Časopis pro pěstování matematiky a fysiky

Karel Koutský

Poznámka ke kvadratickému charakteru čísel

Časopis pro pěstování matematiky a fysiky, Vol. 58 (1929), No. 1-2, 42--52

Persistent URL: http://dml.cz/dmlcz/108920

Poznámka ke kvadratickému charakteru čísel.

Napsal dr. *Karel Koutský.*

Budiž a reálné a celistvé číslo, které splňuje relaci:

$$\left(\frac{a}{p}\right) = \left(\frac{a+1}{p}\right) = \left(\frac{a+2}{p}\right) = \ldots = \left(\frac{a+k-1}{p}\right) \neq \left(\frac{a+k}{p}\right), \quad (1)$$

kdež p značí liché prvočíslo > 1, k je nějaké celé a kladné číslo, $\left(\frac{a}{p}\right)$ je symbol *Legendreův:* pokud je $a \not\equiv 0 \pmod{p}$, jest $\left(\frac{a}{p}\right) = \pm 1$; je-li $a \equiv 0 \pmod{p}$, položme $\left(\frac{a}{p}\right) = 0$.

O číslu a, které splňuje předešlou relaci říkáme, že *toto číslo a vzhledem k modulu p je stupně k.*

Je-li $a \equiv 0, -1 \pmod{p}$, potom vždy podle naší definice platí $\left(\frac{a}{p}\right) \neq \left(\frac{a+1}{p}\right)$, což znamená, že 0 i (-1) jest právě prvního a ne vyššího stupně (mod p); obráceně však tato věta neplatí, neboť je-li nějaké číslo a právě prvního a ne vyššího stupně (mod p), neznamená to ještě, že by muselo býti: $a \equiv 0, -1 \pmod{p}$. Je-li však číslo a vyššího než prvního stupně (mod p), potom jest nutně $a \not\equiv 0, -1 \pmod{p}$.

Dále jest zřejmé, že každá dvě kongruentní čísla (mod p) jsou téhož stupně (mod p).

Všechna celá čísla jsou kongruentní (mod p) s nějakým číslem řady:

$$0, 1, 2, 3, \ldots, p-2, p-1. \quad (2)$$

Počet čísel z této řady, která jsou aspoň k-tého stupně (mod p), označme $P_k(p)$.

Naším úkolem je stanovení nutných a dostačujících podmínek k tomu, aby číslo a bylo aspoň k-tého stupně (mod p), jakož i určení počtu těchto čísel,[1]) t. j. stanovení hodnot $P_k(p)$.

---

[1]) Stanovení nutných podmínek, aby číslo a bylo aspoň 2. stupně (mod p), jakož i určení hodnot $P_2(p)$, $P_3(p)$, viz též: Grosschmid Lajos: *A négyzet-maradékok eloszlásáról.* — Mathematikai és természettudományi értesitö, sv. 34, str. 236—252. (A Magyar Tud. Akadémia III. osztályának folyóirata, Budapest 1916.)

Je-li $k \geqq 1$, jest celá otázka triviální, neboť všechna čísla řady (2) jsou aspoň 1. stupně (mod p). Definujeme tedy:

$$P_1(p) = p. \tag{3}$$

Mezi těchto p čísel patří jedno číslo $a \equiv 0 \pmod{p}$ a dalších $(p-1)$ různých, vzájemně nekongruentních čísel $a \not\equiv 0 \pmod{p}$.

I.

Stanovení nutných a dostačujících podmínek pro číslo a, které má býti k-tého stupně (mod p).

1. Jestliže nějaké číslo a má býti aspoň 2. stupně (mod p), musí platiti:

$$\left(\frac{a}{p}\right) = \left(\frac{a+1}{p}\right).$$

Podle předešlého jest však zřejmo, že žádné z čísel a, $(a+1)$ nesmí býti kongruentní s nulou (mod p) a tedy, že musí platiti: $a \not\equiv 0, -1 \pmod{p}$; dále pak, že obě tato čísla musí býti současně buď kvadratickými zbytky nebo kv. nezbytky (mod p) a tudíž jejich součin $a(a+1)$ musí býti kvadratickým zbytkem (mod p).[2])

Kongruence:

$$x^2 \equiv 4a(a+1) \pmod{p}$$

jest tedy řešitelná.

