תקציר הגדרות, משפטים ולמות – תורת המספרים תש"פ (מעודכן) עריכה: אייל לוי

עיקרון האינדוקציה והסדר הטוב

הגדרה: קבוצת המספרים הטבעיים $\mathbb{N}$ מוגדרת באופן הבא:

1. האיבר 1 הינו איבר ב $\mathbb{N}$.
2. אם x הינו איבר ב $\mathbb{N}$ אזי גם $x+1$ ב $\mathbb{N}$.

עקרון הסדר הטוב (WOP): *לכל תת קבוצה לא ריקה של $\mathbb{N}$ או $\mathbb{Z}^+$ יש איבר מינימלי.*

אינדוקציה חלשה

משפט 1:

תהי $S \subseteq \mathbb{N}$ תת קבוצה המקיימת:

(I.1) $1 \in S$ וגם

(I.2) אם $k \in S$ אזי $k+1 \in S$

אזי $S = \mathbb{N}$.

משפט 2:

תהי $S(n)$ טענה מתמטית התלויה ב $n \in \mathbb{N}$,

בסיס: $S(1)$ נכונה.

צעד: אם $S(k)$ נכונה אזי $S(k+1)$ נכונה.

אזי הטענה $S(n)$ נכונה לכל $n \in \mathbb{N}$.

אינדוקציה חזקה/שלמה

משפט 3:

תהי $S \subseteq \mathbb{N}$ תת קבוצה המקיימת:

(S.1) $1 \in S$ וגם

(I.2) אם $\{0,1,2,\dots,n\} \in S$ אזי $n+1 \in S$.

אזי $S = \mathbb{N}$.

משפט 4:

תהי $S(n)$ טענה מתמטית התלויה ב $n \in \mathbb{Z}^+$ המקיימת את התנאים הבאים: יהיו $n_0, n_1 \in \mathbb{Z}^+$ כך ש $n_0 \le n_1$.

בסיס: $S(n_0), S(n_0+1), \dots S(n_1)$ כולן נכונות.

צעד: אם $S(n_0), S(n_0+1), \dots, S(k-1), S(k)$ נכונות אז גם $S(k+1)$ נכונה.

אזי הטענה $S(n)$ נכונה לכל $n_0 \le n$.

למה 5: אינדוקציה חלשה גוררת אינדוקציה חזקה.

למה 6: עיקרון האינדוקציה החזקה גורר את WOP.

משפט 7:

העקרונות של אינדוקציה חלשה, אינדוקציה חזקה, ו-WOP הינם שקולים.

אי-רציונאליות של שורש 2

משפט 1. $\sqrt{2}$ הינו אי-רציונאלי.

למה 2. יהי $a \in \mathbb{Z}$. אזי a^2 הינו אי-זוגי אם ורק אם a הינו אי-זוגי.

משפט החלוקה

הגדרה: נאמר כי b מחלק את a ונסמן $b|a$ אם קיים מספר טבעי c כך שמתקיים $a = bc$.

משפט 1 (משפט החלוקה): אם a, b מספרים שלמים כך ש $b > 0$ אזי קיימים מספרים טבעיים ייחודיים q, r כך ש $a = bq + r,\ \ 0 \le r < b$.

מחלק משותף מקסימלי

הגדרה: (מחלק משותף מקסימלי): יהיו $0 \neq a, b \in \mathbb{Z}$. נאמר כי $d \in \mathbb{Z}$ הינו המחלק המשותף המקסימלי (מכאן ואילך נקרא לו- **gcd**) של a ו-b אם מתקיים:

I. $d|a$ וגם $d|b$. ובנוסף,
II. אם קיים מספר c כך ש $c|a$ וגם $c|b$ אזי $c \le d$.

נרשום $\gcd(a,b)$ או (a,b) לציון מספר זה.

הגדרה חלופית: נרשום $D(a) = \{m \in \mathbb{Z} : m|a\}$, כלומר, קבוצת כל המחלקים של a. אזי נקבל:

$$(a,b) = \max\{D(a) \cap D(b)\}.$$

למה 1: יהיו a, b מספרים ויהי $d = (a,b)$. אזי $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. כלומר, המספרים $\frac{a}{d}, \frac{b}{d}$ הם זרים.

הגדרה: יהיו a, b מספרים שלמים. אזי אוסף הקומבינציות הליניאריות של a, b הוא הקבוצה

$$L(a,b) \coloneqq \{ma + nb : m, n \in \mathbb{Z}\}.$$

למה 2 (*Bezout*): לכל שני שלמים a, b מתקיים $(a,b) \in L(a,b)$.

למה 3 (*Euclid*) אם $a|bc$ וגם $(a,b) = 1$ אזי $a|c$.

למה 4: יהיו $a, b > 0$ ויהי $c \in \mathbb{Z}^+$ אזי $(ca, cb) = c(a,b)$.

טענה:

יהי $b \in \mathbb{N}$. מבין כל b שלמים עוקבים, לפחות אחד מהם כפולה של b.

LCM

נסתכל כעת על "בן דודו" של המחלק המשותף המקסימלי, אשר *מכפלה משותפת מינימלית*. תחילה נגדיר מה זו כפולה משותפת.

הגדרה:

יהיו a ו-b שני מספרים שלמים. נאמר שמספר שלם c, הוא כפולה משותפת של a ו-b אם $a|c$ וגם $b|c$.

לדוגמה, $-ab, 0, ab$ הינם כפולות משותפות של a ו-b. כעת עבור $a, b \in \mathbb{Z}^+$, נשקול את הקבוצה $S \coloneqq \{c > 0 : a|c, b|c\}$, של המכפלות החיוביות של a ו-b. מכיוון ש-$ab \in S$, קבוצה זו אינה ריקה, ולכן לפי עיקרון הסדר הטוב (WOP), יש לה איבר מינימלי. לאיבר זה נקרא *הכפולה המשותפת המינימלית*, כפי שנגדיר כעת.

הגדרה:

יהיו a ו-b שני מספרים חיוביים ושלמים. הכפולה המשותפת המינימלית שלהם, אותה נסמן ב$\mathrm{lcm}(a,b)$, הינה מספר $m \in \mathbb{Z}^+$ המקיים את שני התנאים הבאים.

1. $a|m$ וגם $b|m$.
2. *לכל כפולה משותפת $\ell \in \mathbb{Z}^+$ של a ו-b, מתקיים $m \le \ell$.*

נשים לב כי בהכרח מתקיים $\mathrm{lcm}(a,b) \le ab$.

משפט:

יהיו $a, b \in \mathbb{Z}^+$. אזי

$$(a,b) \cdot \mathrm{lcm}(a,b) = ab$$

אלגוריתם אוקלידס

למה 1: לכל שלושה מספרים טבעיים a,b,c מתקיים $(a+cb,b)=(a,b)$.

