Časopis pro pěstování mathematiky a fysiky

Matyáš Lerch

O součtech Gaussových

Časopis pro pěstování mathematiky a fysiky, Vol. 28 (1899), No. 1, 1--24

Persistent URL: http://dml.cz/dmlcz/122506

O součtech Gaussových.

Referuje **M. Lerch**,
professor university ve Freiburku ve Švýcarech.

Stanovení součtů

$$\sum_{a=0}^{n-1} e^{\frac{2ha^2\pi i}{n}}$$

pochází od Gausse*), který byl k nim veden svými úvahami o rovnicích kruhodílných. Později podali pro výsledky Gaussovy nové důkazy Dirichtet**), Cauchy***) a Lebesgue (na témž místě), v posledních letech svého života věnoval jim Kronecker několik duchaplných rozprav.

Z knih o tomto předmětě jednajících některé podávají výsledky neúplné (Dedekind, Dirichletovy přednášky o theorii čísel, první dodatek), některé nepřehledné (na př. J. de Seguier, Formes quadratiques et multiplication complexe). Tyto okolnosti mne pohnuly uveřejniti následující úvahy provedené původně toliko jakožto příprava k mým přednáškám na universitě Freiburské. Ony těsně přiléhají k článku Kroneckerovu „Ueber den vierten Gauss'schen Beweis des Reciprotitätsgesetzes für die quadratischen Reste“ †), a kde se odchylují, stalo se k vůli přesnosti neb podrobnému objasnění.

*) Disquisitiones, článek 356; německého překladu Maserova str. 426. Dále Summatio quarumdam serierum singularium (Maserova překladu str. 463.)

**) Crelleův žurnál sv. 17. (Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies) a sv. 19. (Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres).

***) Liouvilleův žurnál sv. V. (1840).

†) Monatsbericht berlínské Akademie z r. 1880.

1. Pomocný vzorec z theorie funkcí elliptických. Budiž a veličina buď realná a kladná, aneb komplexní s kladnou částí realnou; pak konverguje řada

$$f(u) = \sum_{n=-\infty}^{\infty} e^{-\frac{\pi}{a}(u+n)^2},$$

nechť jest u jakákoli veličina. Tato funkce jest stále konečná a má periodu 1, poněvadž se obdrží tvar $f(u+1)$, píše-li se $n+1$ za n, čímž se pouze členové řady „pošinou".

Z té příčiny bude lze — a to na základě rozmanitých vět analytických, z nichž nejjednodušší snad je věta Laurentova — rozvinouti tuto funkci v řadu trigonometrickou

$$f(u) = \sum_{m=-\infty}^{\infty} A_m e^{2mu\pi i}.$$

Součinitel A_m má hodnotu

$$A_m = \int_0^1 f(u)\, e^{-2mu\pi i}\, du$$

a dosadíme-li sem za $f(u)$ hodnotu (1), obdrží se

$$A_m = \sum_{n=-\infty}^{\infty} \int_0^1 e^{-\frac{\pi}{a}(u+n)^2 - 2mu\pi i}\, du.$$

V posledním integrálu proveďme substituci $u + n = x$, čímž tento obdrží tvar

$$\int_n^{n+1} e^{-\frac{\pi}{a}x^2 - 2mx\pi i}\, dx,$$

a řada pro A_m nalezená přejde tedy v integrál

$$A_m = \int_{-\infty}^{\infty} e^{-\frac{\pi}{a}x^2 - 2mx\pi i}\, dx.$$

Výraz tento lze několika způsoby stanoviti v zakončeném tvaru, jichž volba závisí na přípravě čtenářově; pro čtenáře se základy Cauchyovy theorie funkcí seznámené bude nejjednodušším odvození následující. Udělíme-li exponentu

$$-\frac{\pi}{a}x^2 - 2mx\pi i$$

tvar

$$-\pi\left(\frac{x}{\sqrt{a}} + mi\sqrt{a}\right)^2 \quad am^2\pi,$$

obdržíme

$$A_m = e^{-am^2\pi}\int_{-\infty}^{\infty} e^{-\pi\left(\frac{x}{\sqrt{a}}+mi\sqrt{a}\right)^2} dx.$$

Zde nechť nám $\sqrt{a}$ znamená onu z obou hodnot druhé odmocniny, jejíž realná část je kladná. Zavedeme-li nyní integrační proměnnou

$$z = \frac{x}{\sqrt{a}} + mi\sqrt{a},$$

obdržíme výraz

$$A_m = e^{-am^2\pi}\sqrt{a}\int e^{-\pi z^2} dz,$$

kde však integrace neděje se více podél osy realné, nýbrž podél přímky vedené bodem $z = mi\sqrt{a}$ v komplexní rovině rovnoběžně s vektorem $\frac{1}{\sqrt{a}}$ a sice od $-\infty$ do $+\infty$. Z Cauchyovy věty základní však soudíme, že se obdrží táž hodnota integrálu, přeložíme-li cestu integrační do osy realné, takže bude

$$A_m = e^{-am^2\pi}\sqrt{a}\int_{-\infty}^{\infty} e^{-\pi z^2} dz$$

čili

$$A_m = c\sqrt{a}\, e^{-am^2\pi},$$

znamená-li nám c čistě numerickou konstantu

$$c = \int_{-\infty}^{\infty} e^{-\pi z^2} dz.$$

Hledaná řada bude tedy zníti

$$\sum_{n=-\infty}^{\infty} e^{-\frac{\pi}{a}(u+n)^2} = c\sqrt{a} \sum_{m=-\infty}^{\infty} e^{-am^2\pi+2mu\pi i};$$

abychom určili c, klaďme $u = 0$, $a = 1$; i vyjde

$$\sum e^{-n^2\pi} = c \sum e^{-m^2\pi}$$

a poněvadž řada tu se vyskytující není nullou, máme $c = 1$, takže platí vzorec základní

$$(1) \qquad \sum_{\nu=-\infty}^{\infty} e^{-\frac{\pi}{a}(u+\nu)^2} = \sqrt{a} \sum_{\nu=-\infty}^{\infty} e^{-a\nu^2\pi+2\nu u\pi i},$$

který patří do theorie funkcí elliptických, byl však Cauchyem způsobem právě vyloženým odůvodněn před objevením této theorie a přichází také v rukopisné pozůstalosti Gaussově. Jest důležito připomenouti, že zde $\sqrt{a}$ musí míti kladnou svoji část realnou.

