שדות סופיים

שדות סופיים

הגדרה

Definition

תהי p מספר ראשוני. **שדה סופי** $\mathbb{Z}_p$ הוא קבוצת מחלקות השארית מודולו p:

$$\mathbb{Z}_p = \{\bar{0},\ \bar{1},\ \bar{2},\ \ldots,\ \overline{p-1}\}$$

כאשר $\bar{k}$ מסמנת את קבוצת כל המספרים השלמים הנותנים שארית k בחילוק ב-p.

על $\mathbb{Z}_p$ מוגדרות שתי פעולות:

- **חיבור:** $a \oplus b = (a+b) \bmod p$
- **כפל:** $a \odot b = (a \cdot b) \bmod p$

(בסימון מקוצר: $\oplus \to +$, $\odot \to \cdot$)

דוגמה - טבלאות פעולות מעל $\mathbb{Z}_5$

טבלת חיבור ($+$ mod 5):

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

טבלת כפל ($\cdot$ mod 5):

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

ממ"ל מעל $\mathbb{Z}_p$

פותרים בדיוק כמו ממ"ל רגיל (שיטת גאוס), אלא שכל החישובים מתבצעים מודולו p.

ההבדל המרכזי מממ"ל מעל $\mathbb{R}$: במקרה של "אינסוף פתרונות" מקבלים מספר **סופי** של פתרונות.

מצב	מסקנה
אין שורת סתירה, מס' איברים מובילים = מס' נעלמים	**פתרון יחיד**
שורת סתירה	**אין פתרון**
אין שורת סתירה, k משתנים חופשיים	p^k **פתרונות**