Karel Koutský

# Rozdělení n-tých potenčních zbytků pro prvočíselný modul

*Časopis pro pěstování matematiky a fysiky*, Vol. 59 (1930), No. 2, 65--82

Persistent URL: http://dml.cz/dmlcz/122744

# Rozdělení n-tých potenčních zbytků pro prvočíselný modul.

*Dr. Karel Koutský*, profesor čes. reálky v Hodoníně.

## Úvod.

1. Budiž $n$ nějaké celé a kladné číslo, $p$ pak budiž liché prvočíslo $> 1$, tak, že největší společná míra čísel $n$, $(p-1)$ jest:

$$\mu = (n,\ p-1) \tag{1}$$

Z této relace pak plyne, že číslo $(p-1)$ jest dělitelno číslem $\mu$, což lze psáti:

$$\mu/(p-1). \tag{1'}$$

*n-tým potenčním charakterem nějakého čísla* $a \not\equiv 0 \pmod p$ *nazývám pak hodnotu* $x$, *splňující kongruenci*:

$$x \equiv a^{\frac{p-1}{\mu}} \pmod p. \tag{2}$$

Umocníme-li tuto kongruenci číslem $\mu$, potom vzhledem k Fermatově poučce obdržíme:

$$x^{\mu} \equiv 1 \pmod p, \tag{3}$$

z čehož pak plyne, že každý $n$-tý potenční charakter nějakého čísla $\not\equiv 0 \pmod p$ jest kořenem této kongruence (3).

Vzhledem k vztahu (1') má kongruence (3) právě $\mu$ vzájemně nekongruentních i od nuly odlišných kořenů (mod $p$). Je-li nyní $\varrho$ nějaký primitivní kořen kongruence (3), t. j. číslo, které patří právě k exponentu $\mu$, t. j. číslo, jehož žádná nižší až teprve $\mu$-tá mocnina jest kongruentní s $+1 \pmod p$, potom všechny kořeny kongruence (3) jsou obsaženy v řadě:

$$\varrho^1,\ \varrho^2,\ \varrho^3, \ldots . \varrho^{\mu-1},\ \varrho^{\mu} \equiv 1 \pmod p \tag{4}$$

Žádné dva členy této řady nejsou spolu kongruentní (mod $p$), neboť jinak $\varrho$ by patřilo již k nižšímu exponentu než $\mu$, což však podle předchozí úmluvy jest vyloučeno. Poněvadž pak tyto kořeny jsou, jak již bylo řečeno, $n$-tými potenčními charaktery čísel $\not\equiv 0 \pmod p$, plyne odtud věta:

*Počet rozličných n-tých potenčních charakterů všech čísel nekongruentních s nulou (mod p) rovná se číslu μ.*

Potom ale pro každé číslo $a \not\equiv 0 \pmod p$ lze nalézti jisté celé a kladné číslo $i \leqq \mu$ tak, aby platilo:

$$a^{\frac{p-1}{\mu}} \equiv \varrho^i \pmod p. \tag{5}$$

Kongruence tato jest jistě řešitelná podle $a$, neboť $\varrho^i$ jest (pro každý exponent $i$) vždy $\frac{p-1}{\mu}$-tým potenčním zbytkem (mod $p$), a proto kongruence (5) má $\frac{p-1}{\mu}$ právě rozličných kořenů; platí totiž:

$$(\varrho^i)^{\frac{p-1}{\mu}} \equiv (\varrho^i)^\mu \equiv (\varrho^\mu)^i \equiv 1 \pmod p$$

Z toho pak plyne, že *všechna čísla* $\not\equiv 0$ *(mod p) rozpadají se podle svého n-tého potenčního charakteru (mod p) na μ skupin tak, že každá z těchto skupin obsahuje právě* $\frac{p-1}{\mu}$ *vzájemně nekongruentních členů (mod p).*

Poznámky: *a)* Čísla, jejichž $n$-tý potenční charakter (mod $p$) rovná se $\varrho^\mu \equiv 1 \pmod p$, jsou $n$-tými potenčními zbytky (mod $p$).

*b)* Čísla kongruentní s nulou (mod $p$) nemají (podle předešlého) vůbec žádného $n$-tého potenčního charakteru (mod $p$). Mohli bychom však analogicky říci, že $n$-tý potenční charakter čísel kongruentních s nulou (mod $p$) rovná se nule (není v řadě (4) obsažený); místo toho však z důvodů, které se ukáží později, říkáme, že $n$-tý potenční charakter (mod $p$) čísla kongruentního s nulou (mod $p$) jest nultého stupně (mod $p$).

Obráceně pak, jestliže $n$-tý potenční charakter nějakého čísla jest nultého stupně (mod $p$), potom toto číslo jest kongruentní s nulou (mod $p$).

*c)* Samozřejmé jest dále, že každá dvě kongruentní čísla (mod $p$) mají tentýž $n$-tý potenční charakter (mod $p$).

*d)* Pro $n = \mu = 2$ dostáváme pak kvadratické charaktery čísel. Charaktery jsou tu dva, totiž:

$$\varrho^1 \equiv -1, \quad \varrho^2 \equiv +1 \pmod p$$

které se obyčejně symbolisují Legendreovým symbolem $\left(\frac{a}{p}\right)$.

2. *O každém čísle* $a \not\equiv 0$ *(mod p), které splňuje vztah:*

$$a^{\frac{p-1}{\varkappa}} \equiv (a+1)^{\frac{p-1}{\mu}} \equiv (a+2)^{\frac{p-1}{\mu}} \equiv \ldots$$

$$\ldots \equiv (a + k - 1)^{\frac{p-1}{\mu}} \not\equiv (a + k)^{\frac{p-1}{\mu}} \pmod{p}, \qquad (6)$$

*kdež $k$ jest nějaké celé a kladné číslo, říkám, že jeho $n$-tý potenční charakter jest $k$-tého stupně (mod $p$).*

Číslo $a \equiv -1 \pmod{p}$ má $n$-tý potenční charakter právě 1. stupně (mod $p$), neboť předešlý vztah jest splněn pro $k = 1$, nikoliv však pro $k > 1$.

Každé jiné číslo $a \not\equiv 0 \pmod{p}$ má $n$-tý potenční charakter aspoň 1. stupně (mod $p$), t. j. buď právě 1. stupně nebo stupně vyššího, neboť vztah (6) jest splněn buď pro $k = 1$ nebo pro $k > 1$.

Číslo 0 (mod $p$) splňuje též vztah (6) pro $k = 1$, nikoliv však pro $k > 1$, a patřilo by tedy vlastně mezi čísla, jejichž $n$-tý potenční charakter jest právě 1. stupně (mod $p$). Avšak všechna čísla $\not\equiv 0 \pmod{p}$, jejichž $n$-tý potenční charakter jest buď prvního anebo vyššího stupně (mod $p$), dají se vyjádřiti jistými kongruencemi, z nichž však žádná neposkytuje číslo 0. Tvoří tedy číslo 0 (mod $p$) jakousi skupinu samo pro sebe a z tohoto důvodu říkám, že $n$-tý potenční charakter čísla 0 jest nultého stupně (mod $p$).

