DEDEKINDOVE VSOTE IN KVADRATNI RECIPROCITETNI ZAKON

REBEKA RENKO ZVER

Prva gimnazija Maribor

Math. Subj. Class. (2010): 11F20

Predstavili bomo Dedekindove vsote in z njimi povezano reciprocitetno formulo ter pokazali, kako je iz le-te možno izpeljati znani kvadratni reciprocitetni zakon.

DEDEKIND SUMS AND THE QUADRATIC RECIPROCITY LAW

We will introduce the Dedekind sums with a related reciprocity formula which will lead us to the derivation of the known quadratic reciprocity law.

Uvod

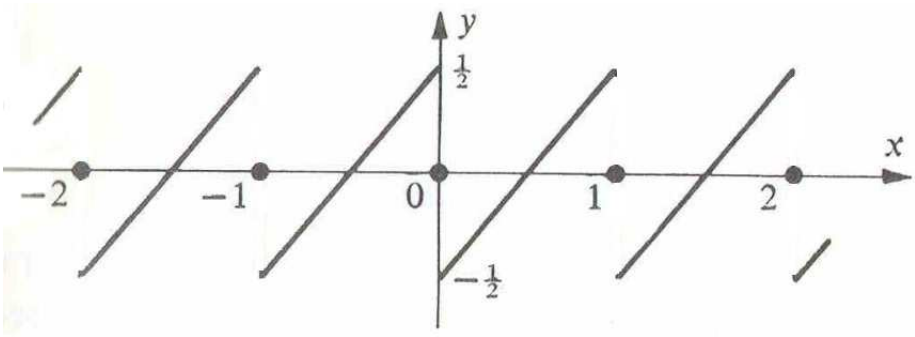
Dedekindove vsote so pomemben del klasične teorije števil in še danes pogosto uporabljena tema tudi na drugih področjih matematike. Sestavni del njihove definicije je naslednja funkcija:

Definicija 1 (Dvojni oklepaj).

$$((x)) = \begin{cases} x - [x] - \frac{1}{2}\,; & \text{če } x \text{ ni celo število,} \\ 0\,; & \text{če je } x \text{ celo število,} \end{cases} \tag{1}$$

kjer je $[x]$ največje celo število, ki ne presega $x \in \mathbb{R}$.

Njen graf je žagaste oblike:



Z uporabo dvojnega oklepaja (1) lahko definiramo najpomembnejši pojem tega sestavka:

Definicija 2 (Dedekindove vsote).

$$s(h,k) = \sum_{j=1}^{k} \left(\left(\frac{j}{k}\right)\right)\left(\left(\frac{hj}{k}\right)\right), \quad h \in \mathbb{Z}, k \in \mathbb{N}. \tag{2}$$

Dedekindove vsote so dobile ime po znanem nemškem matematiku **Richardu Dedekindu**[1].

Ena njihovih glavnih lastnosti je simetričnost, predstavljena z naslednjo **reciprocitetno formulo**, ki je veljavna za tuji si naravni števili h, k:

$$12(s(h,k) + s(k,h)) = -3 + \frac{h}{k} + \frac{k}{h} + \frac{1}{hk}. \tag{3}$$

Reciprocitetna formula je pomembna sama po sebi, koristna pa je npr. pri izpeljavi splošnega (Jacobijevega) kvadratnega reciprocitetnega zakona. V zvezi s tem se spomnimo **Legendrovega simbola**, pri katerem za vsako naravno število n in liho praštevilo p, ki ne deli n, velja

$$\left(\frac{n}{p}\right) = \begin{cases} 1\,; & \text{če obstaja tak } x, \text{ da je } x^2 \equiv n \pmod{p}, \\ -1\,; & \text{sicer.} \end{cases}$$

Če pa dovolimo za n tudi negativna cela števila, pa lahko povemo, da velja:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1\,; & \text{če je } p \equiv 1 \pmod{4}, \\ -1\,; & \text{če je } p \equiv 3 \pmod{4}. \end{cases}$$

Ob upoštevanju multiplikativnosti Legendrovega simbola v n od tod sledi, da je dovolj poznati vrednosti simbola za naravne n. Vrednost $(-1/p)$ pa je tesno povezana s predstavljivostjo praštevila p kot vsote dveh kvadratov naravnih števil.

