סיכום מבנים אלגבריים - תשפ"ו 2026

6 ביוני 2026

גיא יער־און

הסיכום נכתב במהלך סמסטר ב' תשפ"ו (2026), ומבוסס על הרצאותיו של ד"ר ארז שיינר, לכן יתכן שנפלו טעויות בסיכום, כך שהשימוש בו על אחריותכם בלבד.

תוכן עניינים

1 הקדמה . . . 1
1.1 חבורה $(Group)$ . . . 2
1.2 חוג $(Ring)$ . . . 2
1.3 שדה $(Field)$ . . . 2
2 חבורות . . . 3
2.1 דוגמאות מרכזיות לחבורות . . . 3
2.2 תת חבורה . . . 4
2.3 סדרים . . . 6
2.4 מכפלה ישרה של חבורות . . . 7
2.5 תמורות . . . 8
2.6 הומומורפיזם ואיזומורפיזם . . . 11
2.7 משפט קיילי . . . 13
2.8 משפט לגראנז' . . . 14
2.9 חבורת אוילר . . . 16
2.9.1 אלגוריתם אוקלידס . . . 17
2.9.2 lcm . . . 18
2.10 חישוב פונקציית אוילר . . . 19
3 הצפנה . . . 21
3.1 דיפי הלמן . . . 23
3.2 ראשוניים גדולים - אלגוריתם מילר רבין . . . 25

1 הקדמה

מהם מבנים אלגבריים? למעשה, כבר למדנו מבנה אלגברי מסויים בקורס אלגברה לינארית: **שדה**. למשל, $\mathbb{Z}_7$ הוא מופע של שדה. בקורס, נעסוק בעיקר במבנה אלגברי שנקרא **חבורה**, ומעט במבנה אלגברי שנקרא **חוג**. כמו כן, נרחיב על מושג השדה.

אנחנו סטודנטים למדעי המחשב, למה שנלמד קורס מתקדם על מבנים אלגבריים? נלמד בקורס זה על שני שימושים חשובים של מבנים אלגבריים אלו שקשורים לעולם מדעי המחשב:

- הצפנה
- קידוד

מה זה **הצפנה**? אפשר לחשוב על כך **כהסתרה** של מידע, זו המטרה העיקרית של הצפנה. נרצה לדאוג גם ל**אמינות** ו**שלמות** של המידע. למשל: כאשר מייקרוסופט מורידים עדכון גרסה, הוא לא צריך להיות מוסתר - אבל אנחנו צריכים להיות בטוחים שמייקרוסופט הם אלו שכתבו את העדכון, על מנת שלא נוריד בטעות וירוס - זה נקרא אמינות, ושלמות הכוונה היא שלא "יתנקשו" לי במידע ואקבל את כולו.

מה זה **קידוד**? מוסכמה לתבנית להעברת מידע. למשל: "יום ההולדת שלי הוא 2", הכוונה היא שכנראה אפשר להסתכל על כך כיום השני בשנה. שני הצדדים כמובן, צריכים להסכים על הקידוד: אחרת - יהיו לנו כמה וכמה פרשנויות שונות למידע. למשל, אפשר להתייחס למשפט אודות

יום ההולדת כ"יום ההולדת שלי הוא בשני לחודש הבא" או "אני בן שנתיים" וכדומה. **פרוטוקול** (פרוטוקול תקשורת הוא סט של חוקים ומוסכמות המגדירים כיצד מכשירים דיגיטליים מעבירים נתונים ביניהם, כדי שיבינו את המידע הנשלח ויגיבו אליו בצורה תקינה.) למשל, הוא סוג של קידוד. בקורס נתמקד בעיקר בזיהוי ותיקון של שגיאות בקידוד ונלמד על RSA (אלגוריתם הצפנה).

האנלוגיה הכי קרובה למבנים אלגבריים מעולם מדעי המחשב, היא תכנות מונחה עצמים ובפרט ממשק (interface).
כפי שאמרנו, נתקלנו בעבר בשדות (מבנה אלגברי) ואף הוכחנו את הטענה הבאה:

משפט 1. יהי שדה $\mathbb{F}$, איבר האפס $0_{\mathbb{F}} \in \mathbb{F}$, ויהי $a \in \mathbb{F}$, אזי מתקיים: $a \cdot 0_{\mathbb{F}} = 0_{\mathbb{F}}$.

1.1 חבורה $(Group)$

הגדרה 2. חבורה היא קבוצה G יחד עם פעולה (בהיעדר מידע נוסף, נשתמש בסימון הכפל) שתסומן $(G, \cdot)$ כך שמתקיימות התכונות הבאות:

1. סגירות: $\forall a, b \in G : a \cdot b \in G$
2. אסוציאטיביות: $\forall a, b, c \in G : (ab)c = a(bc)$
3. ניטרלי (איבר יחידה): $\exists e_G \in G$ המקיים: $\forall a \in G : a \cdot e_G = e_G \cdot a = a$
4. קיום איבר הופכי: $\forall a \in G, \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e_G$

הערה 3. מניטרליות, נקבל כי בהכרח חבורה G לא יכולה להיות ריקה: תמיד קיים איבר ניטרלי. את האיבר הניטרלי נסמן בe_G לרוב.

הערה 4. אנחנו לא דורשים קומוטטיביות (חילופיות) בחבורה.

הגדרה 5. תהי G חבורה עם פעולה $\cdot$. נאמר כי G היא חבורה אבלית / קומוטטיבית / חילופית אם הפעולה $\cdot$ מקיימת את חוק החילוף: כלומר $\forall a, b \in G : ab = ba$.

דוגמה 6. נתבונן ב$G = (\mathbb{N}, +)$. האם מדובר בחבורה? אפילו אם $0 \in G$, אין בחבורה איברים הופכיים. הרי 0 הוא איבר ניטרלי לחיבור, ולכן עבור $2 \in \mathbb{N}$ למשל צריך להתקיים: $2 + 2^{-1} = 0$, כלומר $2^{-1} = -2$, אך $-2 \notin \mathbb{N}$ ולכן לא מדובר בחבורה.

דוגמה 7. לעומת זאת, $G = (\mathbb{Z}, +)$ היא כן חבורה. האיברים ההופכיים הם הנגדיים. מיהו האיבר ההופכי של 0? נבחין כי 0 הוא האיבר ההופכי (ה"נגדי") של עצמו.

דוגמה 8. האם $(\mathbb{Q}, \cdot)$ חבורה? לא! ל0 אין הופכי. אך, $(\mathbb{Q}\backslash\{0\}, \cdot)$ וכן $(\mathbb{Q}, +)$ הן חבורות.

1.2 חוג $(Ring)$

הגדרה 9. חוג הוא קבוצה R עם שתי פעולות (שנקרא להן חיבור וכפל, וכמובן רק נקרא להם כך), כך שמתקיימות התכונות הבאות:

1. $(R, +)$ הוא חבורה אבלית.
2. הכפל סגור, אסוציאטיבי ויש איבר יחידה.
3. פילוג: $\forall a, b, c \in G : (a + b)c = ac + bc = \wedge[a(b + c) = ab + ac]$

הערה 10. נבחין שוויתרנו על חילופיות (קומוטטיביות) ואיבר הופכי עבור הכפל. כיוון שאין חילוף, היינו חייבים לכתוב פעמיים את הפילוג.

דוגמה 11. ישנם שני מופעים מוכרים ביותר לחוג שאינם שדות:

1. $\mathbb{Z}_n$ - חוג השאריות עם פעולות מודלו n.
2. **המטריצות הריבועיות מסדר** n - החיבור טוב כחבורה, אך הכפל לא חילופי ולא כל המטריצות הפיכות! נראה כי חוג בדיוק מתאים עבור עולם המטריצות.

1.3 שדה $(Field)$

הגדרה 12. שדה הוא קבוצה $\mathbb{F}$ עם שתי פעולות (להן נקרא חיבור וכפל) כך שמתקיימות התכונות הבאות:

1. $(\mathbb{F}, +)$ היא חבורה אבלית.
2. $(\mathbb{F}\backslash\{0\}, \cdot)$ היא חבורה אבלית.
3. פילוג: $\forall a, b, c \in \mathbb{F} : a(b + c) = ab + ac$

הערה 13. נשים לב להבדל בין שדה לחבורה - בחבורה אנחנו דורשים שלכולם יש הופכי, בשדה לכולם פרט לאפס יש הופכי. לכן השדה ללא אפס הוא אכן חבורה.

הערה 14. האם צריך לומר במפורש כי $1 \neq 0$? לא, שהרי $1 \in \mathbb{F}\backslash\{0\}$ ולכן $1 \neq 0$.

הערה 15. כל שדה הוא בפרט חוג (גם זה מזכיר OOP - הורשה).

2 חבורות

הערה 16. כאשר ייאמר לנו החבורה $\mathbb{R}$ או החבורה $\mathbb{Z}$ - אנחנו ישר נניח כי מדובר בחבורה ביחס לפעולת החיבור. מדוע? כי $(\mathbb{R},\cdot)$ איננו חבורה! שכן עם פעולת הכפל אין הפיכות וכו'.

הערה 17. החבורה הטריוואלית תסומן $(\{e\},^*\}$ כאשר $*$ היא פעולה. מדובר בחבורה אבלית!

משפט 18. (משפט חלוקה עם שארית) יהי $n \in \mathbb{N}_+$ ויהי $b \in \mathbb{Z}$. אזי קיימים $q, r \in \mathbb{Z}$ יחידים כך ש: $b = n \cdot q + r$ וכן $0 \le r \le n-1$. q יקרא המנה של החלוקה של b בn וr היא השארית.

הוכחה: נחלק למקרים:

אם $b \ge 0$ (עבור $b < 0$ הוכחה דומה). אזי $(b+1)n > b$ בהכרח שהרי $n \ge 1$. כמו כן, $-1 \cdot n < b$. כלומר, קיים מס' שלם k כך ש$kn < b$ וקיים מס' שלם k כך ש$kn > b$. לכן נבחר את המס' השלם הגדול ביותר $q \in \mathbb{Z}$ כך ש$qn \le b$. נסמן: $r = b - qn$ (השארית). נראה כי: $qn \le b$ ולכן $r \ge 0$. כעת, נב"ש כי $r \ge n$ אזי $b - qn \ge n$ ולכן $b \ge (q+1)n$ בסתירה לכך שq הוא הגדול ביותר. ולכן סה"כ $0 \le r \le n-1$. כעת, לאחר שהראינו קיום, נוכיח יחידות:

נניח כי ישנם שני פירוקים: $b = q_1 n + r_1 = q_2 n + r_2$. נעביר אגפים ונקבל: $(q_1 - q_2)n = r_2 - r_1$. נב"ש כי $q_1 \ne q_2$ ולכן $|q_1 - q_2| \ge 1$ ולכן $|(q_1 - q_2)n| \ge n$. עם זאת, $|r_2 - r_1| \le n-1$ (שהרי $r_1, r_2 \in [0, n-1]$ ובפרט המרחק שלהם לא יכול לעבור את הטווח). לכן קיבלנו סתירה - שהרי צד אחד של המשוואה מקיים שערכו גדול שווה מn, וצד אחד קטן מn. סתירה! לכן $q_1 = q_2$ ומכאן גם בהכרח לפי המשוואה $r_1 = r_2$, ולכן הפירוק הוא יחיד.

■

הגדרה 19. יהיו $a, b \in \mathbb{Z}$. נאמר כי a **מחלק את** b אם קיים $k \in \mathbb{Z}$ כך ש$b = ka$ ונסמן $a|b$.

הגדרה 20. יהיו $a, b \in \mathbb{Z}$ ויהי $n \in \mathbb{N}$. נאמר כי a, b שקולים מודלו n אם $n|(a-b)$. (כלומר, יש להם אותה חלוקה בשארית r).

משפט 21. שקילות מודלו n היא יחס שקילות.

הגדרה 22. יהי $n \in \mathbb{N}$. נגדיר את אוסף מחלקות השקילות מודלו n כך: $\mathbb{Z}_n = \{[a] | a \in \mathbb{Z}\}$. לרוב, נסמן $\mathbb{Z}_n = \{0, ..., n-1\}$ אם כי האיברים הם מחלקות שקילות וצריך לסמן פורמלית כך: $\mathbb{Z}_n = \{[0], ..., [n-1]\}$. נגדיר חיבור מודלו n לפי: $[a] + [b] = [a+b]$.

משפט 23. יהי $n \in \mathbb{N}$. אזי, $(\mathbb{Z}_n, +)$ היא חבורה אבלית.