3. Uvažujme nyní dvě sousední celá čísla $a$, $(a + 1)$, z nichž ani jedno není kongruentní s nulou (mod $p$) a jejichž $n$-té potenční charaktery buďtež $\varrho^i$, $\varrho^k$.

Symbolem:

$$x_{i,k} = (\varrho^i, \varrho^k) \qquad (7)$$

označme počet dvojskupin $a$, $(a + 1)$ v řadě:

$$1, 2, 3, \ldots\ldots, p - 2, p - 1, \qquad (8)$$

z nichž první číslo má $n$-tý potenční charakter $\varrho^i$, druhé číslo má pak $n$-tý potenční charakter $\varrho^k$.

Obecně pak jest: $x_{i,k} \neq x_{k,i}$ a obdržíme tedy $\mu^2$ hodnot $x_{i,k}$, pro něž stanovíme určité relace.

4. Vyjádření čísel, jejichž $n$-tý potenční charakter jest právě 1. stupně anebo aspoň 2. stupně.

Budiž $a$ číslo, které vyhovuje kongruenci:

$$au^s t^n \equiv a + 1 \pmod{p},$$

z níž plyne:

$$a \equiv \frac{1}{u^s t^n - 1} \pmod{p}. \qquad (9)$$

Při tom $t$ jest nějaké proměnlivé číslo (mod $p$), $s$ pak určité číslo z řady 1, 2, 3, ...., $\mu$ a $u$ číslo, jehož $n$-tý potenční charakter (mod $p$) jest právě $\varrho$:

$$u^{\frac{p-1}{\mu}} \equiv \varrho \pmod{p} \qquad (10)$$

Nechť $t$ jest nyní jakékoliv číslo, kongruence (9) nikdy neposkytne číslo $a$, jež by bylo kongruentní s nulou (mod $p$). Jest tedy zcela obecně: $a \not\equiv 0 \pmod{p}$. V tom leží právě důvod, proč o $n$-tém potenčním charakteru čísla 0 (mod $p$) říkáme, že jest nultého stupně (mod $p$).

Je-li však $t \equiv 0 \pmod{p}$, potom kongruence (9) pro jakékoliv číslo $s$ vždy poskytne $a \equiv -1 \pmod{p}$. Obráceně pak kongruence $a \equiv -1 \pmod{p}$ má za svůj následek, podle kongruence (9), $t \equiv 0 \pmod{p}$. — Poněvadž však číslo $(-1)$ nemůže státi na prvním místě v našich dvojskupinách $(a, a+1)$, vylučme toto číslo ze svých úvah, což má za následek $t \not\equiv 0 \pmod{p}$.

Mimo to v kongruenci (9) nesmí býti jmenovatel zlomku na její pravé straně býti kongruentní s nulou (mod $p$), neboť to by vedlo k nesrovnalosti. Přistoupí tedy k naší kongruenci (9) ještě podmínka:

$$t(u^s t^n - 1) \not\equiv 0 \pmod{p} \qquad (9')$$

Každé číslo $a$ reprodukované kongruencí (9) za podmínky (9') jest nyní kongruentní (mod $p$) s jedním a jen jedním číslem řady:

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

a může tedy státi na prvním místě ve skupině $(a, a+1)$, kterou počítáme do počtu $x_{i,k} = (\varrho^i, \varrho^k)$.

Z kongruence (9) pak plyne dále:

$$a + 1 \equiv \frac{u^s t^n}{u^s t^n - 1} \pmod{p} \qquad (11)$$

Hledejme nyní vztah mezi $n$-tými potenčními charaktery čísel $a$, $(a+1)$. Tu bude:

$$(a+1)^{\frac{p-1}{\mu}} \equiv \frac{(u^s t^n)^{\frac{p-1}{\mu}}}{(u^s t^n - 1)^{\frac{p-1}{\mu}}} \pmod{p},$$

čili vzhledem k podmínce (9') a relaci (10) též:

$$(a+1)^{\frac{p-1}{\mu}} \equiv \varrho^s \left(\frac{1}{u^s t^n - 1}\right)^{\frac{p-1}{\mu}} = a^{\frac{p-1}{\mu}} \cdot \varrho^s \pmod{p} \qquad (12)$$

Je-li nyní $n$-tý potenční charakter čísla $a$ rovný $\varrho^i$, $n$-tý potenční charakter čísla $(a+1)$ bude $\varrho^{i+s}$, takže číslo $a$ bude patřiti mezi čísla skupiny:

$$x_{i,i+s} = (\varrho^i, \varrho^{i+s}), \qquad (13)$$

při čemž $s$ jest nějaké pevné číslo v mezích $[1, 2, \ldots\ldots, \mu]$.

Z toho jest zřejmo, že pro $s \not\equiv 0 \pmod{\mu}$, kongruence (9) udává čísla, jejichž $n$-tý potenční charakter jest právě 1. stupně (mod $p$), naproti tomu pro $s \equiv 0 \pmod{\mu}$ kongruence (9) reprodukuje čísla, jejichž $n$-tý potenční charakter jest aspoň 2. stupně (mod $p$).

Jestliže nyní číslo $i$ probíhá všechny možné hodnoty $1, 2, \ldots, \mu$, potom výraz:

$$\sum_{i=1}^{\mu} x_{i,\,i+s} \tag{14}$$

udává počet všech nekongruentních čísel $a$, jež jsou reprodukována kongruencí (9) za podmínky (9′) pro konstantní $s$.

Při tom indexy u veličin $x_{i,\,i+s}$ nutno vzíti in modulo $\mu$.

Tento počet čísel reprodukovaných kongruencí (9) lze snadno stanoviti.

Mají-li dvě čísla $t_1$, $t_2$ vésti podle kongruence (9) k témuž číslu $a$. musí býti splněn vztah:

$$\frac{1}{u^s t_1^{\,n} - 1} \equiv \frac{1}{u^s t_2^{\,n} - 1} \pmod{p},$$

z něhož po úpravě plyne:

$$t_1^{\,n} \equiv t_2^{\,n} \pmod{p}.$$

Tato kongruence jest ale nyní řešitelná. Poněvadž: $t_1 \not\equiv 0$, $t_2 \not\equiv 0$, možno ji psáti v tvaru:

$$\left(\frac{t_1}{t_2}\right)^n \equiv 1 \pmod{p}$$

a tu lehce, vzhledem k relaci (1), vidíme, že tato kongruence má právě $\mu$ vzájemně nekongruentních kořenů, udaných řadou (4), takže jest:

$$\frac{t_1}{t_2} \equiv \varrho^j \pmod{p},$$

čili: $$j = 1, 2, \ldots, \mu$$

$$t_1 \equiv \varrho^j \cdot t_2 \pmod{p}.$$

Jestliže $t$ jest nyní číslo, které vede k číslu $a$, potom k témuž číslu $a$ vede $\mu$ nekongruentních hodnot, totiž:

$$t \cdot \varrho,\ t \cdot \varrho^2, \ldots, t \cdot \varrho^{\mu-1},\ t \cdot \varrho^{\mu} \equiv t \pmod{p}. \tag{15}$$

Nyní jest třeba stanoviti počet přípustných hodnot $t$. Vyloučeny jsou pro $t$ jen ty hodnoty, které odporují ppdmínce (9′). Nejprve jest to hodnota $t \equiv 0 \pmod{p}$ a potom hodnoty splňující kongruenci:

$$u^s t^n \equiv 1 \pmod{p} \tag{16}$$

Aby tato kongruence byla řešitelná, muselo by $u^s$ býti $n$-tým potenčním zbytkem (mod $p$), t. j. muselo by platiti:

$$(u^s)^{\frac{p-1}{\mu}} \equiv 1 \pmod{p},$$

čili vzhledem ke kongruenci (10) též:

$$\varrho^s \equiv 1 \pmod{p}.$$

Poněvadž však $\varrho$ patří právě k exponentu $\mu$, předešlá kongruence bude splněna jen tenkráte, bude-li:

$$s \equiv 0 \pmod{\mu\ p}$$

Tedy pokud jest: $s \not\equiv 0 \pmod{\mu}$, vyloučena jest pro $t$ jen jedna hodnota, totiž: $t \equiv 0 \pmod{p}$, takže počet přípustných hodnot $t$ jest udán číslem $(p-1)$.