למה 2: יהיו $a>b\geq 1$. אזי $(a,b)=(b,a\ mod\ b)$.

אלגוריתם *Euclid*:

קלט: $a,b\in\mathbb{Z}^+$.

פלט: (a,b).

כל עוד $a\neq bk$ עבור איזשהו $k\in\mathbb{Z}$, בצע:

1. השתמש במשפט החלוקה על a,b ורשום $a=bq+r$.
2. בצע $a\leftarrow b$.
3. בצע $b\leftarrow r$.

הוצא את b כפלט.

אלגוריתם *Euclid* רקורסיבי:

קלט: $a,b\in\mathbb{Z}^+$, $a\geq b>0$.

פלט: (a,b).

Euclid(a,b)

1. If $b=0$ return a
2. Return Euclid$(b,\ a\ mod\ b)$

(הסבר קצר: Euclid(a,b) משמעו פונקציה בשם Euclid שמקבלת שני פרמטרים, a ו-b)

למה 3: האלגוריתם עוצר.

הערה: מדוע לא נעבור את 0? כי תוצאת הפעולה $a\ mod\ b$ היא תמיד אי-שלילית.

למה 4: יהיו $a\geq b>0$. אזי האלגוריתם אכן מחזיר את (a,b).

אלגוריתם *Euclid* המורחב

לפי משפט *Bezout*, (a,b) יכול להיות מבוטא באופן ייחודי כקומבינציה לינארית של a ו-b כלומר:

$$(a,b)=am+bn$$

בכדי למצוא את m ו-n, נציג שימוש חדש לאלגוריתם *Euclid*. זה ייקרא **אלגוריתם Euclid המורחב**.

הגדרה (בעיית אלגוריתם אוקלידס המורחב):

קלט: $a\geq b>0$ מספרים שלמים.

פלט: שלשה (d,x,y) של מספרים שלמים כך ש:

$$d=(a,b)=ax+by$$

משוואות דיאפנטיות

בהינתן a,b,c שלמים, נתעניין בשאלה האם יש פתרון למשוואה מהצורה

$$ax+by=c$$

כאשר בפתרון הכוונה $x,y\in\mathbb{Z}$ הפותרים את המשוואה.

למה 1: למשוואה $ax+by=c$ קיים פתרון ב-$\mathbb{Z}$ אם ורק אם $(a,b)|c$.

למה 2: יהי (x_0,y_0) פתרון ל-$ax+by=c$ אזי כל פתרון אחר (x,y) ל-$ax+by=c$ הוא מהצורה:

$$y=y_0-\left(\frac{a}{d}\right)t,x=x_0+\left(\frac{b}{d}\right)t$$

כאשר $d=(a,b)$, ו-$t\in\mathbb{Z}$ שרירותי.

פירוק ייחודי לגורמים ראשוניים

הגדרה: מספר טבעי חיובי ייקרא **ראשוני** אם זה גדול מ-1 ומתחלק אך ורק בעצמו וב-1.

הגדרה: מספרים טבעיים שאינם ראשוניים נקראים **פריקים**. כלומר, n פריק אם קיימים $2\leq a,b<n$ כך ש $n=ab$.

הגדרה: הראשוניים השונים המופיעים בפירוק של מספר נקראים ***גורמים ראשוניים*** של המספר.

הגדרה: נאמר כי b מחלק את a ונסמן $b|a$ אם קיים k שלם כך ש$kb=a$.

למה 1: יהיו a,b,n מספרים טבעיים. אם $a|n$ וגם $b|a$ אזי $b|n$.

למה 2: לכל מספר שלם גדול מ-1 יש מחלק ראשוני.

משפט 3: אם n פריק, אז יש לו מחלק ראשוני שאינו גדול מ $\sqrt{n}$.

משפט 4 (המשפט היסודי של האריתמטיקה): כל מספר שלם גדול מ-1 יכול להירשם בצורה יחידה

$$n=p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_k^{a_k}$$

כאשר לכל $i\in[k]$ מתקיים $a_i>0$, כל p_i הוא ראשוני וגם $p_1<p_2<\cdots<p_k$.

תרגול משפט יסודי

הגדרה: יהי $n\in\mathbb{Z}$. נאמר על n שהוא מספר ריבועי (***Perfect Square***) אם קיים $a\in\mathbb{Z}$ כך שמתקיים $n=a^2$.

הגדרה: יהי $n\in\mathbb{Z}$. נאמר על n שהוא חופשי מריבועים (***Square Free***) אם מלבד 1 לא קיים $b\in\mathbb{Z}$ כך ש-$b^2|n$. (כלומר n איננו מתחלק באף מספר ריבועי פרט ל-1)

הגדרה: נאמר על מספר n שהוא מתחלק בריבוע ראשוני (***Prime Square Divisible***) אם לכל p ראשוני, המקיים $p|n$ מתקיים שגם $p^2|n$.

הגדרה: נאמר על מספר n שהוא מספר קובי (***Perfect Cube***) אם קיים $a\in\mathbb{Z}$ המקיים $n=a^3$.

יש אינסוף ראשוניים בעולם

משפט (Euclid): יש אינסוף ראשוניים בעולם.

מסקנה: יהיו $p_1,p_2,\ldots,p_n$ קבוצת ראשוניים. למספר מהצורה

$$N=\prod_{i=1}^{n}p_i+1$$

יש מחלק ראשוני שאינו מהקבוצה $p_1,p_2,\ldots,p_n$ או שהמספר N הוא ראשוני.

משפט 3: יש אינסוף ראשוניים מהצורה $4n+3$.

משפט 4: יש אינסוף ראשוניים מהצורה $4n-1$.

משפט (*Dirichlet*) אם $(a,b)=1$ אזי קיימים אינסוף ראשוניים מהצורה $an+b$.

תפוצת הראשוניים

הגדרה: עבור $n\in\mathbb{Z}^+$ נגדיר את p_n להיות הראשוני ה-n. עבור $x\in\mathbb{R}$ נגדיר את $\pi(x)$ להיות כמות הראשוניים עד x.

לפי ההוכחה של *Euclid* לאינסוף ראשוניים, ניתן לרשום את המסקנה הבאה:

מסקנה 1: לכל $n\geq 1$ מתקיים

$$p_{n+1}\leq p_1\cdot p_2\cdot\ldots\cdot p_n+1.$$

משפט 2 (Bonse): לכל $n\geq 5$ מתקיים

$$p_{n+1}^2<p_1\cdot p_2\cdot\ldots\cdot p_n.$$

משפט 3: $p_n\leq 2^{2^n}$.

מסקנה 4: עבור $n\geq 1$ קיימים לפחות n ראשוניים קטנים מ-2^{2^n}.