Položme nyní:

$$x \equiv t - 2a - 1 \pmod{p},$$

kdež t značí nějaké celé číslo. Dosazením obdržíme po úpravě:

$$4a \equiv t + \frac{1}{t} - 2 \pmod{p}, \tag{4}$$

kdež $\frac{1}{t} \equiv t^{p-2} \pmod{p}$ značí číslo sociované k číslu t, vyhovující kongruenci: $t \cdot \frac{1}{t} \equiv 1 \pmod{p}$.

Snadno lze nahlédnouti, že v kongruenci (4) číslo t nemůže býti kongruentní s nulou (mod p); ale ani hodnoty $t \equiv \pm 1 \pmod{p}$ nejsou přípustné, neboť v prvém případě $(t \equiv +1 \pm 1)$ bylo by $a \equiv 0 \pmod{p}$, v druhém případě $(t \equiv -1)$ by pak bylo $a \equiv -1 \pmod{p}$, kteréžto hodnoty jsme hned na začátku této práce vyloučili z řady čísel, jež jsou aspoň 2. stupně (mod p); číslo t musí tedy splňovati ještě podmínku:

$$t(t^2 - 1) \not\equiv 0 \pmod{p}. \tag{4'}$$

Řešitelnost kongruence (4) podle t za platnosti podmínky (4'), jest tedy *nutnou* podmínkou proto, aby číslo a bylo aspoň 2. stupně

[2]) *Weber:* Lehrbuch d. Algebra I., (2. vyd.), str. 487, Braunschweig 1898.

(mod p). Diskriminant této kongruence jest $4a(a+1)$ a kongruence sama bude řešitelná vždy, jakmile tento diskriminant bude kvadratickým zbytkem (mod p), což nastane vždy, jakmile číslo a bude aspoň 2. stupně (mod p).

Podmínky tyto jsou však též dostačující, neboť existuje-li nějaké číslo t splňující podmínky (4) a (4'), potom jest:

$$a(a+1) \equiv \left(\frac{t^2-1}{4t}\right)^2 \equiv 0 \pmod{p},$$

odkudž plyne:

$$\left(\frac{a}{p}\right) \equiv \left(\frac{a+1}{p}\right),$$

c. b. d.

Poznámka 1. Z předešlého jest patrno, že kořeny kongruence:

$$x^2 \equiv a(a+1) \pmod{p},$$

kdež a jest číslo aspoň 2. stupně (mod p), dají se vyjádřiti tvarem:

$$x \equiv \frac{1}{4}\left(t - \frac{1}{t}\right) \pmod{p}.$$

Tím zároveň jest řešena úloha: *Nalézti takové bitrigonální zbytky* $a(a+1)$ *(mod* p*), které jsou současně kvadratickými zbytky (mod* p*).* Stačí za a položiti nějaké číslo, jež jest aspoň 2. stupně (mod p).

Poznámka 2. Z kongruence (4) však plyne dále:

$$4at \equiv (t-1)^2 \pmod{p},$$

odkudž je zřejmo, že musí býti:

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

Je-li nyní $\left(\frac{t}{p}\right) = +1$ a označíme-li jeden z kořenů kongruence:

$$x^2 \equiv t \pmod{p}$$

symbolicky $\sqrt{t}$ ($\sqrt{t}$ znamená tedy jisté celé číslo), potom z (4) plyne:

$$a \equiv \left(\frac{1}{2}\left(\sqrt{t} + \frac{1}{\sqrt{t}}\right)\right)^2 \pmod{p};$$

tím jest též řešena kongruence:

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

v níž a jest číslo aspoň 2. stupně (mod p).

2. Je-li nyní a aspoň k-tého stupně (mod p), potom platí relace (1). Z ní jest zřejmo, že všechny podvojné součiny čísel obsažených v řadě:

$$a,\ a+1,\ a+2,\ a+3,\ \ldots,\ a+k-1, \tag{5}$$

jsou vesměs kvadratickými zbytky (mod p).

