Matyáš Lerch
O jisté arithmetické větě Zolotareva

Rozpravy Čes. akademie, II. tř., 5 (1896), 8. 17, 1–8

Persistent URL: http://dml.cz/dmlcz/501486

O jisté arithmetické větě Zolotareva.

Sdílí **M. Lerch.**

Předloženo dne 13. března 1896.

Roku 1872 uveřejnil znamenitý ruský mathematik *Zolotarev* nový důkaz zákona reciprocity u zbytků kvadratických,*) jenž spočívá v úvahách kombinatorických a jemuž slouží za základ velmi zajímavý theorém. Abychom jej stručně vyslovili, uvažujme kmenné číslo p a z řady

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

utvořme rozmanité permutace. Jeli

$$i_1, i_2, i_3, \ldots i_{p-1}$$

jedna z těchto permutac, znamenejme μ počet *inversí* v ní se vyskytujících a nazveme číslo $(-1)^\mu$ *známkou* (caractère) její.

Je známo ze základů nauky o determinantech, že známka ta jest $+1$ neb -1, dle toho, jeli počet transposic, které v základní permutaci provésti třeba, aby se vyvolala permutace (i), sudý neb lichý. Pak zní věta ona takto:

Budiž k celistvé číslo kmenným číslem p nedělitelné; nahradímeli v řadě

$$k, 2k, 3k, \ldots (p-1)k \tag{1}$$

každý člen jeho nejmenším kladným zbytkem vzatým dle modulu p, vznikne permutace čísel od 1 do $p-1$, jejíž známka se rovná znaménku Legendrovu $\left(\frac{k}{p}\right)$.

Nežli vyložíme důkaz tohoto theorému, přihlédněme k jeho důsledkům.

Znamenejme pro libovolnou kladnou veličinu ξ symbolem $[\xi]$ její t. zv. celky, takže pak výraz

$$\mathfrak{R}(\xi) = \xi - [\xi]$$

slouží k označení nejmenšího kladného zbytku, jejž z ξ obdržíme odečtením nejblíže menšího čísla celistvého.

*) Nouvelle démonstration de la loi de réciprocité de Legendre (Nouvelles Annales de Mathématiques, 2me série, tome XI, 1872).

Uvažovaná právě řada sestává z členů, které děleny p poskytnou veličiny

$$(1^a) \qquad \mathfrak{R}\left(\frac{k}{p}\right), \mathfrak{R}\left(\frac{2k}{p}\right), \mathfrak{R}\left(\frac{3k}{p}\right), \ldots \mathfrak{R}\left(\frac{(p-1)k}{p}\right);$$

veškery inverse řady této pocházejí od záporných rozdílů

$$\mathfrak{R}\left(\frac{\nu k}{p}\right) - \mathfrak{R}\left(\frac{\nu' k}{p}\right), \qquad (\nu > \nu' = 1, 2, \ldots p-2).$$

Avšak rozdíl $\mathfrak{R}(\xi) - \mathfrak{R}(\xi')$ zbytků dvou veličin ξ a ξ' v případě $\xi > \xi'$ jest kladný neb záporný, jeli výraz $[\xi] - [\xi'] - [\xi - \xi']$ rovný 0 neb 1, a tedy — značíli nám sgn. z znamení veličiny z — máme rovnici

$$\operatorname{sgn.}\left[\mathfrak{R}(\xi) - \mathfrak{R}(\xi')\right] = (-1)^{[\xi]-[\xi']-[\xi-\xi']},$$

takže každá inverse řady (1^a) odpovídá záporné hodnotě výrazu

$$\varepsilon_{\nu,\nu'} = (-1)^{\left[\frac{\nu k}{p}\right]-\left[\frac{\nu' k}{p}\right]-\left[\frac{\nu-\nu'}{p}k\right]}, \qquad (\nu > \nu' = 1, 2, \ldots p-2).$$

Veškery tyto výrazy dlužno vespolek násobiti, aby se obdržela známka uvažované permutace (1^a). Věta Zolotareva redukuje se tedy na tvrzení

$$\left(\frac{k}{p}\right) = (-1)^{\sum_{\nu=2}^{p-1}\sum_{\nu'=1}^{\nu-1}\left\{\left[\frac{\nu k}{p}\right]-\left[\frac{\nu' k}{p}\right]-\left[\frac{\nu-\nu'}{p}k\right]\right\}}.$$