2.1 דוגמאות מרכזיות לחבורות

משפט 24. נגדיר את S_A להיות אוסף הפונקציות ההפיכות $f : A \to A$ עם פעולת ההרכבה. אזי, $(S_A, \circ)$ היא חבורה ונקראת **חבורת התמורות.**

הוכחה: נוכיח שאכן מדובר בחבורה. לכן, נעבור תכונה תכונה:

1. **סגירות:** תהיינה $f, g \in S_A$ שתי פונקציות הפיכות. נרצה להראות כי $fg = f \circ g \in S_A$. לפי בדיקה, הרכבת הפיכות היא פונקציה הפיכה כנדרש.
2. **אסוציאטיביות:** תהיינה $f, g, h \in S_A$. הרי, שוב לפי בדיקה הרכבת פונקציות היא פעולה אסוציאטיביות ולכן $(fg)h = f(gh)$
3. **ניטרלי:** פונקציית הזהות $Id \in S_A$ כי הפיכה ומקיימת לכל $f \in S_A$ כי: $f \circ Id = Id \circ f = f$
4. **קיום איבר הופכי:** תהי $f \in S_A$, אזי קיימת לf פונקציה הופכית ונסמנה f^{-1} (והרי בבירור ההופכית היא הפיכה בעצמה) והרי בבירור לפי בדיקה מתקיים $f \circ f^{-1} = f^{-1} \circ f = Id$.

■

משפט 25. נגדיר את הקבוצה הבאה:

$$GL_n(\mathbb{F}) = \{A \in \mathbb{F}^{n \times n} : |A| \ne 0\}$$

כלומר, קבוצת כל המטריצות ההפיכות. אזי, $(GL_n(\mathbb{F}), \cdot)$ היא חבורה.

הוכחה: נוכיח שאכן מדובר בחבורה. לכן, נעבור תכונה תכונה:

1. **סגירות:** תהיינה $A, B \in GL_n(\mathbb{F})$. אזי, כפל מטריצות הפיכות היא מטריצה הפיכה לפי לינארית 1 ולכן אכן $AB \in GL_n(\mathbb{F})$.
2. **אסוציאטיביות:** כפל מטריצות כמובן אסוציאטיבי.
3. **ניטרלי:** מטריצת הזהות I מקיימת לכל $A \in GL_n(\mathbb{F})$ כי: $AI = IA = A$.
4. **קיום איבר הופכי:** תהי $A \in GL_n(\mathbb{F})$. אזי, כיוון שA הפיכה קיימת לה הופכית A^{-1} שגם היא הפיכה. מכאן, מתקיים: $AA^{-1} = A^{-1}A = I$.

■

משפט 26. תהיינה חבורות $(G, \cdot_G)$ ו$(H, \cdot_H)$. נביט במכפלה הקרטזית: כלומר אוסף הזוגות

$$G \times H = \{(g, h) | g \in G, h \in H\}$$

ונגדיר את הפעולה: $(g_1, h_1) \cdot_{G \times H} (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$. אזי מדובר בחבורה.

הערה 27. $(GL_n(\mathbb{F}),+)$ איננה חבורה! $I,-I$ הן הפיכות אך $I+(-I)$ אינה הפיכה. אין סגירות (וחסר עוד הרבה תכונות).

משפט 28. יהי $\mathbb{F}$ שדה. נסמן ב$M_n(\mathbb{F})$ את המטריצות מגודל $n\times n$ מעל $\mathbb{F}$. אזי, $(M_n(\mathbb{F}),\cdot)$ היא חבורה אבלית.

הגדרה 29. תהי G חבורה. המרכז של G הוא:

$$Z(G)=\{x\in G|\forall y\in G: xy=yx\}$$

כלומר, מרכז החבורה הוא קבוצת האיברים בחבורה שמתחלפים עם כולם.

משפט 30. G היא חבורה אבלית $\iff Z(G)=G$

הערה 31. תמיד מתקיים $e_G\in Z(G)$.

2.2 תת חבורה

הגדרה 32. תהי חבורה G ותהי $H\subseteq G$ תת קבוצה. נאמר כי H היא תת חבורה של G ונסמן $H\leq G$ אם H היא חבורה ביחס לפעולה של G.

משפט 33. תהי חבורה G ויהיו $a,b,c\in G$ כך ש$ab=ac$ אזי $b=c$.
הוכחה:

$$ab=ac\Longrightarrow(a^{-1})(ab)=(a^{-1})(ac)\Longrightarrow(a^{-1}a)b=(a^{-1}a)c\Longrightarrow e_Gb=e_Gh\Longrightarrow b=h$$

■

משפט 34. (קריטריון מקוצר לתת חבורה). תהי חבורה G ותהי $H\subseteq G$. אזי, $H\leq G$ אם ורק אם שני התנאים הבאים מתקיימים:
1. $e_G\in H$
2. לכל $a,b\in H$ מתקיים כי $a\cdot_G b^{-1}\in H$.

הוכחה:
$\Longleftarrow$ בכיוון ראשון, נניח כי $H\leq G$ ונראה כי מתקיימים התנאים $1+2$. נרצה להוכיח $e_G\in H$. כיוון שH תת חבורה, בH חייב להיות איבר יחידה כי זו חבורה ונסמנו e_H. אך $e_H\in G$. G חבורה ולכן יש לו איבר יחידה e_G. (כיוון שגוי להוכחה: לומר כי ישנו איבר יחידה יחיד, זה שגוי כי יתכן וe_H איבר יחידה רק בתת החבורה הנ"ל ולא עבור שאר האיברים).
נרצה להוכיח $e_G=e_H$. נביט ב$e_H\cdot e_G$. מצד אחד, $e_H\in H\subseteq G$ ובפרט $e_H\in G$. כמו כן גם $e_G\in G$ ובגלל שG חבורה, יש סגירות לפעולה, וכן e_G ניטרלית לפעולה ולכן $e_H\cdot e_G=e_H$. כמו כן, $e_H\cdot e_H=e_H$ (כאן e_H כן ניטרלי). כעת מטרנזטיביות: $e_H\cdot e_H=e_H\cdot e_G$ ומתכונת הצמצום (משפט 29) הרי שקיבלנו $e_H=e_G$.
כעת נרצה להראות את התכונה השנייה. יהיו $a,b\in H$. נרצה להוכיח $ab^{-1}\in H$. אם כן, כיוון שH היא חבורה וכן $b\in H$ קיים לו הופכי, נסמנו c. אזי $bc=cb=e$. מצד שני, עבור b^{-1} (ההופכי של b בG) מתקיים: $bb^{-1}=b^{-1}b=e$. ושוב מטרנזטיביות קיבלנו $bc=bb^{-1}$ ומתכונת הצמצום $c=b^{-1}$. כלומר, הוכחנו כי $b^{-1}\in H$ (ההופכי הוא יחיד, ובפרט הוא קיים גם בתת חבורה). כעת, כיוון ש$a,b^{-1}\in H$ מסגירות של H נקבל $ab^{-1}\in H$.
$\Longrightarrow$ בכיוון השני, נניח כי התנאים מתקיימים ונוכיח כי H חבורה.
סגירות: יהיו $a,b\in H$. נרצה להוכיח $ab\in H$. אם כן, $b^{-1}\in H$ ממה שראינו כבר, וכן $a\in H$. לפי תנאי 2 אם נסמן $c=b^{-1}$ נקבל $ac^{-1}\in H$. אך:

$$ac^{-1}=a(b^{-1})^{-1}=ab\in H$$

אסוציאטיביות: כיוון שהפעולה אסוציאטיבית על כל איברי G, היא בפרט אסוציאטיבית על איברי H ולכן ישנה אסוציאטיביות גם כאן.
קיום איבר יחידה: ראשית, $e_G\in H$ ובבירור הוא ניטרלי בH, כי ניטרלי לכל איברי H.
הפיכות: יהי $b\in H$. נרצה להוכיח $b^{-1}\in H$ (יודעים כי הוא קיים, אך בG. אם נראה כי הוא בH אזי יש הופכי לb). אם כן, $e_G\in H$ וכן $b\in H$ ולפי תנאי 2 שמניחים שמתקיים $e_Gb^{-1}\in H$, אך $e_Gb^{-1}=b^{-1}\in H$ כנדרש.
ולכן סה"כ H היא תת חבורה.

■

דוגמה 35. נתבונן ב$SL_n(\mathbb{F})=\{A\in\mathbb{F}^{n\times n}|det(A)=1\}\subseteq GL_n(\mathbb{F})$. אזי, $SL_n(\mathbb{F})\leq GL_n(\mathbb{F})$.
הוכחה: נוכיח לפי הקריטריון המקוצר.
אם כן, $det(I)=1$ ולכן $I\in SL_n$ והרי $I=e_{GL_n}$.
שנית, יהיו $A,B\in SL_n$. אזי, נרצה להראות $AB^{-1}\in SL_n$. והרי ש:

$$det(AB^{-1})=det(A)\cdot det(B)^{-1}=1\cdot 1^{-1}=1$$

ולכן $AB^{-1} \in SL_n$, כנדרש.

■

הגדרה 36. תהי חבורה G ויהי $a \in G$. נגדיר את תת החבורה הציקלית הנוצרת מa להיות:

$$< a >= \{a^k | k \in \mathbb{Z}\}$$

באשר נגדיר את פעולת החזקה: עבור $n \in \mathbb{N}_+$ נגדיר $a^n = a \cdot a \cdot ..... \cdot a$ וכן $a^0 = e_G$ וכן $a^{-n} = (a^{-1})^n = (a^n)^{-1}$.

הערה 37. סימון החזקה עשוי להיות מבלבל מאוד כאשר הפעולה אינה כפל. למשל, $G = (\mathbb{Z}, +)$. אזי, $< 1 >= \mathbb{Z}$. מדוע? כי $1^4 = 1 + 1 + 1 + 1 = 4$, אז לשים לב. לכן לעיתים אם נדע מראש שהפעולה חיבורית, במקום a^n נכתוב na.

דוגמה 38. נביט בחבורה $(\mathbb{C}\backslash\{0\}, \cdot)$ ונביט בתת החבורה הציקלית $< 2 >$. נראה כי:

$$< 2 >= \{2^k | k \in \mathbb{Z}\} = \{1, 2, 4, 8, ...\frac{1}{2}, \frac{1}{4}, ...\}$$

בדומה,

$$< i >= \{i^k | k \in \mathbb{Z}\} = \{1, i, -1, \frac{1}{i} = -i\}$$

כיצד אכן אנחנו יודעים כי לא חסרים עוד איברים ב$< i >$? מדוע גודל תת החבורה הציקלית הוא 4? מיד נגלה. (רמז: $i^4 = 1 = e_G$).

הגדרה 39. יהי $n > 1$ כך ש$n \in \mathbb{N}$. נגדיר את חוג השאריות $\mathbb{Z}_n = \{0, ..., n-1\}$ עם פעולות כפל וחיבור מודולו n כלומר: $a +_{\mathbb{Z}_n} b$ מוגדר להיות שארית החלוקה של $a + n$ בn.

משפט 40. $\mathbb{Z}_n$ הוא שדה $\iff$ n הוא מס' ראשוני.

הגדרה 41. חבורה G ששווה לתת חבורה ציקלית כלשהי $< a > a \in G$, כלומר $G =< a >$ נקראת חבורה ציקלית. האיבר a שממנו נוצרה תת החבורה הציקלית נקרא **יוצר** של החבורה.

דוגמה 42. נתבונן ב$(\mathbb{Z}_5, +)$. ונתבונן ב$< 2 >$.
$2^0 = 0$. מדוע? שהרי החזקה מתייחסת לפעולה, והכוונה לחבר את 2 אפס פעמים - זה שווה אפס.
$2^1 = 2$ שהרי מחברים את 2 פעם אחת.
$2^2 = 2 + 2 = 4$ שמחברים את 2 שני פעמים.
$2^3 = 2 + 2 + 2 = 6 \equiv 1$
$2^4 = 2 + 2 + 2 + 2 = 8 \equiv 3$
וקיבלנו $< 2 >= \{0, 1, 2, 3, 4\} = \mathbb{Z}_5$ ולכן מדובר בחבורה ציקלית, עם יוצר 2. בדומה, $< 4 >= \mathbb{Z}_5$ ולכן גם 4 הוא יוצר.

משפט 43. תת החבורה הציקלית היא תת חבורה.

הוכחה: תהי חבורה G ויהי $a \in G$. נביט בתת החבורה הציקלית של a. כלומר, $< a >$. נוכיח שהיא תת חבורה של G באמצעות הקריטריון המקוצר:
א. נראה כי עבור $a^0 = e_G$ (שהרי עבור $k = 0$ נקבל $a^0 = e_G$ שהרי מדובר בהפעלת הפעולה 0 פעמים על a, ולכן מקבלים את איבר היחידה).
ב. נרצה להראות כי לכל $a^k, a^m \in G$ מתקיים $a^k \cdot (a^m)^{-1} \in G$. והרי:

$$a^k \cdot (a^m)^{-1} = a^k \cdot a^{-m} = a^{k-m} \in G$$

שהרי $k - m$ הוא מס' שלם כחיסור של מס' שלמים.
לכן סה"כ $< a >$ היא תת חבורה של G לכל $a \in G$.

