

## תוכן העניינים

1	הגדרות
5	משפטים

### 1 הגדרות

#### הגדרה 1: שלם שמחוק שלם

יהיו  $a, b$  מספרים שלמים. אומרים כי  $b$  מחלק את  $a$  אם קיימים מספר שלם  $q$  כך ש-

$$a = qb.$$

כלומר  $\frac{a}{b}$  שווה למספר שלם  $q$ . הסימון  $a | b$  אומר כי  $b$  מחלק את  $a$ .

#### הגדרה 2: יחס שקולות בין $a$ ל- $b$

נניח כי  $a, b \in \mathbb{Z}$  מספרים שלמים ו-  $m$  מספר שלם חיובי. היחס

$$a \equiv b \pmod{m}$$

אומר כי  $m$  מחלק את ההפרש  $a - b$ , כלומר  $m | a - b$ .

התנאים הבאים שקולים:

$$a \equiv b \pmod{m} \iff m | a - b \iff \exists q, r : a = qm + r$$

אומרים גם כי " $a$  שקול ל- $b$  מודולו  $m$ ".

#### הגדרה 3: השארית

נתונים מספרים שלמים  $a, b \in \mathbb{Z}$ , היחס

$$a \bmod b$$

מציאן את השארית בחלוקת  $a$  ב- $b$ .

#### הגדרה 4: המחלק המשותף הגדול ביותר gcd

נתונים שני מספרים שלמים  $a, b > 0$ .

המחלק המשותף הגדול ביותר של  $a$  ו-  $b$  מסומן gcd( $a, b$ ) ומוגדר להיות המספר שלם הגדול ביותר שמחולק גם  $a$  וגם  $b$ .

#### הגדרה 5: כפולה משותפת קטנה ביותר

נתונים שני מספרים שלמים  $a, b > 0$ .

הכפולה המשותפת הקטנה ביותר במסומן lcm( $a, b$ ) ומוגדר להיות המספר השלם החיובי הקטן ביותר ש-  $a$  ו-  $b$  מחלקים אותו.

#### הגדרה 6: מספרים זרים

נניח כי  $a \geq 1$  ו-  $b \geq 2$  מספרים שלמים. אומרים כי  $a$  ו-  $b$  **מספרים זרים** אם  $\gcd(a, b) = 1$ .

במילים פשוטות, שני מספרים שלמים נקראים **מספרים זרים** אם המחלק המשותף המקסימלי שלהם הוא 1, כלומר, אין אף מספר גדול מכך שמחולק את שניהם.

#### הגדרה 7: פונקציית אוילר

יהי  $m$  מספרשלם.

הפונקציית אוילר מסומנת ב-  $\phi(m)$  ומוגדרת להיות השלמים שקטנים ממש מ-  $m$  וזרים ביחס ל-  $m$ .  

$$\phi(m) := \{a \in \mathbb{N} \mid \gcd(a, m) = 1, a < m\}$$
.

#### הגדרה 8: צופן ההזזה

יהיו  $0 \leq k \leq 25$ . Über  $P = C = K = \mathbb{Z}_{26}$  נגדיר

$$e_k(x) = (x + k) \bmod 26, \quad x \in \mathbb{Z}_{26}$$

-1

$$d_k(y) = (y - k) \bmod 26, \quad y \in \mathbb{Z}_{26}.$$

צופן ההזזה מוגדר מעל

#### הגדרה 9: צופן החלפה (substitution cipher)

בצופן החלפה,  $P = C = \mathbb{Z}_{26}$

$K$  מורכב מכל החלפות האפשריות של ה- 26 סמלים  $0, 1, 2, \dots, 25$

עבור כל החלפה  $\pi \in K$  נגדיר כלל מצפין

$$e_\pi(x) = \pi(x)$$

ונגדיר כלל מפענה

$$d_\pi(x) = \pi^{-1}(x),$$

כאשר  $\pi^{-1}$  החלפה ההפוכה של  $\pi$ .

