1. *Adjuk meg az alábbi permutációk diszjunkt ciklusfelbontását:*

a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$; *b)* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix}$; *c)* $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$;

d) $(1\,2\,3\,4\,5)^{-1}(1\,2\,3)(4\,5)(1\,2\,3\,4\,5)$ *e)* $(1\,2)(1\,3)(1\,4)\cdots(1\,n)$.

Megoldás: a) $(1\,2\,4\,3)$ b) $(1\,2\,4)(3\,6\,5)$

c) $(1\ n)(2\ n-1)(3\ n-2)\cdots$, a végén páros n-re $(\frac{n}{2}\ \frac{n+2}{2})$ van, páratlan n-re $(\frac{n-1}{2}\ \frac{n+3}{2})$ (az $\frac{n+1}{2}$ fixpont).

d) $(1\,5)(2\,3\,4)$ e) $(1\,2\,\dots n)$.

2. *Írjuk fel transzpozíciók szorzataként az alábbi permutációkat:*

a) $(1\,2\,3)(1\,2\,4)$; *b)* $(1\,2\,3\dots n)$; *c)* $(n\,n-1\,\dots 1)$.

Megoldás:

a) Az 1.e) alapján $(1\,2)(1\,3)(1\,2)(1\,4)$, de ennek a permutációnak a diszjunkt ciklusokra bontása is transzpozíciókból áll: $(1\,4)(2\,3)$. Általában is, ha a permutációt előállítjuk diszjunkt ciklusok szorzataként, aztán azokat bontjuk fel az 1.e) mintájára, akkor belátható, hogy így minimális számú transzpozíció szorzataként írjuk fel a permutációt.

b) $(1\,2)(1\,3)(1\,4)\cdots(1\,n)$

c) Mivel ez az előző inverze, elég annak a felbontását invertálni: $(1\,n)\dots(1\,4)(1\,3)\cdots(1\,2)$.

3. *Ha k és n relatív prímek, akkor a k-val való szorzás egy permutációt definiál a modulo n maradékosztályok (redukált maradékosztályok) halmazán. Adjuk meg a 2-vel való szorzás ciklusfelbontását $n = 5$-re, $n = 7$-re és $n = 9$-re. Mikor lesz a redukált maradékosztályok k-val való szorzásának ciklusfelbontásában pontosan 1 darab ciklus? Mit mondhatunk általában a ciklusok hosszáról, ill. számáról?*

Megoldás: $n = 5$-re: $(1\,2\,4\,3)$

$n = 7$-re: $(1\,2\,4)(3\,6\,5)$

$n = 9$-re: $(1\,2\,4\,8\,7\,5)$.

Minden esetben azonos hosszúságú ciklusokra bomlik a permutáció, mert egy n-hez relatív prím b számra $b \cdot 2^k \equiv b \pmod n \Leftrightarrow 1 \equiv 2^k \pmod n$. A ciklushosszakat az határozza meg, hogy mennyi a 2 rendje modulo n, azaz mi a legkisebb k, amelyre $2^k \equiv 1 \pmod n$. Másképpen, ez a minimális k a 2 rendje a $\mathbb{Z}_n^*$ csoportban (és ekkor a ciklusok száma $\varphi(n)/k$). Akkor van egyetlen ciklus, ha a 2 generálja az egész csoportot (és ennek persze szükséges, de nem elégséges feltétele, hogy $\mathbb{Z}_m^*$ ciklikus legyen).

4. *Számítsuk ki g^2-et, g^3-öt és g^{-1}-et, ha a)* $g = (1\,2\,3\,4\,5\,6\,7\,8)$ *b)* $g = (1\,2\,3\,4)(5\,6\,7)$.

Megoldás: a) $g^2 = (1\,3\,5\,7)(2\,4\,6\,8)$, $g^3 = (1\,4\,7\,2\,5\,8\,3\,6)$, $g^{-1} = (8\,7\,6\,5\,4\,3\,2\,1)$.

b) $g^2 = (1\,3)(2\,4)(5\,7\,6)$, $g^3 = (1\,4\,3\,2)$, $g^{-1} = (4\,3\,2\,3\,1)(7\,6\,5)$,

5. *Mekkora a rendje a következő permutációknak? Melyek permutációk párosak, illetve páratlanok?*

a) $(1\,2\,3)(4\,5\,6\,7)(8\,9)$ *b)* $(1\,2\,3)(2\,3\,4)$ *c)* $(1\,2\,3)(3\,4\,5\,6\,7)(5\,6\,7)$

Megoldás: a) Ez diszjunkt ciklusok szorzatára van bontva, így a rendje a ciklushosszak legkisebb közös többszöröse, ami 12. Páros a permutáció, mert egy páros és két páratlan permutáció szorzata (egy k-ciklus akkor páros permutáció, ha k páratlan).

b) Írjuk fel a diszjunkt ciklusfelbontását: $(13)(24)$. Ebből látszik, hogy a rendje 2, a paritása pedig akár az eredeti megadásából is leolvasható: két páros permutáció szorzata, ezért páros, de az újból is: az előállításában páros a páros hosszúságú ciklusok száma, ezért a permutáció páros.

c) Diszjunkt ciklusfelbontásban: (1246573), ezért a rendje 7, és a permutáció páros.

