Elemrendek összege feloldható csoportokban

Szőnyi Laura

1. Bevezetés

A csoportokban az elemrendek összegét és szorzatát is vizsgálták már korábban, ezek közül az előbbit vizsgáltam Marcel Herzog, Patrizia Longobardi és Mercede Maj cikkéből kiindulva, illetve Herendi Zsolt szakdolgozatát is felhasználva.

2. Fontosabb előzetes eredmények

Jelölje C_n az n elemű ciklikus csoportot, $\Psi(G) = \sum_{g\in G} o(g)$ a G csoport elemrendjeinek összegét, n a G véges csoport rendjét.

Nem nehéz belátni, hogy $\Psi(G) < \Psi(C_n)$, amennyiben nem izomorf vele, de ennél többet is lehet tudni.

2.1. Tétel. *Ha G nem ciklikus, n rendű csoport, akkor $\Psi(G) \le \frac{7}{11}\Psi(C_n)$.*

Az állítás éles, ugyanis $n = 4k$ esetén $\Psi(C_{2k} \times C_2) = \frac{7}{11}\Psi(C_n)$.

Egyes esetekben ugyanakkor lehet még javítani a becslést.

2.2. Tétel. *Ha G nem ciklikus, n rendű csoport, q az n legkisebb prímosztója, akkor $\Psi(G) \le \frac{1}{q-1}\Psi(C_n)$.*

Látható, hogy páratlan rendű csoportoknál ez többet mond, mint az előző tétel, ugyanis ekkor $\Psi(G) \le \frac{1}{2}\Psi(C_n)$ biztosan teljesül, páros rendűekre viszont nem állít semmi újat.

Hasznos tudni az alábbi, egyszerű számolás után adódó képletet.

2.3. Tétel. *Ha $n = p^r$, azaz prímhatvány, akkor $\Psi(C_n) = \frac{p^{2r+1}+1}{p+1}$.*

Az Euler-féle φ-függvénnyel való kapcsolatáról a következőt állíthatjuk.

2.4. Tétel. *Legyen q az n legkisebb prímosztója. Ekkor $\Psi(G) \ge \frac{n}{q}\varphi(n)$.*

3. Az elemrendek összegének felső becslése

Könnyen látható, hogy a $\frac{\Psi(C_n)}{n\varphi(n)}$ kifejezés $n > 1$ esetén mindig nagyobb, mint 1, hiszen az n-nel relatív prím elemek mind n-edrendűek, továbbá $o(1) = 1$ miatt szigorú az egyenlőtlenség. Felvetődik a kérdés, hogy lehet-e felső korlátot mondani.

3.1. Tétel. $\frac{\Psi(C_n)}{n\varphi(n)} < 2,1666$

Bizonyítás. Rövid számolással adódik az alábbi becslés.

$$\frac{\Psi(C_n)}{n\varphi(n)} = \prod_{p|n} \frac{\Psi(C_{p^{r_p}})}{p^{r_p}\varphi(p^{r_p})} = \prod_{p|n} \frac{p^{2r_p+1}+1}{(p^2-1)p^{2r_p-1}} \leq \prod_{p|n} \frac{p^3+1}{p^3-p} = \prod_{p|n}(1+\frac{p+1}{p^3-p}) \leq e^{\sum_{p|n}\frac{p+1}{p^3-p}}$$

Ekkor a $\sum_{p\ prím} \frac{p+1}{p^3-p}$ kifejezést lehet tovább vizsgálni.

$$\sum_{p\ prím} \frac{p+1}{p^3-p} = \sum_{p\ prím} \frac{1}{p^2-1} + \sum_{p\ prím} \frac{1}{p^3-p}$$

Jelölje $P(s) = \sum_{p\ prím} \frac{1}{p^s}$ a prím zeta-függvényt, ez minden $s > 1$-re konvergens. Ennek használatával adódik az alábbi.

$$\frac{1}{p^2-1} = \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + \dots$$

tehát

$$\sum_{p\ prím} \frac{1}{p^2-1} = P(2) + P(4) + P(6) + \dots$$

Hasonlóan

$$\frac{1}{p^3-p} = \frac{1}{p^3} + \frac{1}{p^5} + \frac{1}{p^7} + \dots$$

így

$$\sum_{p\ prím} \frac{1}{p^3-p} = P(3) + P(5) + P(7) + \dots$$

Ebből következik, hogy

$$\sum_{p\ prím} \frac{p+1}{p^3-p} = P(2) + P(3) + P(4) + P(5) + P(6) + P(7) + \dots = 0,7731566690\dots$$

Így

$$\frac{\Psi(C_n)}{n\varphi(n)} \leq e^{\sum_{p|n} \frac{p+1}{p^3-p}} < e^{\sum_{p\ prím} \frac{p+1}{p^3-p}} = 2,16659469\ldots$$

□

Ugyanakkor ennél több is igaz, ez látható az alábbiakban.

