots + \frac{a_n}{g^n},\ \bar{A}_n = A_n + \frac{1}{g^n},\ n = 0, 1, 2, \ldots;$$

i bude

$$A_{n+1} = A_n + \frac{a_{n+1}}{g^{n+1}},\ \bar{A}_{n+1} = A_n + \frac{a_{n+1}+1}{g^{n+1}} =$$

$$= \bar{A}_n - \frac{g - (a_{n+1}+1)}{g^{n+1}}$$

a z toho plyne

$$A_n \leqq A_{n+1} < \bar{A}_{n+1} \leqq \bar{A}_n \tag{2}$$

$$\bar{A}_n - A_n = \frac{1}{g^n}. \tag{3}$$

Čísla $A_1, A_2, A_3, \ldots$ tvoří podle (2) posloupnost neklesající ohraničenou; tato má tedy limitu, a ta je právě α. $\bar{A}_1, \bar{A}_2, \bar{A}_3, \ldots$ tvoří posloupnost nestoupající ohraničenou, která na základě (3) má opět limitu α. Bude pak platiti

$$A_n \leqq \alpha \leqq \bar{A}_n.$$

A_n jsou přibližné hodnoty dolní, $\bar{A}_n$ přibližné hodnoty horní pro α. Pro $n = 0$ bude

$$a_0 \leqq \alpha \leqq a_0 + 1. \tag{4}$$

§ 37. Budiž α libovolné číslo reální; položme $\alpha = a_0 + \alpha_0$, kdež $a_0 = [\alpha]$, takže $0 \leqq \alpha_0 < 1$. Klaďme dále $g\alpha_0 = a_1 + \alpha_1$, kdež $a_1 = [g\alpha_0]$, takže bude $0 \leqq \alpha_1 < 1$, $g\alpha_1 = a_2 + \alpha_2$, kdež $a_2 = [g\alpha_1]$, takže $0 \leqq \alpha_2 < 1$. Takovým způsobem můžeme dále pokračovati a dostaneme obecně, klademe-li

$$g\alpha_{n-1} = a_n + \alpha_n, \tag{1}$$

kdež $a_n = [g\alpha_{n-1}]$, že o α_n platí

$$0 \leqq \alpha_n < 1. \tag{2}$$

Tento postup nazveme g-adickým algoritmem prvního druhu. Postup ten přiřaďuje číslu reálnímu α posloupnost čísel celých $a_0, a_1, a_2, \ldots$. Při tom $a_1, a_2, \ldots$ jsou g-adické číslice. Z $0 \leqq \alpha_n < 1$ plyne totiž $0 \leqq g\alpha_n < g$, tedy $0 \leqq [g\alpha_n] < g$, t. j. $0 \leqq a_{n+1} < g$ pro $n \geqq 0$. O a_0 to ovšem platiti nemusí; je to libovolné číslo celé.

g-adický algoritmus prvního druhu přiřaďuje číslu reálnímu α zlomek g-adický $a_0 + a_1/g + a_2/g^2 + \ldots$. Lze snadno dokázati, že jeho hodnota je α. Je totiž $\alpha = a_0 + a_1/g + a_2/g^2 + \ldots + a_n/g^n +$

$+\alpha_n/g^n$; necháme-li pak n růsti do nekonečna, bude $\lim_{n\to\infty} \alpha_n/g^n = 0$ na základě (2), z čehož tvrzení ihned plyne.

Lze snadno nahlédnouti, že pomocí g-adického algoritmu prvního druhu nelze z žádného čísla reálního obdržeti zlomek o periodě $g-1$, t. j. zlomek, u něhož od jistého n počínajíc je stále $a_n = g-1$. Dejme tomu, že by pro $n > h$ bylo stále $a_n = g-1$. Z (1) by plynulo $g\alpha_n = g - 1 + \alpha_{n+1}$, t. j.

$$1 - \alpha_n = \frac{1-\alpha_{n+1}}{g} = \frac{1-\alpha_{n+2}}{g^2} = \ldots = \frac{1-\alpha_{n+\nu}}{g^\nu}$$

$$\text{pro } n > h, \quad \nu > 0.$$

Bylo by tedy $1 - \alpha_n \leqq 1/g^\nu$, a necháme-li ν růsti do nekonečna, $1 - \alpha_n \leqq 0$, t. j. $\alpha_n \geqq 1$ pro $n > h$, což odporuje podmínce (2).

Dalšího omezení není třeba. Platí totiž věta:

Každé číslo reální α lze jediným způsobem znázorniti g-adickým zlomkem

$$a_0 + \frac{a_1}{g} + \frac{a_2}{g^2} + \ldots, \tag{3}$$

pro který platí

$$a_\nu < g - 1 \tag{4}$$

pro nekonečně mnoho ν, takže zlomek ten nemá periodu $g-1$; a_n lze nalézti z α pomocí g-adického algoritmu prvního druhu.

Že jedno takové znázornění existuje, právě jsme dokázali: je to zlomek g-adický vzniklý z α pomocí g-adického algoritmu prvního druhu. Bude tedy věta zcela dokázána, ukážeme-li, že každý zlomek g-adický (3), o němž platí (4), má za hodnotu číslo reální α, z něhož užitím g-adického algoritmu prvního druhu dostaneme právě čísla $a_0, a_1, a_2, \ldots$.

Položme

$$\alpha_n = \frac{a_{n+1}}{g} + \frac{a_{n+2}}{g^2} + \ldots \tag{5}$$

I bude podle (4) § 36 $0 \leqq \alpha_n \leqq 1$ pro $n \geqq 0$. Dokážeme, že není možno, aby $\alpha_n = 1$. Ať je n jakkoliv veliké, bude aspoň pro jedno $\nu > n$ platiti $a_\nu \leqq g-2$. Číslo $\alpha_n + 1/g^\nu$ bude vyjádřeno zlomkem g-adickým, který vznikne z α_n, dáme-li místo a_ν číslici $a_\nu + 1$. I bude zase $\alpha_n + 1/g^\nu \leqq 1$, t. j. $\alpha_n \leqq 1 - 1/g^\nu < 1$ pro každé n. Platí tedy $0 \leqq \alpha_n < 1$ pro $n \geqq 0$. Je však podle (5) $g\alpha_{n-1} = a_n + \alpha_n$, takže $a_n = [g\alpha_{n-1}]$.

§ 38. Můžeme však k rozvoji čísla reálního α ve zlomek g-adický dojíti též, užíváme-li operace $[\,]'$. (Viz § 2 str. 8.)

$$\begin{aligned} \text{Položme } \alpha &= a_0 + \alpha_0, \quad \text{kdež } a_0 = [\alpha]', \quad \text{t. j. } 0 < \alpha_0 \leqq 1, \\ g\alpha_0 &= a_1 + \alpha_1, \quad \text{kdež } a_1 = [g\alpha_0]', \text{ t. j. } 0 < \alpha_1 \leqq 1, \\ g\alpha_1 &= a_2 + \alpha_2, \quad \text{kdež } a_2 = [g\alpha_1]', \text{ t. j. } 0 < \alpha_2 \leqq 1, \\ &\ldots\ldots\ldots\ldots \\ g\alpha_{n-1} &= a_n + \alpha_n, \quad \text{kdež } a_n = [g\alpha_{n-1}]', \qquad (1) \\ &\text{t. j. } 0 < \alpha_n \leqq 1. \qquad (2) \end{aligned}$$

Tento postup nazveme g-adickým algoritmem druhého druhu. Z $0 < \alpha_n \leqq 1$ plyne $0 < g\alpha_n \leqq g$ a tedy zase $0 \leqq a_{n+1} < g$ pro $n \geqq 0$. Čísla $a_1, a_2, a_3, \ldots$ jsou g-adické číslice. g-adický algoritmus druhého druhu přiřaďuje zase číslu reálnímu α zlomek g-adický $a_0 + a_1/g + a_2/g^2 + \ldots$, jehož hodnota je opět α.

Lze snadno nahlédnouti, že existují zlomky g-adické, které nemohou vzniknouti z čísla reálného g-adickým algoritmem druhého druhu. Jsou to g-adické zlomky konečné. Je-li totiž $a_n = 0$ pro $n > h$, pak $g\alpha_n = \alpha_{n+1}$ pro $n > h$, tedy $\alpha_n = \alpha_{n+1}/g = \alpha_{n+2}/g^2 = \ldots = \alpha_{n+r}/g^r$ pro $n > h$, $r \geqq 1$. Nechme r růsti do nekonečna. I bude $\alpha_n = 0$ pro $n > h$, takže nemůže býti $\alpha_n > 0$.

Nyní platí věta:

Každé číslo reální α lze jediným způsobem znázorniti nekonečným zlomkem g-adickým

$$a_0 + a_1/g + a_2/g^2 + \ldots, \qquad (3)$$

při čemž a_n lze ustanoviti z α pomocí g-adického algoritmu druhého druhu.

Právě jsme dokázali, že existuje aspoň jedno takové znázornění. Věta pak bude úplně dokázána, dokážeme-li, že každý zlomek g-adický nekonečný (3) má za hodnotu číslo reální α, z něhož pomocí g-adického algoritmu druhého druhu dostaneme právě čísla $a_0, a_1, a_2, \ldots$

Položme $\alpha_n = a_{n+1}/g + a_{n+2}/g^2 + \ldots$ I bude podle (4) z § 36, ježto (3) je zlomek nekonečný, $0 < \alpha_n \leqq 1$ pro $n \geqq 0$. Ježto $g\alpha_{n-1} = a_n + \alpha_n$, bude $a_n = [g\alpha_{n-1}]'$.

Není-li x číslo celé, je $[x] = [x]'$. Nebude-li tedy žádné z čísel $\alpha, g\alpha_0, g\alpha_1, \ldots$ celé, budou se oba algoritmy g-adické ztotožňovati a bude stále $0 < \alpha_n < 1$.

Nechť je $g\alpha_{h-1}$ první celé číslo v řadě $g\alpha_0, g\alpha_1, \ldots$ I bude podle algoritmu prvního druhu $a_h = g\alpha_{h-1}$, $\alpha_h = 0$, a dále $a_n = 0$ pro $n > h$, $\alpha_n = 0$ pro $n \geqq h$. Algoritm prvního druhu poskytne konečný zlomek g-adický

$$\alpha = a_0 + 0,\ a_1 a_2 \ldots a_h.$$

Podle algoritmu druhého druhu bude $a'_h = g a_{h-1} - 1 = a_h - 1$, $a'_h = 1$, a dále $a'_n = g - 1$ pro $n > h$, $a'_n = 1$ pro $n \geqq h$.

Algoritm druhého druhu dává zlomek g-adický o periodě $g - 1$

$$\alpha = a_0 + 0,\ a_1 a_2 \ldots \overline{a_h - 1\ g - 1\ g - 1} \ldots$$

(Pro případ, že by α bylo číslo celé, dostaneme tak

$$\alpha = \alpha - 1,\ g - \overline{1\ g - 1\ g - 1} \ldots).$$

§ 39. Je-li α číslo racionální vyjadřitelné redukovaným zlomkem $\alpha = r/m$, $m > 0$, klaďme $a_n = r_n/m$, $n = 0, 1, 2, \ldots$

Budeme uvažovati pouze algoritm prvního druhu, ježto v případě, kde oba algoritmy poskytují různé výsledky, lze k algoritmu druhého druhu snadno přejíti.

I dostaneme:

$$\begin{aligned}
r &= a_0 m + r_0, & a_0 &= \left[\frac{r}{m}\right], & 0 \leqq r_0 < m \\
g r_0 &= a_1 m + r_1, & a_1 &= \left[\frac{g r_0}{m}\right], & 0 \leqq r_1 < m \\
g r_1 &= a_2 m + r_2, & a_2 &= \left[\frac{g r_1}{m}\right], & 0 \leqq r_2 < m \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
g r_{n-1} &= a_n m + r_n, & a_n &= \left[\frac{g r_{n-1}}{m}\right], & 0 \leqq r_n < m.
\end{aligned}$$

Čísla $r_0, r_1, r_2, \ldots$ jsou vesměs celá, r_0 nesoudělné s m. I bude $r/m = a_0 + 0, a_1 a_2 \ldots$ a tento zlomek g-adický nebude míti periodu $g - 1$.

Pro r_n/m platí $r_n/m = 0, a_{n+1} a_{n+2} \ldots$ Zlomky ty jsou vesměs ryzí. Takových zlomků je však na počet m, musí se tedy opakovati. Nechť jsou r_h/m a r_{h+f}/m první z řady těchto ryzích zlomků, které se sobě rovnají,

$$r_h/m = r_{h+f}/m. \tag{1}$$

Pak jest

$$0,\ a_{h+1}\ a_{h+2} \ldots = 0,\ a_{h+f+1}\ a_{h+f+2} \ldots$$

Z jednoznačnosti znázornění g-adickými zlomky uvedeného tvaru bude nutně plynouti $a_{h+1} = a_{h+f+1}$, $a_{h+2} = a_{h+f+2} \ldots$, t. j. pro $n > h$ bude

$$a_n = a_{n+f}. \tag{2}$$

h, f jsou nejmenší celá čísla $h \geqq 0$, $f \geqq 1$ té vlastnosti, že pro

každé číslo celé $n > h$ platí (2). Kdyby analogické relace platily již pro $\bar{h}<h, \bar{f}<f$, bylo by již $r_{\bar{h}}/m = r_{\bar{h}+\bar{f}}/m$, takže by zlomky (1) nebyly první, které v řadě r_n/m $(n \geqq 0)$ jsou si rovny.

I platí věta:

Každé racionální číslo lze rozvinouti v g-adický zlomek periodický.

Počet číslic před periodou h a délku periody lze snadno u zlomku r/m ustanoviti. Zjistíme, že závisí jen na m a g, nikoliv však na r. Je-li $r/m = a_0 + 0, a_1 a_2 \ldots a_h a_{h+1} \ldots, a_{h+f}$, budou zlomky $g^h \frac{r}{m}$ a $g^{h+f} \frac{r}{m}$ první z řady $g^n \frac{r}{m}$, $n \geqq 0$, jejichž rozdíl bude číslo celé, t. j. kdy $g^h (g^f - 1) \frac{r}{m}$ bude číslo celé. Ježto je r nesoudělné s m, bude odtud plynouti, že h, f jsou nejmenší čísla celá, $h \geqq 0$, $f \geqq 1$, pro něž platí

$$g^h (g^f - 1) \equiv 0 \pmod{m}. \tag{3}$$

Těmito podmínkami jsou h a f jednoznačně určeny.

