חבורות

נושא החבורות הופיע במתמטיקה כבר במאה ה-18 ושימש בסיס למציאת פתרונות למשוואות פולינומיות ממעלות גבוהות. גם היום לתורת החבורות יש שימושים רבים אחרים במתמטיקה, בפיזיקה ובתחומים אחרים. לדוגמה הם מסייעים במחקרים על סימטריה בגבישים ובמולקולות. נושא החבורות נלמד היום הרחבה במסגרת לימודים אקדמיים גבוהים ובקורסים מתמטיים מתקדמים. בפרק זה התלמידים ייחשפו למספר מושגים בסיסיים של תורת החבורות וילמדו את הנושא בצורת "טעימות". בפרק לא מופיעות הוכחות מורכבות והרבה מושגים ותכונות נלמדים בצורה אינטואיטיבית.

שיעור ראשון: **פעולות בינאריות**, עמ' 37 (כשיעור אחד).

מושגים מרכזיים:

פעולה בינארית – פעולה על שני איברים שנותנת תוצאה אחת ויחידה לכל שני איברים.
פעולה בינארית בקבוצה מסוימת – פעולה בין שני איברים בקבוצה שיש לה תוצאה אחת ויחידה בכל זוג איברים.
פעולה בינארית חילופית - כאשר בפעולה בינארית המתקיימת בקבוצה, חל חוק חילוף.

המלצה להוראה:

מומלץ להעביר את הדוגמאות וההסברים שבעמ' 37 במליאה, במהלך דיון כיתתי. כדאי לבדוק היטב שהתלמידים הבינו את המושגים של **פעולה בינארית** שכוללת שני תנאים:

א) הפעולה מתאימה לכל זוג איברים תוצאה.

ב) תוצאה היא יחידה עבור כל זוג.

יש להדגיש את החשיבות של כל תנאי בנפרד. במהלך ההסבר יש להביא דוגמאות פשוטות של פעולות, כולל "דוגמאות קצה" כגון: עבור כל זוג מספרים התוצאה היא אפס. מומלץ לתת לילדים לבנות פעולות ולדון האם הפעולות שבנו הן בינאריות או לא.

דוגמאות:

- פעולות החשבון הן בינאריות.
- הפעולות "שורש" ו"חזקה" אינן בינאריות, כי הן מופעלות על איבר אחד בלבד.
- חיסור של מספרים טבעיים אינו בינארי, כי לכמה זוגות אין תוצאה טבעית.
- הפעולה שלשני מילים סמוכות במילון מתאימה מילה כלשהי הקודמת להם אינה בינארית כי לכל זוג של מילים יותר מתוצאה אחת.

אחרי שהתלמידים הבינו את ההגדרה של פעולה בינארית, יש לעבור על הדוגמאות שבעמ' 37 – 38 וביחד לדון מדוע אלה פעולות בינאריות/לא בינאריות. אפשר לתת את תרגילים 1 – 4 לעבודה עצמית (לבד או בזוגות) ולבדוק תשובות לתרגילים נבחרים.

אפשר לתת לתלמידים לקרוא לבד את ההגדרה של פעולה בינארית חילופית, ולהסביר במליאה מה הבינו ולהביא דוגמאות של פעולות בינאריות חילופיות ופעולות בינאריות לא חילופיות (פעולה שלוקחת זוג מספרים ובוחרת את הראשון מהם, פעולה שלוקחת כל זוג מספרים ומחזירה את הנגדי של הגדול מהם וכד').

את התרגילים 6 – 11 ניתן לתת לעבודה עצמית, כאשר מומלץ לבדוק את התשובות לתרגילים 6 (קשר עם גיאומטריה), 10 (לא קל להבין את הפעולה ולהבין שהיא לא בינארית חילופית), 11 ג' (להציג על הלוח כמה שיותר דוגמאות שבנו תלמידים).

תשובות והערות לתרגילים:

(1) פעולת החזקה על המספרים הטבעיים היא פעולה בינארית. על שני איברים a ו-b מקבלים תוצאה אחת ויחידה.

(2) הפעולה לא בינארית, כי היא אינה מוגדרת על שני איברים.

(3) הפעולה בינארית. לכל זוג סדור מקבלים תוצאה אחת ויחידה שהיא 7.

(4) הפעולה אינה בינארית. נתון רק מספר אחד ולא שניים.

(5) פעולת החיסור אינה בינארית חילופית. $a-b \neq b-a$.

חבורות

(6) הפעולה בינארית חילופית. הפעולה בינארית: לכל שתי נקודות יש רק מספר אחד המציין את המרחק ביניהן. הפעולה חילופית: המרחק לא תלוי בבחירת הנקודה הראשונה מבין השתיים מכיוון שמפעילים ערך מוחלט.

(7) הפעולה חילופית. בחירת המספר הגדול מבין שני מספרים לא מושפעת מסדר המספרים.

(8) פעולת החילוק אינה בינארית חילופית. $a \div b \neq b \div a$.

(9) א) הפעולה היא חזקה. a^b. ב) הפעולה אינה בינארית חילופית $a^b \neq b^a$.

(10) א) 4*2=8 , 3*4=11, a*b=a+b+b. ב) a כוכבית b היא סכום של a ופעמיים b.
ג) הפעולה אינה בינארית חילופית: עבור $a \neq b$, $a+b+b \neq b+a+a$

(11)

#	1	2	3	4
1	1	1.5	2	2.5
2	1.5	2	2.5	3
3	2	2.5	3	3.5
4	2.5	3	3.5	4

א) פעולת הממוצע היא בינארית חילופית. כיוון ש- a+b=b+a, גם חילוק הסכום ב-2 נשאר חילופי. ניתן להסתכל על האלכסון הראשי, מהפינה השמאלית העליונה אל הפינה הימנית התחתונה, ולראות את הסימטריה.

