Predavanje 10

GAUSOV ZAKON KVADRATNE RECIPROČNOSTI

U prethodnom predavanju videli smo da se za svaki ceo broj a takav da $p \nmid a$ (gde je $p > 2$ fiksiran prost broj) Ležandrov simbol (a/p) može izraziti, na osnovu faktorizacije na proste faktore $a = (\pm 1)2^{\alpha_0} q_1^{\alpha_1} \cdots q_k^{\alpha_k}$, kao

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{\alpha_0}\left(\frac{q_1}{p}\right)^{\alpha_1}\cdots\left(\frac{q_k}{p}\right)^{\alpha_k},$$

gde su prosti brojevi q_i neparni i različiti od p. (Zapravo, gornji izraz se može dodatno pojednostaviti primedbom da se faktori kod kojih je odgovarajući eksponent α_i paran mogu brisati, dok se neparni eksponenti mogu zameniti sa 1. Ista ova primedba povlači da važi $(k^2 a/p) = (a/p)$ ukoliko $p \nmid k$.) To u prvi plan izbacuje značaj izračunavanja vrednosti simbola $(2/p)$ i (q/p), gde je $q \neq p$ neparan prost broj. U ostvarenju tog cilja ključnu ulogu igra sledeće tvrđenje.

Lema 10.1 (Gausova lema)**.** *Neka je $a \in \mathbb{Z}$ takav da je $p \nmid a$. Posmatrajmo ostatke koje brojevi*

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

daju pri deljenju sa p; neka među njima ima v onih koji su veći od $p/2$. Tada je

$$\left(\frac{a}{p}\right) = (-1)^v.$$

Dokaz. Označimo sa $r_1, \ldots, r_v$ ostatke veće od $p/2$ koje daju posmatrani brojevi, dok su $s_1, \ldots, s_m$ preostali ostaci (oni koji su manji od $p/2$). Imamo da je $v + m = (p-1)/2$. Svi uočeni ostaci su međusobno različiti (po Tvrđenju 4.6) i nijedan od njih nije 0.

Posmatrajmo sada brojeve $p - r_i$, $1 \leqslant i \leqslant v$. Oni su svi međusobno različiti, manji od $p/2$, i nijedan od njih nije 0. Štaviše, tvrdimo da nijedan od njih nije jednak nekom od s_j, $1 \leqslant j \leqslant m$. U suprotnom, imali bismo $p - r_i = s_j$ za neke indekse i, j, odnosno $r_i + s_j = p$, pa kako je

$$r_i \equiv ka \pmod{p}, \quad s_j \equiv \ell a \pmod{p}$$

za neke $1 \leqslant k, \ell \leqslant (p-1)/2$, sledilo bi da $p \mid ka + \ell a = (k+\ell)a$. Međutim, ovo je nemoguće, jer $p \nmid a$ i $2 \leqslant k + \ell \leqslant p - 1 < p$.

Dakle, brojevi $p - r_1, \ldots, p - r_v, s_1, \ldots, s_m$ su međusobno različiti, manji od $p/2$ i različiti od 0, pa kako ih ima tačno $(p-1)/2$, sledi da su u pitanju upravo brojevi $1, 2, \ldots, (p-1)/2$ u nekoj permutaciji. Zbog toga je

$$(p - r_1)\cdots(p - r_v)s_1 \cdots s_m = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!\,,$$

pa sledi

$$\left(\frac{p-1}{2}\right)! \equiv (-r_1)\cdots(-r_v)s_1\cdots s_m = (-1)^v r_1\cdots r_v s_1\cdots s_m$$
$$\equiv (-1)^v \cdot a\cdot(2a)\cdots\left(\frac{p-1}{2}\,a\right) = (-1)^v a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \pmod p.$$

Pošto $p \nmid ((p-1)/2)!$, ova kongruencija se sme skratiti sa $((p-1)/2)!$, pa dobijamo da je $1 \equiv (-1)^v a^{(p-1)/2} \pmod p$, odnosno

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

kao što se i tražilo. □

Na osnovu Gausove leme se sada može ustanoviti za koje proste module p je 2 kvadratni ostatak.

Tvrđenje 10.2.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{ako je } p \equiv \pm 1 \pmod 8, \\ -1 & \textit{ako je } p \equiv \pm 3 \pmod 8. \end{cases}$$

Napomena. Za neparne (ne nužno proste) brojeve p uvek važi da $8 \mid p^2 - 1$. Primetimo da $16 \mid p^2 - 1$ (tj. $(p^2-1)/8$ je paran broj) ako i samo ako je $p \equiv \pm 1 \pmod 8$; zato se prethodno tvrđenje u kompaktnijem vidu može zapisati kao

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

Dokaz. Primenjujemo Gausovu lemu za slučaj $a = 2$: dobijamo da je

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

gde je v broj ostataka većih od $p/2$ koje brojevi $2, 4, \ldots, p-1$ daju pri deljenju sa p. Međutim, svi navedeni brojevi su manji od p, pa se poklapaju sa svojim (pozitivnim) ostacima $\bmod p$, tako da među njima ima $\lfloor (p-1)/4 \rfloor$ manjih od $p/2$, što znači da je

$$v = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor.$$

Prema tome, ako je $p = 8k \pm 1$ za neko k, tada je $v = 2k$, pa je $(2/p) = (-1)^{2k} = 1$. S druge strane, ako je $p = 8k+3$, tada je $v = 2k+1$, dok se za $p = 8k-3$ dobija $v = 2k-1$; u oba slučaja sledi $(2/p) = -1$. □

Takođe, za neparne vrednosti $a > 1$, jedna od posledica Gausove leme jeste sledeća njena reformulacija.

