תזכורת: יהי $m \in \mathbb{N}$. נגיד ש $x \equiv y \mod m$ אם $m|x-y$.
למשל:

$$7 \equiv 4 \mod 3$$

משפט: יהיו m, n מספרים זרים. $(m,n)=1$. אז לכל $a, b \in \mathbb{Z}$, קיים $x \in \mathbb{Z}$ כך ש:

$$x \equiv a \mod m$$

$$x \equiv b \mod n$$

למשל: $3, 5$ זרים. אז קיים

$$x \equiv 2 \mod 3$$

$$x \equiv 1 \mod 5$$

פתרון אפשרי: $x = 11$.
הערה: הx הנ"ל הוא יחיד עד כדי מודולו mn.
למשל בדוגמא שלנו, ראינו ש11 מקיים את התנאים. אז כל מספר ששקול ל11 מודולו 15 גם יקיים. וכל מספר שלא שקול ל11 מודולו 15 לא יקיים את זה.
הוכחה:רוצים למצוא x שמקיים:

$$x \equiv a \mod m$$

$$x \equiv b \mod n$$

נתון m, n זרים. בתרגול הקודם הוכחנו שזה שקול לכך ש1 הוא צירוף לינארי שלהם.
קיימים $\alpha, \beta \in \mathbb{Z}$. כך ש:

$$\alpha m + \beta n = 1$$

נקח

$$x = b\alpha m + a\beta n$$

$$x - a = (b\alpha m + a\beta n) - a(\alpha m + \beta n) = m(b\alpha - a\alpha)$$

לכן

$$x \equiv a \mod m$$

$$x - b = (b\alpha m + a\beta n) - b(\alpha m + \beta n) = n(a\beta - b\beta)$$

לכן

$$x \equiv b \mod n$$

דוגמא: מצאו

$$x \equiv 1 \mod 3$$

$$x \equiv 2 \mod 5$$

פתרון: ידוע ש5 ו3 זרים זה אומר שיש להם צירוף לינארי ששווה 1.

$$-3 \cdot 3 + 2 \cdot 5$$

$$x = -2 \cdot 3 \cdot 3 + 1 \cdot 2 \cdot 5 = -8$$

אם רוצים דווקא מספר חיובי נמצא מספר חיובי ששקול לו מודולו $3 \cdot 5$. למשל, 7.
הכללה: יהיו $n_1, n_2, ...n_m$ מספרים זרים בזוגות. לכל $a_1, ...a_m$ קיים $x \in \mathbb{Z}$ כך ש:

$$x \equiv a_1 \mod n_1$$

$$\vdots$$

$$x \equiv a_m \mod n_m$$

הוכחה: כל פעם נצמצם את מספר התנאים. כלומר, נקח שני תנאים, ונחליף אותם בתנאי 1 ע"י האלגוריתם שהבאנו. כלומר, נניח שמצאנו x' שמקיים את שני התנאים הראשונים. אז עכשיו נחליף את שני התנאים הראשונים בתנאי:

$$x \equiv x' \mod n_1 n_2$$

נדגים: מצאו

$$x \equiv 1 \mod 3$$

$$x \equiv 2 \mod 5$$

$$x \equiv 3 \mod 7$$

פתרון: את שני התנאים הקודמים פתרנו בתרגיל הקודם. קיבלנו 7. לכן עכשיו נותר לפתור:

$$x \equiv 7 \mod 15$$

$$x \equiv 3 \mod 7$$

צירוף לינארי ששווה 1:

$$15 - 2 \cdot 7$$

$$x = 3 \cdot 15 - 7 \cdot 2 \cdot 7 = -53$$

אם רוצים מספר חיובי, אפשר להוסיף כפולות של $15 \cdot 7$

$$x = 52$$

ניצחנו.
הערה: כפל וחיבור מוגדרים מודולו n. כלומר, אם

$$a_1 \equiv b_1 \mod n$$

$$a_2 \equiv b_2 \mod n$$

אז:

$$a_1 a_2 \equiv b_1 b_2 \mod n$$

$$a_1 + a_2 \equiv b_1 + b_2 \mod n$$

דוגמא: מצאו את הספרה האחרונה של המספר

$$333^{333}$$

פתרון: למצוא ספרה אחרונה של מספר, זה בעצם למצוא מה השארית חלוקה שלו מודולו 10.

$$333^{333} \mod 10 \equiv (333 \mod 10)^{333} \mod 10 \equiv$$

$$(3 \mod 10)^{333} \mod 10 = 3^{333} \mod 10$$

ידוע $3^4 = 81 \equiv 1 \mod 10$.