Předpokládáme-li $k \geqq 2$, potom číslo a jest jistě aspoň 2. stupně (mod p) a musí tedy býti splněny podmínky (4) a (4'). Čísla řady (5) dají se potom vyjádřiti tvary:

$$\left.\begin{aligned} a &\equiv \frac{(t-1)^2}{4t}, \\ a+1 &\equiv \frac{(t+1)^2}{4t}, \\ a+2 &\equiv \frac{t^2+6t+1}{4t}, \\ a+3 &\equiv \frac{t^2+10t+1}{4t}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ a+(k-1) &\equiv \frac{t^2+2(2k-3).t+1}{4t}, \end{aligned}\right\} \pmod{p}.$$

Jestliže všechny podvojné součiny těchto čísel mají býti současně kvadratickými zbytky (mod p), musí býti splněny relace:

$$\left(\frac{t^2+2(2i-3)t+1}{p}\right) = +1 \qquad (6)$$

$$i = 1, 2, 3, \ldots, k.$$

Relace tyto spolu s podmínkami (4) a (4') představují nutné podmínky pro číslo a, jež má býti aspoň k-tého stupně (mod p).

Podmínky tyto jsou však též *dostačující*, neboť jestliže existuje nějaké číslo t, které splňuje podmínky (4') a (6), potom kongruence (4) poskytne jisté číslo a té vlastnosti, že všechny podvojné součiny z čísel řady (5) jsou kvadratickými zbytky (mod p), což značí, že číslo a musí býti aspoň k-tého stupně (mod p).

Hledáme-li však číslo a, které jest *právě* k-tého stupně (mod p), potom tyto podmínky nejsou dostačující, neboť kdyby t bylo číslo vyhovující relacím (4') a (6) tak, že pro toto číslo t bylo by též:

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

potom podle naší definice bylo by číslo a aspoň $(k+1)$-ho stupně (mod p). Tedy pro číslo a, které jest právě k-tého stupně (mod p) nesmí býti předešlá rovnice splněna, což znamená, že relace (6) nesmí býti splněna pro $i = k+1$.

II.

Kongruence, jimž vyhovují čísla aspoň 2. a 3. stupně (mod p).

1. Pro čísla aspoň 2. stupně (mod p) nalezli jsme jako nutnou a dostačující podmínku kongruenci (4), v níž však číslo t musí vyhovovati podmínce (4′). Jestli tedy zvolíme si za t jakékoliv číslo splňující podmínku (4′), potom kongruence (4) poskytne jisté číslo a, jež jest aspoň 2. stupně (mod p).

2. Podobně jako pro čísla aspoň 2. stupně (mod p), lze i pro čísla, jež jsou aspoň 3. stupně (mod p) získati určitou kongruenci.

Abychom získali číslo, jež jest aspoň 3. stupně (mod p), stačí do kongruence (4) dosaditi takové číslo t, které mimo podmínku (4′), splňuje ještě další podmínku, totiž:

$$\left(\frac{t^2+6t+1}{p}\right) = +1,$$

která je totožná s podmínkou (6) pro $i = 3$. Stačí tedy hledati číslo t, jež vyhovuje předešlé podmínce.

Je-li tato podmínka splněna, potom kongruence:

$$x^2 \equiv t^2 + 6t + 1 \pmod{p}$$

jest jistě řešitelná a to jak podle x tak i podle t.
Položme nyní:

$$x \equiv t - s + 3 \pmod{p},$$

kdež s značí nějaké celé číslo. Dosazením obdržíme po malé úpravě:

$$t \equiv \frac{s^2 - 6s + 8}{2s} \pmod{p}. \tag{7}$$

Jestliže nyní dosadíme za s do kongruence (7) nějaké celé číslo, získáme určité číslo t, jež dosazeno do kongruence (4) poskytne jisté číslo a, které je aspoň 3. stupně (mod p).

