Bevezetés a Számításelméletbe II.

13. gyakorlat

1. Döntsd el, hogy a megadott halmazok a rajtuk értelmezett $\oplus$ "összeadás" és $\odot$ "szorzás" művelettel gyűrűt, ferdetestet, illetve testet alkotnak–e?

a) Egy X halmaz összes részhalmazának $P(X)$ halmaza, $\oplus = \bigcup$, $\odot = \bigcap$;

b) egy X halmaz összes részhalmazának $P(X)$ halmaza, $\oplus = \triangle$ (szimmetrikus differencia), $\odot = \bigcap$;

c) a valós számok halmaza, $a \oplus b = \sqrt[3]{a^3 + b^3}$, $a \odot b = a \cdot b$ (hagyományos szorzás);

d) az $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ alakú valós mátrixok halmaza, a $\oplus$ és a $\odot$ a hagyományos mátrixműveletek;

e) a pozitív valós számok halmaza, $a \oplus b = a \cdot b$, $a \odot b = a^{\lg b}$.

2. A $\mathbb{Z}_{13}$ testben dolgozunk. Vezessük be az $\frac{a}{b}$ jelölést az $a \cdot b^{-1}$ szorzat helyett. Számítsd ki az alábbi műveletek eredményét!

a) $\frac{1}{5}$ b) $\frac{7}{9}$ c) $\frac{5}{3}\left(\frac{1}{2} + \frac{1}{7}\right)$

3. Tetszőleges (kommutatív) testben vezessük be az $\frac{a}{b}$ jelölést az $a \cdot b^{-1}$ szorzat helyett. Bizonyítsd be az alábbi azonosságokat!

a) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ b) $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$

4. Bizonyítsd be, hogy kommutatív testben minden elemnek legföljebb két négyzetgyöke lehet (vagyis az $x^2 = a$ egyenletnek legföljebb két megoldása lehet a test tetszőleges a elemére).

5. Az (angol) ábécé huszonhat betűjét a $0, 1, \ldots 25$ számokkal helyettesítem ($A = 0$, $B = 1$, $C = 2$, stb., $Z = 25$). Nyilvános kódolófüggvényem:

$$x \mapsto x^{43} \pmod{85}.$$

(Ezzel a $0, 1, \ldots, 84$ számokat lehet kódolni, de csak az első huszonhat számnak van valódi jelentése.) Ezzel a függvénnyel kódoltam titkos üzenetemet is:

59 2 59 20 44 52

Törd fel a kódomat, vagyis készíts a fenti kódolófüggvényhez dekódolófüggvényt, majd fejtsd meg vele titkos üzenetemet!

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

$$x^{k \cdot \varphi(n)+1} \equiv x \pmod{n}$$

teljesül tetszőleges k pozitív egészre. Ez az állítás könnyen bizonyítható, ha az Euler-Fermat tételből nyert $x^{\varphi(n)} \equiv 1 \pmod{n}$ összefüggést k-adik hatványra emeljük, majd x-szel szorozzuk. Azonban az Euler-Fermat tétel alkalmazásához szükség van arra is, hogy $(x, n) = 1$ teljesüljön.

Bizonyítsd be, hogy ha n két különböző prím szorzata (és a nyilvános kulcsú titkosírásnál ez a helyzet), akkor a fenti állítás teljesüléséhez nincs szükség arra, hogy $(x, n) = 1$ igaz legyen!

7. Bizonyítsd be, hogy 561 ($= 3 \cdot 11 \cdot 17$) Carmichael-szám!