

תרגיל מספר 9 מבנים אלגבריים

להגשה עד 30.1.2015

1. 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 .

(א) כיוון ש 2^3 זר ל $3^2 5^2$ ניתן למצוא c, d שלמים כך ש

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

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

(ב) 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

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

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

.2

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

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

.3

(א) 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 $ax \equiv 3 \pmod{n}$

(ב) 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 $ax \equiv 3 \pmod{n}$