Je-li však $s \equiv 0 \pmod{\mu}$, potom mimo hodnotu 0 jest vyloučeno ještě dalších $\mu$ hodnot, které splňují kongruenci (16), takže počet přípustných hodnot $t$ rovná se v tomto případě číslu $(p-1-\mu)$.

Z těchto přípustných hodnot pro $t$ vede jich vždy $\mu$ k témuž číslu $a$, takže pro výraz (14) dostáváme relace:

*a*) pokud jest:

$$s \not\equiv 0 \pmod{\mu}$$

čili:

$$s = 1, 2, 3, \ldots, \mu - 1$$

platí:

$$\sum_{i=1}^{\mu} x_{i,i+s} = \frac{p-1}{\mu}; \tag{17}$$

*b*) je-li však:

$$s \equiv 0 \pmod{\mu},$$

platí:

$$\sum_{i=1}^{\mu} x_{i,i+s} \equiv x_{1,1} + x_{2,2} + x_{3,3} + \ldots + x_{\mu,\mu} = \frac{p-1}{\mu} - 1. \tag{18}$$

Indexy při veličinách $x_{i,i+s}$ nutno ovšem vzíti (mod $\mu$). Takto jsme získali $\mu$ nezávislých rovnic pro $\mu^2$ neznámých. Že rovnice tyto jsou skutečně nezávislé, plyne již z té okolnosti, že každá z nich obsahuje jiné neznámé.

5. **Počet nekongruentních čísel, jejichž $n$-tý potenční charakter jest právě prvního stupně (mod $p$).**

Číslo, jehož $n$-tý potenční charakter jest právě prvního stupně (mod $p$), musí splňovati vztah (6) pro $k = 1$. Musí tedy býti:

$$a^{\frac{p-1}{\mu}} \not\equiv (a+1)^{\frac{p-1}{\mu}} \pmod{p},$$

tedy $a^{\frac{p-1}{\mu}} \equiv \varrho^i$, $(a+1)^{\frac{p-1}{\mu}} \equiv \varrho^{i+s} \pmod p$

kdež:

$$s \not\equiv 0 \pmod \mu.$$

Snadno pak vidíme, že počet vzájemně nekongruentních čísel, jejichž $n$-tý potenční charakter jest právě 1. stupně (mod $p$) a která jsou při tom obsažena v řadě $1, 2, \ldots, p-2$, jest udán součtem rovnic (17) pro všechna přípustná $s$; obdržíme tedy:

$$\sum_{s=1}^{\mu-1} \sum_{i=1}^{\mu} x_{i,\,i+s} = \frac{(\mu-1)(p-1)}{\mu}$$

*Počet všech nekongr. čísel, jejichž n-tý potenční charakter jest právě prvního stupně* (mod $p$), jest pak o jednotku větší, neboť přistupuje ještě číslo $(p-1)$, které nemůže státi na 1. místě v našich dvojskupinách $(a, a+1)$. Tento počet jest pak udán číslem:

$$\frac{(\mu-1)(p-1)}{\mu} + 1 \qquad (19)$$

Poznámka: Pro $n = \mu = 2$ obdržíme čísla, jejichž kvadratický charakter jest právě 1. stupně (mod $p$).[1]) Jejich počet jest pak vyjádřen číslem:

$$\frac{p-1}{2} + 1 = \frac{p+1}{2}$$

6. Počet nekongruentních čísel, jejichž $n$-tý potenční charakter jest aspoň 2. stupně (mod $p$), jest udán rovnicí (18). Tento počet možno též vypočítati, jestliže od počtu všech čísel, jež nejsou kongruentní s nulou (mod $p$), odečteme počet čísel, jejichž $n$-tý potenční charakter jest právě 1. stupně (mod $p$). V obou případech obdržíme tentýž výsledek, takže *počet všech nekongruentních čísel, jejichž n-tý potenční charakter jest aspoň 2. stupně* (mod $p$), jest udán číslem:

$$\frac{p-1}{\mu} - 1 \qquad (20)$$

Poznámka: Pro $n = \mu = 2$ obdržíme počet nekongr. čísel, jejichž kvadratický charakter jest aspoň 2. stupně (mod $p$). Těchto

[1]) Pojem čísel, jejichž kvadratický charakter jest $k$-tého stupně (mod $p$) a která tedy vyhovují vztahu (6) pro $\mu = 2$, jest úplně totožný *s pojmem čísel k-tého stupně*, tak jak jsem ho užíval ve své práci: *Poznámka ke kvadratickému charakteru čísel.* (Časopis pro pěst. mat. a fys., roč. 58, str. 42—52, Praha 1929). Podobně viz moji práci: *O kvadratickém charakteru čísel a zobecnění jisté Lagrangeovy věty o rozdělení kvadratických zbytků*, kterou jsem právě předložil České Akademii věd a umění v Praze.

čísel jest právě $\frac{1}{2}(p-1)-1 = \frac{1}{2}(p-3)$. Jsou to pak ona čísla, jež jsem nazýval v již citovaných pracích čísly aspoň 2. stupně (mod $p$).

7. Určení hodnot $x_{i,k} = (\varrho^i, \varrho^k)$.

Uvažujme nyní všechna čísla, která splňují kongruenci:

$$(a+1)^{\frac{p-1}{\mu}} \equiv \varrho^s a^{\frac{p-1}{\mu}} \pmod{p} \tag{21}$$

jež jest totožná s kongruencí (12).

O této kongruenci možno dokázati, že:

*a*) počet jejích kořenů rovná se: $\frac{p-1}{\mu}$, je-li: $s \not\equiv 0 \pmod{\mu}$;

*b*) počet jejích kořenů rovná se: $\frac{p-1}{\mu} - 1$, je-li: $s \equiv 0 \pmod{\mu}$.

Důkaz byl již vlastně proveden během předešlého vyšetřování. Poněvadž však tato okolnost jest pro nás velmi důležitá, proveďme důkaz nový.

