מבוא לקריפטוגרפיה מודרנית (0368-3049)

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

10 בנובמבר 2025

תוכן העניינים

פרק 1

מבוא

1.1 הגדרות ומושגים ראשונים

מערכת הצפנה סימטרית

תהינא קבוצות $\mathcal{K}, \mathcal{M}, \mathcal{C}$.

הגדרה 1.1 [פונקציית הצפנה]. $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$, לכל $k \in \mathcal{K}, m \in \mathcal{M}$ נסמן ב-$E_k(m) = E(k,m) = c$ את ה-**ciphertext**.

הגדרה 1.2 [פונקציית פיענוח]. $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$, לכל $k \in \mathcal{K}, c \in \mathcal{C}$ נסמן ב-$D_k(c) = D(k,c) = m$ את ה-**plaintext**.

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

1.1.1 מודל התקשורת

- שתי צדדים - אליס ובוב
- קו תקשורת אמין
- סכמת הצפנה משותפת: E, D, k.
- מטרה: לשלוח בבטיחות הודעה 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 משמעותית לגבי m

1.1.3 שאלות חשובות

- מה היריב יודע מראש?
- מה המגבלות החישוביות של היריב?
- **האם בכלל אפשר לפרמל מתמטית את מושג הסודיות?**

1.1.4 מודל היריב: מאזין פאסיבי

- איב מנסה לגלות אינפורציה לגבי m
- איב יודעת את האלגוריתמים E, D (עיקרון קרכהוף)
- איב יודעת את מרחב ההודעות
- איב תפסה את $E_k(m)$
- איב לא יודעת את k

1.2 דוגמאות

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

- כל אות מיוצגת כמספר $p \in \{0, 1, \dots, 25\}$.
- הצפנה: $E_k(p) = p + k \bmod 26$.
- פיענוח: $D_k(p) = p - k \bmod 26$.
- פתרון: חיפוש ממצה.
- מסקנה: דרוש מרחב מפתחות גדול.

דוגמה 1.5 [צופן 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 $26! \approx 4 \cdot 10^{27}$ מפתחות ולכן חיפוש ממצה לא יעבוד.
- ניתן לשבור את ההצפנה באמצעות סטטיסטיקות של שפה טבעית, שכן התדירות שימוש במילים לא אחידה.

דוגמה 1.6 [צופן ויז'נר]. 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?
- ויז'נר: אני לא מצליח לשבור אותו אז הוא מאובטח.
- קסיסיקי (1863): שבר אותו.

1.3 בטיחות מושלמת

1.3.1 התקפה כללית (נראות מירבית)

נניח ולריב יש מידע מקדים על ההודעות, הנתון כהתפלגות M על מרחב ההודעות $\mathcal{M}$.
בהינתן סייפרטקסט $\mathcal{K} \xleftarrow{R} C = E_k(M)$, עשה:

- פענח לכל מפתח אפשרי:

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

- בהתבסס על ההתפלגות M בחר את ההודעה הכי סבירה

שאלה: האם ניתן להביס כזה יריב?

1.3.2 הגדרה מתמטית של בטיחות

הגדרה 1.7 [פילוגים שווים]. $X \equiv Y$ עבור התפלגויות מעל $\mathcal{D}$ אם $\forall d \in \mathcal{D}.\ \Pr[X = d] = \Pr[Y = d]$.

בטיחות מושלמת

הגדרה 1.8 [בטיחות מושלמת (שאנון 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 [פנקס חד-פעמי].

- מרחב ההודעות $\mathcal{M} = \{0,1\}^n$
- מרחב המפתחות $\mathcal{K} = \{0,1\}^n$. המפתח נבחר באקראי.
- כדי להצפין/לפענח נחשב XOR של ההודעה/הטקסט המצופן 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.

- יתרון: בטיחות מושלמת.
- בעיה: גודל מרחב המפתחות.

הערה 1.13 להשתמש במפתח רק פעם אחת! אחרת נקבל ויז'נר.

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

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 מטרנזטיביות שוויון ההתפלגות לכל $m_0, m_1 \in \{0,1\}^n$ מתקיים

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

כעת נוכיח את הטענה.

נקבע $m, c \in \{0,1\}^n$, אזי:

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

כי $m \oplus c$ קבוע ו-$k \sim U_n$. ■

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

1.3.4 מגבלות של מערכות בטוחות מושלם

משפט שאנון

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

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

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

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

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

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

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

משום ש-$\{m, c\} \in E$ אזי יש $k' \in \mathcal{K}$ עבורו $E_{k'}(m) = c$ ולכן $\Pr_k[E_k(m) = c] \geq \frac{1}{|\mathcal{K}|} > 0$.