Mocnitel má zde hodnotu

$$S = \sum_{\nu=2}^{p-1}(\nu-1)\left[\frac{\nu k}{p}\right] - \sum_{\nu'<\nu}\left[\frac{\nu' k}{p}\right] - \sum_{\nu'<\nu}\left[\frac{\nu-\nu'}{p}k\right];$$

po substituci $\nu - \nu' = \mu$ máme však

$$\sum_{\nu'<\nu}\left[\frac{\nu-\nu'}{p}k\right] = \sum_{\nu=2}^{p-1}\sum_{\mu=1}^{\nu-1}\left[\frac{\mu k}{p}\right] = \sum_{\nu'<\nu}\left[\frac{\nu' k}{p}\right],$$

a tedy vyjde

$$S = \sum_{\nu=2}^{p-1}(\nu-1)\left[\frac{\nu k}{p}\right] - 2\sum_{\nu'<\nu}\left[\frac{\nu' k}{p}\right].$$

Poněvadž pro $\nu = 3, 5, \ldots p-2$ členové součtu prvního jsou čísla sudá, je zřejmo, že zbývá

$$S = \sum_{\mu=1}^{\frac{1}{2}(p-1)}\left[\frac{2\mu k}{p}\right] + 2m,$$

a tedy obdržíme rovnici

$$(2) \qquad \left(\frac{k}{p}\right) = (-1)^{\sum_{\mu=1}^{\frac{1}{2}(p-1)}\left[\frac{2\mu k}{p}\right]}$$

jakožto první důsledek věty Zolotareva.

Užijeli se vzorce*)

$$(-1)^{[2x]} = \operatorname{sgn}. R(x),$$

v němž $R(x)$ značí absolutně nejmenší zbytek, jenž vznikne z veličiny x odečtením nejblíže ležícího čísla celistvého, takže

$$-\frac{1}{2} \leqq R(x) < \frac{1}{2},$$

obdržíme známou rovnici**)

$$\left(\frac{k}{p}\right) = \operatorname{sgn}. \prod_{\mu=1}^{\frac{1}{2}(p-1)} R\left(\frac{\mu k}{p}\right). \tag{3}$$

Porovnámeli výraz (2) s výrazem odjinud známým***)

$$\left(\frac{k}{p}\right) = (-1)^{\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left[\frac{\nu k}{p}\right] + \frac{p^2-1}{8}(k-1)},$$

obdržíme shodu

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left[\frac{2k\nu}{p}\right] - \sum_{\nu=1}^{\frac{1}{2}(p-1)} \left[\frac{k\nu}{p}\right] \equiv \frac{p^2-1}{8}(k-1), \pmod 2.$$

2. Úvahu předešlou považovati lze za verifikaci věty Zolotareva. Stejnou roli hraje úvaha následující, která vede na nové vyjádření znaménka $\left(\frac{k}{p}\right)$.

Znamenejme Δ determinant

$$\begin{vmatrix} a'_1 & a'_2 & \ldots & a'_{p-1} \\ a''_1 & a''_2 & \ldots & a''_{p-1} \\ \ldots & \ldots & \ldots & \ldots \\ a_1^{(p-1)} & a_2^{(p-1)} & \ldots & a_{p-1}^{(p-1)} \end{vmatrix},$$

a Δ_k buď determinant, jenž z něho vznikne dosazením prvků $a_{k\nu}^{(\mu)}$ za prvky $a_\nu^{(\mu)}$, při čemž index $k\nu$ dlužno redukovati na jeho zbytek modulo p. Pak bude podle Zolotareva

$$\Delta_k = \left(\frac{k}{p}\right) \Delta,$$

i je patrno, že obdržíme nové vyjádření znaménka $\left(\frac{k}{p}\right)$, volímeli vhodně prvky determinantu Δ. My zvolíme

$$a_\nu^{(\mu)} = \omega^{\mu\nu},$$

---

*) Vzorec ten plyne z okolnosti, že rozdíl $[2x] - 2[x]$ rovná se nulle neb jedné, dle toho, jeli $R(x)$ kladné neb záporné.

