DIREKT SZORZATRA NEM BONTHATÓ CSOPORTOK RENDJÉRŐL

ERDŐS PÁL és PÁLFY PÉTER PÁL

Ebben a dolgozatban *felbonthatatlan*nak fogunk nevezni egy csoportot, ha nem bontható két valódi részcsoportjának direkt szorzatára. C. Sudler [7] vetette föl a kérdést, hogy mely n számokra létezik n-edrendű felbonthatatlan csoport. Ha n páros, akkor könnyű ilyen csoportot találni (1. Állítás). Ezzel szemben dolgozatunk fő eredménye (7. Tétel) azt mondja ki, hogy *majdnem minden* páratlan n számra minden n-edrendű csoport valódi részcsoportok direkt szorzatára bontható, azaz azoknak a páratlan n számoknak a halmaza, amelyekhez van n-edrendű felbonthatatlan csoport, nulla sűrűségű.

A bizonyításban a csoportelmélet és a számelmélet ötvöződik. Mindkét területről jól ismert eredményeket és gyakran alkalmazott módszereket fogunk felhasználni. Ám ami az egyik terület ismerőjének kézenfekvő, azt a másik terület specialistáinak kedvéért igyekeztünk részletezni.

A vizsgált csoportok mindig végesek; p és q mindig prímet, C, c_1, ... abszolút konstansokat jelöl.

1. Állítás. *Ha* $n=2^k m$, m *páratlan*, $k \geqq 1$, *akkor a*

$$G = \langle a, b \mid a^m = 1,\ b^{2^k} = 1,\ b^{-1}ab = a^{-1} \rangle$$

definiáló relációkkal megadott csoport felbonthatatlan és rendje n.

Bizonyítás. Tegyük föl, hogy $G=G_1 \times G_2$, és legyen $a=a_1 a_2$, $b=b_1 b_2$, a_i, $b_i \in G_i$ $(i=1, 2)$. Mivel b rendje b_1 és b_2 rendjének legkisebb közös többszöröse, ezért — mondjuk — b_1 rendje is 2^k. Ekkor 2^k osztja G_1 rendjét, így G_2 páratlan rendű és $b_2=1$. A $b^{-1}ab=a^{-1}$ relációból azt kapjuk, hogy $(b_1^{-1}a_1 b_1)a_2 = a_1^{-1}a_2^{-1}$, ahonnan $a_2^2=1$. Ám láttuk, hogy $|G_2|$ páratlan, ezért $a_2=1$. Tehát $G_2=1$, így G-nek csak triviális felbontása van.

A továbbiakban — ha szükségünk lesz rá — mindig feltehetjük, hogy n páratlan. Nehéznek látszik pontos feltételt adni arra, hogy mely páratlan számokra létezik ilyen rendű felbonthatatlan csoport. A dolgozat végén bizonyítás nélkül közlünk két erre vonatkozó részeredményt. Ezekből következik, hogy például van $3 \cdot 7$ és $7 \cdot 29$ rendű, de nincs $3 \cdot 7 \cdot 29$ rendű felbonthatatlan csoport; van $3^5 \cdot 11$ és 3^6 rendű, de nincs $3^6 \cdot 11$ rendű felbonthatatlan csoport. Ezért azzal a könnyebben kezelhető kérdéssel fogunk foglalkozni, hogy mikor lehet minden n-edrendű csoportot egységesen direkt szorzatra bontani, azaz mikor létezik olyan $n=n_1 n_2$ $(n_1, n_2 > 1)$ faktorizáció, hogy minden n-edrendű csoport egy n_1-edrendű és egy n_2-edrendű részcsoportjának direkt szorzata. Először azt az esetet vizsgáljuk, amikor n_1 prímszám.

2. Segédtétel. *Legyen $p|n$, p prím. Akkor és csak akkor lehet minden n-edrendű csoportot egy p-edrendű és egy n/p-edrendű részcsoportjának direkt szorzatára bontani, ha (i) $p^2 \nmid n$, (ii) nincs olyan $q^k|n$ (q prím, $k \geqq 1$), amelyre $p|q^k-1$, és (iii) nincs olyan $q|n$ prím, amelyre $q|p-1$.*

Bizonyítás. A feltételek szükségességét a következő csoportok mutatják: (i) az n-edrendű ciklikus csoport, C_n; (ii) $\{x \to ax+b \mid a, b \in GF(q^k),\ a^p=1\} \times C_{n/pq^k}$; (iii) $\{x \to ax+b \mid a, b \in GF(p),\ a^q=1\} \times C_{n/pq}$.

