

## תרגיל מספר 8 מבנים אלגבריים

1. יהיו  $a(x), b(x) \in \mathbb{F}[x]$  שני פולינומים. נחלק את  $a(x)$  ב  $b(x)$  ע"י אלגוריתם לחילוק פולינומים ונקבל  $q(x), r(x)$  כך ש

$$a(x) = q(x)b(x) + r(x)$$

הוכיחו כי  $\gcd(a(x), b(x)) = \gcd(b(x), r(x))$   
**פתרון :**

טענה: לכל  $y(x)$  מתקיים כי:

$$y(x) | a(x), b(x) \iff y(x) | b(x), r(x)$$

בכיוון אחד: נתון  $y(x) | a(x), b(x)$  ולכן  $r(x) = a(x) - q(x)b(x)$  ולכן  $y(x) | b(x), r(x)$ .

בכיוון השני: נתון  $y(x) | b(x), r(x)$  ולכן  $a(x) = y(x)q(x) + r(x)$  ולכן  $y(x) | a(x), b(x)$ .

בפרט  $\gcd(a(x), b(x)), \gcd(b(x), r(x))$  מחלקים אחד את השני. בפרט קיימים  $\alpha(x), \beta(x)$  כך ש

$$\gcd(a(x), b(x)) = \alpha(x) \cdot \gcd(b(x), r(x))$$

$$\gcd(b(x), r(x)) = \beta(x) \cdot \gcd(a(x), b(x))$$

ביחד נקבל כי

$$\gcd(a(x), b(x)) = \alpha(x) \cdot \gcd(b(x), r(x)) = \alpha(x) \cdot \beta(x) \cdot \gcd(a(x), b(x))$$

ולכן  $\alpha(x) \cdot \beta(x) = 1$  בפרט  $\alpha(x), \beta(x)$  פולינומים קבועים, כלומר  $\alpha(x) = c_1, \beta(x) = c_2$  עבור  $c_1, c_2 \in \mathbb{F}$  קבועים. לכן

$$\gcd(a(x), b(x)) = c_1 \cdot \gcd(b(x), r(x))$$

כיוון ששני הפולינומים מתוקנים (לפי הגדרה) נקבל כי  $c_1 = 1$  ולכן  $\gcd(a(x), b(x)) = \gcd(b(x), r(x))$

2. יהיו  $a(x), b(x), c(x) \in \mathbb{F}[x]$  שלושה פולינומים הוכיחו כי אם  $\gcd(a(x), c(x)) = 1$  ו- $\gcd(b(x), c(x)) = 1$

$$\gcd(a(x)b(x), c(x)) = 1$$

**פתרון :** לפי המפשט קיימים פולינומים  $t_1(x), s_1(x), t_2(x), s_2(x)$  כך ש

$$t_1(x)a(x) + s_1(x)c(x) = 1$$

$$t_2(x)b(x) + s_2(x)c(x) = 1$$

נכפיל ונקבל כי

$$[t_1(x)a(x) + s_1(x)c(x)][t_2(x)b(x) + s_2(x)c(x)] = 1$$

אחרי פתיחת סוגריים נקבל

$$t(x)a(x)b(x) + s(x)c(x) = 1$$

[ כאשר  $t(x) = t_1(x)t_2(x), s(x) = t_1(x)a(x)s_2(x) + s_1(x)t_2(x)b(x) + s_1(x)c(x)s_2(x)$ .

טענה:  $\gcd(a(x)b(x), c(x)) = 1$ . ברור כי 1 מחלק את  $a(x)b(x), c(x)$ . נניח  $d(x) | c(x), a(x)b(x)$  אזי  $d(x) | t(x)a(x)b(x) + s(x)c(x) = 1$  ולכן  $d(x) | 1$  ולכן  $d(x) \in \mathbb{F}$  בפרט

$$\deg(d) = 0 \leq \deg(1)$$

וסיימו.