**) Kronecker, Sitzungsberichte der kön. preuss. Akad. d. Wiss., 1884, p. 519.

***) Srov. Jornal de Sciencias mathematicas, vol. IX, p. 137.

kde ω značí komplexní jednotku kruhodílnou $e^{\frac{2\pi i}{p}}$; pak bude

$$a_{\nu k}^{(\mu)} = \omega^{k\mu\nu},$$

a poněvadž vyjádříme Δ jako racionalnou funkci $\varphi(\omega)$, obdrží se $\Delta_k = \varphi(\omega^k)$.

Skutečně jest

$$\varphi(\omega) = \omega^{1+\binom{3}{2}+\binom{4}{2}+\ldots+\binom{p}{2}} (\omega-1).(\omega^2-1)(\omega-1)$$
$$.(\omega^3-1)(\omega^2-1)(\omega-1).(\omega^4-1)(\omega^3-1)(\omega^2-1)(\omega-1)$$
$$\ldots.(\omega^{p-2}-1)\ldots(\omega-1),$$

čili při označení

$$s = 1+\binom{3}{2}+\binom{4}{2}+\ldots+\binom{p}{2}$$

$$\varphi(\omega) = \omega^s \prod_{\nu=1}^{p-2} (\omega^\nu - 1)^{p-\nu-1}.$$

Máme tedy

$$(4) \qquad \left(\frac{k}{p}\right) = \frac{\varphi(\omega^k)}{\varphi(\omega)} = \omega^{(k-1)s} \prod_{\nu=1}^{p-2} \left(\frac{\omega^{k\nu}-1}{\omega^\nu-1}\right)^{p-\nu-1};$$

poněvadž však

$$\frac{\omega^{k\nu}-1}{\omega^\nu-1} = e^{(k-1)\frac{\nu\pi i}{p}} \frac{\sin\frac{k\nu\pi}{p}}{\sin\frac{\nu\pi}{p}},$$

vyjde

$$\left(\frac{k}{p}\right) = e^{(k-1)\frac{\pi i}{p}\left[2s-\sum_{\nu=1}^{p-2}\nu(p-\nu-1)\right]} \prod_{\nu=1}^{p-2} \left(\frac{\sin\frac{k\nu\pi}{p}}{\sin\frac{\nu\pi}{p}}\right)^{p-\nu-1}$$

Avšak

$$\frac{1}{p}\sum_{\nu=1}^{p-2}\nu(p-\nu-1) = \binom{p-1}{2} - \frac{2}{p}\left[1+\binom{3}{2}+\binom{4}{2}+\ldots+\binom{p-1}{2}\right],$$

a tedy exponent v posledním výrazu zní

$$2\frac{(k-1)\pi i}{p}\cdot\binom{p}{2} - (k-1)\pi i\binom{p-1}{2}$$
$$= (k-1)(p-1)\pi i - \frac{(k-1)(p-1)}{2}(p-2)\pi i,$$

takže náš výsledek bude

$$(4^*) \qquad \left(\frac{k}{p}\right) = (-1)^{\frac{(k-1)(p-1)}{2}} \prod_{\nu=1}^{p-2} \left(\frac{\sin\frac{k\nu\pi}{p}}{\sin\frac{\nu\pi}{p}}\right)^{p-\nu-1}$$

Poněvadž tu běží pouze o znamení, možno v součinu na pravé straně vynechati veškery činitele, v nichž ν je sudé, any jsou vesměs kladné, i zbývá tak

$$(5)\quad \left(\frac{k}{p}\right) = (-1)^{\frac{(k-1)(p-1)}{2}} \operatorname{sgn.} \prod_{\lambda} \sin\frac{k\lambda\pi}{p}, \qquad (\lambda = 1, 3, 5, \ldots p-2).$$