Jacobijev simbol potem definiramo (za poljubno naravno število n in za liho naravno število m, ki si je tuje z n in ima praštevilski razcep $m =$

[1] **Julius Wilhelm Richard Dedekind (1831–1916)** se je rodil v Braunschweigu v Nemčiji, kjer je obiskoval osnovno in srednjo šolo, študiral pa je na univerzi v Göttingenu in Berlinu. Doktoriral je leta 1852 pri Gaussu v Göttingenu kot njegov zadnji študent, habilitacijo pa je opravil leta 1854 v Berlinu istočasno z Riemannom, s katerim sta bila kasneje nekaj časa tudi učiteljska kolega. Vrnil se je v Göttingen, kjer je kot prvi poučeval Galoisovo teorijo. Kasneje je nekaj časa učil v Zürichu in nato do upokojitve 1894 v rodnem Braunschweigu. Znan je po svojem delu in rezultatih iz algebre (definicija idealov, algebraični dokaz Riemann-Rochovega izreka za kompaktne Riemannove ploskve), analize (prerezi kot model za realna števila) in teorije množic (definiciji neskončne množice). Na njegove matematične raziskave so največ vplivali Gauss, Dirichlet in Riemann, katerih zbrana dela je urejal. Zbrani in dopolnjeni Riemannovi zapiski so izšli leta 1876 s Heinrichom Webrom kot glavnim urednikom. Rokopisa, ki sta obravnavala teorijo eliptičnih modularnih funkcij, pa je uredil sam Dedekind [2].

$\prod_{j=1}^{r} p_j$ na ne nujno različne prafaktorje) kot produkt ustreznih Legendrovih simbolov:

$$\left(\frac{n}{m}\right) = \prod_{j=1}^{r} \left(\frac{n}{p_j}\right).$$

Splošni kvadratni reciprocitetni zakon pravi, da za tuji si lihi naravni števili h in k z Jacobijevima simboloma $\left(\frac{h}{k}\right)$ in $\left(\frac{k}{h}\right)$ velja enakost

$$\left(\frac{h}{k}\right)\left(\frac{k}{h}\right) = (-1)^{\frac{h-1}{2}\cdot\frac{k-1}{2}}.$$

Pred leti je Obzornik že pisal [5] o posebnem primeru tega zakona, ko sta h in k različni lihi praštevili.

V nadaljevanju bomo najprej spoznali nekatere elementarne lastnosti Dedekindovih vsot (2) in prek njih izpeljali reciprocitetno formulo (3). Nato bomo (ob privzetku posplošene Gaussove leme) z uporabo reciprocitetne formule dokazali splošni kvadratni reciprocitetni zakon, na koncu pa dodali še nekaj opomb o drugih vidikih Dedekindovih vsot.

Dedekindove vsote in reciprocitetna formula

Najprej dokažimo, da je funkcija dvojni oklepaj periodična in liha.

Trditev 1. *Za poljubno celo število n in poljubno realno število x velja:*

(a) $((x+n)) = ((x))$,

(b) $((-x)) = -((x))$.

Dokaz. (a) Za celo število x je $((x+n)) = 0 = ((x))$, sicer pa zaradi $[x+n] = [x] + n$ velja

$$((x+n)) = x + n - [x+n] - \tfrac{1}{2} = x + n - [x] - n - \tfrac{1}{2} = ((x)).$$

(b) Za $x \in \mathbb{Z}$ je dokaz trivialen, za $x \notin \mathbb{Z}$ pa rezultat sledi iz enakosti $[x] + [-x] = -1$. ∎

Sedaj se spomnimo pojma, ki ga bomo potrebovali v nadaljevanju.

Popolni sistem ostankov po modulu k je taka množica celih števil $P = \{j_1, j_2, \ldots, j_k\}$, da je $j_i \equiv i \pmod{k}$ za vsak $i = 1, 2, ..., k$.