■

2.3 סדרים

הגדרה 44. תהי G חבורה. נגדיר את הסדר של G להיות עוצמתה כקבוצה. כלומר, כמה איברים יש בG. נסמן זאת ב$|G|$.

דוגמה 45. $|\mathbb{Z}_4| = 4$ וכן $|\mathbb{Z}| = \aleph_0$.

הגדרה 46. תהי G חבורה ויהי $g \in G$. הסדר של האיבר g הוא המס' הטבעי n הקטן ביותר כך שמתקיים $g^n = e_G$. נסמן זאת ע"י $o(g) = n$. אם אין מס' טבעי שכזה, נאמר כי הסדר של g הוא אנסוף. וכן מתקיים $a = e_G \iff o(a) = 1$.

משפט 47. תהי G חבורה ויהי $a \in G$. אזי, $o(a) = o(a^{-1})$

הוכחה: כטענת עזר - נראה כי תמיד $aa^{-1} = a^{-1}a = e$ ובפרט $aa^{-1} = a^{-1}a$ כלומר כל איבר מתחלף עם עצמו.
נחלק למקרים:

1. הסדר של a הוא סופי כלומר $o(a) = n < \infty$. אזי, לפי הגדרה: $a^n = e$. וכן:

$$e = e^n = (a^{-1}a)^n =_* (a^{-1})^n a^n =_{**} (a^{-1})^n e = (a^{-1})^n$$

שכן $*$ נכון בגלל שכל איבר a מתחלף עם עצמו (זה לא נכון תמיד בחבורה) ו$**$ נכון כי $a^n = e$. כלומר קיבלנו $e = (a^{-1})^n$. מכאן, $o(a^{-1}) \leq n$. אם נחזור בדומה על התהליך עם a^{-1}, נקבל כי $n = o(a) \leq o(a^{-1})$. לכן סה"כ $o(a) = o(a^{-1})$

2. הסדר של a אינו סופי. דהיינו $o(a) = \infty$. נניח כי $o(a^{-1}) = n$ עבור n טבעי כלשהו בשלילה, כלומר שהסדר של ההופכי סופי. אזי, לפי המקרה הקודם נקבל כי $o(a^{-1}) = o(a) = n$ אך $o(a) = \infty$ בסתירה.

■

משפט 48. תהי חבורה G ויהי $a \in G$. אזי, $o(a) = |< a >|$. כלומר, הסדר של איבר הוא גודלה של תת החבורה הציקלית. כמו כן, אם $o(a) = n$ אזי $< a >= \{e, a, a^2, ..., a^{n-1}\}$ וכן הם שונים זה מזה.

הוכחה: תהי חבורה G ויהי $a \in G$. נחלק למקרים:

ראשית נניח כי הסדר סופי: כלומר $o(a) = n$. נרצה להוכיח כי $< a >= \{e, a, a^2, ..., a^{n-1}\}$. נבחין כי אם נוכיח זאת ושהם שונים אכן נקבל כי $|< a >| = n$ (שכן לא יתכנו עוד איברים שאלו כל החזקות כי זה שווה ל$o(a)$) ונסיים. נבצע הכלה דו כיוונית על מנת להוכיח שוויון זה.

$\subseteq$ לפי הגדרה, כל החזקות השלמות של a אכן נמצאות ב$< a >$ לפי הגדרת הסדר כלומר אכן $\{e, a, a^2, ..., a^{n-1}\} \subseteq < a >$.

$\supseteq$ יהי $a^k \in < a >$. נרצה להוכיח כי בהכרח $a^k \in \{e, ..., a^{n-1}\}$. נבצע חלוקה עם שארית של k בn: $k = qn + r$. מכאן:

$$a^k = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = (e)^q \cdot a^r = a^r$$

ולכן בהכרח $k = r \in [n-1]$ כפי שרצינו.

כעת נוכיח כי איברי הקבוצה שונים זה מזה. נג"ש כי קיימים $0 \leq n_1 < n_2 \leq n-1$ כך ש: $a^{n_1} = a^{n_2}$. נכפול את שני הצדדים בa^{-n_1} ונקבל:

$$e = a^{n_2 - n_1}$$

כעת, אנחנו יודעים כי $n_2 - n_1 > 0$ וכיוון ש$n_2 \leq n-1$ נקבל $n_2 - n_1 \leq n-1$ ומצאנו ערך $(n_2 - n_1)$ קטן מn שעבורו מתקיים $a^{n_2-n_1} = e$, ולכן $o(a) = n_2 - n_1 < n$ בסתירה. לכן איברי החבורה שונים זה מזה.

מקרה שני: נניח כי $o(a) = \infty$ במקרה האינסופי. נג"ש כי $o(a)$ סופי. לכן, בהכרח ישנן לפחות 2 חזקות שנותנות את אותה התוצאה. כלומר, $a^{n_1} = a^{n_2}$ (כי אנחנו במקרה הסופי). שוב, נקבל כי $a^{n_2-n_1} = e$ ונקבל $o(a) = n_2 - n_1$ בסתירה לכך שהסדר אינסופי (שהרי לפי ההגדרה, אף חזקה חיובית לא מגיעה לe).

■

דוגמה 49. אם G סופית, אזי כל תת חבורה שלה מוכלת בה ולכן גם היא בהכרח סופית, לכן בפרט כל תתי החבורות הציקליות הן סופיות, ולכן לכל איבר בחבורה יש סדר סופי.

הערה 50. נבחין כי בחבורה ציקלית, הסדר של יוצר הוא הסדר של החבורה. מדוע? כי לפי הגדרה מתקיים $< a >= G$. וכן, $|< a >| = o(a)$ וכן $|G|$ זהו סדר החבורה ומטרנזטיביות השוויון נקבל: $|G| = o(a)$.

משפט 51. תהי G חבורה ציקלית, אזי G אבלית.

הוכחה: תהי G חבורה ציקלית, אזי קיים איבר $a \in G$ כך ש$G =< a >$. נרצה להוכיח כי לכל $g_1, g_2 \in G$ מתחלפים. אם כן, G ציקלית לכן קיימים $g_1 = a^i, g_2 = a^j$. מכאן:

$$g_1 g_2 = a^i a^j = a^{i+j} = a^{j+i} = a^j a^i = g_2 g_1$$

כנדרש.

■

משפט 52. אם G ציקלית, אזי כל תת חבורה של G ציקלית.
הוכחה: תהי $H \leq G$ תת חבורה של G וכן G ציקלית. נרצה להראות כי H ציקלית בהכרח. נסמן $G =< a >$. אם כן, כל האיברים בG מהצורה a^i. לכן, גם כל האיברים בH מצורה זו. נחלק למקרים:
אם $H = \{e\}$ אזי $H =< e >$ וסיימנו.
אחרת, לא טריוואלי. יהי $s \in \mathbb{Z}\backslash\{0\}$ המספר המינימלי בערך מוחלט כך ש$a^s \in H$. נניח כי $s \in \mathbb{N}$. נרצה להראות כי $H =< a^s >$. נראה זאת ע"י הכלה.
תחילה, בבירור $< a^s > \subseteq H$, שכן לפי הגדרה $< a^s >$ זו תת החבורה הקטנה ביותר שמכילה את a^s והרי $a^s \in H$ ולכן H מכילה את $< a^s >$.
בכיוון השני, יהי $h \in H$. אזי, קיים k עבורו $h = a^k$ כי $h \in G$. לפי משפט חלוקה עם שארית, קיימים q וr עבורם: $k = qs + r$ כך ש$0 \leq r < s$. מכאן:

$$a^k = a^{qs+r} = a^{qs} \cdot a^r = (a^s)^q \cdot a^r$$

ולכן, $a^r = a^k \cdot ((a^s)^q)^{-1}$. אז, $a^s, a^k \in H$ ומכאן גם $a^r \in H$ (מסגירות לכפל ולהופכי). אם $r \neq 0$, נבחין כי זו סתירה למינימליות של s כי $a^r \in H$ וגם $0 < r < s$ ומצאנו חזקה קטנה מs בסתירה. ולכן $r = 0$. כלומר, $k = qs$. ולכן, $s|k$. כלומר, $a^k \in < a^s >$.

■

משפט 53. תהי G חבורה ויהי $a \in G$. אזי, $a^n = e$ אמ"מ $o(a)|n$.
הוכחה: בכיוון ראשון, נניח $o(a)|n$. לכן קיים k עבורו $n = k \cdot o(a)$. מכאן,

$$a^n = a^{k \cdot o(a)} = (a^{o(a)})^k = (e)^k = e$$

בכיוון שני, נניח $a^n = e$. נרצה להראות כי $o(a)|n$. מכאן בהכרח נקבל $o(a) \leq |n|$. לפי משפט חלוקה עם שארית, קיימים q וr עבורם $n = q \cdot o(a) + r$ עם $0 \leq r < o(a)$. מכאן:

$$e = a^n = a^{q \cdot o(a) + r} = (a^{o(a)})^q \cdot a^r = (e)^q \cdot a^r = a^r$$

כלומר קיבלנו $a^r = e$, אך אנחנו יודעים כי $o(a)$ הוא המס' הטבעי הקטן ביותר כך ש$a^{o(a)} = e$. מכאן, $r = 0$ בהכרח שכן לא יתכן אצלנו כי $0 < r < o(a)$. לכן, $n = q \cdot o(a)$ ונקבל כי אכן $o(a)|n$.

■

2.4 מכפלה ישרה של חבורות

תהיינה $(G, *), (H, \bullet)$ חבורות. נתבונן במכפלה הקרטזית בניהן $G \times H$ עם פעולת רכיב רכיב שנסמנה $\odot$ כך:

$$(g_1, h_1) \odot (g_2, g_2) = (g_1 * g_2, h_1 \bullet h_2)$$

אזי מתקיים כי $G \times H$ ביחס ל$\odot$ היא חבורה. איבר היחידה בחבורה זו הינו (e_G, e_H).

משפט 54. $\mathbb{Z}^n \times \mathbb{Z}^n$ איננה ציקלית לכל $n \geq 2$.
הוכחה: כמובן, ביחס לחיבור. יהי איבר (a, b) בחבורה. נראה כי:

$$(a, b)^n = (a, b) \cdot (a, b) \cdot .... \cdot (a, b) = (a + ... + a, b + ...b) = (na, nb) = (0, 0)$$

מכאן, בהכרח $o(a, b) \leq n$. כלומר, לכל זוג איברים הסדר לכל היותר n. עם זאת, $|\mathbb{Z}_n \times \mathbb{Z}_n| = n^2$ וכן אם החבורה הייתה ציקלית, היה בה איבר מסדר n^2, כיוון ש$n^2 > n$ לכל $n \geq 2$ נקבל כי בהכרח החבורה לא ציקלית.

■

2.5 תמורות

דוגמה 55. נביט בלוח הכפל של $\mathbb{Z}_5\backslash\{0\}$ עם פעולת הכפל:

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

נבחין: כל שורה בטבלה מהווה תמורה של המספרים $\{1,2,3,4\}$ (איברי החבורה). נבחין ־ לא כל תמורה (שהרי יש $n!$ ובטבלה n שורות) נכנסת לטבלה. אלא ־ נכנסות כמה תמורות נבחרות שמייצגות את החבורה.

תזכורת: לכל קבוצה A, קבוצת הפונקציות ההפיכות $A \to A$ עם פעולת ההרכבה מסומנת S_A, ונקראת חבורת התמורות.

הגדרה 56. נגדיר S_n להיות אוסף כל הפונקציות $f:\{1,...,n\}\to\{1,...,n\}$ ההפיכות. פורמלית,

$$S_n = \{f:\{1,..n\}\to\{1,..,n\}|\text{f is onto and 1-1}\}$$

כיצד נסמן תמורות? באופן בזבזני, נוכל לכתוב בשורה ראשונה את המספרים $(1,2,...,n)$ ושורה מתחתיו לאן כל איבר נשלח, כלומר $f(i)$ $\forall i\in[n]$:.

דוגמה 57. אם נקח את S_4, ונקח את Id_4: נקבל את התמורה (פונקציה) הבאה:

$$Id_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

בדומה,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \in S_4 \mid f(1)=2, f(2)=1, f(3)=3, f(4)=4$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \in S_4 \mid f(1)=3, f(2)=1, f(3)=2, f(4)=4$$

נרצה לחשב את ההרכבה של התמורות.

$$f\circ g(1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(g(1))=3 & f(g(2))=2 & f(g(3))=1 & f(g(4))=4 \end{pmatrix}$$

דוגמה 58. נרצה לחשב תת חבורה ציקלית של תמורה.

$$<\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}>=\{I,\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2,...\}=\{I,\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$$

ונראה כי כבר $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^3 = I$ ולכן נקבל $o(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}) = 3$.
בדומה,

$$<\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}>=\{I,\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}$$

נבחין כי $o(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}) = 2$.
נשים לב כי $|S_3| = 3! = 6$. האם זה מקרי שתתי החבורות הציקליות מגודל (סדר) שמחלק את גודל החבורה S_3? כמובן שלא ־ נלמד בהמשך (משפט לגראנז').

