SzA XIII. gyakorlat

Lineáris kongruenciák, továbbá absztrakt algebrát akarunk alkalmazni

2011. november 29.

4. **Mi az alábbi lineáris kongruenciák megoldása?**

   (a) $8x \equiv 3 \pmod{21}$
   Mivel $(21, 8) = 1$, és $1 \mid 3$, ezért létezik megoldás, és pontosan 1 megoldás létezik.

   $$\begin{aligned} 8x &\equiv 24 \pmod{21} \\ x &\equiv 3 \pmod{21} \end{aligned}$$

   (b) $9x \equiv 24 \pmod{96}$
   Mivel $(96, 9) = 3$, és $3 \mid 24$, ezért létezik megoldás, és pontosan 3 megoldás létezik.

   $$\begin{aligned} 3x &\equiv 8 \pmod{\mathbf{32}} \\ 3x &\equiv 72 \pmod{32} \\ x &\equiv 24 \pmod{32} \\ x_1 &\equiv 24 \pmod{96} \\ x_2 &\equiv 56 \pmod{96} \\ x_3 &\equiv 88 \pmod{96} \end{aligned}$$

5. **Bizonyítsuk be, hogy tetszőleges p prímszámra:**

   $$\binom{2p}{p} \equiv 2 \pmod{p}$$

   $$\begin{aligned} \frac{(2p)!}{p!p!} &\equiv 2 \pmod{p} \\ \frac{2\cancel{p}(2p-1)\dots(p+1)\cancel{p!}}{\cancel{p}(p-1)!\cancel{p!}} &\equiv 2 \pmod{p} \end{aligned}$$

   A tört nevezőjében a szorzat minden eleme relatív prím p-hez (hiszen az prím), így $(p-1)!$-sal bátran szorozhatunk.

   $$\begin{aligned} 2(2p-1)\dots(p+1) &\equiv 2(p-1)! \pmod{p} \\ 2(p-1)(p-2)\cdot\dots\cdot 2\cdot 1 &\equiv 2(p-1)! \pmod{p} \\ 2(p-1)! &\equiv 2(p-1)! \pmod{p} \end{aligned}$$

   És kész is vagyunk, persze a Wilson-tétel segítségével még szebbé tehetjük:

   $$-2 \equiv -2 \pmod{p}$$

6. **A $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ halmazon az alábbi táblázatokban látható műveleteket értelmezzük.**

+	♣	♢	♡	♠
♣	♣	♢	♡	♠
♢	♢	♣	♠	♡
♡	♡	♢	♣	♠
♠	♠	♡	♢	♣

∗	♣	♢	♡	♠
♣	♣	♣	♣	♣
♢	♣	♢	♢	♢
♡	♣	♢	♡	♡
♠	♣	♢	♡	♠

(a) $((\spadesuit * \diamondsuit) + \clubsuit) * (\spadesuit + \diamondsuit) =?$

$$((\spadesuit * \diamondsuit) + \clubsuit) * (\spadesuit + \diamondsuit) = (\diamondsuit + \clubsuit) * \heartsuit = \diamondsuit * \heartsuit = \diamondsuit$$

(b) **Ezek a műveletek asszociatívak? Kommutatívak? Van egységelemük?**
+: emlékeim szerint asszociatív (annyira nem érdekes), nyilván nem kommutatív ($\heartsuit + \diamondsuit \neq \diamondsuit + \heartsuit$), egységelem ♣.
$*$: emlékeim szerint asszociatív (annyira nem érdekes), kommutatív (átlóra szimmetrikus a műveleti tábla), egységelem ♠.