Kongruenci (21) jistě nesplňují hodnoty: $a \equiv 0, -1 \pmod{p}$, neboť to by vedlo k nesrovnalosti. Dělme tedy tuto kongruenci číslem $a^{\frac{p-1}{\mu}}$ a tak získáme:

$$y^{\frac{p-1}{\mu}} \equiv \left(1 + \frac{1}{a}\right)^{\frac{p-1}{\mu}} \equiv \varrho^s \pmod{p} \tag{22}$$

Poněvadž pak $\varrho^s$ jest $n$-tý potenční charakter (mod $p$), což znamená, že $\varrho^s$ jest též $\frac{p-1}{\mu}$-tým potenčním zbytkem (mod $p$), má předešlá kongruence právě $\frac{p-1}{\mu}$ kořenů. Budiž $y_r$ jeden kořen této kongruence. Potom jest:

$$y_r \equiv 1 + \frac{1}{a} \pmod{p}$$

čili:

$$a \equiv \frac{1}{y_r - 1} \pmod{p} \tag{22'}$$

Má-li však tato kongruence míti význam, nesmí v ní býti $y_r \equiv 1 \pmod{p}$.

A skutečně, pokud jest: $s \not\equiv 0 \pmod{\mu}$, žádný z kořenů kongruence (22) není kongruentní s $+1 \pmod{p}$, a tedy kongruence (22') poskytuje tolik hodnot $a$, kolik jest hodnot $y_r$, a těchto jest: $\frac{p-1}{\mu}$, čímž dokázána první část našeho tvrzení.

Je-li však: $s \equiv 0 \pmod{\mu}$, potom jest $\varrho^s \equiv 1 \pmod{p}$, a jeden kořen $y_r$ kongruence (22) jest kongruentní s jednotkou (mod $p$). Tento kořen pak nevede podle kongruence (22′) k žádnému číslu $a$. Žádný z $\frac{p-1}{\mu} - 1$ zbývajících kořenů $y$ kongruence (22) pak není kongruentní s jednotkou (mod $p$) a každý z nich vede pak k jednomu číslu $a$, čímž dokázána i druhá část našeho tvrzení.

Nechť kongruence (21) má $d$ kořenů:

$$a_1, a_2, a_3, \ldots\ldots, a_{d-1}, a_d, \tag{23}$$

kdež: $d = \frac{p-1}{\mu}$, pokud: $s \equiv | \equiv 0 \pmod{\mu}$, resp.: $d = \frac{p-1}{\mu} - 1$, je-li: $s \equiv 0 \pmod{\mu}$.

Z těchto kořenů (23) bude jich právě $x_{i,\,i+s}$ míti vlastnost, že jejich $n$-tý potenční charakter (mod $p$) bude se rovnati číslu $\varrho^i$ (mod $p$). — Jestliže nyní číslo $i$ probíhá řadu $1, 2, 3, \ldots\ldots, \mu$, potom obdržíme postupně všechny kořeny kongruence (21).

Označme nyní:

$$\lambda_{k,s} \equiv \sum a^{k\frac{p-1}{\mu}} \equiv a_1^{k\frac{p-1}{\mu}} + a_2^{k\frac{p-1}{\mu}} + \ldots + a_d^{k\frac{p-1}{\mu}} \pmod{p}. \tag{24}$$

Vzhledem k tomu, co bylo právě řečeno o kořenech (23) kongruence (21) a o veličinách $x_{i,\,i+s}$, možno tuto kongruenci psáti též ve tvaru:

$$\lambda_{k,s} \equiv \varrho^k \,.\, x_{1,\,1+s} + \varrho^{2k} \,.\, x_{2,\,2+s} + \varrho^{3k} \,.\, x_{3,\,3+s} + \ldots$$
$$\ldots + \varrho^{\mu k} \,.\, x_{\mu,\,\mu+s} \pmod{p}, \tag{25}$$

kdež $s$ jest pevné číslo, $k$ pak proměnlivé číslo (mod $\mu$). Indexy při veličinách $x_{i,\,i+s}$ nutno opět vzíti (mod $\mu$). Klademe-li nyní za $k$ postupně hodnoty $1, 2, 3, \ldots\ldots, \mu$. a pokládáme-li $s$ za pevné, získáme tak právě $\mu$ nezávislých kongruencí pro $\mu$ neznámých $x_{i,\,i+s}$:

$$\left.\begin{array}{l}
\varrho \,.\, x_{1,1+s} + \varrho^2 \,.\, x_{2,2+s} + \varrho^3 \,.\, x_{3,3+s} + \ldots + \varrho^{\mu} \,.\, x_{\mu,\mu+s} \equiv \lambda_{1,s} \\
\varrho^2 \,.\, x_{1,1+s} + \varrho^4 \,.\, x_{2,2+s} + \varrho^6 \,.\, x_{3,3+s} + \ldots + \varrho^{2\mu} \,.\, x_{\mu,\mu+s} \equiv \lambda_{2,s} \\
\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
\varrho^k \,.\, x_{1,1+s} + \varrho^{2k} \,.\, x_{2,2+s} + \varrho^{3k} \,.\, x_{3,3+s} + \ldots + \varrho^{k\mu} \,.\, x_{\mu,\mu+s} \equiv \lambda_{k,s} \\
\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
\varrho^{\mu} \,.\, x_{1,1+s} + \varrho^{2\mu} \,.\, x_{2,2+s} + \varrho^{3\mu} \,.\, x_{3,3+s} + \ldots + \varrho^{\mu^2} \,.\, x_{\mu,\mu+s} \equiv \lambda_{\mu,s}
\end{array}\right\} \pmod{p}, \tag{25′}$$

z nichž potom tyto neznámé $x_{i,\,i+s}$ možno lineárně vyjádřiti na základě nových neznámých $\lambda_{k,\,s}$.

Nezávislost kongruencí předešlé soustavy snadno stanovíme, určíme-li si determinant soustavy. Tento jest:

$$\Delta \equiv \begin{vmatrix} \varrho & \varrho^2 & \varrho^3 & \dots & \varrho^{\mu-1} & \varrho^{\mu} \\ \varrho^2 & \varrho^4 & \varrho^6 & \dots & \varrho^{2(\mu-1)} & \varrho^{2\mu} \\ \varrho^3 & \varrho^6 & \varrho^9 & \dots & \varrho^{3(\mu-1)} & \varrho^{3\mu} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \varrho^{\mu} & \varrho^{2\mu} & \varrho^{3\mu} & \dots & \varrho^{\mu(\mu-1)} & \varrho^{\mu^2} \end{vmatrix} \pmod{p}. \qquad (26)$$

Determinant jest zvláštním případem determinantu Vandermondeova; jeho vyčíslením získáme:

$$\Delta \equiv \varrho^{\frac{\mu(\mu^2-1)}{6}} (\varrho^{\mu-1} - 1)(\varrho^{\mu-2} - 1)^2 (\varrho^{\mu-3} - 1)^3 \dots$$
$$\dots (\varrho^2 - 1)^{\mu-2} (\varrho - 1)^{\mu-1} \pmod{p} \qquad (27)$$

