

כדי לבנות שדה מסדר 16 צריך למצוא פולינום אי-פריק ממעלה 4 מעל  $\mathbb{Z}_2$ . נחפש:  $x^4 + 1$  פריק כי יש לו שורש (1), הכי פשוט אחריו הוא  $x^4 + x + 1$ , שאין לו שורשים (מציבים 0,1). **זהירות:** זה עדיין לא אומר שהוא אי-פריק! המשפט "קיים שורש אמ"ם פריק" נכון רק עבור פולינומים ממעלה קטנה ממש מ-4 וכאן יש לנו פולינום ממעלה 4. איך מוכיחים שהוא אי-פריק? אם בפירוק שלו היה גורם לינארי (ממעלה 1) אז היה לו שורש. לכן האפשרות היחידה (במקרה זה) היא שהוא יתפרק למכפלה של שני פולינומים ריבועיים (ממעלה 2) אי-פריקים. צריך לבדוק "בידיים" ששום מכפלה של שני פולינומים אי-פריקים ממעלה 2 לא יתן  $x^4 + x + 1$ . באופן כללי זאת יכולה להיות משימה מפרכת, אבל בגלל שאנחנו מעל  $\mathbb{Z}_2$  יש ממש מעט פולינומים אי-פריקים ממעלה 2, למעשה יש רק אחד: נרשום את כל הפולינומים ממעלה 2:

$$x^2$$

$$x^2 + 1$$

$$x^2 + x$$

$$x^2 + x + 1$$

השלושה הראשונים הם פריקים (כי יש להם שורשים). השלישי אי פריק (כי הוא פולינום ממעלה 2 ואין לו שורשים). אם כך רק נשאר לבדוק ש- $(x^2 + x + 1)(x^2 + x + 1)$  לא שווה ל- $x^4 + x + 1$  וזה יראה שאכן  $x^4 + x + 1$  הוא אי-פריק. אכן:

$$(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1 = x^4 + x^2 + 1$$

מרגע שמצאנו את הפולינום האי-פריק ממשיכים לבנות את השדה כרגיל, כמו שעשינו בדוגמאות של שדות מסדר 4,8,9,27... (תזכורת: בונים את חוג המנה  $\mathbb{Z}_2[x] / \langle x^4 + x + 1 \rangle$ , רושמים את האיברים שלו: מחלקות שקילות של פולינומים ממעלה 3 ומטה, והכפל בשדה זה מתבצע לפי הכלל שנותן לנו הפולינום האי-פריק שמצאנו:  $x^4 + x + 1 = \bar{0}$  לכן  $x^4 = -x - 1 = x + 1$ )