מסקנה 5: $\pi(x)=\Omega(\log\log x)$.

משפט 6: (*Bertrand's postulate*): עבור $n\geq 2$, האינטרוול $(n,2n)$ מכיל לפחות ראשוני אחד.

מסקנה 7: $p_{n+1}<2p_n$.

משפט 8: עבור $n\geq 2$ מתקיים $p_n<2^n$.

מסקנה 9: $\pi(x)=\Omega(\log x)$.

תרגול ראשוניים

המסננת של ארסטותנס

רעיון האלגוריתם: למצוא את כל הראשוניים עד n.

בהינתן מספר שלם n המסננת תעבוד בצורה הבאה . המסננת תאתחל רשימה המכילה את כל המספרים בין2 ל-n. לאחר מכן, נבחר מספרים מתחילת הרשימה בצורה הבאה: עבור כל מספר x שלא נמחק עדיין, המקיים $x \le \sqrt{n}$ המסננת תמחק כל כפולה של x מהרשימה.

<u>טענה</u>: בסיום האלגוריתם $A[k] = 1$ אמ"מ k הינו מספר ראשוני.

<u>למה</u>: לכל $k \in [2, \lfloor\sqrt{n}\rfloor + 1]$ האלגוריתם מקיים: לכל $2 \le i \le n$ בתחילת האיטרציה ה-k של הלולאה החיצונית $A[i] = 0$ אמ"מ i מתחלק במספר ראשוני כלשהו הקטן מ-k.

הערה: הטענה נובעת מהלמה ע"י הצבת $k = \lfloor\sqrt{n}\rfloor + 1$ ושימוש בכך שלכל פריק n יש גורם ראשוני $\le \lfloor\sqrt{n}\rfloor$.

עוד הערה: כאשר אנחנו אומרים "תחילת האיטרציה ה-$k = \lfloor\sqrt{n}\rfloor + 1$" (בעצם אין איטרציה כזו), נסכים כי כוונתנו היא לסוף האיטרציה ה-$k - 1 = \lfloor\sqrt{n}\rfloor$.

שקילויות

הגדרה: יהי $m \in \mathbb{Z}^+$ ויהיו $a, b \in \mathbb{Z}$. נאמר כי a שקול ל-b מודולו m ונרשום $a \equiv b \ (mod\ m)$ אם $m|a - b$.

משפט 1: יהי $m \in \mathbb{Z}^+$ ויהיו $a, b \in \mathbb{Z}$. אזי $a \equiv b \ (mod\ m)$ אם ורק אם $a = b + km$ עבור $k \in \mathbb{Z}$ כלשהו.

הגדרה: בהינתן $m \in \mathbb{Z}^+$ נגדיר את היחס

$$R_m := \{(a, b) \in \mathbb{Z}^2 : a \equiv b \ (mod\ m)\}.$$

משפט 2: יהי $m \in \mathbb{Z}^+$. היחס R_m מגדיר מחלקות שקילות "מודולו m". כלומר, הוא מקיים את התכונות הבאות:

1. <u>רפלקסיביות</u>: $a \equiv a \ (mod\ m)$ לכל $a \in \mathbb{Z}$.
2. <u>סימטריות</u>: אם $a \equiv b \ (mod\ m)$ אזי $a, b \in \mathbb{Z}$ אם ורק אם $b \equiv a \ (mod\ m)$.
3. <u>טרנזיטיביות</u>: אם $a, b, c \in \mathbb{Z}$ כך ש $a \equiv b \ (mod\ m)$ וגם $b \equiv c \ (mod\ m)$ אזי $a \equiv c \ (mod\ m)$.

הגדרה: *מערכת שאריות שלמה מודולו* m היא קבוצת שלמים כך שכל $a \in \mathbb{Z}$ שקול לאיבר יחיד של אותה קבוצה מודולו m.

משפט 3 (עיקרון שובך היונים): אם n יונים מתחלקים בין לכל היותר $n - 1$ שבכים, אזי לאחר החלוקה קיים שובך המכיל לפחות שני יונים.

משפט 4: יהי $m \in \mathbb{Z}^+$. כל קבוצה של m מספרים לא שקולים מודולו m מהווה מערכת שאריות שלמה מודולו m.

משפט 5: (אריתמטיקה מודולרית)

יהיו $a, b, c, d \in \mathbb{Z}$ ויהי $m \in \mathbb{Z}^+$ כך ש $a \equiv b \ (mod\ m), c \equiv d \ (mod\ m)$. אזי:

1. <u>חיבור</u>: $a + c \equiv b + d \ (mod\ m)$.
2. <u>חיסור</u>: $a - c \equiv b - d \ (mod\ m)$.
3. <u>הכפלה</u>: $ac \equiv bd \ (mod\ m)$.

משפט 6: יהיו $a, b, c \in \mathbb{Z}$ ויהי $m \in \mathbb{Z}^+$ כך ש $d = (c, m)$. אזי $ac \equiv bc \ (mod\ m)$ אם ורק אם $a \equiv b \ (mod\ {}^{m}/_{d})$.

שקילות ליניארית

הגדרה: משוואה מהצורה

$$ax \equiv b \ (mod\ m)$$

נקראת *שקילות ליניארית*.

אבחנה: אם $x = x_0 \in \mathbb{Z}$ הינו פתרון למשוואה $ax \equiv b \ (mod\ m)$, אזי כל איבר במחלקת השקילות של x_0 מודולו m הינו פתרון למשוואה.

למה 1: יהיו $x_1 = x_0 + \left(\frac{m}{d}\right)t_1,\ x_2 = x_0 + \left(\frac{m}{d}\right)t_2$ שני פתרונות למשוואה $ax \equiv b \ (mod\ m)$. אזי $x_1 \equiv x_2 \ (mod\ m)$ אם ורק אם $t_1 \equiv t_2 \ (mod\ d)$.

משפט 2: יהי $m \in \mathbb{Z}^+$ ויהיו $a, b \in \mathbb{Z}$, ויהי $d = (a, m)$.

1. אם $d \nmid b$ אזי ל $ax \equiv b \ (mod\ m)$ אין פתרון.
2. אחרת ל- $ax \equiv b \ (mod\ m)$ יש d פתרונות לא שקולים מודולו m.

מסקנה 3: אם במשוואה $ax \equiv b \ (mod\ m)$ מתקיים $(a, m) = 1$ אזי יש לה פתרון יחיד מודולו m. אמנם יש אינסוף פתרונות, אך כולם נמצאים באותה מחלקת שקילות מודולו m.