Poněvadž však $\varrho$ jest číslo, které patří právě k exponentu $\mu$, žádný z faktorů determinantu $\Delta$ není kongruentní s nulou (mod $p$), z čehož pak plyne:

$$\Delta \not\equiv 0 \pmod{p} \qquad (27')$$

čímž jest dokázáno, že kongruence soustavy (25′) jsou skutečně nezávislé. Lze tedy veličiny $x_{i,i+s}$ skutečně vypočítati na základě veličin $\lambda_{k,s}$. Abychom vypočítali na př. veličinu $x_{i,i+s}$, násobme kongruence soustavy (25′) postupně hodnotami:

$$\varrho^{\mu-i}, \varrho^{2(\mu-i)}, \varrho^{3(\mu-i)}, \dots, \varrho^{\mu(\mu-i)}$$

a sečteme. Tím dostaneme:

$$\varrho^{\mu-i} \cdot \lambda_{1,s} + \varrho^{2(\mu-i)} \cdot \lambda_{2,s} + \varrho^{3(\mu-i)} \cdot \lambda_{3,s} + \dots + \varrho^{\mu(\mu-i)} \cdot \lambda_{\mu,s} \not\equiv$$
$$\not\equiv x_{1,1+s} \sum_{k=1}^{\mu} \varrho^{(\mu+i+1)k} + x_{2,2+s} \sum_{k=1}^{\mu} \varrho^{(\mu-i+2)k} + \dots, \qquad (28)$$
$$\dots + x_{i,i+s} \sum_{k=1}^{\mu} \varrho^{\mu k} + \dots + x_{\mu,\mu+s} \sum_{k=1}^{\mu} \varrho^{2\mu-i} \pmod{p},$$

což pak lze jednoduše upraviti. — Koeficienty při neznámých $x_{i,i+s}$ mají tvar:

$$\sum_{k=1}^{\mu} \varrho^{rk} \equiv \varrho^r + \varrho^{2r} + \varrho^{3r} + \dots + \varrho^{\mu r} \pmod{p}. \qquad (29)$$

*a*) Je-li nyní: $r \not\equiv 0 \pmod{\mu}$, potom jest:

$$\sum_{k=1}^{\mu} \varrho^{rk} \equiv \frac{1 - \varrho^{\mu r}}{1 - \varrho^r} \varrho^r \pmod{p}$$

Poněvadž ale $\varrho$ jest číslo, které patří právě k exponentu $\mu$, jest v případě $r \not\equiv 0 \pmod{\mu}$: $\varrho^r - 1 \not\equiv 0 \pmod{p}$ a : $\varrho^{\mu r} - 1 \equiv 0$

(mod $p$), z čehož pak plyne:

$$\sum_{k=1}^{\mu} \varrho^{rk} \equiv 0 \pmod{p}.$$

*b*) Je-li však: $r \equiv 0 \pmod{\mu}$, potom z kongruence (29) plyne:

$$\sum_{k=1}^{\mu} \varrho^{rk} \equiv \mu \pmod{p}$$

Vzhledem k tomuto se potom kongruence (28) zjednoduší a nabude tvaru:

$$\mu x_{i,i+s} \equiv \varrho^{\mu-i} \cdot \lambda_{1,s} + \varrho^{2(\mu-i)} \cdot \lambda_{2,s} + \ldots + \varrho^{\mu(\mu-i)} \cdot \lambda_{\mu,s} \pmod{p} \quad (30)$$

Nyní však $x_{i,i+s}$ udává počet dvojskupin čísel $a$, $a + 1$ obsažených v řadě:

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

jejichž $n$-té potenční charaktery (mod $p$) jsou $\varrho^i$ resp. $\varrho^{i+s}$. Musí tedy tyto hodnoty $x_{i,i+s}$ splňovati ještě nerovnici:

$$0 \leqq x_{i,i+s} \leqq p-1 \quad (30')$$

Známe-li pak veličiny $\lambda_{k,s}$, potom *hodnoty* $x_{i,i+s}$ *jsou kongruencí* (30) *a nerovnicí* (30') *jednoznačně určeny.* —

Hodnoty $\lambda_{k,s}$ lze však lehce vypočítati, neboť, jak jest patrno z kongruence (24), hodnota $\lambda_{k,s}$ jest rovna součtu $k \cdot \frac{p-1}{\mu}$-tých mocnin kořenů kongruence (21), a lze tedy tyto hodnoty $\lambda_{k,s}$ lehce vypočítati užitím Newtonova pravidla pro součty stejných mocnin kořenů. Tím jsme určili skutečně veličiny $x_{i,i+s}$.

8. Specielní vztahy mezi veličinami $x_{i,k}$.

Budiž $a$ číslo, které splňuje vztahy:

$$a^{\frac{p-1}{\mu}} \equiv \varrho^i, \; (a+1)^{\frac{p-1}{\mu}} \equiv \varrho^k \pmod{p} \quad (31)$$

Samozřejmě jest $a \not\equiv 0, -1 \pmod{p}$. Počet všech vzájemně nekongruentních čísel $a$, které splňují vztahy (31), jest pak udán veličinou $x_{i,k}$.

Ke každému takovému číslu $a$ lze potom přiřaditi jednoznačně dalších pět čísel, totiž:

$$\frac{1}{a}, \; -a-1, \; -\frac{1}{a}-1, \; -\frac{a}{a+1}, \; \frac{a}{a+1}-1. \quad (32)$$

*A*) Budiž nyní *číslo* $(p-1)$ *n-tým potenčním zbytkem* (mod $p$). Potom platí:

$$(-1)^{\frac{p-1}{\mu}} \equiv +1 \equiv \varrho^{\mu} \pmod{p}. \quad (33)$$

Poznámka: Je-li $p$ lichým prvočíslem $> 1$, potom číslo $(p - 1)$ jest vždy $n$-tým potenčním zbytkem (mod $p$), je-li buď:

$\alpha$) největší spol. míra $\mu$ čísel $n$, $p - 1$ číslem lichým:

$$\mu \equiv 1 \pmod 2;$$

(v tomto případě může býti $p$ jakékoliv liché prvočíslo);

$\beta$) nebo je-li nejv. spol. míra $\mu$ číslem sudým, tak, že jest:

$$\mu \equiv 0 \pmod{2^r}, \quad \mu \not\equiv 0 \pmod{2^{r+1}},$$

kdež:

$$r \geqq 1,$$

potom prvočíslo $p$ musí splňovati podmínku:

$$p \equiv 1 \pmod{2^{r+1}},$$

t. j. $p$ musí býti prvočíslem tvaru: $(2^{r+1}v + 1)$, kdež $v$ jest nějaké celé číslo. —

Pro $n$-té potenční charaktery čísel (32) potom vzhledem k kongruencím: (4), (31) a (33) obdržíme:

$$\left.\begin{array}{ll} \left(\frac{1}{a}\right)^{\frac{p-1}{\mu}} \equiv \varrho^{\mu-i}, & \left(\frac{1}{a}+1\right)^{\frac{p-1}{\mu}} \equiv \varrho^{k-i}, \\ (-a-1)^{\frac{p-1}{\mu}} \equiv \varrho^{k}, & [(-a-1)+1]^{\frac{p-1}{\mu}} \equiv \varrho^{i}, \\ \left(-\frac{1}{a}-1\right)^{\frac{p-1}{\mu}} \equiv \varrho^{k-i}, & \left[\left(-\frac{1}{a}-1\right)+1\right]^{\frac{p-1}{\mu}} \equiv \varrho^{\mu-i}, \\ \left(-\frac{a}{a+1}\right)^{\frac{p-1}{\mu}} \equiv \varrho^{i-k}, & \left(-\frac{a}{a+1}+1\right)^{\frac{p-1}{\mu}} \equiv \varrho^{\mu-k}, \\ \left(\frac{a}{a+1}-1\right)^{\frac{p-1}{\mu}} \equiv \varrho^{\mu-k}, & \left[\left(\frac{a}{a+1}-1\right)+1\right]^{\frac{p-1}{\mu}} \equiv \varrho^{i-k}, \end{array}\right\} \pmod p$$

