

מבוא לקריפטוגרפיה מודרנית (0368-3049)

נכתב ע"י רון גולדמן
 על הרצאות של פרופ' בני אפלבאום

8 בנובמבר 2025

תוכן העניינים

2	1	מבוא
2	1.1	הגדירות ומושגים ראשוניים
3	1.2	דוגמאות
4	1.3	בטיחות מושלמת
6	2	פסאודו-אקראיות וצפני זרם
6	2.1	בטיחות חישובית
7	2.2	פסאודו-אקראיות
8	2.3	בטיחות למספר ה教导ות
8	2.4	צפני זרם
10	3	נושאים מתוך המספרים והחבורות
10	3.1	נושאים מתוך המספרים
12	3.2	נושאים מתוך החבורות

פרק 1

מבוא

1.1 הגדרות ומושגים ראשוניים

מערכת הצפנה סימטרית

תהיינה קבוצות $\mathcal{K}, \mathcal{M}, \mathcal{C}$

הגדרה 1.1 [**פונקציה הצפנה**]. $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$ את $\forall k \in \mathcal{K}, m \in \mathcal{M}$ נסמן ב- $E_k(m) = E(k, m)$

הגדרה 1.2 [**פונקציה פיענוח**]. $D : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$ את $\forall c \in \mathcal{C}, k \in \mathcal{K}$ נסמן ב- $D_k(c) = D(c, k)$

הגדרה 1.3 [**נכונות**]. לכל הودעה $m \in \mathcal{M}$ ומפתח $k \in \mathcal{K}$ מתקיים $D_k(E_k(m)) = m$

1.1.1 מודל התקשרות

- שני צדדים - אליס וbob
- קו תקשורת אמין
- סכמת הצפנה משותפת: E, D, k .
- מטרה: לשלווח בביטחון הودעה m .

1.1.2 מטרות אבטחה

- אף יריב לא יכול לקבוע את m
- אף יריב לא יכול לקבוע אף אינפורציה לגבי m
- אף יריב לא יכול לקבוע אינפורציה ממשמעותית לגבי m

1.1.3 שאלות חשובות

- מה היריב יודע מראש?
- מה המגבילות החישוביות של היריב?
- האם בכלל אפשר לפורמל מתמטית את מושג הסודיות?

1.1.4 מודל היריב: מАЗין פאסיבי

- איב מנשה לגלוות אינפורציה לגבי m
- איב יודעת את האלגוריתמים E, D (עיקרון קרכחוי)
- איב יודעת את מרחב ההודעות
- איב תפסה את $E_k(m)$
- איב לא יודעת את k

1.2 דוגמאות

דוגמה 1.4 [צופו קיסר]. • מפתח: $.k \in \{0, 1, \dots, 25\}$

- כל אות מיוצגת כמספר $.p \in \{0, 1, \dots, 25\}$
- **הצפנה:** $E_k(p) = p + k \text{ mod } 26$
- **פיענוח:** $D_k(p) = p - k \text{ mod } 26$
- **פתרון:** חיפוש ממצאה.

• **מסקנה:** דרוש מרחב מפתחות גדול.

דוגמה 1.5 [צופו החלפה]. • מפתח: תמורה $\sigma : [26] \hookrightarrow [26]$

- כל אות מיוצגת כמספר $.p \in \{0, 1, \dots, 25\}$
- **הצפנה:** $E_\sigma(p) = \sigma(p)$
- **פיענוח:** $D_\sigma(p) = \sigma^{-1}(p)$

• יש $\approx 4 \cdot 10^{27}$ מפתחות ולכן חיפוש ממצאה לא עובד.

• ניתן לשבור את ההצפנה באמצעות סטטיסטיות של שפה טבעית, שכן התדריות שימוש במילים לא אחידה.

דוגמה 1.6 [צופו ויזיר]. המפתח הוא **:beads**

t	h	e	m	a	n	a	n	d	t	h	e	w	o	m	a	n
b	e	a	d	s	b	e	a	d	s	b	e	a	d	s	b	e
V	M	F	Q	T	P	F	O	H	M	J	J	X	S	F	C	S

- האם הוא מאובטח?
- ויזיר: אני לא מצליח לשבור אותו אז הוא מאובטח.
- קסיסקי (1863): שבר אותו.