2. Buďte nyní λ a μ celistvá čísla, poslední od nully různé, i vyšetřme, jak se chová řada

$$\varphi(x) = \sum_{n=-\infty}^{\infty} e^{-n^2\pi\left(x+\frac{\lambda i}{\mu}\right)}$$

pro nekonečně malá x.

Položme $n = 2\mu m + \varrho$, kde m probíhá veškery celistvé hodnoty a ϱ pouze řadu čísel $\varrho = 0, 1, 2, \ldots |2\mu| - 1$: tak obdržíme veškery celistvé hodnoty n a každou toliko jednou. Bude tedy

$$\varphi(x) = \sum_{\varrho=0}^{|2\mu|-1} e^{-\frac{\varrho^2\lambda\pi i}{\mu}} \sum_{m=-\infty}^{\infty} e^{-(2m+\varrho)^2 x\pi}$$

a zbývá jen vyšetřiti hodnotu řady

$$\varphi_\varrho(x) = \sum_{m=-\infty}^{\infty} e^{-(2\mu m+\varrho)^2 x\pi}$$

pro nekonečně malá x. Řadu tuto lze psáti

$$\varphi_\varrho(x) = \sum_{m=-\infty} e^{-4\mu^2 x\pi\left(m+\frac{\varrho}{2\mu}\right)^2},$$

obdržíme pro ni výhodnější tvar, užijeme-li vzorce (1) v případě

$$a = \frac{1}{4\mu^2 x},$$

takže bude

$$\varphi_\varrho(x) = \frac{1}{|2\mu| \,.\, \sqrt{x}} \sum_{\nu=-\infty}^{\infty} e^{-\frac{\nu^2\pi}{4\mu^2 x} + \frac{\nu\varrho\pi i}{\mu}}.$$

Na pravé straně vyskytuje se totiž řada, kterou lze sloučením členů $+\nu$ a $-\nu$ psáti

$$1 + 2e^{-\frac{\pi}{4\mu^2 x}} \cos\frac{\varrho\pi}{\mu} + 2e^{-\frac{4\pi}{4\mu^2 x}} \cos\frac{2\varrho\pi}{\mu}$$
$$+ 2e^{-\frac{9\pi}{4\mu^2 x}} \cos\frac{6\varrho\pi}{\mu} + 2e^{-\frac{16\pi}{4\mu^2 x}} \cos\frac{8\varrho\pi}{\mu} + \ldots$$

a v té všecky členy se blíží nulle, stává-li se x nekonečně malým, ovšem tak, aby realná část nebyla části pomyslné nekonečně menší. A sice jest ubývání členů této řady toho druhu, že též součet řady sám se blíží nulle. Odtud plyne

$$\lim_{x=0} \sqrt{x}\,\varphi_\varrho(x) = \frac{1}{|2\mu|}$$

a tedy

$$\lim_{x=0} \sqrt{x}\,\varphi(x) = \frac{1}{2|\mu|} \sum_{\varrho=0}^{|2\mu|-1} e^{-\frac{\varrho^2\lambda\pi i}{\mu}},$$

t. j.

$$(2) \qquad \lim_{x=0} \sqrt{x} \sum_{n=-\infty}^{\infty} e^{-n^2\pi\left(x+\frac{\lambda i}{\mu}\right)} = \frac{1}{2|\mu|} \sum_{\varrho=0}^{|2\mu|-1} e^{-\frac{\varrho^2\lambda\pi i}{\mu}}.$$

Ze vzorce (1) máme dále pro $u = 0$

$$\sqrt{a} \sum_{\nu=-\infty}^{\infty} e^{-a\nu^2\pi} = \sum_{\nu=-\infty}^{\infty} e^{-\frac{\nu^2\pi}{a}};$$

vložme sem

$$a = x + \frac{\lambda i}{\mu}$$

a ve vzorci tak vzniklém

$$\sqrt{x + \frac{\lambda i}{\mu}} \sum_{\nu} e^{-\nu^2\pi\left(x + \frac{\lambda i}{\mu}\right)} = \sum_{\nu} e^{-\frac{\nu^2\pi}{x + \frac{\lambda i}{\mu}}}$$

násobme obě strany $\sqrt{x}$ a přejděme k limitě pro $x = 0$.

Na levé straně se tímto způsobem podle vzorce (2) obdrží limita

$$\sqrt{\frac{\lambda i}{\mu}} \cdot \frac{1}{2\,|\,\mu\,|} \sum_{\varrho=0}^{|2\mu|-1} e^{-\varrho^2 \frac{\lambda \pi i}{\mu}},$$

i zbývá jen stanoviti limitu pravé strany, t. j.

$$\lim_{x=0} \sqrt{x} \sum_{\nu} e^{\frac{-\nu^2\pi\left(x - \frac{\lambda i}{\mu}\right)}{x^2 + \frac{\lambda^2}{\mu^2}}} = \lim \sqrt{x} \sum_{\nu} e^{\frac{-\nu^2\pi\left(\frac{\mu^2}{\lambda^2} x - \frac{\mu i}{\lambda}\right)}{1 + \frac{\mu^2 x^2}{\lambda^2}}}.$$

Při tom předpokládáme, že $\lambda \gtrless 0$. Abychom tuto limitu stanovili, ukažme, že rozdíl

$$\varDelta = \sum \left\{ e^{-\frac{\nu^2\pi}{1 + \frac{\mu^2}{\lambda^2} x^2}\left(\frac{\mu^2}{\lambda^2} x - \frac{\mu i}{\lambda}\right)} - e^{-\nu^2\pi\left(\frac{\mu^2}{\lambda^2} x - \frac{\mu i}{\lambda}\right)} \right\}$$

zůstává konečným při nekonečně ubývajícím x.