Tegyük most föl, hogy $p|n$ és teljesülnek az (i), (ii), (iii) feltételek. Legyen G egy n-edrendű csoport, P egy Sylow p-részcsoport G-ben. Az (i) feltétel folytán $|P|=p$. A P részcsoport G-beli $N_G(P)$ normalizátorának elemeivel való konjugálások P-nek automorfizmusait indukálják. P automorfizmuscsoportja $p-1$ elemű, ezért a (iii) feltétel miatt $N_G(P)$ minden eleme az identikus automorfizmust indukálja, azaz centralizálja P-t. Burnside nevezetes tétele (lásd [3], 252. old.) szerint ekkor létezik G-ben olyan K normálosztó, hogy $KP=G$ és $K \cap P=1$, azaz $|K|=n/p$.

Vegyük n-nek egy p-től különböző q prímosztóját. Mivel K rendje p-vel nem osztható, ezért van K-nak olyan Q Sylow q-részcsoportja, amelyet P normalizál (lásd [3], 224. old.). Ha $|Q|=q^m$, akkor Q automorfizmuscsoportjának rendje osztója $q^{m(m-1)/2}(q^m-1)(q^{m-1}-1)\ldots(q^2-1)(q-1)$-nek (lásd [5], 275. old.), ám ez a (ii) feltétel szerint p-vel nem osztható, így P elemenként felcserélhető Q-val, $Q \leqq C_K(P)$. Tehát $C_K(P)$ K rendjének minden q prímosztójához tartalmaz egy Sylow q-részcsoportot, ennélfogva $C_K(P)=K$, és így valóban $G=P \times K$.

Az első két feltételnek eleget tevő prímosztót általában igen könnyen találunk.

3. Segédtétel. *Majdnem minden n szám minden* log log *n-nél nagyobb prímosztója első hatványon szerepel n prímtényezős felbontásában.*

Bizonyítás. Azoknak az n, $1 \leqq n \leqq x$ számoknak a száma, amelyek oszthatók egy log log $\sqrt{x}$-nél nagyobb szám négyzetével, vagy kisebbek $\sqrt{x}$-nél, legfeljebb

$$\sum_{\log\log\sqrt{x}<k\leqq\sqrt{x}} \frac{x}{k^2}+\sqrt{x} < \frac{x}{\log\log\sqrt{x}}+\sqrt{x} = o(x).$$

4. Segédtétel. *Legyen $\varepsilon>0$. Majdnem minden n számnak nincsenek olyan p és q^k osztói, ahol p és q prímek, $k \geqq 1$, hogy $p>(\log\log n)^{1+\varepsilon}$ és $q^k \equiv 1 \pmod p$.*

Bizonyítás. Azoknak az n számoknak a száma, amelyekhez van olyan p, q prímszám és $k \geqq 1$, hogy $pq^k|n$, $p>(\log\log\sqrt{x})^{1+\varepsilon}$ és $q^k \equiv 1 \pmod p$, vagy $n \leqq \sqrt{x}$, legfeljebb

$$\sum_{\substack{p>(\log\log\sqrt{x})^{1+\varepsilon} \\ q^k\equiv 1\,(p) \\ q^k\leqq x}} \frac{x}{pq^k}+\sqrt{x} = x\sum_p \frac{1}{p} \sum_{\substack{q^k\equiv 1(p) \\ q^k\leqq x}} \frac{1}{q^k}+o(x) \leqq$$

$$\leqq x\sum_p \frac{1}{p}\cdot\frac{C\log\log x}{p-1}+o(x)$$

(lásd [6], 147. old.; most $p<\sqrt{x}$)

$$\leqq x\cdot\frac{C\log\log x}{(\log\log\sqrt{x})^{1+\varepsilon}}+o(x) = o(x).$$

A harmadik feltételnek eleget tevő prímek számának meghatározásához már mélyebb számelméleti segédeszközökre lesz szükségünk.