3. תרגיל: הוכיחו כי אם  $p(x) \in \mathbb{F}[x]$  פולינום אי פריק אזי הוא ראשוני. [היעזרו בתרגיל הקודם]

**פתרון :** נתחיל עם ההנחה כי  $p(x)$  מתוקן.

כעת יהיו  $a(x), b(x)$  כך ש  $p(x) | a(x)b(x)$  נוכיח כי  $p(x) | b(x)$  או  $p(x) | a(x)$ . נסמן  $d(x) = \gcd(a(x), p(x))$

אזי בפרט  $d(x) | p(x)$  ולכן קיים  $q(x)$  כך ש  $p(x) = d(x)q(x)$  כיוון ש  $p(x)$  אי פריק חייב להיות כי הדרגה של  $d(x)$  או  $q(x)$  שווה ל  $p(x)$  ושל הפולינום השני היא 0.

אם  $\deg(d(x)) = \deg(p(x))$  אזי הם שווים (כי שניהם מתוקנים מאותה דרגה) ובפרט  $p(x) = d(x)a(x)$  וסיימו

אחרת  $\deg(d(x)) = 0$  ואז  $d(x) = 1$ .

באותו אופן נסמן  $d'(x) = \gcd(b(x), c(x))$ . ואז אם  $\deg(d'(x)) = \deg(p(x))$  אז הם שווים ו  $p(x) | b(x)$  וסיימו.

אחרת  $d'(x) = 1$  ואז  $\gcd(a(x), c(x)) = \gcd(b(x), c(x)) = 1$  ולפי תרגיל קודם  $\gcd(a(x)b(x), c(x)) = 1$  אבל  $\gcd(a(x)b(x), p(x)) = p(x)$  כי  $p(x)$  מתוקן מחלק את  $p(x)$  וגם  $a(x)b(x)$ .

בחיבור הנתונים נקבל  $p(x) = 1$  סתירה לכך שמדרגתו גדולה מ-0 (כמו כל פולינום אי פריק).

כעת, אם  $p(x)$  אינו מתוקן נגדיר

$$p'(x) = c^{-1}p(x)$$

כאשר  $c$  הוא המקדם המוביל של  $p(x)$  ואז  $p'(x)$  פולינום מתוקן ומתקיים כי  $p(x)$  מחלק את  $p'(x)$  וכן להיפך. לכן:

אם  $p(x)|a(x)b(x)$  אזי  $p'(x)|a(x)b(x)$  ואז לפי ראשית התרגיל  $p'(x)|a(x)$  או  $p'(x)|b(x)$  ואז  $p(x)|a(x)$  או  $p(x)|b(x)$  וסיימנו.

.4

(א) נגדיר:  $a(x) = 1 + 2x^2, b(x) = 2 + x \in \mathbb{R}[x]$  מצא  $d = \gcd(a, b)$  ומצא  $p, q$  כך ש  $ap + qb = d$

פתרון : נחשב

$$\begin{aligned} a(x) &= b(x) \cdot (2x - 4) + 9 \\ b(x) &= (9) \left( \frac{1}{9}x + \frac{2}{9} \right) + 0 \end{aligned}$$

ולכן

$$9 = a(x) - b(x) \cdot (2x - 4)$$

ומכאן ש

$$1 = \frac{1}{9}a(x) - \frac{2x-4}{9}b(x)$$

לכן  $\gcd(a, b) = 1$  כאשר  $p(x) = \frac{1}{9}, q(x) = -\frac{2x-4}{9}$   
 (ב) נגדיר:  $a(x) = 7x^7 + 6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x, b(x) = x^3 + x^2 \in \mathbb{R}[x]$  מצא  $d = \gcd(a, b)$  ומצא  $p, q$  כך ש  $ap + qb = d$

פתרון : נחשב

$$\begin{aligned} a(x) &= b(x) \cdot (7x^4 - x^3 + 6x^2 - 2x + 5) + (-3x^2 + x) \\ b(x) &= (-3x^2 + x) \left( -\frac{x}{3} - \frac{4}{9} \right) + \left( \frac{4}{9}x \right) \\ (-3x^2 + x) &= \left( \frac{4}{9}x \right) \cdot \left( -\frac{27}{4}x + \frac{9}{4} \right) + 0 \end{aligned}$$