1.3 בטיחות מושלמת

1.3.1 התקפה כללית (נראות מירבית)

נניח וליריב יש מידע מקדים על ההודעות, הנთון כהתפלגות M על מרחב ההודעות \mathcal{M} .
בاهינתן סיירטקסט $C = E_k(M) \xleftarrow{R} \mathcal{K}$, עשה:

- פענה לכל מפתח אפשרי:

$$D_{000}(C) = \text{blabla}, D_{001}(C) = \text{lunch}, \dots, D_{111}(C) = \text{attack}$$

- בהתבסס על התפלגות M בחר את ההודעה הכי סבירה

שאלה: האם ניתן להביס זהה יריב?

1.3.2 הגדרה מתמטית של בטיחות

הגדרה 1.7 [פילוגיס שויס]. $X \equiv Y$ עבור התפלגותיות מעל \mathcal{D} אם $\forall d \in \mathcal{D}. \Pr[X = d] = \Pr[Y = d]$.

בטיחות מושלמת

הגדרה 1.8 [בטיחות מושלמת (שאנו 1949)]. מתקיים $M|C \equiv M$.

הגדרה 1.9 [בטיחות - הגדרה אלטרנטיבית]. מתקיים כי לכל $m_0, m_1 \in \mathcal{M}$ באורך זהה, לכל $c \in \mathcal{C}$

$$\Pr_{k \xleftarrow{R} \mathcal{K}}[E_k(m_0) = c] = \Pr_{k \xleftarrow{R} \mathcal{K}}[E_k(m_1) = c]$$

טענה 1.10. ההגדרות שקולות.

1.3.3 דוגמא למערכת בטוחה

הגדרה 1.11 [פינקס חד-פעמי]. • מרחב ההודעות $\mathcal{M} = \{0,1\}^n$.

• מרחב המפתחות $\mathcal{K} = \{0,1\}^n$. המפתח נבחר באקראי.

• כדי להצפין/לפענה נחשב XOR של ההודעה/הטקסט המוצפן עם המפתח:

$$E_k(m) = m \oplus k$$

$$D_k(c) = c \oplus k$$

בטיחות פנקס חד-פעמי

משפט 1.12. לפנקס חד-פעמי יש בטיחות מושלמת.

- **יתרונות:** בטיחות מושלמת.

- **בעיה:** גודל מרחב המפתחות.

הערה 1.13. להשתמש במפתח רק פעם אחד! אחרת נקבל ויז'ר.

נוכיח את משפט 1.12, כלומר, לכל $k \xleftarrow{R} \mathcal{K}$, $E_k(m_0) \equiv E_k(m_1)$ מתקיים $m_0, m_1 \in \{0, 1\}^n$, כאשר

הוכחה. מספיק להוכיח את הטענה הבאה:

טענה 1.14. לכל $m, c \in \{0, 1\}^n$ מתקיים

$$\Pr_{k \xleftarrow{R} \mathcal{K}} [E_k(m) = c] = \frac{1}{2^n} \iff E_k(m) \sim U_n$$

הטענה גוררת את המשפט כי מטרזטיביות שווין החתפנות לכל m מתקיים

$$E_k(m_0) \equiv U_n \equiv E_k(m_1)$$

כעת נוכיח את הטענה.

נקבע $m, c \in \{0, 1\}^n$, אז:

$$\Pr_k [E_k(m) = c] = \Pr_k [m \oplus k = c] = \Pr_k [k = m \oplus c] = \frac{1}{2^n}$$

כי $m \oplus c$ קבוע $.k \sim U_n$

נשים לב שלפנקס חד-פעמי יש מפתחות בגודל הקלט, שהוא נראה מאוד ביבני, אך כעת נראה שהוא הכרחי לבטיחות.

