**Bsc algebra1 gyakorlat**

*Második zárthelyi dolgozat (2023. december 15.) – megoldások*

**1.** **a)** A megadott mátrix determinánsa (pl. a Sarrus-szabállyal számolva) $-5$ (1 pont). A második sorhoz és harmadik oszlophoz tartozó előjeles aldetermináns $(-1)^{2+3}\begin{vmatrix}1 & 6\\ 1 & 7\end{vmatrix} = -1$ (1 pont). Tehát az inverz mátrix képletét használva a keresett elem $\frac{1}{5}$ (1 pont).

**b)** A keresett szorzat $(124)(12)(132) = (1324)$ (1 pont). Ez páratlan permutáció, mivel egyetlen páros hosszú ciklus van a ciklusfelbontásában (1 pont).

**c)** Ha $\sigma_1, \sigma_2, \sigma_3$ jelöli a gyökök elemi szimmetrikus polinomjait, akkor a gyökök és együtthatók közötti összefüggések miatt $\sigma_1 = 0$, $\sigma_2 = p$, $\sigma_3 = -q$ (2 pont). Másrészt $\alpha_1^2\alpha_2^2+\alpha_1^2\alpha_3^2+\alpha_3^2\alpha_1^2 = \sigma_2^2-2\sigma_1\sigma_3 = p^2$ (3 pont).

**2.** **a)** Először vegyük észre, hogy $x_0 \not\equiv 0 \pmod 7$, ha $x_0$ megoldása bármelyik kongruenciának a kettő közül (1 pont). Tehát $x_0^6 \equiv 1 \pmod 7$, ezért a mod 7 megoldás $d = 3$ esetén $x_0 \equiv 4 \pmod 7$, $d = 2$ esetén pedig $x_0 \equiv 2 \pmod 7$ (1 pont). Viszont $(x^6 + 4x - d)' = 6x^5 + 4$, aminek $x_0 \equiv 2 \pmod 7$ gyöke modulo 7, de $x_0 \equiv 4 \pmod 7$ nem gyöke (1 pont). A Hensel-lemma miatt így $d = 3$ esetén pontosan 1 megoldás van (1 pont), de mivel $2 \cdot 4^6 + 4 \cdot 4 \not\equiv 2 \pmod{49}$, ezért $d = 2$ esetén nincs megoldás (1 pont).

**b)** Az indextáblázat a következő:

| $j$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^j \pmod{13}$ | 1 | 2 | 4 | 8 | 3 | 6 | 12 | 11 | 9 | 5 | 10 | 7 |

(3 pont)

Tehát $11 \equiv 2^7$, $3 \equiv 2^4 \pmod{13}$. Így (mivel az $x \equiv 0$ nem megoldás), az $x \equiv 2^y \pmod{13}$ alakban kereshetjük a megoldást és az eredeti egyenlet a $7+3y \equiv 4 \pmod{12}$ egyenlettel ekvivalens (1 pont). Ennek az $y \equiv -1 \pmod 4$ a megoldása, azaz $y \equiv -1, 3, 7 \pmod{12}$, amiből $x \equiv 7, 8, 11 \pmod{13}$ megoldások adódnak (1 pont).

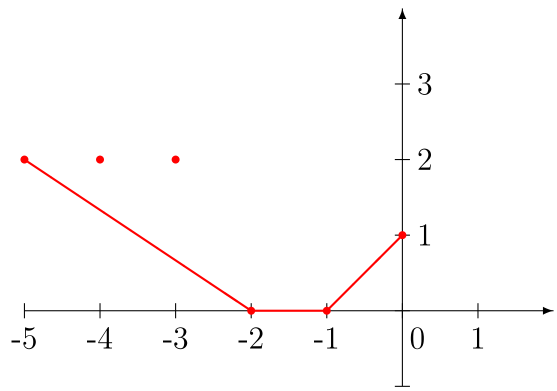
**3.** **a)** Az $x^{24} - 1 = \prod_{d|24} \Phi_d(x)$ (1 pont) és $x^{12} - 1 = \prod_{d|12} \Phi_d(x)$ azonosságokat használva $x^{24} - 1 = (x^{12} - 1)\Phi_8(x)\Phi_{24}(x)$ (1 pont). Innen $\Phi_{24}(x) = \frac{x^{12}+1}{x^4+1} = x^8 - x^4 + 1$ (1 pont).

**b)** Egy test fölötti harmadfokú polinom pontosan akkor irreducibilis, ha nincs gyöke a testben (1 pont). Tehát az olyan $\mathbb{F}_3$ fölötti harmadfokú polinomokat keressük, melyeknek a $0, \pm 1$ számok nem gyökei. Ezek $x^3 - x + 1$, $x^3 - x - 1$, $x^3 + x^2 - 1$, $x^3 + x^2 + x - 1$, $x^3 + x^2 - x + 1$, $x^3 - x^2 + 1$, $x^3 - x^2 + x + 1$, $x^3 - x^2 - x - 1$ (3 pont; $5 \le$helyes$-$helytelen$\le 7$: 2 pont, $2 \le$helyes$-$helytelen$\le 4$: 1 pont).