בפרט מתקיים כי $E_k(m^*) \not\equiv E_k(m)$ וזו סתירה לבטיחות המושלמת. ■

פרק 2

פסאודו-אקראיות וצפני זרם

2.1 בטיחות חישובית

הגדרה 2.1 [בטיחות מושלמת כמשחק]. לכל יריב $\mathcal{A}:\mathcal{C}\to\{0,1\}$, ולכל $m_0,m_1\in\mathcal{M}$ ו-$k\sim\mathrm{Un}(\mathcal{K})$ כאשר $c_0=E_k(m_0),c_1=E_k(m_1)$ מתקיים:

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

בטיחות חישובית (גולדווסר ומיקלי 1982)

הגדרה 2.2 [בטיחות חישובית]. המערכת (E,D) **בטוחה חישובית** (t,ε) אם לכל זוג של הודעות שונות $m_0,m_1\in\mathcal{M}$ באורך שווה, ה-ciphertexts c_0,c_1 צריכות להיות לא ניתנים להבחנה עבור יריב עם כוח חישובי חסום.
כלומר, עבור $k\xleftarrow{R}\mathcal{K}$ ו-$c_0=E_k(m_0),c_1=E_k(m_1)$:

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

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

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

הערה 2.4. זהו מודל לא יוניפורמי.

הגדרה 2.5 [יתרון האבחנה של $\mathcal{A}$ בין X ל-Y]. עבור זוג פילוגים X,Y מעל תחום $\mathcal{D}$ ויריב $\mathcal{A}:\mathcal{D}\to\{0,1\}$ נגדיר

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

הגדרה 2.6 X,Y **הם** (t,ε) **לא ניתנים להבחנה].** $X\approx_{t,\varepsilon}Y$ אם $\forall|\mathcal{A}|=t$ מתקיים $\Delta_{\mathcal{A}}(X,Y)\le\varepsilon$.

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

הגדרה 2.8 [בטיחות סמנטית - לא פורמלי]. "כל מה שאתה יכול לחשב בצורה יעילה בהינתן ה-ciphertext אתה יכול גם בלי".

משפט 2.9. בטיחות סמנטית שקולה לבטיחות חישובית.

2.2 פסאודו-אקראיות

הגדרה 2.10 [פנקס חד-פעמי חישובי].

- נבחר מפתח אקראי קצר $k \xleftarrow{R} \mathcal{K}$ (זרע)
- נרחיב 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 שנקבל בטיחות חישובית?

הגדרה 2.11 [מחולל פסאודו-אקראיות]. פונקציה חשיבה פולינומית $G : \{0,1\}^n \to \{0,1\}^\ell$, $\ell \gg n$, אשר מקיימת עבור $k \xleftarrow{R} \{0,1\}^n$ ו-$y_1 \xleftarrow{R} \{0,1\}^\ell$, כי אם $y_0 = G(k)$ אז $y_0 \approx_{t,\varepsilon} y_1$. נאמר כי G היא (t,ε) **פסאודו-אקראית**.

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

בטיחות פנקס חד-פעמי חישובי

משפט 2.13. אם $\mathrm{PRG} : \{0,1\}^n \to \{0,1\}^\ell$ (t,ε) פסאודו-אקראי, אז "הפנקס חד-פעמי החישובי" הוא $(t-\ell, 2\varepsilon)$ בטוח.

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

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

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

טענה 2.16. $\mathcal{U}_\ell \equiv \mathcal{U}_\ell \oplus m \approx_{t',\varepsilon} \mathrm{PRG}(\mathcal{U}_n) \oplus m$.

מטרנזטיביות נסיק כי $(\mathrm{PRG}(\mathcal{U}_n) \oplus m_1) \approx_{t',\varepsilon'} (\mathrm{PRG}(\mathcal{U}_n) \oplus m_0)$. ■

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

$\mathcal{A}'(z) = \mathcal{A}(z \oplus m)$, וקל לראות (הוכחה לבית) כי $\Delta_{\mathcal{A}'}(\mathrm{PRG}(\mathcal{U}_n), \mathcal{U}_\ell) = \Delta_{\mathcal{A}}(\mathrm{PRG}(\mathcal{U}_n) \oplus m, \mathcal{U}_\ell \oplus m) > \varepsilon$.
הסיבוכיות של $\mathcal{A}'$ היא לכל היותר $t' + \ell = t$ ולכן קיבלנו סתירה.

