

# ספירת פולינומים אי-פריקים מעל שדה סופי

## מרגיל מנחה

כמה גורמים אי-פריקים יש ל- $x^{64} - x$  מעל  $\mathbb{F}_2$ ?

נסמן ב- $n_q(k)$  את מספר הפולינומים האי-פריקים ממעלה  $k$  מעל  $\mathbb{F}_q$ .  
אם  $f$  פולינום אי-פריק ממעלה  $k$  מעל  $\mathbb{F}_q$  אזי הוא מחלק את  $x^{q^k} - x$ .  
הוספת שורש של  $f$  ל- $\mathbb{F}_q(\alpha)$  אזי  $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = k$ .  
השדה  $\mathbb{F}_q(\alpha)$  הוא שדה מפצל של  $f$  (כל שאר השורשים של  $f$  הם  $\alpha, \alpha^q, \dots, \alpha^{q^{k-1}}$ ).  
זהו שדה עם עצמה  $q^k$  ולכן כל איבריו הם שורשים של  $x^{q^k} - x$ .  
בצורה דומה עבור כל  $k \mid 64$ , כל פולינום אי-פריק מדרגה  $d$  מחלק גם את  $x^{64} - x$ .

## טענה

$$q^k = \sum_{d|k} d \cdot n_q(d)$$

זה נכון לפי סכימת הדרגות של הפולינומים האי-פריקים.

## מסקנה

מספר הגורמים האי-פריקים של  $x^{q^k} - x$  הוא  $\sum_{d|k} n_q(d)$ .

## נחזור לתרגיל המנחה

במקרה שלנו  $k=6$  (כי  $2^6 = 64$ )

$$n_2(1) = 2 \quad n_2(2) = 1$$

$$n_2(1) + 2 \cdot n_2(2) + 4 \cdot n_2(4) = 2^4$$

$$2 + 2 \cdot 1 + 4n_2(4) = 2^4$$

$$n_2(4) = 3$$

( $4 \nmid 6$  שכן  $n_2(4)$  מיותר, שכן  $4 \nmid 6$ )

$$1 \cdot n_2(1) + 3 \cdot n_2(3) = 2^3 = 8 \implies n_2(3) = 2$$

$$1 \cdot \underbrace{n_2(1)}_{=2} + 2 \cdot \underbrace{n_2(2)}_{=2} + 3 \cdot \underbrace{n_2(3)}_6 + 6 \cdot n_2(6) = 64$$

$$n_2(6) = 9$$

מספר הגורמים האי-פריקים של  $x^{64} - x$  ?

$$\sum_{d|k} n_2(d) = 14$$

### נוסחת ההיפוך של מביוס

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & a^2 \mid n, a > 1 \\ (-1)^k & n = p_1 \cdots p_k, p_i \neq p_j \end{cases} \quad \text{פונקציית מביוס היא}$$

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) \quad \text{אזי} \quad g(n) = \sum_{d|n} f(d) \quad \text{אם}$$


---

$$n_q(n) = \frac{\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d}{n}$$

### משפט(שטייניץ)

הרחבה סופית  $E/F$  היא פשוטה אם ורק אם יש לה מספר סופי של שדות ביניים.

### הוכחה

אם ההרחבה  $E/F$  פשוטה, אזי  $E = F(a)$ . יהי  $B$  שדה ביניים. אזי  $B(a) = E$ .  
 יהי  $f(x) \in F[x]$  הפולינום המינימלי של  $a$  מעל  $F$ . נסמן ב  $B[x]$  את הפולינום המינימלי של  $a$  מעל  $B$ .  
 $B[x] \mid f(x) \iff$   
 נסמן ב  $b_1, \dots, b_k$  את המקדמים של  $g(x)$  ב  $B$ .  $B' = F(b_1, \dots, b_k) \subseteq B$ .



$g(x) \in B'[x]$  והוא אי־פריק שם.

$$B'(a) = E$$

$$[E : B'] = \deg g(x) = [E : B]$$

$$\implies B = B'$$

הפולינום  $g(x)$  קובע את השדה. יש מספר סופי של פולינומים מתוקנים שמחלקים את  $f(x)$ , ולכן יש מספר סופי של שדות ביניים. בכיוון השני: נניח שיש מספר סופי של שדות ביניים בין  $E$  ל- $F$ . אפשר להניח ש- $F$  שדה אינסופי (כי ראינו שהרחבה סופית של שדה סופי היא פשוטה). ההרחבה  $E/F$  סופית (לפי הנתון).

$$E = F(a_1, \dots, a_n)$$

נוכיח באינדוקציה: מספיק להוכיח עבור  $E = F(a_1, a_2)$ . נסתכל על צירופים  $a_1 + ta_2$  כאשר  $t \in F$ : אינסופי ויש מספר סופי של שדות ביניים ולכן  $F(a_1 + t_1 a_2) = F(a_1 + t_2 a_2)$  עבור  $t_1 \neq t_2$ . השדה מכיל  $\frac{a_1 + t_1 a_2}{a_1 + t_2 a_2}$  וניתן להחליף את  $a_1, a_2$ , ולכן  $F(a_1 + t_1 a_2) = F(a_1, a_2)$ .

## משפט האיבר הפרימיטיבי

כל הרחבה סופית ספרבילית היא פשוטה.

## הוכחה

$$E/F$$

$$E = F(a_1, \dots, a_n)$$

לוקחים את שדה הפיצול של  $f(x) = m_{a_1}(x) \cdots m_{a_n}(x)$ , וזאת הרחבת גלואה של  $F$  (ניתן להחליף את  $f$  בפולינום ספרבילי). יש ל- $E'/F$  מספר סופי של שדות ביניים (לפי התאמת גלואה). לפי שטייניץ ההרחבה  $E'/F$  פשוטה.

## בניית הרחבת גלואה עם חבורת גלואה סופית כלשהי

שלב א: מימוש החבורה  $S_n$  כחבורת גלואה

יהי  $F$  שדה כלשהו. שדה שברים של  $F[x_1, \dots, x_n] \leftarrow K = F(x_1, \dots, x_n)$

יש פעולה של  $S_n$  על  $K$  - מפעילים את התמורה של האינדקסים של ה- $x_i$ . בנוסף כל תמורה היא אוטומורפיזם של  $K$ .  
 נגדיר  $S = K^{S_n}$  שדה הפונקציות הסימטריות. לדוגמה:  $x_1 + \dots + x_n \in S$ .

$$[K : S] = [K : S^{S_n}] = |S_n| = n!$$

בנוסף  $\text{Gal}(K/S) = S_n$ .  
 כל חבורה סופית איזומורפית לתת חבורה של  $S_n$  (לפי קיילי). לכן אם יש לנו  $H \leq S_n$ , אזי  $\text{Gal}(K/K^H) = H$ .  
 $K$  הוא שדה מפצל של איזה פולינום מעל  $S$ ?

$$f(\lambda) = \prod (\lambda - x_i)$$

$S$  פועלת טריווילית על  $f(x)$  ולכן  $f(\lambda) \in S[x]$  היא הרחבת גלואה.  
 $S$  נוצר ע"י המקדמים של  $f(\lambda)$  שהם הפונקציות הסימטריות האלמנטריות.