Podle vzorce

$$|\, f(u) - f(v) \,| \leqq |\, f'(w) \,| \,.\, |\, u - v \,|,$$

v němž w značí neznámou veličinu obsaženou na přímce $(u \ldots v)$, bude

$$\left| e^{-\frac{\nu^2\pi}{1 + \frac{\mu^2}{\lambda^2} x^2}\left(\frac{\mu^2}{\lambda^2} x - \frac{\mu i}{\lambda}\right)} - e^{-\nu^2\pi\left(\frac{\mu^2}{\lambda^2} x - \frac{\mu i}{\lambda}\right)} \right|$$

$$\leqq \nu^2\pi \left(1 - \frac{1}{1 + \frac{\mu^2}{\lambda^2} x^2}\right) \left| \frac{\mu^2}{\lambda^2} x - \frac{\mu i}{\lambda} \right| . \left| e^{-\frac{\nu^2\pi}{1+\varepsilon}\left(\frac{\mu^2}{\lambda^2} x - \frac{\mu i}{\lambda}\right)} \right|,$$

kde

$$0 < \varepsilon < \frac{\mu^2}{\lambda^2} x^2.$$

Poslední veličina je však menší než

$$\nu^2\pi \frac{\mu^2}{\lambda^2} \,.\, x^2 e^{-\frac{\mu^2\nu^2\pi}{2\lambda^2}.x} ,$$

z čehož plyne

$$|\varDelta| < \frac{2\mu^2\pi}{\lambda^2} x^2 \sum_{\nu=1}^{\infty} \nu^2 e^{-\frac{\mu^2\nu^2\pi}{2\lambda^2}.x}$$

aneb, znamená-li

$$\frac{\mu^2}{2\lambda^2} x = a ,$$

$$(\alpha) \qquad |\varDelta| < \frac{8a^2\lambda^2\pi}{\mu^2} \sum_{\nu=1}^{\infty} \nu^2 e^{-\nu^2 a\pi} .$$

Z rovnice

$$\sqrt{a} \sum_{\nu=-\infty}^{\infty} e^{-a\nu^2\pi} = \sum_{\nu=-\infty}^{\infty} e^{-\frac{\nu^2\pi}{a}}$$

plyne differencováním

$$\frac{1}{2\sqrt{a}} \sum e^{-a\nu^2\pi} - \sqrt{a} \sum_{-\infty}^{\infty} \nu^2\pi e^{-a\nu^2\pi} = \sum_{\nu=-\infty}^{\infty} \frac{\nu^2\pi}{a^2} e^{-\frac{\nu^2\pi}{a}}$$

čili

$$a\sqrt{a}\,.\pi \sum_{\nu=1}^{\infty} \nu^2 e^{-a\nu^2\pi} = \frac{1}{4}\sqrt{a} \sum_{\nu=-\infty}^{\infty} e^{-a\nu^2\pi} - \sum_{\nu=1}^{\infty} \frac{\nu^2\pi}{a} e^{-\frac{\nu a^2\pi}{a}} .$$

Pro nekonečně malá a má na pravé straně první řada hodnotu blízkou $\frac{1}{4}$, druhá je nekonečně malá; z toho plyne, že řada

$$a\sqrt{a\pi} \sum_{\nu=1}^{\infty} \nu^2 e^{-a\nu^2\pi}$$

pro nekonečně malá a se blíží $\frac{1}{4}$, a tedy pravá strana rovnice (α) je nekonečně malá zároveň s x, t. j.

$$\lim_{x=0} \varDelta = 0.$$

Odtud plyne nejprve

$$\lim_{x=0} \sqrt{x} \sum_{\nu=-\infty}^{\infty} e^{-\frac{\nu^2\pi}{1+\frac{\mu^2}{\lambda^2}x^2}\left(\frac{\mu^2}{\lambda^2}x-\frac{\mu i}{\lambda}\right)} = \lim \sqrt{x} \sum_{\nu=-8}^{\infty} e^{-\nu^2\pi\left(\frac{\mu^2}{\lambda^2}x-\frac{\mu i}{\lambda}\right)}$$

a tedy máme rovnici

$$\sqrt{\frac{\lambda i}{\mu}} \frac{1}{2\,|\,\mu\,|} \sum_{\varrho=0}^{|2\mu|-1} e^{-\frac{\varrho^2\lambda\pi i}{\mu}} = \left|\frac{\lambda}{\mu}\right| \lim \sqrt{\frac{\mu^2 x}{\lambda^2}} \sum_{\nu=-\infty}^{\infty} e^{-\nu^2\pi\left(\frac{\mu^2 x}{\lambda^2}-\frac{\mu i}{\lambda}\right)}.$$

Pravá strana určí se pomocí vzorce (2) ve tvaru

$$\left|\frac{\lambda}{\mu}\right| \cdot \frac{1}{2\,|\,\lambda\,|} \sum_{\varrho=0}^{|2\lambda|-1} e^{\frac{\varrho^2\mu\pi i}{\lambda}},$$

čímž nabudeme výsledku

$$\text{(3)} \qquad \sqrt{\frac{\lambda i}{\mu}} \cdot \frac{1}{2} \sum_{\varrho=0}^{|2\mu|-1} e^{-\frac{\varrho^2\lambda\pi i}{\mu}} = \frac{1}{2} \sum_{\varrho=0}^{|2\lambda|-1} e^{\frac{\varrho^2\mu\pi i}{\lambda}}.$$

3. Znamenejme nyní

$$\text{(4)} \qquad \Phi(\lambda, \mu) = \frac{1}{2} \sum_{\varrho=0}^{|2\mu|-1} e^{-\frac{\varrho^2\lambda\pi i}{\mu}},$$

i obdrží rovnice (3) tvar

$$\text{(3*)} \qquad \sqrt{\frac{\lambda i}{\mu}}\, \Phi(\lambda, \mu) = \Phi(-\mu, \lambda).$$

Připomeňme, že zde odmocninu

$$\sqrt{\frac{\lambda i}{\mu}}$$

dlužno stanoviti tak, aby její realná část byla kladná.

Výraz $\Phi(\lambda, \mu)$ má následující vlastnosti:

1°. $\Phi(\lambda + 2h\mu, \mu) = \Phi(\lambda, \mu)$, ($h$ celistvé číslo),

2°. $\Phi(2h, 1) = 1$,

3°. $\Phi(\mu, 2) = 1 - i^\mu$, μ liché,

4°. $\Phi(\lambda n^2, \mu) = \Phi(\lambda, \mu)$,

značí-li n celistvé číslo nesoudělné s 2μ. Věc je samozřejma, poněvadž součin ϱn probíhá čísla, jež jsou dle modulu 2μ shodna s čísly $0, 1, 2 \ldots |2\mu| - 1$, v jistém pořádku vzatými. Je-li λ sudé, stačí, je-li n nesoudělno s μ.