#### הגדרה 10: צופן אפייני

יהי  $P = C = \mathbb{Z}_{26}$  ויהי

$$K = \{a, b \in \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\}.$$

עבור  $x \in \mathbb{Z}_{26}$  ועבור  $k = (a, b) \in K$  נגדיר כלל המצפין

$$e_k(x) = (ax + b) \bmod 26,$$

ועבור  $y \in \mathbb{Z}_{26}$  נגדיר כלל המפענה

$$d_k(y) = a^{-1}(y - b) \bmod 26.$$

### הגדרה 11: צופן ויז'נר (Vigenere Cipher)

יהי  $m$  מספר שלם חיובי.

$$P = C = K = \mathbb{Z}_{26}^m$$

עבור מפתח  $k = (k_1, k_2, \dots, k_m)$  נגדיר כלל מצפין

$$e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, x_3 + k_3, \dots, x_m + k_m) \bmod 26$$

ונגדיר כלל מפענה

$$d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, y_3 - k_3, \dots, y_m - k_m) \bmod 26$$

כאשר כל הפעולות נקבעות ב-  $\mathbb{Z}_{26}$ .

### הגדרה 12: צופן הייל

נניח כי  $2 \leq m$  מספר שלם.

$$P = C = \mathbb{Z}_{26}^m$$

$$k = \mathbb{Z}_{26}^{m \times m}$$

מטריצה בחוג  $\mathbb{Z}_{26}$  מסדר  $m \times m$ .

עבור מפתח  $k \in K$  נגדיר כלל מצפין

$$e_k(x) = x \cdot k \bmod 26$$

ונגדיר כלל מפענה

$$d_k(y) = y \cdot k^{-1} \bmod 26$$

כאשר כל הפעולות נקבעות ב-  $\mathbb{Z}_{26}$ .

### הגדרה 13: המטריצה של קופקטוריים

תהי  $A \in \mathbb{R}^{n \times n}$ .

הקובקטור ה-  $(i, j)$  של  $A$  מוגדר להיות הדטרמיננטה של המטריצה המתקבלת מ-  $A$  ע"י מחיקת שורה  $i$  ועמודה  $j$ , כפול  $(-1)^{i+j}$ .

המטריצה של קופקטוריים של המטריצה  $A$  מוגדרת

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}$$

כאשר  $C_{ij}$  הקובטור ה-  $(i, j)$  של  $A$ .

### הגדרה 14: המטריצה המכורעת

תהי  $A \in \mathbb{R}^{n \times n}$ . המטריצה המכורעת של  $A$  היא מטריצה מסדר  $n \times n$  שמסומנת  $\text{adj}(A)$  ומוגדרת

$$\text{adj}(A) = C^t$$

כאשר  $C$  המטריצה של קופקטוריים של  $A$ .

## הגדירה 15: צופן RSA

יהי  $p, q$  מספרים ראשוניים שונים. תהי הקבוצת טקסט גלי  $P = \mathbb{Z}_n$ , והקבוצת טקסט מוצפן  $C = \mathbb{Z}_n$ . נגידיר קבוצת המפתחות

$$K = \left\{ (n, p, q, a, b) \mid ab \equiv 1 \pmod{\phi(n)} \right\}$$

לכל  $K$ ,  $x \in P$  ו-  $y \in C$  נגידיר כלל מצפין

$$e_k(x) = x^b \pmod{n},$$

ונגידיר כלל מפענה

$$d_k(x) = y^a \pmod{n}.$$

הערכים של  $n$  ו-  $b$  הם ערכים ציבוריים בעוד  $p, q, a$  ערכים סודיים.

