

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 המשואות

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

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

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

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 .

(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!)

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

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

מצאו את e_1

פתרון: נחשב

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

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

(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

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

פתרון : נחשב

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

ולכן

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

$$e_2 = 1 - 89 \cdot 3^2 = -800$$

נחשב

$$\begin{aligned}2^3 3^2 &= 5^2 \cdot 2 + 22 \\5^2 &= 22 \cdot 1 + 3 \\22 &= 3 \cdot 7 + 1\end{aligned}$$

ולכן

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

$$e_3 = 1 + 23 \cdot 5^2 = 576$$

(ג) 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

$$\begin{aligned}922 &\equiv 2 \pmod{2^3} \\922 &\equiv 4 \pmod{3^2} \\922 &\equiv 22 \pmod{5^2}\end{aligned}$$

(א) נגדיר: $b(x) = 2 + x$, $a(x) = 1 + 2x^2$ 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

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

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

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

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

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

.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 $ax \equiv 3 \pmod n$
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 $-163 \cdot 3 = -489 \equiv 78 \pmod n$

(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 $ax \equiv 3 \pmod n$
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 $\gcd(a, b) = 143$ אין ההופכי ל a מודולו n