5. Segédtétel. *Legyenek* $p_1, \ldots, p_t$ *különböző prímszámok. Ekkor*

$$\sum_{\substack{q \text{ prim} \\ q \leqq x \\ p_i \mid q-1}} \frac{1}{q} = (1+o(1)) \prod_{i=1}^{t} \left(1-\frac{1}{p_i-1}\right) \cdot \log\log x.$$

Bizonyítás. Legyen $k=p_1 \ldots p_t$. Azok a q prímszámok, amelyekre $p_i \mid q-1$ a k-hoz relatív prím $\varphi(k)=(p_1-1)\ldots(p_t-1)$ maradékosztály közül $(p_1-2)\ldots$ $\ldots(p_t-2)$-ben helyezkednek el. A Dirichlet tétel kvantitatív alakja (lásd [6], 138. old.) azt mondja, hogy egy-egy ilyen maradékosztályban x-ig aszimptotikusan

$$\frac{1}{\varphi(k)} \cdot \frac{x}{\log x}$$

prím van. Innen állításunk parciális szummációval könnyen adódik.

6. Tétel. *Jelölje* $g(n)$ *az* n *páratlan szám olyan* q *prímosztóinak számát, amelyekre* $q-1$ *n-hez retíval prím. Majdnem minden páratlan n-re*

$$g(n) = (1+o(1)) \prod_{p \mid n} \left(1-\frac{1}{p-1}\right) \cdot \log\log n.$$

Bizonyítás. Elegendő azt megmutatnunk, hogy minden pozitív ε-ra és η-ra a páratlan számok egy legfeljebb 2η felső sűrűségű részhalmazának kivételével

$$\left| \frac{g(n)}{\prod_{p \mid n} (1-1/(p-1)) \cdot \log\log n} - 1 \right| < \varepsilon$$

teljesül a többi páratlan n számra. Ehhez alkalmasan nagyra fogjuk választani az A számot, amelyet aztán rögzítettnek tekintünk.

Jelölje M az A-ig terjedő prímek szorzatát (a 2-t is beleértve), és az $n \equiv a \pmod M$ maradékosztályon, ahol $1 \leqq a < M$ páratlan, vizsgáljuk azt a $g_A(n)$ függvényt, amivel az n (páratlan) szám olyan q prímosztóinak számát jelöljük, amelyekre $q > A$ és $q-1$ nem osztható n-nek egyetlen $p \leqq A$ prímosztójával sem.

A $g_A(n)$ függvény átlagos viselkedését Turán módszerével állapítjuk meg. A maradékosztály minden elemének ugyanazok az A-nál nem nagyobb prímosztói, legyenek ezek $p_1, \ldots, p_t$. Ekkor

$$\sum_{\substack{n \equiv a(M) \\ n \leqq x}} g_A(n) = \sum_{\substack{n \equiv a(M) \\ n \leqq x}} \sum_{\substack{q \mid n \\ p_i \mid q-1}} 1 = \sum_{\substack{q \leqq x \\ p_i \mid q-1}} \sum_{\substack{n \equiv a(M) \\ q \mid n \\ n \leqq x}} 1 = \sum_{\substack{q \leqq x \\ p_i \mid q-1}} \left(\frac{x}{Mq} + \delta_q\right),$$

ahol $|\delta_q| < 1$. Így $g_A(n)$ átlagértéke az $n \equiv a \pmod M$ maradékosztályon x-ig

$$\sum_{\substack{q \leqq x \\ p_i \mid q-1}} \frac{1}{q} + O\left(\frac{1}{\log x}\right).$$

Az 5. Segédtétel szerint

$$K = \sum_{\substack{q \leqq x \\ p_i \mid q-1}} \frac{1}{q} = (1+o(1)) \prod_{i=1}^{t} \left(1-\frac{1}{p_i-1}\right) \cdot \log\log x.$$

A $g_A(n)$ függvénynek K-tól vett négyzetes eltérésére a következő adódik (ahol minden $|\delta_i|<1$):

$$\sum_{\substack{n\equiv a(M)\\ n\leqq x}}(g_A(n)-K)^2=\sum_n g_A(n)^2-2K\sum_n g_A(n)+$$

$$+\left(\frac{x}{M}+\delta_1\right)K^2=\sum_{\substack{q_1\leqq x\\ p_i\mid q_1-1}}\sum_{\substack{q_2\leqq x\\ p_i\mid q_2-1}}\sum_{\substack{n\equiv a(M)\\ n\leqq x\\ q_1\mid n\\ q_2\mid n}}1-K^2\frac{x}{M}+o(x)=\sum_{\substack{q\leqq x\\ p_i\mid q-1}}\left(\frac{x}{Mq}+\delta_q\right)+$$

$$+\sum_{\substack{q_1\leqq x\\ p_i\mid q_1-1}}\sum_{\substack{q_2\leqq x\\ p_i\mid q_2-1}}\left(\frac{x}{Mq_1q_2}+\delta_{q_1q_2}\right)-\sum_{\substack{q\leqq x\\ p_i\mid q-1}}\left(\frac{x}{Mq^2}+\delta_{q^2}\right)-$$

$$-K^2\frac{x}{M}+o(x)\leqq K\frac{x}{M}+K^2\frac{x}{M}-K^2\frac{x}{M}+O(x)=K\frac{x}{M}+O(x).$$