הופכיים

לפי משפט 2 בהרצאת "שקילות ליניארית", ראינו שלמשוואה $ax \equiv b \ (mod\ m)$ קיים פתרון אם ורק אם $(a, m)|b$. כעת נחקור את המשוואה הזו: $ax \equiv 1 \ (mod\ m)$ (1)

הגדרה 1: יהיו $a \in \mathbb{Z}, m \in \mathbb{Z}^+$ כך ש-$(a, m) = 1$. אזי הפתרון ל-(1) נקרא *ההופכי המודולרי של* a *מודולו* m.

מסקנה 2: יהי p ראשוני. אזי לכל $a \in [p - 1]$ יש הופכי מודולו p.

למה 3: יהיו $a \in \mathbb{Z}$ ו-p ראשוני. אזי a הינו ההופכי של עצמו במודולו p אם ורק אם $a \equiv 1 \ (mod\ p)$ או $a \equiv -1 \ (mod\ p)$.

תרגול שקילויות

טענה (כלל הצמצום):

יהיו $a, b, c \in Z$, $m \in Z^+$ ו-$d = (c, m)$. אזי:

$$a \equiv b \ (mod\ \frac{m}{d}) \Leftrightarrow a \cdot c \equiv b \cdot c \ (mod\ m)$$

0

<u>טענה (כלל ההרחבה):</u>

יהיו $a, b, c \in \mathbb{Z}$, $c \neq 0$ ויהי $m \in \mathbb{Z}^+$

אזי $a \equiv b \ (mod\ m) \Leftrightarrow a \cdot c \equiv b \cdot c \ (mod\ m \cdot c)$

טענה:

יהיו $m_1, m_2, \dots, m_k$ מספרים שלמים עבור $k \in \mathbb{Z}^+$.

אם $a \equiv b \ (mod\ m_i)$ עבור כל $i \in [1, k]$ **אז**:

$$a \equiv b \ (mod\ lcm(m_1, m_2, \dots, m_k))$$

טענה:

יהיו $m_1, m_2, \dots, m_k$ מספרים שלמים עבור $k \in N$, אזי:

1. $a \equiv b \ (mod\ m_i), \forall i \in [1, k] \Leftrightarrow a \equiv b \ (mod\ lcm(m_1, m_2, \dots, m_k))$
2. במידה $m_1, m_2, \dots, m_k$ מספרים שלמים **זרים** אזי: $a \equiv b \ (mod\ m_i), \forall i \in [1, k] \Leftrightarrow a \equiv b \ (mod\ m_1 \cdot m_2 \cdot \dots \cdot m_k)$

טענה

יהיו m_1, m_2 מספרים שלמים כלשהם

אם $x \equiv r \ (mod\ lcm(m_1, m_2))$

אז

$$x \equiv (r\ mod\ m_1)\ (mod\ m_1)$$
$$x \equiv (r\ mod\ m_2)\ (mod\ m_2)$$

משפט השאריות הסיני

הגדרה אלטרנטיבית ל-LCM: *יהיו a ו-b שני מספרים חיוביים ושלמים. הכפולה המשותפת המינימלית שלהם, אותה נסמן ב*$\mathrm{lcm}(a, b)$, *הינה מספר $m \in N$ המקיים את שני התנאים הבאים:*

1. $a|m$ וגם $b|m$.
2. *לכל כפולה משותפת $\ell \in \mathbb{Z}^+$ של a ו-b, מתקיים $m|\ell$.*

הוכחת שקילות ההגדרה האלטרנטיבית וההגדרה המקורית כבר נעשתה בתירגול LCM כחלק מהוכחת המשפט המרכזי בעמוד 2 שם.

למה 1: יהיו $m_1, m_2, \dots, m_k \in N$. אם $a \equiv b \ (mod\ m_i)$ לכל $i \in k$ אזי $a \equiv b \ (mod\ lcm(m_1, m_2, \dots, m_k))$.

למה 2: יהיו $m_1, m_2 \in \mathbb{Z}$ כך שמתקיים $x \equiv r \ (mod\ lcm(m_1, m_2))$. אזי $x \equiv r \ (mod\ m_1)$ וגם $x \equiv r \ (mod\ m_2)$.

למה 3: יהיו $n_1, n_2, \dots, n_r$ זרים בזוגות. יהי $M = \prod_i n_i$, ויהי $M_k = M/n_k$. אזי $(M_k, n_k) = 1$.

משפט השאריות הסיני (משפט 4): יהיו $n_1, n_2, \dots, n_r$ זרים בזוגות. אזי למערכת מהצורה (1) יש פתרון ייחודי מודולו $M = \prod_i n_i$.

משפט וילסון

משפט 1 (וילסון): יהי p ראשוני. אזי

$$(p - 1)! \equiv -1 \ (mod\ p)$$

משפט 2 (משפט וילסון ההפוך):

יהי $2 \le n \in \mathbb{Z}$. אם $(n - 1)! \equiv -1 \ (mod\ n)$ אזי n ראשוני.

מסקנה 3: n ראשוני $\Leftrightarrow (n - 1)! \equiv -1 \ (mod\ n)$.

מסקנה 4: כל $1 < n \in \mathbb{Z}$ הינו ראשוני $\Leftrightarrow (n - 2)! \equiv 1 (mod\ n)$.

משפט פרמה הקטן

משפט 1 (משפט פרמה הקטן): יהי p ראשוני ויהי $a \in \mathbb{Z}^+$ כך ש $p \nmid a$. אזי

$$a^{p-1} \equiv 1 \ (mod\ p)$$

מסקנה 2: יהי p ראשוני ויהי $a \in \mathbb{Z}^+$. אזי

$$a^p \equiv a \ (mod\ p)$$

מסקנה 3: אם p ראשוני ו-$a \in \mathbb{Z}^+$ כך ש-$p \nmid a$ אזי a^{p-2} הינו ההופכי של a במודולו p.

Pseudoprimes

רקע: ראינו אפיון של וילסון למספרים ראשוניים. אלא שחישוב עצרת למספר גדול לוקחת זמן רב. אולי נוכל להיעזר בפרמה לשם בדיקת ראשוניות?

הגדרה 2: מספר n ייקרא *פסודו-ראשוני ביחס לבסיס* b אם n פריק ומתקיים $b^n \equiv b \ (mod\ n)$.

משפט 4: לכל $b \in \mathbb{Z}^+$ קיימים אינסוף פסודו-ראשוניים ביחס לבסיס b. (ללא הוכחה)

למה 5: אם $d, n \in \mathbb{Z}^+$ כך ש-$d|n$ אזי $2^d - 1 \ |2^n - 1$.

משפט 6: יש אינסוף פסודו-ראשוניים ביחס לבסיס 2.

מספרי קרמייקל

רקע: מספרים פסודו-ראשוניים מקשים על השימוש במשפט הקטן של פרמה כדי לבדוק ראשוניות. מספרי קרמייקל הופכים את זה לבלתי אפשרי.