1.3.4 מגבלות של מערכות בטיחות מושלמות

משפט שאנו

משפט 1.15. אם מערכת הצפנה $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}, D : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$ בעלת בטיחות מושלמת, אז $|\mathcal{K}| \geq |\mathcal{M}|$.

הוכחה. נגידר גרף דו-צדדי $G = (V, E)$ כאשר $V = \mathcal{M} \uplus \mathcal{C}$ (בה"כ נזהה אותם כמרחבים שונים) ו- \forall אם ורק אם קיימים $k \in \mathcal{K}$ כך ש- $E_k(m) = c$.

נניח בשילילה כי $|\mathcal{M}| < |\mathcal{K}|$, נקבע $\{m, c\} \in E$.

טענה 1.16. c יכול להיות מחובר לכל היותר ל- $|\mathcal{K}|$ הוודעות, כלומר $\deg(c) \leq |\mathcal{K}|$.

הוכחת הטענה. נניח בשילילה כי $\deg(c) > |\mathcal{K}|$, אז מיעירון שובך היונים יש מפתח k ו- $m_0 \neq m_1$ כך ש- $E_k(m_0) = E_k(m_1)$ וזה סתירה לנכונות ההצפנה.

מסקנה 1.17. קיימת הוודה m^* כך שאינה שכנה של c .

לכל $k \in \mathcal{K}$, $E_k(m^*) \neq c$, ולכן $\Pr_k [E_k(m^*) = c] = 0$.

משמעותו $\Pr_k [E_k(m) = c] \geq \frac{1}{|\mathcal{K}|} > 0$ עבורו $E_k(m) = c$ מושום ו- $\{m, c\} \in E$ אז יש $k' \in \mathcal{K}$ ו- m' בפרט מתקיים כי $E_k(m^*) \neq E_k(m')$ וזה סתירה לבטיחות המושלמת.

פרק 2

פסאודו-אקראיות וצפוני זרם

2.1 בטיחות חישובית

הגדרה 2.1 [בטיחות מושלמת כמשחק]. המערה $(\mathcal{A}, \mathcal{C})$ היא מושלמת אם לכל יריב $\mathcal{A} : \mathcal{C} \rightarrow \{0, 1\}$ ולכל $m_0, m_1 \in \mathcal{M}$ $\Pr[\mathcal{A}(m_0) = 1] = \Pr[\mathcal{A}(m_1) = 1]$ כאשר $\mathcal{C} \sim \text{Un}(\mathcal{K})$.

$$\Pr[\mathcal{A}(c_0) = 1] = \Pr[\mathcal{A}(c_1) = 1]$$

בטיחות חישובית (גולדוזסר ומיקלי 1982)

הגדרה 2.2 [כטיחות חישובית]. המערה (E, D) היא כטיחת חישובית אם לכל אוג של הודעות שונות $m \in \mathcal{M}$ באורך k שווה, ה- c_0, c_1 ciphertexts ניידים להבחנה עבור יריב עם כוח חישובי חסום. כלומר, עבור $c_0 = E_k(m_0), c_1 = E_k(m_1)$ ו- $k \xleftarrow{R} \mathcal{K}$:

$$|\Pr[\mathcal{A}(c_0) = 1] - \Pr[\mathcal{A}(c_1) = 1]| < \varepsilon$$

לכל יריב $\mathcal{A} : \mathcal{C} \rightarrow \{0, 1\}$ בסיבוכיות לכל היותר t .

הגדרה 2.3 [סיבוכיות ייריב]. גודל המעגל הקטן ביותר שמחשב את היריב \mathcal{A} .

הערה 2.4. זהו מודל לא יוניפורמי.

הגדרה 2.5 [יתרונות האבחנה של \mathcal{A}]. גין X ל- Y אם $\mathcal{A} : \mathcal{D} \rightarrow \{0, 1\}$ מעלה תחום \mathcal{D} ויריב \mathcal{A} נגידיר

$$\Delta_{\mathcal{A}}(X, Y) = |\Pr[\mathcal{A}(X) = 1] - \Pr[\mathcal{A}(Y) = 1]|$$

הגדרה 2.6 [טיפוח סינטטי]. $\Delta_{\mathcal{A}}(X, Y) \leq \varepsilon$ אם $X \approx_{t, \varepsilon} Y$ ו- $t = |\mathcal{A}|$ מתקיים $X \approx_{\infty, 0} Y$ אם $X \equiv Y$.