(c) **Oldjuk meg a következő egyenletet:** $(\heartsuit * x) + \diamondsuit = \diamondsuit$**!**

$$\begin{aligned} (\heartsuit * x) + \diamondsuit &= \diamondsuit \\ \text{első eset:} & \\ \heartsuit * x &= \clubsuit \\ x &= \clubsuit \\ \text{másik eset:} & \\ \heartsuit * x &= \heartsuit \\ x &= \heartsuit \text{ vagy } \spadesuit \end{aligned}$$

(d) **Mit alkotnak ezek a műveletek az adott halmazzal? (semmit/félcsoportot/csoportot/Abel-csoportot)**
Házi feladat :)

7. **Csoportot alkotnak-e az alábbi H halmazok a megadott műveletekre?**

(a) $H = \mathbb{R}$ **a valós számok halmaza, a művelet pedig a hagyományos szorzás.**
A szorzás művelet, az asszociativitás rendben, egységelem az 1, de sajnos a 0-nak nincs inverze, így csak félcsoport.

(b) $H = \mathbb{R} \setminus \{0\}$**, ahol $\mathbb{R}$ a valós számok halmaza, a művelet pedig a következő:** $a * b = 2ab$**, ahol a jobboldalon a hagyományos szorzás szerepel.**
A műveletség stimmel, az asszociativitás ellenőrzése:

$$(a * b) * c = (2ab) * c = 4abc = a * (2bc) = a * (b * c),$$

tehát rendben. Egységelem $\frac{1}{2}$, hiszen $a * \frac{1}{2} = 2a\frac{1}{2} = a$. Inverz $\frac{1}{4a}$, hiszen $a * \frac{1}{4a} = 2a\frac{1}{4a} = \frac{1}{2}$, és mivel a nem 0, ezért mindenkinek tényleg van inverze. Tehát csoport, sőt, Abel-csoport.

(c) $H = \{2k + 1 : k \in \mathbb{Z}\}$**, a művelet pedig az összeadás.**
Két páratlan szám összege páros, így az összeadás még csak nem is művelet.

(d) $H = \{2k : k \in \mathbb{Z}\}$**, a művelet pedig a szorzás.**
Két páros szám szorzata páros, így művelet, valamint az asszociativitás is rendben van, így félcsoport. Több nem lehet, mert az egységelemmel és az inverzzel is komoly bajok vannak.

(e) $H = \{2k + 1 : k \in \mathbb{Z}\}$**, a művelet pedig a szorzás.**
Lásd mint előbb, az egységelemmel már nincs baj, de inverz még mindig nincs.

(f) H **a** $\pmod m$ **szerint vett teljes maradékrendszer (**$H = \{0, 1, \dots m-1\}$**), a művelet pedig a maradékosztályokon értelmezett összeadás.**
Abel-csoport, hiszen művelet, asszociatív, kommutatív, egységelem a 0, inverz pedig $-a \pmod m$.

8. **Legyen** G **olyan csoport, ahol** $a^2 = e$ **teljesül minden** $a \in G$ **elemre. Bizonyítsuk be, hogy** G **Abel-csoport!**
Tfh nem Abel-csoport, azaz létezik olyan $a, b \in G$, hogy $ab \neq ba$. Ekkor

$$\begin{aligned} ab &\neq ba \\ aab &\neq aba \\ aabb &\neq abab \\ (aa)(bb) &\neq (ab)(ab) \\ a^2b^2 &\neq (ab)^2 \\ ee &\neq e \\ e &\neq e \end{aligned}$$

ami nyilván lehetetlen.

9. **Egy** G **csoportban minden** $a, b \in G$ **elempárra teljesül, hogy** $(ab)^{-1} = a^{-1}b^{-1}$**. Bizonyítsuk be, hogy ekkor** G **Abel-csoport!**
Tfh nem Abel-csoport, azaz létezik olyan $a, b \in G$, hogy $ab \neq ba$. Ekkor

$$\begin{aligned} ab &\neq ba \\ ab(ba)^{-1} &\neq (ba)(ba)^{-1} \\ abb^{-1}a^{-1} &\neq e \\ aa^{-1} &\neq e \\ e &\neq e \end{aligned}$$

ami nyilván lehetetlen.