Jsou-li obě čísla λ i μ lichá, ruší se členové součtu (4) po dvou a tedy $\Phi(\lambda, \mu)$ vymizí. A sice jsou členové, jež se ruší, vždy ϱ a $\varrho + |\mu|$; neboť v druhém případě zní exponent

$$-(\varrho + |\mu|)^2 \frac{\lambda \pi i}{\mu} = -\frac{\varrho^2 \lambda \pi i}{\mu} \pm 2\varrho\lambda\pi i - \lambda\mu\pi i$$

a poněvadž $\lambda\mu$ jest liché, bude

$$e^{-(\varrho+|\mu|)^2 \frac{\lambda\pi i}{\mu}} = -e^{-\varrho^2 \frac{\lambda\pi i}{\mu}}.$$

Je-li dále m celistvé číslo nesoudělné s λ, bude

5°. $\Phi(\lambda, m^2\mu) = m\Phi(\lambda, \mu)$, $m > 0$.

Důkaz. Podle vzorce (3*) bude

$$\Phi(\lambda, m^2\mu) = \sqrt{\frac{\mu m^2}{\lambda i}}\, \Phi(-m^2\mu, \lambda),$$

což podle vlastnosti 4°. jest

$$= m\sqrt{\frac{\mu}{\lambda i}}\, \Phi(-\mu, \lambda)$$

čili

$$\Phi(\lambda, m^2\mu) = m\Phi(\lambda, \mu).$$

Další vlastnost jest dána vzorcem

(5) $$\Phi(\lambda\nu, \mu)\, \Phi(\lambda\mu, \nu) = \Phi(\lambda, \mu\nu),$$

platným pro *nesoudělná* μ a ν; důkaz se vede takto: Probíhá-li k_1 úplnou soustavu zbytků dle modulu 2μ, k_2 úplnou soustavu zbytků dle modulu 2ν, probíhá číslo

$$\nu k_1 + \mu k_2$$

úplnou soustavu zbytků dle modulu $2\mu\nu$ a sice dvakráte; odtud plyne

$$\sum_{k_1,k_2} e^{-(\nu k_1+\mu k_2)^2 \frac{\lambda\pi i}{\mu\nu}} = \sum_{\varrho=0}^{|2\mu\nu|-1} e^{-\frac{\varrho^2\lambda\pi i}{\mu\nu}}.$$

Levá strana má exponent

$$-\left(\frac{\nu k_1^2}{\mu}+\frac{\mu k_2^2}{\nu}\right)\lambda\pi i - 2k_1k_2\lambda\pi i$$

a tedy zní

$$\sum_{k_1} e^{-\frac{k_1{}^2\lambda\nu\pi i}{\mu}} \cdot \sum_{k_2} e^{-\frac{k_2{}^2\lambda\mu\pi i}{\nu}};$$

součin tento jest $4\Phi(\lambda\nu, \mu)\,\Phi(\lambda\mu, \nu)$ a jeho hodnota výše uvedená zní $2 \, . \, 2\Phi(\lambda, \mu\nu)$; tím vzorec (5) dokázán.

4. Hodnota součtu $\Phi(\lambda, \mu)$ se určí velmi snadno, je-li $\mu = p$ kmenné číslo liché. Znamenejme pak $a, a', a'', \ldots$ veškery kvadratické zbytky dle modulu p (počet jich rovná se $\frac{p-1}{2}$) a dále buď b libovolné číslo, jež není zbytkem kvadratickým; pak čísla $1, 2, 3, \ldots p-1$ budou v jistém pořadu shodna s čísly

$$a, a', a'', \ldots \qquad ab, a'b, a''b \ldots$$

a následovně

$$\sum_{\lambda=1}^{p-1}\Phi(2\lambda, p) = \Phi(2a, p) + \Phi(2a', p) + \Phi(2a'', p) + \ldots$$
$$+ \Phi(2ab, p) + \Phi(2a'b, p) + \Phi(2a''b, p) + \ldots.$$

Podle vlastností 1. a 4. však plyne z definice zbytků kvadratických, t. j.

$$a \equiv k^2 \pmod{p}$$

obecně

$$\Phi(2a\nu, p) = \Phi(2\nu, p)$$

a tedy výraz náš zní

$$\frac{p-1}{2}\Phi(2, p) + \frac{p-1}{2}\Phi(2b, p).$$

Hodnota levé strany jest však nullou, poněvad

$$\sum \Phi(2\lambda, p) = \frac{1}{2}\sum_{\varrho=0}^{2p-1}\sum_{\lambda=1}^{p-1} e^{-\frac{2\varrho^2\lambda\pi i}{p}}$$

$$= \sum_{\lambda=1}^{p-1} e^{-0} + \sum_{\varrho=1}^{p-1}\sum_{\lambda=1}^{p-1} e^{-\frac{2\varrho^2\lambda\pi i}{p}};$$

ježto první součet má hodnotu $p-1$ a dále

$$\sum_{\lambda=1}^{p-1} e^{-\frac{2\varrho^2\lambda\pi i}{p}} = -1,$$

jest

$$\sum_{1}^{p-1} \Phi(2\lambda, p) = 0.$$

Podle toho tedy

$$\Phi(2b, p) = -\Phi(2, p)$$

a

$$\Phi(2a, p) = +\Phi(2, p).$$

Užijeme-li Legendreova znaménka definovaného rovnicemi

$$(6) \qquad \left(\frac{a}{p}\right) = 1, \qquad \left(\frac{b}{p}\right) = -1,$$

máme obecně

$$\Phi(2\nu, p) = \left(\frac{\nu}{p}\right)\Phi(2, p),$$

pokud celistvé číslo ν jest nesoudělné s p.

Abychom stanovili

$$\Phi(2, p),$$

převeďme tento symbol užitím vzorce (3) na tvar

$$\Phi(2, p) = \sqrt{\frac{-pi}{2}}\,\Phi(-p, 2) = \sqrt{\frac{-pi}{2}}(1 + i^p).$$

Poněvadž p jest kladné, máme

$$\sqrt{\frac{-pi}{2}} = \frac{1}{2}\sqrt{p}\,(1-i),$$

takže

$$\Phi(2,p) = \frac{1}{2}(1-i)(1+i^p)\sqrt{p};$$

je-li p tvaru $4k+1$, bude $i^p = i$ a pravá strana zní $\sqrt{p}$; je-li však $p = 4k-1$, jest $i^p = -i$ a výraz $\Phi(2,p)$ bude míti hodnotu

$$\frac{1}{2}(1-i)^2\sqrt{p} = -i\sqrt{p},$$

t. j., sloučíme-li oba případy,

$$\Phi(2,p) = (-i)^{\left(\frac{p-1}{2}\right)^2}\sqrt{p}.$$

Tím dokázán vzorec platný *pro kmenná* p

(7) $$\Phi(2\nu,p) = \left(\frac{\nu}{p}\right)(-i)^{\left(\frac{p-1}{2}\right)^2}\sqrt{p},$$

v němž $\sqrt{p}$ je kladný; i lze jej jinak psáti, přejde-li se hned k hodnotě sdružené