## הגדירה 16: רשות פיעיטל (Feistel)

נתון טקסט גלי  $x = \{0, 1\}^{2n}$  כרץף סיביות.

$$x = \underbrace{x_1 \dots x_n}_{L_0} \quad \underbrace{x_n \dots x_{2n}}_{R_0}$$

מחלקים את  $x$  לשני חצאים שננסמן  $L_0$  ו-  $R_0$ :

ברשות פיעיטל יש 4 מרכיבים:

- מספר שלם  $N$  אשרקובע את המספר של השלבים בתהליך הצפנה.

- מפתח התחלתי  $k$ .

- מערכת של  $N$  תת-מפתחות  $(k_1, \dots, k_N)$ , אחד לכל שלב של התהליך הצפנה.

- פונקציית ליבה  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ .

$$1) \text{ מגדירים } R_0 = x_n \dots x_{2n}, L_0 = x_1 \dots x_n$$

$$. L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

בשלב ה-  $i$  ית  $(1 \leq i \leq N)$ :

$$. y = R_N L_N$$

בשלב ה-  $N$  קיבל את הטקסט מוצפן לפי

## הגדירה 17: משוואות פיעיטל

משוואות פיעיטל להצפנה:

נתון טקסט גלי  $x = L_0 R_0$ . לכל  $1 \leq i \leq N$ .

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i), \quad y = R_N L_N$$

משוואות פיעיטל למפענה:

נתון טקסט גלי  $y = R_N L_N$ . לכל  $1 \leq i \leq N$ .

$$R_i = L_{i+1}, \quad L_i = R_{i+1} \oplus f(R_i, k_{i+1}), \quad x = L_0 R_0$$

### הגדרה 18: סודיות מושלמת

אומרים כי קרייפטו-מערכת יש סודיות מושלמת אם

$$P(X = x|Y = y) = P(X = x)$$

לכל  $x \in X, y \in Y$ .

ז"א הסתברות כי הטקסט גלי  $x = X$ , במידעה כי הטקסט מוצפן  $y = Y$  שווה רק להסתברות כי הטקסט גלי  $x = X$  והבחירה של המפתח שבאמצעותו מתקבל הטקסט מוצפן  $y$  לא משפייע על הסתברות כי הטקסט גלי  $x = X$ .

### הגדרה 19: מידע של מאורע (שאנו)

נתון משתנה מקרי  $X$ . המידע של ערך מסוים של  $X$  מסומן ( $I_X(x)$ ) ומוגדר להיות

$$I(X = x) = \log_2 \left( \frac{1}{P_X(x)} \right) = -\log_2(P_X(x))$$

כאשר  $P_X(x)$  פונקציית ההסתברות של המשתנה מקרי  $X$ .

### הגדרה 20: הצפנת האפמן

נתון משתנה מקרי  $X$ . נגידר הצפנת האפמן של  $X$  להיות הפונקציה (כלל מוצפין)

$$f : X \rightarrow \{0, 1\}^*$$

כאשר  $\{0, 1\}^*$  קבוצת רצפים של סיביות סופיים.

נתון רצף מאורעות  $x_1, \dots, x_n$ . נגידר

$$f(x_1 \dots x_n) = f(x_1) || \dots || f(x_n)$$

כאשר " $||$ " מסמן שרשור (concatenation).

### הגדרה 21: תוחלת האורך של הצפנת האפמן

נתונה הצפנת האפמן  $f$ . תוחלת האורך של ההצפנה מוגדרת

$$l(f) = \sum_{x \in X} P(X = x) |f(x)| .$$

## 2 משפטיים

### משפט 1:

יהיו  $n, a, b$  מספרים שלמים.

