II. Kongruence

In: Karel Rychlík (author): Úvod do elementární teorie číselné. (Czech). Praha: Jednota čs. matematiků a fysiků, 1931. pp. 30–55.

Persistent URL: http://dml.cz/dmlcz/402939

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 $\pmod{m_i}$, 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

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