Obsahuje-li nejprve m tytéž prvočinitele jako g, je $g^f - 1$ pro $f \geqq 1$ nesoudělné s m. Je tedy $f = 1$ a h je nejmenší celý mocnitel $\geqq 0$, pro který je

$$g^h \equiv 0 \pmod{m}. \tag{4}$$

Nechť je rozklad čísel g a m v prvočinitele

$$g = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\mu^{\alpha_\mu}, \quad m = p_1^{\beta_1} p_2^{\beta_2} \ldots p_\mu^{\beta_\mu},$$

kdež α_i i β_i jsou čísla celá, $\alpha_i > 0$, $\beta_i \geqq 0$. g^h bude nejnižší mocnina g dělitelná m, je-li h nejmenší číslo celé kladné, pro něž $h\alpha_i \geqq \beta_i$, t. j. $h \geqq \beta_i/\alpha_i$ pro všechna $i = 1, 2, \ldots \mu$.

Zde $r_0/m = 0, a_1 a_2 \ldots a_h a_{h+1} a_{h+2} \ldots$, $g^h r_0/m = a_1 a_2 \ldots a_h, a_{h+1} a_{h+2} \ldots$, kdež $a_1 a_2 \ldots a_h$ je číslo celé $\geqq 0$ psané v soustavě g-adické (§ 2 str. 9). Toto číslo má býti vzhledem ke kongruenci (4) číslo celé. Musí tedy býti $a_{h+1} = a_{h+2} = \ldots = 0$. V tomto případě je zlomek g-adický pro r/m konečný. Počet jeho číslic za čárkou, h, je nejmenší číslo celé $\geqq 0$ hovící kongruenci (4). Tento konečný zlomek g-adický dostaneme pomocí algoritmu prvního druhu. Algoritm druhého druhu poskytl by zlomek g-adický o h číslicích před jednočlennou periodou $g - 1$.

Je-li na druhé straně m nesoudělné s g, platí kongruence (3) tehdy a jen tehdy, je-li

$$g^f \equiv 1 \pmod{m}. \tag{5}$$

I je $h = 0$ a f je nejmenší mocnitel, pro který platí (5), t. j. mocnitel, ke kterému patří g (mod m). (Viz § 35).

Zlomky r/m, jejichž čitatel je nesoudělný s g, dávají zlomky g-adické ryze periodické a počet číslic v periodě je roven mocniteli f, ke kterému patří g (mod m).

Jsou-li konečně m a g libovolná, lze rozložiti m na dva činitele $m = m_1 m_2$, takže m_1 obsahuje všechny prvočinitele z m, které se vyskytují také v g, a m_2 je nesoudělné s g. Z kongruence (3) plyne podle věty na konci § 19., že h, f jsou nejmenší čísla celá $h \geqq 0$, $f \geqq 1$, pro něž platí kongruence

$$g^h \equiv 0 \pmod{m_1} \tag{6}$$
$$g^f \equiv 1 \pmod{m_2}. \tag{7}$$

V tomto případě je zlomek neryze periodický, počet číslic před periodou h dán je kongruencí (6) a počet číslic v periodě f kongruencí (7).

Ukážeme nyní, že periodický zlomek g-adický je roven číslu racionálnímu. Důkaz stačí provésti pro zlomek

$$\alpha_0 = 0,\ a_1 a_2 \ldots a_h \dot{a}_{h+1} \ldots \dot{a}_{h+f}.$$

I bude

$$g^h \alpha_0 = a_1 a_2 \ldots a_h,\ \dot{a}_{h+1} \ldots \dot{a}_{h+f},$$
$$g^{h+f} \alpha_0 = a_1 a_2 \ldots a_h\, a_{h+1} \ldots a_{h+f},\ \dot{a}_{h+1} \ldots \dot{a}_{h+f},$$

tedy rozdíl

$$g^h (g^f - 1)\, \alpha_0 = a_1 a_2 \ldots a_h a_{h+1} \ldots a_{h+f} - a_1 a_2 \ldots a_h,$$

t. j.

$$\alpha_0 = \frac{a_1 a_2 \ldots a_h\, a_{h+1} \ldots a_{h+f} - a_1 a_2 \ldots a_h}{g^h (g^f - 1)}.$$

Nechť je nyní m nesoudělné s g a nechť g patří k exponentu f (mod m). Zlomek g-adický pro r/m je ryze periodický. Označme jeho periodu $P(r/m)$. I bude

$$P\left(\frac{r}{m}\right) = a_1 a_2 \ldots a_f$$
$$P\left(g\,\frac{r}{m}\right) = a_2 a_3 \ldots a_f a_1$$
$$P\left(g^2 \frac{r}{m}\right) = a_3 a_4 \ldots a_f a_1 a_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$P\left(g^{f-1}\,\frac{r}{m}\right) = a_f\, a_1 a_2 \ldots a_{f-1}.$$

$P\left(g^f \frac{r}{m}\right)$ by bylo zase $= P(r/m)$. $P\left(g^{i+1} \frac{r}{m}\right)$ vznikne z $P\left(g^i \frac{r}{m}\right)$ (i číslo celé $\geqq 0$) cyklickou záměnou. Uvedené periody tvoří tak zvaný cykl period. Ježto $g^f \equiv 1 \pmod m$, je f dělitelem $\varphi(m)$. Je-li tedy $\varphi(m) = ef$, $e > 1$, dlužno utvořiti tyto periody pro e různých hodnot r, abychom dostali periody všech zlomků o jmenovateli m. Je e cyklů period. Je-li $e = 1$, $f = \varphi(m)$, tedy g primitivní kořen (mod m), existuje jen jeden cykl: stačí vzíti za r číslo celé nesoudělné s m (třeba $r = 1$) a dostaneme periody všech zlomků o jmenovateli m z této cyklickou záměnou.

§ 40. Užijeme těchto výsledků k rozvinutí čísla racionálního ve zlomek desetinný, uvažujme tedy případ $g = 10 = 2 \cdot 5$. Redukovaný zlomek, jehož jmenovatel je tvaru $m = 2^{\beta_1} 5^{\beta_2}$ (β_1, β_2 čísla celá $\geqq 0$), dává konečný zlomek desetinný; počet číslic h napravo od desetinné čárky je roven většímu z čísel β_1, β_2.

Redukovaný zlomek lze tehdy a jen tehdy proměniti na desetinný zlomek ryze periodický, není-li jeho jmenovatel dělitelný ani 2 ani 5. Délka periody je rovna exponentu, k němuž patří 10 vzhledem ke jmenovateli jako modulu.

Zlomek $r/2^{\beta_1} 5^{\beta_2} m_2$ je roven neryze periodickému zlomku desetinnému, který má tolik číslic před periodou, kolik udává větší z mocnitelů β_1, β_2 a jenž má délku periody rovnou exponentu, k němuž patří 10 (mod m_2).

Osvětleme věty dříve vyslovené příklady pro zlomky desetinné. Rozveďme $\frac{1}{7}$ v zlomek desetinný. Dělme obyčejným způsobem:

$$
\begin{array}{l}
1_0 : 7 = 0{\cdot}\dot{1}42857\dot{} \\
\quad 3_0 \\
\quad\quad 2_0 \\
\quad\quad\quad 6_0 \\
\quad\quad\quad\quad 4_0 \\
\quad\quad\quad\quad\quad 5_0 \\
\quad\quad\quad\quad\quad\quad 1.
\end{array}
$$

Perioda je zde 142857, čísla 1, 3, 2, 6, 4, 5 jsou zbytky mocnin 10 (mod 7). Číslo 10 je (mod 7) primitivní kořen, periody zlomků o jmenovateli 7 tvoří jediný cykl. Je pak

$$
\begin{array}{ll}
\frac{1}{7} = 0{\cdot}\dot{1}42857\dot{} & \frac{6}{7} = 0{\cdot}\dot{8}57142\dot{} \\
\frac{3}{7} = 0{\cdot}\dot{4}28571\dot{} & \frac{4}{7} = 0{\cdot}\dot{5}71428\dot{} \\
\frac{2}{7} = 0{\cdot}\dot{2}85714\dot{} & \frac{5}{7} = 0{\cdot}\dot{7}14285\dot{}.
\end{array}
$$

Rozveďme nyní $\frac{1}{13}$ ve zlomek desetinný:

$$
\begin{array}{l}
10 : 13 = 0{\cdot}\dot{0}76923\dot{0} \\
100 \\
\ \ 90 \\
\ \ 120 \\
\ \ \ 30 \\
\ \ \ \ 40 \\
\ \ \ \ \ 1.
\end{array}
$$

I dostaneme cykl

$$
\begin{array}{ll}
\frac{1}{13} = 0{\cdot}\dot{0}76923\dot{0} & \frac{12}{13} = 0{\cdot}\dot{9}23076\dot{9} \\
\frac{10}{13} = 0{\cdot}\dot{7}69230\dot{7} & \frac{3}{13} = 0{\cdot}\dot{2}30769\dot{2} \\
\frac{9}{13} = 0{\cdot}\dot{6}92307\dot{6} & \frac{4}{13} = 0{\cdot}\dot{3}07692\dot{3}.
\end{array}
$$

Abychom dostali periody všech zlomků o jmenovateli 13, je třeba rozvésti ve zlomek desetinný ryzí zlomek o jmenovateli 13, který mezi uvedenými není, třeba $\frac{2}{13}$. I dostaneme

$$
\begin{array}{l}
20 : 13 = 0{\cdot}\dot{1}53846\dot{1} \\
\ \ 70 \\
\ \ \ 50 \\
\ \ 110 \\
\ \ \ \ 60 \\
\ \ \ \ \ 80 \\
\ \ \ \ \ \ 2.
\end{array}
$$

Tak dostaneme druhý cykl

$$
\begin{array}{ll}
\frac{2}{13} = 0{\cdot}\dot{1}53846\dot{1} & \frac{11}{13} = 0{\cdot}\dot{8}46153\dot{8} \\
\frac{7}{13} = 0{\cdot}\dot{5}38461\dot{5} & \frac{6}{13} = 0{\cdot}\dot{4}61538\dot{4} \\
\frac{5}{13} = 0{\cdot}\dot{3}84615\dot{3} & \frac{8}{13} = 0{\cdot}\dot{6}15384\dot{6}.
\end{array}
$$

Tím vyčerpány jsou rozvoje všech ryzích zlomků o jmenovateli 13 v zlomky desetinné.

V obou případech, i pro zlomky o jmenovateli 7 i pro zlomky o jmenovateli 13 skládá se perioda ze dvou polovic a číslice jedné poloviny doplňují se s číslicemi druhé poloviny na 9. Říká se, že jedna polovina je desítkovým doplňkem druhé. To nastane, když periody zlomků r/m a $1 - r/m = (m - r)/m$ patří k témuž cyklu. Pak musí býti

$$
\begin{array}{ll}
 & m - r \equiv r\,10^a \pmod{m}, \\
\text{t. j.} & -1 \equiv 10^a \pmod{m}.
\end{array}
$$

Perioda zlomku desetinného pro zlomek o jmenovateli m skládá se ze dvou polovin, které se desítkově doplňují, je-li mezi zbytky mocnin čísla 10 mod m zbytek — 1.

Je-li f délka periody pro jmenovatele m, je $10^f - 1$ dělitelno m. Jsou tedy jmenovatelé m poskytující délku periody f děliteli čísla $10^f - 1$. Naopak je délka periody zlomku, jehož jmenovatel je dělitel $10^f - 1$, buď f neb dělitel f. Zlomků, jejichž rozvoj v desetinný zlomek má danou délku periody f, je konečný počet. Jednočlenné periody dávají zlomky o jmenovatelích 3, 9, dělitelích 9:

$$\tfrac{1}{3} = 0{\cdot}333\ldots, \quad \tfrac{1}{9} = 0{\cdot}111\ldots$$

Dále je $10^2 - 1 = 99 = 9 \,.\, 11$.

Dvojčlenné periody dají zlomky o jmenovatelích 11, 33, 99.

IV. Kvadratické zbytky, kvadratický zákon reciprocity.

§ 41. Budeme uvažovati kongruenci

$$x^2 \equiv a \pmod{p}, \tag{1}$$

kdež a je číslo celé a p liché prvočíslo.

Je-li a dělitelno p, je kongruence (1) splněna pro každé $x \equiv 0 \pmod{p}$. Není-li a dělitelno p a existuje-li číslo celé, hovící kongruenci (1), nazveme a kvadratickým zbytkem (mod p), neexistuje-li pak takové číslo celé, nazveme a kvadratickým nezbytkem (mod p).

Předpokládejme tedy, že a není dělitelno p.

Lze snadno nahlédnouti, že, je-li kongruence (1) řešitelná, má právě dvě spolu (mod p) nekongruentní řešení. Je-li α kořen kongruence (1), tedy $\alpha^2 \equiv a \pmod{p}$, vyhovuje (1) též $x \equiv -\alpha \pmod{p}$, ježto je $(-\alpha)^2 \equiv \alpha^2 \equiv a \pmod{p}$. α a $-\alpha$ nejsou spolu kongruentní (mod p). Z $\alpha \equiv -\alpha \pmod{p}$ by plynulo $2\alpha \equiv 0 \pmod{p}$, $\alpha \equiv 0 \pmod{p}$, tedy i $a \equiv 0 \pmod{p}$ proti předpokladu o a.

Každý zbytek kvadratický je (mod p) kongruentní s jedním z čísel

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Žádná dvě z těchto čísel nejsou spolu kongruentní (mod p). Označíme-li totiž dvě z těch čísel x, y, $x > y$, bylo by pak $x^2 - y^2 = (x+y)(x-y)$ dělitelno p, což není možno, ježto i $x+y$ i $x-y$ jsou čísla celá kladná $< p$.

Platí tedy věta:

Mezi čísly $1, 2, 3, \ldots, p-1$ *redukované soustavy zbytků (mod* p*) je právě* $\frac{1}{2}(p-1)$ *zbytků a stejný počet nezbytků spolu nekongruentních (mod* p*).*

Je-li g primitivní kořen (mod p), tvoří čísla $1, g, g^2, \ldots g^{p-2}$ redukovanou soustavu zbytků (mod p) (§ 35, str. 53). Čísla

$1, g^2, g^4, \ldots, g^{p-3}$ jsou kvadratické zbytky (mod p) spolu nekongruentní (mod p). Ježto je těchto čísel na počet $\frac{1}{2}(p-1)$, jsou jimi všechny kvadratické zbytky (mod p) spolu (mod p) nekongruentní vyčerpány. Čísla $g, g^3, g^5, \ldots, g^{p-2}$ jsou pak spolu (mod p) nekongruentní kvadratické nezbytky (mod p).