הערה 2.7. $X \approx_{\infty, 0} Y \iff X \equiv Y$.

הגדרה 2.8 [כטיחות סינטטית - לא פורמלי]. "כל מה שאתה יכול לחשב בצורה ייעילה בהינתן ה- c ciphertexts אתה יכול גם בלי".

משפט 2.9. בטיחות סמנטיבית שקופה לבטיחות חישובית.

2.2 פסאודו-אקראיות

הגדעה 2.10 [פינקט חד-פעמי חישובי].

- נבחר מפתח אקראי קצר $k \xleftarrow{R} \mathcal{K}$ (זרע)
- נרchieב למפתח ארוך עם זרם מפתח $G(k)$
- נצפין את m עם $c = G(k) \oplus m$
- נפענח את c ל- $m = c \oplus G(k)$

מה צריך G לקיים כדי שנוביל בטיחות חישובית?

הגדעה 2.11 [מחולל פסאודו-אקראיות]. פונקציה חשיבה פולינומית ℓ , אשר מקיימת עבור $k \xleftarrow{R} \{0,1\}^n$, $G : \{0,1\}^n \rightarrow \{0,1\}^\ell$, אשר מוגדרת על ידי $y_1 = G(k)$ אז $y_0 = y_{t,\varepsilon} \approx y_1$. נאמר כי G היא (t, ε) פסאודו-אקראית.

הערה 2.12. הפלט של G לא יכול להיות אקראי לחלווטין!

בטיחות פנקס חד-פעמי חישובי

משפט 2.13. אם (t, ε) פסאודו-אקראי, אז "הפנקס חד-פעמי החישובי" הוא $(t - \ell, 2\varepsilon)$.

טענה 2.14. אם f פונק' בסיבוכיות ℓ או $f(X) \approx_{t-\ell+\varepsilon} f(Y)$

טענה 2.15. אם $X \approx_{t,\varepsilon_1+\varepsilon_2} Z$ אז $X \approx_{t,\varepsilon_1} Y \approx_{t,\varepsilon_2} Z$

הוכחת המשפט. יהיו $t' = t - \ell, \varepsilon' = 2\varepsilon$, $(\text{PRG}(\mathcal{U}_n) \oplus m_0) \approx_{t', \varepsilon'} (\text{PRG}(\mathcal{U}_n) \oplus m_1)$, $m_0, m_1 \in \mathcal{M}$, צריך להוכיח כי $\text{PRG}(\mathcal{U}_n) \oplus m \approx_{t', \varepsilon'} \mathcal{U}_\ell \oplus m$.

טענה 2.16. מטריצטיביות נסיק כי $(\text{PRG}(\mathcal{U}_n) \oplus m_0) \approx_{t', \varepsilon'} (\text{PRG}(\mathcal{U}_n) \oplus m_1)$.

■ הוכחת הטענה. נב"ש כי קיים יריב \mathcal{A} בסיבוכיות t' כך ש- $\varepsilon > \Delta_{\mathcal{A}}(\text{PRG}(\mathcal{U}_n) \oplus m_0, \mathcal{U}_\ell \oplus m)$, נתאר יריב \mathcal{A}' ששובר את ה- PRG .

$\Delta_{\mathcal{A}'}(\text{PRG}(\mathcal{U}_n), \mathcal{U}_\ell) = \Delta_{\mathcal{A}}(\text{PRG}(\mathcal{U}_n) \oplus m, \mathcal{U}_\ell \oplus m) > \varepsilon$, וכך ניתן לראות (הוכחה לבית) כי $\Delta_{\mathcal{A}'}(\text{PRG}(\mathcal{U}_n), \mathcal{U}_\ell) > \varepsilon$, כלומר \mathcal{A}' הצליח לשבור את הסיבוכיות של \mathcal{A} .