אם השלושה תנאים הבאים מתקיימים:

$$a \text{ ו- } b \text{ זרים, } \quad (1)$$

$$, a \mid n \quad (2)$$

$$, b \mid n \quad (3)$$

הוכחה:

$$a \mid n, \quad b \mid n$$

לכן קיימים שלמים  $k$  ו-  $l$  כך ש-

$$n = ak, \quad n = bl.$$

$$\therefore n = ak = bl$$

$$\therefore b \mid ak$$

$$\text{מכאן כי } k = bq, \text{ כלומר } b \mid k. \text{ לכן}$$

$$\therefore n = ak = abq$$

$$\text{לכן } \gcd(a, b) \mid k.$$

## משפט 2: תכונות של gcd

$$\gcd(ma, mb) = m \gcd(a, b) . \blacksquare$$

$$\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a, b)}{m} \text{ אם } m \mid b \text{ ו- } m \mid a \text{ וגם } m > 0 . \blacksquare$$

$$3. \text{ המספרים } \frac{b}{\gcd(a, b)} \text{ ו- } \frac{a}{\gcd(a, b)} \text{ הם זרים.}$$

$$4. \text{ אם } c \mid a \text{ ו- } c \mid b \text{ אז } c \mid ab.$$

$$5. \text{ אם } a, c \text{ הם זרים ו- } b, c \text{ הם זרים אז } ab \mid c \text{ ו- } ab \text{ זר ל- } c.$$

$$\gcd(a, b) = \gcd(a + cb, b) . \blacksquare$$

הוכחה:

$$1. \text{ יהיו } d = \gcd(a, b). \text{ אז קיימים שלמים } s, t \text{ עבורם}$$

$$sa + tb = d .$$

מכאן

$$msa + mtb = md \Rightarrow s(ma) + t(mb) = md .$$

$$\text{לכן } \gcd(ma, mb) = md = m \gcd(a, b)$$

$$2. \text{ יהיו } d = \gcd(a, b)$$

ו-  $\exists$  שלמים  $s, t$  כך ש-

$$sa + tb = d .$$

(\*)

נחלה (\*1) ב-  $m$  ונקבל

$$s \frac{a}{m} + t \frac{b}{m} = \frac{d}{m} . \quad (**)$$

$$\text{נשים לב } \frac{a}{m} \text{ שלם ו- } \frac{b}{m} \text{ שלם. לכן } \frac{a}{m} \mid b \text{ ו- } m \mid a .$$

לכן  $\frac{d}{m}$  בהכרח שלם ולפי משפט באו  
 $\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a, b)}{m}$ .

.3

4. שלמים לכך קיימים שלמים  $s, t, d$  עבורם

$$sa + tb = d$$

$$\text{כasher } d = \gcd(a, b)$$

מכאן

$$s\left(\frac{a}{d}\right) + t\left(\frac{b}{d}\right) = 1.$$

נשים לב ש-  $d = \gcd(a, b)$  ו-  $\frac{b}{d}$  שלמים. לכן קיבלונו שלמים  $s, t$  עבורם

$$s\left(\frac{a}{\gcd(a, b)}\right) + t\left(\frac{b}{\gcd(a, b)}\right) = 1.$$

לכן השלמים  $\frac{b}{\gcd(a, b)}$  ו-  $\frac{a}{\gcd(a, b)}$  זרים.

5. אם  $a, c$  מספרים זרים ו-  $b, c$  מספרים זרים אז  $c$  ו-  $ab$  מספרים זרים.

1-  $c$  זרים אז קיימים  $s$  ו-  $t$  שלמים עבורם

$$sa + tc = 1.$$

2-  $c$  זרים אז  $\bar{c}$  ו-  $\bar{t}$  שלמים עבורם

$$\bar{s}b + \bar{t}c = 1.$$

לכן

$$(sa + tc)(\bar{s}b + \bar{t}c) = 1$$

$$\Rightarrow s\bar{s}(ab) + (t\bar{s}b + \bar{t}c + s\bar{t}a)c = 1$$

זה א' קיימים שלמים  $x, y$  עבורם  $x(ab) + yc = 1$  לכן  $c$  ו-  $ab$  זרים.