ב) הפעולה אינה בינארית חילופית. עבור הזוג הסדור (a,b) נקבל: a*b=3a+b. עבור הזוג הסדור (b,a) נקבל: b*a=3b+a. עבור $a \neq b$ גם $3a+b \neq 3b+a$.

ג) פעולה בינארית חילופית: a*b=7a·b – 1, פעולה בינארית לא חילופית: a*b = 7a : b - 1

שיעור שני: **תכונות נוספות של פעולות בינאריות על קבוצה**, עמ' 41 (כשני שיעורים)

מושגים מרכזיים:

קבוצה סגורה לפעולה – כשתוצאה של פעולה על כל שני איברים היא איבר בקבוצה.

פעולה "*" נקראת קיבוצית – אם הפעולה היא בינארית בקבוצה A, ו- A סגורה ביחס לפעולה זו, ובנוסף מתקיים (a*b)*c = a*(b*c).

איבר e הוא איבר ניטרלי בפעולה בינארית "*" אם עבור כל איבר בקבוצה a, קיים איבר e יחיד שעבורו מתקיים: e*a = a*e = a.
הערה: התנאי הוא שמתקיים e*a = a*e = a, גם אם הפעולה אינה חלופית.

איבר נגדי – נאמר שאיבר b הוא איבר נגדי ל- a (וכן a הוא איבר נגדי ל- b) אם בקבוצה שבה פעולה בינארית * ואיבר ניטרלי e מתקיים: b*a = a*b = e.

חבורה – קבוצה A היא חבורה ביחס לפעולה * אם מתקיימים 4 תנאים:
1. הקבוצה סגורה ביחס לפעולה *;
2. הפעולה * היא פעולה קיבוצית;
3. קיים בקבוצה איבר ניטרלי;
4. לכל איבר בקבוצה A קיים איבר נגדי.

חבורה חילופית – אם בחבורה לכל a ו- b מתקיים: a*b=b*a.

המלצה להוראה:
בשיעור זה התלמידים ילמדו הרבה מושגים חדשים ולא פשוטים. יש לוודא הבנה של כל אחד ואחד מהמושגים ולהביא דוגמאות רבות להמחשתם. מומלץ להתחיל מהגדרה של **קבוצה סגורה** בעמ' 41. יש לעבור על דוגמאות המופיעות בשיעור וביחד לדון מדוע פעולה זו סגורה או לא. על מנת להקל על התלמידים, יש לפרק את ההגדרה ולראות כמה תנאים חייבים להתקיים על מנת שהקבוצה תהיה סגורה. התנאים הם: 1) קיום פעולה בינארית, 2)התוצאה של פעולה בינארית שייכת לאותה קבוצה. בכל פעם שהתלמידים נדרשים להחליט אם קבוצה מסוימת היא סגורה או לא לגבי פעולה מסוימת, עליהם לבחון את שני התנאים. יש לבקש מהתלמידים להביא דוגמאות רבות ככל הניתן לקבוצות סגורות ולקבוצות שאינן סגורות. עליהם לנמק את הדוגמאות על-ידי קיום שני התנאים/ אי-קיום של תנאי מסוים.

חבורות

לאחר הלימוד של ההגדרה מומלץ לתת את תרגיל 1 לעבודה עצמית ולהתייחס במיוחד לסעיף ה'. מומלץ לתת כמה שיותר דוגמאות לקבוצות סגורות ולא סגורות (לדוגמה ; קבוצת כל המספרים הטבעיים, הפעולה : עבור כל שני מספרים עוקבים מתקבל הסכום שלהם וכדי).
יש להסביר במליאה את מושג הקיבוציות שמופיע בעמ' 42. גם את ההגדרה הזו יש לפרק ל- 3 חלקים : 1) הפעולה בינארית, 2) הקבוצה סגורה 3) חוק הקיבוץ מתקיים בין כל 3 איברים של הקבוצה.
יש להדגיש את שלושת התנאים ולדון בדוגמאות ובדוגמאות נגדיות של פעולה קיבוצית על ידי קיום או אי-קיום של התנאים של ההגדרה. לפני שניגשים לתרגילים, מומלץ לבקש מהתלמידים להביא דוגמאות או דוגמאות נגדיות של פעולה קיבוצית ולנמק את הדוגמה על ידי קיום או אי קיום של התנאים.
אחר הלימוד של המושג סגירות, מומלץ לתת לעבודה עצמית את התרגילים 2- 4. יש לוודא שהנתון של תרגיל 4 ברור. בתרגיל 4, מעבר למושג "פעולה קיבוצית" חשוב להדגיש את מהות ההוכחה של טענה. חשוב להדגיש שמספיקה דוגמה נגדית אחת על מנת להפריך טענה, אך חייבים להוכיח על מנת לטעון שטענה נכונה, כי לא ניתן לבדוק את כל המקרים.
את המושגים "איבר ניטרלי" ו"איבר נגדי" שמופיעים בעמ' 43, ניתן ללמד ביחד. במושג "איבר ניטרלי" יש להדגיש את כל התנאים : 1) פעולה בינארית, 2) a*e=a 3) e*a=a.
תנאים עבור איבר נגדי (a ו- b איברים נגדיים) : 1) פעולה בינארית, 2) קיום איבר ניטרלי e, 3) b*a=e, 4) a*b=e. את תרגילים 5 – 7 יש לתת לעבודה עצמית ולבדוק תרגילים נבחרים. מומלץ לבדוק את תרגילים 5ב. (להדגיש את העניין של פעולה בינארית, ושהממוצע משנה את הערך של המספרים) ; תרגיל 7 (התלמידים עלולים לשכוח את 1-).
יש ללמד את המושג "חבורה" בעמ' 44 על ידי הצגת 4 התנאים. בשלב הזה כדאי לרשום את התנאים על הלוח (4 תנאים לחבורה ותנאים לכל סעיף – מהי קבוצה סגורה וכדי). יש לראות ביחד את הדוגמה ולבדוק במליאה את תרגיל 8. מומלץ מאוד לבקש מתלמידים דוגמאות ודוגמאות נגדיות לחבורה.
למשל, קבוצת המס' הזוגיים/אי זוגיים ופעולת חיבור/חיסור/כפל/חילוק. להמציא ביחד חבורות מעולם הגיאומטריה וכדי. המושג לא קל לתפיסה, וניתן להבין את הרעיון גם ללא לזכור את כל התנאים.