האובייקט של PRGs הוא מרכזי בתורת הקרייפטוגרפיה. נשים לב שגם $P = NP$ או אין PRGs (עבור יריבים בזמן פוליאי):

$$L = \{z : \exists x \text{ } \text{PRG}(x) = z\} \in NP$$

از הקיום של PRGs יכול רק להיות משוער עד ש- $P \neq NP$.

יש לנו סיבות טובות להאמין בכך.

להרבה מועמדים ידועים הבטיחות מתקובלת מרדווקציה של בעיות קשות. יתרה מכך, אפשר לבסס ש-PRGs ניתן לבנות מפונקציות חד-כיווניות.

2.3 בטיחות למספר הודעות

בטיחות חישובית למספר הודעות

הגדרה 2.17 [בטיחות חישובית (t, ε) למספר הודעות]. לכל אוג וקטורים $\vec{x}, \vec{y} \in \mathcal{M}^n$. לכל k ו| |
| --- |
| עבור $\mathcal{K} \xleftarrow{R} \mathcal{K}$, אזי |

$$\vec{c}_0 = (E_k(x_1), \dots, E_k(x_n)) \approx_{t, \varepsilon} (E_k(y_1), \dots, E_k(y_n)) = \vec{c}_1$$

הערה 2.18. ראיינו סכמאות הצפנה שבוטוחות להודעות בודדות, מסתבר שזה הכלרי.

אין בטיחות למספר הודעות בהצפנה דטרמיניסטית

משפט 2.19. אם אלגוריתם הצפנה הוא פונקציה דטרמיניסטית אשר תליה בהודעה m ובפתח k בלבד, אזי הוא לא בטוח למספר הודעות (אפילו שתיים).

הוכחה. יהיו $a, b \in \mathcal{M}$ שונים ובאורך זהה. אזי עבור

$$\begin{aligned}\vec{x} &= (a, a) \\ \vec{y} &= (a, b)\end{aligned}$$

מתקיים לכל $k \in \mathcal{K}$ כי $\vec{c}_1 = (E_k(a), E_k(b))$ וכן $\vec{c}_0 = (E_k(a), E_k(a))$ 噫. יריב שבודק שווין בין האיברים בטקסט המוצפן, אזי:

$$\Pr_k[\mathcal{A}(\vec{c}_0) = 1] = 1 \neq 0 = \Pr_k[\mathcal{A}(\vec{c}_1) = 1]$$

ולכן בפרט הם ניתנים להבדלה לכל $\varepsilon \in [0, 1]$, ולכן המערכת לא בטוחה חישובית למספר הודעות. ■

2.4 צפני זרם

2.4.1 הצפנה בטוחה למספר הודעות

תהא (E, D) מערכת הצפנה בטוחה להודעה אחת. נבנה סכמה חדשה:

- אתחול $S \xleftarrow{R} \mathcal{K}$.
- נצפין הודעה m עם מצב S :
נבחר מפתח חדש $S' \xleftarrow{R} \mathcal{K}$, נשלח $E_S(m, S')$ ונפלוט m .
נעדכן את המצב ל- S' .
- נפענח את הטקסט המוצפן עם מצב S :
נחשב $D_S(c) = (m, S')$ ונפלוט m .
נעדכן את המצב החדש ל- S' .

2.4.2 צפוי זרם סינכרוניים

- נניח $\mathcal{K} \xleftarrow{R} S_0$ מצב התחלתי.
- כדי להציג את הבית $-i$ בהודעה m_i נבצע:
 - $(b_i, S_{i+1}) \leftarrow \text{PRG}(S_i)$ -
 - $c_i = m_i \oplus b_i$ -
- בעיה:** מה קורה אם בית אחד נעלם בהעברת ההודעה?
- אידיאלית נרצה רובסטיות כנגד איבוד מידע.