Tehát $g_A(n)/K$-nak 1-től vett átlagos négyzetes eltérése

$$\frac{1}{K}+O\left(\frac{1}{K^2}\right),$$

így a Csebisev egyenlőtlenség szerint majdnem minden n-re

$$g_A(n)=(1+o(1))\prod_{\substack{p\mid n\\ p\leqq A}}\left(1-\frac{1}{p-1}\right)\cdot\log\log n.$$

Nézzük most $g(n)$-et! $g_A(n)$ kiszámításánál nem vettük tekintetbe azokat a prímeket, amelyek A-nál nem nagyobbak, így $g(n)\leqq g_A(n)+\pi(A)$. Másrészt viszont számoltunk olyan q prímeket is, amelyekre $q\mid n$ és van olyan $p\mid n$ prím, $p>A$, hogy $p\mid q-1$. Felülről becsülve az ilyen prímek számának átlagát, azt kapjuk, hogy

$$\frac{1}{x}\sum_{n\leqq x}\sum_{\substack{p>A\\ q\equiv 1(p)\\ pq\mid n}}1\leqq\frac{1}{x}\sum_{\substack{p>A\\ p\leqq x}}\sum_{\substack{q\equiv 1(p)\\ q\leqq x}}\frac{x}{pq}<\sum_{p>A}\frac{1}{p}\sum_{\substack{q\equiv 1(p)\\ q\leqq x}}\frac{1}{q}\leqq\sum_{p>A}\frac{1}{p}\cdot\frac{C\log\log x}{p-1}<\frac{C\log\log x}{A},$$

vö. a 4. Segédtétellel. Így egy legfeljebb ηx elemű halmaz kivételével

$$g(n)\leqq g_A(n)-\frac{C\log\log x}{A}\cdot\frac{1}{\eta}.$$

A megmaradó legalább $(1-\eta)x-o(x)$ számra tehát

$$1+o(1)\leqq\frac{g(n)}{g_A(n)}\leqq 1-(1+o(1))\frac{C}{A\prod_{3\leqq p\leqq A}\left(1-\frac{1}{p-1}\right)}\cdot\frac{1}{\eta}.$$

Vegyük észre, hogy itt

$$A\prod_{3\leqq p\leqq A}\left(1-\frac{1}{p-1}\right)\leqq A\exp\left(-(\log 8)\sum_{3\leqq p\leqq A}\frac{1}{p}\right)\leqq$$

$$\leqq c_1 A\exp\left(-(\log 8)\log\log A\right)=\frac{c_1 A}{(\log A)^{\log 8}}.$$

Továbbá, tekintetbe kell még vennünk, hogy a tétel kimondásában $\prod(1-1/(p-1))$-et az összes prímosztóra képeztük. Becsüljük meg a

$$\prod_{\substack{p|n\\p>A}}\left(1-\frac{1}{p-1}\right)>1-\sum_{\substack{p|n\\p>A}}\frac{1}{p-1}$$

szorzatot! Itt átlagban

$$\frac{1}{x}\sum_{n\leqq x}\sum_{\substack{p|n\\p>A}}\frac{1}{p-1}\leqq\frac{1}{x}\sum_{A<p\leqq x}\frac{x}{p}\cdot\frac{1}{p-1}\leqq\frac{1}{A}.$$

Ezért legfeljebb ηx szám kivételével

$$\sum_{\substack{p|n\\p>A}}\frac{1}{p-1}\leqq\frac{1}{A}\cdot\frac{1}{\eta},$$

azaz

$$\prod_{\substack{p|n\\p>A}}\left(1-\frac{1}{p-1}\right)>1-\frac{1}{A}\cdot\frac{1}{\eta}.$$

