Bevezetés a számításelméletbe II.

2011. MÁJUS 9.

13. gyakorlat: Gyűrűk, testek; primtesztelés, titkosítás

1. 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?

2. 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!

3. Gyűrűt, testet vagy kommutatív testet alkotnak-e az alábbi halmazok (a szokásos összeadással és szorzással)?

   (a) egész együtthatós polinomok,

   (b) $\{0, 1\}$ a modulo 2 összeadással és szorzással,

   (c) a 4×4-es mátrixok,

   (d) a 4×4-es mátrixok, melyek determinánsa nem nulla, valamint a 4×4-es nulla mátrix

4. 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!

5. A mod 12 maradékosztályok gyűrűjében mely elemeknek van multiplikatív inverzük? Melyek a nullosztók?

6. Igazoljuk, hogy ha egy testben $a + a = 0$ teljesül valamely $a \neq 0$ elemre, akkor minden elemre teljesül!