Je-li číslo a, nedělitelné p, kvadratickým zbytkem (mod p), existuje číslo celé α té vlastnosti, že pro ně platí $\alpha^2 \equiv a \pmod{p}$. α je opět nedělitelné p. I bude

$$a^{p-1} \equiv a^{\frac{1}{2}(p-1)} \pmod{p},$$

tedy podle věty Fermatovy $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$.

Kongruence $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ má za kořeny $\frac{1}{2}(p-1)$ spolu (mod p) nekongruentních kvadratických zbytků (mod p), a ježto je stupně $\frac{1}{2}(p-1)$, nemá podle věty z § 33 str. 49 jiných kořenů (mod p).

Podle věty Fermatovy má kongruence $x^{p-1} - 1 \equiv 0 \pmod{p}$ za kořeny všechna čísla celá nedělitelná p. Je však $x^{p-1} - 1 = (x^{\frac{1}{2}(p-1)} - 1)(x^{\frac{1}{2}(p-1)} + 1)$. Pro každé číslo celé nedělitelné p je tedy buď $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ anebo $x^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$. Obě tyto kongruence nemohou býti splněny pro totéž číslo x, sice by jejich rozdíl 2 musil býti $\equiv 0 \pmod{p}$, což při $p > 2$ je nemožno. Kongruence $x^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$ má tedy za kořeny kvadratické nezbytky.

Platí tedy věta (Eulerovo kriterium):

Číslo celé a nedělitelné p je kvadratický zbytek, je-li $a^{\frac{1}{2}(p-1)} \equiv 1$ (mod p), kvadratický nezbytek, je-li $a^{\frac{1}{2}(p-1)} \equiv -1$ (mod p).

§ 42. Legendre zavedl jednoduchý symbol na označení kvadratického charakteru čísla celého a nedělitelného prvočíslem $p > 2$, t. j. na označení, zda a je kvadratický zbytek nebo nezbytek (mod p). Klade

$$\left(\frac{a}{p}\right) = 1, \text{ je-li } a \text{ kvadratický zbytek,}$$

$$\left(\frac{a}{p}\right) = -1, \text{ je-li } a \text{ kvadratický nezbytek.}$$

I bude podle Eulerova kriteria $a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

$\left(\frac{a}{p}\right)$ je absolutně nejmenší zbytek (mod p) čísla $a^{\frac{1}{2}(p-1)}$.

Je patrno, že

$$\left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right), \text{ je-li } a' \equiv a \pmod{p}.$$

Je-li totiž $a' \equiv a \pmod{p}$, je též $a'^{\frac{1}{2}(p-1)} \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$ a tedy, ježto

$$a'^{\frac{1}{2}(p-1)} \equiv \left(\frac{a'}{p}\right), \quad a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

též

$$\left(\frac{a'}{p}\right) \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Z této kongruence plyne ihned rovnost $\left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right)$, ježto obě ta čísla jsou absolutně nejmenší zbytky (mod p).

Jsou-li a, a' celá čísla nedělitelná p, je

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a'}{p}\right).$$

Je totiž podle Eulerova kriteria

$$a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \pmod{p}, \quad a'^{\frac{1}{2}(p-1)} \equiv \left(\frac{a'}{p}\right) \pmod{p},$$

$$(aa')^{\frac{1}{2}(p-1)} \equiv \left(\frac{aa'}{p}\right) \pmod{p}.$$

Násobením prvých dvou kongruencí dostaneme

$$(aa')^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{a'}{p}\right) \pmod{p}$$

a tedy

$$\left(\frac{aa'}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right) \pmod{p}.$$

Rovnost odtud plyne jako v předešlém případě.

Z definice Legendreova znaménka plyne ihned, že $\left(\frac{1}{p}\right) = 1$ a obecně $\left(\frac{a^2}{p}\right) = 1$ pro každé celé a nesoudělné s p.

Eulerovo kriterium poskytuje možnost určiti $\left(\frac{-1}{p}\right)$. Je

totiž

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)} \pmod{p},$$

a ježto $(-1)^{\frac{1}{2}(p-1)} = \pm 1$, plyne z této kongruence rovnost $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$.

Je tedy

$$\left(\frac{-1}{p}\right) = 1 \text{ pro } p \equiv 1 \pmod 4,$$

$$\left(\frac{-1}{p}\right) = -1 \text{ pro } p \equiv -1 \pmod 4.$$

§ 43. Budiž p libovolné celé číslo liché kladné a a celé číslo nesoudělné s p. Určeme absolutně nejmenší zbytky (mod p) čísel

$$1 \,.\, a,\ 2 \,.\, a,\ 3 \,.\, a,\ \ldots,\ \pi a,\ \pi = \tfrac{1}{2}(p-1).$$

Ty nechť jsou

$$\varepsilon_1 1',\ \varepsilon_2 2',\ \ldots,\ \varepsilon_\pi \pi',$$

kdež $1', 2', 3', \ldots, \pi'$ jsou absolutní hodnoty těchto zbytků a $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\pi = \pm 1$. Mezi $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\pi$ nechť se vyskytuje μ-krát -1. Je tedy

$$ia \equiv \varepsilon_i i' \pmod p,\quad i = 1, 2, 3, \ldots, \pi. \tag{1}$$

$1', 2', 3', \ldots, \pi'$ jsou, jak lze snadno dokázati, až snad na pořádek, rovna číslům $1, 2, 3, \ldots, \pi$. Nejsou totiž žádná dvě z těchto čísel sobě rovna. Z $i' = j'$, $i \neq j$ $(j = 1, 2, \ldots, \pi)$ by totiž plynulo na základě (1)

$$\varepsilon_i i \equiv \varepsilon_j j \pmod p,$$

což není možno, ježto čísla $-\frac{1}{2}(p-1), \ldots, -2, -1, 0, 1, 2, \ldots, \frac{1}{2}(p-1)$ tvoří úplnou soustavu zbytků (mod p), takže není možno, aby $i \equiv \pm j \pmod p$. Předpokládejme nejprve, že p je prvočíslo. Z (1) pak plyne znásobením

$$1 \,.\, 2 \,.\, 3 \ldots \pi a^\pi \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\pi \,.\, 1' \,.\, 2' \ldots \pi' \pmod p$$

a tedy podle toho, co právě dokázáno, $a^\pi \equiv \varepsilon_1 . \varepsilon_2 \ldots \varepsilon_\pi \pmod p$. Ježto pak $a^\pi \equiv \left(\frac{a}{p}\right) \pmod p$, je $\left(\frac{a}{p}\right) \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\pi \pmod p$. Odtud plyne $\left(\frac{a}{p}\right) = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\pi = (-1)^\mu$.

Platí tedy věta, která nazývá se Gaussovo lema:

Budiž a číslo celé nedělitelné lichým prvočíslem p. Pak $\left(\frac{a}{p}\right) = (-1)^{\mu}$, *kdež μ značí, kolik mezi absolutně nejmenšími zbytky čísel*

$$1 \,.\, a,\ 2 \,.\, a,\ 3 \,.\, a,\ \ldots,\ \pi \,.\, a,\quad \pi = \tfrac{1}{2}(p-1)$$

je záporných.

§ 44. Předpokládejme nyní, že p je číslo liché kladné, a číslo celé s ním nesoudělné. Podle Scheringa a Kroneckera budeme definovati symbol $\left(\frac{a}{p}\right)$ pomocí $(-1)^{\mu} = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{\pi}$. Udává tedy μ, kolik absolutně nejmenších zbytků (mod p) čísel

$$1 \,.\, a,\ 2 \,.\, a,\ 3 \,.\, a,\ \ldots,\ \pi a \tag{1}$$

je záporných, neboli kolik nejmenších kladných zbytků těchto čísel (mod p) je $> \frac{1}{2} p$. V případě, že je p prvočíslo, shoduje se $\left(\frac{a}{p}\right)$ na základě Gaussova lematu se symbolem Legendreovým.

Nejprve je patrno, že platí

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right),$$

je-li $a' \equiv a \pmod{p}$.

Z $a' \equiv a \pmod{p}$ plyne, že a' je nesoudělné s p, takže, má-li význam $\left(\frac{a}{p}\right)$, má význam i $\left(\frac{a'}{p}\right)$. Rovnost $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ plyne pak ihned z té okolnosti, že čísla $1 \,.\, a', 2 \,.\, a', 3 \,.\, a', \ldots \pi \,.\, a'$ poskytují tytéž absolutně nejmenší zbytky (mod p) jako $1 \,.\, a$, $2 \,.\, a$, $3 \,.\, a, \ldots, \pi \,.\, a$.

Dále dokážeme, že, jsou-li a, a' čísla nesoudělná s p, tedy i aa' nesoudělné s p, je

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right).$$

Abychom určili $\left(\frac{aa'}{p}\right)$, nutno určiti počet záporných, absolutně nejmenších zbytků (mod p) čísel

$$1 \,.\, aa',\ 2 \,.\, aa',\ 3 \,.\, aa',\ \ldots,\ \pi aa'. \tag{2}$$

Ježto $1 \,.\, a, 2 \,.\, a, \ldots, \pi a$ jsou (mod p) kongruentní resp. s čísly

$$\varepsilon_1 1',\ \varepsilon_2 2',\ \ldots,\ \varepsilon_{\pi} \pi',$$

budou čísla (2) poskytovati tytéž absolutně nejmenší zbytky (mod p) jako čísla

$$\varepsilon_1 1'a', \varepsilon_2 2'a', \ldots, \varepsilon_\pi \pi' a'.$$

Čísla $1', 2', \ldots, \pi'$ jsou až na pořádek rovna číslům $1, 2, 3, \ldots, \pi$. Jsou-li tedy $\varepsilon'_1 1'', \varepsilon'_2 2'', \ldots, \varepsilon'_\pi \pi''$ absolutně nejmenší zbytky (mod p) čísel $1'a', 2'a', \ldots, \pi' a'$, při čemž $\varepsilon'_i = \pm 1$, pak čísla $1'', 2'', \ldots, \pi''$ jsou až na pořádek rovna číslům $1, 2, \ldots, \pi$, a bude

$$\left(\frac{a'}{p}\right) = \varepsilon'_1 \varepsilon'_2, \ldots \varepsilon'_\pi.$$

Vidíme tudíž, že absolutně nejmenší zbytky čísel (2) jsou

$$\varepsilon_1 \varepsilon'_1 1'', \varepsilon_2 \varepsilon'_2 2'', \ldots, \varepsilon_\pi \varepsilon'_\pi \pi'',$$

takže

$$\left(\frac{aa'}{p}\right) = \varepsilon_1 \varepsilon'_1 \varepsilon_2 \varepsilon'_2 \ldots \varepsilon_\pi \varepsilon'_\pi = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right).$$

Je ihned patrno, že $\left(\frac{1}{p}\right) = 1$ a obecně $\left(\frac{a^2}{p}\right) = 1$ pro každé celé a nesoudělné s p.

Obraťme se nyní k určení $\left(\frac{-1}{p}\right)$ a $\left(\frac{2}{p}\right)$ (věty doplňkové k zákonu reciprocity).

Pro $a = -1$ je $\varepsilon_i = -1$ $(i = 1, 2, \ldots, \pi)$; i bude $\left(\frac{-1}{p}\right) = (-1)^\pi = (-1)^{\frac{1}{2}(p-1)}$ jako pro případ, že p je prvočíslo.

Pro $a = 2$ zní řada (1)

$$2, 4, 6, 8, \ldots, p - 1. \tag{3}$$

Jsou to nejmenší kladné zbytky (mod p). Je tedy $\left(\frac{2}{p}\right) = (-1)^\mu$, kdež μ udává, kolik z čísel (3) je $> \frac{1}{2} p$.

Budiž nejprve $p = 4k + 1$. Pak je řada (3):

$$2, 4, 6, \ldots, 2k \mid 2k + 2, 2k + 4, \ldots, 4k.$$

Členy této řady za čárkou | jsou $> \frac{1}{2} p$, jejich počet je k, tedy $\mu = k$.

$\left(\frac{2}{p}\right) = 1$, je-li k sudé $= 2h$, tedy $p = 8h + 1$,

$\left(\frac{2}{p}\right) = -1$, je-li k liché $2h - 1$, tedy $p = 8h - 3$.

Uvažujme nyní případ $p = 4k + 3$. Pak je řada (3)

$$2, 4, 6, \ldots, 2k \mid 2k + 2, 2k + 4, \ldots, 4k + 2$$

a počet zbytků $> \frac{1}{2}p$ je $\mu = k + 1$. Z toho plyne

$$\left(\frac{2}{p}\right) = 1, \text{ je-li } k \text{ liché } 2h - 1, \text{ tedy } p = 8h - 1,$$

$$\left(\frac{2}{p}\right) = -1, \text{ je-li } k \text{ sudé } 2h, \text{ tedy } p = 8h + 3.$$

Je tedy

$$\left(\frac{2}{p}\right) = 1 \text{ pro } p = 8h \pm 1,$$

$$\left(\frac{2}{p}\right) = -1 \text{ pro } p = 8h \pm 3.$$

Je však

pro $p = 8h \pm 1$, $\frac{1}{8}(p^2 - 1) = 8h^2 \pm 2h$ sudé,
pro $p = 8h \pm 3$, $\frac{1}{8}(p^2 - 1) = 8h^2 \pm 6h + 1$ liché,

takže

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

§ 45. Kvadratický zákon reciprocity.

Buďtež p, q dvě čísla celá lichá kladná spolu nesoudělná. Pak je

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)},$$

$$\text{t. j. } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

vyjma v případě, kdy $p \equiv q \equiv -1 \pmod 4$; *v tomto případě je*

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Z celé řady důkazů snad je nejjednodušší důkaz Zellerův v modifikaci Frobeniově*); ten zde podáváme.

V rovnicích

$$\left(\frac{q}{p}\right) = (-1)^{\mu}, \quad \left(\frac{p}{q}\right) = (-1)^{\nu}$$

μ, ν mají tento význam:

*) Frobenius: Über das quadratische Reziprozitätsgesetz I, II. Sitzungsber. d. k. preuss. Akad. d. Wiss. 10, 18; 1914. K historii zákona reciprocity srov. Bachmann *3*. I.

μ značí počet násobků čísla q:

$$1 \,.\, q, 2 \,.\, q, 3 \,.\, q, \ldots, \frac{p-1}{2} q, \qquad (P)$$

jichž absolutně nejmenší zbytky (mod p) jsou záporné.

ν pak značí počet násobků čísla p:

$$1 \,.\, p, 2 \,.\, p, 3 \,.\, p, \ldots, \frac{q-1}{2} p, \qquad (Q)$$

jichž absolutně nejmenší zbytky (mod q) jsou záporné. Dlužno dokázati, že $\mu + \nu \equiv \frac{1}{2}(p-1) \,.\, \frac{1}{2}(q-1) \pmod 2$.