הגדרה 1: מספר n ייקרא *מספר קרמייקל* אם לכל $b \in \mathbb{Z}^+$ עבורו $(n,b) = 1$ מתקיים $b^{n-1} \equiv 1 \ (mod\ n)$

כלומר מספר קרמייקל הוא פסאודו-ראשוני ביחס לכל בסיס הזר לו.

הגדרה 2: נסמן $C(x)$ כמות המספרי קרמייקל הקטנים מ-x.

משפט 3: יש אינסוף מספרי קרמייקל. בנוסף עבור x מספיק גדול מתקיים $C(x) > x^{\frac{2}{7}}$.

משפט 5: יהי $n = q_1 \cdot q_2 \cdot \ldots \cdot q_k$ מכפלת ראשוניים זרים. אם מתקיים

$$\forall i \in [k]: (q_i - 1)|(n-1)$$

אזי n הינו מספר קרמייקל.

משפט 6: (*הקריטריון של Korselt*) מספר n הינו מספר קרמייקל אם ורק אם $n = q_1 \cdot q_2 \cdot \ldots \cdot q_k$ מכפלת ראשוניים זרים עבורם

$$\forall i \in [k]: (q_i - 1)|(n-1)$$

פונקציית Euler

רקע: משפט פרמה עוזר לחשב שקילויות בהן המודולו ראשוני. משפט Euler יסייע בחישוב שקילות בה המודולו פריק או ראשוני, ולכן זוהי הכללה של משפט פרמה[1].

הגדרה 1: פונקציה f תיקרא *פונקציה-כפלית* (Multiplicative) אם $f(mn) = f(m) \cdot f(n)$ לכל $(m,n) = 1$. פונקציה f תיקרא *פונקציה-כפלית-שלמה* אם $f(mn) = f(m) \cdot f(n)$ לכל $m, n \in \mathbb{Z}^+$.

משפט 3: תהי f פונקציה-כפלית ויהי $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$. אזי

$$f(n) = f(p_1^{a_1}) \cdot f(p_2^{a_2}) \cdot \ldots \cdot f(p_k^{a_k})$$

הגדרה 4: יהי $n \in \mathbb{Z}^+$. יהי $\varphi(n)$ כמות המספרים הטבעיים הקטנים מ-n וזרים אליו. כלומר

$$\varphi(n) := |\{k \in [n]: (k,n) = 1\}|$$

הפונקציה $\varphi(\cdot)$ נקראת *Euler's totient function*.

למה 6: לכל $n > 1$ מתקיים $\varphi(n) \leq n - 1$.

למה 7: לכל n פריק מתקיים $\varphi(n) \leq n - 2$.

מסקנה 8: $\varphi(n) = n - 1$ אם ורק אם n ראשוני.

למה 9: יהי p ראשוני ויהי $k > 0$. אזי

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$$

למה 10: $(a,bc) = 1 \Leftrightarrow (a,b) = 1 \wedge (a,c) = 1$.

למה 11: $(qm + r, m) = (r, m)$.

משפט 12: $\varphi(\cdot)$ הינה פונקציה-כפלית.

מסקנה 13: יהי $1 < n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$. אזי

$$\varphi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \cdot \ldots \cdot (p_k^{a_k} - p_k^{a_k-1})$$
$$= n(1 - 1/p_1) \cdot (1 - 1/p_2) \cdot \ldots \cdot (1 - 1/p_k)$$

משפט Euler

הגדרה 1: יהי $n \in \mathbb{Z}^+$. קבוצה של $\varphi(n)$ מספרים כך שמתקיים

(1) כל איבר בה זר ל-n

(2) כל שני איברים בה אינם שקולים מודולו n

נקראת מערכת מצומצמת של שאריות מודולו n.

למה 3: יהי $n \geq 1$ ויהי $a \geq 1$ כך שמתקיים $(a,n) = 1$. אם $r_1, r_2, \ldots, r_{\varphi(n)}$ היא מערכת שאריות מצומצמת מודולו n אזי גם $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(n)}$ היא מערכת שאריות מצומצמת מודולו n.

מסקנה 5: תהי $r_1, r_2, \ldots, r_{\varphi(n)}$ מערכת שאריות מצומצמת מודולו n ויהי $a \in \mathbb{Z}$ כך ש-$(a,n) = 1$. אזי

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \equiv a \cdot r_1\ a \cdot r_2, \ldots, a \cdot r_{\varphi(n)} \ (mod\ n)$$

משפט 6 (*Euler*): יהי $n \in \mathbb{Z}^+$ ויהי $a \in \mathbb{Z}$ כך שמתקיים $(a,n) = 1$. אזי

$$a^{\varphi(n)} \equiv 1 \ (mod\ n)$$

מסקנה 7: יהי $1 < n \in \mathbb{Z}^+$ ויהי $a \in \mathbb{Z}$ כך ש-$(a,n) = 1$. אזי ההופכי של a במודולו n הינו $a^{\varphi(n)-1}$.

<u>הגדרה</u>: עבור $n \in \mathbb{Z}^+$ יהי $R_n = \{l \in [n]: (l,n) = 1\}$. כלומר, R_n הינו מערכת השאריות המצומצמת הקנונית מודולו n.

<u>הצפנות- הקדמה</u>

הגדרה: פרמוטציה הינה פונקציה מקבוצה לעצמה.

אלגוריתם RSA

נותר לתאר את האלגוריתם שיפיק את S_A, P_A עבור אליס (ואת S_B, P_B עבור בוב).

1. השג שני מספרים ראשוניים גדולים p, q. (כיצד? זו שאלה שפותרים בקורס "אלגוריתמים 2 מתקדמים", בשנה ב' סמסטר ב')
2. קבע $n := p \cdot q$.
3. מצא (איך? באלגוריתמים 2 מתקדמים) מספר אי-זוגי e עבורו מתקיים $(e, \varphi(n)) = 1$.
4. מצא d שהוא ההופכי של e במודולו $\varphi(n)$.
5. מפתח ציבורי:= (e,n) (זוג סדור, לא ה gcd). מפתח פרטי:= (d,n). (שוב, זוג סדור).

האלגוריתם לא מפיק פונקציות אלא זוגות סדורים! אז מהן הפונקציות המובטחות?

בהינתן $m \in \{[0]_n, [1]_n, \ldots [n-1]_n\}$ (כלומר, m הינה נציגים מודולו n) יהיו

$$P_A(m) := m^e (mod\ n), \quad S_A(m) := m^d (mod\ n)$$

(המתרגלים הראו בתרגול שקילויות חלק 4 איך לחשב חזקות מודולריות)

נוכיח שהאלגוריתם עובד.