האובייקט של PRGs הוא מרכזי בתורת הקריפטוגרפיה.
נשים לב שאם $\mathrm{P} = \mathrm{NP}$ אז אין PRGs (עבור יריבים בזמן פולי'):

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

אז הקיום של PRGs יכול רק להיות משוער עד ש- Pvs.NP.
יש לנו סיבות טובות להאמין שכן.
להרבה מועמדים ידועים הבטיחות מתקבלת מרדוקציה 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 זוג וקטורים $\vec{x},\vec{y}\in\mathcal{M}^n$ של הודעות באורך שווה $|x_i|=|y_i|$, עבור $\mathcal{K}\xleftarrow{R}k$, 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. ראינו סכמות הצפנה שבטוחות להודעות בודדות, מסתבר שזה הכרחי.

אין בטיחות למספר הודעות בהצפנה דטרמיניסטית

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

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

$$\vec{x}=(a,a)$$
$$\vec{y}=(a,b)$$

מתקיים לכל $k\in\mathcal{K}$ כי $\vec{c}_0=(E_k(a),E_k(a))$ וכן $\vec{c}_1=(E_k(a),E_k(b))$.
יהי $\mathcal{A}:\mathcal{C}\to\{0,1\}$ יריב שבודק שוויון 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 $\mathcal{K}\xleftarrow{R}S$.
- נצפין הודעה m עם מצב S:
  נבחר מפתח חדש $\mathcal{K}\xleftarrow{R}S'$, נשלח $E_S\left(m,S'\right)$.
  נעדכן את המצב ל- S'.
- נפענח את הטקסט המוצפן עם מצב S:
  נחשב $D_S(c)=\left(m,S'\right)$ ונפלוט m.
  נעדכן את המצב החדש ל- S'.

2.4.2 צפני זרם סינכרוניים

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

2.4.3 צפני זרם א-סינכרוניים

- נתחיל ממפתח אקראי $k \xleftarrow{R} \mathcal{K}$
- נייצר זרם מפתח על הקו
- הביט ה-i הוא פונקציה של המפתח הסודי ושל t הביטים האחרונים של הצופן, $\text{public state} = (c_{i-t}, \ldots, c_{i-1})$.
- בפרט, ההצפנה היא $c_i = m_i \oplus h\left(k, c_{i-t}, \ldots, c_{i-1}\right)$
- באשר הפענוח הוא $m_i = c_i \oplus h\left(k, c_{i-t}, \ldots, c_{i-1}\right)$

פרק 3

נושאים מתורת המספרים והחבורות

3.1 נושאים מתורת המספרים

3.1.1 חילוק

הגדרה 3.1 [חלוקה]. יהיו $a \in \mathbb{Z} \setminus \{0\}, b \in \mathbb{Z}$, נאמר כי a **מחלק את** b (סימון $a|b$) אם קיים $d \in \mathbb{Z}$ כך ש-$b = da$.

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

משפט 3.3 [החלוקה]. לכל $a, n \in \mathbb{Z}$ קיימים ויחידים **מנה** $q \in \mathbb{Z}$ **ושארית** $r \in \mathbb{Z} \cap [0, n)$ כך ש-$a = nq + r$.

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

הגדרה 3.5 [יחס השקילות המודולרי]. עבור $a, b \in \mathbb{Z}$ מתקיים $a \equiv b \pmod n$ (או $a =_n b$) אם $a \bmod n = b \bmod n$ 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 הקונבנציה $\gcd(a, 0) = a$ עבור $a \geq 0$.

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

- אם $b = 0$ אז תוציא a
- אחרת, תוציא $\gcd(b, a \bmod b)$

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

<u>$d|a \wedge d|b \Longleftarrow d|r \wedge d|b$:</u> יהי d מחלק משותף של a ו-b, צריך להראות כי $d|r$. ממשפט החלוקה $r = a - bq$, כלומר $r = \alpha a + \beta b$ עבור $\alpha = 1, \beta = -q$ ולכן מטענה 3.2 מתקיים כי $d|r$.

<u>$d|a \wedge d|b \Longrightarrow d|r \wedge d|b$:</u> יהי d מחלק משותף של b ו-r, צריך להראות $d|a$. ממשפט החלוקה $a = bq + r$, ולכן עבור $\alpha = q, \beta = 1$ מטענה 3.2 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 $x,y\in S_{a,b}$ מתקיים $x \bmod y\in S_{a,b}$.
2. $\min(S_{a,b}\cap\mathbb{N}_{>0})=\gcd(a,b)$.