Důkaz: Provedeme-li skutečně toto dosazení, obdržíme po úpravě:

$$a \equiv \frac{(s^2-8s+8)^2}{8s(s^2-6s+8)} \pmod{p}, \tag{8}$$

z kteréž kongruence však plyne dále:

$$\left.\begin{aligned} a+1 &\equiv \frac{(s^2-4s+8)^2}{8s(s^2-6s+8)} \\ a+2 &\equiv \frac{(s^2-8)^2}{8s(s^2-6s+8)} \end{aligned}\right\} \pmod{p}, \tag{8′}$$

odkudž jest patrno, že jest:

$$\left(\frac{a}{p}\right) = \left(\frac{a+1}{p}\right) = \left(\frac{a+2}{p}\right) = \left(\frac{8s(s^2-6s+8)}{p}\right),$$

což značí, že číslo a jest skutečně aspoň 3. stupně (mod p). Tím jsme získali žádanou kongruenci pro čísla aspoň 3. stupně (mod p).

Snadno lze nyní nahlédnouti, že v kongruenci (8) nemůže býti s kongruentní s nulou (mod p). Mimo to však existují ještě další hodnoty s, které nevedou k číslům, jež jsou skutečně aspoň 3. stupně (mod p). Jak na začátku této práce bylo poznamenáno, čísla 0 a (-1) z řady (2) jsou právě 1. stupně (mod p). Lze však stejně snadno nahlédnouti, že číslo (-2) jest maximálně 2. stupně (mod p). Z toho pak plyne, že všechny hodnoty s, které vedou podle kongruence (8) k číslům a, 0, -1, -2, jsou vyloučeny. K těmto číslům však vedou dle kongruencí (8′) ty hodnoty s, jež vyhovují kongruencím:

$$s^2 - 8s + 8 \equiv 0, \quad s^2 - 4s + 8 \equiv 0, \quad s^2 - 8 \equiv 0 \pmod{p}.$$

Prvé dvě dvojice vedou k $t \equiv \pm 1$, poslední dvojice hodnot s vede pak k hodnotě t, jež je dána kongruencí:

$$t^2 + 6t + 1 \equiv 0 \pmod{p},$$

jež však odporuje podmínce (6) pro $k = 3$.

Konečně pak jsou vyloučeny ony hodnoty s, které vedou k $t \equiv 0$; tyto hodnoty s vyhovují pak kongruenci:

$$s^2 - 6s + 8 \equiv 0 \pmod{p}.$$

Musí tedy číslo s v kongruenci (8) vyhovovati ještě dalším podmínkám, abychom dostali skutečně číslo aspoň 3. stupně (mod p) a sice:

$$s(s^2 - 8)(s^2 - 4s + 8)(s^2 - 6s + 8)(s^2 - 8s + 8) \not\equiv 0 \pmod{p}. \quad (8'')$$

Poznámka: Kongruence pro čísla, jež jsou aspoň 4. stupně (mod p) se mi nepodařilo sestrojiti.

III.

Určení počtu vzájemně nekongruntních čísel (mod p), jež jsou aspoň k-tého stupně (mod p).

1. Je-li $k \geqq 2$, potom obdržíme čísla, jež jsou aspoň 2. stupně (mod p); čísla tato vyhovují kongruenci (4), v níž celistvé číslo t je vázáno podmínkou (4′). Každé určité hodnotě tohoto čísla t, obsažené v řadě:

$$2, 3, 4, \ldots, p - 3, p - 2, \quad (9)$$

odpovídá pak podle kongruence (4) jisté číslo a (mod p), které jest aspoň 2. stupně (mod p). Jest však nyní otázka, zda-li některá z takto získaných čísel a nejsou spolu kongruentní (mod p)?

Jestliže dvěma různým hodnotám t z předešlé řady, na př. $t_1 \not\equiv t_2$ (mod p), mají odpovídati dvě kongruentní čísla a (mod p),

potom podle kongruence (4) musí platiti:

$$t_1 + \frac{1}{t_1} - 2 \equiv t_2 + \frac{1}{t_2} - 2 \pmod{p},$$

čili:

$$(t_1 - t_2)(t_1 \,.\, t_2 - 1) \equiv 0 \pmod{p},$$

odkudž, vzhledem k učiněnému předpokladu, plyne:

$$t_1 \,.\, t_2 - 1 \equiv 0 \pmod{p}.$$

Ke každému číslu t patří tedy ještě jedno číslo (sociované) $\frac{1}{t} \equiv t^{p-2} \pmod{p}$, které poskytuje tutéž hodnotu a. Tedy všechna čísla v řadě (9) se rozpadají na dvojice tak, že každá dvojice vede k témuž číslu $a \pmod{p}$. Jsou-li nyní t_1, t_2 dvě sociovaná čísla, potom vztah $t_1 \equiv t_2 \pmod{p}$, může platiti jen tenkrát, je-li $t \equiv \pm 1 \pmod{p}$. Avšak čísla ± 1 se v řadě (9) nevyskytují, tudíž každá dvě sociovaná čísla z této řady jsou nekongruentní $(\mathrm{mod}\ p)$. Poněvadž pak v celé řadě (9) jest $(p - 3)$ čísel, obdržíme takto celkem $\frac{p-3}{2}$ dvojic, z nichž každá vede k jednomu číslu a, jež jest aspoň 2. stupně $(\mathrm{mod}\ p)$. Čísla z různých dvojic vedou potom k dvěma nekongruentním číslům $a \pmod{p}$.

Z toho plyne, že *existuje* $\frac{p-3}{2}$ *různých nekongruentních čísel* a, *jež jsou aspoň 2. stupně* $(\mathrm{mod}\ p)$, čili podle našeho označení platí:

$$P_2(p) = \frac{p-3}{2}. \tag{10}$$

Počet vzájemně nekongruentních čísel $(\mathrm{mod}\ p)$, která jsou právě prvního a ne vyššího stupně $(\mathrm{mod}\ p)$, potom jest:

$$P_1(p) - P_2(p) = \frac{p+3}{2}. \tag{10'}$$

2. Je-li nyní $k \geqq 3$, potom obdržíme čísla, jež jsou aspoň 3. stupně $(\mathrm{mod}\ p)$; čísla tato získáme z kongruence (4), jestliže za t zvolíme si číslo, vyhovující kongruenci (7), v níž celistvé číslo s jest vázáno podmínkou (8″). Číslo s může nabývati kterékoliv hodnoty z řad (2), vyjímaje ty hodnoty, pro něž levá strana podmínky (8″) rovnala by se nule. Jestli nyní označíme kořeny kongruence:

$$x^2 \equiv c \pmod{p},$$

pokud tato ovšem je možná, t. j. pokud c jest kvadratickým zbytkem $(\mathrm{mod}\ p)$, symbolicky $\pm\sqrt{c}$, potom hodnoty čísla s, pro něž levá strana podmínky (8″) se rovná nule, jsou:

$$0;\ +2\sqrt{2};\ -2\sqrt{2};\ 2 \pm 2\sqrt{-1};\ 2,\ 4;\ 4 \pm 2\sqrt{2}. \tag{11}$$

Tudíž některá čísla z řady (2) pro s odpadají a sice vždy odpadají čísla: 0, 2, 4, takže zbývá $(p-3)$ hodnot, z nichž však ještě odpadají další hodnoty, jestliže (-1) resp. 2 kvadratickým zbytkem (mod p).

Je-li nyní:

a) $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = +1$, potom odpadají ještě čísla: $\pm 2\sqrt{2}$, $2 \pm 2\sqrt{-1}$, $4 \pm 2\sqrt{2}$, tedy celkem 6 čísel;

b) je-li však: $\left(\frac{-1}{p}\right) = -\left(\frac{2}{p}\right) = +1$, potom odpadají toliko další dvě čísla a sice: $2 \pm 2\sqrt{-1}$, neboť $\sqrt{2}$ nemá významu;

c) je-li: $\left(\frac{-1}{p}\right) = -\left(\frac{2}{p}\right) = -1$, potom odpadají další 4 čísla, totiž: $\pm 2\sqrt{2}$, $4 \pm 2\sqrt{2}$, neboť $\sqrt{-1}$ nemá významu;

d) je-li konečně $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$, potom neodpadá již žádné další číslo, neboť ani $\sqrt{-1}$, ani $\sqrt{2}$ nemá významu.