משפט: יהיו P_A, S_A כפי שתיארנו. אזי:

$$S_A(P_A(m)) = S_A((m)^e)(mod\ n) = (m^e)^d (mod\ n) = m^{de} (mod\ n)$$

$$P_A(S_A(m)) = P_A((m)^d)(mod\ n) = (m^d)^e (mod\ n) = m^{de} (mod\ n)$$

<u>תמורות</u>

<u>הגדרה 1</u> (תמורה/פרמוטציה): תמורה היא העתקה חד-חד-ערכית ועל מ-X ל-X כאשר X קבוצה לא ריקה.

<u>סימון</u>: נסמן תמורה בצורת טבלה בעלת שתי שורות- השורה העליונה היא איברי הקבוצה המקורית לפי הסדר (התחום), והשורה השנייה היא האיברים אליהם מועתקים איברי הקבוצה בסדר כלשהו (הטווח).

<u>הגדרה 3</u>: עבור תמורה על הקבוצה $X = [1 \ldots n]$ נסמן ב-S_n את אוסף כל התמורות מעל X.

<u>הגדרה 5</u>: שתי תמורות $\sigma, \tau \in S_n$ נקראות **מתחלפות** אם $\sigma\tau = \tau\sigma$.

<u>הגדרה 7</u> (תמורת הזהות): $1_{S_n} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. לכל תמורה σ מתקיים

$$1_{S_n}\sigma = \sigma = \sigma 1_{S_n}$$

<u>אבחנה 9</u>: תמורת הזהות מתחלפת עם כל תמורה.

<u>הגדרה 10</u> (תמורה הופכית) לכל תמורה $\sigma \in S_n$ קיימת תמורה הופכית $\sigma^{-1} \in S_n$ כך שמתקיים

$$\sigma\sigma^{-1} = 1_{S_n} = \sigma^{-1}\sigma$$

<u>חוק הצמצום לתמורות 12</u>: יהיו $\alpha, \beta, \gamma \in S_n$.

1. אם $\alpha\beta = \alpha\gamma$ אזי $\beta = \gamma$ (צמצום משמאל)
2. אם $\beta\alpha = \gamma\alpha$ אזי $\beta = \gamma$ (צמצום מימין)

מעגלים בפרמוטציות

הגדרה:

עבור פרמוטציה (תמורה) $\sigma \in S_X$ נסמן

$$M_\sigma = \{x \in X : \sigma(x) \neq x\}$$

להיות קבוצת הנקודות שאינן נקודות שבת של σ.

הגדרה:

יהי $\sigma \in S_X$. אם $M_\sigma = \{i_1, i_2, \dots, i_r\}$ וגם

$$i_1 \xrightarrow{\sigma} i_2, \dots, i_{r-1} \xrightarrow{\sigma} i_r$$

אזי נאמר שσ הוא מעגל באורך r, ונכתוב אותו כ-$(i_1, \dots, i_r)$.

מעגלים באורך 2 מחליפים זוגות של איברים ולכן נקרא להם *חילופים* (או טרנספוזיציות).

אבחנה:

אם σ מעגל באורך r אזי σ^{-1} מעגל באורך r גם כן. יתרה מכך, אם $\sigma = (i_1, \dots, i_r)$ אזי $\sigma^{-1} = (i_r, \dots, i_1)$.

למה:

יהיו α וβ מעגלים בS_n. אם קיים $i \in M_\alpha \cap M_\beta$ עבורו $\alpha^k(i) = \beta^k(i)$, לכל $k \geq 1$, אזי $\alpha = \beta$.

משפט:

כל פרמוטציה $\alpha \in S_n$ הינה מעגל או ניתנת לכתיבה כמכפלה של מעגלים זרים בזוגות.

הגדרה: שתי פרמוטציות $\sigma, \tau \in S_X$ תיקראנה זרות אם $M_\sigma \cap M_\tau = \emptyset$.

טענה:

כל שתי פרמוטציות $\sigma, \tau \in S_X$ זרות הינן מתחלפות, כלומר $\sigma\tau = \tau\sigma$.

טענה:

יהי $\alpha = \beta\gamma \in S_n$, כאשר β וγ פרמוטציות זרות. אם $i \in M_\beta$ אזי $\alpha^k(i) = \beta^k(i)$ לכל $k \geq 0$.

משפט:

יהי $\alpha \in S_n$ ויהי $\alpha = \beta_1 \cdots \beta_t$ פירוק כלשהו של α למעגלים זרים בזוגות. אזי פירוק זה יחיד עד כדי שינוי הסדר של ה-β_i במכפלה.

טענה:

יהי $\beta \in S_n$ ויהי $\beta = \alpha_1 \cdots \alpha_t$ הפירוק של β למעגלים זרים בזוגות, כאשר α_i הינו מעגל באורך r_i. אזי השלם $\ell \in \mathbb{Z}^+$ הקטן ביותר המקיים $\beta^\ell = \mathbf{1}_{[n]}$ הוא $\ell = \mathrm{lcm}(r_1, \dots, r_t)$.

<u>חבורות</u>

<u>הגדרה 1</u> (חבורה): חבורה היא זוג $(G,*)$ של קבוצה G ופעולה בינארית $*$ המקבלת זוג איברים ומחזירה איבר יחיד $G * G \to G$, המקיימת:

א. סגירות (G סגורה תחת $*$, כלומר, $\forall a, b \in G: a * b \in G$)

ב. $*$ אסוציאטיבית: לכל $a, b, c \in G$ מתקיים $(a * b) * c = a * (b * c)$.

ג. קיים איבר ניטרלי: $e \in G$ כך שלכל $a \in G$ מתקיים $ea = ae = a$.

ד. קיום הופכי: לכל $a \in G$ קיים איבר ב-G שנסמנו a^{-1}, כך ש $a * a^{-1} = a^{-1} * a = e$.

<u>טענה 3</u>: לכל $n \in N$ מתקיים $(S_n, \circ)$ היא חבורה.

<u>הוכחה</u>:

א. סגירות: ראינו כי לכל $\sigma, \tau \in S_n$ מתקיים $\sigma \circ \tau \in S_n$. (הרכבת פונקציות חח"ע ועל היא פונקציה חח"ע ועל)

ב. אסוציאטיביות: לכל $\sigma, \tau, \alpha \in S_n$ מתקיים

$$(\sigma \circ \tau) \circ \alpha = \sigma \circ (\tau \circ \alpha)$$

כי לכל $1 \leq i \leq n$

$$(\sigma \circ \tau) \circ \alpha(i) = (\sigma \circ \tau)(\alpha(i)) = \sigma\left(\tau(\alpha(i))\right)$$

$$\sigma \circ (\tau \circ \alpha)(i) = \sigma((\tau \circ \alpha)(i)) = \sigma\left(\tau(\alpha(i))\right)$$

ג. קיום ניטרלי: ראינו כי לכל $\sigma \in S_n$ מתקיים כי הפרמוטציה $e = 1_{S_n} \in S_n$ מקיימת $1_{S_n} \circ \sigma = \sigma \circ 1_{S_n} = \sigma$

ד. קיום הופכי: ראינו כי לכל $\sigma \in S_n$ קיימת $\sigma^{-1} \in S_n$ כך ש $\sigma \circ \sigma^{-1} = \sigma^{-1}\sigma = 1_{S_n}$.

