Matyáš Lerch

Úvahy o theorii kvadratických zbytků pro kmenné moduly s novými vztahy k theorii kvadratických forem s kmennými zápornými determinanty

SPISY
VYDÁVANÉ
PŘÍRODOVĚDECKOU FAKULTOU
MASARYKOVY UNIVERSITY
REDAKTOR

PUBLICATIONS
DE LA
FACULTÉ DES SCIENCES
DE L'UNIVERSITÉ MASARYK
RÉDIGÉES PAR

BOHUSLAV HOSTINSKÝ

ROK 1923 Čís. 34

ÚVAHY O THEORII KVADRATICKÝCH ZBYTKŮ PRO KMENNÉ MODULY

S NOVÝMI VZTAHY K THEORII KVADRATICKÝCH FOREM S KMENNÝMI ZÁPORNÝMI DETERMINANTY.

(ÉTUDES SUR LA THÉORIE DES RÉSIDUS QUADRATIQUES SUIVANT UN MODULE PREMIER.
RELATIONS NOUVELLES AVEC LA THÉORIE DES FORMES QUADRATIQUES AYANT UN DÉTERMINANT NÉGATIF ET PREMIER.)

NAPSAL

M. LERCH.

VLASTNÍM NÁKLADEM VYDÁVÁ
PŘÍRODOVĚDECKÁ FAKULTA
BRNO, KOUNICOVA 59

NA SKLADĚ MÁ | EN VENTE CHEZ
KNIHKUPECTVÍ A. PÍŠA, BRNO, ČESKÁ 28

TISKEM POLYGRAFIE V BRNĚ.

V pozůstalosti M. Lercha byl mezi jiným rukopis práce nadepsané „Úvahy o theorii kvadratických zbytků pro kmenné moduly s novými vztahy k theorii kvadratických forem s kmennými zápornými determinanty“.

Tato práce, velmi pozoruhodná jak svými výsledky tak svou methodou, nebyla dosud uveřejněna. Redaktor Spisů vydávaných přírodovědeckou fakultou Masarykovy university domníval se, že je vhodno uveřejniti právě zde toto posmrtné dílo vynikajícího učence, jenž nás náhle opustil k největšímu zármutku fakulty v době, kdy se zabýval zařízením mathematického ústavu a jenž sledoval s nejživějším zájmem založení těchto Spisů.

V Brně, 24. srpna 1923.

Le manuscrit du travail intitulé „Études sur la théorie des résidus quadratiques suivant un module premier. Relations nouvelles avec la théorie des formes quadratiques ayant un déterminant négatif et premier“ (en tchèque) se trouvait dans les papiers laissés par M. Lerch.

Ce travail si remarquable autant par ses résultats que par sa méthode n'a pas encore été publié. Le rédacteur de ces Publications a pensé que c'est ici que doit trouver place cette oeuvre posthume du savant éminent qui, au plus grand regret de la Faculté, nous a été enlevé subitement au moment où il s'occupait de l'organisation de l'Institut mathématique et qui apportait le plus vif intérêt à la fondation de ce recueil.

Brno, le 24 août 1923.

B. Hostinský.

ÚVAHY O THEORII KVADRATICKÝCH ZBYTKŮ PRO KMENNÉ MODULY S NOVÝMI VZTAHY K THEORII KVADRATICKÝCH FOREM S KMENNÝMI ZÁPORNÝMI DETERMINANTY.

(AVEC UN RÉSUMÉ EN FRANÇAIS.)

I.

1. Znamenej nám q kladné kmenné číslo tvaru $4a+3$, a užívejme symbolu ε_ν k označení Legendreova znaménka

$$\varepsilon_\nu = \left(\frac{\nu}{q}\right) = -\left(\frac{-q}{\nu}\right), \quad (\nu = 1, 2, \ldots q-1),$$

s obvyklými doplňky

$$\varepsilon_o = \varepsilon_q = 0.$$

Pro záporné indexy $\nu = -\mu$ pak bude vždy předpokládáno

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

Polynom

$$Q(x) = \sum_{\nu=1}^{q-1} \varepsilon_\nu x^\nu \tag{1}$$

hoví algebraické shodě

$$Q^2(x) + q \equiv 0 \mod \frac{x^q - 1}{x - 1};$$

tu chceme prohloubiti v tom směru, že určíme podíl levé strany dělené modulem.

Při tom nám bude zavésti čísla $e_1, e_2, e_3, \ldots$ definovaná rovnicí

$$e_n = \sum_{\mu=1}^{n-1} \varepsilon_\mu \varepsilon_{n-\mu} = \sum_{\mu=1}^{n} \varepsilon_{n\mu-\mu^2} \tag{2^1}$$

pro $n \leq q$, aneb obecněji

$$e_n = \Sigma \varepsilon_\mu \varepsilon_\nu = \Sigma \varepsilon_{\mu\nu}, \quad \left(\begin{matrix}\mu,\ \nu = 1, 2, 3, \ldots q-1 \\ \mu + \nu = n\end{matrix}\right), \tag{2^2}$$

takže největší přípustná hodnota n jest $2q-2$, a jest $e_{2q-1} = 0$.

Indexy větší než $q-1$ znamenejme $q+n$; podmínka

$$\mu + \nu = q + n, \ \mu < q, \ \nu < q$$

se vyjádří hodnotou

$$\nu = q + n - \mu, \ \mu > n$$

tedy

$$e_{q+n} = \sum_{\mu=n+1}^{q-1} \varepsilon_\mu \varepsilon_{q+n-\mu}.$$

Zde pišme $q-\mu=\mu'$, i máme dle vztahu

$$\varepsilon_{q-\mu'}=-\varepsilon_{\mu'}$$

$$e_{q+n}=\sum_{\mu'=1}^{q-n-1}\varepsilon_{q-\mu'}\,\varepsilon_{n+\mu'}=-\sum_{\mu=1}^{q-n-1}\varepsilon_\mu\varepsilon_{n+\mu}.$$

Mimo to jest dle původní definice, ježto $\varepsilon_{q-n-\mu}=-\varepsilon_{n+\mu}$

$$e_{q-n}=\sum_{\mu=1}^{q-n-1}\varepsilon_\mu\varepsilon_{q-n-\mu}=-\sum_{1}^{q-n-1}\varepsilon_\mu\varepsilon_{n+\mu},$$

a tedy máme vztahy

$$(2^3)\qquad e_{q+n}=e_{q-n}=-\sum_{\mu=1}^{q-n-1}\varepsilon_\mu\varepsilon_{n+\mu},\quad (0\leq n<q).$$

Po každé jest

$$e_1=0,\quad e_{2q-1}=0$$

ve shodě s posledním vztahem.

Z rovnice (2^1) máme

$$e_{n+1}-e_n=-\sum_{\mu=1}^{n-1}\varepsilon_\mu(\varepsilon_{n+1-\mu}-\varepsilon_{n-\mu})+\varepsilon_n,$$

a tedy pro mod. 4

$$e_{n+1}-e_n-\varepsilon_n+\sum_{1}^{n-1}(\varepsilon_{n+1-\mu}-\varepsilon_{n-\mu})=\varepsilon_n+(\varepsilon_n-1)\equiv 1$$

odtud sečtením pro $n,\ n+1,\ldots n+k-1$:

$$e_{n+k}-e_n\equiv k\ (\text{mod. }4).$$

Klademe-li $n=1$, a znamenáme $k+1$ literou n, máme tedy

$$(2^4)\qquad e_n\equiv n-1\ (\text{mod. }4).$$

Na př. pro $q=7$ jsou Legendreova znaménka

$$\varepsilon_\nu=++-+--$$

a tedy

$$e_1=0,\ e_2=1,\ e_3=2,\ e_4=-1,\ e_5=0,\ e_6=1.$$

V důsledku definice čísel e_n rovnicí (2^2) jest čtverec polynomu $Q(x)$

$$(3)\qquad Q^2(x)=\sum_{n=1}^{2q-2}e_n x^n;$$

výraz ten pišme jak následuje

$$Q^2(x)=\sum_{1}^{q-1}e_n x^n+\sum_{0}^{q-2}e_{q+n}x^n+(x^q-1)\sum_{n=0}^{q-2}e_{q+n}x^n,$$

aneb připojivše na obou stranách číslo q,

$$(\alpha)\quad Q^2(x)+q=[e_{q-1}x^{q-1}+(e_q+q)+\sum_{n=1}^{q-2}(e_n+e_{q+n})x^n]+(x^q-1)\sum_{0}^{q-2}e_{q+n}x^n.$$

Levá strana, jakož i poslední člen vpravo obsahují dělitele

$$\frac{x^q-1}{x-1}=x^{q-1}+x^{q-2}+x^{q-3}+\ldots+x^2+x+1,$$

i musí jím býti tedy dělitelen též výraz v hranaté závorce; an tento jest stupně $q-1$, bude podíl konstanta a sice e_{q-1}. Tedy

$$e_{q-1}x^{q-1}+(e_q+q)+\sum_{n=1}^{q-2}(e_n+e_{q+n})x^n=e_{q-1}\frac{x^q-1}{x-1};$$

odtud máme porovnáním stálých členů

$$e_q+q=e_{q-1},$$

mimo to jest dle definice (2^1) pro $n=q$

$$e_q=\sum_{1}^{q-1}\varepsilon_\mu\varepsilon_{q-\mu}=-(q-1),$$

čímž vychází

$$(4^1)\qquad e_q=1-q,\quad e_{q-1}=1$$

a naše identita poslední se zjednoduší na

$$(4)\qquad x^{q-1}+1+\sum_{n=1}^{q-2}(e_n+e_{q+n})x^n=\frac{x^q-1}{x-1};$$

z ní vychází porovnáním součinitelů vztahy

$$(4^2)\qquad e_n+e_{q+n}=1,\ (o<n<q),$$

které ji úplně vyčerpávají. Vzhledem k (2^3) máme odtud

$$(4^3)\qquad e_{q+n}=e_{q-n}=1-e_n,\ (o<n<q).$$

Vložíme-li hodnotu (4) do hořejšího vzorce pro $Q^2(x)+q$, obdržíme

$$Q^2(x)+q=\frac{x^q-1}{x-1}+(x^q-1)\sum_{n=0}^{q-2}e_{q+n}x^n;$$

tu jest

$$\sum_{0}^{q-2}e_{q+n}x^n=e_q+\sum_{1}^{q-2}(1-e_n)x^n=\sum_{1}^{q-1}(1-e_n)x^n+1-q=$$
$$=\frac{x^q-1}{x-1}-q-\sum_{1}^{q-1}e_nx^n,$$

čímž vychází

$$Q^2(x)+q=\frac{x^q-1}{x-1}+\frac{(x^q-1)^2}{x-1}-q(x^q-1)-(x^q-1)\sum_{1}^{q-1}e_nx^n,$$

čili

$$(I)\qquad Q^2(x)=\frac{x^q-1}{x-1}+\frac{(x^q-1^2)}{x-1}-qx^q+(1-x^q)\sum_{n=1}^{q-1}e_nx^n,$$

2. Z rovnice (2^3) a (4^3) plyne

$$(4^*)\qquad \sum_{\mu=1}^{q-n-1}\varepsilon_\mu\varepsilon_{n+\mu}=e_n-1=-1+\sum_{\mu=1}^{n-1}\varepsilon_\mu\varepsilon_{n-\mu},$$

tedy zvláště

$$(4^4)\qquad \sum_{1}^{q-2}\varepsilon_\mu\varepsilon_{\mu+1}=-1,\quad \sum_{\mu=1}^{q-3}\varepsilon_\mu\varepsilon_{\mu+2}=0$$
$$\sum_{1}^{q-4}\varepsilon_\mu\varepsilon_{\mu+3}=2\varepsilon_2-1,\quad \sum_{1}^{q-5}\varepsilon_\mu\varepsilon_{\mu+4}=2\varepsilon_3.$$

První z těchto rovnic podává bezprostředně větu:

Pro kmenné moduly q tvaru $4a+3$ obsahuje úplná řada Legendreových znamének

(L) $$\varepsilon_1\ \varepsilon_2\ \varepsilon_3\ \ldots\ \varepsilon_{q-1}$$

o jednu změnu více než sledů, t. j. obsahuje $\frac{q-3}{2}$ *sledů a* $\frac{q-1}{2}$ *změn.*

Ustanovme počet případů, kdy v řadě (L) jsou dvě sousední znaménka kladná; je patrně dán výrazem

$$\sum_1^{q-2}\frac{(1+\varepsilon_\nu)(1+\varepsilon_{\nu+1})}{4},$$

jenž má hodnotu

$$\frac{q-2}{4}+\sum_1^{q-3}\frac{\varepsilon_\nu+\varepsilon_{\nu+1}}{4}+\tfrac{1}{4}\sum_1^{q-2}\varepsilon_\nu\varepsilon_{\nu+1},$$

tedy dle (4[4]) a vzhledem k identitám

$$\sum_1^{q-2}\varepsilon_\nu=\sum_1^{q-1}\varepsilon_\nu-\varepsilon_{q-1}=1,\quad\sum_1^{q-2}\varepsilon_{\nu+1}=-1$$

bude

$$\sum_1^{q-2}\frac{1+\varepsilon_\nu}{2}\frac{1+\varepsilon_{\nu+1}}{2}=\frac{q-3}{4}:$$

V řadě (L) jest $\frac{q-3}{4}$ dvojic sousedních členů kladných a tolikéž dvojic sousedních členů záporných. Jinak vysloveno:

V řadě čísel (při kmenném q)

$$1,\ 2,\ 3,\ldots q-1 \qquad (q\equiv 3\ mod.\ 4)$$

jest $\frac{q-3}{4}$ *kvadratických zbytků, po nichž následuje zbytek, a tolikéž nezbytků, po nichž následuje nezbytek.*

Na př. pro $q=11$ máme znaménka

$$\varepsilon=+\ -\ +\ +\ +\ -\ -\ -\ +\ -$$

tedy zbytky v párech (3, 4) (4, 5); $\frac{11-3}{4}=2$

nezbytky v párech (6, 7) (7, 8).

