

## תרגול 5

7 באפריל 2019

### משפט לגרנז'

משפט לגרנז':  $G$  חבורה סופית  $H$  ת"ח אזי  $|H|$  מחלק את  $|G|$  בפרט הסדר של איבר מחלק את סדר החבורה. בנוסף  $|G/H| = \frac{|G|}{|H|}$ .  
מסקנה: בחבורה סופית  $G$ ,  $|G| = n$  מתקיים:

$$1. \forall g \in G : o(g) | n$$

$$2. \forall g \in G : g^n = e$$

תרגילים:

1. תהא  $G$  חבורה. יהיו  $H_1, H_2$  תתי חבורות מסדר סופי. נסמן  $|H_1| = n_1, |H_2| = n_2$ .  
נניח כי  $n_1, n_2$  מספרים זרים. הוכיחו כי

$$H_1 \cap H_2 = \{e\}$$

2. תהא  $G$  חבורה עם ארבעה איברים. הוכיחו ש- $G$  אבליה.

פתרון:

1.  $H_1 \cap H_2$  תת חבורה של  $H_1, H_2$  ולכן הסדר שלה מחלק את  $n_1, n_2$  כיוון שהספרים זרים נקבל כי הסדר הוא 1 כלומר  $H_1 \cap H_2 = \{e\}$ .

2. סדרי האיברים יכולים להיות 1, 2, 4. אם יש איבר מסדר 4 אז זו חבורה ציקלית ובפרט אבליה. אם לא, אז לכל  $g \in G$  נקבל  $g^2 = e$ , ולפי תרגיל בית  $G$  אבליה.

### משפטי אוילר ופרמה

פונקציית אוילר היא:  $\phi : \mathbb{N} \rightarrow \mathbb{N}$  המוגדרת ע"י:

$$\phi(n) = |\{1 \leq a \leq n - 1 : \gcd(a, n) = 1\}|$$

ומתקיים:  $\{1 \leq a \leq n-1 : \gcd(a, n) = 1\}$  עם כפל מודולו  $n$  היא חבורה אבלית. סימון:  $U_n$ . דוגמאות:

$$1. U_6 \cong \mathbb{Z}_2$$

$$2. U_7 \cong \mathbb{Z}_6$$

$$3. U_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$4. U_9 \cong \mathbb{Z}_6$$

$$5. U_{10} \cong \mathbb{Z}_4$$

משפט אוילר: לכל  $n \in \mathbb{N}$  ולכל  $1 \leq a \leq n-1$  הזר ל- $n$  מתקיים:  $a^{\phi(n)} \equiv 1 \pmod{n}$ , או באופן שקול:  $1 - a^{\phi(n)} \mid n$ .

משפט פרמה: לכל  $p$  ראשוני ולכל  $1 \leq a \leq p-1$  מתקיים:  $a^{p-1} \equiv 1 \pmod{p}$ , או באופן שקול:  $1 - a^{p-1} \mid p$ . תרגילים:

$$1. \text{ חשב את } 13^{613} \pmod{103}.$$

$$2. \text{ מהן 2 הספרות האחרונות של } 7^{2002}?$$

פתרון:

$$1. \text{ כיון ש-} 103 \text{ ראשוני נקבל ממשפט פרמה ש- } 13^{102} \equiv 1 \pmod{103}, \text{ ולכן } 13^{613} = (13^{102})^6 \cdot 13 \equiv 13 \pmod{103}.$$

$$2. \text{ נחשב את } \phi(100). \text{ המחלקים הם: } 2, 5. \text{ יש 49 זוגיים בין 1 ל-99, ועוד עשרה מספרים המתחלקים ב-5 ולא ב-2. סה"כ נותרו 40 מספרים שלא זוגיים ולא מתחלקים ב-5, לכן } \phi(100) = 40. \text{ כעת ממשפט אוילר נקבל (כיון ש-7 זר ל-100): } 7^{40} \equiv 1 \pmod{100}, \text{ ולכן: } 7^{2002} = (7^{40})^{50} \cdot 7^2 \equiv 49 \pmod{100}. \text{ לכן התשובה היא 49.}$$