Užijeli se tu samozřejmé rovnice

$$\operatorname{sgn} \sin z\pi = \operatorname{sgn.} R\left(\frac{z}{2}\right),$$

obdržíme

$$(5^*)\quad \left(\frac{k}{p}\right) = (-1)^{\frac{(k-1)(p-1)}{2}} \operatorname{sgn.} \prod_{\lambda} R\left(\frac{k\lambda}{2p}\right), \qquad (\lambda = 1, 3, 5, \ldots p-2),$$

kterážto rovnice jest opět takměř bezprostředním důsledkem theorému Zolotareva; užijeli se tu vzorce

$$\operatorname{sgn.} R\left(\frac{k\lambda}{2p}\right) = (-1)^{\left[\frac{k\lambda}{p}\right]},$$

vznikne

$$(6)\quad \left(\frac{k}{p}\right) = (-1)^{\frac{(k-1)(p-1)}{2} + \sum_{\lambda}\left[\frac{k\lambda}{p}\right]}, \qquad (\lambda = 1, 3, 5, \ldots p-2).$$

Výsledek ten není nesnadno převésti v rovnici (2), užijeli se vztahu

$$\sum_{\alpha=1}^{p-1}\left[\frac{k\alpha}{p}\right] = \frac{(k-1)(p-1)}{2}.$$

3. Předešlé úvahy platí pro libovolné celistvé číslo p (složené), které jest liché a nesoudělné s číslem k, definujeli se symbol $\left(\frac{k}{p}\right)$ jakožto známka permutace (1^a). Proto bude třeba studovati symbol

$$(7)\quad \left(\frac{n}{m}\right) = \operatorname{sgn.} \prod_{h=1}^{\frac{1}{2}(m-1)} R\left(\frac{hn}{m}\right),$$

v němž m značí celistvé kladné číslo liché, a n číslo s m nesoudělné, kladné neb záporné. Kronecker verifikoval vztah

$$(8)\quad \left(\frac{n}{m}\right)\cdot\left(\frac{n'}{m}\right) = \left(\frac{nn'}{m}\right)$$

jak následuje.

Činitele součinu

$$\left(\frac{n'}{m}\right) = \operatorname{sgn.} \prod_{h'=1}^{\frac{1}{2}(m-1)} R\left(\frac{h'n'}{m}\right)$$

seřaďme s činiteli součinu (7) v páry (h, h'), jichž přípony se nacházejí v souvislosti definované shodou

$$nh \equiv \pm h' \pmod{m}.$$

Odtud vychází

$$R\left(\frac{nh}{m}\right) = \pm \frac{h'}{m}, \qquad R\left(\frac{nn'h}{m}\right) = R\left(\pm \frac{n'h'}{m}\right) = \pm R\left(\frac{n'h'}{m}\right),$$

a tedy

$$\text{sgn. } R\left(\frac{nn'h}{m}\right) = \text{sgn. } R\left(\frac{nh}{m}\right) . \text{sgn. } R\left(\frac{n'h'}{m}\right).$$

Znásobíme-li tyto rovnice pro $h = 1, 2, 3, \ldots \frac{m-1}{2}$, vznikne

$$\prod_h \text{sgn. } R\left(\frac{nn'h}{m}\right) = \prod_h \text{sgn. } R\left(\frac{nh}{m}\right) . \prod_{h'} \text{sgn. } R\left(\frac{n'h'}{m}\right),$$

čímž rovnice (8) verifikována.

O symbolu (7) dokázal dále Kronecker přímou verifikací zákon reciprocity

$$\left(\frac{n}{m}\right) . \left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}, \tag{9}$$

v němž n značí taktéž číslo liché, kladné neb záporné, při čemž v případě $n < 0$ symbol

$$\left(\frac{m}{n}\right) \text{ má značiti číslo } \left(\frac{m}{-n}\right).$$

Pro důkaz vzorce (9) se ovšem nejprve předpokládá $n > 0$, $m > 0$, načež se z rovnice (7) odvodí

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

a z rovnice (8) pak plyne

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

takže bude při $m > 0$, $n > 0$

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

čímž dokázán vzorec (9) obecně.

