

תרגיל מספר 8 מבנים אלגבריים

15 בינואר 2017

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

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

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

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

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 $ap + qb = d$

(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 $ap + qb = d$

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 (וקיום \gcd): לכל $a, b \in \mathbb{Z}$ קיים $d = \gcd(a, b) \in \mathbb{N}$ המקיים

1. $d \mid a, b$

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

3. בנוסף קיימים $m, n \in \mathbb{Z}$ 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 $ac \equiv 1 \pmod{p}$.

(ב) הוכח כי עבור p ראשוני אכן $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ הינו שדה.

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

$$ax \equiv b \pmod{n}$$

והוכח כי פתרון זה יחיד אם נוסיף את הדרישה כי $0 \leq x < n$

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

(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 $ax \equiv 3 \pmod{n}$

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

$$x \equiv c_1 \pmod{p_1^{n_1}}$$

$$x \equiv c_2 \pmod{p_2^{n_2}}$$

$$x \equiv c_3 \pmod{p_3^{n_3}}$$

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!)

$$\begin{aligned} e_1 &= 1 \pmod{2^3} \\ e_1 &= 0 \pmod{3^2 5^2} \end{aligned}$$

מצאו את e_1

(א) באותו אופן מצאו e_2 שלם המקיים

$$\begin{aligned} e_2 &= 1 \pmod{3^2} \\ e_2 &= 0 \pmod{2^3 5^2} \end{aligned}$$

ו e_3 שלם המקיים

$$\begin{aligned} e_3 &= 1 \pmod{5^2} \\ e_3 &= 0 \pmod{2^3 3^2} \end{aligned}$$

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