*, (שלם), עם פעולות חיבור וכפל:*

*יהי*

*נגדיר יחס שקילות ב:*

*לכן אפשר לקחת מחלקות עם יחס השקילות הזאת. קבוצת מחלקות השקילות נקראת קבוצת שאריות*

לכן

# הערה

אם n פריק() אזי ב יש מחלקים של 0, כלומר כך ש אבל

## דוגמה

=>

# משפט:

בשדה אין מחלקים של 0

## הוכחה

תרגיל(רמז: קיום של הפכי לכל איבר שונה מ0)

## תוצאה:

לn פריק אינו שדה

# משפט

יהי ראשוני אזי הוא שדה.

(p מוגדר ראשוני אם בכל פירוק מתקיים )

### הגדרה אחרת

P ראשוני אם מתקיים

## הוכחה

נוכיח שלכל קיים כך ש

דוגמה ל: ניקח :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

לכן נתבונן בסידרה של p איברים ב:

כל האיברים הם שונים ב: כלומר לכל המספרים השלמים יש שאריות שונות מודולו p:

אבל כי =>

לכן => בסדרה אין איברים זהים בגלל ש

= > קיים כך ש

# משפט

יהי F שדה סופי(כלומר F הוא קבוצה סופית), אזי קיים ראשוני ו שלם כך ש

בפרט לא קיים שדה עם 6 איברים

### הערה

מתברר שנכונה גם הטענה ההפוכה: לכל ראשוני, שלם קיים שדה יחיד F כך ש

מקובל לסמן את אותם שדות

## דוגמה – שדה עם 4 איברים

*לוח החיבור:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + |  |  | x | y |
|  |  |  | X | y |
|  |  | Y |  | x |
| X | x |  | Y |  |
| Y | Y | x |  |  |

*לוח הכפל:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \* |  |  | x | y |
|  |  |  |  |  |
|  |  |  |  | y |
| X |  |  | Y |  |
| Y |  | y |  |  |

*שדה – נוכיח לפי זה שגם שדה*

*הערה: למשוואה אין שורש ממשי.*

מאפיין של שדה

יהי F שדה. הגדרות השדה מבטיחות לנו שני איברים. כדי ליצור איבר חדש צריך לחבר 1:

לדוגמה אם אזי נקבל

אבל אם אז נקבל

# הגדרה:

אם השדה היא קבוצה אינסופית אזי אומרים שלF יש מאפיין אפס

אחרת לF יש מאפיין חיובי

## הערה

אם אזי

# משפט

אם אזי קיים p ראשוני כך ש

## הוכחה

הערה – עובדים בתוך F, לא בתוך המספרים הרגילים

אם בסדרה הזאת אין איברים שווים אזי היא אינסופית.

אם בסדרה הזו יש שני איברים שווים:

לדוגמה האיבר הראשון זהה לרביעי

נבחר זוג של איברים זהים כך ש מינימלי חיובי אזי הוא ראשוני:

נתבונן ב

אם איננו ראשוני אזי אפשר לכתוב

לכן או

כלומר p אינו מינימלי

# תרגיל

נתבונן בסדרה

המספר המינימלי p כך ש p פעמים

2 "הוכיחו" כי אם אז