Nazveme-li u sousedních členů pořad znamének $-+$ vzestupem a pořad $+-$ sestupem, podává nám výraz

$$\sum_1^{q-3}\frac{1-\varepsilon_\nu}{2}\frac{1+\varepsilon_{\nu+1}}{2}=\frac{q-1}{4}+\tfrac{1}{4}\left(\sum_1^{q-2}\varepsilon_{\nu+1}-\sum_1^{q-2}\varepsilon_\nu\right)=\frac{q-3}{4}$$

počet vzestupů a výraz

$$\sum_1^{q-2}\frac{1+\varepsilon_\nu}{2}\cdot\frac{1-\varepsilon_{\nu+1}}{2}=\frac{q+1}{4}$$

počet sestupů, jinak vyjádřeno:

V řadě čísel

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

přichází $\frac{q+1}{4}$ *kvadratických zbytků, po nichž následuje nezbytek, a* $\frac{q-3}{4}$ *nezbytků, po nichž následuje kvadratický zbytek.*

Na př. pro $q=11$ jsou první případy

$$(1,\ 2),\ (5,\ 6),\ (9,\ 10);\ \left(\frac{11+1}{4}=3\right)$$

druhé případy

$$(2,\ 3),\ (8,\ 9);\ \left(\frac{11-3}{4}=2\right).$$

Výsledek ten lze též takto vyjádřiti:

Nejmenší kladné zbytky mod. q čísel

$$1^2,\ 2^2,\ 3^2,\ \ldots\ \frac{(q-1)^2}{4},$$

seřazené vzestupně dle velikosti tvoří $\frac{q+1}{4}$ *skupin v přirozené posloupnosti*.*

Př. $q=7$; $1,\ 2\,|\,4$; $\quad\frac{q+1}{4}=2$

$q=11$; $1\,|\,3,\ 4,\ 5\,|\,9$; $\quad\frac{q+1}{4}=3$

$q=19$; $1\,|\,4,\ 5,\ 6,\ 7\,|\,9\,|\,11\,|\,16,\ 17$; $\quad\frac{q+1}{4}=5.$

3. Znamenejme nyní

$$\frac{q-1}{2}=m,$$

takže v našem případě m je liché.

Na pravé straně rovnice (v . (4^4))

$$-1=\sum_{1}^{2m-1}\varepsilon_\mu\varepsilon_{\mu+1}$$

proveďme rozklad v agregáty $\mu<m$ a $\mu\geq m$; u členů tohoto pišme $q-\mu-1=\nu$; vyjde

$$-1=\sum_{\nu=1}^{m-1}\varepsilon_\mu\varepsilon_{\mu+1}+\sum_{\nu=1}^{m}\varepsilon_{q-\nu-1}\varepsilon_{q-\nu},$$

a ježto druhá část je

$$\sum_{1}^{m}\varepsilon_\nu\varepsilon_{\nu+1}=\sum_{1}^{m-1}\varepsilon_\nu\varepsilon_{\nu+1}+\varepsilon_m\varepsilon_{m+1},$$

dále

$$\varepsilon_m\varepsilon_{m+1}=\varepsilon_{2m}\varepsilon_{2m+2}=\varepsilon_{q-1}\varepsilon_{q+1}=-1,$$

vychází vztah

(5) $$\sum_{1}^{m-1}\varepsilon_\mu\varepsilon_{\mu+1}=0;\quad m=\frac{q-1}{2}.$$

---

* Při tom se béře isolovaný zbytek jako řada o jednom členu.

To podává bezprostředně větu:

V poloviční řadě Legendreových znamének pro kmenný modul $q = 4a + 3$

(M) $\varepsilon_1\ \varepsilon_2\ \varepsilon_3\ \ldots\ \varepsilon_m$

je právě tolik sledů co změn.

$q = 11$, $m = 5$; znaménka

$$+\ -\ +\ +\ +$$

dávají dvě změny $+\,-$, $-\,+$ a dva sledy $+\,+$.

Hledejme počet vzestupů $(-\,+)$ v řadě (M). Je dán výrazem

$$\sum_1^{m-1} \frac{1-\varepsilon_\nu}{2}\,\frac{1+\varepsilon_{\nu+1}}{2} = \frac{m-1}{4} + \tfrac{1}{4}\left(\sum_1^{m-1}\varepsilon_{\nu+1} - \sum_1^{m-1}\varepsilon_\nu\right);$$

uzávorkovaný výraz $= \varepsilon_m - \varepsilon_1$; ježto pro naše moduly

$$\varepsilon_m = -\,\varepsilon_2,$$

vychází pro počet vzestupů výraz

$$\frac{m-1}{4} - \frac{1+\varepsilon_2}{4},$$

kdežto počet sestupů jest

$$\frac{m-1}{4} + \frac{1+\varepsilon_2}{4}.$$

V řadě čísel

$$1,\ 2,\ 3,\ \ldots\ \frac{q-1}{2}$$

přichází

$$\frac{q-3}{8} + \frac{1+\varepsilon_2}{4}$$

kvadratických zbytků mod. q, po nichž následuje nezbytek, a

$$\frac{q-3}{8} - \frac{1+\varepsilon_2}{2}$$

nezbytků, po nichž následuje zbytek.

Př. $q = 7$; čísla ta jsou resp. 1, 0. Pořad znamenék $+\,+\,-$; po zbytku 2 následuje nezbytek 3, a po žádném nezbytku nenásleduje zbytek.

$q = 11$; obě čísla jsou $= 1$; $\varepsilon = +\ -\ +\ +\ +$
$q = 19$; obě čísla jsou $= 2$; $\varepsilon = +\ -\ -\ +\ +\ +\ +\ -\ +$.

Znamenáme-li $Cl(-q)$ počet tříd kladných forem

$$ax^2 + bxy + cy^2$$

diskriminantu $-q = b^2 - 4ac$, a literou H počet tříd kvadratických forem Gaussových

$$a_1x^2 + 2b_1xy + c_1y^2$$

determinantu $-q = b_1^2 - a_1 c_1$, jest dle Dirichleta

$$H = (2 - \varepsilon_2)\, Cl\,(-q) = \sum_1^m \varepsilon_\nu .$$

Tohoto vztahu bude nám užíti při stanovení kladných dvojic $(+\,+)$ sousedních znamének, a rovněž pro počet dvojic záporných $(-\,-)$.

Počet kladných dvojic v řadě (M) jest

$$\sum_1^{m-1} \frac{1+\varepsilon_\mu}{2}\,\frac{1+\varepsilon_{\mu+1}}{2} = \frac{m-1}{4} + \tfrac{1}{4}\left(\sum_1^{m-1}\varepsilon_\mu + \sum_1^{m-1}\varepsilon_{\mu+1}\right) =$$

$$\frac{m-1}{4} + \frac{1}{4}\left(2\sum_1^m \varepsilon_\mu - \varepsilon_1 - \varepsilon_m\right) = \frac{q-3}{8} + \tfrac{1}{2}\left(H - \frac{1-\varepsilon_2}{2}\right),$$

a počet dvojic záporných patrně

$$\frac{q-3}{8} - \tfrac{1}{2}\left(H - \frac{1-\varepsilon_2}{2}\right).$$

Pro $\varepsilon_2 = 1$ jest $H \geq 1$, a pro $\varepsilon_2 = -1$ jest $H \geq 3$, ve všech případech tedy uzávorkovaný výraz je kladný.

V poloviční řadě Legendreových znamének (M) jest větší počet dvojic sousedních členů kladných než dvojic záporných. Rozdíl obnáší

$$H - \frac{1-\varepsilon_2}{2}.$$

Oba počty jsou dány vzorci

$$\frac{q-3}{8} \pm \tfrac{1}{2}\left(H - \frac{1-\varepsilon_2}{2}\right).$$

Př. $q = 11$, $H = 3$; počty jsou $1 + 1$; jsou dvě dvojice kladné (3, 4), (4, 5), a žádná dvojice záporná.

$q = 19$, $H = 3$; počty $= 2 \pm 1$;
3 dvojice kladné (4, 5), (5, 6), (6, 7),
1 dvojice záporná (2, 3).

Jinak vysloveno:

V řadě čísel

$$1,\ 2,\ 3,\ \ldots\ \frac{q-1}{2}$$

příslušné ke kmennému modulu $q = 4a + 3$ jest

$$\frac{q-3}{8} + \tfrac{1}{2}\left(H - \frac{1-\varepsilon_2}{2}\right)$$

párů sousedních zbytků kvadratických, a

$$\frac{q-3}{8} - \tfrac{1}{2}\left(H - \frac{1-\varepsilon_2}{2}\right)$$

dvojic sousedních nezbytků.

Stůj zde ještě příklad

$$q = 23, \quad m = 11, \quad H = 3,$$
$$\varepsilon = + + + + - + - + + - -;$$

počty $\frac{5}{2} \pm \frac{3}{2}$ udávají čtyři dvojice kladné a jednu dvojici zápornou.

4. Druhá z rovnic (4^4)

$$\sum_{1}^{q-3} \varepsilon_\mu \varepsilon_{\mu+2} = 0$$

obsahuje výsledek, že

v řadě (L) právě tolik členů odděluje dvě znamení stejná, kolik jich odděluje dvě znamení opačná.

Trojiny s kladnými okraji $(+ \pm +)$ jsou v počtu

$$\sum_{1}^{q-3} \frac{1+\varepsilon_\mu}{2} \frac{1+\varepsilon_{\mu+2}}{2} = \frac{q-3}{4} + \frac{1}{4}\left(\sum_{1}^{q-3} \varepsilon_\mu + \sum_{1}^{q-3} \varepsilon_{\mu+2}\right) = \frac{q-3}{4}:$$

V řadě čísel

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

stane se $\frac{q-3}{4}$ *kráte, že jeden prvek jest obklopen dvěma zbytky a tolikéž případů jest, kdy prvek obklopen jest dvěma nezbytky.*

$q = 7; \quad \varepsilon = + + - + - -$

1. (2, 3, 4)
2. (3, 4, 5).

V rovnici

$$\sum_{\mu=1}^{q-3} \varepsilon_\mu \varepsilon_{\mu+2} = 0$$

oddělme členy $\mu \geqq m-1$ a kladme v nich $\mu = q-2-\nu$; bude

$$\sum_{m-1}^{q-3} \varepsilon_\mu \varepsilon_{\mu+2} = \sum_{\nu=1}^{m} \varepsilon_\nu \varepsilon_{\nu+2} = \sum_{\nu=1}^{m-2} \varepsilon_\nu \varepsilon_{\nu+2} + \varepsilon_{m-1}\varepsilon_{m+1} + \varepsilon_m \varepsilon_{m+2}.$$

Ježto

$$\varepsilon_{m-1}\varepsilon_{m+1} = -\varepsilon_3, \quad \varepsilon_m \varepsilon_{m+2} = -\varepsilon_3,$$

nacházíme

$$\sum_{1}^{m-2} \varepsilon_\mu \varepsilon_{\mu+2} = \varepsilon_3. \tag{6}$$

První člen vlevo $\mu = 1$ má hodnotu $\varepsilon_1 \varepsilon_3 = \varepsilon_3$; vynecháme-li jej na obou stranách, vznikne věta:

Řada $\varepsilon_3 \varepsilon_5 \ldots . \varepsilon_{m-2}$ *obsahuje tolik změn co řada* $\varepsilon_2 \varepsilon_4 \ldots . \varepsilon_{m-3}$ *sledů.*

$q = 23$; řady naše jsou tu

$$+ - - + -$$
$$+ + + + -.$$

Počet členů řady (M) sevřených dvěma členy kladnými obnáší dle (6)

$$\sum_1^{m-2} \frac{1+\varepsilon_\mu}{2}\,\frac{1+\varepsilon_{\mu+2}}{2} = \frac{m-2}{4} + \frac{\varepsilon_3}{4} + \tfrac{1}{4}\left(\sum_1^{m-2}\varepsilon_\mu + \sum_1^{m-2}\varepsilon_{\mu+2}\right).$$

Závorka má hodnotu

$$2H - \varepsilon_{m-1} - \varepsilon_m - \varepsilon_1 - \varepsilon_2 = 2H - (1-\varepsilon_6),$$

a tedy zní počet trojin s kladnými okraji v řadě (M)

$$\frac{m-3}{4} + \frac{\varepsilon_3+\varepsilon_6}{4} + \tfrac{1}{2}H,$$

kdežto počet trojin s okraji zápornými jest

$$\frac{m-1}{4} + \frac{\varepsilon_3-\varepsilon_6}{4} - \tfrac{1}{2}H;$$

první mají převahu nad druhými o

$$H - \frac{1-\varepsilon_6}{2}.$$

Výsledky lze takto vyjádřiti:

V řadě čísel

$$1,\ 2,\ 3,\ \ldots.\ m \qquad \left(m = \frac{q-1}{2},\ q \text{ kmenné} = 4a+3\right)$$

jest

$$\frac{m-3}{4} + \frac{1+\varepsilon_2}{4}\varepsilon_3 + \tfrac{1}{2}H$$

prvků obklopených dvěma kvadratickýma zbytky mod. q, dále

$$\frac{m-1}{4} + \frac{1-\varepsilon_2}{4}\varepsilon_3 - \tfrac{1}{2}H$$

prvků obklopených dvěma nezbytky.

Př. $q = 23$, $H = 3$, $\varepsilon_3 = 1$; výrazy znějí

$$2 + \tfrac{1}{2} + \tfrac{3}{2} = 4, \quad \tfrac{5}{2} - \tfrac{3}{2} = 1.$$

Zbytky jsou obklopena čísla $\nu = 2,\ 3,\ 5,\ 7,$ nezbytky jest obklopeno číslo $\nu = 6.$

$$\varepsilon = + + + + - + - + + - -.$$

Trojiny vzestupné $(- \pm +)$ řady (M) jsou v počtu

$$\sum_1^{m-2} \frac{1-\varepsilon_\mu}{2}\,\frac{1+\varepsilon_{\mu+2}}{2} = \frac{m-2}{4} - \frac{\varepsilon_3}{4} + \tfrac{1}{4}\left(\sum_1^{m-2}\varepsilon_{\mu+2} - \sum_1^{m-2}\varepsilon_\mu\right);$$

závorka má hodnotu $\varepsilon_m + \varepsilon_{m-1} - \varepsilon_1 - \varepsilon_2 = -(1 + 2\varepsilon_2 + \varepsilon_6)$ a tedy pravá strana

$$= \frac{m-2-\varepsilon_2}{4} - \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4}.$$

Trojiny sestupné jsou v počtu

$$\frac{m-2}{4} - \frac{\varepsilon_3}{4} + \tfrac{1}{4}(1 + 2\varepsilon_2 + \varepsilon_6) = \frac{m-2-\varepsilon_2}{4} + \varepsilon_2 + \frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}.$$

V řadě čísel

$$1,\ 2,\ 3,\ \ldots\ m \quad \left(m = \frac{q-1}{2},\ q \text{ kmenné} = 4a+3\right)$$

jest

$$\frac{m-2-\varepsilon_2}{4} - \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4} = \left[\frac{q}{8}\right] - \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4}$$

prvků, jimž předchází nezbytek, a po nichž přichází kvadratický zbytek.