Budiž x proměnná, která může nabývati hodnot

$$1, 2, 3, \ldots, \tfrac{1}{2}(p-1). \qquad (x)$$

a y proměnná nabývající hodnot

$$1, 2, 3, \ldots, \tfrac{1}{2}(q-1). \qquad (y)$$

Čísla z řady (P) lze psáti ve tvaru qx a čísla z řady (Q) ve tvaru py. Absolutně nejmenší zbytek čísla $qx \pmod p$ je $qx - pm$, zvolíme-li m tak, že tento rozdíl je mezi $-\frac{1}{2}p$ a $\frac{1}{2}p$. Ke každému x lze zvoliti m podle § 2 str. 9 jediným způsobem. Udává tedy μ, kolikrát bude při tom $-\frac{1}{2}p < qx - pm < 0$. Zde neodpovídá každé z $\frac{1}{2}(p-1)$ hodnot x hodnota m, nýbrž jen μ hodnotám x odpovídá jisté m a to každé z oněch hodnot x jediné m. Pro takové m je $0 < qx < pm < qx + \frac{1}{2}p < \frac{1}{2}pq + \frac{1}{2}p$, t. j. $0 < m < \frac{1}{2}(q+1)$; m je tedy omezeno na řadu (y). Lze tedy místo m psáti y a říci: μ udává, pro kolik dvojic (x, y), při nichž x je z řady (x), y z řady (y), platí $-\frac{1}{2}p < qx - py < 0$, t. j. $0 < py - qx < \frac{1}{2}p$. Podobně bude ν udávati, pro kolik dvojic (x, y), při nichž x je z řady (x), y z řady (y), platí $-\frac{1}{2}q < py - qx < 0$. Všech možných dvojic (x, y) je na počet $\varrho = \frac{1}{2}(p-1) \,.\, \frac{1}{2}(q-1)$, je-li x omezeno na hodnoty z (x) a y na hodnoty z (y). Pro každou z těchto ϱ dvojic je buď

	I	$\frac{1}{2}p < py - qx$,
neb	II	$0 < py - qx < \frac{1}{2}p$,
neb	III	$-\frac{1}{2}q < py - qx < 0$,
nebo konečně	IV	$py - qx < -\frac{1}{2}q$.

Pro žádnou dvojici není

$$py - qx = 0.$$

Podmínce I nechť vyhovuje δ, podmínce IV δ' dvojic. Pak je

$$\varrho = \mu + \nu + \delta + \delta'.$$

Je však

$$\delta' = \delta.$$

neboť substitucemi

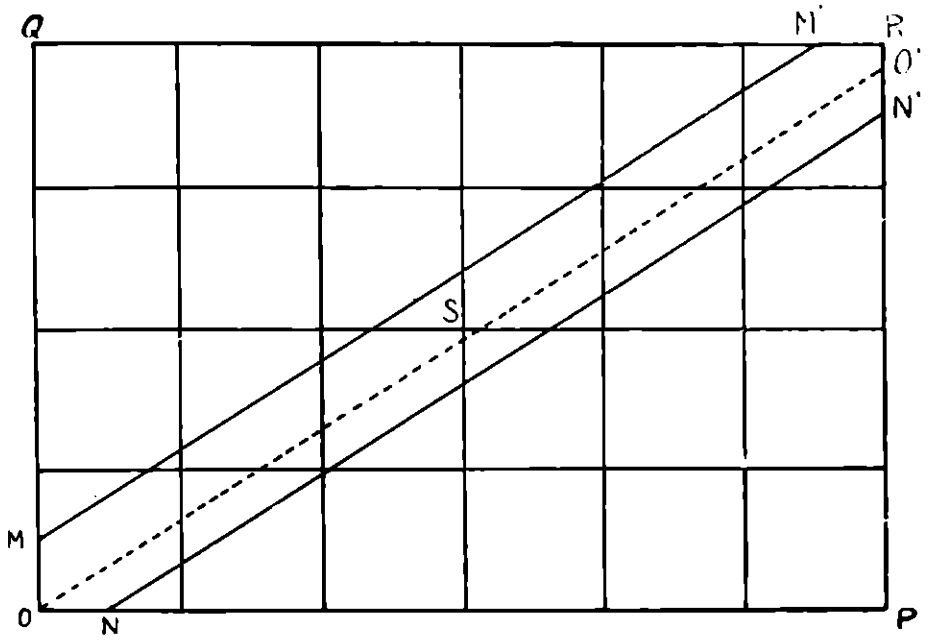
$$x = \tfrac{1}{2}(p+1) - x', \quad y = \tfrac{1}{2}(q+1) - y' \qquad (S)$$

přejde I ve IV, a probíhá-li x hodnoty (x), probíhá x' tytéž hodnoty (x). Stejně, probíhá-li y hodnoty (y), probíhá i y' hodnoty (y). Je tedy skutečně $\delta' = \delta$, t. j.

$$\varrho \equiv \mu + \nu \pmod 2$$

a konečně

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$



Geometrický význam těchto úsudků je jasný. (Obrazec je proveden pro $p = 11$, $q = 7$.) R má souřadnice $\frac{1}{2}(p+1)$, $\frac{1}{2}(q+1)$. M, M', N, N' jsou středy stran příslušných čtverců. Spolu rovnoběžné přímky OO', MM', NN' mají rovnice

$$py = qx,\ py = qx + \tfrac{1}{2}p,\ py = qx - \tfrac{1}{2}q.$$

Substitucí (S) jsou si přiřazeny body ležící souměrně vzhledem ke středu S obdélníku $OPRQ$. S má souřadnice $\frac{1}{4}(p+1), \frac{1}{4}(q+1)$. Uvnitř obdélníku $OPRQ$ leží ϱ bodů mřížových (t. j. bodů, jejichž souřadnice x, y jsou čísla celá), μ jich leží mezi OO' a MM', ν mezi OO' a NN'. Připadne-li δ bodů na trojúhelník $MM'Q$, připadne jich na trojúhelník $NN'P$ symetrický vzhledem ke středu S stejný počet. Je tedy

$$\varrho = \mu + \nu + 2\delta.$$

Lze však souditi též takto:

Podle II a III je $\mu + \nu$ počet hodnot x, y hovících podmínkám

$$-\tfrac{1}{2}q < py - qx < \tfrac{1}{2}p. \qquad (*)$$

Tyto přejdou substitucí (S) samy v sebe. Patří-li (x, y) k oněm $\mu + \nu$ párům splňujícím (*), patří k nim i (x', y'). Je tedy $\mu + \nu$ sudé vyjma v případě, že

$$x = x' = \tfrac{1}{4}(p + 1), \quad y = y' = \tfrac{1}{4}(q + 1)$$

jsou čísla celá, t. j. kdy $p \equiv q \equiv -1 \pmod 4$. Jen v tomto případě je $\mu + \nu$ liché.

Leží-li bod (x, y) v proužku obdélníku $OPRQ$ mezi MM' a NN' (v šestiúhelníku $ONN'RM'M$), leží bod (x', y'), symetrický vzhledem k S, tamtéž. Tento proužek (i body mřížové v něm obsažené) je totiž sám k sobě symetrický vzhledem k S. Je tedy počet $\mu + \nu$ mřížových bodů uvnitř proužku toho sudý, vyjma v případě, kdy střed souměrnosti $\frac{1}{4}(p + 1)$, $\frac{1}{4}(q + 1)$ je bod mřížový.

Dokážeme nyní platnost vztahu

$$\left(\frac{a}{p}\right)\left(\frac{a}{p'}\right) = \left(\frac{a}{pp'}\right), \qquad (1)$$

kdež p, p' značí čísla lichá kladná, a číslo celé nesoudělné s p i s p', tedy i s pp'.

Předpokládejme nejprve, že a je liché kladné. Pak je podle zákona reciprocity

$$\left(\frac{a}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(a-1)}\left(\frac{p}{a}\right) \qquad (2)$$

$$\left(\frac{a}{p'}\right) = (-1)^{\frac{1}{2}(p'-1)\cdot\frac{1}{2}(a-1)}\left(\frac{p'}{a}\right) \qquad (3)$$

$$\left(\frac{a}{pp'}\right) = (-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(a-1)}\left(\frac{pp'}{a}\right).$$

Násobením (2) a (3) dostaneme

$$\left(\frac{a}{p}\right)\left(\frac{a}{p'}\right) = (-1)^{\frac{1}{2}(a-1)\left[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)\right]}\left(\frac{p}{a}\right)\left(\frac{p'}{a}\right) =$$

$$= (-1)^{\frac{1}{2}(a-1)\left[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)\right]}\left(\frac{pp'}{a}\right), \quad \text{podle § 44.}$$

Bude tedy platiti (1), bude-li

$$\tfrac{1}{2}(a-1)\,[\tfrac{1}{2}(p-1)+\tfrac{1}{2}(p'-1)] \equiv \tfrac{1}{2}(a-1)\,.\,\tfrac{1}{2}(pp'-1) \pmod 2. \quad (4)$$

Je však

$$pp' = [1+(p-1)]\,[1+(p'-1] \equiv 1+(p-1)+ \\ +(p'-1) \pmod 4.$$

Součin $(p-1)(p'-1)$ je totiž dělitelný 4 jako součin dvou čísel sudých. I je

$$\tfrac{1}{2}(pp'-1) \equiv \tfrac{1}{2}(p-1)+\tfrac{1}{2}(p'-1) \pmod 2.$$

Odtud pak ihned plyne (4).

Předpokládejme dále, že a je sudé, kladné. Pak $\bar{a} = a + pp'$ je liché kladné, takže platí pro $\bar{a}$ vzorec $\left(\frac{\bar{a}}{p}\right)\left(\frac{\bar{a}}{p'}\right) = \left(\frac{a}{pp'}\right)$.

Je však $\bar{a} \equiv a \pmod p$ i $(\mathrm{mod}\ p')$ i $(\mathrm{mod}\ pp')$, takže

$$\left(\frac{\bar{a}}{p}\right) = \left(\frac{a}{p}\right), \quad \left(\frac{\bar{a}}{p'}\right) = \left(\frac{a}{p'}\right), \quad \left(\frac{\bar{a}}{pp'}\right) = \left(\frac{a}{pp'}\right).$$

Platí tedy (1) i pro a.

Tak dokázali jsme (1) pro a kladné.

Budiž nyní a záporné. I lze určiti $\bar{a} \equiv a \pmod{pp'}$ tak, aby $\bar{a}$ bylo kladné. Pak bude $\bar{a} \equiv a$ též $(\mathrm{mod}\ p)$ a $(\mathrm{mod}\ p')$. Pro $\bar{a}$ platí (1), tedy i pro a.

Tím dokázáno (1) úplně.

Je-li p liché kladné číslo $p = p_1 p_2 \ldots p_\nu$, kdež $p_1, p_2, \ldots p_\nu$ jsou prvočísla lichá, bude pro a nesoudělné s p

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_\nu}\right).$$

Takto definoval $\left(\frac{a}{p}\right)$ pro případ čísla složeného p Jacobi.

Buďtež p, q čísla lichá, kladná, spolu nesoudělná. Ze zákona reciprocity plyne

$$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\left(\frac{q}{p}\right).$$

Dále je

$$\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(q-1)}\left(\frac{p}{q}\right) =$$

$$= (-1)^{\frac{1}{2}(q-1)}\,(-1)^{\frac{1}{2}(p-1).\frac{1}{2}(q-1)}\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(q-1)[1+\frac{1}{2}(p-1)]}\left(\frac{q}{p}\right) =$$

$$= (-1)^{\frac{1}{2}(p+1)\cdot\frac{1}{2}(q-1)}\left(\frac{q}{p}\right),$$

ježto pak $-p-1 \equiv p+1 \pmod 4$, tedy

$$\left(\frac{-p}{q}\right) = (-1)^{\frac{1}{2}(-p-1).\frac{1}{2}(q-1)} \left(\frac{q}{p}\right).$$

Jsou-li tedy p, q čísla lichá spolu nesoudělná, q kladné, p kladné neb záporné, je

$$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1).\frac{1}{2}(q-1)} \left(\frac{q}{p}\right).$$

§ 46. Obrátíme se nyní k úloze, určiti všechna čísla celá kladná lichá n taková, že při daném číslu m symbol $\left(\frac{m}{n}\right)$ má význam a platí

$$\left(\frac{m}{n}\right) = 1 \quad \text{neb} \quad \left(\frac{m}{n}\right) = -1.$$

Doplňovací věty řeší nám úlohu pro $m = -1$ a $m = 2$.

$\left(\frac{-1}{n}\right) = 1$ pro všechna čísla celá kladná tvaru $n = 4k+1$ (k celé),

$= -1$ pro všechna čísla celá kladná tvaru $n = 4k+3$.

$\left(\frac{2}{n}\right) = 1$ pro všechna čísla celá kladná tvaru $n = 8k+1, 8k+7$,

$\left(\frac{2}{n}\right) = -1$ pro všechna čísla celá kladná tvaru $n = 8k+3, 8k+5$.

Z toho plyne dále

$\left(\frac{-2}{n}\right) = 1$ pro všechna čísla celá kladná tvaru $n = 8k+1, 8k+3$,

$\left(\frac{-2}{n}\right) = -1$ pro všechna čísla celá kladná tvaru $n = 8k+5, 8k+7$.

Vidíme, že čísla celá n, pro něž -1 má určitý kvadratický charakter, tvoří jednu posloupnost aritmetickou, číslo n, pro něž ± 2 má určitý kvadratický charakter, tvoří dvě posloupnosti aritmetické.

Dokážeme, že obecně všechna čísla celá n, pro něž $\left(\frac{m}{n}\right)$ má jednu z hodnot $+1$ neb -1, tvoří několik aritmetických postoupností.

Celé číslo m, které může býti kladné neb záporné, sudé neb liché, lze psáti ve tvaru

$$m = 2^c r s^2,$$

kdež $c=0$ neb 1, r je číslo celé liché nedělitelné čtvercem žádného prvočísla, tedy součin lichých mezi sebou různých prvočísel s kladným neb záporným znaménkem neb ± 1, s je číslo celé kladné.

Pak je

$$\left(\frac{m}{n}\right) = \left(\frac{2^c r s^2}{n}\right) = \left(\frac{2^c r}{n}\right).$$

Lze se tedy omeziti na případ

$$m = 2^c r$$

a o r lze předpokládati, že není $= 1$ ani -1, ježto pak bychom přišli k některému z případů již projednaných $m = \pm 1, \pm 2$; r je tedy součin lichých mezi sebou různých prvočísel s kladným neb záporným znaménkem.