■

הגדרה 59. לכל תמורה סופית $f \in S_n$ נגדיר את הסימן של התמורה כך:

$$sign(f) = \prod_{1 \le j < i \le n} \frac{f(i) - f(j)}{i - j}$$

הגדרה 60. מחזור (או עגיל) בS_n הוא תמורה המציינת מעגל אחד של החלפות של מספרים שונים $a_1 \to a_2 \to .... \to a_k \to a_1$ ושאר המספרים נשלחים לעצמם. כותבים את התמורה הנ"ל בקיצור $(a_1, ..., a_k)$ ואורך המחזור הוא k.

לדוגמה:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

התמורה הנ"ל היא המחזור $(1, 2, 3)$. מדוע? $1 \to \sigma(1) = 2 \to \sigma(2) = 3 \to \sigma(3) = 1$.

משפט 61. כל תמורה ניתנת לכתיבה כהרכבת מחזורים זרים, כאשר הכוונה ב"זרים" היא שאין להם מס' משותף שהם משנים את מיקומו.

דוגמה 62. נתבונן בתמורה הבאה:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 1 & 5 & 2 & 6 \end{pmatrix} \in S_7$$

נקח מספר ונתחיל לעבור על המחזור שמתחיל בו. למשל: $1 \to 4 \to 1$. כלומר $(1, 4)$.
ושוב, $2 \to 7 \to 6 \to 2$ וקיבלנו $(2, 7, 6)$.
ושוב, $3 \to 3$ וקיבלנו (3).
ושוב, $5 \to 5$ וקיבלנו (5).
כיוון שהמספרים הולכים לעצמם הם מחזורים בודדים ולרוב לא נכתוב אותם. לכן נוכל לכתוב את התמורה כ:

$$\sigma = (1\ 4)(2\ 7\ 6)$$

נראה שימוש לדרך זו - ניתן לחשב את σ^2 בקלות. כיוון שמחזורים זרים מתחלפים זה עם זה, כלומר,

$$\sigma^2 = ((1\ 4)(2\ 7\ 6))^2 = (1\ 4)^2(2\ 7\ 6)^2$$

כעת, $(1, 4)^2$ כאשר נפעיל פעולה פעמיים נחזור לאותה נקודה. לכן, $1 \to 4 \to 1$ וכן $4 \to 1 \to 4$ וקיבלנו $(1)(4)$ ולא נכתוב זאת בתמורה (נשלחים לעצמם).
בדומה, $2 \to 7 \to 6$ וכן $7 \to 6 \to 2$ וכן $6 \to 2 \to 7$. קיבלנו: $(2, 6, 7)$ כמחזור. לכן:

$$\sigma^2 = (2, 6, 7)$$

■

משפט 63. מתקיים $sign(f) = \prod_{1 \le j < i \le n} \frac{f(i) - f(j)}{i - j} = \pm 1$.
הוכחה: בעקרון, אם נרצה להוכיח פחות פורמלית בשורה: כיוון שf היא פונקציה חח"ע ועל, אנחנו מקבלים זוגות בפונה מהצורה $(f(i), f(j))$ ובמכנה (i, j). כיוון שf היא תמורה ובפרט חח"ע ועל כל הזוגות שיופיעו בפונה ובמכנה יהיו זהים. לכן $|sign(f)| = 1$. מכאן, בהתאם לסימן נקבל ± 1. כעת, להוכחה פורמלית:
נסמן את קבוצת האיברים הלא סדורים של זוגות איברים שונים ב$\{1, .., n\}$ כ- $A = \{(i, j) | 1 \le i, j \le n \wedge i \ne j\}$. נגדיר פונקציה $\Phi : A \to A$ ע"י $\Phi(\{i, j\}) = \{f(i), f(j)\}$. קל לראות כי Φ היא פונקציה חח"ע ועל לפי החח"ע ועל של f. אם כן נקבל:

$$sign(f) = \prod_{1 \le j < i \le n} \frac{f(i) - f(j)}{i - j} = \frac{\prod_{1 \le j < i \le n} f(i) - f(j)}{\prod_{1 \le j < i \le n} i - j}$$

כיוון שf היא תמורה,

$$\{|f(i) - f(j)| 1 \le j < i \le n\} = \{|i - j| 1 \le i < j \le n\}$$

ולכן המונה והמכנה שווים בערכם המוחלט לכן נקבל $|sign(f)| = 1$ כלומר $sign(f) = \pm 1$.
יתרה מכן, כל זוג (i,j) המקיים $i > j$ אך $f(i) < f(j)$ תורם -1 למכפלה. לכן, סימן התמורה הוא מס' החילופים N ומתקיים: $sign(f) = (-1)^N$.

■

משפט 64. יהיו שתי תמורות f, g. אזי: $sing(f \circ g) = sign(f) \cdot sign(g)$.
הוכחה:

$$sing(f \circ g) = \prod_{i>j} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_i - x_j} = \prod_{i>j} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_{g(i)} - x_{g(j)}} \cdot \frac{x_{g(i)} - x_{g(j)}}{x_i - x_j} =$$

$$\prod_{i>j} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_{g(i)} - x_{g(j)}} \times \prod_{i>j} \frac{x_{g(i)} - x_{g(j)}}{x_i - x_j}$$

כיוון שf היא תמורה, אוסף הזוגות $i > j$ שווה לאוסף הזוגות $g(i), g(j)$ לכן: $\prod_{i>j} \frac{x_{f(g(i))} - x_{f(g(j))}}{x_{g(i)} - x_{g(j)}} = sing(f)$. סה"כ נקבל:

$$sing(f \circ g) = sing(f) \times sign(g)$$

■

הגדרה 65. יהיו $1 \leq p_1 \neq p_2 \leq n$ זוג איברים. נגדיר את תמורת החילוף $f = (p_1 p_2) \in S_n$ להיות:

$$f(x) = \left\{ \begin{array}{cc} p_2 & x = p_1 \\ p_1 & x = p_2 \\ x & o.w \end{array} \right\}$$

אזי, f היא תמורה.

משפט 66. תהי f תמורת חילוף. אזי, $sign(f) = -1$.
הוכחה: בה"כ שהאיברים שמבצעים את החילוף הם p_1, p_2 ויהיו $(p_3, ..., p_n)$ שאר האיברים. אם כן:

$$sign((p_1 p_2)) = \frac{p_1 - p_2}{p_2 - p_1} \times \frac{p_3 - p_2}{p_3 - p_1} \times ... \times \frac{p_n - p_2}{p_n - p_1} \times \frac{p_3 - p_1}{p_3 - p_2} \times ... \times \frac{p_n - p_1}{p_n - p_2} \times \frac{p_4 - p_3}{p_4 - p_3} ... \times \frac{p_n - p_{n-1}}{p_n - p_{n-1}} = -1 \cdot 1 \cdot ... \cdot 1 = -1$$

כנדרש.

■

הגדרה 67. יהיו $1 \leq p_1, ..., p_k \leq n$ שונים. נגדיר את המחזור:

$$(p_1 p_2 .... p_k) = (p_1 p_2)(p_2 p_3)(p_3 p_4) \cdot ... \cdot (p_{k-1} p_k)$$

כלומר, כהרכבה של חילופים. נבחין כי מכפליות הסימן ומכך שסימן חילוף הוא שלילי נקבל כי: $sing(p_1 .... p_k) = (-1)^{k-1}$.

דוגמה 68. נתבונן במחזור הבא: $(4,2,6,3) \in S_6$. (וכן $1,5$ נשלחים לעצמם). נראה כי לפי הגדרה:

$$(4,2,6,3) = (4,2)(2,6)(6,3) = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 2 & 5 & 3 \end{array} \right)$$

כעת נרצה לחשב זאת.
נתחיל מ1. מהו החילוף ש3 עושה ל1? כלום. ומ$(6,3)$ מקבלים 1. וכן הלאה - כיוון ש1 לא מופיע במחזורים: מקבלים 1.
נעבור ל2. הוא עובר במחזור ראשון $(6,3)$ ולא קורה לו כלום. משם: מגיע ל$(2,6)$ ומוחלף ל6. לא מושפע מ$(4,2)$ וסה"כ מקבלים 6.
וכן הלאה.
נבחין, כי קיבלנו תמורה שפשוט שולחת את 4 ל2, את 2 ל6 וכן הלאה. נרצה להוכיח שזה מה שקורה באופן כללי:

משפט 69. יהי $f = (p_1....p_k)$ מחזור. אזי,

$$f(x) = \left\{ \begin{array}{cc} p_1 & x = p_k \\ p_i & x = p_{i-1} \forall i \geq 2 \\ x & o.w \end{array} \right\}$$

דוגמה 70. נתבונן בדוגמה הבאה:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}$$

נרצה לחשב את $sing(f)$ בקלות. ראשית, נפרק את התמורה להרכבה של מחזורים זרים. נבחין כי:

$$f = (1,3,4)(2,7,5,6)$$

מכאן, נבחין כי $sing(1,3,4) = sing((1,3)(3,4)) = (-1)^2 = 1$. וכן: $sing(2,7,5,6) = sing((2,7)(7,5)(5,6)) = (-1)^3 = -1$.
סה"כ מכפליות הסימן נקבל $sing(f) = 1 \cdot -1 = -1$.

2.6 הומומורפיזם ואיזומורפיזם

הגדרה 71. תהיינה שתי חבורות G, H ותהי פונקציה $f : G \to H$. נאמר כי f היא הומומרפיזם אם לכל $a, b \in G$ מתקיים:

$$f(a \cdot_G b) = f(a) \cdot_H f(b)$$

הגדרה 72. נאמר כי $f : G \to H$ פונקציה בין חבורות היא איזומורפיזם אם:
1. f היא הומומורפיזם.
2. f היא חח"ע ועל.

הערה 73. הומומורפיזם שומר במובן מסוים על מבנה החבורה ואיזומורפיזם מראה שהחבורות הן "אותה גברת בשינוי אדרת" - ועל כך נרחיב בהמשך במשפט קיילי.

משפט 74. אם $f : G \to H$ היא הומומורפיזם אזי $f(e_G) = e_H$
הוכחה: מתקיים $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot_H f(e_G)$. כעת, קיבלנו בפרט $f(e_G) = f(e_G) \cdot_H f(e_G)$ ומתכונת הצמצום נקבל $e_H = f(e_G)$.

■

משפט 75. יהי $f : G \to H$ הומומורפיזם. אזי, מתקיים $o(f(g)) \leq o(g)$ ואם f איזומורפיזם אזי יש שוויון. כמו כן מתקיים $o(f(g))|o(g)$.
הוכחה: נחלק למקרים.
מקרה ראשון: $o(g) = n$ סופי. אזי, $g^n = e_G$. מכאן: $f(g^n) = f(g \cdot g \cdot ... \cdot g) = (f(g))^n$. אבל גם $f(g^n) = f(e_G) = e_H$ וקיבלנו $(f(g))^n = e_H$ ולכן $o(f(g)) \leq n = o(g)$.
מקרה שני: $o(g)$ לא סופי. אזי בהכרח מתקיים $o(f(g)) \leq \infty$ באופן טריוואלי.
כעת, נניח כי f איזומורפיזם. כעת נטען כי $o(g) \leq o(f(g))$.
אם כן, נניח כי $o(f(g))$ סופי אחרת הטענה נכונה באופן טריוואלי. נסמן $o(f(g)) = k$. אזי, $(f(g))^k = e_H$. אם כן,

$$f(g)^k = f(g) \cdot .... \cdot f(g) = f(g^k) = e_H$$

כיוון שf היא איזומורפיזם, ואנו יודעים כי $f(e_G) = e_H$ וגם $f(g^k) = e_H$ אזי נקבל $e_G = g^k$ כלומר $o(g) \leq k = o(f(g)$.
סה"כ אכן אם f איזומורפיזם נקבל $o(g) = o(f(g))$ לכל $g \in G$.

■

משפט 76. יהי f הומומורפיזם, ויהי $a \in G$. אזי $f(a^{-1}) = (f(a))^{-1}$
הוכחה: נראה כי $f(a) \cdot_H f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$. ולכן, אם נכפיל ב$(f(a))^{-1}$ (שקיים, כי מדובר באיבר בחבורה שקיים לו הופכי) משמאל נקבל את הדרוש.

■

הערה 77. לא צריך במשפט הקודם לדרוש הפיכות (איזומורפיזם). בפרט, האיברים בתוך חבורה ולהם קיים הפיך. נבחין כי לא מתקיים $f^{-1}(a) = f(a^{-1})$ שכן $f(a^{-1}) \in H$ וכן $f^{-1} \in G$ וכלל זה לא מוגדר.