3.2. Tétel. $\frac{\Psi(C_n)}{n\varphi(n)} < 1,9436$

Bizonyítás. Az iménti számolás elejét is felhasználva adódik az alábbi.

$$\frac{\Psi(C_n)}{n\varphi(n)} \leq \prod_{p\ prím} \frac{p^3+1}{p^3-p} = \prod_{p\ prím} \frac{p^6-1}{(p^3-1)(p^2-1)p} = \prod_{p\ prím} \frac{1-\frac{1}{p^6}}{(1-\frac{1}{p^3})(1-\frac{1}{p^2})} =$$

$$= \frac{\prod(1-\frac{1}{p^6})}{\prod(1-\frac{1}{p^3})\prod(1-\frac{1}{p^2})}$$

A mértani sor összegképletéből adódik az alábbi számítás.

$$\prod \frac{1}{1-\frac{1}{p^k}} = \prod(1+\frac{1}{p^k}+\frac{1}{p^{2k}}+\ldots) = \sum_{n=1}^{\infty} \frac{1}{n^k} = \zeta(k)$$

Tehát az eredeti kifejezés az alábbi alakra hozható.

$$\frac{\Psi(C_n)}{n\varphi(n)} \leq \frac{\prod(1-\frac{1}{p^6})}{\prod(1-\frac{1}{p^3})\prod(1-\frac{1}{p^2})} = \frac{\zeta(3)\zeta(2)}{\zeta(6)} = 1,943596436820759\ldots$$

□

Látható, hogy ez az eredmény tovább már nem javítható, mert az $n_i = p_1 \cdot p_2 \cdot \ldots \cdot p_i$ sorozattal, ahol p_i az i. prím, $\frac{\Psi(C_{n_i})}{n_i\varphi(n_i)}$ pont ezen számhoz konvergál, n_{1229}-re már $1,943577\ldots$ a tört értéke.

Ez az eredmény azt is jelenti, hogy nem ciklikus, páratlan elemrendű csoport esetén $\Psi(G) < n\varphi(n)$, páros elemrendű csoport esetén pedig $\Psi(G) < 1,24n\varphi(n)$.

Alsó becslést tekintve a $n = 2^k$ esetből látható, hogy $\Psi((C_2)^k) = 2n-1$, ennél jobbat nem lehet mondani, mert egy elem rendje 1, az összes többi elem rendje pedig legalább 2, tehát $\Psi(G) \geq 2n-1$.

4. Prímhatvány rendű csoportok prímnégyzet indexű ciklikus normálosztóval

Herendi Zsolt szakdolgozatának végén volt szó azon prímhatvány rendű csoportok elemrend-összegéről, ahol van prímindexű ciklikus részcsoport. A következőkben a prímnégyzet-indexű ciklikus részcsoporttal rendelkező prímhatvány csoportokról lesz szó.

Legyen $|G| = p^n$ ahol $n > 2$, p páratlan prím, $H < G$, $|H| = p^{n-2}$, ahol H maximális ciklikus részcsoport. A H csoport normalizátorát $N_G(H)$-val jelölve ha $N_G(H) = G$, akkor $H \lhd G$, azaz H normálosztó G-ben. Ellenkező esetben van egy M maximális részcsoport, amire $H \lhd M \lhd G$ $(M = N_G(H))$. Ekkor az M csoport p^{n-1} elemű, de nem ciklikus. Mivel az M a H csoport normalizátora, és nem egyenlőek, ezért egy $g \in G$ elemmel konjugálva $g^{-1}Hg \lhd M$, $|M : H \cap g^{-1}Hg| = p^2$ (amennyiben $H \neq g^{-1}Hg$), $H \cap g^{-1}Hg \leq Z(M)$. Tegyük fel, hogy M nem Abel. Mivel M nem lehet ciklikus, így $M \simeq C_{p^{n-2}} \times C_p = \langle u, v \mid u^{p^{n-2}} = 1, v^p = 1 \rangle$.