<u>תשובות והערות לתרגילים</u>:

(1) א) הפעולה בינארית. לכל שני איברים יש תוצאה אחת ויחידה. ב) הקבוצה אינה סגורה. התוצאה "משושה" המתקבלת אינה איבר בקבוצה. ג) קבוצת המספרים הזוגיים החיוביים סגורה לגבי פעולת הכפל. מכפלת כל שני מספרים זוגיים היא זוגית. ד) קבוצת המספרים הטבעיים סגורה לגבי פעולת החזקה. תוצאת פעולת החזקה של מספרים טבעיים היא מספר טבעי. ה) פעולת ה"מרחק" אינה סגורה. האיברים הם נקודות במלבן, התוצאה היא מספר.

(2) פעולת החיסור המוגדרת על המספרים השלמים אינה קיבוצית. $(a-b)-c \neq a-(b-c)$.

(3) א) פעולת החיתוך היא בינארית חילופית. ב) פעולת החיתוך היא בינארית קיבוצית.

(4) א) C (15, 20), D (60, 80) ; ב) הפעולה היא בינארית - מוגדרת עבור כל זוג של נקודות בצורה חד-משמעית, הפעולה לא חילופית וכן קיבוצית. נדגים על נקודות : A (0, 1), B (1,2), C (2,3).
A@B = (0, 2). לעומת זאת, B@A= (1, 2), A@B ≠ B@A. מכך נובע שהפעולה **לא חילופית** (כדאי להדגיש שמספיקה דוגמה נגדית אחת על מנת להוכיח שפעולה לא חילופית, אך חייבים הוכחה על מנת להוכיח שפעולה כן חילופית. כנ"ל לגבי פעולה קיבוצית או לא).
נוכיח שהפעולה כן קיבוצית (כדאי לבדוק על מס' דוגמאות, ואחרי כן לגשת להוכחה) :
הוכחה :
ניקח שלוש נקודות A (a, b), B (c, d), C (e, f).
נבדוק למה שווה (A @ B) @ C :

$$(A@B) @ C = ((a,b) @ (c,d)) @ (e,f)$$
$$= (ad, bd) @ (e,f) = (adf, bdf)$$

נבדוק למה שווה A@(B@C) :

$$A @ (B @ C) = (a,b) @ ((c,d) @ (e,f)) =$$
$$= (a,b) @ (cf, df) = (adf, bdf)$$

קיבלנו ש- (A@B) @ C = A @ (B @ C) = (adf, bdf) לכן הפעולה @ היא קיבוצית.

(5) א) לא קיים בקבוצה איבר ניטרלי לגבי פעולת החיבור. האיבר הניטרלי לגבי פעולת החיבור הוא 0, אבל 0 אינו שייך לקבוצה.
ב) לחישוב ממוצע יש לחבר את כל הנתונים ולחלקם במספר הנתונים.

חבורות

אם e הוא איבר ניטרלי, מתקיים **לכל** a $\frac{a+e}{2}=a$, כלומר $a=e$, כלומר כל איברי קבוצת השלמים שווים והדבר אינו נכון.
0 אינו משפיע על הסכום, אבל משפיע על מספר הנתונים.

- בפעולת המקסימום 1 הוא ניטרלי, כיוון שהוא תמיד המספר הקטן ביותר מבין המספרים הטבעיים.
- הקבוצה הריקה היא האיבר הניטרלי לגבי פעולת איחוד קבוצות, כיוון שאיחוד קבוצה עם הקבוצה הריקה נותן כתוצאה את הקבוצה עצמה. האיחוד עם הקבוצה הריקה לא מוסיף איברים לקבוצת האיחוד.

(6) האיבר ההפוך לאיבר כלשהו a (שונה מ-0), בקבוצת המספרים הרציונאליים הוא 1/a.

(7) מספרים 1 ו- 1-.

(8) התכונות החסרות לקבוצת המספרים הטבעיים כדי תהיה חבורה ביחס לחיבור הן: קיום איבר נגדי וקיום איבר ניטרלי.

שיעור שלישי: **חשבון מודולרי – חיבור מודולרי**, עמ' 45 (כשלושה שיעורים)

מושגים מרכזיים:

מחלקות השארית
חיבור מודולרי
טבלאות חיבור (mod n)
חבורות מודולריות – קיימים בהן חמשת התנאים לחבורות חילופיות: תכונת הסגירות בקבוצה; חוק החילוף בפעולת מודולו; חוק הקיבוץ בפעולה; קיום איבר ניטרלי ביחס לפעולה "מודולו"; קיום איבר נגדי אחד ויחיד לכל איבר בקבוצה.
כלל: במקום לחבר שני מספרים כלשהם בחיבור מודולרי, אפשר לחבר שני מספרים השייכים לאותן מחלקות. נוח לחבר בין מספרים החיוביים הקטנים ביותר במחלקות אלו.

