Bevezetés a számításelméletbe II.

2011. MÁJUS 2.

12. gyakorlat: Szimmetrikus csoport, mellékosztályok, számelméleti algoritmusok

1. Írjuk át a következő két permutációt ciklikus alakra, majd számítsuk ki a szorzatukat! Mi a kapott permutáció fixpontja?

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

2. Határozzuk meg a következő két elem rendjét az S_8 szimmetrikus csoportban!

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 5 & 6 & 8 & 7 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 8 & 7 & 4 & 3 & 1 & 2 \end{pmatrix}$$

3. Végezd el az alábbi műveleteket az S_n szimmetrikus csoportban. Add meg az eredmény ciklusfelbontását és határozd meg a rendjét!

   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 1 & 4 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}$

   (b) $(35)(1432)(35)(1234)$

   (c) $[(134)(342)]^{-1}$

   (d) $[(34)(23)(12)]^{2011}$

4. Határozd meg a megadott G csoportok H részcsoportja szerinti baloldali és jobboldali mellékosztályait!

   (a) $G = S_3$, $H = \{I, (12)\}$;

   (b) G az egész számok az összeadással, H a 2005-tel osztható egészek;

   (c) G a nemnulla valós számok a szorzással, $H = \{-1, 1\}$;

5. Döntsd el, hogy a megadott csoportokban baloldali mellékosztályt alkotnak-e (valamilyen részcsoport szerint) a megadott részhalmazok.

   (a) az egész számok csoportja az összeadással; a $8k + 5$ ($k \in \mathbb{Z}$) alakú egészek.

   (b) az egész számok csoportja az összeadással; a pozitív prímszámok.

   (c) S_n; azok a permutációk, amik 1-hez 2-t rendelnek.

6. (a) Határozd meg az Euklideszi algoritmussal $(504, 372)$-t!

   (b) Oldd meg a $372x \equiv 36 \pmod{504}$ kongruenciát!

7. A prímtesztelő algoritmusnak inputként a 15-öt adtuk be. Teszteléskor először az $a_1 = 4$, majd az $a_2 = 7$ számokat választotta ki véletlenszerűen a gép. Melyik szám lett árulója, és melyik lett cinkosa a 15-nek? Ezek után számolás nélkül mondjuk meg, hogy a 13 vajon áruló-e?

8. Játsszuk el az RSA titkosítási algoritmust! Legyen a két titkos prímünk a 7 és a 13, és az 5-öt választjuk kódoló kitevőnek. Mi lesz a dekódoló kitevő? Mi lesz a 3 üzenet kódoltja? Ellenőrizzük dekódolással!