

תרגווי מיוחדות 3:

תרגיל: הראה שהפולינום $f(x) = x^2 + 4x + 1$ אינו מתפצל ב- $\mathbb{Z}_m, \mathbb{R}, \mathbb{Q}$.

פתרון: נסתכל על $\mathbb{R}$ ונראה שיש פתרון.

נסתכל ב- $\mathbb{Z}_m$.

טענה: הפולינום $x^2 + bx + c \in \mathbb{Z}_p[x]$ ($p \neq 2$) מתפצל ב- $\mathbb{Z}_p$ אם ורק אם $b^2 - 4c$ הוא ריבוע מושלם ב- $\mathbb{Z}_p$.

ב- $\mathbb{Z}_p$.

$$x^2 + \frac{b}{2}x + c$$

אכן, $p \neq 2$ ולכן המשוואה $x^2 + bx + c = 0$ שקולה ל-

$$(x + \frac{b}{2})^2 = \frac{b^2 - 4c}{4} \Leftrightarrow$$

יש פתרון ב- $\mathbb{Z}_p$ אם ורק אם $b^2 - 4c = y^2$ ב- $\mathbb{Z}_p$. אכן, $\mathbb{Z}_p$ הוא שדה.

$$0 = (x + \frac{b}{2})^2 - (\frac{y}{2})^2 \Leftrightarrow (x + \frac{b}{2} - \frac{y}{2})(x + \frac{b}{2} + \frac{y}{2})$$

ורואה שיש פתרון (משפט) $(\frac{y}{2} - \frac{b}{2})$.

$$b^2 - 4c = 4(x + \frac{b}{2})^2 = 4(\frac{y}{2})^2 \Leftrightarrow (x + \frac{b}{2})^2 = \frac{b^2 - 4c}{4} = (\frac{y}{2})^2$$

ריבוע מושלם ב- $\mathbb{Z}_p$.

$$b^2 - 4c = 4^2 - 4 = 16 - 4 = 12 \equiv 1 \pmod{16}$$

1-1 הוא ריבוע ב- $\mathbb{Z}_m$ (נניח $1 \equiv 1$), p פריק מס $\mathbb{Z}_m$.

נמנה את הפתרון באי-פריק מס $\mathbb{Z}_m$: $x^2 + 4x + 1$

$$p(x) = (x-4)(x-3) \quad \begin{matrix} \leftarrow \frac{-3}{2} = \frac{3}{2} = 4 \\ \leftarrow \frac{-5}{2} = \frac{5}{2} = 3 \end{matrix} \quad \begin{matrix} \leftarrow \frac{-4 \pm \sqrt{2}}{2} = \frac{-4 \pm 1}{2} \end{matrix}$$