(7*) $$\sum_{\varrho=0}^{p-1} e^{\frac{2\varrho^2\nu\pi i}{p}} = \left(\frac{\nu}{p}\right) i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p}.$$

5. Vzorec (7) poskytne (čtvrtý Gaussův) důkaz zákona reciprocity kvadratických zbytků, zvolí-li se v něm za ν kmenné číslo q. Neboť dle (3*) jest

$$\Phi(2q,p) = \Phi(-p,2q)\sqrt{\frac{p}{2qi}},$$

i zbývá jen vyjádřiti

$$\Phi(-p,2q).$$

Tu jest dle vzorce (5) pro

$$\lambda = -p, \qquad \mu = 2, \qquad \nu = q$$
$$\Phi(-pq,2)\,\Phi(-2p,q) = \Phi(-p,2q),$$

tedy

$$\Phi(-p, 2q) = \Phi(-2p, q)(1 + i^{pq}),$$

takže máme

$$\Phi(-2p, q)(1 + i^{pq})\sqrt{\frac{p}{2qi}} = \Phi(2q, p)$$

aneb podle vzorce (7)

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

a užijeme-li vzorce

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

a rovnice

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

plynoucí ze shody Fermatovy a Eulerovy

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

obdržíme

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

Rozeznáváme-li případy $(p \equiv 1, q \equiv 1)$, $(p \equiv 1, q \equiv -1)$, $(p \equiv -1, q \equiv 1)$, $(p \equiv -1, q \equiv -1)$ mod. 4., obdržíme pořadem

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

t. j znamení $\left(\frac{p}{q}\right)$ a $\left(\frac{q}{p}\right)$ se liší pouze v případě, kdy obě čísla p a q jsou tvaru $4k-1$, což se vyjadřuje známou rovnicí

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

aneb

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

Toť Eulerův a Legendreův zákon reciprocity kvadratických zbytků, Gaussem poprvé dokázaný.

6. Znaménko Legendreovo podléhá následujícím zákonům

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

$$\left(\frac{m}{p}\right)\left(\frac{m'}{p}\right) = \left(\frac{mm'}{p}\right).$$

Ty zůstanou v platnosti, i když m nebo m' je dělitelno číslem p, ve kterémžto případě klademe $\left(\frac{m}{p}\right)$ rovno nulle.

Jacobi zobecnil Legendreovo znaménko pro libovolné moduly, i klade

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\ldots, \text{ je-li } P = p\,p'\,p''\ldots,$$

a volí

$$\left(\frac{m}{-P}\right) = \left(\frac{m}{P}\right).$$

U Jacobiho tedy jmenovatel P je vždy lichý. Ještě dále šel Kronecker, připustiv též sudé moduly; poněvadž symbol $\left(\frac{m}{2}\right)$ nemá přímo patrného významu, položil

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

Tedy definitivní význam symbolu $\left(\frac{m}{n}\right)$ je tento:

Mají-li čísla m a n společného dělitele většího než 1, jest

$$\left(\frac{m}{n}\right) = 0.$$

Dále jest

$$\left(\frac{m}{1}\right) = \left(\frac{1}{n}\right) = 1.$$

Je-li n liché a

$$n = p^{\alpha} p'^{\alpha'} p''^{\alpha''} \ldots.$$

jeho rozklad v kmenné činitele, bude

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p}\right)^{\alpha} \left(\frac{m}{p'}\right)^{\alpha'} \left(\frac{m}{p''}\right)^{\alpha''} \ldots.$$

Je-li m liché a

$$n = 2^{\beta} p^{\alpha} p'^{\alpha'} p''^{\alpha''} \ldots,$$

bude

$$\left(\frac{m}{n}\right) = \left(\frac{2}{m}\right)^{\beta} \left(\frac{m}{p}\right)^{\alpha} \left(\frac{m}{p'}\right)^{\alpha'} \left(\frac{m}{p''}\right)^{\alpha''} \ldots..$$

Konečně jest

$$\left(\frac{m}{-n}\right) = \left(\frac{m}{n}\right).$$

Vlastnosti tohoto symbolu jsou následující:

a) Je-li n liché, jest

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \text{ pro } n > 0, \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

b) Jsou-li m, n čísla lichá, platí obecný zákon reciprocity

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

je-li aspoň jedno z obou čísel kladné.

Důkazy se nalézají v Dirichletových přednáškách, vydaných Dedekindem.

Jsou-li obě čísla m, n záporná, obdržíme příslušnou modifikaci jak následuje.

Poněvadž

$$\left(\frac{m}{n}\right) = \left(\frac{m}{-n}\right), \quad -n > 0,$$

obdržíme

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

a ježto $-m > 0$,

$$\left(\frac{-n}{m}\right) = \left(\frac{n}{m}\right)\left(\frac{-1}{-m}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m+1}{2}}$$

a tedy

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

Lze tedy zákon reciprocitní takto vyjádřiti:

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}+\frac{1-sgn.\,m}{2}\cdot\frac{1-sgn.\,n}{2}}$$

$$[m \equiv n \equiv 1 \pmod{2}].$$

Při tom znamená sgn. x buď $+1$ neb -1, dle toho, jak jest $x > 0$ neb $x < 0$ (signum x).

c) Je-li n liché, neb čtyřmi dělitelné, platí

$$\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right), \text{ jakmile } m \equiv m' \pmod{n}.$$

Důkazy se vedou velmi snadno na základě definice.

d) Bezprostředně jasny jsou následující rovnice

$$\left(\frac{m}{n}\right)\left(\frac{m'}{n}\right) = \left(\frac{mm'}{n}\right),\ \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right) = \left(\frac{m}{nn'}\right).$$

e) Znamenejme D číslo mající tvar diskriminantní, t. j. pro něž buď $D \equiv 1 \pmod{4}$ aneb $D \equiv 0 \pmod{4}$.

Pak platí $\left(\frac{D}{m}\right) = \left(\frac{m}{D}\right)(-1)^{\frac{1-sgn.\,D}{2}\cdot\frac{1-sgn.\,m}{2}}$, je-li D liché, a dále obecně $\left(\frac{D}{k}\right) = \left(\frac{D}{k'}\right)$, je-li $D > 0$, $k \equiv k' \pmod{D}$,

$\left(\frac{D}{k}\right) = \left(\frac{D}{k'}\right)$ sgn. kk', je-li $D < 0$, $k \equiv k' \pmod{D}$.