Összegezve eddigi számításainkat, azt kapjuk, hogy egy legfeljebb 2η felső sűrűségű halmaz kivételével már minden más n páratlan számra

$$\left|\frac{g(n)}{\prod_{p|n}\left(1-\frac{1}{p-1}\right)\cdot\log\log n}-1\right|=$$

$$=\left|\frac{g(n)}{g_A(n)}\cdot\frac{g_A(n)}{\prod_{\substack{p|n\\p\leqq A}}\left(1-\frac{1}{p-1}\right)\log\log n}\cdot\frac{1}{\prod_{\substack{p|n\\p>A}}\left(1-\frac{1}{p-1}\right)}-1\right|\leqq$$

$$\leqq c_2\left\{\left|\frac{g(n)}{g_A(n)}-1\right|+\left|\frac{g_A(n)}{\prod_{\substack{p|n\\p\leqq A}}\left(1-\frac{1}{p-1}\right)\cdot\log\log n}-1\right|+\left|\prod_{\substack{p|n\\p>A}}\left(1-\frac{1}{p-1}\right)-1\right|\right\}\leqq$$

$$\leqq c_2\left\{\frac{(1+o(1))C(\log A)^{\log 8}}{c_1 A}\cdot\frac{1}{\eta}+o(1)+\frac{1}{A}\cdot\frac{1}{\eta}\right\}<\varepsilon,$$

ha A-t elég nagynak választjuk.

Ezzel tételünket bebizonyítottuk.

Eddigi eredményeink együttesen szolgáltatják a dolgozat fő tételét.

7. Tétel. *Majdnem minden páratlan n számnak*

$$(1+o(1))\prod_{p|n}\left(1-\frac{1}{p-1}\right)\cdot\log\log n$$

olyan q prímosztója van, hogy minden n-edrendű csoport egy q-adrendű és egy n/q-adrendű részcsoportjának direkt szorzatára bontható.

Bizonyítás. A 2. Segédtétel szerint az olyan q prímosztók számát kell meghatároznunk, amelyekre (i) $q^2 \nmid n$, (ii) $q \nmid p^k - 1$ n egyetlen p^k prímhatvány-osztójára sem és (iii) $(n, q-1)=1$. A 6. Tétel megadja a (iii) feltételnek megfelelő prímosztók számát. Azt kell megmutatnunk, hogy majdnem minden n-re ezen prímosztók $1-o(1)$ része teljesíti az (i) és (ii) feltételt is. A 3. és a 4. Segédtétel szerint majdnem minden szám minden $(\log\log n)^{1+\varepsilon}$-nál nagyobb prímosztója eleget tesz az (i) és (ii) feltételeknek. A $(\log\log n)^{1+\varepsilon}$-nál kisebb prímosztók száma viszont majdnem minden n-re csupán $O(\log\log\log\log n)$ (lásd [1]), és ez a (iii) feltételnek megfelelő prímosztók számához,

$$(1+o(1))\prod_{p\mid n}\left(1-\frac{1}{p-1}\right)\cdot \log\log n\text{-hez}$$

képest elenyésző, ugyanis páratlan n-re

$$\prod_{p\mid n}\left(1-\frac{1}{p-1}\right) \geqq \exp\left(-\log 8 \sum_{p\mid n}\frac{1}{p}\right),$$

és itt átlagban

$$\frac{1}{x}\sum_{n\leqq x}\sum_{p\mid n}\frac{1}{p} \leqq \frac{1}{x}\sum_{p\leqq x}\frac{1}{p}\cdot\frac{x}{p} < \sum_{p}\frac{1}{p^2} < 1,$$

így majdnem minden n-re

$$\prod_{p\mid n}\left(1-\frac{1}{p-1}\right) > \exp(-\log\omega(n)) = \frac{1}{\omega(n)},$$

ahol $\omega(n)$ tetszőlegesen lassan tart végtelenhez.

Kimutatható, hogy a páratlan számok pozitív százalékára q-nak az n legnagyobb prímosztója is választható.

Most általánosítjuk a 2. Segédtételt az n tetszőleges — nemcsak prím — osztóira. A bizonyításban felhasználjuk Feit és Thompson híres tételét [2] is, miszerint minden páratlan rendű csoport feloldható.

8. Segédtétel. *Legyen $n=n_1n_2$ páratlan szám. Akkor és csak akkor lehet minden n-edrendű csoportot egy n_1-edrendű és egy n_2-edrendű részcsoportjának direkt szorzatára bontani, ha (i) n_1 és n_2 relatív prímek, (ii) nincs olyan $p\mid n_1, q^k\mid n_2$ (p, q prímek, $k\geqq 1$), amelyekre $p\mid q^k-1$, és szimmetrikusan (iii) nincs olyan $p^k\mid n_1$, $q\mid n_2$ (p, q prímek, $k\geqq 1$), amelyekre $q\mid p^k-1$.*

Bizonyítás. A feltételek szükségességét a következő csoportok mutatják: (i) C_n; (ii) $\{x\to ax+b \mid a, b\in GF(q^k),\ a^p=1\}\times C_{n/pq^k}$; (iii) ugyanez, p és q szerepét fölcserélve.