Počty vzájemně nekongruentních čísel (mod $p$), které vyhovují předešlým kongruencím, jsou:

$$x_{\mu-i,k-i};\ x_{k,i};\ x_{k-i,\mu-i};\ x_{i-k,\mu-k};\ x_{\mu-k,i-k}.$$

Z jednoznačnosti přiřazení čísel (32) k číslu $a$, které splňuje kongruence (31), pak plyne důležitý vztah:

$$x_{i,k} = x_{k,i} = x_{\mu-i,k-i} = x_{k-i,\mu-i} = x_{\mu-k,i-k} = x_{i-k,\mu-k}. \quad (34)$$

Indexy v předešlém vztahu nutno bráti (mod $\mu$).

Vztah (34) poskytuje obecně 5 rovnic pro veličiny $x_{i,k}$, ovšem jen tenkráte, jestliže všechny indexy veličin v něm se vyskytujících jsou různé (mod $\mu$); jestliže však aspoň některé indexy při veličinách $x_{i,k}$ ve vztahu (34) jsou stejné (mod $\mu$), potom tento vztah poskytuje méně než 5 rovnic (po př. žádnou) pro veličiny $x_{i,k}$.

*a*) Je-li nyní:

$$(\mu, 3) = 1, \tag{35}$$

potom nastávají 4 případy, v nichž indexy veličin (34) jsou, aspoň částečně, stejné (mod $\mu$); jak snadno lze nahlédnouti, tyto případy jsou:

$\alpha)$ $i \equiv k \equiv 0 \pmod{\mu}$,
$\beta)$ $i \equiv 0,\ k \not\equiv 0 \pmod{\mu}$,
$\gamma)$ $i \not\equiv 0,\ k \equiv 0 \pmod{\mu}$,
$\delta)$ $i \equiv k \not\equiv 0 \pmod{\mu}$.

V případě $\alpha$) jsou indexy všech 6 veličin ve vztahu (34) stejné (mod $\mu$). Vztah tento vede k identitě: $x_{\mu,\mu} = x_{\mu,\mu}$, t. j. neposkytuje žádnou rovnici pro veličiny $x_{i,k}$.

Případy $\beta$), $\gamma$), $\delta$) vedou pak k témuž výsledku:

$$x_{\mu-i,\mu} = x_{\mu,\mu-i} = x_{i,i} \tag{34'}$$

Klademe-li nyní za $i$ postupně hodnoty $1, 2, \ldots, \mu - 1$, snadno poznáme, že získáme $2(\mu - 1)$ nezávislých rovnic mezi $3(\mu - 1)$ neznámými $x_{i,k}$. V každém jiném případě pak oněch 6 veličin $x_{i,k}$ ve vztahu (34) má rozličné indexy (mod $\mu$).

Případy $\alpha$)—$\delta$) vyčerpávají celkem $1 + 3(\mu - 1) = 3\mu - 2$ neznámých $x_{i,k}$ a poskytují dohromady $2(\mu - 1)$ nezávislých rovnic. — Ze zbývajících $\mu^2 - (3\mu - 2) = (\mu - 1)(\mu - 2)$ neznámých $x_{i,k}$ vede jich vždy 6 k jednomu vztahu tvaru (34), který pak platí za 5 nezávislých rovnic. Z toho pak plyne, že *vztah* (34) *za podmínky* (35) *poskytuje právě*

$$2(\mu - 1) + \frac{5(\mu - 1)(\mu - 2)}{6} = \frac{(\mu - 1)(5\mu + 2)}{6}$$

*nezávislých rovnic k určení* $\mu^2$ *neznámých* $x_{i,k}$.

K úplnému určení těchto $\mu^2$ neznámých $x_{i,k}$ nedostává se v tomto případě ještě $\frac{1}{6}(\mu + 1)(\mu + 2)$ nezávislých rovnic.

*b*) Je-li však:

$$(\mu, 3) = 3 \tag{36}$$

potom, jak snadno lze nahlédnouti, nastává 6 případů, v nichž indexy veličin $x_{i,k}$ ve vztahu (34) jsou, aspoň částečně, stejné (mod $\mu$). Tyto případy jsou:

$\alpha)$ $i \equiv k \equiv 0 \pmod{\mu}$,
$\beta)$ $i \equiv \frac{1}{3}\mu,\ k \equiv \frac{2}{3}\mu \pmod{\mu}$,
$\gamma)$ $i \equiv \frac{2}{3}\mu,\ k \equiv \frac{1}{3}\mu \pmod{\mu}$,
$\delta)$ $i \equiv 0,\ k \not\equiv 0 \pmod{\mu}$,
$\varepsilon)$ $i \not\equiv 0,\ k \equiv 0 \pmod{\mu}$,
$\eta)$ $i \equiv k \not\equiv 0 \pmod{\mu}$.

Případ $\alpha$) vede k identitě $x_{\mu,\mu} = x_{\mu,\mu}$, t. j. neposkytuje žádnou rovnici pro veličiny $x_{i,k}$.

Případy $\beta$), $\gamma$) vedou pak k témuž výsledku, totiž:

$$x_{\frac{\mu}{3},\frac{2\mu}{3}} = x_{\frac{2\mu}{3},\frac{\mu}{3}}, \tag{34''}$$

t. j. poskytují jednu rovnici mezi dvěma neznámými. —

Podobně případy $\delta$)—$\eta$) vedou k týmž výsledkům (viz (34)) a poskytují tedy $2(\mu - 1)$ nezávislých rovnic mezi $3(\mu - 1)$ neznámými.

V každém jiném případě potom oněch 6 veličin $x_{i,k}$ ve vztahu (34) má rozličné indexy (mod $\mu$). — Případy $\alpha$)—$\eta$) vyčerpávají celkem $1 + 2 + 3(\mu - 1) = 3\mu$ neznámých $x_{i,k}$ a poskytují pro ně dohromady $1 + 2(\mu - 1) = 2\mu - 1$ nezávislých rovnic. — Ze zbývajících $\mu^2 - 3\mu = \mu(\mu - 3)$ neznámých $x_{i,k}$ vede jich vždy 6 k jednomu vztahu tvaru (34), který pak poskytne 5 nezávislých rovnic. Z toho pak plyne, že *vztah* (34) *za podmínky* (36) *poskytuje právě*:

$$1 + 2(\mu - 1) + \frac{5\mu(\mu - 3)}{6} = \frac{\mu(5\mu - 3)}{6} - 1$$

*nezávislých rovnic k určení* $\mu^2$ *neznámých* $x_{i,k}$.