2.4.3 צפוי זרם א-סינכרוניים

- נתהיל מפתח אקראי $k \xleftarrow{R} \mathcal{K}$
- נייצר זרם מפתח על הkey
- הבית $-i$ הוא פונקציה של המפתח הסודי ושל t הביטים האחרונים של הצופן, $(c_{i-t}, \dots, c_{i-1}) = \text{public state}$
- בפרט, ההצפנה היא $c_i = m_i \oplus h(k, c_{i-t}, \dots, c_{i-1})$
- באשר הפענוח הוא $m_i = c_i \oplus h(k, c_{i-t}, \dots, c_{i-1})$

פרק 3

נושאים מתורת המספרים והחברות

3.1 נושאים מתורת המספרים

3.1.1 חילוק

הגדרה 3.1 [חלוקת]. יהיו $a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$. נאמר כי a מחלק את b (סימן $a|b$) אם קיימים $d \in \mathbb{Z}$ כך ש-

טענה 3.2. יהיו $a, b \in \mathbb{Z}$, $m \in \mathbb{Z} \setminus \{0\}$. אז לכל $\alpha, \beta \in \mathbb{Z}$ מתקיים $m|\alpha a + \beta b$.

משפט 3.3 [החלוקת]. לכל $a, n \in \mathbb{Z}$ קיימים ויחידים מנה $q \in \mathbb{Z} \cap [0, n]$ ושארית r כך ש-

הגדרה 3.4 [מודולו]. לכל $a, n \in \mathbb{Z}$ $a \bmod n = r$, כאשר r השארית המשפט החלוקת.

הגדרה 3.5 [יחס השקילות המודולרי]. עבור $a, b \in \mathbb{Z}$ מתקיים $a \equiv b \pmod{n}$ אם או באופן שקול $n|a - b$.

3.1.2 מחלק משותף גדול ביותר

הגדרה 3.6 [GCD]. המחלק המשותף הגדול ביותר של $a, b \in \mathbb{Z}$ הוא

$$\gcd(a, b) = \max\{d \in \mathbb{N} : d|a \wedge d|b\}$$

לפי הקובונציה $a \geq 0$ $\gcd(a, 0) = a$ עבור

אלגוריתם 3.7 [אלגוריתם אוקליידס לחישוב $\gcd(a, b)$]. עבור $a \geq b$:

• אם $b = 0$ אז תוצאה a

• אחרת, תוצאה $\gcd(b, a \bmod b)$

כוננות. נסמן $r = a \bmod b$, נוכיח כי המחלקים המשותפים של (a, b) זהים ולכן גם הגדול ביותר, כלומר $\gcd(b, a \bmod b) = \gcd(b, r)$.

$r = \alpha a + \beta b$: יהיו $d|r \wedge d|b \iff d|a \wedge d|b$ עבור $d|r$ מחלק משותף של a ו- b , צריך להראות כי $d|a$. משפט החלוקת כיוון $d|r$, כלומר $d|a$ ו- $d|b$.

$\alpha = q, \beta = 1$, $\beta = -q$ מטענה 3.2 מתקיים כי $d|r$ עבור $d|a + bq + r = a$, צריך להראות כי $d|a$. משפט החלוקת כיוון $d|r$ מתקיים כי $d|a$.

סיבוכיות. מבצעים $O(\log(a+b))$ רדוקציות מודולריות.

משפט 3.8. יהיו $a, b \in \mathbb{Z}$ ונגדיר $S_{a,b} = \{\alpha a + \beta b : \alpha, \beta \in \mathbb{Z}\}$. אז:

1. לכל $x \bmod y \in S_{a,b}$ מתקיים $x, y \in S_{a,b}$.

$$\min(S_{a,b} \cap \mathbb{N}_{>0}) = \gcd(a, b) \quad .2$$

הוכחה. נוכחת:

1. יהיו $x, y \in S_{a,b}$ اي יש $x = \alpha_1 a + \beta_1 b, y = \alpha_2 a + \beta_2 b$ כך ש- $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}$. לכן ממשפט החלוקה:

$$\alpha_1 a + \beta_1 b = q(\alpha_2 a + \beta_2 b) + x \bmod y$$

$$\iff x \bmod y = (\alpha_1 - q\alpha_2)a + (\beta_1 - q\beta_2)b \in S_{a,b}$$

2. נסמן $s = \min(S_{a,b} \cap \mathbb{N}_{>0})$, נראה כי זהו ה-GCD.

