Bevezetés a számításelméletbe II.

10. gyakorlat 2002. április 18-19.

`Csütörtök 10-12 IB-140 és péntek 8-10 IB-145`

Csoportok

1. Csoportot illetve félcsoportot alkot-e az alább megadott H halmaz a $*$ művelettel?
   (a) H az egész számok halmaza és az $a, b \in H$ számokra $a * b := a + b + 1$, ahol a szokásos összeadás szerepel;
   (b) Legyen m egy rögzített szám és $H := \{1, 2, \ldots, m-1\}$. Továbbá $a * b := ab \pmod{m}$; (Megjegyzés: a válasz függ attól, hogy m milyen szám.)
   (c) H az egész számok halmaza és az $a, b \in H$ számokra $a * b := a^b$;
   (d) H azon f függvények halmaza, melyek $f(x) = cx + d$ alakúak, ahol $c \neq 0$. A $*$ művelet pedig a függvények egymás után való alkalmazása (amit analízisből $f \circ g$-vel jelöltetek.) (ZH feladat)
   (e) **HF** H azon modulo m maradékosztályok halmaza, amelyek m-mel relatív prímek. Továbbá $a * b := ab \pmod{m}$;
   (f) **HF** H egy halmaz hatványhalmaza (összes részhalmazinak halmaza), és az $a, b \in H$ részhalmazokkal $a * b := (a \setminus b) \cup (b \setminus a)$ (amit szimmetrikus differenciának is neveznek);
   (g) **HF** H a valós számok halmaza és $a * b := a + b + ab$. (ZH feladat)
   (h) **HF** H a 2002 pozitív osztóinak halmaza, és az $a, b \in H$ számokra $a * b := d(a, b)$, azaz a és b legnagyobb közös osztója.
2. Ciklikus csoport-e az $\{1, 2, 3, 4, 5, 6\}$ számhalmaz a modulo 7 szorzással? (ZH feladat)
3. Legyen a és b egy csoport két tetszőleges eleme. Bizonyítsuk be, hogy ekkor b rendje megegyezik $a^{-1}ba$ rendjével.
4. Hány eleme van a D_5 diédercsoportnak? (A D_n diéder csoport alatt a szabályos n szög egybevágósági transzformációiból alkotott csoportot értjük.) Ciklikus-e a csoport? Keressünk néhány valódi részcsoportot bennük és vizsgáljuk meg, hogy azok ciklikusak-e.
5. **HF** A kocka szimmetria csoportjának (azaz egybevágósági transzformációiból alkotott csoportjának) mekkora a legnagyobb rendű részcsoportja, amely részcsoport marad,
   (a) ha egy lapot kékre festünk;
   (b) ha két párhuzamos lapot kékre festünk?

   (1. megjegyzés: tehát csak a kék részt kékbe vivő transzformációk fordulhatnak elő egy részcsoportban. 2. megjegyzés: egy „alakzat szimmetria csoportja” és a permutációkból alkotott „szimmetrikus csoport” nem keverendő össze.)
6. **HF** Mutassuk meg, hogy tetszőleges $n > 0$ számhoz található olyan véges csoport, melynek rendje pontosan n? És ciklikus csoport?
7. **HF** Legyen $n \geq 4$. Az n hosszú 0-1 sorozatok H_1 halmazán jelölje $+$ a bitenkénti modulo 2 összeadást. Álljon H_2 azokból a sorozatokból, melyekben az egyesek száma kettővel osztható. H_3 pedig azokból, melyekben az egyesek száma osztható hárommal. Az előbb definiált művelettel csoportot alkot-e H_2? Csoport-e H_3? (ZH feladat)
8. **HF** Bizonyítsuk be, hogy egy csoport nem állhat elő két valódi részcsoportjának uniójaként.

---

9. **HF** Mutassuk meg, hogy tetszőleges p prím esetén $\binom{2p}{p} \equiv 2 \pmod{p}$. (Segítség: használjuk Wilson tételét.)
10. **HF** Mennyi x, ha
    (a) $x^{12001} \equiv 5 \pmod{13}$;
    (b) $x^{11999} \equiv 5 \pmod{13}$? (Ez a feladat visszavezethető egy lineáris kongruencia megoldására.)
11. **HF** Tudjuk, hogy az a egész számra $a^{100} \equiv 5 \pmod{31}$ és $a^{101} \equiv 19 \pmod{31}$. Milyen maradékot ad 31-gyel való osztáskor az a szám? (ZH feladat)
12. **HF** Mi az utolsó két számjegye (tízes számrendszerben) az alábbi számnak: (ZH feladat)

$$1997^{2001^{2005}}$$