Pri tem smo upoštevali, da velja $k \equiv 0 \pmod{k}$, zato bomo posledično za popoln sistem ostankov po modulu k venomer uporabljali množico $\{1, 2, \ldots, k\}$.

V primeru, ko je h tuj proti k, je potem tudi $hP = \{hj_1, hj_2, ..., hj_k\}$ popolni sistem ostankov po modulu k, saj je $hj_i \equiv hi \pmod{k}$ in je preslikava $i \mapsto hi \pmod{k}$ v tem primeru injektivna, torej permutacija množice $\{1, 2, ..., k\}$.

Trditev 2. *Naj bo P poljuben popolni sistem ostankov po modulu k. Tedaj velja:*

(a) $$\sum_{j\in P}\left(\left(\frac{j}{k}\right)\right)=\sum_{j=1}^{k}\left(\left(\frac{j}{k}\right)\right)=0.$$

(b) *Če je k naravno, h pa celo število, tuje proti k, je tudi*

$$\sum_{j=1}^{k}\left(\left(\frac{hj}{k}\right)\right)=0. \tag{4}$$

Dokaz. (a) Izberimo elemente iz popolnega sistema ostankov P in jih zapišimo v obliki:

$$\begin{aligned} j_1 &= 1+k\cdot n_1, \quad j_2 = 2+k\cdot n_2, \quad \ldots \\ j_{k-1} &= (k-1)+k\cdot n_{k-1}, \quad j_k = k\cdot n_k, \end{aligned}$$

kjer so $n_1,\ldots,n_k$ iz množice celih števil. Tedaj je po trditvi 1

$$\begin{aligned} \sum_{j\in P}\left(\left(\frac{j}{k}\right)\right) &= \left(\left(\frac{1}{k}+n_1\right)\right)+\left(\left(\frac{2}{k}+n_2\right)\right)+\ldots+\left(\left(\frac{0}{k}+n_k\right)\right) \\ &= \sum_{j=1}^{k-1}\left(\left(\frac{j}{k}\right)\right). \end{aligned}$$

To pa je po definiciji 1 in dejstvu $\left[\frac{j}{k}\right]=0$ za $1\le j<k$ naprej enako:

$$\begin{aligned} \sum_{j=1}^{k-1}\left(\left(\frac{j}{k}\right)\right) &= \left(\frac{1}{k}-\frac{1}{2}\right)+\left(\frac{2}{k}-\frac{1}{2}\right)+\ldots+\left(\frac{k-1}{k}-\frac{1}{2}\right) \\ &= \frac{k(k-1)}{2k}-\frac{k-1}{2}=0. \end{aligned}$$

(b) Dokaz sledi iz točke (a), saj je tudi hP popolni sistem ostankov po modulu k. ∎

Opomba 1. Opazimo, da je zadnji člen v vsoti $\sum_{j=1}^{k}\left(\left(\frac{j}{k}\right)\right)$ ali $\sum_{j=1}^{k}\left(\left(\frac{hj}{k}\right)\right)$ enak nič, zato je vseeno, ali v takih vsotah seštevamo do k ali do $k-1$. To bomo v nadaljevanju še večkrat upoštevali.

Dokažimo še nekaj **osnovnih lastnosti Dedekindovih vsot**.

Trditev 3. *Imejmo poljuben popolni sistem $P = \{j_1, j_2, \ldots, j_k\}$ ostankov po modulu k. Naj bo h poljubno celo, k pa naravno število, tuje s h. Tedaj velja:*

$$s(h,k) = \sum_{j \in P} \left(\left(\frac{j}{k}\right)\right)\left(\left(\frac{hj}{k}\right)\right).$$

Trditev pomeni, da je Dedekindova vsota $s(h,k)$ v primeru tujih si števil h, k neodvisna od izbire popolnega sistema ostankov po modulu k. Dokažemo jo na popolnoma enak način kot trditev 2, če le upoštevamo definicijo popolnega sistema ostankov po modulu k in periodičnost dvojnega oklepaja.

