

Név: Unger Tamás István
(FTDIY7)

Összpontszám:

16 p
CC

Algebra és számelmélet

2. zárthelyi

(2018. 11. 24.)

1. Feladat. (4 pont)

Igazak-e a következő állítások. Válaszait röviden indokolja.

(A) Ha $n > 2$ egész, akkor $\varphi(n)$ páros.

(B) Az $x^3 + \bar{1}$ polinom irreducibilis a $\mathbb{Z}_3[x]$ polinomgyűrűben.

(C) Az $(x^2 + \bar{1})u \equiv \bar{1} \pmod{m}$ kongruencia nem oldható meg a $\mathbb{Z}_2[x]$ polinomgyűrűben, ahol $m = x^3 + x^2 + \bar{1}$

2. Feladat. (4 pont)

Határozzon meg olyan $u, v \in \mathbb{R}[x]$ polinomokat, amelyekre $fu + gv = \text{ln. k. o.}(f, g)$, ha

$$f = x^5 + 3x^4 + x^3 + x^2 + 3x + 1, \text{ és } g = x^4 + 2x^3 + x + 2.$$

3. Feladat. (4 pont)

Oldja meg az $fu + gv = \bar{1}$ egyenletet a $\mathbb{Z}_5[x]$ polinomgyűrűben, ahol

$$f = x^2 + \bar{3}x + \bar{1} \quad \text{és} \quad g = x^3 + \bar{2}x^2 + \bar{4}x + \bar{2}.$$

4. Feladat. (4 pont)

Adjon meg a $\mathbb{Z}_7$ test fölött két olyan különböző polinomot, amelyek ugyanazt a polinomfüggvényt adják meg. Indokolja meg választását.

5. Feladat. (4 pont)

Adja meg egy 4 elemű test művelet táblázatait.

② I.) $(x^5 + 3x^4 + x^3 + x^2 + 3x + 1) : (x^4 + 2x^3 + x + 2) = x + 1$

$$\begin{array}{r} x^5 + 3x^4 + x^3 + x^2 + 3x + 1 \\ - (x^5 + 2x^4 + x^2 + 2x) \\ \hline \end{array}$$

$$\begin{array}{r} x^4 + x^3 + x + 1 \\ - (x^4 + 2x^3 + x + 2) \\ \hline \end{array}$$

$$\boxed{-x^3 - 1}$$

Kaptuk: $f = g(x+1) + (-x^3 - 1)$

II.) $(x^4 + 2x^3 + x + 2) : (-x^3 - 1) = -x - 2$

$$\begin{array}{r} x^4 + 2x^3 + x + 2 \\ - (-x^4 - x) \\ \hline \end{array}$$

$$\begin{array}{r} 2x^3 + 2 \\ - (2x^3 + 2) \\ \hline 0 \end{array}$$

Kaptuk: $\text{lnko}(f, g) = x^3 + 1$

(előjele nemdegy.)

Az első lépésből:

$$-x^3 - 1 = f - g(x+1) \quad / \cdot (-1)$$

$$\underbrace{x^3 + 1}_{\text{lnko}(f, g)} = g(x+1) - f$$

Tehát: $\underbrace{f(-1)}_u + \underbrace{g(x+1)}_v = x^3 + 1 = \text{lnko}(f, g).$ $\square$

③ $\mathbb{Z}_5[x]$ van.

I.) $(x^3 + 2x^2 + 4x + 2) : (x^2 + 3x + 1) = x + 4$
 $\begin{array}{r} x^3 + 2x^2 + 4x + 2 \\ - (x^3 + 3x^2 + x) \\ \hline 4x^2 + 3x + 2 \\ - (4x^2 + 2x + 4) \\ \hline x + 3 \end{array}$

Kapjuk: $g = f(x+4) + (x+3).$

II.) $(x^2 + 3x + 1) : (x+3) = x$
 $\begin{array}{r} x^2 + 3x + 1 \\ - (x^2 + 3x) \\ \hline 1 \end{array}$

Kapjuk: $f = (x+3)x + 1$

$$1 = f - (x+3)x$$

$$1 = f - [g - f(x+4)]x$$

$$1 = f - g(x) + f(x^2 + 4x)$$

$$1 = \underbrace{f(x^2 + 4x + 1)}_u + \underbrace{g(4x)}_v.$$

$$(x+3) = g - f(x+4).$$

$\Updownarrow$

oda be.

①

(A) Igaz. A φ -függvény gyengén multiplikatív,
a szorzat tényleg: rögzített pedig csak akkor működik,
pontos, ha $n \leq 2$, de ez is van ráva.

$$\varphi(a) = a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) = (p_1 - 1)(p_2 - 1).$$

$\uparrow$
 $a = p_1 p_2$

(B) $\mathbb{Z}_3$ elemei: $\bar{0}, \bar{1}, \bar{2}$.