Označíme-li nyní počet čísel s, pro něž levá strana podmínky (8″) rovná se nule, písmenem S, potom všechny tyto čtyři případy dají se vyjádřiti jedním vzorcem:

$$S = 6 + \left(\frac{-1}{p}\right) + 2\left(\frac{2}{p}\right). \qquad (11')$$

o jehož správnosti lze se přesvědčiti přímým dosazením.

Takto získáme právě $(p-S)$ čísel s, která poskytují podle kongruence (7) takové hodnoty t, pro něž číslo a, určené kongruencí (4) jest aspoň 3. stupně (mod p). Avšak některé z takto získaných hodnot t budou kongruentní (mod p) a povedou tady ke kongruentním číslům a.

Mají-li nyní dvě nekongruentní hodnoty s (mod p) na př. s_1, s_2, vésti k témuž číslu t (mod p), musí býti splněna kongruence:

$$\frac{s_1^2 - 6s_1 + 8}{2s_1} \equiv \frac{s_2^2 - 6s_2 + 8}{2s_2} \pmod{p},$$

kterouž možno upraviti na tvar:

$$(s_1 - s_2)(s_1 s_2 - 8) \equiv 0 \pmod{p}$$

a poněvadž jest: $s_1 \not\equiv s_2 \pmod{p}$, tedy na:

$$s_1 s_2 \equiv 8 \pmod{p}. \qquad (12)$$

Každá dvě čísla s, která vyhovují předešlé kongruenci, vedou k téže hodnotě t (mod p). Kdyby v předešlé kongruenci bylo ještě:

$s_1 \equiv s_2 \pmod{p}$, platilo by: $s^2 - 8 \equiv 0 \pmod{p}$, kteréž hodnoty s jsou však vyloučeny. Podobně i pro zbývající vyloučené hodnoty s jest předešlá podmínka splněna. Z toho plyne, že oněch $(p - S)$ hodnot s lze seřaditi do $\frac{p-S}{2}$ párů tak, že čísla jednoho páru vyhovují kongruenci (12) a vedou tedy k témuž $t \pmod{p}$. Jest tedy právě $\frac{p-S}{2}$ hodnot t, které vedou k číslům a, jež jsou aspoň 3. stupně (mod p). Seznali jsme však v předešlém odstavci, že dvě sociovaná čísla t_1, t_2, t. j. čísla, vyhovující kongruenci: $t_1 \cdot t_2 \equiv 1 \pmod{p}$, vedou k téže hodnotě a. Musí tedy získané hodnoty t dáti se seřaditi do párů vzájemně sociovaných čísel tak, že čísla jednoho páru povedou k témuž číslu a. (Mezi našimi čísly t nemohou se vyskytovati čísla vzájemně sociovaná a při tom kongruentní, neboť by muselo býti: $t \equiv \pm 1 \pmod{p}$, kteréž hodnoty jsou však vyloučeny.)

Z této úvahy plyne, že počet nekongruentních čísel, jež jsou aspoň 3. stupně (mod p), jest udán vzorcem:

$$P_3(p) = \frac{p-S}{4}. \tag{13}$$

Dosazením z rovnice (11) a malou úpravou získáme:

$$P_3(p) = \frac{p - 2 + \left(\frac{-1}{p}\right)}{4} - 1 - \frac{\left(\frac{-1}{p}\right) + \left(\frac{2}{p}\right)}{2},$$

kterýžto vzorec lze však ještě upraviti.

Je-li $\left(\frac{-1}{p}\right) = +1$, potom prvočíslo p jest tvaru $(4k + 1)$ a tedy výraz $\frac{1}{4}\left(p - 2 + \left(\frac{-1}{p}\right)\right)$ má hodnotu k, čili $\left[\frac{p}{4}\right]$, kdež $\left[\frac{p}{4}\right]$ jest Gaussova funkce čísla $\frac{p}{4}$ (největší celé číslo, které jest obsažené ve zlomku $\frac{p}{4}$).

Je-li $\left(\frac{-1}{p}\right) = -1$, potom p jest prvočíslo tvaru $(4k + 3)$ a zmíněný výraz nabývá opět hodnoty k čili $\left[\frac{p}{4}\right]$.