V posebnem primeru je od izbire popolnega sistema ostankov P neodvisna tudi vsota

$$s(1,k) = \sum_{j \in P} \left(\left(\frac{j}{k}\right)\right)\left(\left(\frac{j}{k}\right)\right) = \sum_{j \in P} \left(\left(\frac{j}{k}\right)\right)^2. \tag{5}$$

Računanje Dedekindovih vsot pa se da še nekoliko poenostaviti; zapišemo jih lahko samo z enim dvojnim oklepajem.

Trditev 4. *Za vsako celo število h in naravno število k, ki si je tuje s h, velja:*

$$s(h,k) = \sum_{j=1}^{k} \frac{j}{k}\left(\left(\frac{hj}{k}\right)\right).$$

Dokaz. Zadnji člen v vsoti (2) je enak nič, tako da imamo:

$$s(h,k) = \sum_{j=1}^{k-1} \left(\left(\frac{j}{k}\right)\right)\left(\left(\frac{hj}{k}\right)\right) = \sum_{j=1}^{k-1} \left(\frac{j}{k} - \left[\frac{j}{k}\right] - \frac{1}{2}\right)\left(\left(\frac{hj}{k}\right)\right).$$

Upoštevajmo, da je $\left[\frac{j}{k}\right] = 0$, za $j < k$ in enakost (4), pa dobimo:

$$s(h,k) = \sum_{j=1}^{k-1} \left(\frac{j}{k} - \frac{1}{2}\right)\left(\left(\frac{hj}{k}\right)\right) = \sum_{j=1}^{k-1} \frac{j}{k}\left(\left(\frac{hj}{k}\right)\right) = \sum_{j=1}^{k} \frac{j}{k}\left(\left(\frac{hj}{k}\right)\right).$$

■

Najpomembnejša lastnost Dedekindovih vsot $s(h,k)$ je reciprocitetna formula. V literaturi zanjo obstaja več dokazov, enega bomo navedli sedaj.

Izrek 5 (Reciprocitetna formula). *Za poljubni tuji si naravni števili h in k velja naslednja enakost:*

$$12(s(h,k)+s(k,h)) = -3 + \frac{h}{k} + \frac{k}{h} + \frac{1}{hk}. \tag{6}$$

Dokaz. Za $h = k = 1$ je enakost izpolnjena, saj sta obe strani enaki nič. V vseh drugih primerih pa lahko zaradi simetričnosti reciprocitetne formule predpostavimo, da je $k > 1$. Kot vemo, je zaradi tujosti števil h in k poleg $P = \{1, 2, ..., k\}$ tudi $P' = \{hj;\ j \in P\}$ popolni sistem ostankov po modulu k, zato zaradi (5) velja:

$$\sum_{j=1}^{k} \left(\left(\frac{hj}{k} \right) \right)^2 = \sum_{i \in P'} \left(\left(\frac{i}{k} \right) \right)^2 = \sum_{j=1}^{k} \left(\left(\frac{j}{k} \right) \right)^2.$$

Torej po eni strani dobimo

$$\begin{aligned} \sum_{j=1}^{k} \left(\left(\frac{hj}{k} \right) \right)^2 &= \sum_{j=1}^{k} \left(\left(\frac{j}{k} \right) \right)^2 = \sum_{j=1}^{k-1} \left(\frac{j}{k} - \frac{1}{2} \right)^2 \\ &= \frac{1}{k^2} \sum_{j=1}^{k-1} j^2 - \frac{1}{k} \sum_{j=1}^{k-1} j + \frac{1}{4} \sum_{j=1}^{k-1} 1, \end{aligned} \tag{7}$$

po drugi strani pa imamo:

$$\begin{aligned} \sum_{j=1}^{k} \left(\left(\frac{hj}{k} \right) \right)^2 &= \sum_{j=1}^{k-1} \left(\frac{hj}{k} - \left[\frac{hj}{k} \right] - \frac{1}{2} \right)^2 = \\ &= 2h \sum_{j=1}^{k-1} \frac{j}{k} \left(\frac{hj}{k} - \left[\frac{hj}{k} \right] - \frac{1}{2} \right) + \sum_{j=1}^{k-1} \left[\frac{hj}{k} \right] \left(\left[\frac{hj}{k} \right] + 1 \right) - \\ &\quad - \frac{h^2}{k^2} \sum_{j=1}^{k} j^2 + \frac{1}{4} \sum_{j=1}^{k-1} 1 = \\ &= 2h \sum_{j=1}^{k-1} \frac{j}{k} \left(\left(\frac{hj}{k} \right) \right) + \sum_{j=1}^{k-1} \left[\frac{hj}{k} \right] \left(\left[\frac{hj}{k} \right] + 1 \right) - \frac{h^2}{k^2} \sum_{j=1}^{k} j^2 + \frac{1}{4} \sum_{j=1}^{k-1} 1. \end{aligned} \tag{8}$$

Če primerjamo (7) in (8), dobimo

$$2h \sum_{j=1}^{k-1} \frac{j}{k} \left(\left(\frac{hj}{k} \right) \right) + \sum_{j=1}^{k-1} \left[\frac{hj}{k} \right] \left(\left[\frac{hj}{k} \right] + 1 \right) - \frac{h^2}{k^2} \sum_{j=1}^{k} j^2 = \frac{1}{k^2} \sum_{j=1}^{k-1} j^2 - \frac{1}{k} \sum_{j=1}^{k-1} j$$

in z uporabo trditve 4 najdemo

$$2hs(h,k)+\sum_{j=1}^{k-1}\left[\frac{hj}{k}\right]\left(\left[\frac{hj}{k}\right]+1\right)=\frac{h^2+1}{k^2}\sum_{j=1}^{k-1}j^2-\frac{1}{k}\sum_{j=1}^{k-1}j. \qquad (9)$$

V vsoti na levi strani imamo $0\le\left[\frac{hj}{k}\right]\le h-1$. Za lažje računanje označimo

$$\left[\frac{hj}{k}\right]=i-1,\quad \text{za neki}\quad i=1,2,\ldots,h. \qquad (10)$$

Skušajmo ugotoviti, za katere j doseže $\left[\frac{hj}{k}\right]$ vrednost $i-1$. Ker $\frac{hj}{k}$ ni celo število, je enakost (10) ekvivalentna pogoju

$$i-1<\frac{hj}{k}<i,$$

zato lahko zapišemo

$$\frac{k(i-1)}{h}<j<\frac{ki}{h}.$$

Če torej j teče od $\left[\frac{k(i-1)}{h}\right]+1$ do vključno $\left[\frac{ki}{h}\right]$, je za $i<h$ vrednost $\left[\frac{hj}{k}\right]$ enaka $i-1$. Če pa je $i=h$, je $\frac{ki}{h}=k$ in $\left[\frac{hj}{k}\right]=h-1$ natanko takrat, ko j zavzame vrednosti od $\left[\frac{k(h-1)}{h}\right]+1$ do vključno $k-1$. Tako dobimo

$$\begin{aligned}
&\sum_{j=1}^{k-1}\left[\frac{hj}{k}\right]\left(\left[\frac{hj}{k}\right]+1\right)=\\
&=\sum_{i=1}^{h-1}(i-1)i\left\{\left[\frac{ki}{h}\right]-\left[\frac{k(i-1)}{h}\right]\right\}+(h-1)h\left\{(k-1)-\left[\frac{k(h-1)}{h}\right]\right\}=\\
&=\sum_{i=1}^{h-1}(i-1)i\left[\frac{ki}{h}\right]-\sum_{i=1}^{h}(i-1)i\left[\frac{k(i-1)}{h}\right]+(h-1)h(k-1).
\end{aligned}$$