הגדרה 78. יהי $f : G \to H$ הומומורפיזם. נגדיר:
א. התמונה של f:

$$Im(f) = \{f(g)|g \in G\}$$

ב. הגרעין של f:

$$Ker(f) = \{g \in G|f(g) = e_H\}$$

הגדרה 79. יהי $f : G \to H$ הומומורפיזם. אזי f חח"ע אמ"מ $Ker(f) = \{e_G\}$.

משפט 80. יהי $f : G \to H$ הומומורפיזם. אזי, $Ker(f) \leq G$ ו$Im(f) \leq H$.
הוכחה:
יהי הי $f : G \to H$ הומומורפיזם.
ו. נוכיח כי $Ker(f) \leq G$:
ראשית, אכן לפי הגדרה מתקיימת ההכלה שהרי $Ker(f) = \{g \in G|f(g) = e_H\} \subseteq G$. כעת, נוכיח לפי הקריטריון המקוצר.
א. מתקיים $f(e_G) = e_H$ ולכן אכן $e_G \in Ker(f)$.
ב. יהיו $a, b \in Ker(f)$. נרצה להראות כי $ab^{-1} \in Ker(f)$. אם כן, מתקיים:

$$f(ab^{-1}) = f(a) \cdot_H f(b^{-1}) = f(a) \cdot_H (f(b))^{-1} =_{a \in Ker(f)} e_H \cdot_H (f(b)^{-1}$$

$$= (f(b))^{-1} =_{b \in Ker(f)} (e_H)^{-1} = e_H$$

לכן אכן $ab^{-1} \in Ker(f)$.
סה"כ לפי הקריטריון המקוצר $Ker(f)$ תת חבורה של G.
ז. נראה כי $Im(f) \leq H$.
ראשית, נבחין כי אכן ההכלה מתקיימת שהרי $Im(f) = \{f(g) \in H|g \in G\} \subseteq H$. כעת נוכיח לפי הקריטריון המקוצר.
א. מקיים $f(e_G) = e_H$ לכן $e_H \in Im(f)$.
ב. יהיו $a, b \in Im(f)$. $a \in Im(f)$ ולכן קיים $g_1 \in G$ כך ש$f(g_1) = a$. בדומה, קיים $g_2 \in G$ כך ש$f(g_2) = b$. מכאן: נרצה להראות כי $ab^{-1} \in Im(f)$. אנו יודעים כי מתקיים $f(x^{-1}) = (f(x))^{-1}$. בפרט עבור g_2 נקבל:

$$f(g_2^{-1}) = (f(g_2)^{-1} = (b)^{-1}$$

כלומר, המקור של b^{-1} תחת f הוא g_2^{-1} (שמוגדר כי G חבורה). מכאן, נראה כי:

$$f(g_1 g_2^{-1}) = f(g_1)f(g_2^{-1}) = ab^{-1}$$

מסגירות להופכי $g_2^{-1} \in G$ ומסגירות כחבורה מקבלים $g_1 g_2^{-1} \in G$. לכן נסמן $x = g_1 g_2^{-1}$ וקיבלנו כי x מקור של ab^{-1} כלומר אכן $ab^{-1} \in Im(f)$.
לכן סה"כ $Im(f)$ היא תת חבורה של H. כנדרש.

■

הערה 81. נסמן $A \cong B$ עבור איזומורפיזם בין קבוצות.

משפט 82. יהי $f : G \to H$ הומומורפיזם חח"ע. אזי $G \cong Im(f)$ (G איזומורפית לתמונה שהיא תת חבורה של H).
הוכחה: ההוכחה פשוטה, צריך לצמצם את H לתמונה שלה ונקבל פונקציה $f : G \to Im(f)$ שהיא גם חח"ע וגם על: ולכן איזומורפיזם.

הערה 83. תהי חבורה G ונביט בחבורת התמורות S_G. כלומר, כל הפונקציות ההפיכות מG לעצמה עם פעולת ההרכבה.

הגדרה 84. יהי $f : G \to H$ הומומורפיזם. אזי,
א. אם f חח"ע נאמר כי f מונומורמיזם או שיכון. במקרה זה נאמר כי G משוכנת בH אם קיים שיכון $f : G \to H$.
ב. אם f על נאמר כי f אפמיורפיזם. במקרה זה H היא תמונה אפימורפית של G.
ג. איזומורפיזם $f : G \to G$ נקרא גם אוטומורפיזם.

משפט 85. איזומורפיזם היא תכונה סימטרית, רפלקסיבית וטרנזטיבית.

משפט 86. כל חבורה ציקלית $(G =< a >)$ איזומורפית או ל$\mathbb{Z}_n$ או ל$\mathbb{Z}$.

משפט 87. ההעתקה $i : G \to G$ המוגדרת לפי: $i(g) = g^{-1}$ היא אוטומורפיזם (איזומורפיזם) רק אם G אבלית.
פתרון: בבירור כי i היא פונקציה הפיכה. נותר לבדוק מתי $i(gh) = i(g)i(h)$. אם כן:

$$i(gh) = (gh)^{-1} = h^{-1}g^{-1} = i(h)i(g) = i(hg)$$

כיוון שi חח"ע זה יקרה אמ"מ $gh = hg$ לכל $g, h \in G$. כלומר: אמ"מ G אבלית.

■

הגדרה 88. חבורת החילופין A_n מוגדרת באופן הבא:

$$A_n = \{\sigma \in S_n | sign(\sigma) = 1\}$$

ומתקיים $A_n \leq S_n$.
הוכחה: בבירור שיש הכלה. מכאן לפי הקריטריון המקוצר בקלות:
1. Id, תמורת הזהות אכן מקיימת כי $sign(Id) = 1$ לכן $Id \in A_n$.
2. יהיו ϕ, τ זוג תמורות בA_n. מכאן לפי כפליות הסימן: $sign(\phi\tau^{-1}) = sign(\phi)sign(\tau)^{-1} = 1 \cdot 1^{-1} = 1$.

הערה 89. **מטרתנו להמשך הדרך:** תהי G חבורה ותהי S_G חבורת התמורות. נבנה פונקציה $\phi : G \to S_G$ ששולחת כל איבר מG לתמורה כלשהי. ההומומורפיזם חח"ע יקרא שיכון כי הוא משכן את G בתוך הטווח כך שכל איבר מקבל מיקום פרטי. משם - נסיק את משפט קיילי שאומר שכל חבורה איזומורפית לתת חבורה של חבורת התמורות. כלומר: $G \cong Im(\phi)$. כלומר - כל חבורה בעולם היא תת חבורה של חבורת התמורות (בשינוי אדרת) וכל פעולה בעצם לבסוף היא הרכבה.

משפט 90. יהי $f : G \to H$ איזומורפיזם. אזי גם $f^{-1} : H \to G$ איזומורפיזם.

2.7 משפט קיילי

נרצה לבנות פונקצייה ϕ מחבורה G לS_G (חבורת כל הפונקציות ההפיכות מG לעצמה - חבורת התמורות). נרצה כי בהינתן איבר מG הפונקציה תחזיר תמורה, ושהפונקציה תהיה:
1. מוגדרת היטב.
2. הומומורפיזם.
3. חח"ע

אם נבנה כזו - נקבל את משפט קיילי: $G \cong Im(\phi)$ (כל חבורה איזומורפית לתמונה של הפונקציה - חבורת התמורות).

משפט 91. משפט קיילי: כל חבורה איזומורפית לתת חבורה של חבורת התמורות.

כעת נרצה להוכיח את משפט קיילי:

לכן, לכל איבר $a \in G$ נגדיר פונקציה f_a שמוגדרת ע"י:

$$f_a(g) = ag$$

כיוון ש$a, g \in G$ גם $ag \in G$ ולכן $f_a : G \to G$. כלומר הפונקציה מקבלת איבר g ומפעילה עליו את הפעולה של G עם a.

הפונקציה f_a אכן מוגדרת היטב. אך עלינו להראות כי $f_a \in S_G$. כלומר - שמדובר בפונקציה חח" ועל.
חח"ע: נניח $f_a(x_1) = f_a(x_2)$ אזי $ax_1 = ax_2$. ל$a \in G$ קיים הופכי a^{-1}. נכפיל משמאל ונקבל $x_1 = x_2$, חח"ע.
על: יהי $y \in G$. נבחין כי:

$$y = (aa^{-1})y = a(a^{-1}y) = f_a(a^{-1}y)$$

לכן מקור של $y \in G$ תחת f_a הוא $a^{-1}y \in G$ וסה"כ לכל y קיים מקור.

נגדיר את **שיכון קיילי** ע"י:

$$\phi(a) = f_a$$

כלומר - שולחים כל איבר לפונקציה ש"כופלת" באותו איבר.
כיוון ש$f_a \in S_G$ (פונקציה הפיכה מ$G \to G$ מוגדרת היטב) נקבל כי $\phi : G \to S_G$.

כעת נרצה להראות כי שיכון קיילי הוא הומומורפיזם. לשם כך: יהיו $a_1, a_2 \in G$:

$$\phi(a_1 \cdot_G a_2) = \phi(a_1) \circ \phi(a_2)$$

נרצה למעשה להוכיח כי: $f_{a_1a_2} = f_{a_1} \circ f_{a_2}$. כלומר - שוויון בין פונקציות. ראשית, נראה כי התחום והטווח אכן שווים וכעת נרצה להראות כי לכל איבר x הוא נשלח לאותו מקום. אם כן:

$$f_{a_1a_2}(x) = (a_1a_2)x$$

$$f_{a_1} \circ f_{a_2}(x) = f_{a_1}(a_2x) = (a_1)(a_2x) =_* (a_1a_2)x$$

שכן * נכון שכן מדובר בחבורה ויש אסוציאטיביות.

כעת - נותר להראות כי ϕ היא פונקציה חח"ע.
יהיו $a_1, a_2 \in G$ כך ש$\phi(a_1) = \phi(a_2)$. אזי, $f_{a_1} = f_{a_2}$. נרצה להוכיח כי $a_1 = a_2$. אנו יודעים כי לכל איבר $x \in G$, ובפרט עבור e_G נקבל כי:

$$f_{a_1}(e_G) = f_{a_2}(e_G) \Longrightarrow a_1e_G = a_2e_G \Longrightarrow a_1 = a_2$$

חח"ע.

סה"כ הראינו שמדובר בהומומורפיזם מוגדר היטב, חח"ע, ואם נצמצם את התחום ל$Im(\phi)$ נקבל כי אכן מדובר באיזומורפיזם: $G \cong Im(\phi)$.
כנדרש.

■

כעת, אם נחפש תת חבורה של תמורות שהיא איזומורפית לחבורה G - נקח את התמונה של שיכון קיילי.

משפט 92. כל חבורה סופית מגודל n איזומורפית לתת חבורה של S_n.

2.8 משפט לגראנז'

הגדרה 93. תהי חבורה G, ותהי תת חבורה $H \subseteq G$.
לכל איבר $a \in G$ נגדיר את המחלקה

$$aH = \{ah | h \in H\}$$

לדוגמה:
עבור חבורת התמורות S_3 ניתן להגדיר את תת החבורה :

$$H = \{I, (1,3)\}$$

למשל, עבור התמורה $(1,2) \in S_3$ נקבל:

$$(1,2)H = \{(1,2), (1,2)(1,3)\} = \{(1,2), (2,1)(1,3)\} = \{(1,2), (2,1,3)\}$$

משפט 94. גודל כל המחלקות מהצורה aH יהיה $|H|$. כלומר לכל $a \in G$ מתקיים $|aH| = |H|$.

מסקנה 95. ממשפט לגראנז': כיוון שהגודל של כל תת חבורה צריך לחלק את גודל החבורה, כלומר $|H| \mid |G|$, אזי אם $|G| = p$ עבור p ראשוני, אזי בהכרח לG ישנן תתי חבורות מגודל 1 ו$|G|$ בלבד. כלומר זוג חבורות: החבורה הטריוואלית $\{e_G\}$ וG.

משפט 96. תהי חבורה G ותת חבורה שלה H. נגדיר יחס שקילות R על G ע"י:
לכל $g_1, g_2 \in G$ נגדיר: $g_1 R g_2 \iff g_1^{-1} g_2 \in H$ (כלומר, זוג נמצא ביחס אמ"מ ה"הפרש" $(g_1 g_2^{-1})$ בניהם נמצא באותה תת חבורה).
אזי:
1. R יחס שקילות
2. לכל איבר $a \in G$ מתקיים $[a]_R = aH$
3. לכל $a \in G$ מתקיים $|aH| = |H|$.