Pak dostaneme

$$\left(\frac{m}{n}\right) = \left(\frac{2^c r}{n}\right) = \left(\frac{2}{n}\right)^c \left(\frac{r}{n}\right) = (-1)^{\frac{1}{8}c(n^2-1)} (-1)^{\frac{1}{2}(n-1)\cdot\frac{1}{2}(r-1)} \left(\frac{n}{r}\right).$$

Položme

$$(-1)^{\frac{1}{2}(r-1)} = \delta, \quad (-1)^c = \varepsilon.$$

Pak bude

$\delta = \quad 1$ pro $r \equiv 1 \pmod 4$, $\quad \varepsilon = \quad 1$ pro $c = 0$,
$\delta = -1$ pro $r \equiv 3 \pmod 4$, $\quad \varepsilon = -1$ pro $c = 1$.

I dostaneme

$$\left(\frac{m}{n}\right) = \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{r}\right). \qquad (*)$$

Na základě tohoto vzorce bude míti $\left(\frac{m}{n}\right)$ tutéž hodnotu pro čísla n patřící do téže třídy (mod $8r$), při $\varepsilon = 1$ již pro čísla n patřící do téže třídy (mod $4r$), a je-li též $\delta = 1$, dokonce pro čísla n patřící do téže třídy (mod $2r$). Stačí tedy uvažovati n jen z redukované soustavy zbytků podle uvedených modulů.

Označíme v redukované soustavě zbytků (mod $2r$) čísla n, pro něž $\left(\frac{n}{r}\right) = 1$, písmenem a, čísla, pro něž $\left(\frac{n}{r}\right) = -1$,

písmenem b. Počet čísel a je roven počtu čísel b. Dokážeme nejprve, že existuje aspoň jedno číslo b.

Budiž p prvočíslo obsažené v r, tedy $|r| = pr'$, r' číslo celé kladné nedělitelné p, β nezbytek (mod p). Určeme b_0 kongruencemi

$$b_0 \equiv \beta \pmod{p}, \quad b_0 \equiv 1 \pmod{r'}.$$

Pak je

$$\left(\frac{b_0}{|r|}\right) = \left(\frac{b_0}{pr'}\right) = \left(\frac{\beta}{p}\right)\left(\frac{1}{r'}\right) = -1,$$

takže b_0 je skutečně číslo druhu b.

O b_0 lze nad to předpokládati, že je liché. Kdyby totiž bylo sudé, byla by $b_0 + |r|$ liché a o $b_0 + |r|$ by platilo $\left(\frac{b_0 + |r|}{|r|}\right) = \left(\frac{b_0}{|r|}\right) = -1$. Pak je b_0 nesoudělné s $2r$. Násobme b_0 každé číslo z množství čísel a i b, t. j. z redukované soustavy zbytků (mod $2r$). Dostaneme zase redukovanou soustavu zbytků (mod $2r$). I dostáváme

$$\sum\left(\frac{n}{|r|}\right) = \sum\left(\frac{b_0 n}{|r|}\right) = \left(\frac{b_0}{|r|}\right)\sum\left(\frac{n}{|r|}\right) = -\sum\left(\frac{n}{|r|}\right),$$

t. j.

$$\sum\left(\frac{n}{|r|}\right) = 0,$$

kdež Σ se vztahuje na redukovanou soustavu zbytků (mod $2r$).

Avšak

$$\sum\left(\frac{n}{|r|}\right) = \sum_a\left(\frac{a}{|r|}\right) + \sum_b\left(\frac{b}{|r|}\right) = 0,$$

takže počet čísel druhu a je roven počtu čísel druhu b.

Je-li nejprve $\delta = 1$, $\varepsilon = 1$, tedy $m \equiv 1 \pmod 4$, bude podle (*)

$$\left(\frac{m}{n}\right) = \quad 1 \quad \text{pro } n \equiv a \pmod{2r}$$

$$\left(\frac{m}{n}\right) = -1 \quad \text{pro } n \equiv b \pmod{2r}.$$

Lichá čísla n, pro něž $\left(\frac{m}{n}\right) = 1$ neb -1, tvoří $\frac{1}{2}\varphi(2r) = \frac{1}{2}\varphi(r) = \frac{1}{2}\varphi(m)$ aritmetických posloupností o diferenci $2r = 2m$.

Je-li za druhé $\delta = -1$, $\varepsilon = 1$, tedy $m \equiv 3 \pmod 4$, bude

$$\left(\frac{m}{n}\right) = 1, \text{ je-li buď } n \equiv 1 \pmod 4, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 3 \pmod 4, \quad n \equiv b \pmod r,$$

$$\left(\frac{m}{n}\right) = -1, \text{ je-li buď } n \equiv 3 \pmod 4, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 1 \pmod 4, \quad n \equiv b \pmod r.$$

Lichá n, pro něž $\left(\frac{m}{n}\right)$ má hodnotu $+1$ neb -1, jsou čísla r jistých aritmetických posloupností, jichž je na počet $\frac{1}{2}\varphi(4r) = \frac{1}{2}\varphi(4m)$.

Je-li za třetí $\delta = 1$, $\varepsilon = -1$, tedy $m \equiv 2 \pmod 8$, bude

$$\left(\frac{m}{n}\right) = 1, \text{ je-li buď } n \equiv 1, 7 \pmod 8, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 3, 5 \pmod 8, \quad n \equiv b \pmod r,$$

$$\left(\frac{m}{n}\right) = -1, \text{ je-li buď } n \equiv 3, 5 \pmod 8, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 1, 7 \pmod 8, \quad n \equiv b \pmod r.$$

Je-li konečně za čtvrté $\delta = -1$, $\varepsilon = -1$, tedy $m \equiv 6 \pmod 8$, bude

$$\left(\frac{m}{n}\right) = 1, \quad \text{je-li buď } n \equiv 1, 3 \pmod 8, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 5, 7 \pmod 8, \quad n \equiv b \pmod r,$$

$$\left(\frac{m}{n}\right) = -1, \text{ je-li buď } n \equiv 5, 7 \pmod 8, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 1, 3 \pmod 8, \quad n \equiv b \pmod r.$$

Ve třetím a čtvrtém případě lichá n, pro něž $\left(\frac{m}{n}\right)$ má určitou hodnotu, tvoří aritmetické posloupnosti o diferenci $8r = 4m$, na počet $\frac{1}{2}\varphi(8r) = \frac{1}{2}\varphi(4m)$.

Je-li $\left(\frac{m}{p}\right) = 1$ pro prvočíslo p, je kongruence $t^2 - m \equiv 0 \pmod p$ řešitelná celým číslem t nedělitelným p. Lze snadno nahlédnouti, že kongruence $t^2 - m \equiv 0 \pmod p$ je řešitelná celým číslem t nedělitelným p tehdy a jen tehdy, existují-li celá čísla x, y nedělitelná p taková, že platí

$$x^2 - my^2 \equiv 0 \pmod p.$$

Z řešitelnosti $t^2 - m \equiv 0 \pmod p$ celým číslem t nedělitelným p plyne $x^2 - my^2 \equiv 0 \pmod p$, klademe-li $x = t$, $y = 1$. Je-li $x^2 - my^2 \equiv 0 \pmod p$, x, y čísla celá nedělitelná p, pak pro

$t \equiv x/y \pmod{p}$ (viz § 23 str. 34), což je číslo celé nedělitelné p, bude

$$t^2 - m \equiv 0 \pmod{p}.$$

Existují-li celá čísla x, y nedělitelná prvočíslem p taková, že platí $x^2 - my^2 \equiv 0 \pmod{p}$, říká se (podle Eulera a Legendrea), že p je dělitelem formy kvadratické $x^2 - my^2$. Jsou tedy prvočísla p, pro něž $\left(\frac{m}{p}\right) = 1$, dělitelé formy $x^2 - my^2$.

Budiž N celé číslo. Existují-li celá čísla x, y taková, že $N = x^2 - my^2$, říká se, že N se dá znázorniti formou $x^2 - my^2$. Znázornění je vlastní, jsou-li x, y čísla nesoudělná, nejsou-li nesoudělná, je znázornění nevlastní.

Je-li p prvočíslo obsažené v N, je podmínka nutná pro vlastní znázornění N formou $x^2 - my^2$, aby p bylo dělitelem formy $x^2 - my^2$.

Hledejme čísla celá n, pro něž $\left(\frac{5}{n}\right) = 1$.

Zde $m = 5$, $c = 0$, $r = 5$, $\delta = 1$, $\varepsilon = 1$, $m \equiv 1 \pmod 4$, (případ první). Redukovaná soustava zbytků mod $2m = 2r = 10$ je

$$1, 3, 7, 9.$$

Kvadratické zbytky jsou 1, 9, nezbytky 3, 7.

Je tedy

$\left(\frac{5}{n}\right) = 1$ pro $n \equiv 1, 9 \pmod{10}$, t. j. pro $n \equiv \pm 1 \pmod{10}$,

$\left(\frac{5}{n}\right) = -1$ pro $n \equiv 3, 7 \pmod{10}$, t. j. pro $n \equiv \pm 3 \pmod{10}$.

Dělitelé formy $x^2 - 5y^2$ jsou prvočísla tvaru $p = 10k \pm 1$, k číslo celé kladné.

Uvažujme nyní případ $m = -6$.

Zde $m = -6 = 2 \cdot -3$, $c = 1$, $r = -3$, $\delta = 1$, $\varepsilon = -1$, $m \equiv 2 \pmod 8$ (případ třetí).

Redukovaná soustava zbytků mod $2r$, t. j. mod 6, je 1, 5;

1 je zbytek (mod r), t. j. (mod 3),
5 je nezbytek (mod r), t. j. (mod 3).

Bude tedy

$$\left(\frac{-6}{n}\right) = 1 \text{ pro } n \equiv 1 \pmod 3, \equiv 1, 7 \pmod 8$$

$$n \equiv 5 \equiv 2 \pmod 3, \equiv 3, 5 \pmod 8$$

t. j. pro $n \equiv 1, 5, 7, 11 \pmod{24}$, a pro $n > 0$.*)

§ 47. Znázornění čísla celého formou kvadratickou lze užíti k rozhodnutí, zda číslo ono je prvočíslo neb číslo složené, a v tomto případě provésti rozklad v prvočinitele.

Uvažujme číslo

$$P_{13} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 \ (\S\ 10).$$

Není dělitelno žádným kladným prvočíslem $\leqq 13$. Ježto pak $[\sqrt{30\,031}] = 173$, stačí uvažovati prvočísla $\geqq 17$ a $\leqq 173$.

Lze zjistiti, že $30\,031 = 174^2 - 5 \cdot 7^2$. Prvočinitelé čísla 30 031 budou tedy dělitelé formy $x^2 - 5y^2$, tedy prvočísla tvaru $10k \pm 1$.

V uvedených mezích leží tato prvočísla takového tvaru: 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, 151.

Konečně možno uvážiti, že 30 031 je tvaru $4n - 1$ a má tedy aspoň jednoho prvočinitele tohoto tvaru. Zbývá tedy z uvedených prvočísel uvažovati jen prvočísla tvaru $4n - 1$:

19, 31, 59, 71, 79, 131, 139, 151.

30 031 prvočísly 19, 31 není dělitelno, 59 je však dělitelno. Dostaneme

$$30\,031 = 59 \cdot 509.$$

509 je také prvočíslo.

§ 48. Budeme se zabývati znázorněním prvočísel formami $x^2 + my^2$ pro kladné m v některých jednoduchých případech. Tu platí věta**):

Je-li nejmenší liché prvočíslo, pro které $-m$ je kvadratický zbytek (které tedy je dělitelem formy $x^2 + my^2$), znázornitelno formou $x^2 + my^2$, je každé prvočíslo, pro něž je $-m$ kvadratický zbytek, jediným způsobem touto formou znázornitelno.

---

*) Kraitchik *1.* I. str. 164—186 (errata *2.* II str. 180), *2.* I. str. 205—215 udává tabulku aritmetických posloupností, v nichž leží n při daném m a platí $\left(\frac{m}{n}\right) = 1$ resp. -1 pro m mezi -250 a $+250$. Menší tabulky viz Cahen *1.*, Wertheim *2.*

**) S. Eichenberg, Über das quadr. Reciprocitätsgesetz und einige quadr. Zerfällungen d. Primzahlen, Diss. Göttingen 1886. Viz též: Weber-Wellstein, str. 266—272.

Uveďme nejprve identitu

$$(a^2 + mb^2)(\alpha^2 + m\beta^2) = A^2 + mB^2, \qquad (*)$$

kdež buď

$$A = a\alpha + mb\beta, \qquad B = a\beta - b\alpha,$$

anebo

$$A = a\alpha - mb\beta, \qquad B = a\beta + b\alpha.$$

Tato identita dá se snadno dokázati přímým výpočtem obou jejích stran; ještě snadněji však, když činitele na levé straně rozložíme v komplexní činitele

$$(a + i\sqrt{m}b)(a - i\sqrt{m}b)(\alpha + i\sqrt{m}\beta)(\alpha - i\sqrt{m}\beta).$$

Násobme prvního činitele se čtvrtým, druhého se třetím. I dostaneme

$$[a\alpha + mb\beta - i\sqrt{m}(a\beta - b\alpha)][a\alpha + mb\beta + i\sqrt{m}(a\beta - b\alpha)] = (a\alpha + mb\beta)^2 + m(a\beta - b\alpha)^2.$$

Násobíme-li však prvního činitele se třetím, druhého se čtvrtým, nebo klademe-li $-b$ místo b, dostaneme jako součin hodnotu $(a\alpha - mb\beta)^2 + m(a\beta + b\alpha)^2$.

Dokážeme si nejprve větu pomocnou:

Lze-li číslo znázornitelné formou

$$x^2 + my^2 \qquad (1)$$

rozložiti v součin

$$A^2 + mB^2 = pP, \qquad (2)$$

kdež p je prvočíslo rovněž formou (1) znázornitelné, je též celé číslo P formou (1) znázornitelné.

Budiž $p = a^2 + mb^2$. Položme

$$\alpha = \frac{aA + mbB}{a^2 + mb^2}, \quad \beta = \frac{aB - bA}{a^2 + mb^2}. \qquad (3)$$

I je

$$(aB + bA)(aB - bA) = a^2B^2 - b^2A^2 = B^2(a^2 + mb^2) - b^2(A^2 + mB^2) = p(B^2 - Pb^2).$$

Je tudíž jedno z čísel $aB \pm bA$ dělitelno $p = a^2 + mb^2$. Můžeme však znamení u b voliti tak, aby bylo $aB - bA$ číslo prvočíslem p dělitelné, takže β je číslo celé.