Druga vsota na koncu je enaka vsoti $\sum_{i=1}^{h-1}i(i+1)\left[\frac{ki}{h}\right]$, zato lahko obe vsoti združimo in po krajšem računu dobimo:

$$\sum_{j=1}^{k-1}\left[\frac{hj}{k}\right]\left(\left[\frac{hj}{k}\right]+1\right)=\sum_{i=1}^{h-1}\left[\frac{ki}{h}\right](i(i-1)-i(i+1))+(h-1)h(k-1)=$$

$$=-2\sum_{i=1}^{h-1}i\left(\frac{ki}{h}-\left(\left(\frac{ki}{h}\right)\right)-\frac{1}{2}\right)+(h-1)h(k-1)=$$

$$=-\frac{2k}{h}\sum_{i=1}^{h-1}i^2+2h\sum_{i=1}^{h-1}\frac{i}{h}\left(\left(\frac{ki}{h}\right)\right)+\sum_{i=1}^{h-1}i+(h-1)h(k-1)=$$

$$=2hs(k,h)-\frac{2k}{h}\sum_{i=1}^{h-1}i^2+\sum_{i=1}^{h-1}i+(h-1)h(k-1). \tag{11}$$

Pri tem smo v zadnji vrstici uporabili trditev 4.
Primerjava (9) in (11) nam sedaj pove:

$$2hs(h,k)+2hs(k,h)=$$

$$=\frac{h^2+1}{k^2}\sum_{j=1}^{k-1}j^2-\frac{1}{k}\sum_{j=1}^{k-1}j+\frac{2k}{h}\sum_{i=1}^{h-1}i^2-\sum_{i=1}^{h-1}i-(h-1)h(k-1) \tag{12}$$

oziroma

$$2h(s(h,k)+s(k,h))=\frac{h^2+1}{k^2}\cdot\frac{(k-1)k(2k-1)}{6}-\frac{1}{k}\cdot\frac{(k-1)k}{2}+$$
$$+\frac{2k}{h}\cdot\frac{(h-1)h(2h-1)}{6}-\frac{(h-1)h}{2}-(h-1)h(k-1).$$

Poenostavimo in dobimo:

$$12(s(h,k)+s(k,h))=-3+\frac{h}{k}+\frac{k}{h}+\frac{1}{hk}.$$ ∎

Kvadratni reciprocitetni zakon

Za izpeljavo splošnega kvadratnega reciprocitetnega zakona potrebujemo naslednjo lemo, ki jo navedimo brez dokaza.

Lema 6 (Posplošena Gaussova lema). *Naj bosta h in k tuji si naravni števili, pri čemer je k liho število. Naj pomeni m število najmanjših pozitivnih ostankov, večjih od $\frac{k}{2}$, pri deljenju števil hj, $j=1,2,\ldots,\frac{k-1}{2}$, s številom k. Tedaj velja:*

$$\left(\frac{h}{k}\right)=(-1)^m.$$

Dokaz je možno najti v knjigi [1], str. 144–148. Trditev je posplošitev Gaussove leme, ki je sestavni del dokaza klasičnega Gaussovega kvadratnega reciprocitetnega izreka (glej npr. [5]). Namesto lihega števila k, ki si je tuje s h, tam nastopa liho praštevilo p, ki ne deli h, ter Legendrov simbol namesto Jacobijevega.

Tudi naslednjo trditev navedimo brez dokaza.

Trditev 7. *Za liho naravno število k, naravno število h, ki si je tuje s k, in za Jacobijev simbol $\left(\frac{h}{k}\right)$ velja naslednja modularna enakost*

$$12ks(h,k) \equiv k + 1 - 2\left(\frac{h}{k}\right) \pmod 8. \tag{13}$$

Ideja dokaza je naslednja. Najprej lahko brez težav iz trditve 4 izpeljemo enakost

$$12ks(h,k) = 2h(k-1)(2k-1) - 12\sum_{j=1}^{k-1} j\left[\frac{hj}{k}\right] - 3k(k-1), \tag{14}$$

nato pa z uporabo posplošene Gaussove leme postopoma reduciramo desno stran po modulu 8 (podrobnosti dokaza glej npr. v [4], str. 30–35 ali v [7], str. 97–99).