הוכחה:
1. נוכיח שאכן מדובר ביחס שקילות.
רפלקסיביות - יהי $g_1 \in G$. אזי, נראה כי $g_1^{-1} g_1 = e_G \in H$ מהגדרת תת חבורה תמיד $e_G \in H$ ולכן $g_1 R g_1$.
סימטריות - נניח $g_1 R g_2$. אזי, $g_1^{-1} g_2 \in H$. נרצה להראות כי $g_2^{-1} g_1 \in H$. אם כן, כיוון ש$(g_1^{-1} g_2) \in H$, גם $(g_1^{-1} g_2)^{-1} \in H$ והרי $(g_1^{-1} g_2)^{-1} = g_2^{-1} g_1$ ולכן סה"כ הראינו $g_2^{-1} g_1 \in H$ ולכן $g_2 R g_1$
טרנזטיביות - נניח $g_1 R g_2$ וגם $g_2 R g_3$. אזי, $g_1^{-1} g_2 \in H$ וגם $g_2^{-1} g_3 \in H$. כיוון שH תת חבורה ישנה סגירות ולכן $(g_1^{-1} g_2)(g_2^{-1} g_3) = g_1^{-1}(g_2^{-1} g_2) g_3 = g_1^{-1} e_G g_3 = g_1^{-1} g_3 \in H$ שכן יש אסוציאטיביות בחבורה ובתת חבורה בפרט. סה"כ קיבלנו $g_1 R g_3$.
2. כעת יהי $a \in G$. נרצה להראות כי $[a]_R = aH$. יש לנו כאן שוויון בין קבוצות לכן נבצע הכלה דו כיוונית:
$\subseteq$ יהי $x \in [a]_R$. אזי, aRx, כלומר $a^{-1}x \in H$. כלומר, קיים $h \in H$ כך ש: $a^{-1}x = h$. כעת, נכפיל בa משמאל ונקבל $aa^{-1}x = ah$ כלומר $x = ah$ ולכן $x \in aH$.
$\supseteq$ בכיוון השני, יהי $x \in aH$. אזי קיים $h \in H$ כך ש$x = ah$. נכפול בa^{-1} מימין ונקבל $a^{-1}x = h$, כלומר $a^{-1}x \in H$ כלומר aRx, כלומר $x \in [a]_R$.
3. נרצה להראות עבור $a \in G$ כי $|aH| = |H|$. לכן נבנה פונקציה חח"ע ועל בין שתי הקבוצות. נגדיר $f : H \to aH$ ע"י:

$$f(h) = ah$$

בבירור מוגדרת היטב. כעת נוכיח שחח"ע ועל:
חח"ע: יהיו $h_1, h_2 \in H$, כך ש$f(h_1) = f(h_2)$. אזי $ah_1 = ah_2$. נכפול בa^{-1} משמאל (בחבורה) ונקבל $h_1 = h_2$
על: יהי $x \in aH$. אזי קיים $h \in H$ עבורו $x = ah$. נראה כי $f(h) = ah$ ולכן h מקור לx.
סה"כ נקבל כי $|aH| = |H|$.

■

הגדרה 97. נסמן $[G : H]$ כאינדקס של תת החבורה. ערך זה מוגדר להיות כמות המחלקות השונות שH מגדירה.

משפט 98. משפט לגראנז': עבור חבורה סופית G, ותת חבורה שלה (בהכרח סופית גם היא) H מתקיים:

$$|G| = |H| \cdot [G : H]$$

כלומר: גודל כל חבורה הוא גודל תת חבורה שלה, כפול מס' המחלקות שאותה תת חבורה מגדירה.
מכאן נסיק: הגודל של כל תת חבורה, בהכרח מחלק את גודל החבורה.
הוכחה: כפי שראינו בבדידה, יחס שקילות על קבוצה G מחלק אותה לחלוקה. קבוצות זרות שאיחודן הוא כל G. וכן ראינו כי $[a]_R = aH$ (ולכן כל איבר בG נמצא באחת מהקבוצות aH) כיוון שהראינו כי $|aH| = |H|$, וכן $[G : H]$ הוא מס' המחלקות שH מגדירה, נקבל כי:
G היא קבוצה שמחולקת ל$[G : H]$ חתיכות - גודל כל חתיכה הוא $|H|$ ולכן סה"כ $|G| = |H| \cdot [G : H]$.

■

99. aÿòà¨ כיוון שתת החבורות הציקליות הן תת חבורה, וכן מתקיים $|< a >| = o(a)$, כמסקנה ממשפט לגראנז' הסדר של כל איבר מקיים $o(a) \mid |G|$. (בחבורה סופית!).

100 èôùî. תהי G סופית, אזי G מסדר זוגי אמ"מ קיים בה איבר מסדר 2.

משפט 101. איבר מסדר 2 הוא הופכי לעצמו.

משפט 102. לחבורה מסדר זוגי יש מס' אי זוגי של איברים מסדר 2. (שכן איבר היחידה מסדר אחד).

2.9 חבורת אוילר

הגדרה 103. יהי $n \in \mathbb{N}$. נגדיר יחס שקילות 'מודלו n' על $\mathbb{Z}$ כך:

$$a \equiv_n b \Longleftrightarrow \exists k \in \mathbb{Z} : a = b + kn$$

הגדרה 104. יהי $n \in \mathbb{N}$ ויהיו $a, b \in \mathbb{Z}$ ונסמן את השאריות שלהם בחלוקה בn r_a, r_b. אזי: $ab \equiv_n r_a r_b$. באופן כללי: $(a)^k \equiv_n (r_a)^k$.
הוכחה: מתקיים כי $a = q_a n + r_a, b = q_b n + r_b$. נקבל כי:

$$ab = (q_a n + r_a)(q_b n + r_b) = q_a q_b n^2 + r_b q_a n + r_a q_b n + r_a r_b = n(q_a q_b + r_b q_a + r_a q_b) + r_a r_b \equiv_n r_a r_b$$

■

הגדרה 105. המחלק המשותף הגדול ביותר (gcd): יהיו $n, k \in \mathbb{N}$. נגדיר את: $gcd(n, k)$ להיות המספר הטבעי הגדול ביותר שמחלק גם את n וגם את k.

נבחין כי $gcd(n, k) \geq 1$ שכן 1 מחלק את שניהם. כמו כן, מס' המחלקים תמיד חסום בn, k ולכן גודל הקבוצה סופית. נבחין כי חישוב בצורה הנאיבית:

$$gcd(n, k) \Longrightarrow O(min\{n, k\})$$

אך ניתן לחשב אותו גם ב$O(log(min\{n, k\}))$. ולמה אנחנו מציינים זאת? כי אנחנו שואפים להגיע לדבר על הצפנה - נרצה למצוא אלגוריתמים יעילים.

משפט 106. יהיו $n > k \in \mathbb{N}$ אזי:

$$gcd(n, k) = gcd(n - k, k)$$

הוכחה: נוכיח טענה יותר חזקה. נוכיח כי קבוצת המחלקים המשותפים של $\{n, k\}$ ושל $\{n - k, k\}$ הם בדיוק אותם מחלקים - ואז בבירור המקסימלי משתי הקבוצות זהה. נראה זאת בהכלה דו כיוונית:
בכיוון ראשון, נניח כי $x|n, k$ אזי $n = q_1 x, k = q_2 x$. ולכן $n - k = (q_1 - q_2)x$ ולכן $x|n - k$, וכן $x|k$ ולכן x הוא בקבוצת המחלקים המשותפים של $n - k, k$.
בכיוון שני, נניח כי $x|n - k, k$. אזי $n - k = q_1 x, k = q_2 x$. נציב זאת ונקבל $n = q_1 x + k = q_1 x + q_2 x = (q_1 + q_2)x$ ולכן $x|n$ וכן $x|k$ וסה"כ x בקבוצת המחלקים המשותפים של n, k. ■

אלגוריתם אוקלידס: האלגוריתם נועד לחישוב הgcd באופן יעיל. בכל שלב מבצעים חלוקה עם שארית של האיבר n עם האיבר k שקטן ממנו ונעזרים בטענה הקודמת. לדוגמה:

$$gcd(15, 6) = gcd(15 - 6, 6) = gcd(9, 6) = gcd(9 - 6, 6) = gcd(3, 6) = gcd(3, 6 - 3) = gcd(3, 3) = 3$$

זמן הריצה של אלגוריתם אוקלידס הוא $O(log(min\{n, k\}))$.

משפט 107. לכל $n \in \mathbb{N}$ מתקיים $gcd(n, n) = n$.

כעת נשאל את עצמנו שאלה. יהי $\mathbb{Z}_{11}$ שדה. מיהו 7^{-1}? (ביחס לכפל). באופן הגרוע ניתן לעבור על כל האפשרויות. אנחנו כעת נוכיח שישנה דרך למצוא את האיבר הנ"ל בזמן לוגריתמי.

משפט 108. יהיו $n, k \in \mathbb{N}$. אזי קיימים $a, b \in \mathbb{Z}$ כך ש:

$$gcd(n, k) = an + bk$$

הוכחה: באינדוקציה על $n + k$.

בסיס: $n+k=2$ כלומר $n=k=1$. מכאן, $gcd(1,1)=1$. לכן נקח $a=1, b=0$.
צעד: יהי m עבורו עד אליו הטענה נכונה. נוכיח עבור $k+n=m$. אם כן אם $n=k$ זה בדיוק כמו קודם. אחרת,

$$gcd(n,k)=gcd(n-k,k)$$

אנו יודעים כעת כי $n-k+k=n<n+k=m$ ולכן עבורו נכונה טענת האינדוקציה. כלומר קיימים:

$$gcd(n,k)=gcd(n-k,k)=a(n-k)+bk=an-ak+bk=an+(b-a)k=an+b'k$$

כנדרש. ■

כעת נחזור לשאלה הקודמת. הרי ש$gcd(7,11)=1$. מהטענה הקודמת קיימים וניתן למצוא אותם:

$$gcd(7,11)=1=(-3)\cdot 7+2\cdot 11$$

ולכן, $-3\equiv_{11} 8$ הוא ההופכי של 7. מדוע? נפעיל על המשוואה הקודמת מודלו 11. הרי ש$-3\cdot 7\equiv_{11} 1$. כעת, אכן קיבלנו את הדרוש.

הגדרה 109. כאשר $(n,m)=1$ נאמר כי n,m זרים.

משפט 110. אם $n=qm+r$ אזי $(n,m)=(m,r)$

משפט 111. יהיו $a,b,c\in\mathbb{Z}$ כך ש$(a,b)=1$ וגם $a|bc$. אזי $a|c$
הוכחה: אנו יודעים כי $bc=na$ עבור n שלם כלשהו. בפרט, אנו יודעים שקיימים s,t כך ש: $1=sa+tb$. נכפיל בc משני הצדדים ונקבל $c=sac+tbc$. בנוסף, $c=sac+tna$ ומכאן: $c=a(sc+tn)$ כלומר $a|c$. ■

112 èôùî. מתקיים:
1. עבור $d=(n,m)$ וe כך ש$e|m\wedge e|n$ אזי $e|d$.
2. $(an,am)=|a|(n,m)$ לכל $a\neq 0$.

2.9.1 אלגוריתם אוקלידס

אלגוריתם לחישוב gcd ומציאת a,b כנ"ל. נתבונן בדוגמה:

$$gcd(49,14)=gcd(49-3\cdot 14,14)=gcd(\mathbf{7},14)=gcd(7,\mathbf{7})=7=1\cdot 7+0\cdot 7$$

כעת נרצה למצוא את a,b הנ"ל. כיצד? הולכים לשוויון האחרון, וכל פעם מחליפים את המספר החדש באיך שהגענו אליו ואז מסדרים את הביטוי כצירוף של שני המספרים הקודמים, והרי:

$$gcd(49,14)=1\cdot 7+0\cdot 7=1\cdot 7+(14-7)\cdot 0=1\cdot 7+14\cdot 0+(-7)\cdot 0=1\cdot 7+0\cdot 14=$$

$$1\cdot(49-3\cdot 14)+0\cdot 14=1\cdot 49-3\cdot 14+0\cdot 14=1\cdot 49-3\cdot 14$$

ולכן קיבלנו כי $a=1$ וכן $b=-3$. כלומר, $gcd(49,14)=7=1\cdot 49-3\cdot 14$
דוגמה נוספת:

$$(234,61)=_{3\times 61+51}(61,51)=_{61=51+10}(10,51)=_{51=10\times 5+1}(10,1)=1$$

$$51=234-3\times 61$$

$$10 = 61 - 51 = 61 - (234 - 3 \times 61)$$

$$1 = 51 - 5 \cdot 10 = 51 - 5 \times (61 - (234 - 3 \times 61))$$

$$1 = gcd(234, 61) = 51 - 5(-234 + 4 \cdot 61) = 5 \cdot 234 - 20 \times 61 + 51$$

$$= 5 \cdot 234 - 20 \times 61 + 234 - 3 \times 61 = 6 \cdot 234 - 23 \times 61$$

2.9.2 lcm

הגדרה 113. בהינתן שני מספרים שלמים n, m נסמן את הכפולה המזערית המשותפת שלהם להיות:

$$lcm(n, m) = min\{d \in \mathbb{N} \text{ s.t } n|d \wedge m|d\}$$

לעיתים נסמן $[n, m]$. לדוגמה: $[6, 10] = 30$

משפט 114. אם $m|a$ וכן $n|a$ אזי $[n, m]|a$
הוכחה: יהיו q, r כך ש: $a = q[n, m] + r$ כך ש$0 \leq r < [n, m]$. מהנתון $n, m|a$ ולכן בפרט מחלקים את $n, m|[n, m]$ (שהרי a מחלק את n ואת m). מכאן $n, m|r$ (שכן מחלקים את a ואת $[n, m]$ ומכאן שבהכרח גם את r). אם $r \neq 0$ זו סתירה לכך ש$[n, m]$ מינימלי כי גם $r = 0$ כעת מחלק את n, m ובפרט את nm ולכן $a = q[n, m]$ כלומר $[n, m]|a$.

