

## 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  $ac = 1 \pmod p$ .

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

.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  $0 \leq x < n$ .

(ב) יהיו  $a = 80, n = 567$  מצא  $d = \gcd(a, n)$  ומצא  $p, q$  כך ש  $ap + qn = d$ .

(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  $ax \equiv 3 \pmod n$

.3

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

(ב) נגדיר:  $a(x) = 7x^7 + 6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x, b(x) = x^3 + x^2$  מצא  $d = \gcd(a, b)$  ומצא  $p, q$  כך ש  $ap + qb = d$

.4

(א) הראו שיש בדיוק פולינום אי-פריק אחד ממעלה שניים ב  $\mathbb{Z}_2[x]$

(ב) העזרו בסעיף א כדי לקבוע האם  $x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$  פריק.

### משפט השאריות הסיני

נצטט ונדגים מקרה פרטי של משפט השאריות הסיני:  
משפט: יהיו 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

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

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

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

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  $e_1$

(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

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

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