המלצה להוראה:
בשיעור זה לומדים התלמידים את המושג "מחלקות השארית" ו"חיבור מודולרי" תוך כדי יישום של המושגים שלמדו בשיעורים הקודמים של הפרק. לכן חשוב מאוד לוודא שכל המושגים שקשורים למושג חבורה ושהמושג חבורה ברורים לתלמידים. עקב הריבוי של המושגים הנלמדים במהלך הנושא, ההמלצה היא לרשום בצד את כל המושגים, התנאים וההגדרות ולאפשר לתלמידים לראות את כל ההגדרות במהלך הפתרון של תרגילים בהמשך.
יש להתחיל את השיעור מהיכרות עם המושג "מחלקות שארית" בעמ' 45. ניתן להכין דגם של מעגל עם שנתות מקרטון על מנת להבהיר את הנושא של מחלקות שארית. אחרי שהתלמידים הבינו את הדוגמה של מודולו 8, מומלץ לבקש מהם דוגמאות של מחלקות נוספות, לבקש מהם לתת דוגמה של כמה מספרים ששווים במודולו 3, מודולו 4 וכד'.
תרגילים 1 - 4 מומלצים לעבודה עצמית. מומלץ לבדוק את תרגיל 1ב. עם מספרים שליליים.
אפשר להסביר את התרגיל באמצעות ציר המספרים. אם המחולק הוא מספר שלילי, מחפשים את הכפולה של המודולו הקטנה מהמספר הנתון (על ציר המספרים הכי קרובה מצד שמאל).
-21+1= -20 כלומר 1 + 7·3- = -20. ולכן $-20=1 \pmod 7$.
יש תלמידים שבדומה לפעולה במספרים חיוביים יתייחסו ל- 14- ככפולה של 7, במקום למספר 21-
ויכתבו בטעות $-20=6 \pmod 7$. במקרה זה חשוב לציין שביטוי חילוק אוקלידי (או חילוק עם שארית) הוא $a:b=p\cdot q+r$ שבו השארית היא מספר **חיובי**.
(-6)+ 7·2- = 14- (6- הוא מספר שלילי)
בעמ' 46 לומדים פעולת חיבור מודולרי. לאחר שקוראים את השיעור, אפשר להרחיב את הדיון ליותר משני מספרים, ולראות מהם החוקים שמתקיימים עבור פעולת חיבור מודולרי (חוק החילוף, חוק הקיבוץ). מומלץ לרשום את המסקנות על הלוח. בעמ' 47 מופיעה טבלת חיבור מודולרי "מודולו 7".
מעבר למשימות שמופיעות בתרגיל 5, ניתן לבקש מתלמידים לחקור לבד את הטבלה. ניתן לשאול שאלות מנחות: כיצד בנויה הטבלה? מה ניתן לומר על השורות של הטבלה? על עמודות של הטבלה?

חבורות

סימטריה שקיימת בטבלה; כיצד רואים אם מתקיים חוק החילוף; מהו המקום של אפסים בטבלה? וכד'. לאחר עבודה עצמית עם הטבלה, יש לדון בנקודות מרכזיות.
אץ תרגילים 7-6 ניתן לתת לעבודה עצמית (לבד או בקבוצות).
את השיעור שבעמ' 49 יש ללמוד במליאה. יש לרשום את כל התנאים של חבורה על הלוח ולעבור על כל התנאים ולראות שהם מתקיימים עבור פעולת מודולו. ניתן למלא ביחד לוח "מודולו 4" שבתרגיל 8 ולעשות ביחד את תרגילים 9, 10. לאחר מכן לסכם שפעולת "מודולו 4" היא חבורה מודולרית ולבקש מהתלמידים לעשות לבד את הלוחות "מודולו 2" ו"מודולו 12".
תרגיל 12 – תרגיל חקר שמתאים לעבודה עצמית לבד או בקבוצות.

<u>תשובות והערות לתרגילים:</u>

(1) א) $\{\ldots -25,-18,-11,-4,3,17,24,31\ldots\} : 3 \pmod 7$
$\{\ldots -24,-17,-10,-3,4,18,25,32\ldots\} : 4 \pmod 7$
$\{\ldots -22,-15,-8,-1,6,20,27,34\ldots\} : 6 \pmod 7$
ב) $30=2 \pmod 7$. $-20=1 \pmod 7$.
ג) אפשרות א. מפחיתים 7 או כפולות של 7 מכל מספר. אם השארית שווה, המספרים נמצאים באותה מחלקת שארית.
אפשרות ב. אם ההפרש בין שני המספרים הוא כפולה של 7, המספרים נמצאים באותו מחלקה.
הוכחה: נתונים

$$m > n$$
$$m = 7p + a$$
$$n = 7k + b$$
$$m - n = 7t$$

$$m - n = 7p + a - (7k + b) = 7t$$
$$m - n = 7(p - k) + (a - b) = 7t$$

המשתנים p, q, a ו- b הם מספרים טבעיים. אפשר לכתוב

לכן $a - b = 0$. המספרים m ו- n נמצאים באותה מחלקה.

(2) אחרי 20 צעדים הגעתי למספר 4 מודולו 8. אחרי עוד 15 צעדים הגעתי למספר 3 מודולו 8.
$20=4 \pmod 8$ ו- $15 = 7 \pmod 8$ $20+15=35$ $35=3 \pmod 8$
אפשר גם לכתוב $3 \pmod 8 = 11 \pmod 8 = 7 \pmod 8 + 4 \pmod 8 = 20+15$

(3) א) $100=0 \pmod 4$, $37=1 \pmod 4$, $15=3 \pmod 4$.
ב) $144=0 \pmod{12}$, $132=0 \pmod{12}$, $-82=2 \pmod{12}$, $15=3 \pmod{12}$.