<u>הגדרה 4</u>: נאמר כי השלמים מתחלקים למחלקות שקילות מודולו n ונסמן

$$Z_n = \{[0]_n, [1]_n \dots [n-1]_n\}$$

כעת נראה שתי דוגמות חשובות במיוחד לחבורות הקשורות לחשבון המודולורי:

1. החבורה החיבורית $(Z_n, +)$.

2. החבורה הכפלית $(Z_n^*, \cdot)$.

1. קל לראות את קיום הגדרת החבורה (איבר ניטרלי $[0]_n$, לכל $[k]_n$ ההופכי הוא $[n-k]_n$).

מדוע זה ההופכי? כי $k + (n-k) = n \equiv 0 \ (mod\ n)$.

יש לשים לב כי בחבורה חיבורית ההופכי הוא הנגדי, ולפעמים נסמנו $[-k]_n$.

2. החבורה הכפלית $(Z_n^*, \cdot)$ כאשר $Z_n^* = \{[a]_n \in Z_n \mid (a, n) = 1\}$

<u>חבורה אבלית</u>

<u>הגדרה</u>: חבורה $(G,*)$ תיקרא חבורה *קומוטטיבית* (או *אבלית*) אם לכל $a, b \in G$ מתקיים $a * b = b * a$.

<u>טענה</u> (יחידות הניטרלי): בחבורה $(G,*)$ יש איבר ניטרלי יחיד.

<u>הוכחה</u>: נניח ש-$e, f \in G$ שניהם ניטרליים. אזי $ef = f$ שכן e נייטרלי, וגם $ef = e$ שכן f נייטרלי, ולכן $e = f$.

<u>טענה</u> (יחידות ההופכי): תהי $(G,*)$ חבורה ויהי $a \in G$ אזי $a^{-1} \in G$ יחיד.

<u>הוכחה</u>: נניח בשלילה כי יש ל-a שני הופכיים b, b'. אזי:

$$b' = b'e = b'(ab) = (b'a)b = eb = b$$

כאשר השיוויון השני מימין והשני משמאל נובעים מכך ש b, b' הפכיים ל-a .

<u>סימון</u>: תהי $(G,*)$ חבורה עם נייטרלי $e \in G$ ויהי $a \in G$. אזי נסמן

$$a^0 = e, \ \ a^1 = a, \ \ \forall n \geq 1: a^{n+1} = a * a^n$$

<u>טענה</u>: תהי $(G,*)$ חבורה אבלית סופית $G = \{g_1, g_2, \dots g_r\}$ ויהי $a = g_1 * g_2 * \dots g_r$ אזי $a^2 = e$.

<u>הוכחה</u>: לכל $1 \leq i \leq r$ יש $1 \leq k \leq r$ כך ש-g_k הופכי ל-g_i, ומקומוטטיביות הטענה נובעת.

<u>תכונות נוספות בחבורות</u>

<u>משפט "חוקי חזקות" בחבורה:</u>

תהי $(G,*)$ חבורה, $a \in G$, $0 \leq m, n \in Z$. אזי:

$a^m a^n = a^{m+n} = a^n a^m$ (משמיטים את הסימן $*$ כמו בכפל רגיל)

$(a^m)^n = a^{mn} = (a^n)^m$

אם $ab = ba$ אזי $(ab)^n = a^n b^n$

<u>משפט "תכונות ההופכי" בחבורה:</u>

תהי $(G,*)$ חבורה עם הניטרלי e, ויהיו $a, b, a_1, a_2, \dots, a_n \in G$. אזי:

1) $e^{-1} = e$ 2) $(a^{-1})^{-1} = a$ 3) $(ab)^{-1} = b^{-1}a^{-1}$ (הסדר משפיע!)

4) $(a_1 * a_2 * \dots * a_n)^{-1} = a_n^{-1} * \dots * a_1^{-1}$ 5) $(a^n)^{-1} = (a^{-1})^n$.

חוק הצמצום בחבורה: תהי $(G,*)$ חבורה ויהיו $g,h,f \in G$. אזי:

1. (צמצום שמאלי) אם $gh = gf$ אזי $h = f$.

2. (צמצום ימני) אם $hg = fg$ אזי $h = f$.

הוכחה:

1. לפי הגדרת חבורה קיים g^{-1}. נכפול בו משמאל ונקבל

$$g^{-1}(gh) = g^{-1}(gf) \to (g^{-1}g)h = (g^{-1}gf) \to eh = ef \to h = f$$

הוכחת 2 זהה, רק שנכפיל מימין. השלימו בבית.

טענה: אם G חבורה סופית ו-$g \in G$ אזי קיים n טבעי כך ש-$g^n = e$.

דיון: האם זה נכון לחבורה אינסופית? לא. למשל $(Z,+)$, אם ניקח $g = 2$ אז $2 + 2 + \cdots + 2$ לעולם לא ייתן 0.

הוכחה: נתבונן באוסף .... g^1, g^2, g^3 מסופיות G נובע כי קיימים $m,n \in N$ כך שמתקיים

$$g^m = g^{n+m} \to g^m \cdot e = g^m \cdot g^n \to e = g^n$$

כאשרה המעבר האחרון נובע מכלל הצמצום.

טענה- פתרון שקילות ליניארית בחבורות:

תהי G חבורה, ויהיו $g,h \in G$. אזי:

1. למשוואה $gx = h$ יש פתרון יחיד ב-G, $x = g^{-1}h$.

2. למשוואה $xg = h$ יש פתרון יחיד ב-G, $x = hg^{-1}$.

הוכחת 1. x פתרון, שכן

$$gx = g(g^{-1}h) = (gg^{-1})h = eh = h.$$

נראה שזהו פתרון יחיד- יהי $y \in G$ פתרון למשוואה $gx = h$. אזי $x = y \leftarrow gx = gy$ (חוק הצמצום).

תת חבורה

אינטואיציה: תת חבורה היא תת קבוצה של חבורה, שהיא בעצמה חבורה.

כדי שתת-החבורה תהיה אכן חבורה, נצטרך סגירות לפעולה ולהופכי.

הגדרה: תהי $(G,*)$ חבורה. תהי $S \subseteq G$ תת קבוצה לא ריקה של G המקיימת:

1) סגירות- לכל $s,t \in S$ גם $s * t \in S$

2) סגירות להופכי- לכל $s \in S$ גם $s^{-1} \in S$

אז S נקראת תת-חבורה של G, ומסמנים $S \leq G$.