K úplnému určení těchto $\mu^2$ neznámých $x_{i,k}$ nedostává se tedy v tomto případě ještě $\frac{1}{6}\mu(\mu + 3) + 1$ nezávislých rovnic.

*B*) Budiž nyní číslo $(p - 1)$ $n$-tým potenčním nezbytkem (mod $p$). Potom nutně platí:

$$(-1)^{\frac{p-1}{\mu}} \equiv -1 \pmod{p}. \tag{37}$$

Poznámka: Číslo $(-1)^{\frac{p-1}{\mu}}$ může se rovnati buď $+1$ nebo $-1$. První z těchto případů jest však vyloučen, neboť pak číslo $(-1)^{\frac{p-1}{\mu}}$ bylo by $n$-tým potenčním zbytkem (mod $p$), což by bylo proti předpokladu. Platí tedy (37). Poněvadž však dále $(-1)^{\frac{p-1}{\mu}}$ znamená $n$-tý potenční charakter čísla $(-1)$ (mod $p$), bude zcela obecně platiti:

$$(-1)^{\frac{p-1}{\mu}} \equiv \varrho^k \pmod{p},$$

kdež $k$ bude nějaké celé číslo. Poněvadž však $\varrho^k$ jest kořenem kongruence:

$$\varrho^\mu \equiv 1 \pmod{p} \tag{$\alpha$}$$

(viz odst. 1), musí býti:

$$(\varrho^k)^\mu = (-1)^\mu \equiv +1 \pmod{p},$$

z čehož pak plyne, že *číslo $\mu$ jest v tomto případě vždy číslem sudým.* Budiž tedy:

$$\mu \equiv 0 \pmod{2^r},\ \mu \not\equiv 0 \pmod{2^{r+1}},\ r \geqq 1$$

Číslo $\frac{p-1}{\mu}$ musí však býti číslem lichým, poněvadž jinak kongruence (37) nemohla by obstáti. Musí tedy prvočíslo $p$ vyhovovati podmínkám:

$$p - 1 \equiv 0 \pmod{2^r},\ p - 1 \not\equiv 0 \pmod{2^{r+1}}$$

Lze pak lehce dokázati, že vztah (37) dá se psáti též ve tvaru:

$$(-1)^{\frac{p-1}{\mu}} \equiv -1 \equiv \varrho^{\frac{\mu}{2}} \pmod{p} \qquad (37')$$

Kongruenci $(a)$ lze psáti pak ve tvaru:

$$(\varrho^{\frac{\mu}{2}} - 1)(\varrho^{\frac{\mu}{2}} + 1) \equiv 0 \pmod{p}$$

Poněvadž pak $\varrho$ patří právě k exponentu $\mu$, nemůže faktor $(\varrho^{\frac{\mu}{2}} - 1)$ býti kongruentní s nulou (mod $p$) a jest tedy nutně $\varrho^{\frac{\mu}{2}} \equiv -1 \pmod{p}$, čímž vztah (37') jest dokázán.

Budiž nyní $a$ číslo, které splňuje vztahy (31). Potom čísla (32), která jsou číslu $a$ jednoznačně přiřazena, splňují vztahy:

$$\left.\begin{array}{ll}
\left(\frac{1}{a}\right)^{\frac{p-1}{\mu}} \equiv \varrho^{\mu-i}, & \left(\frac{1}{a}+1\right)^{\frac{p-1}{\mu}} \equiv \varrho^{k-i}, \\
(-a-1)^{\frac{p-1}{\mu}} \equiv \varrho^{\frac{\mu}{2}+k}, & [(-a-1)+1]^{\frac{p-1}{\mu}} \equiv \varrho^{\frac{\mu}{2}+i}, \\
(-\frac{1}{a}-1)^{\frac{p-1}{\mu}} \equiv \varrho^{\frac{\mu}{2}+k-i}, & [(-\frac{1}{a}-1)+1]^{\frac{p-1}{\mu}} \equiv \varrho^{\frac{\mu}{2}-i}, \\
\left(-\frac{a}{a+1}\right)^{\frac{p-1}{\mu}} \equiv \varrho^{\frac{\mu}{2}+i-k}, & \left[-\frac{a}{a+1}+1\right]^{\frac{p-1}{\mu}} \equiv \varrho^{\mu-k}, \\
\left(\frac{a}{a+1}-1\right)^{\frac{p-1}{\mu}} \equiv \varrho^{\frac{\mu}{2}-k}, & \left[\left(\frac{a}{a+1}-1\right)+1\right]^{\frac{p-1}{\mu}} \equiv \varrho^{i-k},
\end{array}\right\} \pmod{p}$$

Počty vzájemně nekongruentních čísel (mod $p$), které vyhovují předešlým kongruencím, jsou:

$$x_{\mu-i,\,k-i};\ x_{\frac{\mu}{2}+k,\,\frac{\mu}{2}+i};\ x_{\frac{\mu}{2}+k-i,\,\frac{\mu}{2}-i};\ x_{\frac{\mu}{2}+i-k,\,\mu-k};\ x_{\frac{\mu}{2}-k,\,i-k}$$

Z jednoznačnosti přiřazení čísel (32) k číslu $a$, které splňuje

vztahy (31), pak plyne důležitý vztah:

$$x_{i,k} = x_{\mu-i,\,k-i} = x_{\frac{\mu}{2}+k,\,\frac{\mu}{2}+i} = x_{\frac{\mu}{2}+k-i,\;\frac{\mu}{2}-i} = x_{\frac{\mu}{2}+i-k,\;\mu-k} = x_{\frac{\mu}{2}-k,\,i-k} \tag{38}$$

Indexy v předešlém vztahu nutno opět bráti (mod $\mu$).

Vztah (38) poskytuje obecně 5 nezávislých rovnic mezi 6 veličinami $x_{i,k}$, ovšem jen tenkráte, jestliže indexy všech veličin v tomto vztahu jsou různé (mod $\mu$); jinak tento vztah poskytne méně než 5 rovnic, po př. ani jednu.

*α*) Je-li nyní:

$$(\mu, 3) = 1, \tag{39}$$

potom, jak snadno lze se přesvědčiti, nastávají 4 případy, v nichž veličin indexy $x_{i,k}$ ve vztahu (38) jsou aspoň částečně stejné (mod $\mu$). Tyto případy jsou:

$$\begin{aligned}
&\alpha)\ i \equiv 0,\ k \equiv \tfrac{1}{2}\mu \pmod{\mu}\\
&\beta)\ i \equiv 0,\ k \not\equiv \tfrac{1}{2}\mu \pmod{\mu}\\
&\gamma)\ i \not\equiv 0,\ k \equiv \tfrac{1}{2}\mu \pmod{\mu}\\
&\delta)\ i - k \equiv \tfrac{1}{2}\mu,\ i \not\equiv 0,\ k \not\equiv \tfrac{1}{2}\mu \pmod{\mu}
\end{aligned}$$

V případě *α*) jsou indexy všech 6 veličin ve vztahu (38) stejné (mod $\mu$). Vztah tento vede k indentitě $x_{\mu,\,\frac{\mu}{2}} = x_{\mu,\,\frac{\mu}{2}}$ a tedy nepodskytuje žádnou rovnici pro veličiny $x_{i,k}$.