6. *a) Milyen rendű elemek vannak S_4-ben, S_5-ben, A_5-ben?*

b) Van-e S_{21}-ben, illetve A_{21}-ben 210-edrendű elem? Hát 25-ödrendű?

c) Hány hatodrendű elem van S_6-ban, és hány negyedrendű van A_8-ban?

d) Bizonyítsuk be, hogy A_4-nek nincs hatodrendű részcsoportja.

Megoldás: a) A rendet a ciklusszerkezet dönti el, ami S_4-ben 4, $3+1$, $2+2$, $2+1+1$ és $1+1+1+1$ lehet, így a rendek 4, 3, 2, (még egyszer 2,) és 1. S_5-ben a ciklusszerkezetek: 5, $4+1$, $3+2$, $3+1+1$, $2+2+1$, $2+1+1+1$ és $1+1+1+1+1$, tehát a rendek 5, 4, 6, 3, 2 és 1. A ciklusszerkezetek közül az 5, $3+1+1$, $2+2+1$ és $1+1+1+1+1$ ad páratlan permutációt, ezért A_5-ben a rendek 5, 3, 2 és 1.

b) $210 = 2\cdot 3\cdot 5\cdot 7$, tehát ahhoz, hogy egy elem 210 rendű legyen, kellenek olyan ciklusok a ciklusfelbontásában, amelyek 2-vel, 3-mal, 5-tel, illetve 7-tel oszthatók (lehet ugyanaz többel is), és minden ciklus hosszának osztania kell a 210-et. Ilyen nyilván van S_{21}-ben, mert $2+3+5+7=17<21$, tehát egy diszjunkt 2-ciklus, 3-ciklus, 5-ciklus és 7-ciklus szorzata megfelel. Ez így páratlan permutáció, de belefér még egy 2-ciklus, és akkor már páros lesz, tehát A_{21}-ben is van 210-edrendű elem. 25-ödrendű elemhez viszont kell egy 25-ciklus a ciklusfelbontásba, tehát olyan nincs S_{21}-ben sem.

c) A 6-odrenű elem vagy egyetlen 6-ciklus, vagy van benne külön egy 2-vel és egy 3-mal osztható rendű ciklus (s mivel a hosszak osztják 6-ot, ez pontosan 2 és 3 hosszúságú lesz), ennél több pedig nem fér bele egy 6 elemen ható permutációba. Tehát a ciklusfelbontás 6 vagy $3+2+1$, és az ilyen elemek száma $5!+6\cdot\binom{5}{2}\cdot 2 = 120+120 = 240$ (a 6-ciklusnál rögzíthetjük a ciklus első elemét, és a maradék 5 elem permutációi mind különböző permutációt adnak, a másodiknál 6-féle lehet a fixpont, $\binom{5}{2}$-féle a transzpozíció, és a maradék három elem két lényegesen különböző 3-ciklust adhat).
4-edrendűhöz kell egy 4-ciklus, és azon kívül a ciklusok hossza 4-nek osztója kell, hogy legyen, tehát ha egy 8 elemen ható páros permutációt keresünk, ezt csak egy 4-ciklussal vagy egy 2-ciklussal egészíthetjük ki. A $4+4$ ciklusszerkezetű elemek száma $\binom{8}{4}\cdot 3!\cdot 3!\cdot\frac{1}{2} = 1260$ (kiválasztjuk, hogy melyik négy legyen az egyik 4-ciklusban, a két 4-ciklusban az egyértelműség kedvéért a legkisebb elemet írva előre, 3!-féleképpen rendezhetjük az elemeket, viszont a két 4-ciklusnak kétféle sorrendje ugyanazt a permutációt adja, ezért leosztunk 2-vel), a $4+2+1+1$ ciklusszerkezetűeké pedig $\binom{8}{4}\cdot\binom{4}{2}\cdot 3! = 2520$, tehát A_8-ban 3780 darab 4-edrendű elem van.

d) Ha $H \le A_4$ rendje 6, akkor H-ban van 3-adrendű elem a Cauchy-tétel miatt. (Vagy a Cauchy-tétel nélkül azt is mondhatjuk, hogy az 1/3. feladat szerint nem lehet minden elem rendje 1 vagy 2, mert akkor H kommutatív lenne, és a 2/4.,5. miatt a rendje 2-hatvány lenne. Másrészt A_4-ben csak 1, 2 és 3 rendű elemek vannak.) Ez csak 3-ciklus lehet, feltehetjük (szükség esetén az elemek átszámozásával), hogy $g = (1\,2\,3) \in H$. Viszont az ez által generált részcsoport H-ban 2 indexű, tehát normálosztó. De $2 \mid |H|$ miatt H-ban van másodrendű elem is, ami csak $2+2$-es ciklusszerkezetű lehet. Ez az $1,2,3$ elemek közül valamelyik kettőt felcseréli, feltehető, hogy épp az 1, 2-t (g-t elforgatva is felírhatjuk), azaz $h = (1\,2)(3\,4) \in H$. De $h^{-1}gh = (214) \notin \langle g\rangle$, ami ellentmond annak, hogy $\langle g\rangle \lhd H$.