(4) בכל השאלות התשובה היא "נכון"
א) $30 = 0 \pmod 2$ וגם $22=0 \pmod 2$.
ב) $50=1 \pmod 7$ לכן $50 = 7 \cdot 7 + 1$.
ג) $-14=1 \pmod 5$ וגם $-4=1 \pmod 5$.
ד) $28=1 \pmod 3$ וגם $13=1 \pmod 3$.

(5) א) בפעולת החיבור מוסיפים למחובר הראשון את המחובר השני התוצאה היא השארית מודולו 7.
ב) פעולת החיבור מודולו 7 סגורה לגבי הקבוצה . כל תוצאות הפעולה הם איברים בקבוצה.
ג) הפעולה בינארית חילופית. פעולת החיבור של כל שני מספרים נותנת תוצאה אחת ויחידה.
פעולת החיבור היא חילופית. אפשר לראות שהמספרים סימטריים לגבי האלכסון הראשי .
ד) קיים איבר ניטרלי. 0.
ה) לכל איבר יש איבר נגדי יחיד. לדוגמה: האיבר הנגדי ל-1 הוא 6, כי רק $1+6=0 \pmod 7$.
ו) הפעולה בינארית קיבוצית. לדוגמה:
$(2 + 3) + 4 = 5 \pmod 7 + 4 \pmod 7 = 9 \pmod 7 = 2 \pmod 7$
וכן $2 + (3 + 4) = 2 \pmod 7 + 0 \pmod 7 = 2 \pmod 7$.
לכן $(2+3) + 4 = 2 + (3 + 4)$. הדבר נכון עבור כל שלושה איברים בקבוצה.

(6) א)

$+ \pmod 5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1

חבורות

3	3	4	0	1	2
4	4	0	1	2	3

ב) הפעולה "$+(\mod 5)$" סגורה לגבי הקבוצה. כל התוצאות הן איברים בקבוצה.
ג) הפעולה "$+(\mod 5)$" בינארית חילופית לגבי הקבוצה. לכל שני איברים יש תוצאה אחת ויחידה. אפשר לראות שמשני צידי האלכסון הראשי יש סימטריה.
ד) הפעולה "$+(\mod 5)$" היא קיבוצית לגבי הקבוצה. לכל שלושה איברים בקבוצה מתקיים $(a+b)+c=a+(b+c)$, כמו בפעולת החיבור.
ה) קיים איבר ניטרלי, 0. ו) המספר הנגדי ל-0 הוא 0. הנגדי ל-1 הוא 4. הנגדי ל-2 הוא 3. הנגדי ל- 3 הוא 2. הנגדי ל-4 הוא 1.

(7) א) דני יחזור בשעה 22:00 , 10:00 בערב.
ב) הרכבת תגיע לפריס בשעה 15:00 למחרת, כלומר ב- 3:00 אחה"צ למחרת.
ג) אפשר לפתור לפי "מודולו 12", אבל אז צריך לציין האם מדובר בשעות לפנה"צ או אחה"צ. כאשר פותרים לפי "מודולו 24" מקבלים את השעה ואין צורך לציין האם לפנה"צ או אחה"צ.

(8)

$+(\mod 2)$	0	1
0	0	1
1	1	0

$+(\mod 12)$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

(9) כל התכונות של חבורה חילופית מתקיימות לגבי החיבור המודולרי.

(10) האיבר הנגדי ל-0 הוא 0. הנגדי ל-1 הוא 3. הנגדי ל-2 הוא 2. הנגדי ל-3 הוא 1.

(11) האיבר הנגדי ל- 0 הוא 0. הנגדי ל- 1 הוא 11. הנגדי ל- 2 הוא 10. הנגדי ל-3 הוא 9. הנגדי ל-4 הוא 8. הנגדי ל- 5 הוא 7. הנגדי ל-6 הוא 6. בגלל החילופיות, הנגדי ל- 7 הוא 5. הנגדי ל-8 הוא 4. הנגדי ל-9 הוא 3. הנגדי ל-10 הוא 2. הנגדי ל-11 הוא 1.

(12) נכון. דוגמה נוספת: $11=1(\mod 10)$, $12=2(\mod 10)$. $11+12=2+1(\mod 10)=3(\mod 10)$

שיעור רביעי: **חשבון מודולרי – חיסור מודולרי**, עמ' 51 (כשיעור אחד)

מושגים מרכזיים: **חיסור מודולרי – בעזרת "חיבור הנגדי".**

תכונות של חיסור מודולרי:
1) בחיסור מודולרי מתבטל החיבור המודולרי הקודם של אותו מספר .
2) בחיבור מודולרי של אותו מספר מתבטל החיסור המודולרי הקודם של אותו מספר.
3) החיבור המודולרי והחיסור המודולרי הם פעולות הפוכות זו לזו.