A je tam

$$\left[\frac{q}{8}\right] + \varepsilon_2 + \frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}$$

prvků, jimž předchází kvadratický zbytek a následuje nezbytek.

Pro $q = 23$ jsou tyto počty resp. $2-1=1$, $2+1=3$.

5. Pro moduly q a úplnou řadu (L) lze jíti o krok dále a stanoviti počet trojin určitého typu, kde všecky tři prvky $\varepsilon_\nu, \varepsilon_{\nu+1}, \varepsilon_{\nu+2}$ mají hodnoty dané.

Uvažujme součet

$$A = \sum_1^{q-1} \varepsilon_{\nu^2-1}\,\varepsilon_\nu;$$

klademe-li $\nu = q-\mu$, vyjde $\nu^2 - 1 \equiv \mu^2 - 1$, a tedy

$$A = -\sum_{\mu=1}^{q-1} \varepsilon_{\mu^2-1}\,\varepsilon_\mu = -A,$$

t. j. $A = 0$, čili*

(A) $$\sum_1^{q-3} \varepsilon_\nu\,\varepsilon_{\nu+1}\,\varepsilon_{\nu+2} = 0.$$

Ve spojení s rovnicemi

$$\sum_1^{q-2} \varepsilon_\nu\,\varepsilon_{\nu+1} = -1, \quad \sum_1^{q-3} \varepsilon_\nu\,\varepsilon_{\nu+2} = 0$$

umožňuje tento vztah stanoviti součty

$$\sum_1^{q-3} \frac{1\pm\varepsilon_\nu}{2} \cdot \frac{1\pm\varepsilon_{\nu+1}}{2} \frac{1\pm\varepsilon_{\nu+2}}{2}.$$

Výsledek zní jak následuje:

V úplné řadě Legendreových znamének pro kmenný modul $q = 4a+3$

$$\varepsilon_1\ \varepsilon_2\ \varepsilon_3\ \ldots\ \varepsilon_{q-1},$$

jest $\dfrac{q-3-2(1+\varepsilon_2)}{8}$ *trojin každého z typů*

$$+++,\ -++,\ ---,\ --+$$

a dále $\dfrac{q-3+2(1+\varepsilon_2)}{8}$ *trojin každého z typů*

$$+-+,\ -+-,\ ++-,\ +--.$$

---

* Ernst Jacobsthal, Anwendungen einer Formel aus der Theorie der quadratischen Reste. Inaugural-Dissertation, Berlin 1906.

Stručněji:

Typy trojin, jaké se vyskytují u modulu $q=7$, *jsou v počtu* $\frac{q-3+2(1+\varepsilon_2)}{8}$; *ostatní jsou v počtu o* $\frac{1+\varepsilon_2}{2}$ *menším.*

II.

6. Uvažujme nyní kmenná čísla p tvaru $4a+1$, a příslušná znaménka Legendreova znamenejme opět

$$\varepsilon_\nu = \left(\frac{\nu}{p}\right) = \left(\frac{p}{\nu}\right);$$

zde ovšem bude $\varepsilon_{p-\nu} = \varepsilon_{-\nu} = \varepsilon_\nu$ na rozdíl od případu kdy modul je kmenné číslo q tvaru $4a+3$.

Zavedeme opět polynom

$$Q(x) = \sum_1^{p-1} \varepsilon_\nu x^\nu,$$

a čísla e_n rovnicí

$$(7) \qquad e_n = \Sigma \varepsilon_\mu \varepsilon_\nu \begin{pmatrix} \mu,\ \nu = 1, 2, \ldots p-1 \\ \mu+\nu = n \end{pmatrix},\ 0 < n < 2p-1,$$

dále $e_{2p-1} = 0$; tedy pro $n \leq p$

$$(7^1) \qquad e_n = \sum_1^{n-1} \varepsilon_\mu \varepsilon_{n-\mu} = \sum_1^{n-1} \varepsilon_{n\mu-\mu^2}.$$

Pro přípony větší než p, které pišme $p+n$, máme $\mu+\nu = p+n$, $\nu < p$, tedy $\mu > n$

$$e_{p+n} = \sum_{\mu=n+1}^{p-1} \varepsilon_\mu \varepsilon_{p+n-\mu}$$

aneb píšeme-li $\mu = p-\nu$,

$$(7^2) \qquad e_{p+n} = \sum_1^{p-n-1} \varepsilon_{p-\nu} \varepsilon_{n+\nu} = \sum_1^{p-n-1} \varepsilon_\nu \varepsilon_{n+\nu}.$$

Číslo

$$e_{p-n} = \sum_1^{p-n-1} \varepsilon_\mu \varepsilon_{p-n-\mu} = \sum_1^{p-n-1} \varepsilon_\mu \varepsilon_{n+\mu},$$

splývá tedy s hodnotou e_{p+n},

$$(7^3) \qquad e_{p+n} = e_{p-n} \qquad (0 < n < p)$$

jako pro moduly q.

Čtverec polynomu $Q(x)$ bude tu rovněž

$$Q^2(x) = \sum_1^{2p-2} e_n x^n = \sum_1^{p-1} e_n x^n + \sum_0^{p-2} e_{p+n} x^{p+n},$$

a lze jej psáti

$$Q^2(x) = \sum_1^{p-1} e_n x^n + \sum_0^{p-2} e_{p+n} x^n + (x^p - 1) \sum_0^{p-2} e_{p+n} x^n,$$

takže

$$Q^2(x) - p = [e_{p-1} x^{p-1} + (e_p - p) + \sum_1^{p-2} (e_n + e_{p+n}) x^n] + \\ + (x^p - 1) \sum_0^{p-2} e_{p+n} x^n.$$

Z dělitelnosti levé strany polynomem

$$\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\ldots+x+1$$

soudíme, že výraz v hranaté závorce obsažený je týmž polynomem dělitelný, a tedy splývá s výrazem

$$e_{p-1}x^{p-1}+(e_p-p)+\sum_1^{p-2}(e_n+e_{p+n})x^n=e_{p-1}\frac{x^p-1}{x-1},$$

z čehož vychází

$$e_p-p=e_{p-1},\ e_n+e_{p+n}=e_{p-1},\ (n<p-1).$$

Ježto $e_p=\Sigma\varepsilon_\mu\varepsilon_{p-\mu}=\Sigma\varepsilon^2{}_\mu=p-1$, máme postupně

$$e_p=p-1,\ e_{p-1}=-1,\ e_n+e_{p+n}=-1, \tag{8}$$

$$e_{p-n}=-1-e_n,\ (n=1,\ 2,\ \ldots.\ p-1). \tag{8*}$$

Poslední vyjádření čtverce $Q^2(x)$ pak přejde v

$$Q^2(x)-p=-\frac{x^p-1}{x-1}+(x^p-1)\sum_0^{p-2}e_{p+n}x^n,$$

a dosadíme-li sem hodnoty

$$e_p=p-1,\ e_{p+n}=-1-e_n \text{ pro } n>0,$$

vyjde

$$Q^2(x)-p=-\frac{x^p-1}{x-1}+(x^p-1)\left[p-\sum_1^{p-1}e_nx^n-\frac{x^p-1}{x-1}\right],$$

takže bude konečně

$$Q^2(x)=px^p-\frac{x^p-1}{x-1}-\frac{(x^p-1)^2}{x-1}-(x^p-1)\sum_1^{p-1}e_nx^n, \tag{II}$$

pro kmenné moduly p tvaru $4a+1$.

Ježto dle (8*) součet

$$\sum_{\mu=1}^{p-n-1}\varepsilon_\mu\varepsilon_{n+\mu}=e_{p-n}$$

má hodnotu

$$-1-e_n=-1-\sum_1^{n-1}\varepsilon_\mu\varepsilon_{n-\mu},$$

máme vztah

$$\sum_1^{p-n-1}\varepsilon_\mu\varepsilon_{n+\mu}=-1-\sum_1^{n-1}\varepsilon_\mu\varepsilon_{n-\mu}. \tag{8^1}$$

Jako zvláštní případy vytkněme

$$\sum_1^{p-2}\varepsilon_\mu\varepsilon_{\mu+1}=-1,\ \sum_1^{p-3}\varepsilon_\mu\varepsilon_{\mu+2}=-2, \tag{8^2}$$

kteréžto rovnice povedou nás k analogickým výsledkům jako výše vztahy (4^4).

Znamenejme opět

$$\frac{p-1}{2}=m,$$

takže tu jest m číslo sudé; levá strana rovnice (8^2) rozštěpí se v součty

$$\sum_1^{m-1}\varepsilon_\mu\varepsilon_{\mu+1}+\sum_m^{2m-1}\varepsilon_\nu\varepsilon_{\nu+1};$$

ve druhém položíme $\nu = p - \mu - 1$, $(\mu = 1, 2, \ldots m)$, čímž obdrží tvar

$$\sum_{\mu=1}^{m} \varepsilon_\mu \varepsilon_{\mu+1} = \sum_{1}^{m-1} \varepsilon_\mu \varepsilon_{\mu+1} + \varepsilon_m \varepsilon_{m+1}.$$

Zde $\varepsilon_m \varepsilon_{m+1} = \varepsilon_{2m} \varepsilon_{2m+2} = \varepsilon_{p-1} \varepsilon_{p+1} = 1$, a tedy vyjde

$$(9) \qquad \sum_{1}^{m-1} \varepsilon_\mu \varepsilon_{\mu+1} = -1, \left(m = \frac{p-1}{2},\ p \text{ kmenné} = 4a+1\right).$$

Z rovnic (8²) a (9) vychází:

V plné řadě Legendreových znamének pro kmenný modul p tvaru $4a + 1$

$$(L') \qquad \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p-1}$$

je změn o jednu více než sledů.

Podobně tomu jest u řady poloviční

$$(M') \qquad \varepsilon_1 \varepsilon_2 \ldots \varepsilon_m, \left(m = \frac{p-1}{2}\right).$$

Následkem vztahu

$$\sum_{1}^{m} \varepsilon_\nu = 0,$$

platného pro moduly p, jsou věty k těmto modulům se vztahující značně jednodušší než v případě modulů q. Tak na př. výraz

$$\sum_{1}^{m-1} \frac{1+\varepsilon_\nu}{2} \frac{1+\varepsilon_{\nu+1}}{2} = \frac{m-1}{4} - \tfrac{1}{4} - \frac{1+\varepsilon_2}{4} = \frac{p-7-2\varepsilon_2}{8}$$

má hodnotu $\left[\frac{p-2}{8}\right]$, kdežto změníme-li znaménka při ε_ν a $\varepsilon_{\nu+1}$, obdržíme hodnotu

$$\frac{m-1}{4} - \tfrac{1}{4} + \frac{1+\varepsilon_2}{4} = \frac{p-3+2\varepsilon_2}{8} = \left[\frac{p}{8}\right].$$

V poloviční řadě (M') *Legendreových znamének pro moduly p vyskytne se* $\left[\frac{p-2}{8}\right]$ *dvojic sousedních členů kladných, a* $\left[\frac{p}{8}\right]$ *dvojic sousedních členů záporných.*

Jinak vyjádřeno:

V řadě čísel

$$1, 2, 3, \ldots \frac{p-1}{2}$$

příslušné ke kmennému modulu $p = 4a + 1$ *stane se* $\left[\frac{p-2}{8}\right]$ *kráte, že po kvadratickém zbytku následuje zbytek, a* $\left[\frac{p}{8}\right]$ *kráte, že po kvadratickém nezbytku následuje nezbytek.*

Př. $p = 17$

$$\varepsilon = + + - + - - - +$$

máme $\left[\frac{p-2}{8}\right] = 1$, dvojice zbytků (1, 2) a $\left[\frac{p}{8}\right] = 2$, dvojice nezbytků (5, 6), (6, 7).

Dále jest

$$\sum_1^{m-1} \frac{1-\varepsilon_\nu}{2}\frac{1+\varepsilon_{\nu+1}}{2} = \frac{m-1}{4} + \tfrac{1}{4} - \frac{1-\varepsilon_2}{4} = \left[\frac{p}{8}\right],$$

$$\sum_1^{m-1} \frac{1+\varepsilon_\nu}{2}\frac{1-\varepsilon_{\nu+1}}{2} = \frac{m-1}{4} + \tfrac{1}{4} + \frac{1-\varepsilon_2}{4} = \left[\frac{p+3}{8}\right],$$

t. j.

Řada (M') vykazuje $\left[\frac{p}{8}\right]$ vzestupů $(-+)$ a $\left[\frac{p+3}{8}\right]$ poklesů $(+-)$.

Je zajímavo, že táž forma výsledku zůstává v platnosti též pro moduly q, takže

pro kterýkoli kmenný modul $p > 3$ vykazuje poloviční řada Legendreových znamének

$$1, \left(\frac{2}{p}\right), \left(\frac{3}{p}\right), \left(\frac{4}{p}\right), \ldots \left(\frac{m}{p}\right), \left(m = \frac{p-1}{2}\right),$$

$\left[\frac{p}{8}\right]$ *vzestupů* $(-+)$ a $\left[\frac{p+3}{8}\right]$ *poklesů* $(+-)$.