Lema 10.3. *Neka je a neparan broj takav da $p \nmid a$. Tada je*

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

gde je

$$t = \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{na}{p} \right\rfloor .$$

Dokaz. Koristićemo istu notaciju kao u dokazu Gausove leme kada su u pitanju ostaci $r_1, \ldots, r_v$, odnosno $s_1, \ldots, s_m$. Po Teoremi 1.6 (deljenje sa ostatkom) za svako n (iz skupa $\{1, 2, \ldots, (p-1)/2\}$) imamo

$$na = p \left\lfloor \frac{na}{p} \right\rfloor + r,$$

pri čemu je $0 < r < p$ ili jedan od ostataka r_i, ili pak jedan od ostataka s_j — kako n prolazi opisanim skupom, tako vrednosti r prolaze nizom ostataka $r_1, \ldots, r_v, s_1, \ldots, s_m$ u nekoj permutaciji. Zato je

$$\sum_{n=1}^{\frac{p-1}{2}} na = p \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{na}{p} \right\rfloor + \sum_{i=1}^{v} r_i + \sum_{j=1}^{m} s_j = pt + \sum_{i=1}^{v} r_i + \sum_{j=1}^{m} s_j.$$

S druge strane, videli smo u dokazu Gausove leme da je $p-r_1, \ldots, p-r_v, s_1, \ldots, s_m$ permutacija brojeva $1, 2, \ldots, (p-1)/2$, pa je stoga

$$\sum_{n=1}^{\frac{p-1}{2}} n = \sum_{i=1}^{v} (p - r_i) + \sum_{j=1}^{m} s_j = vp - \sum_{i=1}^{v} r_i + \sum_{j=1}^{m} s_j.$$

Oduzimanjem poslednje dve jednakosti, dobijamo

$$(a-1) \sum_{n=1}^{\frac{p-1}{2}} n = p(t-v) + 2 \sum_{i=1}^{v} r_i.$$

Kako su a i p neparni brojevi, zaključujemo da $t-v$ mora biti paran broj. Drugim rečima, t i v su iste parnosti, tj. $(-1)^t = (-1)^v$. Imajući u vidu Gausovu lemu, dokaz je okončan. □

Evo, dakle, Gausove "zlatne teoreme" (lat. *Aureum Theorema*).

Teorema 10.4 (Zakon kvadratne recipročnosti)**.** *Neka su $p, q > 2$ različiti prosti brojevi. Tada je*

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

odnosno

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

Drugim rečima, ako je bar jedan od prostih brojeva p, q oblika $4k+1$, tada je q kvadratni ostatak po modulu p ako i samo ako je p kvadratni ostatak po modulu q. U suprotnom, ako su oba broja p, q oblika $4k+3$, tada tačno jedna od kongruencija $x^2 \equiv q \pmod p$, $x^2 \equiv p \pmod q$ ima rešenja.

Dokaz. U realnoj ravni $\mathbb{R}^2$ posmatrajmo (otvoren) pravougaonik

$$\mathcal{A}_{p,q} = \left\{(x,y) : 0 < x < \frac{p}{2},\ 0 < y < \frac{q}{2}\right\}.$$

Skup tačaka sa celobrojnim koordinatama koje su sadržane u $\mathcal{A}_{p,q}$ je upravo

$$\mathcal{A}'_{p,q} = \left\{(x,y) : x,y \in \mathbb{Z},\ 1 \leqslant x \leqslant \frac{p-1}{2},\ 1 \leqslant y \leqslant \frac{q-1}{2}\right\}.$$

Ovaj deo celobrojne rešetke sadrži tačno

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

tačaka.

S druge strane, posmatrajmo pravu zadatu jednačinom

$$y = \frac{q}{p} \cdot x;$$

ona sadrži dijagonalu pravougaonika $\mathcal{A}_{p,q}$. Primetimo da se nijedna tačka skupa $\mathcal{A}'_{p,q}$ ne nalazi na ovoj pravoj, jer bi tada za neke x, y bilo $py = qx$, što je nemoguće zbog $0 < x < p$ i $0 < y < q$. Prema tome, ova prava razbija skup $\mathcal{A}'_{p,q}$ na dve klase: na skup tačaka $\mathcal{B}$ koje su "ispod" i skup tačaka $\mathcal{C}$ koje su "iznad" posmatrane prave.