$$\Psi(M) = (C_{p^{n-2}}) \cdot p + (p-1) \cdot (p-1) = \frac{p^{2n-2} + p}{p+1} + (p-1)^2 = \frac{p^{2n-2} + p^3 - p^2 + 1}{p+1}$$

Tekintsük az M csoport egy p-rendű α automorfizmusát. $u^\alpha = u^x v^y$ ahol $p \nmid x$, $v^\alpha = u^z v^t$ ahol $p^{n-3} \mid z$, $p \nmid t$. Az x és z értékeket modulo p^{n-2}, az y és t értékeket modulo p nézzük.

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix}^p \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Ebből következőleg $x^p \equiv 1 \bmod p$, azaz $x \equiv 1 \bmod p$, illetve hasonlóan $t \equiv 1 \bmod p$.

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} x-1 & y \\ z & 0 \end{bmatrix}$$

A fentit felhasználva adódik az alábbi egyenlőség.

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix}^p \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + p \begin{bmatrix} x-1 & y \\ z & 0 \end{bmatrix} + \binom{p}{2} \begin{bmatrix} (x-1)^2 & 0 \\ 0 & 0 \end{bmatrix} + \ldots + \begin{bmatrix} (x-1)^p & 0 \\ 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} x^p & 0 \\ 0 & 1 \end{bmatrix}$$

Tehát $x^p \equiv 1 \bmod p^{n-2}$, így $x \equiv 1 \bmod p^{n-3}$. Innentől legyen x, y, t, z új, a fenti megkötések nélkül, így $u^\alpha = u^{1+p^{n-3}x} v^y$, $v^\alpha = u^{p^{n-3}z} v$.

$$\begin{bmatrix} 1 + p^{n-3}x & y \\ p^{n-3}z & 1 \end{bmatrix}^p \equiv \begin{bmatrix} 1 + p^{n-2}x + \binom{p}{2} p^{n-3} yz & py \\ p^{n-2}z & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

A fentiek szerint a G csoportra
$G \simeq \langle u, v, w \mid uv = vu, u^{p^{n-2}} = 1, v^p = 1, w^{-1}uw = u^{1+p^{n-3}x} v^y, w^{-1}vw = u^{p^{n-3}z} v \rangle$ teljesül. Továbbá tetszőleges $a \in M$-re $(wa)^p = w^p w^{-(p-1)} a w^{p-1} w^{-(p-2)} \ldots w^3 w^{-2} a w^2 w^{-1} a w a = w^p a^p$.

Tetszőleges k, l-re $(u^k v^l)^\alpha = u^k v^l$ teljesül, ha $u^{p^{n-3}(kx+lz)} v^{ky} = 1$.

Első esetben legyen $y \neq 0$, $y = 1$, és $z = 0$. Ekkor $p \mid k$, azaz $w^{-1}uw = u^{1+p^{n-3}x}v$, $w^{-1}vw = v$, $w^p \in \langle u^p, v \rangle$. Ez ugyan arra vezethető vissza, mint az ötödik eset.

Második esetben legyen $y = 1$, $z \neq 0$. Ekkor $p \mid k, p \mid l$, azaz $w^{-1}uw = u^{1+p^{n-3}x}v$, $w^{-1}vw = u^{p^{n-3}z}v$, $w^p \in \langle u^p \rangle$, ahol feltehető, hogy $w^p = 1$. v helyett $u^{p^{n-3}t}v$-t véve $w^{-1}uw = uv$. A $z = 1, \ldots, p-1$ esetek mindegyike ugyan azt az elemrend-összeget adja, így legyen $z = 1$. Ekkor a harmadik esethez hasonlóan $\Psi(G) = \Psi(M) \cdot p + (p-1) \cdot (p-1) = \frac{p^{2n-1}+p^4-p^2+1}{p+1}$.