$$= 3^{333} \mod 10 = 3^4 3^{329} \mod 10 =$$

$$3^4 \mod 10 \cdot 3^{329} \mod 10 = 3^{329} \mod 10$$

"נוציא 4 מהחזקה שוב ושוב" בעצם מספיק לקחת את שארית החלוקה של 333 ב4. זה שווה 1. בסוף נישאר עם

$$3^1 \mod 10 = 3$$

כלומר, הספרה האחרונה של 333^{333} היא 3.
דוגמא: נניח שרוצים לדעת מה הספרה האחרונה של

$$12 \cdot 13$$

רוצים לחשב:

$$12 \cdot 13 \mod 10$$

$$12 \equiv 2 \mod 10$$

$$13 \equiv 3 \mod 10$$

$$2 \cdot 3 \mod 10$$

מבנים אלגבריים:

תהי A קבוצה. פעולה בינארית על קבוצה A זה פונקציה מ$A \times A$ לA. מקובל לסמן

$$a \cdot b$$

או לפעמים

$$a * b$$

ולפעמים רק

$$ab$$

הגדרה: חבורה למחצה היא קבוצה עם פעולה שמקיימת את תכונת האסוציאטיביות.

$$(ab)c = a(bc)$$

למשל: $(\mathbb{Z}, -)$ זאת פעולה לא אסוציאטיבית. כי למשל

$$3 - (2 - 1) \neq (3 - 2) - 1$$

ולכן זאת לא חבורה למחצה.
דוגמא נוספת: תהי A קבוצה כלשהי. נדיר פעולה

$$ab = b$$

האם זאת חבורה למחצה?

$$a(bc) = ac = c$$

$$(ab)c = bc = c$$

תשובה: כן, כי הפעולה אסוציאטיבית.
דוגמא קלאסית: תהי X קבוצה. אוסף כל הפונקציות מX לX עם פעולת ההרכבה היא חבורה למחצה. (ידוע שהרכבה היא אסוציאטיבית).
הגדרה: תהי $(A, \cdot)$ חבורה למחצה. איבר $e \in A$ נקרא "איבר יחידה" אם הוא מקיים ניטרליות לפעולה. כלומר:

$$\forall a \in A, ae = ea = a$$

(חייב להתקיים משני הכיוונים).
דוגמא: בקבוצה A עם הפעולה $ab = b$ אין איבר יחידה אלא אם כן בקבוצה יש רק איבר אחד בקבוצה.
הסבר: אם e הוא איבר יחידה, אז לכל a צריך להתקיים

$$a \cdot e = a$$

אבל הפעולה מוגדרת כך ש:

$$ae = e$$

ולכן כל האיברים צריכים להיות שווים לe. כלומר, יש רק איבר אחד.
פונקציות מX לX: פונקציית הזהות היא איבר יחידה.
הגדרה: חבורה למחצה עם איבר יחידה נקראת מונואיד.
הערה: אם יש איבר יחידה, הוא יחיד. (מקובל לסמן בe).
דוגמאות:
1. $(\mathbb{N}, +)$ הוא לא מונואיד. אבל $(\mathbb{N} \cup \{0\}, +)$ כן מונואיד.
2. $(\mathbb{Z}, +)$ מונואיד.
3. $(\mathbb{N}, \cdot)$ מונואיד.

סימון: כשנדבר על מונואיד בד"כ נסמן שלשה של הקבוצה, הפעולה, ואיבר היחידה.
תרגיל: תהי X קבוצה. נסתכל על $(P(X),\cap)$ האם זה מונואיד? אם כן- מה איבר היחידה?
פתרון: ראשית, ידוע שפעולת החיתוך היא אסוציאטיבית ולכן זאת חבורה למחצה. והאיבר הנטרלי הוא X. כי לכל $A\in P(X)$ ידוע ש:

$$A\cap X=X\cap A=A$$

מה יקרה אם נחליף את החיתוך לאיחוד? זה יהיה מונואיד, האיבר הנטרלי יהיה הקבוצה הריקה.
מה יקרה אם נחליף ל$\triangle$? מונואיד, והאיבר הנטרלי הוא $\emptyset$.
הגדרה: יהי $(X,\cdot,e)$ מונואיד. איבר $a\in X$ יקרא הפיך, אם קיים $b\in X$ כך ש

$$ab=ba=e$$

דוגמאות:
1. $(P(X),\cap,X)$. יהי $A\in P(X)$. האם קיים B כך ש$A\cap B=X$. זה יכול לקרות רק כאשר $A=X$. אז האיבר ההפיך היחיד זה X בעצמו.
2. $(P(X),\triangle,\emptyset)$. לכל $A\in P(X)$ ידוע ש$A\triangle A=\emptyset$. ולכן כל איבר הפיך, והוא ההופכי של עצמו.