המלצה להוראה:
מומלץ להסביר את המשמעות של חיסור מודולרי שבעמ' 51 במליאה. רצוי להראות את שתי הדרכים לחיסור – חיסור באמצעות חיבור של הנגדי או חיסור בצורה ישירה. חשוב להראות מספר דוגמאות עם שתי הדרכים ולראות שמגיעים לאותה תוצאה. בדרך של חיסור בצורה ישירה יש להיזהר ולא לטעות

חבורות

במקרים שמקבלים תוצאה שלילית. כל תלמיד מוזמן לאמץ דרך שנוחה לו, אך רצוי שיידעו לחשב בשתי הדרכים. יש להבהיר את שלוש התכונות של חיסור מודולרי בכמה וכמה דוגמאות. ייתכן שיהיו תלמידים שלא יבינו מה מיוחד בתכונות הללו, מכיוון שהן מתקיימות בחיבור וחיסור "רגיל". יש להדגיש כי התכונות לא מובנות מאליהן בפעולת מודולו ושכל תכונה כזאת יש להוכיח על מנת להיות בטוחים שהיא מתקיימת גם בפעולות נוספות (במסגרת זו אנו לא עוסקים בהוכחות). בשיעור למטה מופיעה דוגמה לפתרון של משוואה. יש להבהיר כי התשובה למשוואה היא לא תשובה יחידה ושמעבר ל- $x = 5$ יכול להתאים כל מספר ממחלקה $5 \pmod 7$.
תרגילים 1 – 6 מתאימים לעבודה עצמית (לבד או בקבוצות). מומלץ לבדוק תרגילים נבחרים לפי מצב ההתקדמות בכיתה.

<u>תשובות והערות לתרגילים</u>:

(1) א) 2 . ב) 3 . ג) 2 . ד) 1 . ה) 9 . ו) 0 . ז) 1 . ח) 0 . ט) 5 .

(2) א) 3 . ב) 3 . ג) 4 . ד) 4 . המסקנה: עבור כל a, b, ו-c בחיבור מודולרי מתקיים אם $a - b = c \pmod D$ אז $b + c = a \pmod D$ (חיבור וחיסור מודולרי הן פעולות הפוכות).

(3) $(2 + 4 - 4 \pmod 3) = 2 + 1 + 2 \pmod 3) = 2 + 0 \pmod 3) = 2 \pmod 3$
תוצאה של חיבור וחיסור מודולרי של אותו מספר זהה לחיבור האיבר הניטראלי.
$(0 + 1) - 1 \pmod{10} = 1 - 1 \pmod{10} = 1 + 9 \pmod{10} = 10 \pmod{10} = 0 \pmod{10}$

(4)

p / n	1	2	3	4	5	6	7
1	2	3	4	5	6	7	X
2	1	X	3	4	5	6	7
3	7	1	2	X	4	5	6
4	6	7	1	2	3	X	5
5	X	6	7	1	2	3	4
6	4	5	X	7	1	2	3
7	3	4	5	6	X	1	2

במידה שיש זמן אפשר לחקור את החוקיות שבטבלה

(5) חג השבועות יחול ביום רביעי. חיבור מודולו 7. בכל שבוע שבעה ימים. $3+50=4 \pmod 7$.

(6) בקבוצה 25 תלמידים. 25 נותן שארית של 1 לפי מודולו 2, 3 ו-4. ושארית 0 במודולו 5.

שיעור חמישי: **חשבון מודולרי – כפל וחילוק**, עמ' 54 (כשני שיעורים)

<u>מושגים מרכזיים</u>: **כפל מודולרי**

תכונה של כפל מודולרי: במקום לכפול שני מספרים כלשהם בכפל מודולרי, אפשר לכפול שני מספרים השייכים לאותן מחלקות. בדרך-כלל נוח יותר להשתמש במספרים החיוביים הקטנים ביותר במחלקות אלו.

חילוק מודולרי – כפל במספר הפוך.

תכונות של חילוק מודולרי: בחילוק מתבטל כפל קודם באותו מספר.

הקבוצה {0, 1, 2, 3, 4, 5, 6} היא חבורה חילופית בכפל "מודולו 7" ללא ה- 0, מתקיים בה חוק הפילוג.

הקבוצה {0, 1, 2, 3, 4, 5} היא לא חבורה כפלית "מודולו 6".

חבורות

<u>המלצה להוראה</u>:
את השיעור בעמ' 54, כולל תרגילים 1 - 8 מומלץ לתת לעבודה עצמית (לבד או בקבוצות). התרגילים יכולים לסייע להעמקת הבנה של מושגים שנלמדו בשיעורים הקודמים של הנושא (קבוצה סגורה, פעולה בינארית – חילופית ועוד). בסיום הפעילות, שאמורה להיערך כשיעור אחד, כדאי לדון בתשובות לתרגילים 5, 8. כדאי להדגיש את התכונות שנלמדו במהלך הפעולות אשר קשורות לכפל "מודולו 7".
חשוב לרכז את כל המידע לגבי הקבוצה {0, 1, 2, 3, 4, 5, 6} ועבור פעולת "מודולו 7". כדאי להדגיש שאם נוציא את 0, נקבל חבורה חילופית בכפל. חשוב בכל פעם לחזור ולהזכיר שכרגע אנו עוסקים רק בכפל "מודולו 7" ולא בהכרח כל התכונות שמצאנו יהיו נכונות בכפל במודולו אחר ובקבוצות אחרות של מספרים.
את השיעור השני מומלץ להתחיל מלימוד של המושג "חילוק מודולרי" בעמ' 55. כדאי לקרוא במהלך הדיון הכיתתי את השיעור בעמ' 55. חילוק מודולארי מוגדר ככפל במספר הפוך. מספר הפוך הוא מושג לא פשוט וכדאי להקדיש זמן ולהביא דוגמאות למציאת מספרים הפוכים בפעולות כפל שונות.
בהמשך לומדים את תכונת החילוק המודולרי – בחילוק מתבטל כפל קודם באותו מספר. כדאי לבקש מהתלמידים להביא דוגמאות נוספות לתכונה, ולבדוק שהתכונה נכונה עבור מספרים שונים.
בסוף השיעור מופיע הסבר על פתרון משוואות פשוטות בעזרת כפל במספר ההפוך. חשוב להדגיש כי התוצאה של המשוואה אינה יחידה והיא יכולה להיות כל מספר ששייך למחלקה $6 \pmod 7$.
בעמ' 56 מופיע הסבר על חוק הפילוג. ניתן לבקש מהתלמידים לקרוא את ההסבר באופן עצמאי ולהגיע לקיום של חוק הפילוג עבור הפעולה "מודולו 7". את התרגילים 9 – 13 ניתן לתת לעבודה עצמית (לבד או בקבוצות). בסיום העבודה מומלץ לבדוק את תרגילים 12, 13. תרגיל 13 הוא חשוב על מנת להבין כי לא כל פעולת כפל מודולרי תבנה חבורה. חשוב להדגיש שראינו הרבה תכונות של פעולות חיבור/ חיסור/ כפל/ חילוק מודולרי והגענו להרבה מסקנות. בפרק לא עסקנו בהוכחות, ולכן אנו לא יכולים להיות בטוחים שהתכונות אכן מתקיימות. יש צורך בהוכחות פורמאליות של כל הטענות.