Tegyük most fel, hogy teljesülnek az (i), (ii), (iii) feltételek és legyen G egy n-edrendű csoport. Mivel n páratlan, Feit és Thompson tétele [2] szerint G feloldható. Hall tétele (lásd [3], 232. old.) szerint minden p_i prímosztóhoz kiválasztható G-nek egy P_i Sylow p_i-részcsoportja úgy, hogy minden P_i, P_j párra $P_iP_j=P_jP_i$ teljesüljön. Jelölje G_1 az n_1-et osztó prímekhez tartozó kiválasztott Sylow részcsoportok szorzatát, G_2 pedig az n_2 prímosztóihoz tartozókét. Az (i) feltétel alapján $|G_1|=n_1$ és $|G_2|=n_2$. Vegyük most n_1-nek egy p prímosztóját és a hozzá tartozó P Sylow p-részcsoportot és n_2-nek egy q prímosztóját és a megfelelő Q részcsoportot. A Sylow részcsoportoknak a Hall tételben előírt választása folytán $PQ=QP$ részcsoport. A (ii) és (iii) feltételek miatt ez a részcsoport Pazderski eredménye (lásd [5], 285. old.)

szerint nilpotens, azaz P és Q elemenként felcserélhető, $PQ=P\times Q$. Ez bármely prímosztó-párra fennáll, ezért G_1 és G_2 is elemenként felcserélhető, tehát $G=G_1\times G_2$.

Az ilyen faktorizációk vizsgálatához már sokkal mélyebb számelméleti segédtételre lesz szükségünk; ennek bizonyítását csak vázlatosan ismertetjük.

9. Segédtétel. *Legyen* $0<\varepsilon<1$. *Majdnem minden* n *számra igaz a következő:* n *minden* $(\log\log n)^{1-\varepsilon}$*-nál kisebb* d *osztójához van olyan* $q|n$ *prímszám, hogy* $q\equiv 1 \pmod d$.

Bizonyítás. Felső becslést adunk azoknak az $n\leqq x$ számoknak a részarányára, amelyekhez van olyan $d<(\log\log x)^{1-\varepsilon}$, hogy $q\not\equiv 1 \pmod d$ n egyetlen q prímosztójára sem. Először rögzítsük d-t! Ekkor Brun módszerét alkalmazva (lásd [4]) belátható, hogy azon n-ek részaránya x-ig, amelyek egyetlen $q\equiv 1 \pmod d$ prímmel sem oszthatók legfeljebb

$$c_3 \prod_{\substack{q\equiv 1(d)\\ q\leqq x}} \left(1-\frac{1}{q}\right) < c_3 \exp\left(-\sum_{\substack{q\equiv 1(d)\\ q\leqq x}} \frac{1}{q}\right),$$

valamely alkalmas c_3 abszolút konstanssal. Most a számtani sorozatokra vonatkozó Siegel—Walfisz tételből (lásd [6]) parciális szummációval azt nyerjük, hogy

$$\sum_{\substack{q\equiv 1(d)\\ q\leqq x}} \frac{1}{q} = (1+o(1))\frac{\log\log x}{\varphi(d)} \geqq (1+o(1))\frac{\log\log x}{(\log\log x)^{1-\varepsilon}} \geqq c_4 (\log\log x)^{\varepsilon}$$

teljesül minden $d<(\log\log x)^{1-\varepsilon}$ esetén, ahol $c_4>0$ alkalmas konstans. Tehát a kivételes n-ek részaránya összesen is legfeljebb

$$(\log\log x)^{1-\varepsilon} c_3 \exp\left(-c_4 (\log\log x)^{\varepsilon}\right),$$

ami tart 0-hoz, ha $x\to\infty$.

Még két egyszerű észrevételre is szükségünk lesz.