Důkaz první věty:

$$\left(\frac{D}{m}\right) = \left(\frac{m}{D}\right)(-1)^{\frac{1-sgn.\,D}{2}\cdot\frac{1-sgn.\,m}{2}} \text{ pro lichá D.}$$

Buď $m = 2^\alpha n$, n liché, $\alpha \geqq 0$; tu jest

$$\left(\frac{D}{m}\right) = \left(\frac{2}{D}\right)^\alpha \left(\frac{D}{n}\right);$$

poněvadž $D \equiv 1 \pmod{4}$, plyne

$$\left(\frac{D}{n}\right) = \left(\frac{n}{D}\right)(-1)^{\frac{1-sgn.\,D}{2} \cdot \frac{1-sgn.\,m}{2}},$$

tedy

$$\left(\frac{D}{m}\right) = \left(\frac{2}{D}\right)^\alpha \left(\frac{n}{D}\right)(-1)^{\frac{1-sgn.\,D}{2} \cdot \frac{1-sgn.\,m}{2}}$$

$$= \left(\frac{m}{D}\right)(-1)^{\frac{1-sgn.\,D}{2} \cdot \frac{1-sgn.\,m}{2}},$$

jak tvrzeno.

Abychom druhou větu dokázali, předpokládejme k i k' kladné, D liché. Pak bude

$$\left(\frac{D}{k}\right) = \left(\frac{k}{D}\right),\ \left(\frac{D}{k'}\right) = \left(\frac{k'}{D}\right),\ k \equiv k' \pmod{D},$$

tedy

$$\left(\frac{D}{k}\right) = \left(\frac{D}{k'}\right).$$

Je-li však $k > 0$, $k' < 0$, bude při $D < 0$

$$\left(\frac{D}{k}\right) = \left(\frac{k}{D}\right),\ \left(\frac{D}{k'}\right) = -\left(\frac{k'}{D}\right)$$

a tedy
$$\left(\frac{D}{k}\right) = -\left(\frac{D}{k'}\right).$$

Konečně případ $k < 0$, $k' < 0$ se bezprostředně redukuje na první, poněvadž

$$\left(\frac{D}{k}\right) = \left(\frac{D}{-k}\right) = \left(\frac{D}{-k'}\right) = \left(\frac{D}{k'}\right).$$

Zbývá provésti důkaz pro sudé diskriminanty. Zde budou k i k' čísla lichá, poněvadž jinak by čísla k a D měla společného dělitele 2, a znaménka $\left(\frac{D}{k}\right)$ a $\left(\frac{D}{k'}\right)$ byla by nullami. Poněvadž ze shody

$$k \equiv k' \text{ (mod. D)}$$

plyne (ježto D jest dělitelno čtyřmi) $k \equiv k'$ (mod. 4), bude pro $\varepsilon = (-1)^{\frac{k-1}{2}}$ jak εk, tak $\varepsilon k'$ diskriminantem lichým; tedy

$$\left(\frac{D}{k}\right) = \left(\frac{D}{\varepsilon k}\right) = \left(\frac{\varepsilon k'}{D}\right)(-1)^{\frac{1-sgn.\,D}{2}\cdot\frac{1-sgn.\,\varepsilon k}{2}}$$

$$\left(\frac{D}{k'}\right) = \left(\frac{D}{\varepsilon k'}\right) = \left(\frac{\varepsilon k'}{D}\right)(-1)^{\frac{1-sgn.\,D}{2}\cdot\frac{1-sgn.\,\varepsilon k'}{2}}$$

a ježto

$$\left(\frac{\varepsilon k}{D}\right) = \left(\frac{\varepsilon k'}{D}\right),$$

je též

$$\left(\frac{D}{k}\right) = \left(\frac{D}{k'}\right)(-1)^{\frac{1-sgn.\,D}{2}\cdot\frac{sgn.\,\varepsilon k - sgn.\,\varepsilon k'}{2}}$$

čili, což totéž jest,

$$(9)\quad \left(\frac{D}{k}\right) = \left(\frac{D}{k'}\right)(-1)^{\frac{1-sgn.\,D}{2}\cdot\frac{sgn.\,k - sgn.\,k'}{2}}, \quad (k \equiv k' \text{ mod. D}).$$

Vzorec tento obsahuje důkaz našeho tvrzení, kteréž zároveň vyslovuje s největší obecností.

7. Buď nyní n číslo liché, kladné neb záporné, tvaru $4k+1$, a n_1 číslo sudé, s n nesoudělné. Utvořme pak celistvá čísla h_1, n_2, h_2, n_3, ... tak, aby platily rovnice $n = 2h_1 n_1 + n_2$, $n_1 = 2h_2 n_2 + n_3$, $n_2 = 2h_3 n_3 + n_4$, ... a při tom absolutní hodnoty čísel n_1, n_2, n_3, ... klesaly.

Poněvadž $2n_1 \equiv 0$ (mod. 4), bude

$$n \equiv n_2 \text{ (mod. 4)}.$$

Dále plyne z druhé rovnice $2n_1 \equiv 2n_3$, tedy $2n_3 \equiv 0$ (mod. 4), a z rovnice třetí $n_2 \equiv n_4$ (mod. 4), atd. Tedy čísla n, n_2, n_4, n_6, ... jsou vesměs lichá a shodna s 1 dle mod. 4, kdežto $n_1, n_3, n_5, n_7, \ldots$ jsou sudá. Process vyvíjení těchto čísel zakončí se případem $n_{2r} = 1$, t. j. poslední rovnice bude zníti

$$n_{2r-2} = 2h_{2r-1}\, n_{2r-1} + 1.$$

Znamenejme obecně $sgn.\, n = \nu$, $sgn.\, n_k = \nu_k$; poněvadž n má tvar diskriminantu, a podobně $2n_1$, plyne z rovnice $n = 2h_1 n_1 + n_2$, t. j. ze shody $n \equiv n_2 \pmod{2n_1}$ dle vzorce (9)

$$\left(\frac{2n_1}{n}\right) = \left(\frac{2n_1}{n_2}\right)(-1)^{\frac{1-\nu_1}{2} \cdot \frac{\nu-\nu_2}{2}}.$$