Jasno, $(x,y) \in \mathcal{B}$ ako i samo ako $1 \leqslant y \leqslant \lfloor qx/p \rfloor$ i $1 \leqslant x \leqslant (p-1)/2$, pa je zato

$$|\mathcal{B}| = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{xq}{p} \right\rfloor;$$

slično $(x,y) \in \mathcal{C}$ ako i samo ako $1 \leqslant x \leqslant \lfloor py/q \rfloor$ i $1 \leqslant y \leqslant (q-1)/2$, zbog čega je

$$|\mathcal{C}| = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{yp}{q} \right\rfloor.$$

Sada imamo

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = |\mathcal{A}'_{p,q}| = |\mathcal{B} \cup \mathcal{C}| = |\mathcal{B}| + |\mathcal{C}| = \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{nq}{p} \right\rfloor + \sum_{n=1}^{\frac{q-1}{2}} \left\lfloor \frac{np}{q} \right\rfloor,$$

pa po prethodnoj lemi sledi

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

Q.E.D. □

Jakobijev simbol (a/m) definišemo kao proširenje Ležandrovog simbola kada je donji argument proizvoljan neparan broj $m > 1$. Naime, neka je $m = p_1 \cdots p_t$ razlaganje broja m na (ne nužno različite) proste faktore i neka je $(a,m) = 1$.

Tada definišemo da je vrednost Jakobijevog simbola (a/m) jednaka sledećem proizvodu vrednosti Ležandrovih simbola:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_t}\right).$$

Ako je sam broj m prost, tada se Jakobijev i Ležandrov simbol poklapaju, pa je upotreba identične notacije opravdana. Međutim, napomenimo da u opštem slučaju nije tačno da je jednačina $x^2 \equiv a \pmod m$ rešiva ako i sako ako je $(a/m) = 1$ (što pokazuje kontraprimer $a = 2$, $m = 15$); naime, a je kvadratni ostatak po modulu m ako i samo ako je kvadratni ostatak po modulu svakog prostog $p \mid m$, tj. ako i samo ako je $(a/p_i) = 1$ za sve $1 \leqslant i \leqslant t$. Zbog toga Jakobijev simbol treba pre shvatiti kao zgodno pomoćno sredstvo u izračunavanju vrednosti Ležandrovog simbola. Ta njegova uloga zasniva se na sledećem tvrđenju.

Tvrđenje 10.5. *Pretpostavimo da su u svim narednim Jakobijevim simbolima donji argumenti neparni brojevi veći od 1, dok su odgovarajući gornji i donji argumenti uzajamno prosti. Tada važi:*

(i) *Ako je* $a \equiv b \pmod m$, *tada je* $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

(ii) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$, $\quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

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

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

(v) $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{ako je } n \equiv m \equiv -1 \pmod 4, \\ \left(\frac{n}{m}\right) & \text{inače.} \end{cases}$

Dokaz. Sve navedene osobine slede iz definicije Jakobijevog simbola i odgovarajućih osobina Ležandrovog simbola. Ovde ćemo dati samo dokaz osobine (v), analogona zakona recipročnosti. Neka je $m = p_1 \cdots p_t$ i $n = q_1 \cdots q_s$, gde za sve i, j imamo $p_i \neq q_j$. Tada je

$$\left(\frac{m}{n}\right) = \prod_{\substack{1 \leqslant i \leqslant t \\ 1 \leqslant j \leqslant s}} \left(\frac{p_i}{q_j}\right), \qquad \left(\frac{n}{m}\right) = \prod_{\substack{1 \leqslant i \leqslant t \\ 1 \leqslant j \leqslant s}} \left(\frac{q_j}{p_i}\right).$$

Neka u nizu p_i, $1 \leqslant i \leqslant t$ (uključujući i moguća ponavljanja prostih faktora), ima tačno u brojeva oblika $4k - 1$, dok u nizu q_j, $1 \leqslant j \leqslant s$, ima v takvih brojeva. Tada ima tačno uv parova (p_i, q_j) za koje je $(p_i/q_j) = -(q_j/p_i)$, dok je za sve ostale parove $(p_i/q_j) = (q_j/p_i)$. Prema tome, $(m/n) = (-1)^{uv}(n/m)$, pa važi $(m/n) = -(n/m)$ ako i samo ako je uv neparan broj, tj. ako i samo ako su oba broja u, v neparna. Međutim, poslednji uslov je očito ekvivalentan sa $m \equiv n \equiv -1 \pmod 4$. □

Prednost Jakobijevog simbola se sastoji u tome što u njegovom izračunavanju ne moramo faktoristati m na proste faktore kako bismo našli vrednost (m/n).

Dovoljno je izraziti $m = 2^\alpha m'$, gde je m' neparan broj, pa na osnovu (ii) imamo $(m/n) = (m'/n)$ ako je α parno, odnosno $(m/n) = (2/n)(m'/n)$ ako je α neparno. Sada možemo nastaviti izračunavanje (m'/n) sukcesivnom primenom celobrojnog deljenja na osnovu (i), zakona recipročnosti (v) i prethodnog postupka izdvajanja najvišeg stepena dvojke, kako bismo (m/n) sveli na vrednost Jakobijevog simbola za veoma male argumente. Naravno, isti postupak omogućava da se i vrednost Ležandrovog simbola izračuna tumačeći ga kao Jakobijev.