Harmadik esetben legyen $y = 0, x = 0$. Ekkor $p \mid l$, azaz $l = 0$, azaz $w^{-1}uw = u$, $w^{-1}vw = u^{p^{n-3}z}v$ és $w^p = u^k$ határozza meg a csoportot. Legyen $z = 1$. Ekkor $k = 1, \ldots, p-1$ esetekben $o(w) = p^{n-1}$, vagyis ez az eset nem felel meg, így $k = 0$. Tehát $w^{-1}uw = u$, $w^{-1}vw = u^{p^{n-3}}v$, $w^p = 1$. Ekkor $wu = uw$, $vw = wu^{p^{n-3}}v$, illetve tudjuk, hogy $(wa)^p = w^p a^p$ ha $a \in M$, azaz w valamely hatványával bárhogyan szorozva egy M-beli elemet, melynek rendje legalább p (azaz nem 1) az elem rendje megmarad. Így ez esetben $\Psi(G) = \Psi(M) \cdot p + (p-1) \cdot (p-1) = \frac{p^{2n-1}+p^4-p^2+1}{p+1}$.

Negyedik esetben legyen $y = 0, x = 1, z \neq 0$. Ekkor $k \equiv -lz$ modulo p. Feltehető, hogy $l = 1$, ekkor $o(u^{-z}v) = p^{n-2}$, $\langle u^{-z}v \rangle$ a fixen maradó elemek. Így $w^{-1}uw = u^{1+p^{n-3}}$, $w^{-1}vw = u^{p^{n-3}z}v$, $w^p = 1$, ahol $z \in \{1, \ldots, p-1\}$. Ha v-t lecseréljük egy megfelelő v^t-re, akkor elérhető, hogy minden más megtartásával $z = 1$ legyen, ekkor a fix részcsoport $\langle u^{-1}v \rangle$. Ha u helyett vesszük uv^{-1}-t, akkor ugyan azt kapjuk, mint a harmadik esetben.

Ötödik esetben legyen $y = 0, x = 1, z = 0$. Ekkor $p \mid k$, azaz $w^{-1}uw = u^{1+p^{n-3}}$, $w^{-1}vw = v$, $w^p \in \langle u^p, v \rangle$. Feltehető, hogy $w^p \in \langle v \rangle$, azaz vagy $o(w) = p^2$, és elérhető, hogy $v = w^p$ legyen, vagy pedig $\langle u, w \rangle \times \langle v \rangle$ a keresett csoport. Előbbi esetben egy M-beli elem rendje w walamely hatványával bárhogyan szorozva megmarad, ha legalább annyi a rendje, mint a w adott hatványának, $w^p = v$ miatt w legfeljebb $p-1$-edik hatványon van, vagyis $\Psi(G) = \Psi(M) \cdot p + (p-1) \cdot (p^2-1) + (p-1) \cdot (p-1) \cdot (p+1) \cdot (p^2-p) = \frac{p^{2n-1}+p^6-p^5+p^3-p^2+1}{p+1}$. Utóbbi esetben ismét ugyan az a számolás mutatja meg G elemrend-összegét, mint a harmadik pontban, azaz $\Psi(G) = \Psi(M) \cdot p + (p-1) \cdot (p-1) = \frac{p^{2n-1}+p^4-p^2+1}{p+1}$.

Így összesen két különböző elemrend-összeget kaptunk. $\Psi(C_{p^n}) = \frac{p^{2n+1}+1}{p+1}$-vel összehasonlítva az alábbiakat kapjuk:

$$\lim_{n\to\infty} \frac{\Psi(G)}{\Psi(C_{p^n})} = \lim_{n\to\infty} \frac{\frac{p^{2n-1}+p^4-p^2+1}{p+1}}{\frac{p^{2n+1}+1}{p+1}} = \frac{1}{p^2}$$

illetve

$$\lim_{n\to\infty} \frac{\Psi(G)}{\Psi(C_{p^n})} = \lim_{n\to\infty} \frac{\frac{p^{2n-1}+p^6-p^5+p^3-p^2+1}{p+1}}{\frac{p^{2n+1}+1}{p+1}} = \frac{1}{p^2}$$

Tehát minden esetben $\Psi(G)$ értéke körülbelül $\frac{1}{p^3}\Psi(C_{p^n})$.

5. Irodalomjegyzék

Marcel Herzog, Patrizia Longobardi, Mercede Maj. *An exact upper bound for sums of element orders in non-cyclic finite groups*. https://arxiv.org/pdf/1610.03669.pdf

Herendi Zsolt. *Elemrendek összege csoportokban*.
https://web.cs.elte.hu/blobs/diplomamunkak/msc_mat/2021/herendi_zsolt.pdf