ולכן

$$\begin{aligned} \frac{4}{9}x &= b(x) - (-3x^2 + x) \left( -\frac{x}{3} - \frac{4}{9} \right) \\ &= b(x) - [a(x) - b(x) \cdot (7x^4 - x^3 + 6x^2 - 2x + 5)] \left( -\frac{x}{3} - \frac{4}{9} \right) \\ &= b(x) \left[ 1 + (7x^4 - x^3 + 6x^2 - 2x + 5) \left( -\frac{x}{3} - \frac{4}{9} \right) \right] + a(x) \left( \frac{x}{3} + \frac{4}{9} \right) \end{aligned}$$

ומכאן ש

$$x = b(x) \frac{[1 + (7x^4 - x^3 + 6x^2 - 2x + 5) (-\frac{x}{3} - \frac{4}{9})]}{4/9} + a(x) \frac{(\frac{x}{3} + \frac{4}{9})}{4/9}$$

$$p(x) = \frac{9}{4} (\frac{x}{3} + \frac{4}{9}), q(x) = \frac{9}{4} [1 + (7x^4 - x^3 + 6x^2 - 2x + 5) (-\frac{x}{3} - \frac{4}{9})]$$

### מספרים שלמים - אנלוגיות ותרגילים.

משפט (חילוק מספרים שלמים): לכל  $a, b \in \mathbb{Z}^+ = \mathbb{N} \cup \{0\}$  כך ש  $b \neq 0$  קיימים  $r, q \in \mathbb{Z}^+$  כך ש

$$a = qb + r$$

המקסימום  $r < b$  או  $r = 0$ . והם יחידים. משפט ((קיום gcd): לכל  $a, b \in \mathbb{Z}$  קיים  $d = \gcd(a, b) \in \mathbb{N}$  המקיים

$$d \mid a, b \quad .1$$

$$.2 \quad \text{לכל } d' \in \mathbb{Z}^+ \text{ מתקיים: אם } d' \mid a, b \text{ אזי } d \leq d'.$$

$$.3 \quad \text{בנוסף קיימים } m, n \in \mathbb{Z} \text{ כך ש}$$

$$d = an + bm$$

.4

(א) יהיו  $a, p \in \mathbb{N}$  מספרים טבעיים זרים (כלומר  $\gcd(a, p) = 1$ ) הוכח כי קיים  $0 \leq c < p$  שלם כך ש  $ac = 1 \pmod p$ .  
**פתרון:** מתכונת gcd קיימים  $r, s \in \mathbb{Z}$  כך ש

$$ar + ps = \gcd(a, p) = 1$$

נפעיל מוד  $p$  על שני האגפים ונקבל כי

$$1 = ar + ps = ar \pmod p$$

כעת נחלק את מחלקת השקילות של  $r$  (ביחס למוד  $p$ ) שווה למחלקת של  $i$  כך  $i \in \{0, \dots, p-1\}$  [ראינו כי ביחס למוד  $p$ , קבוצת המנה היא  $\{[0], \dots, [p-1]\}$  ולכן  $r \equiv i \pmod p$ ]

$$1 \equiv ar \equiv ai \pmod p$$

(ב) הוכח כי עבור  $p$  ראשוני  $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$  הינו שדה. **פתרון:** ידוע כי  $\mathbb{Z}_p$  הוא חוג חילופי עם יחידה. מספיק להראות כי הוא חוג עם חילוק. כלומר לכל  $a \in \mathbb{Z}_p$ ,  $a \neq 0$  קיים הופכי בחוג. אכן אם  $a \neq 0$  אזי  $\gcd(a, p) = 1$  כי  $p$  ראשוני (המחלקים היחידים של  $p$  הן  $1, p$  אם  $p$  מחלק את  $a$  אזי  $a = 0$  בחוג שלנו). לפי הסעיף הקודם קיים  $0 \leq c < p$  כך ש  $ac = 1 \pmod p$  כלומר  $ac = 1$  כאשר הכפל הוא הכפל של החוג (שזהו כפל  $\pmod p$ ) ולכן  $c$  הוא ההופכי של  $a$ .