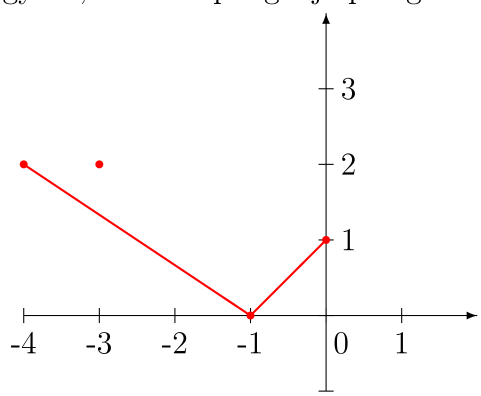
**c)** A $9x + 4 = 11y + 6$ lineáris diofantikus egyenletet kell megoldanunk (1 pont). Ennek megoldás $x = 10 + 11t$, $y = 8 - 9t$, azaz a lábak száma $9x + 4 = 94 + 99t$ alakú ($t \in \mathbb{Z}$) (1 pont). Mivel $99 + 94 > 180$ és $94 - 99 < 0$, ezért az egyetlen lehetséges érték a 94 (1 pont).

**4.** Mivel a $\Phi_n(x)$ körosztási polinom főegyütthatója 1, a $\Phi_n(x^k)\colon \Phi_n(x)$ maradékos osztást el lehet végezni $\mathbb{Z}[x]$-ben is. Így az oszthatóság pontosan akkor teljesül $\mathbb{Z}[x]$-ben, ha $\mathbb{C}[x]$-ben (1 pont). Viszont$\Phi_n(x)$-nek nincsenek többszörös gyökei (1 pont), ezért elég belátni, hogy a bal oldal minden gyöke gyöke a jobb oldalnak is (1 pont). Node $\Phi_n(x)$ gyökei pontosan a primitív $n$-edik egységgyökök (1 pont). Viszont ha $\varepsilon$ egy primitív $n$-edik egységgyök, akkor $\varepsilon^k$ rendje $\frac{n}{(n,k)} = n$ a hatvány rendjének képlete szerint (3 pont), azaz $\varepsilon^k$ is primitív $n$-edik egységgyök (1 pont), speciálisan $\Phi_n(\varepsilon^k) = 0$ (1 pont). Ez pedig azt jelenti, hogy $\varepsilon$ gyöke a $\Phi_n(x^k)$ polinomnak (1 pont).

**5.** A felbontás a következő: $9x^5 + 18x^4 + 9x^3 + x^2 + 4x + 3 = (x + 1)(9x^4 + 9x^3 + x + 3)$ (1 pont). A $p = 3$ prímre a polinom Newton-poligonja az alábbi töröttvonal (3 pont).




Tehát ha a polinomnak van racionális gyöke, akkor annak 3-adikus értékelése 0 vagy 1 (1 pont). Másrészt a polinom minden együtthatója nemnegatív, tehát csak negatív gyök jöhet szóba. Ezt kombinálva a racionális gyökteszttel, a $-1$-et és a $-3$-at elég behelyettesíteni (1 pont). A $-1$ tényleg gyök, a $-3$ viszont nem (1 pont). Tehát $9x^5 + 18x^4 + 9x^3 + x^2 + 4x + 3 = (x + 1)(9x^4 + 9x^3 + x + 3)$, ahol $9x^4 + 9x^3 + x + 3$-nak már nincs gyöke, Newton-poligonja pedig




Viszont a Newton-poligont csak 1 hosszú és 3 hosszú töröttvonal uniójára lehet bontani, ezért a polinom – ha felbomlik – csak első- és harmadfokú polinom szorzatára bomolhat (2 pont). Ez pedig nem lehetséges, hiszen nincs gyöke (1 pont).

**6.** Ha $p = 2$, akkor tetszőleges $b$ egész szám megfelel (1 pont). Legyen $p$ páratlan. Ekkor a Legendre-szimbólum tulajdonságai miatt $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ (3 pont), azaz $\left(\frac{-2}{p}\right)$, $\left(\frac{-1}{p}\right)$, és $\left(\frac{2}{p}\right)$ közül nem lehet mindhárom $-1$ (3 pont). Viszont ha $\left(\frac{a}{p}\right) = 1$, akkor van olyan $b$ egész szám, melyre $b^2 \equiv a \pmod{p}$, azaz $p \mid b^2 - a$ (2 pont), tehát olyan $b$ egész mindenképp van, melyre $p \mid (b^2+1)(b^2-2)(b^2+2)$ (1 pont).

**7.** A mátrix $i$-edik sorának $j$-edik eleme legyen $\alpha_j^{i-1}$ ($1 \le i \le 37$, $1 \le j \le 2023$), ahol $\alpha_1, \dots, \alpha_{2023}$ páronként különböző (komplex) számok. Ekkor tetszőleges $37 \times 37$-es aldetermináns egy Vandermonde-determináns, ami nem 0 (10 pont).