s הוא מחלק משותף: מהגדרת [3.2](#), $a \in S_{a,b}$, $a \bmod s \in S_{a,b}$, וכך לפי סעיף

ממשפט החלוקה $a \bmod s < s$ והוא אי שלילי וקטן ממש מ- s , לכן מהגדרת s קיבל כי

$$s \mid a \bmod s = 0$$

אותו טיעון תקף גם על b וכן $s \mid b$, בפרט הוא מחלק משותף.

s הוא הנadol biyoter:ippi. $d \leq s$ כי $d \mid s$ ומכאן מטענה [3.2](#) מתקיים כי $d \mid s$, משום ש- $s > 0$ כי $d < s$.

הגדרה 3.9 [זרות]. נאמר כי $a, b \in \mathbb{Z}$ הם זרים אם $\gcd(a, b) = 1$.

מסקנה 3.10. מספר מסקנות:

1. אם $d \mid \gcd(a, b)$ אז $d \mid a \wedge d \mid b$.

2. לכל $m \in \mathbb{Z} \setminus \{0\}$ $\gcd(ma, mb) = |m| \gcd(a, b)$.

3. אם זרים אם ורק אם קיימים $a, b \in \mathbb{Z}$ עבורם $xa + yb = 1$ מתקבלת הרחבה של אלגוריתם אוקלידי.

лемה 3.11 [הLemma של אוקלידי]. אם $a \mid cb$ וגם $\gcd(b, c) = 1$ אז $a \mid c$.

3.1.3 מספרים ראשוניים ופירוק

הגדרה 3.12 [מספר ראשוני]. מספר שלם $P \in \mathbb{Z}$ הוא ראשוני אם לכל $a \in \mathbb{Z}$ כז ש- $a \mid P$ אם ורק אם $a \in \{1, P\}$. אם מספר הוא לא ראשוני אי הוא פריך.

המשפט היסודי של האריתמטיקה

משפט 3.13 [פירוק ייחיד]. יהיו $X \in \mathbb{Z}$, $1 < X \in \mathbb{Z}$, איז קיימים יחידים ראשוניים P_1, \dots, P_k כז ש-

$$X = P_1 \cdots P_k$$

3.2 נושאים מתורת החבירות

3.2.1 חבירות

הגדירה 3.14 [חכורה]. קבוצה לא ריקה G ייחד עם פעולה בינארית \oplus נקראת **חבורה אם**

1. **סגירות תחת \oplus :** לכל $a, b \in G$ מתקיים

$$(a \oplus b) \oplus c = a \oplus (b \oplus c) \quad a, b, c \in G$$

3. **קיום איבר ניטרלי:** קיים $e \in G$ כך שלכל $a \in G$ מתקיים

$$a \oplus e = a \quad a \in G$$

4. **קיום הופכי:** לכל $a \in G$ קיים $a^{-1} \in G$ כך ש-

חבורה נקראת **קומוטטיבית** או **אבלית** אם לכל $a, b \in G$ מתקיים

$$a \oplus b = b \oplus a \quad a, b \in G$$

ובור חבורה סופית G , גודל החבורה $|G|$ נקרא **הסדר** של החבורה.

דוגמה 3.15. $\{0, \dots, n-1\} = \mathbb{Z}_n$ היא חבורה חיבורית ביחס לחברות מודולו n (מסומן $+_n$).

טענה 3.16 [היה חסר בתרגום]. לכל חבורה (G, \oplus) קיים איבר ניטרלי יחיד $e \in G$

הוכחה. יהיו $e_1, e_2 \in G$ איברים ניטרליים, מכך ש- $e_2 \oplus e_1 = e_1$ אז $e_1 \oplus e_2 = e_2$ ולכן e_1 ניטרלי, מכאן כי

■ $e_1 = e_2$, אך מכך ש- e_1 ניטרלי $e_2 \oplus e_1 = e_2$ ולכן $e_2 = e_1$.