.5

(א) יהיו  $a, n$  מספרים טבעיים כך ש  $a, n$  זרים (כלומר  $\gcd(a, n) = 1$ ) הוכח כי לכל  $b$  טבעי קיים פתרון למשוואה

$$ax = b \pmod n$$

והוכח כי פתרון זה יחיד אם נוסיף את הדרישה כי  $0 \leq x < n$ . **פתרון:** לפי שאלה קודמת קיים  $c$  כך ש  $ac = 1 \pmod n$ . יהיה  $b$  נתון אזי אם נכפיל את המשוואה

$$ax = b \pmod n$$

ב  $c$  נקבל כי

$$cb = cax = acx = x \pmod n$$

ולכן  $x = cb \pmod n$  ולכן גם  $x = cb + kn$  הוא פתרון לכל  $k$  שלם. נבחר  $k$  כזה כך ש  $0 \leq cb + kn < n$ .

נראה יחידות: נניח  $x_1, x_2$  פתרונות למשוואה ובנוסף  $0 \leq x_1, x_2 < n$  אזי

$$ax_1 = b = ax_2 \pmod n$$

בהכפלה ב  $c$  נקבל כי

$$x_1 = x_2 \pmod n$$

ולכן  $x_1 - x_2 = 0 \pmod n$  כלומר  $x_1 - x_2$  הוא מספר שמתחלק ב  $n$  ובנוסף  $|x_1 - x_2| < n$  ולכן  $x_1 - x_2 = 0$  שגורר כי  $x_1 = x_2$

(ב) יהיו  $a = 80, n = 567$  מצא  $d = \gcd(a, n)$  ומצא  $p, q$  כך ש  $ap + qn = d$ . אם  $a$  הפיך מודולו  $n$  מצא את ההופכי שלו ופתור את המשוואה  $ax \equiv 3 \pmod n$  **פתרון:** נחשב

$$567 = 80 \cdot 7 + 7$$

$$80 = 7 \cdot 11 + 3$$

$$7 = 3 \cdot 2 + 1$$

ולכן

$$1 = 7 - 3 \cdot 2$$

$$= 7 - (80 - 7 \cdot 11) \cdot 2 = 23 \cdot 7 - 2 \cdot 80$$

$$= 23 \cdot (567 - 80 \cdot 7) - 2 \cdot 80 = 23 \cdot 567 - 163 \cdot 80$$

ולכן  $\gcd(a, b) = 1$  כאשר ההופכי של  $a$  מודולו  $n$  הוא  $-163$   
 לכן הפתרון למשוואה הוא  $-163 \cdot 3 = -489 \equiv 78$   
 (ג) יהיו  $a = 1573, n = 65065$  מצא  $d = \gcd(a, n)$  ומצא  $p, q$  כך ש  $ap + qn = d$   
 אם הפיך מודולו  $n$  מצא את ההופכי שלו ופתור את המשוואה  $ax \equiv 3 \pmod n$   
**פתרון:** נחשב

$$\begin{aligned} 65065 &= 1573 \cdot 41 + 572 \\ 1573 &= 572 \cdot 2 + 429 \\ 572 &= 429 \cdot 1 + 143 \\ 429 &= 143 \cdot 3 + 0 \end{aligned}$$

ולכן

$$\begin{aligned} 143 &= 572 - 429 \cdot 1 \\ &= 572 - (1573 - 572 \cdot 2) \cdot 1 = 3 \cdot 572 - 1 \cdot 1573 \\ &= 3 \cdot (65065 - 1573 \cdot 41) - 1 \cdot 1573 = 3 \cdot 65065 - 124 \cdot 1573 \end{aligned}$$

ולכן  $\gcd(a, n) = 143$  בפרט  $a$  אינו הפיך. למה?  
 נניח כי  $a$  הפיך אזי קיים  $b$  כך ש  $ab \equiv 1 \pmod n$   
 נכפיל את שני האגפים ב  $m = \frac{n}{\gcd(a, n)} \in \mathbb{Z}$  ונקבל כי

$$m = amb = \underbrace{\frac{a}{\gcd(a, n)}}_{\in \mathbb{Z}} nb \equiv 0 \pmod n$$