משפט 115. מתקיים: $[n, m] \cdot (n, m) = |nm|$
הוכחה: נסמן את הפירוק של $|n|, |m|$ למכפלת גורמים ראשוניים כך:

$$|n| = \prod_{i=1}^{k} p_i^{\beta_i}, |m| = \prod_{i=1}^{k} p_i^{\alpha_i}$$

באשר p_i ראשוניים וכן $\alpha_i, \beta_i \geq 0$. מכאן בבירור כי:

$$(n, m) = \prod_{i=1}^{k} p_i^{min\{\alpha_i, \beta_i\}}, [n, m] = \prod_{i=1}^{k} p_i^{max\{\alpha_i, \beta_i\}}$$

והרי נקבל כי:

$$[n, m](n, m) = \prod_{i=1}^{k} p_i^{min\{\alpha_i, \beta_i\}} \cdot \prod_{i=1}^{k} p_i^{max\{\alpha_i, \beta_i\}} = \prod_{i=1}^{k} p_i^{\alpha_i + \beta_i} = |nm|$$

משפט 116. תהי G חבורה. יהי $a \in G$ איבר מסדר סופי n. אזי לכל d שלם:

$$o(a^d) = \frac{n}{(d, n)} = \frac{o(a)}{(d, o(a))}$$

הוכחה: ראשית נוכיח שאכן יתכן שזה יהיה שווה לסדר. והרי ש:

$$(a^d)^{\frac{n}{(d,n)}} = (a^n)^{\frac{d}{(d,n)}} = e$$

שכן $o(a) = n$ ולכן $a^n = e$. כעת, נוכיח את המינימליות של הסדר. נניח $(a^d)^t = e$ עבור $t \in \mathbb{N}$. לכן $a^{dt} = e$. בפרט $n|dt$. לכן, $\frac{n}{(d,n)}|\frac{dt}{(d,n)}$. מצד שני,

$$gcd(\frac{n}{(d,n)}, \frac{d}{(d,n)}) = 1$$

שכן לפי הטענה $(am, am) = |a|(n,m)$ נקח $a = (d,n)^{-1}$ ונקבל ששווה ל$|(d,n)^{-1}| \cdot (d,n) = 1$.
קודם ראינו כי אם ישנם שלושה מס' כך ש$(a,b) = 1$ וגם $a|bc$ אזי $a|c$. אצלנו $a = \frac{n}{(d,n)}, b = \frac{d}{(d,n)}$ וכן $c = t$. לכן נקבל כי $\frac{n}{(d,n)}|t$ ובפרט t לא מינימלי. לכן אכן זהו הסדר. ■

משפט 117. מתקיים כי $gcd(n,k)|n,k$ (לפי הגדרה).

הגדרה 118. יהי $n \geq 1$ טבעי. נגדיר את חבורת אוילר U_n להיות אוסף כל המספרים ב$\mathbb{Z}_n$ ההפיכים יחד עם פעולת הכפל.

משפט 119. יהי $n \geq 1$, אזי המספרים ההפיכים ב$\mathbb{Z}_n$ הם בדיוק המספרים עד n שזרים ל$-n$. כלומר:

$$U_n = \{k | 1 \leq k \leq n-1 \wedge gcd(n,k) = 1\}$$

בפרט עבור n ראשוני נקבל $U_n = \mathbb{Z}_n$

מסקנה 120. המשפט הקטן של פרמה: אם p ראשוני ו$1 \leq a \leq p-1$ אזי $a^{p-1} \equiv_p 1$
הוכחה: הרי שהעלינו איבר בגודל החבורה שלו, שכן מדובר ב$a \in U_n$ שזו חבורה המקיימת $|U_n| = p-1$ ותמיד מתקיים $a^{|G|} = e_G$.

הגדרה 121. יהי $n \geq 1$. מגדירים את מס' אוילר להיות:

$$\varphi(n) = |U_n|$$

כלומר כמות המספרים עד n שזרים לn.

משפט 122. משפט אוילר: יהי n טבעי, ויהי $1 \leq a \leq n-1$. אזי,

$$a^{\varphi(n)} \equiv_n 1$$

הוכחה: שכן שוב, מדובר באיבר בחזקת גודל החבורה (וזה שווה לאיבר היחידה).

משפט 123. יהי $a \in U_n$. אזי, $o(a)|\varphi(n)$.

משפט 124. עבור כל p ראשוני מתקיים $\varphi(p) = p-1$ (שהרי $U_p = \{1, 2, ..., p-1\}$. לא זר לעצמו).

משפט 125. יהי $m \in \mathbb{Z}$. אזי $m \in U_n$ אמ"מ $gcd(n,m) = 1$.

2.10 חישוב פונקציית אוילר

נתחיל מדוגמה. הרי ש

$$U_{10} = \{1, 3, 7, 9\} \Longrightarrow |U_{10}| = 4 \Longrightarrow \varphi(10) = 4$$

לפי משפט אוילר גם מתקיים כי:

$$a^{\varphi(n)} \equiv_n 1 \Longrightarrow \text{for example: } 3^4 \equiv_{10} 81 \equiv_{10} 1$$

משפט 126. לפי המשפט היסודי של האריתמטיקה, כל מספר שלם ניתן לפירוק חזקות של מספרים ראשוניים עד כדי סדר וסימן. נסמן $n = \prod_{i=1}^{m} p_i^{k_i}$. אזי,

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot ..... \cdot (1 - \frac{1}{p_m})$$

דוגמה. למשל:

$$\varphi(60) = \varphi(2^2 \times 3 \times 5) = 60 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{5}) = 16$$

דוגמה לתרגיל חשוב: חשב את $(118^{287}) mod 95$
נרצה לפרק את 95 לראשוניים. אם כן,

$$95 = 19 \times 5$$

$$\varphi(95) = 95 \cdot (1 - \frac{1}{19}) \cdot (1 - \frac{1}{5}) = 95 \cdot \frac{18}{19} \cdot \frac{4}{5} = 5 \times 19 \times \frac{18}{19} \cdot \frac{4}{5} = 72$$

כעת,

$$118^{287} = 118^{288-1} = 118^{4 \cdot 72} \cdot 118^{-1} = (118^{\varphi(95)})^4 \cdot 118^{-1}$$

כעת, $118 mod 95 = 23$. 23 ראשוני ולכן $23 \in U_{95}$. נקבל -

$$\equiv (23^{\varphi(95)})^4 \cdot 23^{-1} \equiv 1 \cdot 23^{-1} = 23^{-1}$$

כעת על מנת לחשב את 23^{-1} אנחנו נחפש את $gcd(23, 95)$. הרי ש23 ראשוני וזר ל95 ולכן $gcd(23, 95) = 1$. מכאן, נפעיל את האלגוריתם ונמצא מקדמים:

$$gcd(23, 95) =_{95=23\cdot 4+3} (23, 3) =_{23=3\cdot 7+2} (2, 3) =_{3=2\cdot 1+1} = (2, 1) = 1$$

$$1 = 3 - 2 \cdot 1 \Longrightarrow 3 - (23 - 3 \cdot 7) = 3 - 23 + 3 \cdot 7 = 3 \cdot 8 - 23 \Longrightarrow$$

$$(95 - 23 \cdot 4) \cdot 8 - 23 = 95 \cdot 8 - 32 \cdot 23 - 23 = 8 \cdot 95 - 33 \cdot 23$$

$$1 = gcd(23, 95) = 8 \cdot 95 - 33 \cdot 23$$

לכן, אם נפעיל מודלו 95 על המשוואה נקבל:

$$1 \equiv -33 \cdot 23$$

כלומר, $23^{-1} = -33 = -33 + 95 = 62$. כלומר סה"כ קיבלנו כי:

$$(118^{287}) mod 95 = 62$$

3 הצפנה

מה זה הצפנה? הסתרת מידע, להבטיח את זהות המחבר ושלמות המידע, להסתיר מידע על המידע. ישנם שני סוגים של הצפנה:

1. הצפנה סימטרית - שני הצדדים מתאמים סוד ביניהם במקום בו אף אחד לא מאזין וכך הם מצפינים את המידע ביניהם.
2. הצפנה פומבית - שני הצדדים מתאמים סוד מול כולם ומצפינים את המידע. בעזרת הצפנה פומבית מתאמים סוד להצפנה סימטרית.

נלמד על אלגוריתם ההצפנה RSA. **נתאר את האלגוריתם:**

ישנם שני אנשים, אליס ובוב - הם רוצים להעביר מידע אחד לשני מבלי שאף אחד יכול לקרוא אותו ונניח כי הם לא גרים ביחד ויכולים לתאם מפתח. אליס רוצה לשלוח מידע לבוב, לכן בוב צריך להכין מנעול עם קפיץ (מי שיכול לפתוח מנעול עם קפיץ - הוא רק מי שמחזיק במפתח. אנשים אחרים - יכולים רק לנעול את המנעול).

1. אליס בוחרת שני מספרים ראשוניים גדולים (נניח 2^{1024}). נסמן אותם בp, q.
2. אליס מחשבת את $n = p \cdot q$ ואת $m = (p-1)(q-1)$.
3. כעת אליס בוחרת מספר e זר לm ($gcd(e, m) = 1$).
4. המנעול קפיץ (מפתח פומבי) של אליס הוא הזוג (n, e) - אליס מפרסמת זאת באופן חופשי.
5. בוב נועל את המידע שלו, שהוא מספר $1 < x < n$ באופן הבא:

$$x^e mod n$$

כלומר המידע הנעול הוא שארית החלוקה בn של x^e.

6. מה המפתח של אליס? אליס מחשבת את ההופכי של e מודלו m (נבחין כי ההופכי הנ"ל קיים כי הם זרים - ורק אליס יודעת עליו). נסמן את ההופכי הנ"ל בd.
7. אליס לוקחת את המידע המוצפן $y = x^e mod n$ שחישב בוב. אליס מחשבת את:

$$x = y^d mod n$$

(נבחין כי רק אליס יודע את d)
ואליס הצליחה להשיג את המידע.

ישנם כמה שאלות שעולות בדרך -

- איך מוצאים מספרים ראשוניים גדולים? בהמשך נלמד.
- איך מכפילים ראשוניים גדולים? בזמן לוגריתמי.
- מה הבעיה פשוט לפרק את n ולקבל את כל המידע של בנץ? הסיבוכיות של כך היא $O(\sqrt{n})$ - כיוון שn מאוד גדול, זה ענק. (אם $n = 1024$ זה בערך $1024^{\frac{1}{2}} = 2^{512}$ - לא משהו ישים!)
- נבחין כי אם נדע לפרק את m - נמצא את n, אבל לא יודעים לעשות זאת היום בסיבוכיות טובה.
- לכולם יש את x^e והם רוצים להשיג את x עצמו. אבל זה בחבורה $\mathbb{Z}_n$. זה נקרא להוציא שורש דיסקרטי. בבירור אם יצליחו - RSA נשבר. אבל גם את זה לא הצליחו לפתור.
- שלב 6 - כיצד מחשבים את ההופכי של מס' מסויים? באמצעות אוקלידס המורחב.

משפט 127. יהיו p, q זוג ראשוניים. אזי $\varphi(pq) = (p-1)(q-1)$

הוכחה: הרי ש$\varphi(pq) = |U_{pq}|$. נסמן $n = pq$. כמות המספרים בין 1 לn היא סה"כ n. נוריד ממנה את כל המספרים שלא זרים לpq ונקבל את הערך שרצינו.

נבחין כי מספר לא זר לpq אמ"מ יש להם מחלק משותף , כלומר אמ"מ הוא מתחלק בp או q. אזי נמצא את כל המספרים שמתחלקים בp ושמתחלקים בq ללא חזרות ונסכום אותם.