Na podlagi predhodno zapisanega sedaj dokažimo izrek:

Izrek 8 (Kvadratni reciprocitetni zakon). *Naj bosta h in k lihi, tuji si celi števili. Tedaj za Jacobijeva simbola $\left(\frac{h}{k}\right)$ in $\left(\frac{k}{h}\right)$ velja:*

$$\left(\frac{h}{k}\right)\left(\frac{k}{h}\right) = (-1)^{\frac{h-1}{2}\cdot\frac{k-1}{2}}.$$

Dokaz. Iz enakosti (13) v trditvi 7 sklepamo, da je

$$12hk(s(h,k)+s(k,h)) \equiv 2hk + h + k - 2\left(h\left(\frac{h}{k}\right) + k\left(\frac{k}{h}\right)\right) \pmod 8.$$

Po drugi strani pa po reciprocitetni formuli (6) velja

$$12hk(s(h,k)+s(k,h)) = -3kh + h^2 + k^2 + 1.$$

Ker pa sta h in k liha, je

$$h^2 \equiv 1 \pmod 8 \quad \text{in} \quad k^2 \equiv 1 \pmod 8$$

in zato

$$12hk(s(h,k)+s(k,h)) \equiv -3kh + 3 \pmod 8.$$

Po primerjavi dobimo:

$$5hk + h + k - 3 \equiv 2\left(h\left(\frac{h}{k}\right) + k\left(\frac{k}{h}\right)\right) \pmod 8.$$

To kongruenco preoblikujmo v obliko, ki jo zahteva kvadratni reciprocitetni zakon. Za vrednosti k in h upoštevajmo več možnosti glede deljivosti s številom 4.

1. Naj bo k oblike $\boldsymbol{k = 4m + 1}$, $\boldsymbol{m} \in \mathbb{Z}$.

   Tako je

   $$5h(4m+1)+h+4m+1-3 \equiv 2\left(h\left(\frac{h}{k}\right) + (4m+1)\left(\frac{k}{h}\right)\right) \pmod 8,$$

   kar lahko preuredimo v

   $$(h+1)(2m-1) \equiv h\left(\frac{h}{k}\right) + \left(\frac{k}{h}\right) \pmod 4.$$

   Ker pa je h lih, je $h+1$ sod in zato $2m(h+1) \equiv 0 \pmod 4$, dobimo

   $$-h - 1 \equiv h\left(\frac{h}{k}\right) + \left(\frac{k}{h}\right) \pmod 4$$

   oziroma

   $$h\left(1 + \left(\frac{h}{k}\right)\right) + \left(1 + \left(\frac{k}{h}\right)\right) \equiv 0 \pmod 4. \tag{15}$$

   (a) Naj bo še $\boldsymbol{h \equiv 1 \pmod 4}$. Tedaj iz (15) izpeljemo kongruenco

   $$\left(\frac{h}{k}\right) + \left(\frac{k}{h}\right) \equiv 2 \pmod 4.$$

   Ker lahko $\left(\frac{h}{k}\right)$ in $\left(\frac{k}{h}\right)$ zavzameta le vrednosti ± 1, mora nujno veljati

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

   (b) Če pa je $\boldsymbol{h \equiv -1 \pmod 4}$, neposredno izpeljemo $\left(\frac{h}{k}\right) \equiv \left(\frac{k}{h}\right) \pmod 4$ oziroma $\left(\frac{h}{k}\right) = \left(\frac{k}{h}\right)$.

V obeh primerih je torej

$$\left(\frac{h}{k}\right)\left(\frac{k}{h}\right) = 1 = (-1)^{\frac{h-1}{2}\cdot\frac{k-1}{2}}.$$

2. Naj bo k oblike $\boldsymbol{k = 4m-1}$, $\boldsymbol{m} \in \mathbb{Z}$. Tedaj je

$$5h(4m-1)+h+4m-1-3 \equiv 2\left(h\left(\frac{h}{k}\right)+(4m-1)\left(\frac{k}{h}\right)\right) \pmod 8,$$

kar lahko preuredimo v

$$(h+1)(2m-2) \equiv h\left(\frac{h}{k}\right)-\left(\frac{k}{h}\right) \pmod 4.$$