10. Segédtétel. *Legyen* $0<\varepsilon<1$. *Azoknak az* n *számoknak a halmaza, amelyeknek van* $(\log\log n)^{1-\varepsilon}$ *és* $(\log\log n)^{1+\varepsilon}$ *közé eső prímosztójuk, legfeljebb* $\log(1+\varepsilon)/(1-\varepsilon)$ *felső sűrűségű.*

Bizonyítás. Az ismert módszerek (lásd [1]) azt adják, hogy a $(\log\log n)^{1-\varepsilon}$ és $(\log\log n)^{1+\varepsilon}$ közé eső prímosztók átlagos száma

$$\log\log(\log\log n)^{1+\varepsilon} - \log\log(\log\log n)^{1-\varepsilon} + o(1) = \log\frac{1+\varepsilon}{1-\varepsilon} + o(1).$$

Innen állításunk azonnal következik.

11. Segédtétel. *Legyen* A *pozitív szám. Azoknak a számoknak a halmaza, amelyeknek nincs* A*-nál kisebb prímosztójuk, legfeljebb* $c_5/\log A$ *sűrűségű, valamely* $c_5>0$ *konstanssal.*

Bizonyítás. E halmaz sűrűsége nyilvánvalóan

$$\prod_{p<A}\left(1-\frac{1}{p}\right) < \exp\left(-\sum_{p<A}\frac{1}{p}\right) \leqq \exp(-\log\log A+\log c_5) = \frac{c_5}{\log A}.$$

Eddigi előkészületeink annak megmutatásához kellenek, hogy a 8. Segédtételben megadott tulajdonságú felbontások általában csak néhány, a 2. Segédtételben leírt tulajdonságú „izolált" prím leválasztását jelentik.

12. Tétel. *Majdnem minden n számra igaz a következő: Ha $n=n_1n_2$ olyan faktorizáció, hogy minden n-edrendű csoport egy n_1-edrendű és egy n_2-edrendű részcsoportjának direkt szorzatára bontható, és n legkisebb prímosztója n_1-nek osztója, akkor n_2 minden prímosztója teljesíti a 2. Segédtétel feltételeit, és így minden n_2-edrendű csoport ciklikus.*

Bizonyítás. Azt mutatjuk meg, hogy tetszőleges pozitív η-ra a tételben megfogalmazott tulajdonsággal rendelkező n-ek halmaza legalább $1-\eta$ alsó sűrűségű. Válasszuk ε-t $(0<\varepsilon<1)$ és A-t $(A>0)$ úgy, hogy

$$\log\frac{1+\varepsilon}{1-\varepsilon}+\frac{c_5}{\log A}<\eta$$

legyen. Vegyük azoknak az n számoknak a halmazát, amelyekre a következők mindegyike teljesül:

(a) n minden $(\log\log n)^{1+\varepsilon}$-nál nagyobb prímosztója a prímtényezős felbontásban első hatványon szerepel;

(b) Nincsenek olyan q, r prímek és $k\geqq 1$, hogy $qr^k|n$, $q>(\log\log n)^{1+\varepsilon}$ és $r^k\equiv 1 \pmod q$;

(c) n minden $d<(\log\log n)^{1-\varepsilon}$ osztójához van olyan $q|n$ prím, hogy $q\equiv 1 \pmod d$;

(d) n-nek nincs $(\log\log n)^{1-\varepsilon}/A$ és $(\log\log n)^{1+\varepsilon}$ közé eső prímosztója ; és

(e) n-nek van A-nál kisebb prímosztója.

A 3.. 4., 9., 10. és 11. Segédtételek szerint ennek a halmaznak az alsó sűrűsége legalább

$$1-\log\frac{1+\varepsilon}{1-\varepsilon}-\frac{c_5}{\log A}>1-\eta.$$

Belátjuk, hogy az ilyen tulajdonságú n számokra teljesül a tételbeli állítás. Legyen n egy ilyen szám, és jelölje legkisebb prímosztóját p, (e) szerint $p<A$. Ha $r<(\log\log n)^{1-\varepsilon}/A$ n-nek tetszőleges prímosztója, akkor (c) szerint van olyan $q|n$ prím, hogy $rp|q-1$. A 8. Segédtétel (ii) feltétele szerint ekkor $q|n_1$, a (iii) feltétel szerint pedig r is n_1 prímosztója. Így (i) miatt n_2-nek nincs $(\log\log n)^{1-\varepsilon}/A$-nál kisebb prímosztója. A (d) tulajdonság miatt tehát n_2 minden prímosztója nagyobb mint $(\log\log n)^{1+\varepsilon}$. Legyen $q|n_2$ prím. Ekkor a 2. Segédtétel feltételei közül q-ra teljesül (i) az (a) tulajdonság szerint, (ii) pedig a (b) tulajdonság szerint. Végül $(q-1, n)=1$ is fennáll, hiszen a 8. Segédtétel (ii) pontja szerint $(q-1, n_1)=1$, másrészt (b) alapján $(q-1, n_2)=1$ is teljesül.