7. Druhá z rovnic (8^2)

$$-2 = \sum_1^{m-2} \varepsilon_\mu \varepsilon_{\mu+2} + \sum_{m-1}^{2m-2} \varepsilon_\nu \varepsilon_{\nu+2}$$

podá substitucí $\nu = p - \mu - 2$ vztah

$$(9^1) \qquad \sum_1^{m-2} \varepsilon_\mu \varepsilon_{\mu+2} = -1 - \varepsilon_3.$$

Dle toho

$$\sum_1^{m-2} \frac{1-\varepsilon_\mu}{2}\frac{1+\varepsilon_{\mu+2}}{2} = \frac{m-2}{4} + \frac{1+\varepsilon_3}{4} - \frac{1-\varepsilon_6}{4} =$$

$$= \frac{m-2}{4} - \frac{1+\varepsilon_2}{4} + \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4} = \left[\frac{p-2}{8}\right] + \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4},$$

dále

$$\sum_1^{m-2} \frac{1+\varepsilon_\mu}{2}\frac{1-\varepsilon_{\mu+2}}{2} = \frac{m}{4} + \frac{\varepsilon_3(1-\varepsilon_2)}{4} =$$

$$= \frac{p+1-2\varepsilon_2}{8} - \frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4} = \left[\frac{p+3}{8}\right] - \frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}.$$

Trojiny $(+\pm+)$, pak $(-\pm-)$ mají variace dvě aneb žádnou, a trojiny $(+\pm-)$, pak $(-\pm+)$ mají variaci jen jednu. Můžeme tedy výsledky poslední takto vyjádřiti:

Z trojin řady (M') o jediné variaci jest jich

$$\left[\frac{p-2}{8}\right]+\frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4} \text{ vzestupných, a}$$

$$\left[\frac{p+3}{8}\right]-\frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4} \text{ sestupných.}$$

Rozdíl obnáší $\frac{1-\varepsilon_6}{2}$ s případnou převahou u těchto. Na př. pro $p=73$ zní řada znamének

$$a^4\,b\,a\,b\,a^3\,b^2\,a\,b^3\,a\,b\,a^2\,b^3\,a^3\,b\,a\,b^4\,a\,b^2\,a^2,$$

značí-li $a=+$, $b=-$ a exponent udává, kolikrát jde znaménko za sebou. Zde jest $8+1=9$ trojin vzestupných a $9-0=9$ trojin sestupných.

Počet trojin s kladnými okraji jest

$$\sum_1^{m-2}\frac{1+\varepsilon_\mu}{2}\frac{1+\varepsilon_{\mu+2}}{2}=\frac{m-2}{4}-\frac{1+\varepsilon_3}{4}-\frac{1+2\varepsilon_2+\varepsilon_6}{4}=$$

$$=\frac{m-3-\varepsilon_2}{4}-\frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4}=\left[\frac{p-2}{8}\right]-\frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4},$$

kdežto počet trojin se zápornými okraji obnáší

$$\frac{m-2}{4}-\frac{1+\varepsilon_3}{4}+\frac{1+2\varepsilon_2+\varepsilon_6}{4}=\frac{m-3-\varepsilon_2}{4}+\varepsilon_2+\frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}=$$

$$=\left[\frac{p-2}{8}\right]+\varepsilon_2+\frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}:$$

Řada (M') obsahuje

$$\left[\frac{p-2}{8}\right]-\frac{(1+\varepsilon_2)(1+\varepsilon_3)}{2} \text{ trojin s kladnými}$$

a

$$\left[\frac{p-2}{8}\right]+\varepsilon_2+\frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4} \text{ trojin se zápornými okraji.}$$

Převaha (kladná neb záporná) těchto nad oněmi obnáší $\varepsilon_2+\frac{1+\varepsilon_6}{2}$.

Tak pro modul $p=73$ máme trojiny s kladnými okraji v počtu $8-1=7$, se zápornými okraji v počtu $8+1=9$.

III.

8. Rovnice (I) čl. I., 1. pro moduly $q=4a-1$, t. j.

$$(I)\qquad Q^2(x)=\frac{x^q-1}{x-1}+\frac{(x^q-1)^2}{x-1}-qx^q+(1-x^q)\sum_1^{q-1}e_nx^n$$

dává podnět k různým vztahům, k nimž obrátíme nyní svou pozornost.

Nejprve položíme $x = -1$; poněvadž

$$Q(-1) = \sum_1^{q-1} (-1)^\nu \varepsilon_\nu = \Sigma \varepsilon_{2\nu} - \Sigma \varepsilon_{2\nu-1},$$

a dále

$$0 = \Sigma \varepsilon_{2\nu} + \Sigma \varepsilon_{2\nu-1},$$

vychází

$$Q(-1) = 2 \sum_1^m \varepsilon_{2\nu} = 2\, \varepsilon_2 \sum_{\nu=1}^m \varepsilon_\nu, \quad m = \frac{q-1}{2}.$$

Je však

$$\sum_1^m \varepsilon_\nu = H = (2 - \varepsilon_2)\, Cl(-q),$$

tedy

$$Q(-1) = 2\, \varepsilon_2 H,$$

a rovnice (I) podá pro $x = -1$

$$4H^2 = q - 1 + 2 \sum_{n=1}^{q-1} (-1)^n e_n, \tag{10}$$

kde H je počet tříd kvadratických forem primitivních pro determinant $-q$.

Součet

$$\sum_{n=m+1}^{q-1} (-1)^n e_n = \sum_1^m (-1)^{q-n} e_{q-n}$$

se po dosazení hodnoty

$$e_{q-n} = 1 - e_n$$

objeví ve tvaru

$$\sum_1^m (-1)^{n-1} + \sum_1^m (-1)^n e_n = 1 + \sum_1^m (-1)^n e_n,$$

takže bude

$$2 \sum_1^{q-1} (-1)^n e_n = 2 + 4 \sum_1^m (-1)^n e_n,$$

a tedy

$$H^2 = \frac{q+1}{4} + \sum_{n=1}^m (-1)^n e_n; \quad m = \frac{q-1}{2}. \tag{10*}$$

Pro $q = 11$ máme

$$\varepsilon_\nu = + - - + + +$$
$$e_\nu = 0,\ 1,\ -2,\ 3,\ 0$$

$$\sum_1^5 (-1)^n e_n = 1 + 2 + 3 = 6; \quad \frac{q+1}{4} = 3,\ 6 + 3 = H^2,\ H = 3.$$

V rovnici (I) derivujme dále obě strany na místě $x = 1$; znamenáme-li

$$\varphi(x) = \frac{x^q - 1}{x - 1}, \quad \psi(x) = \frac{(x^q - 1)^2}{x - 1}$$

máme

$$\varphi'(1) = \binom{q}{2}, \quad \varphi''(1) = 2 \binom{q}{3},$$

$$\psi''(1) = q(q-1)\varphi(1) + 2q\varphi'(1) = 2q^2(q-1);$$

tedy výsledek zní

$$2Q'(1)^2 = \frac{q(q-1)(q-2)}{3} + q^2(q-1) - q(q-1) \sum_1^{q-1} e_n - 2q \sum_1^{q-1} n e_n.$$

Tu vychází především z rovnice

$$e_n + e_{q-n} = 1$$

sečtením pro $n = 1, 2, \ldots q-1$ vztah

(a) $$\sum_1^{q-1} e_n = m,$$

dále jest

$$Q'(1) = \sum_1^{q-1} \nu \varepsilon_\nu = -q\, Cl(-q), \quad (q > 3),$$

tedy vychází po redukci

(11) $$q\, Cl(-q)^2 = \frac{(q-1)(q-2)}{6} + \frac{q^2-1}{4} - \sum_1^{q+1} n e_n.$$

Součet

$$\sum_1^{q-1} n e_n = \sum_1^{m} n e_n + \sum_{m+1}^{q-1} n e_n$$

v druhé jeho části substitucí $q-n$ za n obdrží tvar

$$\sum_1^{m} n e_n + \sum_1^{m} (q-n) e_{q-n},$$

ježto

$$e_{q-n} = 1 - e_n,$$

zní týž součet

$$\sum_1^{m} n e_n + \sum_1^{m} n e_n - q \sum_1^{m} e_n + qm - \frac{m(m+1)}{2},$$

takže bude

$$\sum_1^{q-1} n e_n = \sum_1^{m} (2n-q) e_n + qm - \frac{m(m+1)}{2}.$$

Dosazením této hodnoty na pravé straně (11) vznikne

(11*) $$q\, Cl(-q)^2 = \frac{q^2-1}{24} + \sum_1^{m} (q-2n) e_n; \quad \left(m = \frac{q-1}{2}\right).$$

Pro $q = 11$ se to verifikuje hodnotami

$$11 \cdot 1^2 = 5 + (11-4) \cdot 1 - (11-6)\, 2 + (11-8)\, 3.$$

9. Do rovnice (1) vložme nyní $x = i\,(i^2 = -1)$; tu jest

$$i^q = -i, \quad \frac{i^q - 1}{i-1} = i, \quad \frac{(i^q-1)^2}{i-1} = 1 - i,$$

$$Q(i) = A + iB, \quad A = \sum_1^{m} (-1)^\mu \varepsilon_{2\mu} = \varepsilon_2 \sum_1^{m} (-1)^\mu \varepsilon_\mu,$$

$$B = \Sigma (-1)^{\frac{\lambda-1}{2}} \varepsilon_\lambda, \quad (\lambda = 1, 3, 5, \ldots q-2).$$

Rovnice podává

$$(A + iB)^2 = 1 + iq + (1+i) \sum_1^{q-1} e_n i^n,$$

a násobíme-li obě strany $1 - i$,

$$(A^2 - B^2 + 2AB) + i(2AB + B^2 - A^2) = q + 1 + i(q-1) + 2 \sum_1^{q-1} e_n i^n;$$

porovnáním stejnorodých částí obou stran vychází

$$A^2 - B^2 + 2AB = q + 1 + 2\sum_1^m (-1)^\nu e_{2\nu},$$

$$B^2 - A^2 + 2AB = q - 1 + 2\sum_\lambda (-1)^{\frac{\lambda-1}{2}} e_\lambda, \quad (\lambda = 1, 3, 5, \ldots q-2).$$

Klademe-li $q - 2\nu = \lambda$, obdržíme

$$(-1)^\nu \varepsilon_{2\nu} = (-1)^{m-\nu} \varepsilon_{q-2\nu} = (-1)^{\frac{\lambda-1}{2}} \varepsilon_\lambda,$$

a tedy

$$\sum_1^m (-1)^\nu \varepsilon_{2\nu} = \sum_\lambda (-1)^{\frac{\lambda-1}{2}} \varepsilon_\lambda, \quad (\lambda = 1, 3, 5, \ldots q-2),$$

t. j.

$$A = B.$$

Zbývá jen určiti A. Výše bylo ukázáno, že

$$Q(-1) - 2\varepsilon_2 H = \sum_1^{q-1} (-1)^\nu \varepsilon_\nu.$$

Tento součet se štěpí jak následuje

$$Q = \sum_1^m (-1)^\nu \varepsilon_\nu + \sum_1^m (-1)^{q-\nu} \varepsilon_{q-\nu} = 2\sum_1^m (-1)^\nu \varepsilon_\nu = 2\varepsilon_2 A,$$

tedy jest $A = H$, t. j.

$$(12^a) \quad H = \varepsilon_2 \sum_1^m (-1)^\nu \varepsilon_\nu \quad \sum_\lambda (-1)^{\frac{\lambda-1}{2}} \varepsilon_\lambda, \quad (\lambda = 1, 3, 5, \ldots q-2).$$

Hořejší výsledky pak se zjednoduší na

$$(12) \quad H^2 = \frac{q+1}{2} + \sum_1^m (-1)^\nu e_{2\nu} = \frac{q-1}{2} + \sum_\lambda (-1)^{\frac{\lambda-1}{2}} e_\lambda,$$
$$(\lambda = 1, 3, 5, \ldots q-2).$$

Vraťme se k rovnici (10); rozliší-li se členy dle přípon sudých a lichých, vyjde

$$2H^2 = \frac{q-1}{2} + \sum_1^m e_{2\nu} - \sum e_\lambda,$$

rovnice (a) pak dává

$$\frac{q-1}{2} = \sum_1^m e_{2\nu} + \sum_\lambda e_\lambda;$$

sečtením, resp. odečtením posledních dvou rovnic vychází

$$(13) \quad H^2 = \sum_1^m e_{2\nu} = m - \sum_\lambda e_\lambda, \quad (\lambda = 1, 3, 5, \ldots q-2).$$

Sečteme-li první tvary výrazů (12) a (13), vyjde

$$(14) \quad H^2 = \frac{q+1}{4} + \sum_{\nu=1}^{\frac{1}{4}(q-3)} e_{4\nu},$$

poněvadž se členy tvaru $e_{4\nu-2}$ zruší. Odečteme-li tuto rovnici od (12), zruší se členy $e_{4\nu}$ a vyjde

$$(15) \quad e_2 + e_6 + e_{10} + \ldots + e_{2m} = \frac{q+1}{4}.$$

Užijeme-li vztahu

$$e_{4\nu-2} = 1 - e_{q+2-4\nu},$$

obdržíme odtud

(15a) $$e_{q-2} + e_{q-6} + e_{q-10} + \ldots = 0.$$

Na př. pro $q = 11$

$$e_9 + e_5 + e_1 = 0 \quad (e_1 = 0 = e_5 = e_9).$$

Pro $q = 19$; $e_{17} + e_{13} + e_9 + e_5 + e_1 = 0$; skutečně $e_1 = 0$, $e_5 = 4$, $e_9 = -4$, $e_{13} = 0 = e_{17}$.

Následkem (15a) se druhý výraz (13) zjednoduší na

(13*) $$H^2 = m - (e_3 + e_7 + e_{11} + \ldots + e_{q-4}).$$

$q = 19$; $e_3 = e_7 = -2$, $e_{11} = e_{15} = 2$;

$$H^2 = 3^2 = 9 - 0.$$

Obsah rovnic (10), (12), (13) vyčerpán jest vztahy (14), (13*), (15), (15a), t. j.

(A) $$H^2 = \frac{q+1}{4} + \sum_1^{\frac{1}{4}(q-3)} e_{4\nu} = \frac{q-1}{2} - \sum_1^{\frac{1}{4}(q-3)} e_{q-4\nu},$$

$$e_1 + e_5 + e_9 + \ldots + e_{q-2} = 0, \quad e_3 + e_6 + e_{10} + \ldots + e_{q-1} = \frac{q+1}{4}.$$

IV.

10. Analogické úvahy připínají se ke vzorci

(II) $$Q^2(x) = px^p - \frac{x^p - 1}{x-1} - \frac{(x^p - 1)^2}{x-1} - (x^p - 1)\sum_1^{p-1} e_n x^n,$$

který jsme výše dokázali pro kmenné moduly tvaru $4a + 1$, jenže výsledky jsou tu celkem povahy elementárnější.

Tak máme

$$Q(-1) = \sum_1^{p-1} (-1)^\nu \varepsilon_\nu$$

po substituci $\nu = p - \mu$, ježto pak $\varepsilon_{p-\mu} = \varepsilon_\mu$,

$$Q(-1) = -\Sigma(-1)^\mu \varepsilon_\mu = -Q(-1),$$

a tedy $Q(-1) = 0$.