Podle (*) je

$$(aA + mbB)^2 + m(aB - bA)^2 = (a^2 + mb^2)(A^2 + mB^2); \qquad (4)$$

jest tedy též $aA + mbB$ dělitelno p a je tudíž i α celé číslo. Podle (3) a (4) je však

$$\alpha^2 + m\beta^2 = \frac{A^2 + mB^2}{a^2 + mb^2} = P,$$

čímž věta dokázána.

Budiž $-m$ kvadratický zbytek lichého prvočísla, které není nejmenším prvočíslem této vlastnosti. Předpokládejme, že všechna prvočísla $< p$, jejichž zbytkem kvadratickým je $-m$, lze znázorniti pomocí formy $x^2 + my^2$, a dokážeme, že p dá se znázorniti touto formou.

Každé prvočíslo formou $x^2 + my^2$ znázornitelné je $\geqq m$, takže pro p platí $p > m$. Ježto $-m$ je kvadratický zbytek prvočísla p, existuje číslo celé z té vlastnosti, že $z^2 \equiv -m \pmod{p}$.

Tato kongruence má dvě řešení, o nichž lze předpokládati, že jsou kladná a $< p$. Jedno je liché, druhé sudé. Lze tedy vždy dosíci, že

$$z^2 + m = gp \qquad (5)$$

je liché. Pak je i g liché.

Ježto $z \leqq p - 1$ a $m < p$, je $z^2 + m < p^2 - 2p + 1 + p < p^2$, tedy v (5) $g < p$.

Lze tedy najíti celá čísla c, d taková, že $c^2 + md^2 = gp$, při čemž g je liché číslo kladné $< p$. Uvažujme množství $\mathfrak{G}$ všech celých čísel lichých kladných g takových, že pro ně existují čísla celá x, y té vlastnosti, že $x^2 + my^2 = gp$. Podle toho, co právě bylo řečeno, množství $\mathfrak{G}$ jistě není prázdné. Mezi čísly z $\mathfrak{G}$ je jistě jisté nejmenší g_0. Dokážeme, že je rovno 1. Pro g_0 platí $a_0^2 + mb_0^2 = g_0 p$ a podle toho, co dokázáno, je jistě $g_0 < p$. Kdyby nebylo $g_0 = 1$, bylo by g_0 dělitelno aspoň jedním prvočíslem $q < p$. Toto prvočíslo q je dělitelem formy $x^2 + my^2$, $-m$ je pro ně kvadratickým zbytkem. Ježto pak je $q < p$, lze q znázorniti formou $x^2 + my^2$, t. j. existují čísla celá a, b takové, že

$$a^2 + mb^2 = q.$$

Nechť je $g_0 p = qP$. Ježto $qP = a_0^2 + mb_0^2$ a $q = a^2 + mb^2$, je podle věty pomocné $P = \frac{g_0 p}{q} = g_1 p = \alpha^2 + m\beta^2$. Je pak $g_1 < g_0$, proti předpokladu o g_0.

Z toho plyne úplnou indukcí, že, je-li nejmenší liché prvočíslo, jehož kvadratickým zbytkem je $-m$, znázornitelno formou $x^2 + my^2$, je každé prvočíslo, jehož kvadratickým zbytkem je $-m$, znázornitelno onou formou.

Ukážeme ještě, že prvočíslo p lze znázorniti formou $x^2 + my^2$

jen jedním způsobem. Při tom nebudeme čtyři znázornění $(\pm x, \pm y)$, která se od (x, y) liší jen znaménky, považovati za různá.

Kdyby bylo

$$p = x^2 + my^2 = \xi^2 + m\eta^2, \tag{6}$$

kdež $$\xi \neq \pm x, \quad \eta \neq \pm y,$$

bylo by podle (*)

$$p^2 = (x\xi + my\eta)^2 + m(x\eta - y\xi)^2. \tag{7}$$

Jest však

$$(x\eta - y\xi)(x\eta + y\xi) = x^2\eta^2 - y^2\xi^2 = \eta^2(x^2 + my^2) - y^2(\xi^2 + m\eta^2) = p(\eta^2 - y^2),$$

musilo by tedy jedno z obou čísel $x\eta \pm y\xi$ býti p dělitelno a $\neq 0$. Zvolme znamení u y tak, aby bylo $x\eta - y\xi$ dělitelno p. Pak by bylo $(x\eta - y\xi)^2 \geqq p^2$, což podle (7) pro $m > 1$ není možno.

Zbývá všimnouti si případu $m = 1$. Pak by musilo býti

$$x\eta - y\xi = \pm p \quad \text{a} \quad x\xi + y\eta = 0, \quad \text{t. j.}$$

$$\frac{x}{y} = -\frac{\eta}{\xi}. \tag{8}$$

x, y jakož i ξ, η jsou dvojice čísel spolu nesoudělných; bylo by tedy podle (8) $x = \pm\eta$, $y = \mp\xi$, takže by se tato znázornění nelišila. (Při tom znázornění $(\pm x, \pm y)$, $(\pm y, \pm x)$ nepovažujeme za různá.) Tím tvrzení dokázáno.

Užijeme věty nejprve na případ $m = 1$, t. j. na formu $x^2 + y^2$. — 1 je kvadratický zbytek všech prvočísel tvaru $4k + 1$. Nejmenší z nich 5 lze znázorniti pomocí formy $x^2 + y^2$, $5 = 1^2 + 2^2$. Platí tedy věta:

Každé prvočíslo tvaru $4k + 1$ lze znázorniti jediným způsobem jako součet dvou čtverců.

Žádné prvočíslo tvaru $4k + 3$ nelze znázorniti jako součet dvou čtverců, neboť jeden z nich jako čtverec čísla sudého by byl $\equiv 0 \pmod 4$, druhý jako čtverec čísla lichého by byl $\equiv 1 \pmod 4$, takže by součet byl tvaru $4k + 1$.

Samozřejmě platí věta:

Každé liché prvočíslo obsažené v součtu dvou nesoudělných čtverců je tvaru $4k + 1$, tedy zase součet dvou čtverců.

p je totiž dělitelem formy $x^2 + y^2$.

Snadno lze nahlédnouti, že platí identita (podle (*), str. 83)

$$(a^2 + b^2)(\alpha^2 + \beta^2) = (a\alpha + b\beta)^2 + (a\beta - b\alpha)^2$$

a pro $\alpha = \beta = 1$

$$2\,(a^2 + b^2) = (a + b)^2 + (a - b)^2.$$

Součet dvou nesoudělných čtverců je buď lichý (je-li jedno z obou čísel sudé, druhé liché) neb dvojnásobek lichého čísla (jsou-li oba čtverce liché). Plyne tedy z věty předešlé:

Každý celý dělitel součtu dvou nesoudělných čtverců je zase součet dvou čtverců.

$m = 4$ věta také platí:

Každé prvočíslo tvaru $4n + 1$ *lze znázorniti jediným způsobem, formou* $x^2 + 4y^2$.

Ostatně plyne věta tato z předešlé. Při znázornění prvočísel tvaru $4n + 1$ formou $x^2 + y^2$ je jedno z čísel x, y liché, druhé sudé. Je-li tedy na př. $y = 2y'$, je $x^2 + y^2 = x^2 + 4y'^2$.

Užijme věty na případ $m = 2$, t. j. uvažujme formu $x^2 + 2y^2$. -2 je kvadratický zbytek prvočísel tvaru $8k + 1$, $8k + 3$. Nejmenší z nich je $3 = 1^2 + 2 \cdot 1^2$, je tedy znázornitelné pomocí formy $x^2 + 2y^2$. I platí věta:

Každé prvočíslo tvaru $8k + 1$ *aneb* $8k + 3$ *lze znázorniti jediným způsobem jako součet jednoduchého a dvojnásobného čtverce.*

Pro prvočíslo tvaru $8k + 1$ je x liché, y sudé, pro tvar $8k + 3$ je x i y liché.

Prvočísla tvaru $8k + 1$ *lze znázorniti jak formou* $x^2 + y^2$, *tak formou* $x^2 + 2y^2$.

Uvažujme případ $m = 3$, t. j. znázornění formou $x^2 + 3y^2$. -3 je kvadratický zbytek prvočísel tvaru $6k + 1$. Nejmenší z nich $7 = 2^2 + 3 \cdot 1^2$ je znázornitelné pomocí formy $x^2 + 3y^2$. *Každé prvočíslo tvaru* $6k + 1$ *lze jediným způsobem znázorniti jako součet čtverce a trojnásobného čtverce.*

Prvočísla tvaru $24k + 1$ *lze znázorniti každou ze tří forem* $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$.

Klaďme konečně $m = 7$. -7 je kvadratický zbytek prvočísel tvaru $14k + 1$, $14k + 9$, $14k + 11$. Nejmenší z nich je 11 a pro to platí $11 = 2^2 + 7 \cdot 1^2$. I máme větu:

Každé prvočíslo tvaru $14k+1$, $14k + 9$, $14k + 11$ *lze jediným způsobem znázorniti jako součet čtverce jednoduchého a sedminásobného.*

Při znázornění prvočísla $p = 4k + 1$ ve tvaru

$$p = x^2 + 3y^2$$

nesmí býti x dělitelno třemi, zato však y může býti třemi dělitelno. Pak lze psáti

$$4p = (2x)^2 + 3\,(2y)^2 = (2x)^2 + 27\left(\frac{2y}{3}\right)^2.$$

Není-li y dělitelno třemi a je sudé, je buď $\equiv 2$ neb $\equiv 4 \pmod 6$; x musí býti liché, tedy buď $\equiv 1$ neb $\equiv 5 \pmod 6$. V každém případě je pak buď $x + y$ neb $x - y$ dělitelno třemi. Není-li y dělitelno třemi a je liché, je buď $\equiv 1$ neb $\equiv 5 \pmod 6$; x je pak buď sudé, tedy $\equiv 2$ neb $\equiv 4 \pmod 6$, takže je zase buď $x + y$ neb $x - y$ dělitelno třemi.

Jest však

$$4p = (1^2 + 3 \,.\, 1^2)\,(x^2 + 3y^2),$$

a je-li $x + y \equiv 0 \pmod 3$, pišme

$$4p = (x - 3y)^2 + 3\,(x + y)^2 = (x - 3y)^2 + 27\left(\frac{x+y}{3}\right)^2.$$

Je-li však $x - y \equiv 0 \pmod 3$, pak

$$4p = (x + 3y)^2 + 3\,(x - y)^2 = (x + 3y)^2 + 27\left(\frac{x-y}{3}\right)^2.$$

Platí tedy věta:

Čtyřnásobek prvočísla tvaru $4k + 1$ *lze znázorniti ve tvaru*

$$4p = X^2 + 27Y^2.$$

Toto znázornění je možné jediným způsobem.

Kdyby bylo

$$4p = X^2 + 27Y^2 = X_1^2 + 27Y_1$$

a

$$X_1 \neq \pm X,\quad Y_1 \neq \pm Y,$$

bylo by podle (*) str. 83

$$\begin{aligned} 16p^2 &= (X^2 + 27Y^2)\,(X_1^2 + 27Y_1^2) \\ &= (XX_1 + 27YY_1)^2 + 27\,(XY_1 - YX_1)^2. \end{aligned} \tag{9}$$

Jest však

$$\begin{aligned} (XY_1 - YX_1)\,(XY_1 + YX_1) &= X^2Y_1^2 - Y^2X_1^2 = \\ &= Y_1^2\,(X^2 + 27Y^2) - Y^2\,(X_1^2 + 27Y_1^2) = \\ &= 4p\,(Y_1^2 - Y^2). \end{aligned}$$

Bylo by tedy jedno z čísel $XY_1 \pm YX_1$ dělitelno p a $\neq 0$. Vhodným stanovením znamení Y bylo by možno dosíci, aby bylo $XY_1 - YX_1$ dělitelno p, tedy

$$|\,XY_1 - YX_1\,| \geqq p.$$

Pak by v (9) pravá strana byla $\geqq 27p^2$, levá strana je $16p^2$, což by vedlo k rozporu.

V. Znázornění čísel celých kladných formou

$$x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

§ 49. Fermat vyslovil a Lagrange dokázal větu: *Každé celé kladné číslo lze rozložiti na součet čtyř neb méně čtverců celých čísel.* Jinými slovy: *Je-li n celé číslo kladné, je možno určiti čtyři celá čísla x_1, x_2, x_3, x_4 (o nichž lze beze všeho předpokládati, že jsou $\geqq 0$), splňující rovnici $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$.**) (Všechna čísla x_1, x_2, x_3, x_4 nemusí býti $\neq 0$. Je-li na př. n rovno prvočíslu $p \equiv 1 \pmod 4$, je $p = x_1^2 + x_2^2$, takže lze klásti $x_3 = x_4 = 0$.)

Dokážeme si nejprve několik vět pomocných. V prvé řadě tak zvanou Eulerovu identitu.

1. *Jsou-li x_i, y_i libovolná čísla reální, je*

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =$$
$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 +$$
$$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \quad (1)$$

Provedeme-li násobení na levé straně, dostaneme součet 16 členů $x_i^2y_k^2$ $(i, k = 1, 2, 3, 4)$. Na pravé straně vyskytuje se též těchto 16 členů a mimo to ještě dalších 24 členů tvaru $\pm 2x_ix_jy_ky_l$ $(i, j, k, l = 1, 2, 3, 4)$, kdež možno beze všeho předpokládati $i < j$, $k < l$. Ale těchto 24 členů se dohromady ruší, neboť koeficient u:

$$\begin{aligned}
2x_1x_2 &\text{ je } y_1y_2 - y_1y_2 - y_3y_4 + y_3y_4 = 0,\\
2x_1x_3 &\text{ je } y_1y_3 + y_2y_4 - y_1y_3 - y_2y_4 = 0,\\
2x_1x_4 &\text{ je } y_1y_4 - y_2y_3 + y_2y_3 - y_1y_4 = 0,\\
2x_2x_3 &\text{ je } y_2y_3 - y_1y_4 + y_1y_4 - y_2y_3 = 0,\\
2x_2x_4 &\text{ je } y_2y_4 + y_1y_3 - y_2y_4 - y_1y_3 = 0,\\
2x_3x_4 &\text{ je } y_3y_4 - y_3y_4 - y_1y_2 + y_1y_2 = 0.
\end{aligned}$$

Tím dokázána identita (1).