Spet zaradi lihosti števila h velja $2m(h+1) \equiv 0 \pmod 4$ in zato

$$-2h-2 \equiv h\left(\frac{h}{k}\right)-\left(\frac{k}{h}\right) \pmod 4$$

oziroma

$$h\left(2+\left(\frac{h}{k}\right)\right)+\left(2-\left(\frac{k}{h}\right)\right) \equiv 0 \pmod 4. \tag{16}$$

(a) V primeru $\boldsymbol{h \equiv 1 \pmod 4}$ iz (16) takoj dobimo $\left(\frac{h}{k}\right) \equiv \left(\frac{k}{h}\right) \pmod 4$ oziroma

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

(b) Če pa je $\boldsymbol{h \equiv -1 \pmod 4}$, velja $\left(\frac{h}{k}\right)+\left(\frac{k}{h}\right) \equiv 0 \pmod 4$, torej $\left(\frac{h}{k}\right) = -\left(\frac{k}{h}\right)$. V primeru (a) je rezultat produkta torej enak 1, v (b) pa -1, kar lahko v eni vrstici zapišemo kot

$$\left(\frac{h}{k}\right)\left(\frac{k}{h}\right) = (-1)^{\frac{h-1}{2}\cdot\frac{k-1}{2}}.$$

Tako smo dokazali želeno. ∎

Sklep

Z Dedekindovimi vsotami se je kasneje ukvarjalo še veliko matematikov, ki so osnovno definicijo prilagajali svojim potrebam. Tako lahko Dedekindove vsote, poleg omenjene, zapišemo še v več drugih oblikah. Navedimo dva taka možna zapisa, veljavna za tuji si naravni števili h in k (izpeljavo najdemo npr. v [4]):

1. Trigonometrična oblika:

$$s(h,k) = \frac{1}{4k} \sum_{j=1}^{k-1} \cot\left(\frac{j\pi}{k}\right) \cot\left(\frac{jh\pi}{k}\right).$$

2. Kompleksna oblika:

$$s(h,k) = -\frac{1}{k} \sum_{\omega} \frac{1}{(1-\omega^h)(1-\omega)} + \frac{k-1}{4k},$$

kjer seštevamo po vseh k-tih korenih enote ω, različnih od 1.

Dedekindove vsote so pomembne same zase kot posebne aritmetične funkcije s številnimi lepimi lastnostmi in prav tako tudi v povezavi z drugimi področji matematike, npr. s trigonometričnimi funkcijami, s številom celoštevilskih točk v poliedrih v geometriji števil, z Dedekindovo funkcijo *eta* v teoriji eliptičnih funkcij, s teorijo enakomerne porazdelitve, s teorijo particij itd. (primerjaj npr. [4]). Raziskovanje Dedekindovih vsot je še danes zelo živo, saj v matematični bazi podatkov MathSciNet od leta 2000 naprej obstaja več kot 200 člankov na to temo.

Za pomoč pri delu s tem člankom bi se želela zahvaliti dr. Urošu Milutinoviću in dr. Milanu Hladniku.

LITERATURA

[1] P. Bachmann, *Die Elemente der Zahlentheorie*, Teubner, Leipzig, 1892.

[2] R. Dedekind, *Erläuterungen zu zwei Fragmenten von Riemann* Riemann's Gesammelte Math. Werke (1892), 466–478, Dedekind's Gesammelte Math. Werke (1930), 159–173.

[3] E. Grosswald, *Topics from the Theory of Numbers*, Birkhäuser, Boston, 1984.

[4] H. Rademacher in E. Grosswald, *Dedekind sums*, Math. Association of America, 1972.

[5] T. Peklar, *Varianta dokaza kvadratnega recipročnostnega zakona*, Obzornik mat. fiz. **36** (1989), 129–133.

[6] B. Riemann, *Fragmente über die Grenzfälle der elliptischen Modulfunctionen*, Gesammelte Math. Werke, Dover, New York, 1953.

[7] R. Renko, *Dedekindove vsote*, magistrsko delo, Fakulteta za naravoslovje in matematiko Maribor, Univerza v Mariboru, Maribor, 2008.