אבל  $m = \frac{65065}{143} = 455 \not\equiv 0 \pmod n$  סתירה

### משפט השאריות הסיני

נצטט ונדגים מקרה פרטי של משפט השאריות הסיני:  
 משפט: יהיו  $p_1, p_2, p_3$  שלושה מספרים ראשוניים שונים. יהיו  $n_1, n_2, n_3$  מספרים טבעיים.  
 יהיו  $c_1, c_2, c_3$  מספרים שלמים קבועים.  
 אזי למערכת המשוואות

$$\begin{aligned} x &\equiv c_1 \pmod{p_1^{n_1}} \\ x &\equiv c_2 \pmod{p_2^{n_2}} \\ x &\equiv c_3 \pmod{p_3^{n_3}} \end{aligned}$$

קיים פתרון (יחיד עד כדי כפולות של  $p_1^{n_1} p_2^{n_2} p_3^{n_3}$ )  
 נמחיש זאת באמצעות התרגיל הבא:  
 מצא  $x$  שלם המקיים

$$\begin{aligned} x &\equiv 2 \pmod{2^3} \\ x &\equiv 5 \pmod{3^2} \\ x &\equiv 20 \pmod{5^2} \end{aligned}$$

לפי משפט הקודם מובטח כי קיים כזאת  $x$ .

1. כיוון ש  $2^3$  זר ל  $3^2 5^2$  ניתן למצוא  $c, d$  שלמים כך ש

$$c \cdot 2^3 + d \cdot 3^2 5^2 = 1 = \gcd(3^2 5^2, 2^3)$$

ולכן

$$1 - c \cdot 2^3 = d \cdot 3^2 5^2$$

נסמן  $e_1 = 1 - c \cdot 2^3 = d \cdot 3^2 5^2$  ואז (השתכנעו!)

$$e_1 = 1 \pmod{2^3}$$

$$e_1 = 0 \pmod{3^2 5^2}$$

מצאו את  $e_1$   
פתרון : נחשב

$$3^2 5^2 = 2^3 \cdot 28 + 1$$

$$e_1 = 2^3 \cdot 28 + 1 = 225 \text{ לכן}$$

(א) באותו אופן מצאו  $e_2$  שלם המקיים

$$e_2 = 1 \pmod{3^2}$$

$$e_2 = 0 \pmod{2^3 5^2}$$

ו  $e_3$  שלם המקיים

$$e_3 = 1 \pmod{5^2}$$

$$e_3 = 0 \pmod{2^3 3^2}$$

פתרון : נחשב

$$2^3 5^2 = 3^2 \cdot 22 + 2$$

$$3^2 = 2 \cdot 4 + 1$$

ולכן

$$1 = 3^2 - 2 \cdot 4 = 3^2 - (2^3 5^2 - 3^2 \cdot 22) \cdot 4 = 89 \cdot 3^2 - 4 \cdot 2^3 5^2$$

$$e_2 = 1 - 89 \cdot 3^2 = -800 \text{ לכן}$$

נחשב

$$2^3 3^2 = 5^2 \cdot 2 + 22$$

$$5^2 = 22 \cdot 1 + 3$$

$$22 = 3 \cdot 7 + 1$$

ולכן

$$1 = 22 - 3 \cdot 7 = 22 - (5^2 - 22 \cdot 1) \cdot 7 = 8 \cdot 22 - 7 \cdot 5^2$$

$$= 8 \cdot (2^3 3^2 - 5^2 \cdot 2) - 7 \cdot 5^2 = -23 \cdot 5^2 + 8 \cdot 2^3 3^2$$

$$e_3 = 1 + 23 \cdot 5^2 = 576 \text{ לכן}$$

(ב) כעת הגדירו את  $x = 2e_1 + 5e_2 + 20e_3$  ובידקו כי הוא פתרון למערכת שבשאלה.  
**פתרון :** נחשב

$$x = 2e_1 + 5e_2 + 20e_3 = 2 \cdot 225 + 5 \cdot (-800) + 20 \cdot 576 = 7970 \equiv 770 \pmod{2^3 3^2 5^2}$$

ואכן

$$770 \equiv 2 \pmod{2^3}$$

$$770 \equiv 5 \pmod{3^2}$$

$$770 \equiv 20 \pmod{5^2}$$