V důsledku toho plyne z rovnice (II) pro $x = -1$ vztah velmi jednoduchý

(16) $$\sum_1^{p-1} (-1)^n e_n = \frac{p-1}{2} = m.$$

Na základě rovnice

(a) $$e_{p-n} = -1 - e_n$$

zjednoduší se poslední výsledek, rozštěpí-li se levá strana v

$$\sum_1^m (-1)^\nu e_\nu + \sum_1^m (-1)^{p-\nu} e_{p-\nu};$$

druhá část má hodnotu

$$-\Sigma(-1)^{\nu}(-1-e_{\nu}) = \Sigma(-1)^{\nu}e_{\nu} + \Sigma(-1)^{\nu} = \Sigma(-1)^{\nu}e_{\nu},$$

a tedy

$$\sum_{\nu=1}^{m}(-1)^{\nu}e_{\nu} = \frac{p-1}{4}. \tag{16*}$$

Příklad:

$$p = 13;\ -e_1 + e_2 - e_3 + e_4 - e_5 + e_6 = 3;$$

skutečně

$$e_2 = 1,\quad e_3 = -2,\quad e_4 = 3,\quad e_5 = 0,\quad e_6 = -3.$$

Z rovnice (*a*) plyne dále sečtením

$$\sum_{1}^{p-1} e_{\nu} = -m. \tag{b}$$

Ve spojení s (16) podává tato rovnice

$$\sum_{1}^{m} e_{2\nu} = 0,\quad e_1 + e_3 + e_5 + \ldots + e_{p-2} = -m. \tag{16^1}$$

Derivujme rovnici (II) dvakráte na místě $x = 1$; obdržíme tak vzhledem k známé okolnosti, že pro moduly p

$$\sum_{1}^{p-1} \nu\varepsilon_{\nu} = 0,$$

výsledek

$$\sum_{1}^{p-1} \nu e_{\nu} = -\frac{(p-1)(p-2)}{6} - \frac{p^2-1}{4} = -m\frac{5m+2}{3}. \tag{17}$$

Tu opět

$$\sum_{\nu=m+1}^{p-1} \nu e_{\nu} = \sum_{1}^{m}(p-\nu)e_{p-\nu} = -\sum_{1}^{m}(p-\nu) - \sum_{1}^{m}(p-\nu)e_{\nu}$$

a tedy levá strana (17) se může psáti

$$2\sum_{1}^{m}\nu e_{\nu} - p\sum_{1}^{m}e_{\nu} + \frac{m(m+1)}{2} - pm$$

takže po dosazení tohoto tvaru vychází

$$\sum_{1}^{m}(p-2\nu)e_{\nu} = \frac{p^2-1}{24}. \tag{17*}$$

11. Ve vzorci (II) položme $x = i$; především bude

$$i^p = i,\quad \frac{i^p - 1}{i - 1} = 1,$$

dále

$$Q(i) = A + iB,\quad A = \sum_{1}^{m}(-1)^{\nu}\varepsilon_{2\nu},\quad B = \sum_{\lambda}(-1)^{\frac{\lambda-1}{2}}\varepsilon_{\lambda},$$

$$(\lambda = 1,\ 3,\ 5,\ \ldots p-2).$$

Výraz

$$A = \varepsilon_2\sum_{1}^{m}(-1)^{\nu}\varepsilon_{\nu}$$

se zjednoduší, užije-li se vztahu platného pro moduly p

$$\sum_1^m \varepsilon_\nu = 0,$$

a sice vyjde

$$A = 2\varepsilon_2 \sum_1^{\frac{p-1}{4}} \varepsilon_{2\nu} = 2\sum_1^{\frac{p-1}{4}} \varepsilon_\nu.$$

Abychom určili agregát B, uvažme, že lze klásti lichá čísla λ do tvaru $\lambda = p - 2\mu$, načež

$$(-1)^{\frac{\lambda-1}{2}} \varepsilon_\lambda = (-1)^\mu \varepsilon_{2\mu},$$

a tedy

$$B = \sum_1^m (-1)^\mu \varepsilon_{2\mu} = A.$$

Dle známé věty Dirichletovy, vyjádřené v Kroneckerově úpravě theorie forem kvadratických, jest

$$\sum_{h=1}^{[1/4 D]} \left(\frac{D}{h}\right) = \tfrac{1}{2} Cl(-4D),$$

kde D jest lichý diskriminant základní a kladný.

Pro $D = p$ jest

$$\left(\frac{D}{h}\right) = \varepsilon_h,$$

a tedy

$$\sum_1^{\frac{p-1}{4}} \varepsilon_\nu = \tfrac{1}{2} Cl(-4p);$$

následkem toho jest

$$A = Cl(-4p) = H$$

počtem kladných tříd kvadratických forem záporného determinantu $-p$ (diskriminantu $-4p$); máme tedy

$$A = B = H,$$

$$Q(i) = (1+i)H, \quad Q(i)^2 = 2iH^2,$$

a rovnice (II) podává tedy

$$2iH^2 = i(p-1) + (1-i)\sum_1^{p-1} e_n i^n.$$

Zde násobme $1+i$ a porovnejme stejnorodé části obou stran; vyjde

$$H^2 = m - \sum_1^m (-1)^\nu e_{2\nu} = m + \sum_\lambda (-1)^{\frac{\lambda-1}{2}} e_\lambda, \tag{18}$$

$$(\lambda = 1, 3, 5, \ldots p-2)$$

($p = 2m+1$ kmenný modul tvaru $4a+1$).

Druhý tvar vychází z prvního pomocí vztahu (a), položí-li se $\lambda = p - 2\nu$.

Užije-li se vztahů (16[1]), zjednoduší se výsledky (18) jak následuje:

$$H^2 = m - 2\sum_1^{1/4(p-1)} e_{4\nu} = m + 2\sum_1^{1/4(p-1)} e_{4\nu-2},$$

$$H^2 = -2(e_3+e_7+e_{11}+\ldots+e_{p-2}) = p-1+2(e_1+e_5+e_9+\ldots+e_{p-4}).$$

Pro $p=13$ jest $H=2$, a rovnice tyto se verifikují hodnotami

$$4 = 6-2(e_4+e_8+e_{12}) = 6+2(e_2+e_6+e_{10}) = -2(e_3+e_7+e_{11}) = \\ = 12+2(e_5+e_9),$$

$$e_2=1,\quad e_3=-2,\quad e_4=3,\quad e_5=0,\quad e_6=-3,\quad e_7=2,\quad e_8=-1,$$
$$e_9=-4,\quad e_{10}=1,\quad e_{11}=-2,\quad e_{12}=-1.$$

V.

12. Vraťme se k modulům q a k rovnici

$$Q^2(x) = \frac{x^q-1}{x-1} + \frac{(x^q-1)^2}{x-1} - qx^q + (1-x^q)\sum_1^{q-1} e_n x^n.$$

Derivujme její obě strany a vložme do výsledku

$$x = \Theta_h = e^{\frac{2h\pi i}{q}},$$

kde celistvé číslo h má býti nesoudělno s q; vyjde tak dle známých vět o součtech Gaussových

$$(III)\qquad 2\varepsilon_h i\sqrt{q}\sum_{\nu=1}^{q-1}\nu\varepsilon_\nu\Theta_h^\nu = \frac{q}{\Theta_h-1} - q^2 - q\sum_{\nu=1}^{q-1} e_\nu\Theta_h^\nu.$$

V této rovnici násobme obě strany veličinou Θ_h^n, kde n jest jedno z čísel 1, 2, 3, … $q-1$, a výsledky sečtěme pro $h=1, 2, 3, \ldots q-1$

Obecně bude

$$\sum_{h=1}^{q-1}\Theta_h^{\nu+n} = -1,$$

a pouze pro $\nu = q-n$ nastane výjimka, kdy součet tento má hodnotu $q-1$. Tedy se při našem postupu objeví na pravé straně výraz

$$q\sum_h \frac{\Theta_h^n}{\Theta_h-1} + q^2 + q\sum_1^{q-1} e_\nu - q^2 e_{q-n},$$

čili se zřetelem k rovnici (*a*) čl. 8

$$(\alpha)\qquad q\sum_{h=1}^{q-1}\frac{\Theta_h^n}{\Theta_h-1} + q^2(1-e_{q-n}) + mq.$$

Abychom vyčíslili první agregát, užijeme elementárního vzorce

$$\frac{\Theta_h^n}{\Theta_h-1} = \frac{1}{\Theta_h-1} + \sum_{\nu=0}^{n-1}\Theta_h^\nu;$$

sečteme-li na obou stranách vůči h, obdržíme

$$\sum_h \frac{\Theta_h^n}{\Theta_h-1} = \sum_h \frac{1}{\Theta_h-1} + (q-n),$$

a z rovnice

$$\frac{1}{\Theta_h - 1} = \frac{1}{e^{\frac{2h\pi i}{q}} - 1} = \frac{1}{2i}\left(\operatorname{cotg}\frac{h\pi}{q} - i\right)$$

plyne

$$\Sigma \frac{1}{\Theta_h - 1} = -\tfrac{1}{2}(q-1) = -m$$

t. j.

$$\sum_{h=1}^{q-1} \frac{\Theta_h^n}{\Theta_h - 1} = q - m - n, \quad \left(m = \frac{q-1}{2}\right).$$

Dle toho výraz (α) má hodnotu

$$(\alpha') \qquad q(q-n) + q^2 e_n.$$

Na levé straně se pak při našem postupu objeví

$$2i\sqrt{q}\sum_{\nu=1}^{q-1}\nu\varepsilon_\nu \sum_{h=1}^{q-1}\varepsilon_h \Theta_h^{\nu+n} = -2q\sum_{1}^{q-1}\nu\varepsilon_\nu\varepsilon_{\nu+n};$$

porovnáme-li tento výraz s hodnotou pravé strany, t. j. (α'), vyjde vztah

$$(20) \qquad -\sum_{\nu=1}^{q-1}\nu\varepsilon_\nu\varepsilon_{n+\nu} = \frac{q-n}{2} + \frac{q}{2}e_n, \quad (o < n \leq q).$$

Výsledek ten zůstává v platnosti též pro $n = q$ následkem hodnoty

$$e_q = 1 - q.$$

Vraťme se nyní k rovnici (III); násobme $\varepsilon_h \Theta_h^n$ a sečtěme výsledky pro $h = 1, 2, \ldots q-1$; obdržíme nejprve

$$(\beta) \qquad 2i\sqrt{q}\sum_{\nu=1}^{q-1}\nu\varepsilon_\nu\sum_{h=1}^{q-1}\Theta_h^{n+\nu} = q\Sigma\frac{\varepsilon_h\Theta_h^n}{\Theta_h - 1} - q^2\varepsilon_n i\sqrt{q} - q\sum_{\nu=1}^{q-1}e_\nu\sum_{h=1}^{q-1}\varepsilon_h\Theta_h^{n+\nu}.$$

Sečteme-li na obou stranách identity

$$\frac{\varepsilon_h\Theta_h^n}{\Theta_h - 1} = \frac{\varepsilon_h}{\Theta_h - 1} + \sum_{\nu=0}^{n-1}\varepsilon_h\Theta_h^\nu$$

vůči h, obdržíme

$$(\gamma) \qquad \Sigma\frac{\varepsilon_h\Theta_h^n}{\Theta_h - 1} = \Sigma\frac{\varepsilon_h}{\Theta_h - 1} + i\sqrt{q}\sum_{1}^{n-1}\varepsilon_\nu.$$

Podle rovnice

$$\frac{1}{\Theta_h - 1} = \frac{1}{2i}\operatorname{cotg}\frac{h\pi}{q} - \tfrac{1}{2}$$

bude pak

$$\Sigma\frac{\varepsilon_h}{\Theta_h - 1} = -\frac{i}{2}\sum_{h=1}^{q-1}\varepsilon_h\operatorname{cotg}\frac{h\pi}{q};$$

poslední součet určí se podle známého vzorce*

$$\sum_{1}^{\Delta-1}\left(\frac{-\Delta}{\nu}\right)\operatorname{cotg}\frac{\nu\pi}{\Delta} = \frac{4\sqrt{\Delta}}{\tau}\,Cl(-\Delta)$$

---

* V. A. Lebesgue, Journal de math. pures et appl., t. 15 (1e série) 1850.

ve tvaru

$$\Sigma \frac{\varepsilon_h}{\Theta_h - 1} = - i \sqrt{q}\, Cl(-q), \quad (q > 3),$$

a znamenáme-li obecně

$$(21^0) \qquad s_r = \sum_1^r \varepsilon_\nu,$$

bude (γ) zníti

$$\Sigma \frac{\varepsilon_h \Theta_h^n}{\Theta_h - 1} = i \sqrt{q} [s_{n-1} - Cl(-q)].$$

Pravá strana rovnice (β) se dle toho dá psáti

$$iq \sqrt{q} \left\{ s_{n-1} - Cl(-q) - q \varepsilon_n - \sum_{\nu=1}^{q-1} \varepsilon_{n+\nu} e_\nu \right\},$$

a levá strana má hodnotu

$$2i \sqrt{q} \left\{ - \sum_1^{q-1} \nu \varepsilon_\nu + q(q-n) \varepsilon_{q-n} \right\} =$$

$$= 2iq \sqrt{q} \left\{ Cl(-q) - (q-n) \varepsilon_n \right\};$$

srovnáním hodnot obou stran vychází

$$(21) \qquad 3\, Cl(-q) + (2n - q) \varepsilon_n = s_{n-1} - \sum_{\nu=1}^{q-1} \varepsilon_{\nu+n} e_\nu,$$

při čemž $s_o = 0$.