אם כן, אלו שמתחלקים בp:

$$p, 2p, 3p, ..., qp = n$$

באופן דומה, המספרים שמתחלקים בq:

$$q, 2q, ..., qp = n$$

נבחין כי ישנם $p+q$ מספרים שמצאנו. אך אולי חלקם חוזרים על עצמם? כבר pq חוזר על עצמו. מי יכול לחזור על עצמו? מספר שמתחלק גם בp וגם בq - מספר זה לפחות n (שוב כי הכל ראשוני) ולכן n הוא היחיד שחוזר על עצמו. לכן מס' המספרים הוא $(p+q-1)$. מכאן:

$$\varphi(pq) = n - (p+q-1) = pq - (p+q-1) = (q-1)(p-1)$$

משפט 128. (משפט הוכחת נכונות RSA). יהיו p,q ראשוניים. נסמן $n=pq$ וכן $m=(p-1)(q-1)$. ויהי e כך ש$gcd(m,e)=1$. יהי d ההופכי של e בU_m (קיים כזה כי הם זרים והפיך אמ"מ זרים). ויהי $1 \le x < n$ ונסמן $y = x^e \in \mathbb{Z}_n$. אזי,

$$x \equiv_n y^d$$

הוכחה: נחלק לשני מקרים.
1. $gcd(n,x)=1$ - כלומר x וn זרים. אזי $x \in U_n$. ידוע כי $d = e^{-1} \in U_m$ לכן $de \equiv_m 1$. כלומר המספרים שווים מודלו m. ולכן,

$$de = 1 + km$$

עבור k כלשהו. כעת,

$$y^d \equiv_n (x^e)^d \equiv_n x^{ed} = x^{1+km} = x \cdot x^{km} = x \cdot x^{k\cdot(p-1)(q-1)} = x \cdot x^{k\cdot\varphi(n)} = x \cdot (x^{\varphi(n)})^k \equiv_{x\in U_n \Longrightarrow x^{\varphi(n)}=1} x \cdot (1)^k \equiv_n x$$

כלומר הוכחנו כי $y^d \equiv_n x$.
2. $gcd(n,x) > 1$: כלומר x וn אינם זרים. אנו יודעים כי $x < n = pq$ ולכן $gcd(n,x) = p \vee gcd(n,x) = q$
בה"כ $gcd(x,n) = p$. כלומר, $x = tp$ עבור t קבוע. כיוון ש$x < n$ ברור כי $gcd(x,q) = 1$. אחרת x מתחלק בq ולכן x מתחלק גם בp וגם בq כלומר בn בסתירה.
נסמן $ed = 1 + km$, לפי המשפט הקטן של פרמה,

$$x^{q-1} \equiv_q 1 \Longrightarrow x^{k(p-1)(q-1)} \equiv_q 1 \Longrightarrow x^{k\varphi(n)} \equiv_q 1 \Longrightarrow x^{km} \equiv_q 1$$

בעצם הראינו כי $x^{km} = 1 + hq$. (שווה ממש). כעת,

$$x^{ed} = x^{1+km} = x \cdot x^{km} = x(1+hq) = x + qhx = x + qhtp = x + n \cdot ht \equiv_n 1$$

לכן $x^{ed} \equiv_n 1$. והרי $y^d = (x^e)^d \equiv_n 1$ ולכן סיימנו.

דוגמה 129. דוגמה לRSA חישובית:
אליס מגרילה זוג מספרים. $p = 61$ ו$q = 53$.
בשלב ראשון - היא מחשבת $n = pq = 3233$ ואת $m = \varphi(n) = (p-1)(q-1) = 3120$.
בשלב שני - אליס בוחרת $e = 17$. מנעול הקפיץ שהיא מפרסמת של אליס הוא $(3233, 17)$ - כולם יודעים זאת. נבחין כי e הוא זר ל$m = 3120$. שכן:

$$(3120, 17) =_{3120=183\cdot17+9} (9, 17) =_{17=1\cdot9+8} (9, 8) =_{9=1\cdot8+1} (1, 8) = 1$$

בשלב השלישי - אליס צריכה לחשב את ההופכי של e מודולו m. לכן היא משתמשת באוקלידס המורחב:

$$1 = 9 - 1\cdot 8 = 9 - 1\cdot(17-9) = 9 - 17 + 9 = 2\cdot 9 - 17 = 2\cdot(3120 - 183\cdot 17) - 17 = 2\cdot 3120 - 367\cdot 17$$

לכן

$$1 = 2\cdot 3120 - 367\cdot 17 \equiv_{3120} -367\cdot 17$$

$$\Longrightarrow d = -367 \equiv_{3120} 2753$$

בשלב הרביעי - נניח ובוב רוצה לשלוח לאליס את ההודעה $x = 65$. (נבחין שמתקיים $1 < x < n$). אזי הוא מחשב

$$y = x^e mod n = 65^{17} \equiv_{3233} 2790$$

זו הייתה נעילת המידע שלו, והוא שולח לאליס את 2790.
בשלב האחרון - אליס רוצה לדעת את ההודעה של בוב. לכן היא מחשבת (רק היא יכולה כי d בידה):

$$x = y^d (mod n) = 2790^{2753} \equiv_{3233} 65$$

ואכן קיבלה את ההודעה.

3.1 דיפי הלמן

הגדרה 130. בעיית הלוגריתם הבדיד. תהי G חבורה, יהי $g \in G$ ונניח $h = g^x$. המשימה היא למצוא את x בהינתן h. מסמנים את הפתרון ב$log_g h$. מסתבר, כי קשה מאוד למצוא את x הנ"ל בסיבוכיות פולינומית.

דוגמה 131. (**דוגמת תקיפה ללוגריתם הבדיד**). נתון כי 101 ראשוני ונתבונן ב$G = U_{101}$. נתון כי 7 יוצר של G. נרצה למצוא x כך שמתקיים:

$$h = 88 = 7^x (mod 101)$$

נבחין כי: $n = o(7) = |G| = |U_{101}| = \varphi(101) = 101 - 1 = 100$.
ראשית **באופן כללי** נבחין כי אם נסמן $m = \sqrt{n}$ אזי כל x בטווח $[0, n-1]$ ניתן לכתיבה בצורה $x = im + j$. כך ש$0 \le i, j < m$. אם נציב במשוואה נקבל

$$g^{im+j} = h \Longrightarrow g^j = h \cdot (g^{-m})^i$$

כעת במקום למצוא את x, נחפש התאמה בין הצדדים ימין ושמאל.
האלגוריתם עובד באופן הבא -
א. נחשב ונאחסן בטבלה את כל הערכים $g^j (mod p)$ לכל $0 \le j < m$. המפתח בטבלה הוא התוצאה והערך הוא j.
ב. מחשבים את g^{-m} באמצעות אוקלידס המורחב.
ג. רצים עם משתנה i מ0 עד m. בכל שלב בודקים את הערך $h \cdot (g^{-m})^i$. בודקים: האם הערך הזה נמצא בטבלה שחישבנו קודם? אם כן - מצאנו התאמה! הפתרון הוא $x = im + j$.

נבחין: אנחנו מבצעים m פעולות בבניית הטבלה, וm פעולות חיפוש בטבלה. סה"כ $O(m) = O(\sqrt{n})$. זה יעיל מאוד!

דוגמה 132. שלב 1: נסמן $m = \lceil \sqrt{100} \rceil = 10$ ונחשב את כל החזקות $7^j \mod 101$ עבור $0 \le j < m$. נקבל:

j	0	1	2	3	4	5	6	7	8	9
7^j	1	7	49	40	78	41	85	90	24	67

שלב 2: כעת נרצה לחשב את $7^{-1} (mod 101)$ באמצעות אוקלידס המורחב.

$$(7, 101) =_{101=14 \cdot 7+3} (7, 3) =_{7=2 \cdot 3+1} (1, 3) = 1$$

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (101 - 14 \cdot 7) = 29 \cdot 7 - 2 \cdot 101 \equiv_{101} 29 \cdot 7 \Longrightarrow 7^{-1} \equiv_{101} 29$$

כעת מתקיים:

$$g^{-m} = 7^{-10} = (7^{-1})^{10} = 29^{10} \equiv 14(mod 101)$$

שלב 3: נאתחל $\alpha = 88$. נרצה לעבור על כל $h \cdot (g^{-m})^i$. הרי שg^{-m} זה 14 לכן נחפש $88 \cdot 14^i$.
עבור $i = 0$, לא מקבלים בטבלה דבר. עבור $i = 1$ מקבלים 20 (מוד 101) וגם כן לא בטבלה. עבור $i = 2$ נקבל כי 78 במוד 101. לכן עבור $i = 2, j = 4$ נקבל כי:

$$x = im + j = 2 \cdot 10 + 4 = 24$$

ומתקיים כי $88 \equiv_{101} 7^{24}$.

מהי דיפי הלמן? שיטה נוספת לתיאום סיסמה בין שני צדדים שלא נפגשו מעולם. כיצד זה עובד?
1. מגרילים ראשוני מאובטח p שהוא ראשוני מהצורה $p = 2q + 1$ כך שגם q הוא ראשוני.
הראשוני הזה מפורסם לכולם p. נבחין כי:

$$|U_p| = p - 1 = 2q$$

2. אליס בוחרת $a \in U_p$ כלומר $1 \leq a \leq p - 1$ ומחשבת:

$$y_a = g^a \mod p$$

3. בוחרים $1 < g < p - 1$ ב(שאיפה) כי $o(g) = 2q$ [אך גם אם $o(g) = q$ זה לא נורא] p, q הנזכרים לעיל מפורסמים וכך גם g.
4. בוב בוחר b אקראי ומחשב:

$$y_b = g^a \mod p$$

ושולח לאליס בערוץ הפתוח.
5. כעת בערוץ הפתוח:
־ אליס מחזיקה בa ובy_b (רק היא יודעת את a!) ולכן יכולה לחשב:

$$y_b^a \equiv_p g^{ab}$$

־ בוב מחזיק בb ובy_a (קיבל מאליס) ורק הוא יודע את b! ויכול לחשב:

$$y_a^b \equiv_p g^{ab}$$

הפלא ופלא ־ שניהם קיבלו את g^{ab} (הסיסמה המשותפת להם ־ סוד למרות שיש ערוץ פתוח).

האם כיוון שכולם יודעים את g הם יכולים לחשב גם את a? זו בעיית הלוג הדיסקרטי. כאן קריטי שהסדר של g גדול אחרת אפשר לרוץ על כל החזקות.

דוגמה לדיפי הלמן:
1. נגריל ראשוני מאובטח $p = 2 \cdot 11 + 1 = 23$. $q = 11$. כולם יודעים עליו. מכאן, נבחר $a \in U_{23}$. למשל, $g = 5$ (שכן הוא יוצר את החבורה).
2. אליס מגרילה $a = 6 \in U_{23}$. היא שולחת לבוב את המידע:

$$y_a = 5^6 \equiv_{23} 8$$

3. בוב מגריל $b = 15$ למשל. הוא מחשב ושולח לאליס:

$$y_b = 5^{15} \equiv_{23} 19$$

4. עכשיו אליס מחזיקה במידע מבוב, 19 וכן בערך שלה $a = 6$. היא מחשבת $19^6 \equiv_{23} 2$.
5. בוב מחזיק במידע מאליס ובערך שלו $b = 15$ ומחשב $8^{15} \equiv_{23} 2$.
6. הפלא ופלא ־ הם מחזיקים כל אחד את המידע של השני ־ 2 ־ מבלי שאף אחד יודע.

3.2 ראשוניים גדולים ־ אלגוריתם מילר רבין

החסרון בRSA הוא שהוא דורש מספרים ראשוניים גדולים. כיצד נמצא כאלו? נשתמש בשיטה הסתברותית.

משפט 133. ידוע כי ב$[1, n]$ הטבעיים הראשוניים ישנם $\frac{n}{log(n)}$ איברים ראשוניים בערך.

לכן, אם נגריל מn המספרים הטבעיים שלנו ערך ־ מה הסיכוי שהוא ראשוני?

$$\frac{\frac{n}{log(n)}}{n} = \frac{1}{log(n)}$$

אם המספרים בסדר גודל של 2^{1024} אזי הסיכוי הוא בערך 10^{-3}. כלומר ־ אחרי 1000 פעולות נמצא מספר ראשוני. לכן לא נרצה סתם להגריל ערך ראשוני. אבל עדיין ־ אלף זה קבוע, וסביר. אבל נניח והתמזל מזלנו ונפלנו על מספר ראשוני ־ כיצד נדע שהוא ראשוני?

לפי המשפט הקטן של פרמה ־ לכל ראשוני p ולכל $1 \leq a < p$ $a^{p-1} \equiv_p 1$. לכן: נוכל להגריל ראשוני, לחשב את הערך הנ"ל (בעלות לוגריתמית) ולבדוק. אם הוא לא 1 ־ לא ראשוני. נבחין: אם הוא כן 1 ־ זה עדיין לא גורר שהוא ראשוני. הכיוון ההפוך הוא הנכון. אם כן, מה הסיכוי שa ישקר לנו?

ישנם מספרים רבים שאינם ראשוניים p אך עבור **כמעט** כל $a \in [1, p)$ $a^{p-1} \equiv_p 1$.
למשל ־ $302^{2464} \equiv_{2465} 1$ (אך 2465 איננו ראשוני כי מתחלק ב5).