

הערות על ה-3

הערות

1- הנהגת ה-3 היא פשוטה.

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה.

2- \mathbb{Z}_p הוא שדה אם ורק אם p ראשוני.



p^n

3- אם p ראשוני, אז \mathbb{Z}_p הוא שדה, ו- $\mathbb{Z}_p[x]$ הוא שדה.

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה, ו- $\mathbb{Z}_p[x]$ אינו שדה.

4- אם p ראשוני, אז \mathbb{Z}_p הוא שדה, ו- $\mathbb{Z}_p[x]$ הוא שדה.

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה, ו- $\mathbb{Z}_p[x]$ אינו שדה.

5- \mathbb{Z}_p הוא שדה אם ורק אם p ראשוני.

$$\forall a \neq 0 \quad (a^{p^n-1} = 1)$$

$$\Leftrightarrow |\mathbb{F}_{p^n}^\times| = p^n - 1$$



$$x(x^{p^n-1} - 1) = 0$$

6- אם p ראשוני, אז \mathbb{Z}_p הוא שדה, ו- $\mathbb{Z}_p[x]$ הוא שדה.

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה, ו- $\mathbb{Z}_p[x]$ אינו שדה.

7- אם p ראשוני, אז \mathbb{Z}_p הוא שדה, ו- $\mathbb{Z}_p[x]$ הוא שדה.

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה, ו- $\mathbb{Z}_p[x]$ אינו שדה.



8- אם p ראשוני, אז \mathbb{Z}_p הוא שדה, ו- $\mathbb{Z}_p[x]$ הוא שדה.

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה, ו- $\mathbb{Z}_p[x]$ אינו שדה.

9- אם p ראשוני, אז \mathbb{Z}_p הוא שדה, ו- $\mathbb{Z}_p[x]$ הוא שדה.

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה, ו- $\mathbb{Z}_p[x]$ אינו שדה.

$$(x, (1+x)^2)$$

אם p ראשוני, אז \mathbb{Z}_p הוא שדה, ו- $\mathbb{Z}_p[x]$ הוא שדה.

$$(1+x)^2$$

$$x(1+x)$$

(אם p ראשוני) ✓

1 ? \mathbb{Z}_2 הוא שדה

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה, ו- $\mathbb{Z}_p[x]$ אינו שדה.

0

1

0

1

0

$$x^2$$

$$1+x^2$$

$$x+x^2$$

$$1+x+x^2$$

אם p ראשוני, אז \mathbb{Z}_p הוא שדה, ו- $\mathbb{Z}_p[x]$ הוא שדה.

אם p אינו ראשוני, אז \mathbb{Z}_p אינו שדה, ו- $\mathbb{Z}_p[x]$ אינו שדה.

$$\{x, (x-1), (x-2)\}$$

↑
 כל האלה אנחנו סוגים

הם הם \mathbb{Z}_3

$$\mathbb{F}_{3^2} \mid \mathbb{F}_3$$

אנחנו

הם הם

אנחנו יושבים על \mathbb{F}_{3^2}

אנחנו

הם הם

אנחנו יושבים על \mathbb{F}_9 - אנחנו

אנחנו

אנחנו

$$\frac{a_1 + a_2 + a_3 + \dots + a_n}{\mathbb{F}_9 - \mathbb{F}_3}$$

$$\frac{9-3}{2} = 3 \uparrow$$

(המשפט)

\mathbb{F}_9 הם קבוצת-המספרים המרוכבים

$$\mathbb{F}_{p^{n^2}} \mid \mathbb{F}_p$$

$$\mathbb{F}_9 \mid \mathbb{F}_3$$

אנחנו

אנחנו

אנחנו

$$\frac{p^{n^2} - p^n}{2}$$

אנחנו

אנחנו

$$\mathbb{F}_{p^3} \mid \mathbb{F}_p$$

אנחנו

אנחנו

אנחנו

$$\mathbb{F}_{p^3} \mid \mathbb{F}_{p^2} \mid \mathbb{F}_p$$

אנחנו

$$\frac{p^3 - p}{3}$$

אנחנו

$$\frac{p^9 - p}{9}$$

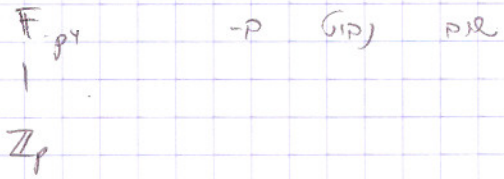
אנחנו

אנחנו

09.01.14

כוכב 5
ת' לקט מלפני

כמה פולינומים אי-פניקים... מובנה \mathbb{Z}_p ?



~~ב~~ פולינום מובנה \mathbb{Z}_p

מחלקים לפי פולינומים אי-פניקים מובנה \mathbb{Z}_p ויש דיון

$$\frac{p^2 - p}{2} \text{ קולה.}$$

למשל, יש חוק כוזב על \mathbb{F}_{p^2} מאי, \mathbb{F}_{p^2}

אחרי, הן יחס פולינומים אי-פניקים מובנה \mathbb{Z}_p