הוכחה. נוכיח:

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

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

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

s הוא מחלק משותף: מהגדרת $S_{a,b}$ $a\in S_{a,b}$, לכן לפי סעיף 3.2, $a \bmod s\in S_{a,b}$.
ממשפט החלוקה $0\le a \bmod s<s$ ולכן $a \bmod s$ הוא אי שלילי וקטן ממש מ-s, לכן מהגדרת s נקבל כי $a \bmod s=0$, כלומר $s|a$.
אותו טיעון תקף גם על b ולכן $s|a\wedge s|b$, בפרט הוא מחלק משותף.

s הוא הגדול ביותר: יהי $0<d\in\mathbb{Z}$ כך ש-$d|a\wedge d|b$, $s\in S_{a,b}$ ולכן מטענה 3.2 מתקיים כי $d|s$, משום ש-$d,s>0$ אזי $d\le s$.

■

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 $d|a\wedge d|b$ אז $d|\gcd(a,b)$.
2. לכל $m\in\mathbb{Z}\setminus\{0\}$, $\gcd(ma,mb)=|m|\gcd(a,b)$.
3. a ו-b הם זרים אם ורק אם קיימים $a,b\in\mathbb{Z}$ עבורם $xa+yb=1$. ניתן למצוא את x,y מתוך הרחבה של אלגוריתם אוקלידס.

למה 3.11 [הלמה של אוקלידס]. אם $a|cb$ וגם $\gcd(b,c)=1$ אז $c|a$.

3.1.3 מספרים ראשוניים ופירוק

הגדרה 3.12 [מספר ראשוני]. מספר שלם $1<P\in\mathbb{Z}$ הוא **ראשוני** אם לכל $a\in\mathbb{Z}$ כך ש-$a|P$ מתקיים $a\in\{1,P\}$. אם מספר הוא לא ראשוני אזי הוא **פריק**.

המשפט היסודי של האריתמטיקה

משפט 3.13 יהי $1<X\in\mathbb{Z}$, אזי קיימים ויחידים ראשוניים $P_1\le P_2\le\ldots\le P_k$ כך ש-

$$X=P_1\cdots P_k.$$

3.2 נושאים מתורת החבורות

3.2.1 חבורות

הגדרה 3.14 [חבורה]. קבוצה לא ריקה G יחד עם פעולה בינארית $\oplus$ נקראת **חבורה** אם

1. **סגירות תחת $\oplus$:** לכל $a, b \in G$ מתקיים $a \oplus b \in G$.
2. **אסוציאטיביות:** לכל $a, b, c \in G$ $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **קיום איבר ניטרלי:** קיים $e \in G$ כך שלכל $a \in G$ מתקיים $a \oplus e = a$.
4. **קיום הופכי:** לכל $a \in G$ קיים $a^{-1} \in G$ כך ש-$a \oplus a^{-1} = a^{-1} \oplus a = e$.

חבורה נקראת **קומוטטיבית** או **אבלית** אם לכל $a, b \in G$ מתקיים $a \oplus b = b \oplus a$.
עבור חבורה סופית G, גודל החבורה $|G|$ נקרא **הסדר** של החבורה.

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

טענה 3.16 [היה חסר בתרגול]. 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 ניטרלי אז $e_1 \oplus e_2 = e_1$ ולכן e_2 הופכי של e_1 כי e_1ניטרלי, מכאן כי $e_2 \oplus e_1 = e_1$, אך מכך ש-e_1 ניטרלי $e_2 \oplus e_1 = e_2$ ולכן $e_1 = e_2$. ■

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

3.2.2 תתי-חבורות

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

טענה 3.19. תהא $(G, \oplus)$ חבורה סופית, ותהא $\emptyset \neq H \subseteq G$. אזי אם 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 תתי-חבורות]. תהא $(G, \oplus)$ חבורה ו-$(H, \oplus)$ תת-חבורה שלה. אזי:

- אם e איבר ניטרלי ב-G אזי הוא גם ניטרלי ב-H.
- a^{-1} ההופכי של a ב-H אם ורק אם הוא ההופכי של a ב-G.

משפט לגראנז'

משפט 3.22. אם $(G, \oplus)$ חבורה סופית ו-$(H, \oplus)$ תת-חבורה שלה, אזי $|H|$ מחלק את $|G|$.

3.2.3 העלאה בחזקה

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

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

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

- $a^k \oplus a^m = a^{k+m}$.
- $\left(a^k\right)^m = a^{km}$.

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

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

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

עבור חבורות מסוימות מאמינים שהבעיות הללו קשות.

3.2.4 הסדר של איברים בחבורה וחבורות 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 $\langle a \rangle = \left\{ a^i : i \in \mathbb{Z} \right\}$ היא תת-חבורה של G עם $\text{order}(a)$ איברים שונים $a^1, \ldots, a^{\text{order}(a)}$.

הגדרה 3.30 [חבורה ציקלית]. חבורה G נקראת **ציקלית** אם קיים $a \in G$ כך ש-$G = \langle a \rangle$, 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 $|G|$ ראשוני אזי 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.