<u>תשובות והערות לתרגילים</u>:

(1) הפעולה "$x \pmod 7$" היא סגורה. כל התוצאות הן איברים בקבוצה.

(2) הפעולה "$x \pmod 7$" היא בינארית חילופית. התוצאות סימטריות לגבי האלכסון הראשי.

(3) הפעולה "$x \pmod 7$" היא בינארית קיבוצית. לכל a, b ו-c מתקיים $(a*b)*c=a*(b*c)$. כמו בכפל. (חשוב להדגיש שלא הוכחנו את התכונה, אלא רק בדקנו כמה דוגמאות ו"הרגשנו" שזה נכון.)

(4) קיים איבר ניטרלי, 1.

(5) ל- 0 אין איבר הפוך. לכל יתר איברי הקבוצה קיים איבר הפוך יחיד. אם נגדיר את הקבוצה ללא 0, היא תהיה חבורה.

(6) כל התוצאות שייכות למחלקת השאריות $1 \pmod 7$.

(7) כן. כאשר כופלים בכפל מודולרי שני מספרים זה בזה, התוצאה היא מכפלת מחלקת השאריות לפי המודולו המתאים (שוב פעם, לא הוכחנו את זה בצורה פורמלית, אלא רק "הרגשנו" שהטענה נכונה באמצעות מספר דוגמאות). ההוכחה מתבססת על חוק הפילוג המורחב.

(8) $7,002*21,708=2*1 \pmod 7=2 \pmod 7$. אין צורך בחילוק ב- 7, כי $7002 = 7000+2$ ו- $21708 =2100 + 700 +7 +1$

(9)

X(mod 5)	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(10) א) ההפוך ל-2 הוא 4 . ב) ההפוך ל-3 הוא 5 . ג) ההפוך ל- 4 הוא 2. ד) ההפוך ל-5 הוא 3.
ה) ההפוך ל-6 הוא 6.

(11) א) $4 : 3=4*5=6 \pmod 7$ ב) $3 : 2=3*4=5 \pmod 7$ ג) $5 : 6=5*6=2 \pmod 7$.
ד) $4 : 1=4*1=4 \pmod 7$ ה) $5 : 3=5*5=4 \pmod 7$ ו) $2 : 5=2*3=6 \pmod 7$

חבורות

(12) השעון יצלצל לראשונה צלצול מתאים לשעה הנכונה ביום ד' בשעה 13:00 (השעון יצלצל פעם אחת).
הסבר: כל 11 שעות "מפספסים" צלצול, לכן אחרי כל פספוס ההפרש בין הצלצול הנכון והצלצול השגוי מצמצם ב- 1. בשעה 8:00 ההפרש הוא 3 צלצולים. ההתאמה בין הצלצול הנכון והצלצול השגוי תקרה אחרי מספר שעות השווה ל- 8 מודולו 11, אך הגדול מ- 22 , כי יש צורך ב- 22 שעות לצמצם 2 צלצולים, כלומר לאחר 30 שעות.

(13)

X(mod 6)	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

א) הלוח סימטרי ביחס לאלכסון הראשי. ב) הכפל חילופי. סימטריה ביחס לאלכסון הראשי.
ג) הכפל קיבוצי. כמו כפל רגיל (לא הוכחנו, ראינו כמה דוגמאות). ד) קיים איבר ניטרלי יחיד, 1.
ה) יש כמה מספרים, השונים מ- 0 שמכפלתם 0. לדוגמה: 2*3 , 3*4.
ו) לא לכל האיברים קיים איבר הפוך. ל: 0 , 2, 4 , לא קיים איבר הפוך.
ז) הקבוצה אינה חבורה כיפלית, כיוון שלא לכל האיברים קיים איבר הפוך.

שיעור שישי: חשבון מודולרי – פתרון משוואות, עמ' 58 (כשני שיעורים)

מושגים מרכזיים: **פתרון משוואות בחשבון מודולרי**

המלצה להוראה:
מומלץ להתחיל את הוראת הפרק מדיון בשתי המשוואות המוצגות בשיעור. כדאי לבקש מהתלמידים להסביר מדוע המספרים שמופיעים בשיעור אכן מהווים פתרון של המשוואות הנתונות.
את תרגילים 1 – 3 מומלץ לתת לעבודה עצמית ולבדוק את הפתרונות שמתקבלים. כדאי להזכיר לתלמידים מה זה מספר הפוך וכיצד מוצאים אותו בטבלה.
אם התלמידים מתקשים בפתירת תרגיל 4, כדאי להנחות אותם, ולהציע לבדוק את כל האפשרויות ל- A עד שיגיעו לפתרון הרצוי. זה יעזור להם גם לענות על השאלות בהמשך.
את התרגילים 5 - 6 מומלץ לתת לעבודה עצמית ולבדוק תרגילים נבחרים.