2. *Je-li p liché prvočíslo, je možno určiti celé číslo x, y splňující kongruenci*

$$x^2 + y^2 + 1 \equiv 0 \pmod p,$$

---

*) Důkaz následující podán v podstatě podle Landaua, I. str. 107.

takže

$$0 \leqq x < \tfrac{1}{2}p,\ 0 \leqq y < \tfrac{1}{2}p.^*)$$

Uvažujme soustavu A čísel x^2 pro $x = 0, 1, 2, \ldots, \frac{p-1}{2}$, t. j. pro $0 \leqq x < \frac{1}{2}p$ a soustavu B čísel $-y^2 - 1$ pro $y = 0, 1, 2, \ldots, \frac{p-1}{2}$, t. j. pro $0 \leqq y < \frac{1}{2}p$. Žádná dvě čísla ze soustavy A nejsou spolu kongruentní (mod p). Z $x'^2 \equiv x''^2 \pmod{p}$ by plynulo $x' \equiv \pm x'' \pmod{p}$, což není možné, ježto čísla $0, \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$ tvoří úplnou soustavu zbytků (mod p) (§ 21). Ze stejného důvodu žádná dvě čísla ze soustavy B nejsou spolu kongruentní (mod p). V každé ze soustav A i B je $\frac{p+1}{2}$ čísel. Musí tedy býti aspoň jedno číslo ze soustavy A kongruentní (mod p) s jedním číslem ze soustavy B, ježto by jinak bylo $p + 1$ čísel, z nichž žádná dvě by nebyla kongruentní (mod p). Tím tvrzení dokázáno.

3. *Ke každému prvočíslu $p > 2$ lze určiti číslo celé m splňující vztah*

$$0 < m < p \tag{2}$$

té vlastnosti, že rovnice

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{3}$$

je řešitelná celými čísly x_1, x_2, x_3, x_4.

(Kdybychom nekladli pro m podmínku (2), byla by věta samozřejmá, neboť je $p \,.\, p = p^2 + 0^2 + 0^2 + 0^2$; pro další byla by pak věta zcela bezcenná.)

Podle předešlé věty je možno určiti celá čísla x, y splňující kongruenci

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

a taková, že $0 \leqq x < \frac{1}{2}p$, $0 \leqq y < \frac{1}{2}p$. Pak je $x^2 + y^2 + 1 = mp$, kdež m je celé číslo kladné. I platí

---

*) Zcela podobně by se dokázala obecnější věta:

Jsou-li a, b celá čísla, a nedělitelné p, lze určiti celá čísla x, y splňující kongruenci

$$x^2 + ay^2 + b \equiv 0 \pmod{p},$$

takže $0 \leqq x < \frac{1}{2}p$, $0 \leqq y < \frac{1}{2}p$. Uvedený důkaz pochází v podstatě od Bolzana a upozornil na něj Daublebsky v. Sterneck, Monatshefte f. Math. u. Phys. 15, 1904, p. 235—238. Je obsažen v rukopisné číselné teorii Bolzanově, uložené v Národní knihovně ve Vídni. Tato vyjde jako další svazek spisů Bolzanových s poznámkami od autora.

$$x^2 + y^2 + 1 < \tfrac{1}{4}p^2 + \tfrac{1}{4}p^2 + 1 = \tfrac{1}{2}p^2 + 1 < p^2,$$

tedy $mp < p^2$, t. j. $m < p$. Je tedy rovnice (3) i vztah (2) splněn, klademe-li $x_1 = x$, $x_2 = y$, $x_3 = 1$, $x_4 = 0$.

4. *Pro každé prvočíslo p je rovnice*

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

řešitelná celými čísly x_1, x_2, x_3, x_4.

Pro $p = 2$ je

$$2 = 1^2 + 1^2 + 0^2 + 0^2,$$

takže věta platí. Zbývá tedy zabývati se dále případem prvočísla lichého, $p > 2$. Označme $\mathfrak{M}$ množství čísel celých m, pro něž rovnice (3) je řešitelná celými čísly x_1, x_2, x_3, x_4. m_0 nechť je nejmenší číslo z množství $\mathfrak{M}$. Pak podle předešlé věty je jistě $0 < m_0 < p$. Dokážeme, že je $m_0 = 1$.

Především je možno o m_0 dokázati, že je liché. Kdyby totiž bylo m_0 sudé, plynulo by z rovnice

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2, \tag{3'}$$

že

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod 2.$$

Tato kongruence může býti splněna, jen když buď všechna čtyři čísla x_1, x_2, x_3, x_4 jsou sudá, neb všechna čtyři lichá neb dvě z nich sudá a druhá dvě lichá. Přečíslujeme-li pak po případě tato čísla, lze dosáhnouti, aby platilo

$$x_1 + x_2 \equiv 0, \quad x_3 + x_4 \equiv 0 \pmod 2.$$

Pak by bylo možno psáti rovnici (3') ve tvaru

$$\tfrac{1}{2}m_0 p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2.$$

Pak by nemohlo býti m_0 nejmenší číslo z množství $\mathfrak{M}$, ježto by tam patřilo též číslo $\frac{1}{2}m_0$, které je $< m_0$. Je tedy m_0 jistě liché. Dokážeme, že nemůže býti $m_0 > 1$. Důkaz provedeme nepřímo. Dokážeme nemožnost předpokladu, že m_0 jest číslo liché > 1.

Budiž tedy m_0 číslo liché > 1.

Ustanovme čtyři celá čísla $y_i (i = 1, 2, 3, 4)$, tak aby platilo

$$y_i \equiv x_i \pmod{m_0}, \quad |y_i| < \tfrac{1}{2}m_0. \tag{4}$$

To je možno, neboť čísla

$$0, \pm 1, \pm 2, \ldots, \pm \frac{m_0 - 1}{2} \tag{5}$$

tvoří úplnou soustavu zbytků (mod m_0) (§ 21, absolutně nejmenší zbytky), takže každé celé číslo je (mod m_0) kongruentní s jedním a jen s jedním z čísel (5).

Podle (3′) je

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}, \tag{6}$$

tedy též

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0},$$

t. j.

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 n, \tag{7}$$

kdež n je celé číslo $\geqq 0$.

Především je možno snadno dokázati, že jest $n \neq 0$. Při $n = 0$ by nutně musilo býti

$$y_1 = y_2 = y_3 = y_4 = 0,$$

t. j.

$$x_1 \equiv x_2 \equiv x_3 \equiv x_4 \pmod{m_0},$$

tedy

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0^2}.$$

Ze (3′) pak by plynulo

$$m_0 p \equiv 0 \pmod{m_0^2},$$

t. j.

$$p \equiv 0 \pmod{m_0},$$

což není možné, ježto p je prvočíslo a $1 < m_0 < p$. Bylo by tedy skutečně $n > 0$.

Dále by bylo $n < m_0$, neboť podle (4) by bylo $|y_i| < \frac{1}{2} m_0$ a tedy podle (7)

$$m_0 n < 4 \cdot \tfrac{1}{4} m_0^2 = m_0^2,$$

z čehož by ihned plynulo

$$n < m_0.$$

Z kongruencí (4) plyne však dále

$$x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod{m_0},$$

z čehož na základě (6) též

$$x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \equiv 0 \pmod{m_0},$$

t. j.

$$x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 = m_0 z,$$

kdež z je celé číslo.

Z týchž kongruencí (4) plyne dále

$$x_i y_k - x_k y_i \equiv x_i x_k - x_k x_i \equiv 0 \pmod{m_0},$$

$$(i, k = 1, 2, 3, 4, i \neq k),$$

t. j. $x_i y_k - x_k y_i = m_0 z_{ik}$, kdež z_{ik} jsou celá čísla.

Z Eulerovy identity pak plyne dále

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =$$
$$= m_0^2 z^2 + m_0^2 (z_{12} + z_{34})^2 + m_0^2 (z_{13} + z_{42})^2 + m_0^2 (z_{14} + z_{23})^2.$$

Dosaďme do této rovnice z rovnic (3′) a (7) a kraťme m_0^2. Dostaneme

$$np = z^2 + (z_{12} + z_{34})^2 + (z_{13} + z_{42})^2 + (z_{14} + z_{23})^2.$$

Ježto $n < m_0$, nebylo by m_0 nejmenší číslo z množství $\mathfrak{M}$. Vede tedy předpoklad $m_0 > 1$ ke sporu a je $m_0 = 1$. Tím pak tvrzení dokázáno.

Tak dokázali jsme tvrzení Fermatovo pro případ, že $n = p$ je prvočíslo. Každé číslo kladné je však možno vyjádřiti jako součin prvočísel $p_1, p_2, \ldots, p_s$: $n = p_1 p_2 \ldots p_s$. Pro každé z prvočísel $p_1, p_2, \ldots, p_s$ věta Fermatova platí, tedy na základě Eulerovy identity i pro jich součin n.

Waring vyslovil větu:

Pro každého mocnitele celého $k > 0$ je možno najíti číslo N_k té vlastnosti, že rovnice

$$n = x_1^k + x_2^k + \ldots + x_{N_k}^k$$

je řešitelná celými čísly $x_i \geqq 0$, ať je n jakékoliv číslo. Větu tuto dokázal Hilbert.

Je tedy $N_2 = 4$ a bylo by na př. $N_3 \leqq 9$, $N_4 \leqq 38$.

O této otázce viz na př. Bachmann 3, II., Landau I., str. 235; literaturu viz Dickson II.

VI. Pytagorovy trojúhelníky, velká věta Fermatova pro $n=4$, racionální trojúhelníky.

§ 50. Nazveme problémem Fermatovým úlohu, řešiti rovnici

$$x^n + y^n = z^n \tag{1}$$

čísly racionálními x, y, z; n je dané číslo celé kladné.

Jsou řešení samozřejmá, při nichž jedna z neznámých má hodnotu 0, totiž

$$x = 0,\ y = \pm z \text{ a } y = 0,\ x = \pm z \text{ pro } n \text{ sudé},$$
$$x = 0,\ y = z;\ y = 0,\ x = z;\ z = 0,\ x = -y \text{ pro } n \text{ liché}.$$

To jsou tak zvaná řešení triviální. Jest však otázka, zda vedle řešení triviálních existují jiná. Fermat vyslovil domněnku, že pro $n > 2$ jiných řešení není. Toto tvrzení se nazývá velkou větou Fermatovou*).

Je-li $n = n_1 n_2$, kdež n_1 a n_2 jsou čísla celá > 1, lze psáti (1) ve tvaru $(x^{n_2})^{n_1} + (y^{n_2})^{n_1} = (z^{n_2})^{n_1}$.

Platí-li tedy věta Fermatova pro mocnitele n_1, platí i pro mocnitele n, který je násobkem n_1. Aby věta Fermatova byla dokázána v plném rozsahu, stačí ji dokázati pro případ, kdy n je buď 4 neb n rovno libovolnému lichému prvočíslu.

Omezíme se na uvažování případů $n = 2$ a $n = 4$.

Nazveme řešením primitivním případ, kdy čísla x, y, z jsou čísla nesoudělná (a tudíž celá, viz § 4 str. 14). Mají-li x, y, z největšího společného dělitele $\neq \pm 1$, nazveme řešení takové neprimitivním. Je patrno, že stačí uvažovati řešení primitivní, ježto, mají-li x, y, z n. s. d. d, je $x/d, y/d, z/d$ řešení primitivní.

*) Fermat vyslovil tuto větu v rukopisné poznámce na okraji exempláře spisů Diofantových vydaných Bachetem.

Má-li řešení býti primitivní, stačí, aby dvě z čísel x, y, z byla spolu nesoudělná. Kdyby na př. x, y měla společného dělitele d, plynulo by z (1), že též z je d dělitelno.*)

§ 51. Případ $n = 2$.

Jedná se o řešení rovnice

$$x^2 + y^2 = z^2 \tag{1}$$

čísly racionálními x, y, z. Bez újmy všeobecnosti lze předpokládati, že x, y, z jsou čísla kladná. Pak x, y jsou odvěsny a z přepona pravoúhlého trojúhelníku. Úloze můžeme dáti tvar geometrický: Nalézti pravoúhlé trojúhelníky, jejichž strany jsou čísla racionální.

Takové trojúhelníky pravoúhlé nazývají se trojúhelníky Pytagorovy.

Konečně stačí se omeziti na řešení primitivní. Příslušný trojúhelník pravoúhlý nazveme také primitivní.

Uvažujeme-li pak rovnici (1) jako kongruenci (mod 2), vidíme, že z čísel x, y, z jsou dvě lichá, jedno sudé. Čísla x, y však nemohou býti lichá, tedy z sudé. Kdybychom totiž rovnici (1) uvažovali jako kongruenci (mod 4), dostali bychom $2 \equiv 0 \pmod 4$, což je nemožné. Je tedy jedna z hodnot x, y sudá, druhá lichá. Jelikož můžeme spolu x a y v (1) zaměniti, budeme předpokládati, že x je sudé, y liché; z pak bude liché.

Rovnici (1) lze psáti ve tvaru $y^2 = z^2 - x^2$ neb

$$y^2 = (z - x)(z + x). \tag{2}$$

Čísla $z - x$ a $z + x$ jsou spolu nesoudělná. Jejich společný dělitel musil by býti dělitelem jejich součtu $2z$ a jejich rozdílu $2x$. Ježto podle předpokladu x a z jsou nesoudělná, je 2 n. s. d. čísel

*) Z literatury, zabývající se větou Fermatovou hlavně na základě elementární číselné teorie, uvádím:

Lind: Über das letzte Fermatsche Theorem, Leipzig 1910.

Dickson, II, Chapter 21, 22, 26.

Teorii čísel algebraických předpokládají:

Hilbert: Theorie d. alg. Zahlkörper, Berlin 1897 (Jahresbericht d. d. Math.-Verein. 4).

Bachmann: Das Fermatproblem in seiner bisherigen Entwicklung, Leipzig-Berlin, 1919.

Landau, III.

Hasse: Bericht über neuere Untersuchungen aus der Theorie der algebraischer Zahlkörpen, T. II., Leipzig-Berlin 1930 (Jahresbericht d. d. Math.-Verein., Erg.-bd. 6).

Z posledně uvedeného spisu uvádím, že věta Fermatova je dokázána pro prvočísla $n < 307$ a pro prvočísla $n < 14.000$ v případě, že žádné z čísel x, y, z není dělitelné n.

$2z$ a $2x$. Avšak $z - x$ a $z + x$ jsou čísla lichá, jsou tedy skutečně nesoudělná.

Ježto součin čísel nesoudělných je čtverec čísla celého, platí

$$z + x = \varepsilon u^2, \quad z - x = \varepsilon v^2,$$

kdež $\varepsilon = \pm 1$ a u, v jsou čísla celá. Jsou to čísla lichá spolu nesoudělná. Ježto však, jak jsme již řekli, stačí uvažovati případ, kdy x, y, z jsou čísla kladná, bude $\varepsilon = 1$, tedy $z + x = u^2$, $z - x = v^2$.