Kell: $X^3 + \bar{1} = \bar{0}$ vagy $X \in \mathbb{Z}_3 \Rightarrow$ ez nem irreducibilis.

$$\bar{0}: \bar{0}^3 + \bar{1} = \bar{1} \neq \bar{0}.$$

$$\bar{1}: \bar{1}^3 + \bar{1} = \bar{2} \neq \bar{0}.$$

$$\bar{2}: \bar{2}^3 + \bar{1} = \bar{2} + \bar{1} = \bar{0} \Rightarrow X^3 + \bar{1} \text{ nem irreducibilis, HAMIS.}$$

$$\bar{2}^3 = \bar{2} \cdot \bar{2} \cdot \bar{2} = \bar{2}$$

$$\text{Amly: } X^3 + \bar{1} =$$

$$(X^3 + \bar{1}) : (X + \bar{1}) = X^2 + \bar{2}X + \bar{1}$$

$$-(X^3 + X^2)$$

$$\underline{2X^2 + \bar{1}}$$

$$-(2X^2 + \bar{2}X)$$

$$\underline{X + \bar{1}}$$

$$-(X + \bar{1})$$

$$\underline{0}.$$

Tehát a felbontás:

$$X^3 + \bar{1} = (X + \bar{1})(X^2 + \bar{2}X + \bar{1}).$$

(C) Nézzük: $(X^2 + \bar{1}) \equiv \bar{1} \pmod{X^3 + X^2 + \bar{1}} \quad \mathbb{Z}_2[X] - \text{ba.}$

$$\text{I.) } (X^3 + X^2 + \bar{1}) : (X^2 + \bar{1}) = X + \bar{1}$$

$$-(X^3 + X)$$

$$\underline{X^2 + X + \bar{1}}$$

$$-(X^2 + \bar{1})$$

$$\underline{X}.$$

$$X^3 + X^2 + \bar{1} = (X^2 + \bar{1})(X + \bar{1}) + X.$$

$$\text{II.) } (x^2 + \bar{1}) : x = \bar{x} \\ \underline{-(x^2)} \\ \bar{1}$$

$\bar{1}$ ← itt a két polinom lineáris, $\bar{1} | \bar{1}$, ezért

a kongruencia megoldható.

$$\text{III.) } x : \bar{1} = x \\ \underline{-(x)} \\ 0$$

↓
HÁNIS az ellátás.

5.) $x^2 + x + 1$ irreduc $\mathbb{Z}_2$ felett?

$$\bar{0}: \bar{0}^2 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0} \Rightarrow \text{IGEW.}$$

$$\bar{1}: \bar{1}^2 + \bar{1} + \bar{1} = \bar{1} \neq \bar{0}$$

Tehát a faktorgyűrű (ami test is!) $\mathbb{Z}_2[x]/(x^2 + x + \bar{1})$. ↑ emiatt.

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

•	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

Mellékadatok:

$$\bar{x} \cdot \bar{x} = \bar{x}^2$$

$$x^2 : (x^2 + x + \bar{1}) = \bar{1} \\ \underline{-(x^2 + x + \bar{1})}$$

$$\bar{x} \cdot \overline{x+1} = \overline{x^2 + x}$$

$$(x^2 + x) : (x^2 + x + \bar{1}) = \bar{1} \\ \underline{-(x^2 + x + \bar{1})}$$

$$\bar{x} \cdot \overline{x+1} = \overline{x^2 + x}$$

$$(x+1)(x+1) = x^2 + 2x + \bar{1}$$

$$(x^2 + 2x + \bar{1}) : (x^2 + x + \bar{1}) = \bar{1} \\ \underline{-(x^2 + x + \bar{1})}$$

④ $\mathbb{Z}_7$ felett vizsgáljuk. Mivel 7 prím, ezért $\mathbb{Z}_7$ test.

Multiplikatív egységelem: 1.

$$\left. \begin{array}{l} p_1 = \bar{2}x \\ p_2 = \bar{3}x + \bar{4} \end{array} \right\} \text{Mégis ugyanazt adják meg}$$

$$\left. \begin{array}{l} \bar{1} \cdot \bar{1} = \bar{1} \\ \bar{2} \cdot \bar{4} = \bar{1} \\ \bar{3} \cdot \bar{5} = \bar{1} \\ \bar{4} \cdot \bar{2} = \bar{1} \\ \bar{5} \cdot \bar{3} = \bar{1} \\ \bar{6} \cdot \bar{6} = \bar{1} \end{array} \right\}$$

$\mathbb{Z}_7$ egységei: $\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$.

MINDEGYIK ELEM.
(Inverze a nulla).
 $\bar{0}$.

•	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Kell: $p_1, p_2 \in \mathbb{Z}_7[X]$,

hogy

$$p_1(x) = p_2(x)$$

$\forall x \in \mathbb{Z}_7$ -re, de

$$p_1(x) \neq p_2(x).$$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
p_1	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
p_2	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$

$$p_1 = \bar{2}x$$

$$p_2 = \bar{3}x + \bar{4}$$

$$p_1 = \bar{2}x$$

$$p_1 = \bar{3}x$$

$$p_2 =$$

Az is előfordulhat, hogy nem is lehet ilyet megadni
a scsótálka mell.