תשובות והערות לתרגילים:

(1) א) ל-2 יש הפוך בכפל מודולו 7 , ההפוך הוא 4. ב) כדי לבודד את x יש לכפול בהפוך של 2.
ג) $x = 2 \pmod 7$ $2*4*x = 4*4 \pmod 7$ $2x = 4 \pmod 7$. אין פתרון נוסף , כיוון שיש רק איבר אחד הפוך ל-2.

(2) א) ל-2 אין איבר הפוך בכפל מודולו 6. ב) כיוון שאין איבר הפוך, אי-אפשר לבודד ע"י כפל בהפוך.
ג) $x = 5$, $x = 2$. יש שני פתרונות.

(3) א) ① $x = 5 \pmod 7$ $= 5 \pmod 7$ $2*4*x = 3*4 \pmod 7$ $2x = 3 \pmod 7$.
② $2x = 3 \pmod 6$. לתרגיל אין פתרון. 2 הוא מספר זוגי, ולכן בכפל מודולו 6 התוצאה צריכה להיות זוגית.
ב) בתרגיל 1 כפל מודולו 7 לכל איבר יש איבר הפוך, ולכן יש פתרון יחיד. בתרגיל 2 למספר 2 אין איבר הפוך. וכן כיוון ש- 2 הוא מספר זוגי התוצאה צריכה להיות אף היא זוגית.

(4) א) A=5. $2*4 = 3 \pmod 5$. x=4 A=3. $2 \cdot 0 = 3 \pmod 3$.
ב) B=4. למשוואה $2x=3 \pmod 4$ אין פתרון. התוצאה צריכה להיות מספר זוגי.
ג) C=8. למשוואה $2x=2 \pmod 8$ יש שני פתרונות. x=5 , x=1.
ד) פתרון אחד. כיוון למספר 2 יש רק הפוך אחד יש רק פתרון אחד.

(5) א) $2x-5=0 \pmod 7$ $2x = 5 \pmod 7$ $2 \cdot 4 \cdot x = 20 \pmod 7$ $x = 6 \pmod 7$.
ב) $2(x-5) = 3x \pmod 7$ $2x - 10 = 3x \pmod 7$ $-10 = x \pmod 7$ $x = 4 \pmod 7$

חבורות

ג) $2+x=2x+1 \pmod 3$ $x=1 \pmod 3$.

ד) $4x + 5 = 3 \pmod 6$ ← $4x = -2 \pmod 6 = 4 \pmod 6$ ← $x = 1 \pmod 6$ $x = 4 \pmod 6$

(לפי טבלה בעמ' 57, אין ל- 4 הופכי בכפל מודולו 6, לכן הפתרון לא יחיד)

ה) לפי הטבלה בעמ' 57, ל- 5 הופכי יחיד – 5.

$5(x+1) = 2 \pmod 6$ ← $5 \cdot 5(x + 1) = 2 \cdot 5 \pmod 6$ ← $x + 1 = 10 \pmod 6$

$x = 9 \pmod 6$ ← $x = 3 \pmod 6$

אפשר גם לפתור כך:

$5(x+1) = 2 \pmod 6$ ← $5x + 5 = 2 \pmod 6$ ← $5x = -3 \pmod 6 = 3 \pmod 6$

$5 \cdot 5 \cdot x = 5 \cdot 3 \pmod 6$ $x = 3 \pmod 6$

ו) $6(x+5) = 5(x+4) \pmod{37}$ ← $6x + 30 = 5x + 20 \pmod{37}$ $x = -10 \pmod{37}$

$X = 17 \pmod{37}$

ז) $3(x+1)=3 \pmod 6$ $3x=0 \pmod 6$ $x=4 \pmod 6$ $x=2 \pmod 6$ $x=0 \pmod 6$.

ח) $3(x-5) + 8 = 4(5-x) + 7 \pmod 9$ $3x – 15 + 8 = 20 – 4x + 7 \pmod 9$

$7x = 34 \pmod 9$ ← $7x = 7 \pmod 9$ ← $x = 1 \pmod 9$

ט) $6x = 8 \pmod 9$ אין פתרון.

(6) $3x + 1 = 7 \pmod{12}$ ← $3x = 6 \pmod{12}$ ← הפתרונות: ← $x = 2 \pmod{12}$

$x = 6 \pmod{12}$ $x = 10 \pmod{12}$.

<u>הערות לפרק</u>:

במהלך פתרון המשוואות אנו נעזרים בחוק הפילוג בחיסור למרות שלא הוכחנו את החוק במפורש. מומלץ להתייחס לעניין בכיתה.

כנ"ל לגבי העברת אגפים עם משתנים. החוקים הללו פועלים גם עבור משוואות מודולריות, אך חובה להתייחס לנושא בכיתה ולהסביר שבפרק אנו "טועמים" את הנושא ולא כל דבר מוכיחים בצורה פורמלית.

מסקנה שניתן להגיע אליה מתוך הפרק: אם במהלך פתרון של משוואה $ax = b \pmod c$ ל- a יש הופכי יחיד, יהיה למשוואה פתרון יחיד. אם ל – a אין הופכי יחיד, ייתכן שלמשוואה יהיו יותר מפתרון אחד או לא יהיו פתרונות.

אם מדובר בחבורה מודולרית כיפלית עבור פעולת כפל "מודולו c", תמיד נקבל פתרון אחד למשוואה.