Při této úvaze nebyla hodnota $n = q$ vyloučena; ponévadž $s_{q-1} = 0$, $\varepsilon_q = 0$, $\varepsilon_o = 0$, zůstává vzorec v platnosti též pro $n = 0$, značí-li tu $s_{-1} = 0$, t. j. platí

$$(21^1) \qquad 3\, Cl(-q) = - \sum_1^{q-1} \varepsilon_\nu e_\nu.$$

Rozštěpíme-li součet ve členy $\nu \leq m$ a $\nu = q - \mu > m$, máme vzhledem ke vztahu

$$e_{q-\mu} = 1 - e_\mu, \quad \varepsilon_{q-\mu} = - \varepsilon_\mu,$$

$$\sum_1^{q-1} \varepsilon_\nu e_\nu = 2 \sum_1^m \varepsilon_\mu e_\mu - \sum_1^m \varepsilon_\mu;$$

ježto dle známého vzorce

$$\sum_1^m \varepsilon_\mu = H = (2 - \varepsilon_2)\, Cl(-q),$$

přechází (21^1) ve tvar

$$(21^2) \qquad - \sum_1^m \varepsilon_\mu e_\mu = \frac{1 + \varepsilon_2}{2} Cl(-q).$$

Podle toho součet

$$\sum_1^m \varepsilon_\nu e_\nu$$

rovná se nulle pro moduly tvaru $q = 8k + 3$, kdežto pro moduly $q = 8k + 7$ je záporný, maje za absolutní hodnotu počet tříd diskriminantu $-q$, čili počet tříd nevlastně primitivních determinantu $-q$.

Uvažujme ještě zvláštní případ $n = m$ v rovnici (21). Tu jest

$$(q - 2n)\,\varepsilon_n + s_{n-1} = \sum_1^m \varepsilon_\nu = (2 - \varepsilon_2)\,Cl(-q)$$

a výsledek

$$-\sum_1^{q-1} \varepsilon_{m+\nu} e_\nu = (1 + \varepsilon_2)\,Cl(-q)$$

se pomocí identity

$$\varepsilon_2\,\varepsilon_{m+\nu} = \varepsilon_{2\nu-1}$$

upraví na

$$-\sum_1^{q-1} \varepsilon_{2\nu-1} e_\nu = (1 + \varepsilon_2)\,Cl(-q). \tag{22}$$

Poněvadž pro $\nu = q - \mu$ jest

$$\varepsilon_{2\nu-1} = -\varepsilon_{2\mu+1},$$

zní levá strana

$$-\sum_1^m \varepsilon_{2\nu-1} e_\nu + \sum_1^m \varepsilon_{2\mu+1}(1 - e_\mu) =$$

$$= -\sum_1^m (\varepsilon_{2\mu+1} + \varepsilon_{2\mu-1})\,e_\mu + \sum_1^m \varepsilon_{2\mu+1}.$$

Avšak

$$\varepsilon_1 + \sum_1^m \varepsilon_{2\mu+1} = \sum_1^{q-1} \varepsilon_\nu - \sum_1^m \varepsilon_{2\nu} = -\varepsilon_2 H,$$

tedy

$$\sum_1^m \varepsilon_{2\mu+1} = -1 - \varepsilon_2(2 - \varepsilon_2)\,Cl(-q)$$

a rovnice (22) podává

$$-\sum_1^m (\varepsilon_{2\mu-1} + \varepsilon_{2\mu+1})\,e_\mu = 1 + 3\varepsilon_2\,Cl(-q). \tag{22*}$$

Rovnici (21^2) lze na základě definice

$$e_\nu = \sum_{\alpha=1}^{\nu-1} \varepsilon_{\alpha\nu-\alpha^2}$$

psáti

$$\sum_{\alpha,\nu} \varepsilon_{\alpha\nu^2-\alpha^2\nu} = -\frac{1 + \varepsilon_2}{2}\,Cl(-q),\quad (\alpha < \nu = 2, 3, \ldots m).$$

Počet členů vlevo obnáší $\binom{m}{2}$, a tedy bude

$$\sum_{\alpha,\nu} \frac{1 + \varepsilon_{\alpha\nu^2-\alpha^2\nu}}{2} = \tfrac{1}{2}\left[\binom{m}{2} - \frac{1 + \varepsilon_2}{2}\,Cl(-q)\right].$$

Členové dvojnásobného součtu jsou rovny jedné neb nulle, a sice přichází mezi nimi tolikráte člen 1, kolik je mezi čísly $\alpha\nu^2 - \alpha^2\nu$ $(\alpha < \nu \leq m)$ kvadratických zbytků mod. q, čili jinak vyjádřeno, kolik dvojic α, ν $(\alpha < \nu \leq m)$ má tu vlastnost, že shoda o neznámé y

$$\alpha\nu^2 - \alpha^2\nu \equiv y^2 \pmod{q}$$

je řešitelna. Připustíme-li podmínku $o < y \leq m$, bude odpovídati každé

dvojici α, ν jen jedno řešení y, a zároveň můžeme na místě shody psáti rovnici

$$\alpha\nu^2 - \alpha^2\nu = y^2 + qu, \quad (0 < \alpha < \nu \leq m, \quad 0 < y \leq m),$$

v níž každé dvojici α, ν odpovídá zcela určité y a u.

Píšeme-li $\alpha = x$, $\nu = z$, nacházíme tak větu:

Je-li q kmenné číslo tvaru $4a + 3$, vyskytne se pro diofantickou rovnici

$$xz^2 - x^2z = y^2 + qu$$

$$N = \frac{m(m-1)}{4} - \frac{1+\varepsilon_2}{4} Cl(-q), \quad \left(m = \frac{q-1}{2}\right),$$

řešení hovících podmínkám

$$0 < x < z \leq m, \quad 0 < y \leq m.$$

Uvažuje-li se součet

$$\sum_{\alpha,\nu} \frac{1 - \varepsilon_{\alpha\nu^2 - \alpha^2\nu}}{2} = \frac{m(m-1)}{4} + \frac{1+\varepsilon_2}{4} Cl(-q),$$

a vzpomeneme-li fakta, že nezbytky lze mod. q klásti ve tvar $-y^2$, dojdeme týmž způsobem k výsledku:

Diofantická rovnice

$$xz^2 - x^2z + y^2 = qu$$

má

$$\frac{m(m-1)}{4} + \frac{1+\varepsilon_2}{4} Cl(-q)$$

řešení s podmínkami

$$0 < x < z \leq m, \quad 0 < y \leq m.$$

Stejným způsobem odvodíme na základě vztahu (21[1]) větu:

Diofantická rovnice

$$xz^2 - x^2z \pm y^2 = qu$$

má

$$\frac{(q-1)(q-2)}{4} \pm \tfrac{3}{2} Cl(-q)$$

řešení hovících podmínce

$$0 < x < z < q, \quad 0 < y \leq m.$$

13. Znamenejme nadále jako výše

$$s_k = \sum_1^k \varepsilon_\nu,$$

a uvažujme součet

$$A = \sum_{n=1}^{q-1} n\varepsilon_n s_{n-1},$$

v němž stále

$$\varepsilon_n = \left(\frac{n}{q}\right).$$

Odečteme-li od součtu s_{n-1} výraz

$$\sum_{1}^{q-1} \varepsilon_\nu = 0,$$

obdržíme

$$s_{n-1} = -\sum_{\nu=n}^{q-1} \varepsilon_\nu,$$

následkem čehož se výraz A přepíše na

$$A = -\sum_{\nu \geq n} n\varepsilon_n\varepsilon_\nu,$$

kdežto podržením původního tvaru s_{n-1} obdržíme

$$A = \sum_{\nu<n} n\varepsilon_n\varepsilon_\nu.$$

Sečtením obou tvarů veličiny A vychází

$$2A = \sum_{\nu=1}^{q-1}\sum_{n=1}^{q-1} n\varepsilon_n\varepsilon_\nu \text{ sgn. } (n-\nu-\tfrac{1}{2}),$$

a vyměníme-li se litery n a ν,

$$2A = -\sum_{\nu=1}^{q-1}\sum_{n=1}^{q-1} \nu\varepsilon_n\varepsilon_\nu \text{ sgn. } (n-\nu+\tfrac{1}{2}).$$

Symboly

$$\text{sgn. } (n-\nu-\tfrac{1}{2}) \text{ a sgn. } (n-\nu+\tfrac{1}{2})$$

se liší pouze v případě $n=\nu$, kdy první jest -1, druhý 1; sečteme-li tedy poslední dva výrazy, vznikne

$$4A = \sum_{\nu=1}^{q-1}\sum_{n=1}^{q-1} \varepsilon_n\varepsilon_\nu\,|\,n-\nu\,| - 2\sum_{\nu=1}^{q-1} n,$$

poněvadž pro $n \gtrless \nu$ jest

$$(n-\nu)\text{ sgn. }(n-\nu+\tfrac{1}{2}) = (n-\nu)\text{ sgn. }(n-\nu) = |\,n-\nu\,|,$$

a pro $n=\nu$ člen v novém výrazu vymizí; členy $n=\nu$ pak podají

$$n\varepsilon_n\varepsilon_\nu = \nu\varepsilon_n\varepsilon_\nu = n.$$

Máme tedy

$$4A = \sum_{1}^{q-1}\sum_{1}^{q-1} \varepsilon_n\varepsilon_\nu\,|\,n-\nu\,| - q(q-1);$$

výměnou ν za $q-\nu$ vznikne tvar souměrný

$$4A = -\sum_{1}^{q-1}\sum_{1}^{q-1} \varepsilon_\mu\varepsilon_\nu\,|\,\mu+\nu-q\,| - q(q-1)$$

Spojme ve skupiny veškery členy, v nichž $\mu+\nu=n$; v těch jest číslo

$$|\,n-q\,| = |\,\mu+\nu-q\,|$$

násobeno činitelem

$$\sum \varepsilon_\mu\varepsilon_\nu = e_n,\ (\mu+\nu=n;\ \mu<q,\ \nu<q),$$

takže bude

$$4A = -\sum_{n=1}^{2q-2} |\,n-q\,|\,e_n - q(q-1).$$

Oddělme členy $n \leq q$ od ostatních, a užijme vztahu

$$e_{q+n} = e_{q-n} = 1 - e_n,$$

tedy

$$4A = -\sum_1^q (q \quad n)\, e_n - \sum_{n-1}^{q-2} n(1 - e_n) - q(q-1);$$

v prvním součtu člen $n = q$ vymizí, dále můžeme přičísti vpravo k druhému součtu člen $n = q-1$
s hodnotou $(q-1)(1 - e_{q-1}) = 0$, a vyjde

$$4A = 2\sum_1^{q-1} n e_n - q\sum_1^{q-1} e_n - \sum_1^{q-1} n - q(q-1) =$$
$$= 2\sum_1^{q-1} n e_n - 2q(q-1).$$

Tím tedy nalezena identita

$$2\sum_1^{q-1} n\varepsilon_n s_{n-1} = -q(q-1) + \sum_1^{q-1} n e_n, \tag{23}$$

v níž nám hodnota pravé strany je známá ze vzorce (11) čl. 8.; její dosazením nabýváme vzorce

$$2\sum_1^{q-1} n\varepsilon_n s_{n-1} = -\frac{(q-1)(7q+1)}{12} - q\,Cl\,(-q)^2. \tag{23*}$$

14. Obraťme se nyní k rovnici (21)

$$3\,Cl\,(-q) + (2n-q)\,\varepsilon_n = s_{n-1} - \sum_{\nu=1}^{q-1} \varepsilon_{n+\nu} e_\nu;$$

násobme ji po obou stranách číslem $n\varepsilon_n$ a sečtěme výsledky pro $n = 1, 2, 3, \ldots q-1$; vzhledem k rovnici

$$\Sigma n\varepsilon_n = -q\,Cl\,(-q)$$

bude výsledek zníti

$$-3q\,Cl\,(-q)^2 + \sum_1^{q-1}(2n^2 - qn) = \sum_1^{q-1} n\varepsilon_n s_{n-1} - \sum_1^{q-1} e_\nu \sum_1^{q-1} n\varepsilon_n \varepsilon_{n+\nu}.$$

Podle rovnice (20) bude však

$$-\sum_{n-1}^{q-1} n\varepsilon_n \varepsilon_{n+\nu} = \frac{q-\nu+qe_\nu}{2},$$

a tak náš výsledek bude lze psáti při hořejším významu litery A

$$-6q\,Cl\,(-q)^2 + 2\sum_1^{q-1}(2n^2 - qn) = 2A + \sum_1^{q-1}(q-\nu)\,e_\nu + q\sum_1^{q-1} e^2{}_\nu. \tag{α}$$

Dle (23) je však

$$2A - \sum_1^{q-1} \nu e_\nu = -q(q-1),$$

a poněvadž

$$q\sum_1^{q-1} e_\nu = \frac{q(q-1)}{2},$$

zní pravá strana (α) jak následuje

$$-\frac{q(q-1)}{2} + q\sum_1^{q-1} e^2{}_\nu. \tag{α'}$$

Z elementární rovnice

$$\sum_1^{q-1} n^2 = \frac{q(q-1)(q-2)}{3} + \frac{q(q-1)}{2}$$

vychází

$$2\sum_1^{q-1}(2n^2 - qn) = \frac{4q(q-1)(q-2)}{3} + 2q(q-1) - q^2(q-1);$$

dosadíme-li tuto hodnotu a převedeme-li ještě elementárnou část pravé strany (α') na stranu levou, obdržíme po malé redukci

$$\sum_1^{q-1} e^2_\nu = \frac{(q-1)(2q-1)}{6} - 6\,Cl\,(-q)^2. \tag{24}$$

Na levé straně podržme členy $\nu \leq m$, ostatní lze psáti

$$\sum_1^m e^2_{q-\nu} = \sum_1^m (1 - e_\nu)^2 = \sum_1^m e^2_\nu - 2\sum_1^m e_\nu + m,$$

i obdržíme na místě (24) vztah

$$\sum_1^m (e^2_\nu - e_\nu) = \frac{(q-1)(q-2)}{6} - 3\,Cl\,(-q)^2. \tag{24*}$$

Jiný tvar vychází z rovnice (24), lišíme-li v ní přípony liché a sudé; tak obdrží levá strana tvar

$$\sum_1^m e^2_{2\nu} + \sum_1^m e^2_{q-2\nu} = 2\sum_1^m e^2_{2\nu} - 2\sum_1^m e_{2\nu} + m;$$

tak lze rovnici (24*) doplniti identitou

$$\sum_1^m (e^2_\nu - e_\nu) = \sum_1^m (e^2_{2\nu} - e_{2\nu}). \tag{24^0}$$

V rovnici tak vzniklé

$$\sum_1^m e^2_{2\nu} - \sum_1^m e_{2\nu} = \frac{(q-1)(q-2)}{6} - 3\,Cl\,(-q)^2$$

dosadme za druhý součet hodnotu

$$\sum_1^m e_{2\nu} = H^2, \tag{13}$$

a uvažme, že z rovnice

$$H = (2 - \varepsilon_2)\,Cl\,(-q)$$

plyne

$$H^2 - 3\,Cl\,(-q)^2 = -2\varepsilon_2(2 - \varepsilon_2)\,Cl\,(-q)^2;$$

tak vychází vztah

$$\sum_1^m e^2_{2\nu} = \frac{(q-1)(q-2)}{6} - 2\varepsilon_2(2 - \varepsilon_2)\,Cl\,(-q)^2. \tag{25}$$

