ACTA UNIVERSITATIS SZEGEDIENSIS DE ATTILA JÓZSEF NOMINATAE
ACTA IUVENUM
SECTIO SCIENTIAE NATURALIS, SERIES NOVA, TOMUS I.
SZEGED, HUNGARIA, 1987

A LEGENDRE-SZIMBÓLUM EGY MEGKÖZELÍTÉSE CAYLEY REPREZENTÁCIÓS TÉTELÉNEK SEGÍTSÉGÉVEL. KVADRATIKUS RECIPROCITÁSI TÉTEL

ZÁDORI LÁSZLÓ

Általában a modulo p négyzetes maradékok kvadratikus reciprocitási tételének levezetéséhez nélkülözhetetlen eszköznek bizonyul az ún. Gauss-lemma, melynek segítségével explicit kifejezést lehet nyerni a Legendre-szimbólumra. A jelen cikk, felhasználva a csoportok Cayley-féle reprezentációját, egy, a négyzetes maradékok vizsgálatára különféle csoportok esetén is alkalmazható eljárással állítja elő ezt a formulát.

1. TÉTEL (CAYLEY). *Bármely G csoport esetén az a ϕ leképezés, amely minden $g\in G$ elemhez a G alaphalmazának azon ϕg permutációját rendeli, melyre $\phi g(x)=xg$, bármely $x\in G$-re, a G csoportnak egy, a G alaphalmazán ható permutációcsoportra való izomorfizmusa. A továbbiak során p mindig páratlan prímszámot jelöl.*

2. TÉTEL. *Tekintsük a modulo p redukált maradékok multiplikatív csoportjának a Cayley-tételben szereplő ϕ reprezentációját. A ϕ leképezésnél a négyzetes maradékok páros, a négyzetes nemmaradékok pedig páratlan permutációba mennek.*

BIZONYÍTÁS. Legyen $P=\{1,2,\ldots,p-1\}$. A bizonyításban felhasználjuk, hogy $(p-1)/2$ darab négyzetes maradék van modulo p, és pontosan ezek a gyökei az $x^{(p-1)/2}\equiv 1 \pmod p$ kongruenciának. Tetszőleges $a\in P$ elem képe a Cayley-leképezésnél:

$$\phi(a)=\begin{pmatrix}1\ldots i\ldots p-1\\ a\ldots ia\ldots (p-1)a\end{pmatrix},$$

ahol az ia $(i\in P)$ szorzatok modulo p értendők.

DEFINÍCIÓ. Azt mondjuk, hogy a az α kitevőhöz tartozik modulo p, ha $a^{\alpha}\equiv 1$, de α-nál kisebb pozitív egész kitevőre nem áll fenn a kongruencia mod p.

Tartozzon a az α kitevőhöz. Ha $i\in P$, akkor i a $\phi(a)$ permutáció páronként idegen ciklusokra bontásában egy α hosszúságú ciklusban szerepel, ugyanis ez a permutáció i-t elviszi ia-ba, ia-t ia^2-be és így tovább; mivel a α-hoz tartozik, $ia^{\alpha}\equiv i \pmod p$ és $0<\beta<\alpha$ esetén $ia^{\beta}\not\equiv i \pmod p$. Ezért $\phi(a)$ $(p-1)/\alpha$ darab α hosszú ciklusra bomlik.

a) Tegyük fel, hogy $a\in P$ négyzetes maradék. Ekkor $a^{(p-1)/2}\equiv 1 \pmod p$. Ebből következik, hogy α osztja $(p-1)/2$-t, és így $(p-1)/\alpha$ páros. Tehát $\phi(a)$ páros sok α hosszúságú ciklus szorzatára bomlik, s ezért páros permutáció.