Dále jest $2n_1 \equiv 2n_3 \pmod{n_2}$ a tedy

$$\left(\frac{2n_1}{n_2}\right) = \left(\frac{2n_3}{n_2}\right),$$

takže máme vztah

$$(a) \qquad \left(\frac{2n_1}{n}\right) = \left(\frac{2n_3}{n_2}\right)(-1)^{\frac{\nu_1-1}{2} \cdot \frac{\nu-\nu_2}{2}}.$$

Uvažujme dále výraz

$$\Phi\,(-n, n_1);$$

poněvadž $-n = -n_2 - 2h_1 n_1$, máme dle první vlastnosti výrazu Φ

$$\Phi\,(-n, n_1) = \Phi\,(-n_2, n_1),$$

a poněvadž dle (3*)

$$\Phi\,(-n_2, n_1) = \Phi\,(n_1, n_2)\sqrt{\frac{n_1 i}{n_2}},$$

bude

$$\Phi\,(-n, n_1) = \sqrt{\frac{n_1 i}{n_2}}\,\Phi\,(n_1, n_2).$$

Avšak z rovnice

$$n_1 = 2h_2 n_2 + n_3$$

plyne dále

$$\Phi\,(n_1, n_2) = \Phi\,(n_3, n_2)$$

a tedy

$$\Phi(-n, n_1) = \sqrt{\frac{n_1 i}{n_2}}\, \Phi(n_3, n_2).$$

Podle (3*) jest dále

$$\Phi(n_1, n) = \Phi(-n, n_1)\sqrt{\frac{n}{n_1 i}}$$

a tedy

$$(b) \qquad \Phi(n_1, n) = \sqrt{\frac{n}{n_1 i}}\sqrt{\frac{n_1 i}{n_2}}\,\Phi(n_3, n_2).$$

Jest nyní důležito vyjádřiti výraz $\sqrt{\frac{n}{n_1 i}}$ pomocí veličin $\sqrt{n}$, $\sqrt{n_1}$, $\sqrt{i}$. Jsou-li n i n_1 téhož znamení, bude

$$\sqrt{\frac{n}{n_1 i}} = \frac{\sqrt{n}}{\sqrt{n_1}\sqrt{i}},$$

znamenáme-li $\sqrt{i} = \frac{1+i}{\sqrt{2}}$ a je-li $\sqrt{n}$ kladný aneb kladně pomyslný (v případě $n < 0$). Neboť v obou případech jest veličina $\frac{\sqrt{n}}{\sqrt{n_1}}$ realnou a kladnou. Zbývá tedy vyšetřiti případ, kdy znamení čísel n a n_1 jsou různá. Je-li n kladné a n_1 záporné, bude

$$\sqrt{\frac{n}{n_1 i}} = -\frac{\sqrt{n}}{\sqrt{n_1}\sqrt{i}},$$

kdežto pro případ $n < 0$, $n_1 > 0$ máme

$$\sqrt{\frac{n}{n_1 i}} = \frac{\sqrt{n}}{\sqrt{n_1}\sqrt{i}}.$$

Tudíž platí obecný vzorec

$$(10) \qquad \sqrt{\frac{n}{n_1 i}} = (-1)^{\frac{1+sgn.\,n}{2}\cdot\frac{1-sgn.\,n_1}{2}}\frac{\sqrt{n}}{\sqrt{n_1}\sqrt{i}}$$

čili v našem označení

$$\sqrt{\frac{n}{n_1 i}} = (-1)^{\frac{\nu+1}{2} \cdot \frac{\nu_1-1}{2}} \frac{\sqrt{n}}{\sqrt{n_1}\sqrt{i}};$$

podobně

$$\sqrt{\frac{n_1 i}{n_2}} = (-1)^{\frac{\nu_2+1}{2} \cdot \frac{\nu_1-1}{2}} \frac{\sqrt{n_1}\sqrt{i}}{\sqrt{n_2}}$$

a tedy bude rovnice (b) zníti

$$(c) \qquad \Phi(n_1, n) = (-1)^{\frac{\nu-\nu_2}{2} \cdot \frac{\nu_1-1}{2}} \frac{\sqrt{n}}{\sqrt{n_2}} \Phi(n_3, n_2) \cdot$$

Násobíme-li rovnice (a) a (c) na souhlasných stranách, obdržíme

$$\left(\frac{2n_1}{n}\right) \frac{\Phi(n_1, n)}{\sqrt{n}} = \left(\frac{2n_3}{n_2}\right) \frac{\Phi(n_3, n_2)}{\sqrt{n_2}}.$$

Odtud soudíme, že bude tento výraz dále roven veličinám

$$\left(\frac{2n_5}{n_4}\right) \frac{\Phi(n_5, n_4)}{\sqrt{n_4}}, \quad \left(\frac{2n_7}{n_6}\right) \frac{\Phi(n_7, n_6)}{\sqrt{n_6}}, \ldots$$

a konečně veličině

$$\left(\frac{2n_{2r-1}}{n_{2r-2}}\right) \frac{\Phi(n_{2r-1}, n_{2r-2})}{\sqrt{n_{2r-2}}} = A.$$

Avšak

$$\left(\frac{2n_{2r-1}}{n_{2r-2}}\right) = \left(\frac{2n_{2r-1}}{n_{2r}}\right) (-1)^{\frac{1-\nu_{2r-1}}{2} \cdot \frac{1-\nu_{2r-2}}{2}},$$

což vůči okolnosti $n_{2r} = 1$, má hodnotu $(-1)^{\frac{1-\nu_{2r-1}}{2} \cdot \frac{1-\nu_{2r-2}}{2}}$,

dále

$$\frac{\Phi(n_{2r-1}, n_{2r-2})}{\sqrt{n_{2r-2}}} = \frac{1}{\sqrt{n_{2r-2}}} \Phi(-n_{2r-2}, n_{2r-1}) \sqrt{\frac{n_{2r-2}}{n_{2r-1} i}}$$

$$= \frac{1}{\sqrt{n_{2r-2}}} \sqrt{\frac{n_{2r-2}}{n_{2r-1} i}} \Phi(-n_{2r}, n_{2r-1}) = A'.$$

Poněvadž $n_{2r} = 1$, jest dle (3*)

$$\Phi(n_{2r}, n_{2r-1}) = \Phi(n_{2r-1}, 1)\sqrt{n_{2r-1}\,i},$$

t. j. $\sqrt{n_{2r-1}\,i}$, takže

$$A' = \frac{1}{\sqrt{n_{2r-2}}}\sqrt{\frac{n_{2r-2}}{n_{2r-1}\,i}}\;\sqrt{n_{2r-1}\,i}\,.$$