Vztahy *β*), *γ*), *δ*) vedou pak k podstatně týmž výsledkům, totiž:

$$x_{\mu,\,k} = x_{\frac{\mu}{2}+k,\,\frac{\mu}{2}} = x_{\frac{\mu}{2}-k,\,\mu-k}. \tag{38'}$$

Klademe-li za $k$ postupně hodnoty 1, 2, 3, ....., $\mu$ (vyjímaje hodnotu $\frac{1}{2}\mu$), snadno poznáme, že získáme $2(\mu - 1)$ nezávislých rovnic mezi $3(\mu - 1)$ neznámými $x_{i,k}$.

V každém jiném případě pak oněch 6 veličin ve vztahu (38) má rozličné indexy (mod $\mu$). —

Případy *α*)—*δ*) vyčerpávají celkem $1 + 3(\mu - 1) = 3\mu - 2$ neznámých $x_{i,k}$ a poskytují dohromady $2(\mu - 1)$ nezávislých rovnic Ze zbývajících $\mu^2 - 3\mu + 2 = (\mu - 1)(\mu - 2)$ neznámých $x_{i,k}$ vede jich vždy 6 k jednomu vztahu tvaru (38), který pak platí za 5 nezávislých rovnic. Z toho pak plyne, že *vztah* (38) *za podmínky* (39) *poskytuje právě*:

$$2(\mu - 1) + \frac{5(\mu - 1)(\mu - 2)}{6} = \frac{(\mu - 1)(5\mu + 2)}{6}$$

*nezávislých rovnic k určení $\mu^2$ neznámých $x$---.*

K úplnému určení těchto $\mu^2$ neznámých nedostává se tudíž v tomto případě ještě $\frac{1}{6}(\mu+1)(\mu+2)$ nezávislých rovnic. —

*b*) Je-li však:

$$(\mu, 3) = 3 \tag{40}$$

potom nastává 6 případů, v nichž indexy veličin $x_{i,k}$ ve vztahu (38) jsou aspoň částečně stejné (mod $\mu$). Případy tyto jsou:

$$\begin{aligned}
&\alpha)\ i \equiv 0,\ k \equiv \tfrac{1}{2}\mu \pmod{\mu},\\
&\beta)\ i \equiv 0,\ k \not\equiv \tfrac{1}{2}\mu \pmod{\mu},\\
&\gamma)\ i \not\equiv 0,\ k \equiv \tfrac{1}{2}\mu \pmod{\mu},\\
&\delta)\ i \equiv k + \tfrac{1}{2}\mu \not\equiv 0 \pmod{\mu},\\
&\varepsilon)\ i \equiv \tfrac{1}{3}\mu,\ k \equiv \tfrac{1}{6}\mu \pmod{\mu},\\
&\eta)\ i \equiv \tfrac{2}{3}\mu,\ k \equiv \tfrac{5}{6}\mu \pmod{\mu}.
\end{aligned}$$

Případ $\alpha$) vede k identitě $x_{\mu, \frac{\mu}{2}} = x_{\mu, \frac{\mu}{2}}$ a neposkytuje tedy žádnou rovnici pro neznámé veličiny $x_{i,k}$.

Případy $\beta$), $\gamma$), $\delta$) vedou pak k týmž výsledkům jako (38′) a poskytují tedy $2(\mu-1)$ nezávislých rovnic pro $3(\mu-1)$ neznámých veličin $x_{i,k}$.

Případy $\varepsilon$), $\eta$) vedou k rovnici:

$$x_{\frac{2\mu}{3}, \frac{5\mu}{6}} = x_{\frac{\mu}{3}, \frac{\mu}{6}} \tag{38″}$$

a poskytují tedy jednu rovnici mezi 2 neznámými.

V každém jiném případě potom oněch 6 veličin $x_{i,k}$ ve vztahu (38) má rozličné indexy (mod $\mu$). Případy $\alpha$)—$\eta$) vyčerpávají celkem $1 + 3(\mu-1) + 2 = 3\mu$ neznámých $x_{i,k}$ a poskytují pro ně dohromady $(2\mu-1)$ nezávislých rovnic. Ze zbývajících $\mu^2 - 3\mu = \mu(\mu-3)$ neznámých $x_{i,k}$ vede jich vždy 6 k jednomu vztahu tvaru (38), který platí za 5 rovnic. Z toho pak plyne, že *vztah* (38) *za podmínky* (40) *poskytuje právě*

$$2\mu - 1 + \frac{5\mu(\mu-3)}{6} = \frac{5\mu^2 - 3\mu - 6}{6}$$

*nezávislých rovnic k určení $\mu^2$ neznámých $x_{i,k}$.*

K úplnému určení těchto $\mu^2$ neznámých $x_{i,k}$ nedostává se tedy v tomto případě ještě $\frac{1}{6}\mu(\mu+3)+1$ nezávislých rovnic.

Tím jsme prozkoumali specielní vztahy mezi veličinami $x_{i,k}$.

Poznámka: Pro hodnoty $x_{i,k}$ lze udati ještě jiné vztahy, z nichž potom tyto hodnoty lze počítati. A tu se ukáže, že problém rozdělení $n$-tých potenčních zbytků pro prvočíselný modul jest ve velmi úzké souvislosti s Fermatovou domněnkou o neřešitelnosti rovnice: $x^n + y^n = z^n$, $n > 2$ celými a od nuly odlišnými čísly $x, y, z$. Tuto souvislost našeho problému s domněnkou Fermatovou ukáži ve své příští práci. —

## La partition des résidus de puissances $n$-ièmes pour un module premier.

(Extrait de l'article précédent.)

Soit $n$ un entier positif, $q$ un nombre premier impair $> 1$, $\mu = (n, p-1)$ le plus grand commun diviseur des nombres $(p-1)$, $n$, $\varrho$ un nombre appartenant à l'exposant $\mu$. Ceci posé, on peut trouver, pour tout nombre $a \not\equiv 0 \pmod{p}$, un exposant $i$ tel que la congruence (5) soit satisfaite. J'appelle *$n$-ième caractère de puissance du nombre $a$* le nombre $\varrho^i$. Si un nombre $a$ satisfait à la relation (6), je dis que son $n$-ième caractère de puissance est de l'ordre $k$ (mod $p$).

Le symbole $x_{i,k}$ désigne le nombre des nombres noncongrus (mod $p$), satisfaisant en même temps à la congruence (31). Ces quantités $x_{i,k}$ sont déterminées univoquement par les congruences (30) et l'inégalité (30'), $\lambda_{k,s}$ désignant la somme des puissances $k(p-1)/\mu$-ièmes des racines de la congruence (21). Il faut prendre les indices des quantités $x_{i,k}$ *mod* $\mu$.

Si le nombre $(-1)$ est un résidu de puissance $n$-ième (mod $p$), les relations (34) ont lieu pour les nombres $x_{i,k}$; s'il n'en est pas ainsi, la relation (38) a lieu. Ces relations donnent $\frac{1}{6}(\mu-1)(5\mu+2)$ ou $\frac{1}{6}\mu(5\mu-3)-1$ équations indépendantes pour les nombres $x_{i,k}$ suivant que 3 n'est pas ou bien est facteur de $\mu$.