טענה: אם S תת חבורה של $(G,*)$ אז S עצמה חבורה עם הפעולה $*$.

הוכחה: נראה את קיום האקסיומות:

1) סגירות- מההגדרה. 2) אסוציאטיביות- תורשתית מ-G.

3) קיום יחידה- $S \neq \phi$ ולכן יש $s \in S$. מסגירות להופכי, גם $s^{-1} \in S$ ומסגירות לפעולה נובע כי $e = ss^{-1} \in S$. 4) קיום הופכי- מההגדרה.

תת חבורות שתמיד קיימות: לכל חבורה G, $\{e\} \leq G$ וגם $G \leq G$. (תת חבורות טריוויאליות)

תת חבורה ששונה מ-G נקראת "תת חבורה proper".

מבחני תת-חבורה:

1) מבחן ראשון: תהי $(G,*)$ חבורה. $S \subseteq G$ תת-חבורה $\leftrightarrow$

א. $e \in S$

ב. לכל $s,t \in S$ גם $st^{-1} \in S$.

הוכחה: ($\leftarrow$) ברור.

($\rightarrow$) נראה כי S מקיימת את תנאי החבורה.

2. סגירות להופכי- יהי $s \in S$. משום שגם $e \in S$ נובע שגם $es^{-1} \in S$ ולכן $s^{-1} \in S$.

1. סגירות לפעולה- יהיו $s,t \in S$. אזי $t^{-1} \in S$ לפי השורה הקודמת, ולכן

$st = s(t^{-1})^{-1} \in S$.

2) מבחן שני: מבחן לתת חבורה סופית:

משפט: תהי H תת קבוצה סופית לא ריקה של חבורה G. אזי:

$H \leq G \leftrightarrow H$ סגורה תחת הפעולה של G (כלומר, כאן מספיק תנאי הסגירות לפעולה, ולא דרוש גם סגירות להופכי)

הוכחה: ($\leftarrow$) ברור.

($\rightarrow$) עלינו להראות כי לכל $h \in H$ מתקיים כי $h^{-1} \in H$.

יהי $h \in H$. מהסגירות נובע כי $h, h^2, h^3, \ldots \in H$. אבל H סופית, ולכן יש $m,n \in N$ כך ש-$h^n = h^{n+m}$ ולכן $e = h^m$ (בגלל חוק הצמצום מחבורה G!) ולכן h^{m-1} הוא ההופכי של h (ב-G) ומתקיים $h^{-1} = h^{m-1} \in H$.

תת חבורה קטנה שמכילה קבוצה

הגדרה: תהי G חבורה ותהי $X \subset G$ תת קבוצה. נאמר כי $X \subset H \leq G$ היא התת-חבורה הקטנה ביותר של G המכילה את X, אם לכל $X \subset S \leq G$ מתקיים $H \leq S$.

כלומר: התת-חבורה הכי קטנה שמכילה קבוצה X היא H אם כל תת-חבורה אחרת S שמכילה את X מכילה את H כתת-חבורה.

לאחר שהגדרנו את המושג, עלינו להוכיח שקיימת H כזו.

טענה: תהי G חבורה, $X \subset G$ תת קבוצה. אז יש תת-חבורה קטנה ביותר של G שמכילה את X.

חבורות ציקליות (מעגליות)

הגדרה 1: תהי G חבורה, ויהי $a \in G$. נגדיר

$< a >= \{a^n | n \in Z\}$ = תת החבורה הציקלית הנוצרת על ידי a.

הגדרה 3: תהי G חבורה. אם קיים $a \in G$ כך שמתקיים $< a >= G$ אזי G נקראת *חבורה ציקלית*, ו-a נקרא *יוצר* של G.

אבחנה: לכל $a \in G$ מתקיים $< a >=< a^{-1} >$.

הגדרה 7 (סדר של איבר בחבורה): תהי G חבורה ויהי $a \in G$. הסדר של a ב-G הוא כמות האיברים ב-$< a >$ (יכול להיות ∞).

למה 9: תהי G חבורה ויהי $a \in G$. אם קיים $k \in Z$ כך ש-k היא החזקה הקטנה ביותר המקיימת $a^k = e$ אזי

$$< a >= \{e, a^1, a^2, \ldots, a^{k-1}\}$$

הוכחה: בהכלה דו כיוונית.

כיוון ראשון: $\{e, a^1, a^2, \ldots a^{k-1}\} \subseteq < a >$ ברור לפי הגדרה.

כיוון שני: $< a > \subseteq \{e, a^1, a^2, \ldots, a^{k-1}\}$: יהי $a^l \in < a >$. לפי משפט החלוקה נרשום $l = q \cdot k + r$ כאשר $0 \leq r < k$. לכן מתקיים

$$a^l = a^{qk+r} = a^{qk} \cdot a^r = (a^k)^q \cdot a^r = e^q \cdot a^r = e \cdot a^r = a^r \in \{e, a^1, \ldots a^{k-1}\}$$ ■

משפט 10: תהי G חבורה ויהי $a \in G$ איבר מסדר סופי (כלומר $|< a >| = m$). אזי m הוא הטבעי הקטן ביותר כך שמתקיים $a^m = e$.

סיכום: אם G חבורה ו-$g \in G$ איבר מסדר n אזי $< g >= \{e, g, g^2, \ldots g^{n-1}\}$. בפרט, אם יש בחבורה G איבר מסדר $|G|$ אזי G ציקלית.

טענה 12: תהי G חבורה ויהי $g \in G$ איבר מסדר n. אזי:

א. $g^k = e \leftrightarrow n|k$

ב. $g^k = g^m \leftrightarrow k \equiv m \ (mod\ n)$

<u>מסקנה 13</u>: תהי $G =< a >$ חבורה מסדר n. אזי $\forall g \in G$, $g^n = e$.

<u>הוכחה</u>: יהי $g \in G$. אזי $g = a^k$ עבור k שלם כלשהו. ולכן מתקיים

$$g^n = (a^k)^n = (a^n)^k = e^k = e$$ ■

<u>טענה</u> (איבר מסדר אינסופי)

תהי G חבורה ויהי $g \in G$ מסדר ∞. אזי:

1) $k = 0 \leftrightarrow g^k = e$

2) $k = m \leftrightarrow g^k = g^m$

3) $< g >= \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ כאשר כל האיברים ברשימה שונים זה מזה.

<u>הוכחה</u>:

1) לפי משפט 10 והוכחתו, אם $g^k = e$ עבור $k > 1$, אזי החל מ-k החזקות מחזוריות, בסתירה לכך שהסדר אינסופי.

2) אם $g^k = g^m$ אזי לפי כלל הצמצום נובע $g^{k-m} = e$.

3) לפי 2). ■