Avšak dle (10)

$$\sqrt{\frac{n_{2r-2}}{n_{2r-1}\,i}} = (-1)^{\frac{1+\nu_{2r-2}}{2}\cdot\frac{1-\nu_{2r-1}}{2}}\;\frac{\sqrt{n_{2r-2}}}{\sqrt{n_{2r-1}}\sqrt{i}},$$

$$\sqrt{n_{2r-1}\,i} = (-1)^{\frac{1-\nu_{2r-1}}{2}}\sqrt{n_{2r-1}}\sqrt{i}$$

a tedy

$$A' = (-1)^{\frac{1-\nu_{2r-1}}{2}\cdot\frac{1-\nu_{2r-2}}{2}},$$

z čehož plyne

$$A = 1,$$

t. j. jinými slovy

$$\left(\frac{2n_1}{n}\right)\frac{\Phi(n_1, n)}{\sqrt{n}} = 1.$$

Tím dokázána obecná věta

$$\text{(11)} \qquad \Phi(n_1, n) = \left(\frac{2\,n_1}{n}\right)\sqrt{n},$$

platná za podmínky $n \equiv 1 \pmod{4}$, n_1 sudé a nesoudělné s n. Odmocnina $\sqrt{n}$ je buď kladná aneb kladně pomyslná. Píšeme-li $n_1 = 2k$, zní tento výsledek

$$\text{(11}^{\text{a}}\text{)} \qquad \sum_{\alpha=0}^{|n|-1} e^{-\frac{2\alpha^2 k\pi i}{n}} = \left(\frac{k}{n}\right)\sqrt{n}, \quad n \equiv 1 \pmod{4},$$

při čemž k je nesoudělno s n, aneb, píšeme-li $-k$ za k,

$$\text{(11}^{\text{b}}\text{)} \qquad \sum_{\alpha=0}^{|n|-1} e^{\frac{2\alpha^2 k\pi i}{n}} = \left(\frac{-k}{n}\right)\sqrt{n} \quad \text{(tytéž podmínky).}$$

Případ sudého jmenovatele vyšetří se na základě tohoto vzorce pomocí vztahu (3*).

Je totiž dle této rovnice

$$\Phi(-n, n_1) = \Phi(n_1, n)\sqrt{\frac{n_1 i}{n}},$$

tedy dle (11)

$$\Phi(-n, n_1) = \left(\frac{2n_1}{n}\right)\sqrt{n}\sqrt{\frac{n_1 i}{n}}.$$

Znamenáme-li $n_1 = -2k$ a užijeme-li samozřejmé identity

$$\Phi(-n, n_1) = \Phi(n, -n_1),$$

máme

$$\Phi(n, 2k) = \left(\frac{-4k}{n}\right)\sqrt{n}\sqrt{\frac{-2ki}{n}}$$

aneb, poněvadž

$$\sqrt{\frac{2k}{ni}} = (-1)^{\frac{1+sgn.k}{2}\cdot\frac{1-sgn.n}{2}}\frac{\sqrt{2k}}{\sqrt{n}\sqrt{i}},$$

$$\Phi(n, 2k) = \left(\frac{-4k}{n}\right)(-1)^{\frac{1+sgn.k}{2}\cdot\frac{1-sgn.n}{2}}\sqrt{k}\,(1-i).$$

Poněvadž $n \equiv 1$ (mod. 4), plyne z obecného zákona reciprocity

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

a rovnice tato platí i pro sudá a. Pro $a = -4k$ tedy bude

$$\left(\frac{-4k}{n}\right) = \left(\frac{n}{4k}\right)(-1)^{\frac{1+sgn.k}{2}\cdot\frac{1-sgn}{}.},$$

takže poslední výsledek lze psáti

(12) $$\Phi(n, 2k) = \left(\frac{n}{k}\right)(1-i)\sqrt{k}, \quad n \equiv 1 \ (\text{mod.} 4)$$

čili

(12*) $$\sum_{a=0}^{|4k|-1} e^{-\frac{a^2 n \pi i}{2k}} = \left(\frac{n}{k}\right)(1-i)\sqrt{4k},$$

kde $n \equiv 1 \pmod{4}$ a čísla n, k jsou nesoudělna. Přejdeme-li k hodnotě sdružené, plyne za stejných podmínek

$$\sum_{a=0}^{|4k|-1} e^{-\frac{a^2 n\pi i}{2k}} = \left(\frac{n}{k}\right)(1-i)\sqrt{-4k}\,.$$

Poznámka k číslům Bernoulliho.

Napsal

Dr. Karel Petr,

professor v Olomouci.

Sčítáme-li 2., 5., 8., 11., . . . člen rekurrentního vzorce *Moivreova* pro čísla Bernoulliho, obdržíme výraz obsahující čísla Bernoulliho o indexech dle modulu 3 shodných. Jest pozoruhodno, že tento výraz jednoduše dá se ustanoviti. Obdržíme tak formuli, kteráž pro výpočet určitého čísla Bernoulliho téměř devětkrát jest výhodnější než formule Moivreova; jednak jest totiž třeba počítat jenom třetinu předcházejících, jednak pro výpočet jednotlivého čísla máme vzorec třikráte kratší.

Okolnost tuto, že z formule Moivreovy část členů jakožto známá se může vyjmouti, která, ač i z jiných ohledů než právě dotčeného, jest dosti zajímavá, dosud byla nepovšimnuta, hodláme v následujícím dokázati.

Kořeny rovnice

$$x(1-x) - 1 = 0$$

označme ε_1, ε_2; platí mezi nimi vztahy, jak z rovnice ihned patrno,

$$\varepsilon_1 = 1 - \varepsilon_2\,, \qquad \varepsilon_1^3 = \varepsilon_2^3 = -1$$
$$s_{3k} = \varepsilon_1^{3k} + \varepsilon_2^{3k} = \mp 2, \quad s_{3k+1} = s_{3k+2} = \pm 1\,.$$

Znaménko horní platí pro indexy liché, dolní pro indexy sudé. Lze psáti tudíž identicky

$$(x - \varepsilon_1)^m = [(x-1) + \varepsilon_2]^m$$
$$(x - \varepsilon_2)^m = [(x-1) + \varepsilon_1]^m.$$

Umocníme-li a sčítáme-li tyto identity, dostaneme