Bevezetés a számításelméletbe II.

13. gyakorlat, 2007. május 9.

Koblinger Egmont <egmont@cs.bme.hu>

Csoportok III. – Titkosírás

131. Mutasd meg, hogy ha egy G csoport azon elemei, melyek önmaguk inverzei, részcsoportot alkotnak, akkor ez egyben normálosztó is. Igaz-e mindig, hogy ez a halmaz részcsoport?

132. Határozzuk meg a megadott G csoportok H részcsoportja szerinti bal- és jobboldali mellékosztályait, majd döntsük el, hogy H normálosztó-e. Ha igen, határozzuk meg a G/H faktorcsoportot!

   a) G a $\{0, 1, \ldots, 11\}$ számok csoportja a modulo 12 összeadásra nézve, $H = \{0, 4, 8\}$.

   b) $G = S_3$ és $H = \{I, (12)\}$.

   c) G a nemszinguláris mátrixok a mátrixszorzással, H az 1 determinánsú mátrixok.

   d) G az egész számok az összeadással, H a 2007-tel oszható egészek.

   e) G az $\{1, 2, \ldots, 10\}$ halmaz összes részhalmazainak halmaza a szimmetrikus differencia műveletével, H azon részhalmazokból áll, melyek a 9-et és a 10-et nem tartalmazzák.

   f) $G = D_n$, $H = \{I, t_1\}$.

133. Legyen G véges csoport és $N \lhd G$ normálosztó. Mutasd meg, hogy a G/N faktorcsoport gN elemének a rendje a legkisebb olyan k pozitív egész, melyre $g^k \in N$.

134. Legyen G csoport, $H \leq G$ és $N \lhd G$. Bizonyítsd be, hogy $H \cap N$ normálosztója H-nak!

135. Aliz és Béla telefonon keresztül sakkoznak. Ha a játszma függőben marad, az utolsó lépést „borítékolni” kell. Hogyan oldjuk meg ezt?

136. A nyilvános kulcsú titkosírás dekódoló kulcsának működése a következő állításon alapszik: ha x és N adottak, akkor

$$x^{k \cdot \varphi(N)+1} \equiv x \qquad (\text{mod } N)$$

   tejesül minden k pozitív egészre. Ez az állítás könnyen bizonyítható, ha az Euler-Fermat tételből nyert $x^{\varphi(N)} \equiv 1 (\text{mod } N)$ összefüggést a k-adik hatványra emeljük, majd x-szel szorozzuk. Azonban az Euler-Fermat tétel alkalmazásához szükség van arra is, hogy $(x, N) = 1$ teljesüljön. Bizonyítsuk be, hogy ha N két különböző prím szorzata (ez a nyilvános kulcsú titkosításnál fennáll), akkor a fenti állítás teljesüléséhez nem kell, hogy $(x, N) = 1$ igaz legyen!

137. Fehérkém 5 titkos információval rendelkezik, amelyek közül az egyiket szívesen eladná Feketekémnek. Az információkat Fehérkém egy-egy borítékban tartja, mindre fel van írva, hogy miről szól. Feketekém az egyik borítékot szívesen megvenné, de fél, hogy másnap Fehérkém már 6 borítékot árulna, az utolsót azzal a felirattal, hogy „Mi érdekli Feketekémet?”. Ajánljunk nekik olyan eljárást, mellyel Feketekém hozzájut pontosan egy boríték tartalmához, de Fehérkém nem tudja, melyikhez!