Ahhoz, hogy a nemmaradékok páratlan permutációkra képződnek, elegendő volna megmutatni, hogy létezik $a\in P$, amelyre $\phi(a)$ páratlan permutáció. Ennek megmutatása azonban ugyanannyi energiát igényel, mint egy tetszőleges nemmaradékról megmutatni, hogy páratlan permutációra képződik le.

b) Tegyük fel, hogy $a\in P$ négyzetes nemmaradék. Ha $p-1=2^m(2k-1)$, akkor 2^m osztja α-t; ellenkező esetben $(p-1)/2\alpha$ egész lenne, és az $a^{\alpha}\equiv 1 \pmod p$ kongruencia mindkét oldalát $(p-1)/2\alpha$-adik hatványra emelve $a^{(p-1)/2}\equiv 1 \pmod p$ adódna, amiből a négyzetes maradék volta következne. Tehát $(p-1)/\alpha$ páratlan. Ekkor $\phi(a)$ páratlan sok páros ciklusból áll, s ezért páratlan permutáció.

Most definiáljuk az $(\frac{a}{p})$ Legendre-szimbólumot, ahol $(a,p)=1$.

DEFINÍCIÓ.

$$\left(\frac{a}{p}\right)=\begin{cases} 1, & \text{ha } \phi(a) \text{ páros} \\ -1, & \text{ha } \phi(a) \text{ páratlan.}\end{cases}$$

A 2. tétel közvetlen következménye: $(\frac{a}{p})=1$, ha a négyzetes maradék, $(\frac{a}{p})=-1$, ha a négyzetes nemmaradék. A 2. tétel segítségével a Legendre-szimbólum alapvető tulajdonságai is könnyen igazolhatók. Ehhez felhasználjuk, hogy a permutáció paritása megegyezik az inverziói számának paritásával. (Azt mondjuk, hogy az

$$\begin{pmatrix} 1 & 2 & \dots & p-1 \\ i_1 & i_2 & \dots & i_{p-1} \end{pmatrix}$$

permutációban i_k és i_ℓ inverziót alkot, ha $k<\ell$ és $i_k>i_\ell$.)

Ha $a\equiv b \pmod p$, akkor $(\frac{a}{p})=(\frac{b}{p})$ a definíció miatt teljesül.

$(\frac{1}{p})=1$, mert $\phi(1)$-ben az inverziók száma 0.

$(\frac{-1}{p})=(-1)^{(p-1)/2}$, ugyanis

$$\phi(-1)=\begin{pmatrix} 1 & 2 & \dots & p-1 \\ p-1 & p-2 & \dots & 1 \end{pmatrix},$$

s itt az inverziók száma $p-2+p-3+\dots+1=(p-1)(p-2)/2$. Mivel $p-2$ páratlan, $(p-1)/2\equiv(p-1)(p-2)/2 \pmod 2$.

Multiplikativitás: $(\frac{a}{p})\cdot(\frac{b}{p})=(\frac{ab}{p})$. Ez abból következik, hogy ha $\phi(a)$, $\phi(b)$ ellenkező paritásúak, akkor $\phi(a)\phi(b)=\phi(ab)$ páratlan, ha pedig $\phi(a)$, $\phi(b)$ azonos paritásúak, akkor $\phi(a)\phi(b)=\phi(ab)$ páros. Itt felhasználtuk, hogy ϕ műveletartó, és azt, hogy $c\equiv d \pmod p$ esetén $(\frac{c}{p})=(\frac{d}{p})$, ugyanis ab-t itt modulo p értjük.

$$(\frac{2}{p})=(-1)^{\frac{p^2-1}{8}}, \text{ mert}$$

$$\phi(2)=\begin{pmatrix} 1 & 2 & \dots & (p-1)/2 & (p-1)/2+1 & \dots & p-1 \\ 2 & 4 & \dots & p-1 & 1 & \dots & p-2 \end{pmatrix},$$

s itt az inverziók száma

$$(p-1)/2+(p-1)/2-1+(p-1)/2-2+\dots+1=\frac{((p-1)/2+1)((p-1)/2)}{2}=\frac{p^2-1}{8}.$$

A következő tételben olyan formulát vezetünk le az $(\frac{a}{p})$ szimbólumra, amely lehetővé teszi a kvadratikus reciprocitási tétel egyszerű bizonyítását.