Pomocí vlastností (8) a (9) dokáže se snadno vzorec další

$$\left(\frac{m}{n}\right)\left(\frac{m}{n'}\right) = \left(\frac{m}{nn'}\right) \tag{10}$$

pokud jest m liché, a jeli m sudé a $= 2^a m^0$, je patrně

$$\left(\frac{m}{n}\right) = \left(\frac{2^a}{n}\right)\left(\frac{m^0}{n}\right),$$

takže zbývá jen ukázati správnost rovnice

$$\left(\frac{2^a}{n}\right)\left(\frac{2^a}{n'}\right) = \left(\frac{2^a}{nn'}\right).$$

Jeli α sudé, jest $\left(\frac{2^\alpha}{n}\right) = \left(\frac{2^{\frac{\alpha}{2}}}{n}\right) \cdot \left(\frac{2^{\frac{\alpha}{2}}}{n}\right) = 1$; jeli α liché, není nesnadno vyšetřiti, že

$$\left(\frac{2^\alpha}{n}\right) = \left(\frac{2}{n}\right) = (-1)^{\frac{n \pm 1}{4}} = (-1)^{\frac{n^2-1}{8}},$$

takže opět

$$\left(\frac{2^\alpha}{n}\right)\left(\frac{2^\alpha}{n'}\right) = (-1)^{\frac{n^2-1}{8} + \frac{n'^2-1}{8}} = (-1)^{\frac{(nn')^2-1}{8}} = \left(\frac{2^\alpha}{nn'}\right).$$

Jeli tedy $m = p_1^{a_1} p_2^{a_2} \ldots$ rozklad čísla m v kmenné činitele, bude dle předeslaných vět

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{a_1}\left(\frac{n}{p_2}\right)^{a_2} \ldots,$$

t. j. symbol $\left(\frac{n}{m}\right)$ se kryje se znaménkem Legendrovým v Jacobiově zobecnění.

Tudíž platí věta:

Redukujíli se čísla

$$(1^b) \qquad k, 2k, 3k, \ldots (m-1)k$$

na nejmenší svoje kladné zbytky dle modulu m, vznikne permutace o známce $\left(\frac{k}{m}\right)$, kde poslední symbol vzat ve smyslu Jacobiově. Při tom jest m číslo liché a kladné, k libovolné.

Stopujeli se úvaha čl. 1., shledáme, že výraz

$$(-1)^{\Sigma\left[\frac{2\mu k}{m}\right]}, \qquad \left(\mu = 1, 2, 3, \ldots \left[\frac{m-1}{2}\right]\right)$$

udává známku naší permutace i v případě sudého m; tu jest však

$$\sum_{\mu=1}^{\frac{m-1}{2}} \left[\frac{2k\mu}{m}\right] = \frac{1}{2}(k-1)\left(\frac{m}{2} - 1\right),$$

a tedy máme větu:

Jeli k celistvé číslo nesoudělné s $2m$, vznikne z řady

$$k, 2k, 3k, \ldots (2m-1)k$$

redukcí všech členů dle modulu $2m$ permutace čísel od 1 do $2m-1$, jejíž známka zní

$$(-1)^{\frac{(k-1)(m-1)}{2}}.$$

4. Budiž nám dovoleno reprodukovati na tomto místě důkaz, jejž o svém základním theorému podal Zolotarev pro případ kmenného p.

Buď a základní kořen pro modul p (racine primitive du nombre p), t. j. celistvé číslo, jehož mocnosti

$$1, a, a^2, a^3, \ldots a^{p-2}$$

jsou modulo p různy, takže každá z nich representuje jednu třídu modulo p. Zvolme nyní exponenty $e_1, e_2 \ldots$ tak, aby řada

(A) $$1, a^{e_1}, a^{e_2}, \ldots a^{e_{p-2}}$$

po redukci přešla v permutaci základní $1, 2, 3, \ldots p-1$. Určíli se pak číslo f shodou

$$k \equiv a^f \pmod{p},$$

budou čísla

(B) $$a^f, a^{e_1+f}, a^{e_2+f} \ldots a^{e_{p-2}+f}$$

pořadem shodna s čísly $k, 2k, 3k, \ldots (p-1)k$. Patrně vznikne permutace (B) ze základní (A), podrobíli se tato f po sobě jdoucím cyklickým záměnám, což se vyrovná $f(p-2)$ transposicím, a toto číslo je s číslem f stejné parity. Známka permutace (B) je tedy $(-1)^f$. Ze shody

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

plyne pak $(-1)^f = \left(\frac{k}{p}\right)$, poněvadž pro sudé f jest k kvadratickým zbytkem dle p, a jest nezbytkem v případě lichého f. Tím věta dokázána přímo a je zřejmo, že může postavena býti v čelo theorie kvadratických zbytků.