הערה: אם איבר הפיך ההופכי שלו יחיד.
הגדרה: מונואיד שבו כל איבר הפיך נקרא חבורה.
דוגמאות:
1. $(\mathbb{Z},+,0)$ היא חבורה.
2. $(\mathbb{N}\cup\{0\},+,0)$ הוא מונואיד שאינו חבורה.

הגדרה: חבורה נקראת "אבלית" אם לכל a,b מתקיים:

$$ab=ba$$

דוגמאות:
1. $(\mathbb{Z},+,0)$ היא חבורה אבלית.
2. $(M_n(\mathbb{F}),\cdot,I)$ אז הכפל לא קומוטטיבי, אבל זאת בכלל לא חבורה, כי לא לכל איבר יש הופכי. זה מונואיד.

אבל- לכל מונואיד M, יש את אוסף האיברים ההפיכים במונואיד, שמסומן $U(M)$ והוא חבורה. (הוכחתם בהרצאה).

$$U(M_n(\mathbb{F}))=GL_n(\mathbb{F})$$

אז זאת דוגמא לחבורה לא אבלית.
תרגיל: תהי $(G,\cdot,e)$ חבורה. ונניח שלכל $x\in G$ מתקיים:

$$x^2=e$$

הוכיחו שG חבורה אבלית.
פתרון: יהיו $a,b\in G$. צריך להוכיח ש$ab=ba$.

$$(ab)^{-1}=b^{-1}a^{-1}$$

הוכחתם בהרצאה.
עכשיו, מהנתון ש$x^2 = e$, יוצא שכל איבר הוא ההופכי של עצמו. לכן

$$(ab)^{-1} = ab$$

וגם

$$b^{-1} = b$$

$$a^{-1} = a$$

נציב בשוויון הראשון ונקבל

$$ab = ba$$

הגדרה: תת חבורה-
תהי G חבורה. $H \subseteq G$ נקראת "תת חבורה" ומסמנים $H \leq G$ אם H היא חבורה בעצמה ביחס לאותן פעולות.
הערה: (קריטריון מקוצר) תהי $H \subseteq G$. בשביל להוכיח שH היא תת חבורה מספיק להוכיח:
1. $e \in H$
2. סגירות לפעולה.
3. סגירות להופכי. (כלומר, אם איבר נמצא, גם ההופכי שלו נמצא)

דוגמא: $G = GL_3(\mathbb{R})$

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

הוכיחו שH היא תת חבורה.
הוכחה:
1.

$$I \in H$$

נקח $a = b = c = 0$
2. סגירות לפעולה: יהיו

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} \in H$$

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a'+a & b'+b+ac' \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{pmatrix} \in H$$

3.

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \in H$$

4. לכל $n \in \mathbb{Z}$,

$$n\mathbb{Z} \leq \mathbb{Z}$$

תרגיל: הוכיחו שחיתוך של תת חבורות הוא תת חבורה.
פתרון: תהי G חבורה ו$\{H_i\}_{i\in I}$ אוסף של תת חבורות של G. נוכיח ש$\bigcap H_i \leq G$
1. $e \in H_i$ לכל $i \in I$ ולכן $e \in \bigcap H_i$
2. סגירות לפעולה: יהיו $a, b \in \bigcap H_i$, אז לכל $a, b \in H_i$ i, ולכן $ab \in H_i$ לכל i, ולכן $ab \in \bigcap H_i$.
3. קיום הופכי: יהי $a \in \bigcap H_i$. אז לכל $a \in H_i$ i, לכן $a^{-1} \in H_i$ לכל i, ולכן $a^{-1} \in \bigcap H_i$.
הגדרה: יהי $a \in G$. (G חבורה). תת החבורה שנוצרת ע"י a היא החיתוך של כל תת החבורות שמכילות את האיבר a. כלומר, התת חבורה הכי קטנה שa נמצא בה.
מסמנים:

$$\langle a \rangle = \{e, a, a^{-1}, a^2, a^3, a^n, a^{-n}\}$$

למעשה, $\langle a \rangle$ זה כל החזקות של a (גם שליליות).
לדוגמא: $\langle 4 \rangle \leq \mathbb{Z}$

$$\langle 4 \rangle = \{4n : n \in \mathbb{Z}\} = 4\mathbb{Z}$$

דוגמא נוספת:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{R})$$

$$\left\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$$