

תרגיל מספר 10 מבנים אלגבריים

11 בינואר 2016

1.

(א) יהיו a, p מספרים טבעיים זרים (כלומר $\gcd(a, p) = 1$) הוכח כי קיים $0 \leq c < p$ טבעי 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

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

כיוון שהמשוואה היא מוד p נוכל במקום r לקחת כל מספר מהצורה $r + kp$ עבור k שלם. בפרט אפשר להחליף את r ב $r + kp$ המקיים $0 \leq r + kp < p$ ולקבל

$$1 = ar \pmod p = ar + akp \pmod p = a(r + kp) \pmod p$$

ואז $c = r + kp$ הוא המספר המבוקש.

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

פתרון: ידוע כי \mathbb{Z}_p הוא חוג חילופי עם יחידה. מספיק להראות כי הוא חוג עם חילוק. כלומר לכל $0 \neq a \in \mathbb{Z}_p$ 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 $ac = 1 \pmod p$ (כאשר $ac = 1 \pmod p$ כפול של החוג (שזהו כפול $\pmod p$) ולכן c הוא ההופכי של a .)

2.

(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 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 $ap + qn = d$.

פתרון : נחשב

$$\begin{aligned} 567 &= 80 \cdot 7 + 7 \\ 80 &= 7 \cdot 11 + 3 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

ולכן

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - (80 - 7 \cdot 11) \cdot 2 = 23 \cdot 7 - 2 \cdot 80 \\ &= 23 \cdot (567 - 80 \cdot 7) - 2 \cdot 80 = 23 \cdot 567 - 163 \cdot 80 \end{aligned}$$

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 a 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 $\gcd(a, b) = 143$ כאשר אין ההופכי ל a מודולו n

(א) נגדיר: $a(x) = 1 + 2x^2, b(x) = 2 + x$ מצא $d = \gcd(a, b)$ ומצא p, q כך ש
 $ap + qb = d$
 פתרון : נחשב

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

ולכן

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

ולכן (אם ניקח פולינום מתוקן) $\gcd(a, b) = 1$ כאשר $p(x) = \frac{4}{9} \left(1 - \frac{1}{2}x\right)$

(ב) נגדיר: $a(x) = 7x^7 + 6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x, b(x) = x^3 + x^2$ 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

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

ולכן (אם ניקח פולינום מתוקן) $\gcd(a, b) = x$ כאשר $p(x) = \frac{9}{4} \left[1 + (7x^4 - x^3 + 6x^2 - 2x + 5) \left(-\frac{x}{3} - \frac{4}{9}\right)\right]$

(א) הראו שיש בדיוק פולינום אי-פריק אחד ממעלה שניים ב $\mathbb{Z}_2[x]$.
פתרון: פולינום מדרגה לכל היותר 2 הוא מהצורה $p(x) = ax^2 + bx + c$ כאשר $a, b, c \in \mathbb{Z}_2$. אם הפולינום הוא אי פריק בפרט אין לו שורשים ולכן $p(0) \neq 0$ שזה גורר כי $c \neq 0$ וגם $p(1) \neq 0$ מה שגורר כי $a + b + c \neq 0$. כיוון שמדובר ב \mathbb{Z}_2 אזי שונה מאפס אומר שווה ל-1 ולכן

$$\begin{aligned} c &= 1 \\ a + b + c &= 1 \end{aligned}$$

וביחד

$$\begin{aligned} c &= 1 \\ a &= b \end{aligned}$$

כיוון שרוצים דרגה בדיוק 2 אזי $a \neq 0$ ולכן $a = 1$ ובס"ה נקבל כי $p(x) = x^2 + x + 1$. הוא אכן לא פריק כי אם הוא היה פריק היה לו שורש (כי אם $p(x) = a(x)b(x)$ אזי a, b פולינומים מדרגה 1 ואז אם $a(x) = x - \text{const}$ נקבל כי $p(\text{const}) = a(\text{const})b(\text{const}) = 0 \cdot \text{const} = 0$ אבל $p(1) \neq 0$ וגם $p(0) \neq 0$ ואלו השורשים היחידים האפשריים בשדה שלנו.

(ב) העזרו בסעיף א כדי לקבוע האם $x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$ פריק.
פתרון: אם $p(x) = x^5 + x^4 + 1$ היה פריק אזי $p(x) = a(x)b(x)$ כאשר המעלה של $a(x)$ היא 0 או 1 או 2 או 3 או 4 או 5. נעבור על האפשרויות מעלה 0 לא יכול לפי הגדרת פריקות של $p(x)$ מעלה 1 אומר של $p(x)$ יש שורש אבל $p(1) = p(0) = 1 \neq 0$ מעלה 2 אומר ש $a(x) = x^2 + x + 1$ לפי סעיף קודם כלומר $x^2 + x + 1$ מחלק את $p(x)$. נבדוק

$$\begin{aligned} p(x) &= a(x)x^3 + (x^3 + 1) \\ x^3 &= (x^3 + 1) \cdot 1 + 1 \\ 1 &= 1 \cdot 1 + 0 \end{aligned}$$

ולכן $\gcd(p, a) = 1$ בפרט a לא מחלק את p .
 מעלה 3/4/5 אומר שהמעלה של $b(x)$ היא 2/1/0 וכמו המקרה של $a(x)$ זה לא אפשרי.

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

$$\begin{aligned} x &\equiv 2 \pmod{2^3} \\ x &\equiv 4 \pmod{3^2} \\ x &\equiv 22 \pmod{5^2} \end{aligned}$$

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
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

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

ו e_3 שלם המקיים

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

פתרון : נחשב

$$\begin{aligned} 2^3 5^2 &= 3^2 \cdot 22 + 2 \\ 3^2 &= 2 \cdot 4 + 1 \end{aligned}$$

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

$$\begin{aligned} 1 &= 22 - 3 \cdot 7 = 22 - (5^2 - 22 \cdot 1) \cdot 7 = 8 \cdot 22 - 7 \cdot 5^2 \\ &= 8 \cdot (2^3 3^2 - 5^2 \cdot 2) - 7 \cdot 5^2 = -23 \cdot 5^2 + 8 \cdot 2^3 3^2 \end{aligned}$$

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

(ב) כעת הגדירו את $x = 2e_1 + 4e_2 + 22e_3$ ובידקו כי הוא פתרון למערכת שבשאלה.

פתרון : נחשב

$$x = 2e_1 + 4e_2 + 22e_3 = 9922 \equiv 922 \pmod{2^3 3^2 5^2}$$

ואכן

$$922 \equiv 2 \pmod{2^3}$$

$$922 \equiv 4 \pmod{3^2}$$

$$922 \equiv 22 \pmod{5^2}$$