V rovnici (11)

$$\sum_1^{q-1} n e_n = \frac{(q-1)(q-2)}{6} + \frac{q^2 - 1}{4} - q\,Cl\,(-q)^2$$

rozlučme členy s příponami sudými a lichými na levé straně, která tak

nabude tvaru

$$\sum_1^m 2\nu e_{2\nu} + \sum_1^m (q-2\nu)(1-e_{2\nu}) = \sum_1^m 4\nu e_{2\nu} - q\sum_1^m e_{2\nu} + m^2;$$

ve spojení s rovnicí (13) tedy odtud vychází

$$4\sum_1^m \nu e_{2\nu} + m^2 - qH^2 = \frac{(q-1)(q-2)}{6} + \frac{q^2-1}{4} - q\,Cl(-q)^2.$$

Poněvadž

$$H^2 - Cl(-q)^2 = 4(1-\varepsilon_2)\,Cl(-q)^2,$$

zní náš výsledek

$$\sum_1^m \nu e_{2\nu} = \frac{q^2-1}{24} + (1-\varepsilon_2)\,q\,Cl(-q)^2. \tag{26}$$

15. Nalezené výsledky dávají podnět k následujícím applikacím. Dle definice čísel e_n jest

$$e_{2\nu} = \sum_{\alpha=1}^{2\nu-1} \varepsilon_{2\nu\alpha-\alpha^2} = \sum_{\alpha=1}^{2\nu-1} \varepsilon_{\nu^2-(\nu-\alpha)^2}$$

a odtud vychází, že

$$e_{2\nu} + (2\nu-1) = 2n_\nu = 2\sum_{\alpha=1}^{2\nu-1} \frac{1+\varepsilon_{\nu^2-(\nu-\alpha)^2}}{2}, \tag{a}$$

kde n_ν značí počet řešení shody o neznámých α, y

$$\nu^2 - (\nu-\alpha)^2 \equiv y^2 \pmod q$$

s omezením $0 < \alpha < 2\nu$, $0 < y \leq m$.

Klademe-li $\nu - \alpha = x$, vychází, že

n_ν jest počet řešení shody

$$x^2 + y^2 \equiv \nu^2 \pmod q$$

s omezením $-\nu < x < \nu$, $0 < y \leq m$.

Z rovnic (*a*) a (13) vychází

$$2\sum_1^m n_\nu = H^2 + m^2,$$

a tím věta:

Řešení pythagorejské shody

$$x^2 + y^2 \equiv z^2 \pmod q$$

podrobená podmínkám

$$0 < y \leq m, \quad 0 < z \leq m, \quad -z < x < z$$

jsou v počtu $\frac{1}{2}(H^2 + m^2)$.

Řešení nezajímavá, v nichž $x = 0$, jsou v počtu m, ostatní se po dvou liší pouze znamením neznámé x. Tedy

Počet řešení pythagorejské shody

$$x^2 + y^2 \equiv z^2 \pmod q$$

s omezením

$$0 < y \leq m, \quad 0 < x < z \leq m, \quad \left(m = \frac{q-1}{2}\right),$$

(*α*) *obnáší*

$$\frac{H^2 + m^2 - 2m}{4}.$$

Stejně nalezneme, že

$$(2\nu - 1) - e_{q,\nu} = 2n'_\nu,$$

kde n'_ν *značí počet řešení shody*

$$x^2 - y^2 \equiv \nu^2, \quad 0 < y \leq m, \ |x| < \nu.$$

Z rovnice

$$2\sum_1^m n'_\nu = m^2 - H^2$$

pak plyne, že

počet řešení shody

$$x^2 \equiv y^2 + z^2$$

s omezením

$$0 < y \leq m, \quad 0 < z \leq m, \quad -z < x < z$$

obnáší

$$\frac{m^2 - H^2}{2}.$$

Jelikož pro moduly q shoda $y^2 \equiv -z^2$ není možna, není v těchto řešeních nikdy $x = 0$ a tedy vychází věta:

Pythagorejská shoda

$$x^2 \equiv y^2 + z^2$$

(β) *s omezením* $0 < y \leq m, \quad 0 < z \leq m, \quad 0 < x < z$ *má*

$$\frac{m^2 - H^2}{4}$$

řešení.

Nazveme řešením základním shody

$$(P) \qquad x^2 + y^2 \equiv z^2 \pmod{q}$$

každé řešení složené z čísel první polovice intervallu, t. j.

$$x, \ y, \ z = 1, 2, 3, \ldots m.$$

Řešení, v nichž $x < z$, jsou šetřena větou (α), kdežto věta (β) (po výměně liter x a z) vztahuje se k řešením $x > z$:

Základní řešení pythagorejské shody (P) jsou v počtu $\frac{m(m-1)}{2}$;

a sice jest pro $\frac{m^2 - H^2}{4}$ *řešení* $x > z$, *a pro* $\frac{m^2 - 2m + H^2}{4}$ *řešení* $x < z$.

Vyhledejme nyní všecka řešení

$$a^2 + b^2 \equiv z^2, \quad a < b,$$

předpokládajíce nejprve $\varepsilon_2 = -1$, kdy řešení $a = b$ není možné. Pak budiž

A počet případů $a < z, \ b < z$

B „ „ $a < z < b$

C „ „ $z < a < b,$

načež theorém podává

$$2A + B = \frac{m^2 - 2m + H^2}{4}$$

$$2C + B = \frac{m^2 - H^2}{4};$$

odtud

$$C - A = \frac{m - H^2}{4}.$$

Poněvadž ze supposice $\varepsilon_2 = -1$ plyne $q = 8k + 3$, $m = 4k + 1$, je toto číslo skutečně celistvé.

Je-li $\varepsilon_2 = +1$, nastanou ještě případy

$$a = b < z \text{ v počtu } A_0,$$
$$a = b > z \text{ „ „ } C_0.$$

Buď

$$2 \equiv d^2 \pmod{q},$$

pak případy $a = b$ plynou ze shody

$$2a^2 \equiv a^2 d^2 \equiv z^2, \quad ad \equiv \pm z,$$

a tato shoda podává pro každé z jen jedno řešení $a \leq m$. Naopak odpovídá zvolenému a jen jedno $z \leq m$. Tedy

$$A_0 \text{ jest počet případů, kdy } \left| R\left(\frac{ad}{q}\right) \right| > \frac{a}{q}$$
$$C_0 \text{ jest počet případů, kdy } \left| R\left(\frac{ad}{q}\right) \right| < \frac{a}{q},$$

při čemž

$$d^2 \equiv 2 \pmod{q}, \quad o < d \leq m.$$

Patrně $A_0 + C_0 = m$.

Z rovnic

$$2A + A_0 + B = \frac{m^2 - 2m + H^2}{4},$$
$$2C + C_0 + B = \frac{m^2 - H^2}{4},$$
$$A_0 - C_0 = 2A_0 - m$$

plyne pak

$$A + A_0 - C = \frac{H^2 + m}{4}.$$

Odtud věty:

I. Pro kmenné moduly $q = 8k + 3$ je mezi základními řešeními pythagorejské shody (P) případů $z < x < y$ o $\frac{m - H^2}{4}$ více než případů $x < y < z$.

Číslo to ovšem může býti záporné, jako na př. pro $q = 11$, aneb nulla ($q = 19$).

II. Pro kmenné moduly $q = 8k + 7$ mají mezi základními řešeními pythagorejské shody (P) případy $x \leq y < z$ převahu nad případy $z < x < y$, a sice o

$$\frac{H^2 + m}{4}.$$

Příklady. 1. $q = 7$; veškera řešení základní jsou

x	y	z
1	1	3
2	2	1
3	3	2;

z těch jedno hoví podmínce první $x \leq y < z$, a žádné podmínce druhé $z < x < y$; a skutečně zde

$$\frac{H^2 + m}{4} = 1.$$

2. $q = 11$. Základní řešení jsou tu

x	y	z
1	2	4
1	5	2
2	4	3
3	4	5
3	5	1.

Z těch dvě mají vlastnost $x < y < z$, a jedno hoví nerovnostem $z < x < y$. Skutečně

$$\frac{H^2 - m}{4} = \frac{3^2 - 5}{4} = 1.$$

16. Z definice (*a*) čl. 15

$$2n_\nu = c_{2\nu} + (2\nu - 1)$$

plyne

$$2\sum_1^m \nu n_\nu = \sum_1^m \nu c_{2\nu} + \sum_1^m \nu (2\nu - 1);$$

tu jest

$$\sum_1^m \nu (2\nu - 1) = m + 5\binom{m}{2} + 4\binom{m}{3},$$

dále dle (26)

$$\sum_1^m \nu c_{2\nu} = \frac{q^2 - 1}{24} + (1 - \varepsilon_2)\, q\, Cl\,(-q)^2.$$

Dosazením těchto hodnot obdržíme po malé redukci

$$\sum_1^m \nu n_\nu = \frac{(q-1)(q^2-1)}{24} + \frac{1 - \varepsilon_2}{2} q\, Cl\,(-q)^2. \tag{27}$$

Avšak n_ν značí počet řešení shody

$$x^2 + y^2 \equiv \nu^2 \pmod{q}$$

s omezením $o < y \leq m$, $-\nu < x < \nu$.

Levá strana (27) tedy udává součet všech hodnot z, jež se vyskytnou v různých řešeních pythagorejské shody

$$x^2 + y^2 \equiv z^2 \pmod{q} \tag{P}$$

s omezením neznámých $o < y \leq m$, $o < z \leq m$, $x^2 < z_2$.

Dále máme pro čísla n'_ν čl. 15.

$$2\sum_1^m \nu n'_\nu = \sum_1^m \nu(2\nu - 1) - \sum_1^m \nu e_{2\nu} = 2\sum_1^m \nu n_\nu - 2\sum_1^m \nu e_{2\nu}$$

a tedy dle (27) a (26)

$$\sum_1^m \nu n'_\nu = \frac{(q-1)(q^2-1)}{24} - \frac{q^2-1}{24} - \frac{1-\varepsilon_2}{2} q\, Cl(-q)^2,$$

t. j.

$$\sum_1^m \nu n'_\nu = \frac{(q-2)(q^2-1)}{24} - \frac{1-\varepsilon_2}{2} q\, Cl(-q)^2. \tag{28}$$

Levá strana udává součet hodnot z, jež se vyskytnou v různých řešeních shody

$$x^2 - y^2 \equiv z^2 \pmod{q}$$

s omezením $o < y \leq m$, $o < z \leq m$, $x^2 < z^2$.

Řešení $x = o$ je tu nemožné a řešení se kupí v dvojice, v nichž x se liší jen znamením.

Omezíme-li se na řešení kladná a vyměníme-li litery x a z, obdržíme větu:

Součet hodnot x, jež se vyskytují mezi různými základními řešeními shody (P) hovícími podmínce $x > z$, obnáší

$$\Sigma x = \frac{(q-2)(q^2-1)}{48} - \frac{1-\varepsilon_2}{4} q\, Cl(-q)^2.$$

Dále máme pro $x = 0$ řešení $y = z_0$ v počtu m; vynecháme-li je, vyskytují se ostatní podvojně s hodnotami $\pm x$, a můžeme je převésti na řešení základní; dle (27) tedy, ježto

$$\Sigma z_0 = \frac{m(m+1)}{2} = \frac{q^2-1}{8},$$

vychází věta:

Pro základní řešení shody (P) hovící podmínce $z > x$ obnáší součet hodnot z

$$\Sigma z = \frac{(q^2-1)(q-4)}{48} + \frac{1-\varepsilon_2}{4} q\, Cl(-q)^2.$$

Pro $q = 7$ máme

$$\Sigma z = 3, \quad \Sigma x = 2 + 3 = 5,$$

v úplné shodě s theorémy.

Pro $q = 11$ (dlužno bráti řešení podvojně (x, y), (y, x)) máme

$$\Sigma x = 5 + 4 + 3 + 5 = 17,$$

$$\frac{9 \cdot 10 \cdot 12}{48} - \tfrac{2}{4} 11 \cdot 1^2 = 17;$$

dále

$$\Sigma z = 4 + 4 + 2 + 3 + 5 + 5 = 23,$$

$$\frac{10 \cdot 12 \cdot 7}{48} + \tfrac{1}{2} 11 \cdot 1^2 = 23.$$

ÉTUDES SUR LA THÉORIE DES RÉSIDUS QUADRATIQUES SUIVANT UN MODULE PREMIER.

RELATIONS NOUVELLES AVEC LA THÉORIE DES FORMES QUADRATIQUES AYANT UN DÉTERMINANT NÉGATIF ET PREMIER.

(RÉSUMÉ *.)

I.

1. Le polynôme (1), où ε_ν est le symbole de Legendre:

$$\varepsilon_\nu = \left(\frac{\nu}{q}\right);\ \nu = 1, 2, \ldots q-1;\ \varepsilon_0 = \varepsilon_q = 1,$$

et q un nombre premier de la forme $4a+3$, satisfait à la congruence algébrique

$$Q^2(x) + q \equiv 0 \left(\mathrm{mod}\ \frac{x^q-1}{x-1}\right);$$

on peut écrire le premier membre de cette congruence sous la forme (α) (p. 8), les nombres e_n étant définis au moyen des équations (2). On en déduit aisément les relations (4) et la formule (I).