3. TÉTEL

$$(\frac{a}{p})=(-1)^{\sum_{x=1}^{(p-1)/2}[2xa/p]}.$$

BIZONYÍTÁS. Mint korábban láttuk, bármely $a\in P$ elemre

$$\phi(a)=\begin{pmatrix}1 & 2 & 3 & \dots & p-1\\ a & 2a & 3a & \dots & (p-1)a\end{pmatrix},$$

ahol a képek modulo p értendők. Tehát $i\in P$ képe megegyezik $\{ia/p\}p$-vel, azaz ia p-vel való pozitív osztási maradékával. Ha $i<j$, akkor az $\{ia/p\}p$, $\{ja/p\}p$ elemek pontosan akkor vannak inverzióban, ha $\{ja/p\}p<\{ia/p\}p$, azaz ha $\{ja/p\}<\{ia/p\}$. Ez ekvivalens azzal, hogy $(j-i)a/p<[ja/p]-[ia/p]$, vagyis $[(j-i)a/p]<$ $<[ja/p]-[ia/p]$. Mivel tetszőleges α,β való számokra $[\alpha+\beta]-$ $-[\alpha]-[\beta]=0$ vagy 1, azt kapjuk, hogy abban az esetben, ha $\phi(i)$, $\phi(j)$ inverzióban vannak, akkor

$$[ja/p]-[ia/p]-[(j-i)a/p]=1,$$

ha pedig $\phi(i)$, $\phi(j)$ nincsenek inverzióban, akkor

$$[ja/p]-[ia/p]-[(j-i)a/p]=0.$$

Ezek szerint az inverziók száma

$$\lambda=\sum_{1\le i<j\le p-1}[ja/p]-[ia/p]-[(j-i)a/p].$$

λ-t három részletösszegre bontjuk. Az $S_1=\sum_{1\le i<j\le p-1}[ja/p]$ összegben, rögzített j-re $j-1$ darab j-nél kisebb i jön számításba, valamint $2\le j\le p-1$. Ezért $S_1=\sum_{j=1}^{p-1}(j-1)[ja/p]$ (a $j=1$ esetben ugyanis 0-val szorzunk). A páratlan j-khez tartozó tagokat kihagyhatjuk az összegből, hisz az csak modulo 2 érdekel bennünket. Így

$$S_1\equiv\sum_{x=1}^{(p-1)/2}(2x-1)[2xa/p]\equiv\sum_{x=1}^{(p-1)/2}[2xa/p]\pmod 2.$$

Tehát, ha a λ-t előállító többi tag összege kongruens 0-val modulo 2, akkor igaz a 3. tétel. A második részletösszeg $S_2=$ $=\sum_{1\le i<j\le p-1}[ia/p]$, ahol rögzített i-hez $p-1-i$ darab j tartozik, és $1\le i\le p-2$. Ezért $S_2=\sum_{i=1}^{p-2}(p-1-i)[ia/p]$. A harmadik összeg $S_3=$ $=\sum_{1\le i<j\le p-1}[(j-i)a/p]$, ahol rögzített d-hez $p-1-d$ darab olyan j,i pár tartozik, melyre $j-i=d$, és $1\le d\le p-2$. Ezért $S_3=\sum_{d=1}^{p-2}(p-1-d)\times$

$\times [da/p]$. Az S_2 és S_3 összegek megegyeznek, ezért összegük (-1)-szerese, amely a λ-ban szerepel, osztható 2-vel. Így a harmadik tételt bebizonyítottuk.

A kvadratikus reciprocitási tételt most már a harmadik tételben bizonyított formula alapján, a (qx, py) $(1 \leq x \leq (p-1)/2,$ $1 \leq y \leq (q-1)/2)$ pontok számát kétféleképpen megszámolva, a jól ismert módon kaphatjuk.

4. TÉTEL. *Tetszőleges p, q páratlan prímekre*

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

Zádori László
tudományos segédmunkatárs
MTA, Szeged, Somogyi u. 20. 6720