Odtud plyne $x = \frac{1}{2}(u^2 - v^2)$, $z = \frac{1}{2}(u^2 + v^2)$, z (2) pak $y = uv$.

Aby bylo skutečně $x > 0$, dlužno voliti $u > v$.

Naopak, zvolíme-li u, v tak, aby splňovala uvedené podmínky, ale jinak libovolně, dostaneme dosazením za x, y, z do (1), že příslušná čísla x, y, z jsou primitivním řešením rovnice (1).

Dostáváme tedy primitivní řešení rovnice (1) *pomocí vzorců*

$$x = \tfrac{1}{2}(u^2 - v^2), \quad y = uv, \quad z = \tfrac{1}{2}(u^2 + v^2),$$

kdež u, v jsou čísla celá kladná lichá, spolu nesoudělná, $u > v$, jinak libovolná.

Vzorcům těm lze dáti trochu jiný tvar. Položme $\frac{1}{2}(u+v) = u'$, $\frac{1}{2}(u - v) = v'$. Lze snadno nahlédnouti, že u, v budou tehdy a jen tehdy vyhovovati podmínkám na ně kladeným, budou-li u', v' čísla celá spolu nesoudělná, kladná, jedno sudé, druhé liché a $u' > v'$. Lze tedy říci, že *primitivní kladná řešení rovnice* (1) *jsou dána vzorci* (*píšeme-li u, v místo u', v'*)

$$x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2,$$

kdež u, v jsou čísla celá kladná, jedno sudé, druhé liché, spolu nesoudělná, $u > v$, jinak libovolná.

Obecné řešení rovnice (1) *čísly racionálními* (*kladnými i zápornými*) *dostaneme pak buď ve tvaru*

$$x = \tfrac{1}{2}\, d(u^2 - v^2), \quad y = duv, \quad z = \tfrac{1}{2}\, d(u^2 + v^2),$$

kdež u, v splňují právě uvedené podmínky a jinak jsou libovolné, neb ve tvaru

$$x = 2duv, \quad y = d\,(u^2 - v^2), \quad z = d\,(u^2 + v^2),$$

kdež u, v jsou čísla celá kladná lichá, spolu nesoudělná, $u > v$, jinak libovolná, d je libovolné číslo racionální.

Označíme-li v trojúhelníku Pytagorově o stranách x, y, z α úhel ležící proti x, β úhel proti y, je

$$\sin\alpha = \cos\beta = \frac{x}{z} = \frac{2uv}{u^2 + v^2} = \frac{2\lambda}{1 + \lambda^2},$$

$$\cos\alpha = \sin\beta = \frac{y}{z} = \frac{u^2 - v^2}{u^2 + v^2} = \frac{1 - \lambda^2}{1 + \lambda^2},$$

klademe-li $\lambda = v/u$.

λ má jednoduchý geometrický význam:

$$\lambda = \operatorname{tg} \tfrac{1}{2}\alpha.$$

Úhel α, jehož sin a cos jsou racionální, nazveme úhlem racionálním. Je-li $\operatorname{tg} \frac{1}{2}\alpha$ racionální, je úhel α racionální. Je totiž

$$\sin\alpha = \frac{2 \operatorname{tg} \frac{1}{2}\alpha}{1 + \operatorname{tg}^2 \frac{1}{2}\alpha}, \quad \cos\alpha = \frac{1 - \operatorname{tg}^2 \frac{1}{2}\alpha}{1 + \operatorname{tg}^2 \frac{1}{2}\alpha}.$$

A naopak u racionálních úhlů je $\operatorname{tg} \frac{1}{2}\alpha$ racionální neb ∞. Je totiž

$$\operatorname{tg} \tfrac{1}{2}\alpha = \frac{\sin\alpha}{1 + \cos\alpha}.$$

§ 52. Věta Fermatova pro $n = 4$.

Dokážeme, že *rovnice obecnější*

$$x^4 + y^4 = z^2 \tag{1}$$

nemá jiných řešení čísly racionálními vyjma ta, kde buď x neb y je rovno 0.

Můžeme předpokládati, že x, y, z jsou čísla celá nesoudělná. Dejme tomu, že by n. s. d. čísel x, y, z byl d, $d \mid \neq 1$. Položme $x = dx'$, $y = dy'$, $z = dz'$. Pak x', y', z' jsou čísla celá nesoudělná. I dostali bychom z rovnice (1)

$$d^2 (x'^4 + y'^4) = z'^2.$$

Pak $(z'/d)^2$ by bylo číslo celé, tedy i z'/d. Položme $z' = dz''$. x', y', z'' by splňovala rovnici $x'^4 + y'^4 = z''^2$, téhož tvaru jako (1). Ježto x', y', z' jsou čísla spolu nesoudělná, jsou spolu také nesoudělná čísla $x', y', z'' = z'/d$.

Z předpokladu, že x, y, z jsou čísla spolu nesoudělná, plyne, že nejsou všechna sudá; není také možno, aby byla dvě sudá a jedno liché, ani aby byla všechna tři lichá. Je tedy jedno sudé, dvě lichá. Uvažujeme-li pak (1) jako kongruenci (mod 4), shledáváme, že není možno, aby x, y byla lichá, z sudé. Je tedy z liché a jedno z čísel x, y sudé, druhé liché.

Předpokládejme, že je x sudé, y liché, $x = 2^n x'$, kdež je n číslo celé $\geqq 1$, x' číslo liché. Z dané rovnice dostaneme

$$2^{4n} x'^4 = z^2 - y^4,$$

kdež x', y, z jsou čísla lichá spolu nesoudělná.

Provedeme důkaz, že rovnice obecnější

$$\varepsilon \cdot 2^{2n}x^4 = z^2 - y^4, \tag{2}$$

kdež $\varepsilon = \pm 1$ a n je číslo celé kladné, není řešitelná čísly lichými nesoudělnými x, y, z. Důkaz provedeme úplnou indukcí.

Pro $n = 1$ dostaneme rovnici

$$4\varepsilon x^4 = z^2 - y^4. \tag{3}$$

Uvažujme ji jako kongruenci(mod 8). Pro lichá čísla x, y, z platí

$$x \equiv \pm 1,\ y \equiv \pm 1,\ z \equiv \pm 1 \pmod 4,$$

tedy

$$x^4 \equiv 1,\ y^4 \equiv 1,\ z^2 \equiv 1 \pmod 8.$$

Tak bychom dostali z (3) nemožnou kongruenci $4\varepsilon \equiv 0 \pmod 8$. Není tedy rovnice (3) řešitelná čísly lichými.

Budiž nyní v (2) $n > 1$. Pišme (2) ve tvaru

$$\varepsilon \cdot 2^{2n}x^4 = (z - y^2)(z + y^2). \tag{4}$$

Snadno lze nahlédnouti, že $z - y^2$ a $z + y^2$ mají n. s. d. 2. Bude tedy

$$z - y^2 = \varepsilon' \cdot 2u^4,\ z + y^2 = \varepsilon'' \cdot 2^{2n-1}v^4 \tag{5}$$

$$\text{neb}\quad z - y^2 = \varepsilon' \cdot 2^{2n-1}u^4,\ z + y^2 = \varepsilon'' \cdot 2v^4 \tag{6}$$

($\varepsilon', \varepsilon'' = \pm 1$, $\varepsilon'\varepsilon'' = \varepsilon$, u, v čísla lichá nesoudělná).

Ale soustavu (6) dostaneme ze soustavy (5), zaměníme-li z v $-z$, ε' v $-\varepsilon''$, ε'' v $-\varepsilon'$, u ve v, v v u. Stačí tedy uvažovati (5). Odtud plyne

$$y^2 = \varepsilon'' \cdot 2^{2n-2}v^4 - \varepsilon' u^4. \tag{7}$$

Je-li $n > 1$, bude, uvažujeme-li tuto rovnici jako kongruenci (mod 4), $y^2 \equiv -\varepsilon' u^4 \pmod 4$, tedy $\varepsilon' = -1$. I dostaneme z rovnice (7) rovnici

$$\varepsilon'' \cdot 2^{2(n-1)}v^4 = y^2 - u^4$$

téhož tvaru jako (2), jenže místo n je $n - 1$. Tím důkaz proveden.

Zároveň je též patrno, že *věta Fermatova platí pro každý exponent dělitelný čtyřmi.*

Rovnice (2) se vyskytuje při důkaze věty:

Plocha pravoúhlého trojúhelníku s celými stranami není nikdy čtvercem, ani dvojnásobným čtvercem čísla racionálního.

Jinak řečeno: Není možno najíti čísla racionální x, y, z, t tak, aby platilo

$$x^2 + y^2 = z^2,$$

$$xy = 2^k t^2,\ k = 0 \text{ neb } 1.$$

Stačí se omeziti na primitivní řešení první rovnice. Čísla x, y jsou pak nesoudělná, jedno z nich, na př. x, sudé, druhé, y, liché. Z rovnice $xy = 2^k t^2$, $k = 0$ neb 1 plyne, že t^2 je číslo celé, takže i t je celé. Pišme rovnici tu ve tvaru $xy = 2^n s^2$, kdež s je číslo celé liché, n číslo celé > 0. I dostaneme, protože x a y jsou nesoudělná,

$$x = 2^n u^2, \quad y = v^2.$$

První pak přejde v rovnici

$$2^{2n} u^4 + v^4 = z^2$$

a ta je skutečně neřešitelná čísly celými $u, v, z \neq 0$.

§ 53. Trojúhelník, jehož strany a, b, c a plocha Δ jsou čísla racionální, nazveme trojúhelníkem racionálním (Heronovým). Trojúhelník Pytagorův je racionální.

V racionálním trojúhelníku jsou výšky v_1, v_2, v_3, poloměr kružnice opsané R, poloměr kružnice vepsané ϱ, poloměry kružnic vně vepsaných $\varrho_1, \varrho_2, \varrho_3$ čísla racionální. Úhly takového trojúhelníku α, β, γ jsou racionální.

Je totiž

$$2\Delta = av_1 = bv_2 = cv_3,$$
$$4\Delta R = abc,$$

$\Delta = s\varrho = (s-a)\varrho_1 = (s-b)\varrho_2 = (s-c)\varrho_3$, kdež $2s = a+b+c$, $\varrho = (s-a)\operatorname{tg}\frac{1}{2}\alpha = (s-b)\operatorname{tg}\frac{1}{2}\beta = (s-c)\operatorname{tg}\frac{1}{2}\gamma$.

Klademe-li

$$\operatorname{tg}\tfrac{1}{2}\alpha = \lambda, \quad \operatorname{tg}\tfrac{1}{2}\beta = \mu,$$

bude

$$\operatorname{tg}\tfrac{1}{2}\gamma = \frac{1}{\operatorname{tg}\frac{1}{2}(\alpha+\beta)} = \frac{1-\lambda\mu}{\lambda+\mu},$$

$$\sin\alpha = \frac{2\lambda}{1+\lambda^2}, \quad \sin\beta = \frac{2\mu}{1+\mu^2}, \quad \sin\gamma = \frac{2(\lambda+\mu)(1-\lambda\mu)}{(1+\lambda^2)(1+\mu^2)}.$$

Ježto

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R,$$

bude

$$a = \frac{4\lambda R}{1+\lambda^2}, \quad b = \frac{4\mu R}{1+\mu^2}, \quad c = \frac{4(\lambda+\mu)(1-\lambda\mu)R}{(1+\lambda^2)(1+\mu^2)},$$

$$\Delta = \frac{16\lambda\mu(\lambda+\mu)(1-\lambda\mu)R^2}{(1+\lambda^2)^2(1+\mu^2)^2},$$

$$s = \frac{4(\lambda+\mu)R}{(1+\lambda^2)(1+\mu^2)}, \quad \varrho = \frac{4\lambda\mu(1-\lambda\mu)R}{(1+\lambda^2)(1+\mu^2)},$$

$$s-a = \frac{4\mu(1-\lambda\mu)R}{(1+\lambda^2)(1+\mu^2)}, \quad s-b = \frac{4\lambda(1-\lambda\mu)R}{(1+\lambda^2)(1+\mu^2)},$$

$$s-c = \frac{4\lambda\mu(\lambda+\mu)R}{(1+\lambda^2)(1+\mu^2)}.$$

Zvolíme-li za λ, μ, R racionální čísla >0, $\lambda\mu<1$ (aby $\operatorname{tg}\frac{1}{2}\gamma>0$), budou a, b, c, Δ, ježto jsou racionální funkce λ, μ, R, též čísla racionální a trojúhelník bude pak racionální.

LITERATURA:

Bachmann: *1.* Zahlentheorie I. Die Elemente der elementaren Zahlentheorie, Lipsko 1925.
2. Grundlehren der neueren Zahlentheorie, 2. vyd. Berlín, Lipsko 1921.
3. Niedere Zahlentheorie, Lipsko I. 1901, II. 1910.

Cahen: *1.* Eléments de la théorie des nombres, Paříž 1900.
2. Théorie des nombres, Paříž I. 1914, II. 1924.

Dickson: History of the theory of numbers, Washington I. 1919, II. 1920, III. 1923.

Encyklopädie der mathematischen Wissenschaften: I C 1, *Bachmann:* Niedere Zahlentheorie.

Hensel: Zahlentheorie, Berlín, Lipsko 1913.

Kraïtchik: 1. Théorie des nombres, Paříž I. 1922, II. 1926.
2. Recherches sur la théorie des nombres, Paříž I. 1924, II. 1929.

Landau: Vorlesungen über Zahlentheorie, I.—III., Lipsko 1927.

Lucas: Théorie des nombres, Paříž 1891.

Lejeune-Dirichlet, Dedekind: Vorlesungen über Zahlentheorie, 4. vyd. Brunšvig 1894.

Studnička: Základové nauky o číslech, Praha 1875.

Weber-Wellstein: Encyklopädie der Elementarmathematik, I. Arithmetik, Algebra u. Analysis, 4. vyd. zpr. Epstein, Lipsko, Berlín 1922.

Wertheim: 1. Elemente der Zahlentheorie, Lipsko 1887.
2. Anfangsgründe der Zahlenlehre, Brunšvig 1902.

Abecední seznam.

Čísla za hesly značí stránky knihy. Číslo stránky, kde jest uvedena definice pojmu, jest vytištěno kursivou.

T

U

V

W

Z

OBSAH.

III. g-adické zlomky.

IV. Kvadratické zbytky, kvadratický zákon reciprocity a znázornění prvočísel formami $x^2 + my^2$.

V. Znázornění čísel celých kladných formou $x_1^2 + x_2^2 + x_3^2 + x_4^2$.

VI. Pytagorovy trojúhelníky, velká věta Fermatova pro $n=4$, racionální trojúhelníky.