Így a 2. Segédtétel értelmében megmutattuk tehát, hogy minden $q|n_2$ prímszámra minden n-edrendű csoport Sylow q-részcsoportja q-adrendű és direkt tényező. Ezért az n_2-edrendű részcsoport ciklikus csoportok direkt szorzata, tehát maga is ciklikus.

Bár dolgozatunkban aszimptotikus kérdésekkel foglalkoztunk, végezetül hadd említsünk meg — bizonyítás nélkül — két pontos eredményt is, amelyek talán érzékeltetik a kérdés bonyolultságát. Nyilvánvalóan minden prímhatvány-rendű ciklikus csoport felbonthatatlan. Eredményeink a nemtriviális esetek közül a két szélsőségre, a négyzetmentes számokra, illetve a csak két különböző prímmel osztható számokra vonatkoznak.

13. Tétel. *Legyen n négyzetmentes szám. Pontosan akkor létezik n-edrendű felbonthatatlan csoport, ha n prímosztóinak halmaza két diszjunkt részre, P-re és Q-ra bontható úgy, hogy az a páros gráf, amelynek csúcshalmaza $P \cup Q$, élhalmaza $\{\{p, q\}: p \in P, q \in Q, p \mid q-1\}$ összefüggő legyen.*

14. Tétel. *Legyen $n=p^a q^b$, $r=\operatorname{ord} p \pmod q$, $s=\operatorname{ord} q \pmod p$. Pontosan akkor létezik n-edrendű felbonthatatlan csoport, ha az alábbiak valamelyike teljesül:*

(1) $r=1$;
(2) *r páros,* $a \geqq r$;
(3) $r \geqq 3$, *páratlan és* $a=r$ *vagy* $a \geqq 2r$; *illetve szimmetrikusan:*
(1′) $s=1$;
(2′) *s páros,* $b \geqq s$;
(3′) $s \geqq 3$, *páratlan és* $b=s$ *vagy* $b \geqq 2s$.

A dolgozat megfogalmazásában nyújtott segítségéért köszönetet mondunk Pintz Jánosnak és Szalay Mihálynak.

IRODALOM

[1] P. Erdős: On the distribution of prime divisors, *Aequationes Math.* **2** (1969), 177—183.
[2] W. Feit, J. G. Thompson: Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 755—1029.
[3] D. Gorenstein: *Finite groups*, Harper and Row, New York, 1968.
[4] H. Halberstam, H. E. Richert: *Sieve methods*, Academic Press, 1974.
[5] B. Huppert: *Endliche Gruppen, I*, Springer, 1967.
[6] K. Prachar: *Primzahlverteilung*, Springer, 1957.
[7] C. Sudler: Query #331, *Notices Amer. Math. Soc.* **32** (1985), 472.

(Beérkezett: 1986. július 16-án)

О ПОРЯДКАХ ПРЯМО НЕРАЗЛОЖИМЫХ ГРУПП

П. ЭРДЁШ и П. П. ПАЛФИ

Неразложимые группы четных порядков легко построятся (Утверждение 1). С другой стороны мы покажем, что почти все нечетные числа n (т.е. за исключением множества плотности 0) имеют

$$(1+o(1)) \prod_{p \mid n} \left(1-\frac{1}{p-1}\right) \cdot \log \log n$$

такие простые делители что соответствующая силовская подгруппа является прямым множителем в каждой группе порядка n (Теорема 7). В теоретико-групповой части доказателства мы покажем что простой делитель p числа n обладает этим свойством тогда и только тогда, когда (i) n не делится на p^2, (ii) если n делится на q^k (q простое, $k \geqq 1$) тогда $p \nmid q^k-1$, и (iii) нод $(p-1, n)=1$ (Лемма 2). Для почти всех чисел n каждый простой делитель больше чем $(\log \log n)^{1+\varepsilon}$ удовлетворяет (i) и (ii) (Леммы 3, 4). Суть теоретико-числовой части доказательства — определение число простых делителей с свойством (iii) (Теорема 6).

Пусть $n=n_1 n_2$ — такое разложение что всякая группа порядка n разлагается в прямое произведение подгрупп порядков n_1 и n_2. Тогда для почти всех чисел n один из множителей всегда является циклической группой (Теорема 12).