2. La première des formules (4^4) donne immédiatement le théorème: *q étant un module premier de la forme $4a+3$ la suite complète de symboles de Legendre (L) $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{q-1}$ offre $\frac{1}{2}(q-3)$ permanences et $\frac{1}{2}(q-1)$ variations.*

L'expression

$$\sum_1^{q-2} \frac{(1+\varepsilon_\nu)\ (1+\varepsilon_{\nu+1})}{4}$$

(voir p. 10) est égale au nombre des cas où il y a, dans la suite (L), deux signes consécutifs positifs; le calcul de cette expression (au moyen des formules 4) donne le théorème suivant: *Il y a dans la suite 1, 2, 3, $\ldots q-1$ [q étant un nombre premier, $q \equiv 3$ (mod. 4)], $\frac{1}{4}(q-3)$ résidus quadratiques suivis par un résidu et autant de non-résidus suivis par un non-résidu.*

On démontre d'une manière analogue en calculant les sommes (voir p. 10)

$$\sum_1^{q-2} \frac{1-\varepsilon_\nu}{2} \cdot \frac{1+\varepsilon_{\nu+1}}{2},\quad \sum_1^{q-2} \frac{1+\varepsilon_\nu}{2} \cdot \frac{1-\varepsilon_{\nu+1}}{2}:$$

La suite 1, 2, $\ldots q-1$, contient $\frac{1}{4}(q+1)$ résidus quadratiques suivis par un non-résidu et $\frac{1}{4}(q-3)$ non-résidus suivis par un résidu quadratique.

---

* Le manuscrit de M. Lerch ne contenait pas de résumé; le résumé qu'on va lire a été rédigé par M. Borůvka et par le rédacteur. (Note du rédacteur.)

3. Voici les théorèmes analogues pour la demi-suite de symboles de Legendre

(M) $$\varepsilon_1, \varepsilon_2, \ldots \varepsilon_m$$

$$m = \frac{q-1}{2}, \quad q \equiv 3 \pmod 4.$$

Le nombre des variations contenues dans la demi-suite de symboles de Legendre de (M), suivant un module premier de la forme $4a+3$, est égal au nombre des permanences.

La suite $1, 2, \ldots \frac{1}{2}(q-1)$ contient $\frac{1}{8}(q-3)+\frac{1}{4}(1+\varepsilon_2)$ résidus quadratiques mod q suivis par un non-résidu et $\frac{1}{8}(q-3)-\frac{1}{2}(1+\varepsilon_2)$ non-résidus suivis par un résidu.

On démontre, en calculant les sommes

$$\sum_1^{m-1} \frac{1+\varepsilon_\mu}{2} \cdot \frac{1+\varepsilon_{\mu+1}}{2}, \quad \sum_1^{m-1} \frac{1-\varepsilon_\mu}{2} \cdot \frac{1-\varepsilon_{\mu+1}}{2}$$

(voir p. 13) le théorème suivant: *La suite $1, 2, 3, \ldots \frac{q-1}{2}$, relative à un module premier de la forme $q = 4a+3$, contient $\frac{1}{8}(q-3)+$ $+\frac{1}{2}\left(H-\frac{1-\varepsilon_2}{2}\right)$ paires de résidus quadratiques consécutifs et $\frac{1}{8}(q-3)-$ $-\frac{1}{2}\left(H-\frac{1-\varepsilon_2}{2}\right)$ paires de non-résidus consécutifs.* Ici H désigne le nombre des classes de formes quadratiques de Gauss $a_1x^2+2bx_1y_1+c_1y^2$ ayant le déterminant $-q = b_1^2 - a_1c_1$.

4. La seconde des équations (4^4) donne le théorème: *Il y a, dans la suite (L), autant de termes qui séparent deux signes égaux, combien il y en a qui séparent deux signes contraires.*

En calculant la somme

$$\sum_1^{q-3} \frac{1+\varepsilon_\mu}{2} \cdot \frac{1+\varepsilon_{\mu+2}}{2}$$

on démontre *la propriété suivante de la suite $1, 2, \ldots q-1$: Il y a $\frac{1}{4}(q-3)$ termes dont les deux voisins sont des résidus et $\frac{1}{4}(q-3)$ termes dont les deux voisins sont des non-résidus.*

De même, en employant la seconde équation (4^4) et la formule (6) on trouve que *la suite $\varepsilon_3, \varepsilon_5, \ldots \varepsilon_{m-2}$ contient autant de variations qu'il y a de permanences dans la suite $\varepsilon_3, \varepsilon_4, \ldots \varepsilon_{m-3}$.*

On démontre de la même manière, en calculant les sommes

$$\sum_1^{m-2} \frac{1+\varepsilon_\mu}{2} \cdot \frac{1+\varepsilon_{\mu+2}}{2}, \quad \sum_1^{m-2} \frac{1-\varepsilon_\mu}{2} \frac{1+\varepsilon_{\mu+2}}{2}$$

(voir p. 15) que *la suite $1, 2, 3, \ldots m$ (où $m = \frac{q-1}{2}$ et q est un nombre premier de la forme $4a+3$) contient $\frac{m-3}{4} + \frac{1+\varepsilon_2}{4}\varepsilon_3 + \frac{1}{2}H$ termes*

dont les deux voisins sont des résidus suivant le module q et $\frac{m-1}{4} + \frac{1-\varepsilon_2}{4}\varepsilon_3 - \frac{1}{2}H$ *termes dont les deux voisins sont des non-résidus.*

La suite 1, 2, ... m (où $m = \frac{q-1}{2}$ et q est un nombre premier de la forme $4a+3$) *contient*

$$\frac{m-2-\varepsilon_2}{4} - \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4} = \left[\frac{q}{8}\right] - \frac{(1+\varepsilon_2)(1+\varepsilon_3)}{4}$$

termes précédés par un non résidu et suivis par un résidu quadratique; la même suite contient

$$\left[\frac{q}{8}\right] + \varepsilon_2 + \frac{(1-\varepsilon_2)(1-\varepsilon_3)}{4}$$

termes précédés par un résidu quadratique et suivis par un non-résidu.

5. Substituons maintenant, dans la somme

$$A = \sum_1^{q-1} \varepsilon_\nu \varepsilon_{\nu-1}\varepsilon_\nu$$

la quantité $q-\mu$ à la place de ν; il vient $\nu^2 - 1 \equiv \mu^2 - 1$, d'où $A = 0$. Ce résultat, combiné avec les équations (4^4), nous permet de calculer les sommes

$$\sum_1^{q-3} \frac{1+\varepsilon_\nu}{2} \cdot \frac{1+\varepsilon_{\nu+1}}{2} \cdot \frac{1+\varepsilon_{\nu+2}}{2};$$

on démontre ainsi le théorème: *La suite complète de symboles de Legendre* $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{q-1}$, *pour un module premier q de la forme $4a+3$, contient*

$$\frac{q-3-2(1+\varepsilon_2)}{8}$$

termes du chacun des types $+++$, $-++$, $---$, $--+$ *et*

$$\frac{q-3+2(1+\varepsilon_2)}{8}$$

termes du chacun des types $+-+$, $-+-$, $++-$, $+--$.

II.

6. On obtient des résultats analogues pour un module premier p de la forme $4a+1$.

Le nombre des variations contenues dans la suite complète (L') de symboles de Legendre $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{p-1}$ *est plus grand d'une unité que le nombre des permanences qui y sont contenues. Même théorème pour la demi suite*

$$(M') \qquad \varepsilon_1, \varepsilon_2, \ldots \varepsilon_m \left(m = \frac{p-1}{2}\right).$$

La demi-suite (M') de symboles de Legendre pour un module p

contient $\left[\frac{p-2}{8}\right]$ *paires de termes consécutifs positifs et* $\left[\frac{p}{8}\right]$ *paires de termes consécutifs négatifs.*

Il y a, dans la suite (M'), *pour un module premier quelconque,* $\left[\frac{p}{8}\right]$ *groupes* $(-+)$ *et* $\left[\frac{p+3}{8}\right]$ *groupes* $(+-)$.

7. Appelons $+\pm-$, $-\pm+$ ternes à une variation; $+\pm+$, $-\pm-$ ternes à deux variations ou ternes sans variation. On a, pour les modules p: *Il y a, parmi les ternes à une variation de la suite* (M')

$$\left[\frac{p-2}{8}\right]+\frac{(1+\varepsilon_2)\,(1+\varepsilon_3)}{4}$$

ternes qui appartiennent à l'un ou à l'autre des types $-++$ *et* $--+$

$$\left[\frac{p+3}{8}\right]-\frac{(1-\varepsilon_2)\,(1-\varepsilon_3)}{4}$$

ternes qui appartiennent à l'un ou à l'autre des types $++-$, $+--$,

$$\left[\frac{p-2}{8}\right]-\frac{(1+\varepsilon_2)\,(1+\varepsilon_3)}{2}$$

ternes aux extrémités positives et

$$\left[\frac{p-2}{8}\right]+\varepsilon_2+\frac{(1-\varepsilon_2)\,(1-\varepsilon_3)}{4}$$

ternes aux extrémités négatives.

III.

8. Substituons $x=-1$ dans la formule (I), q étant un module de la forme $4a+3$. On obtient la formule (*10**) qui donne le nombre H de classes des formes primitives ayant le déterminant $-q$. Différentions l'équation (I) et substituons y $x=1$. On trouve la formule (11*) qui donne le nombre $Cl(-q)$ des classes de formes positives ayant le discriminant $-q=b^2-4ac$.

9. On obtient une autre formule (12) pour H en substituant dans la formule (I), $i=\sqrt{-1}$ à la place de x: En combinant les équations (10) et (12) on trouve les formules (A).

IV.

10. Un module premier p de la forme $4a+1$ donne lieu à des résultats plus simples. L'équation (II) conduit aux équations (16), (16*), (16^1), (17) et (17*).

11. En posant $Q(i)=A+iB$, on trouve $A=B=H$ où $H=Cl(-4p)$ désigne le nombre des classes de formes quadratiques ayant un déterminant négatif $-p$.

V.

12. Différentions l'équation (I) et substituons y $x = \Theta_n = e^{\frac{2h\pi i}{q}}$ (h et q étant des entiers sans diviseur commun); on obtient la formule III, et les équations (20), (21), (22), (22*). L'équation (21²) donne: *q étant un nombre premier de la forme $4a+3$, il y a*

$$N = \frac{m(m-1)}{4} - \frac{1+\varepsilon_2}{4} Cl(-q), \quad \left(m = \frac{q-1}{2}\right)$$

solutions de l'équation indéterminée

$$xz^2 - x^2 z = y^2 + qu$$

qui satisfont aux conditions

$$0 < x < z \leq m, \quad 0 < y \leq m.$$

Il y a

$$\frac{m(m-1)}{4} + \frac{1+\varepsilon_2}{4} Cl(-q)$$

solutions de l'équation indéterminée

$$xz^2 - x^2 z + y^2 = qu$$

qui satisfont aux mêmes conditions.

La formule (21¹) donne: *Il y a*

$$\frac{(q-1)(q-2)}{4} \pm \tfrac{3}{2} Cl(-q)$$

solutions de l'équation indéterminée

$$xz^2 - x^2 z \pm y^2 = qu$$

qui satisfont aux conditions

$$0 < x < z < q, \quad 0 < y \leq m.$$

13. Posons

$$A = \sum_{n=1}^{q-1} n s_{n-1} \varepsilon_n, \quad s_k = \sum_1^k \varepsilon_\nu;$$

on déduit l'identité (23) et la formule (23*).

14. L'équation (21) conduit (voir les équations 20, α, 23, 24) à l'identité (24⁰) et aux équations (25) et (26).

15. Applications. L'équation (α) conduit immédiatement au résultat suivant: *Il y a n_ν solutions de la congruence*

$$x^2 + y^2 \equiv \nu^2 \pmod{q}$$

qui satisfont aux conditions

$$-\nu < x < \nu, \quad 0 < y \leq m.$$

Il résulte des équations (α) et (13) que

$$\sum_1^m n_\nu = \frac{H^2 + m^2}{2},$$

donc: *Il y a* $\frac{1}{2}(H^2+m^2)$ *solutions de la congruence*

$$x^2+y^2\equiv z^2 \pmod q$$

qui satisfont aux conditions

$$0<y\leq m,\quad 0<x<z\leq m,\quad \left(m=\frac{q-1}{2}\right).$$

L'expression

$$\frac{2\nu-1-e_{2\nu}}{2}=n'_\nu$$

est égale au nombre de solutions de la congruence $x^2-y^2\equiv\nu^2$, $0<y\leq m$, $|x|<\nu$; remarquons encore que

$$\sum_1^m n'_\nu=\tfrac{1}{2}(m^2-H^2).$$

On a les théorèmes suivants: *Il y a* $\frac{1}{2}(m^2-H^2)$ *solutions de la congruence* $x^2\equiv y^2+z^2$ *qui satisfont aux conditions* $0<y\leq m$, $0<z\leq m$, $-z<x<z$.

Il y a $\frac{1}{4}(m^2-H^2)$ *solutions de la congruence* $x^2\equiv y^2+z^2$ *qui satisfont aux conditions* $0<y\leq m$, $0<z\leq m$, $0<x<z$.

Appelons „solutions fondamentales“ de la congruence

$$x^2+y^2\equiv z^2 \pmod q \quad (P)$$

toute solution composé des nombres $x, y, z=1, 2, \ldots m$.

Il y a $\frac{1}{2}m(m-1)$ *solutions fondamentales de la congruence* (P); $\frac{1}{4}(m^2-H^2)$ *solutions avec* $x>z$, *et* $\frac{1}{4}(m^2-2m+H^2)$ *solutions avec* $x<z$.

q *étant un nombre premier de la forme* $8k+3$, *le nombre des solutions fondamentales de la congruence* (P) *qui satisfont aux conditions* $z<x<y$ *surpasse de* $\frac{1}{4}(m-H^2)$ *unités celui des solutions fondamentales qui satisfont aux conditions* $x<y<z$.

q *étant un module premier de la forme* $8k+7$, *le nombre des solutions fondamentales de la congruence* (P) *qui satisfont aux conditions* $x\leq y<z$ *surpasse de* $\frac{1}{4}(H^2+m)$ *unités celui des solutions fondamentales qui satisfont aux conditions* $z<x<y$.

16. Enfin, les équations (27) et (28) qui résultent de la relation (a) nous donnent les théorèmes suivants:

La somme des valeurs de x *qui figurent dans les solutions fondamentales de la congruence* (P) *avec la condition* $x>z$ *est égale à*

$$\Sigma x=\frac{(q-2)(q^2-1)}{48}-\frac{1-\varepsilon_2}{4}q\,Cl(-q)^2$$

La somme des valeurs de z *qui figurent dans les solutions fondamentales de la congruence* (P) *avec la condition* $z>x$ *est égal à*

$$\Sigma z=\frac{(q^2-1)(q-4)}{48}+\frac{1-\varepsilon_2}{4}q\,Cl(-q)^2.$$