מסקנה 3.17 [גס לא היה]. לכל $a \in G$, $a \oplus a = a$

3.2.2 תת-חברות

הגדירה 3.18 [**תת-חכורה**]. תהא (G, \oplus) חבורה. $H \subseteq G$ היא **תת-חבורה של (G, \oplus)** אם היא חבורה וגם

טענה 3.19. תהא (H, \oplus) חבורה סופית, ותהא $H \subseteq G$. אז H סגורה תחת \oplus , אז (H, \oplus) היא **תת-חבורה של (G, \oplus)** .

דוגמה 3.20. $(\{0, 2, 4, 6\}, +_8)$ היא תת חבורה של $(\mathbb{Z}_8, +_8)$.

טענה 3.21 [תכונות של תת-חברות]. תהא (G, \oplus) חבורה ו- (H, \oplus) תת-חבורה שלה. אז:

- אם e איבר ניטרלי ב- G אז הוא גם ניטרלי ב- H .

- a^{-1} ההופכי של a ב- H אם ורק אם הוא ההופכי של a ב- G .

משפט לגורנץ'

משפט 3.22 [לגורנץ']. אם (G, \oplus) חבורה סופית ו- (H, \oplus) תת-חבורה שלה, אז $|H|$ מחלק את $|G|$.

3.2.3 העלאה בחזקה

הגדירה 3.23. לכל $a \in G$, $k \in \mathbb{Z}$ נגדיר:

$$a^k \triangleq \begin{cases} \bigoplus_{i=1}^k a, & k > 0 \\ e, & k = 0 \\ (a^{-1})^{-k}, & k < 0 \end{cases}$$

טענה 3.24 [תכונות]. לכל $a \in G$ ו- $k, m \in \mathbb{Z}$

$$a^k \oplus a^m = a^{k+m} \quad \bullet$$

$$(a^k)^m = a^{km} \quad \bullet$$

שאלה 3.25 [סיכוןיות]. בהינתן $a \in G$ ו- $k \in \mathbb{Z}$, כמה פעולות כפל דרושות כדי לחשב את a^k ? באמצעות העלאה חוזרת בריבוע.

בעיה 3.26 [כעיה הלוג הדיטרטי]. בהינתן $G \in a, y \in G$, צריך למצוא $k \in \mathbb{Z}$ כך ש- $y = a^k$.

בעיה 3.27 [חולוץ שורש $[k]$]. בהינתן $G, k \in \mathbb{Z}, y \in G$, צריך למצוא $a \in G$ כך ש- $y = a^k$.

עבור חברות מסוימות מאמינים שהבעיות הללו קשות.

3.2.4 הסדר של איברים בחבורה וחברות ציקליות

הגדרה 3.28 [סדר של איבר]. הסדר של איבר a בחבורה G הוא $n \in \mathbb{Z}^+$ המינימלי עבורו $a^n = e$

טענה 3.29. הקבוצה $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$ היא תת-חבורה של G עם $\text{order}(a) = a^1, \dots, a^{\text{order}(a)}$ איברים שונים

הגדרה 3.30 [חבורה ציקלית]. חבורה G נקראת **ציקלית** אם קיים $a \in G$ כך ש- $a, G = \langle a \rangle$, ו- a נקרא **יוצר** של החבורה.

מסקנה 3.31. תהא (G, \oplus) חבורה סופית.

- לכל $a \in G$ מתקיים כי $\text{order}(a)$ מחלק את $|G|$.

- אם $|G|$ ראשוןוי אז G ציקלית, וכן כל $a \in G \setminus \{e\}$ יוצר שלה.

- לכל $a \in G$ מתקיים $a^{|G|} = e$.

- לכל $a \in G$ ו- $k \in \mathbb{Z}$ מתקיים $a^k = a^{k \bmod |G|} = a^{k \bmod \text{order}(a)}$

- לכל $k \in \mathbb{Z}$, עלות החישוב של a^k היא $O(\log|G|)$ מכפלות.