Bevezetés a számításelméletbe II.

2010. MÁJUS 10.

12. gyakorlat: Gyűrűk, testek; primtesztelés, titkosítás

1. Mi az egyes elemek rendje C_{12}-ben (a 12 rendű ciklikus csoportban)?
2. Legyen a G csoport elemeinek halmaza $\{1, 2, 3, 4, 5, 6\}$, a művelet a mod 7 szorzás. Igazoljuk, hogy a G csoport ciklikus!
3. $|G| = 81$ és $\exists a \in G : \ a^{27} \neq 1 \Longrightarrow$ a csoport kommutatív.
4. Van-e olyan 20 rendű csoport, melyben van 5 rendű elem, de nincs 20 rendű elem?
   És van-e olyan 20 rendű csoport, melyben van 20 rendű elem, de nincs 5 rendű elem?
5. Gyűrűt, testet vagy ferdetestet alkotnak-e az alábbi halmazok (a szokásos összeadással és szorzással)?
   (a) $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$,
   (b) egész együtthatós polinomok,
   (c) $\{0, 1\}$ a modulo 2 összeadással és szorzással,
   (d) a 4×4-es mátrixok,
   (e) a 4×4-es mátrixok, melyek determinánsa nem nulla, valamint a 4×4-es nulla mátrix
6. Egy $x \neq 0$ gyűrűelem baloldali nullosztó, ha $\exists y \neq 0$, hogy $xy = 0$. Legyen x_1 és x_2 baloldali nullosztó. Bizonyítsuk be, hogy feltéve, hogy $x_1 x_2 \neq 0$, akkor ő is baloldali nullosztó, de $x_1 + x_2$ nem feltétlenül az!
7. A mod 12 maradékosztályok gyűrűjében mely elemeknek van multiplikatív inverzük? Melyek a nullosztók?
8. Igazoljuk, hogy ha egy testben $a + a = 0$ teljesül valamely $a \neq 0$ elemre, akkor minden elemre teljesül!
9. 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?
10. 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!