Lze tedy předešlému vzorci dáti definitivní tvar:

$$P_3(p) = \left[\frac{p}{4}\right] - 1 - \tfrac{1}{2}\left(\left(\frac{-1}{p}\right) + \left(\frac{2}{p}\right)\right). \tag{14}$$

K tomuto vzorci přišel též Grosschmid ve své, již citované

práci, ale jeho odvození jest nepřímé a příliš dlouhé, kdežto zde jest podáno odvození přímé a o mnoho kratší.

Počet čísel, jež jsou právě druhého a ne vyššího nebo nižšího stupně (mod p) jest potom:

$$P_2(p) - P_3(p) = \frac{p-1}{2} - \left[\frac{p}{4}\right] + \tfrac{1}{2}\left(\left(\frac{-1}{p}\right) + \left(\frac{2}{p}\right)\right). \qquad (14)$$

Tomuto vzorci možno dáti jednodušší tvar, totiž:

$$P_2(p) - P_3(p) = \left[\frac{p}{4}\right] + \tfrac{1}{2}\left(1 + \left(\frac{2}{p}\right)\right). \qquad (15)$$

Oba vzorce poskytují tytéž výsledky, o čemž se můžeme lehce přesvědčiti. Je-li p prvočíslo tvaru $(4k+1)$, potom jest:

$$\frac{p-1}{2} = k, \left[\frac{p}{4}\right] = k, \left(\frac{-1}{p}\right) = +1;$$

je-li pak p prvočíslem tvaru $(4k+3)$, potom jest:

$$\frac{p-1}{2} = k+1, \left[\frac{p}{4}\right] = k, \left(\frac{-1}{p}\right) = -1.$$

Výsledky dosazení do obou vzorců jsou totožné.

Poznámka. Při určování počtu čísel, jež jsou aspoň 4. stupně (mod p), jakož i při určování kongruencí, jímž tato čísla vyhovují, setkal jsem se s mnohými obtížemi, které však vesměs by odpadly, kdyby se podařilo určiti proměnou x tak, aby funkce:

$$ax^4 + bx^3 + cx^2 + dx + e \pmod{p},$$

kdež a, b, c, d, e jsou celá čísla, nekongruentní s nulou (mod p), byla kvadratickým zbytkem (mod p).

*

Remarque concernant le caractère quadratique des nombres.

(Extrait de l'article précédent.)

On apelle nombre du k-ième ordre (mod p) un nombre entier a satisfaisant à la relation (1) où $p > 1$ est un nombre premier impair, k un nombre entier positif, $\left(\frac{a}{p}\right)$ le symbole de Legendre. On obtient les nombres du 2-ème ordre (mod p) en posant dans la congruence (4) pour t un nombre entier satisfaisant à la relation (4'). La condition nécessaire et suffisante pour que a soit du 2-ème degré au moins (mod p) est que la congruence (4) soit résoluble par rapport à t. La considération respective est en rapport avec le problème: Trouver des résidus bitrigonaux $a(a+1)$ qui soient, en même temps, des residus quadratiques (mod. p). Il

suffit, en effet, de substituer, pour a, un nombre du 2-ème degré au moins (mod p).

Pour que a soit de l'ordre k au moins (mod p), il faut et il suffit que t satisfasse aux relations (6). On obtient, en particulier, pour $k = 3$ la condition (7) où satisfait à la relation (8″). Alors, les nombres a, de l'ordre 3 au moins (mod p), sont déterminés par la congruence (8).

Si $P_k(p)$ est le nombre des nombres incongrus a, de l'ordre k au moins (mod p), le nombre $P_1(p)$ est défini par l'équation (3), $P_2(p)$ par l'équation (10) et $P_3(p)$ par l'équation (14), où $\left[\frac{p}{4}\right]$ désigne la fonction de Gauss du nombre $\frac{1}{4}p$ (à savoir, le plus grand nombre entier contenu dans la fraction $\frac{1}{4}p$).

Des considérations analogues pour $k = 4$ conduisent au problème: Déterminer la variable x de manière qu'une fonction de x du 4-e ordre aux coefficients entiers soit un résidu quadratique (mod p).