6. אם  $a, b$  שלמים אז קיימים שלמים  $s$  ו-  $t$  עבורם  $sa + tb = d$ . מכאן

$$sa + tb = d$$

$$s(a + cb) + tb = d + scb$$

$$s(a + cb) + tb - scb = d$$

$$s(a + cb) + (t - sc)c = d$$

לכן קיימים שלמים  $y = t - cb$  ו-  $x = s$  עבורם

$$x(a + cb) + yb = d$$

$$\text{ולכן } \gcd(a + cb, b) = d = \gcd(a, b)$$



### משפט 3: תנאי לקיום איבר הופכי של חוג

$\cdot \gcd(a, m) = 1$ . קיים איבר הופכי  $a^{-1} \in \mathbb{Z}_m$  של  $a$  אם ורק אם  $a \in \mathbb{Z}_m$ .

**הוכחה:** יש להוכיח שקיימים האיבר הופכי  $a^{-1}$  של  $a$  ב-  $\mathbb{Z}_m$  אם ורק אם  $\gcd(a, m) = 1$ .

כיוון ⇐

אם  $d = \gcd(a, m)$  אז לפי משפט באז'ו קיימים שלמים  $s, t, d$  כך ש-  $sa + tm = d$  וגם  $sa + tm = 1 \Rightarrow sa = 1 - tm \Rightarrow sa \equiv 1 \pmod{m}$ .

לפיכך קיים שלם  $s$  אשר הוא האיבר הופכי של  $a$  ב-  $\mathbb{Z}_m$ .

כיוון ⇒

אם קיים איבר הופכי  $a^{-1}$  של  $a$  ב-  $\mathbb{Z}_m$  אז  $\gcd(a, m) = 1$ .  
 $a^{-1}a = 1 + qm \Rightarrow a^{-1}a + (-q)m = 1$ .

לכן קיימים שלמים  $s = a^{-1}$  ו-  $t = -q$  כך ש-

$$sa + tm = 1$$

ולכן לפי משפט באז'ו  $\gcd(a, m) = 1$ .

### משפט 4:

יהיו  $a, b, c$  שלמים חיוביים. אם לא זרים אז לא קיים  $c$  עבורו  $ac \equiv 1 \pmod{b}$ .

**הוכחה:** נניח בsvilleה כי  $a, b$  זרים וקיים  $c$  עבורו  $ac \equiv 1 \pmod{b}$  אז קיים שלם  $q$ :

$$ac = qb + 1 \Rightarrow ac - qb = 1.$$

לכן קיימים שלמים  $s = c$  ו-  $t = -q$  עבורם  $sa + tb = 1$ . לפיכך משפט באז'ו  $a$  ו-  $b$  זרים, בסתרה לכך  $a$  ו-  $b$  לא זרים.

### משפט 5: חיסור של שאריות

אם  $a, b, m$  מספרים שלמים חיוביים אז  
 $((a + b) \bmod m - b) \bmod m = a \bmod m$ .

**הוכחה:** לפי משפט החילוק של אוקלידס קיימים שלמים  $q_1, r_1$  כך ש-  
 $a + b = q_1m + r_1$ ,  $0 \leq r_1 < m$ ,

כasher  $r_1 = (a + b) \bmod m$  ו גם  $q_1 = \left\lfloor \frac{a + b}{m} \right\rfloor$ . מכאן:

$$((a + b) \bmod m) - b = r_1 - b = a - q_1m.$$

ו"א קיימים שלם  $-q_1 = Q$  כך ש:

$$((a+b) \bmod m) - b = Qm + a$$

ולכן

$$((a+b) \bmod m) - b \equiv a \pmod{m}$$

ולפיכך, מכיוון שהשני שלמים  $b$  ו-  $a$  שקיימים מודולריים ביחס ל-  $m$ , אז בהכרח יש להם אותן שאריות בחלוקת ב-  $m$ :

$$[((a+b) \bmod m) - b] \bmod m = a \bmod m .$$



#### משפט 6: צופן אפיני ניתן לפענוח

יהי  $e_k(x)$  הכלל מצפין של צופן אפיני ויהי  $d_k(y)$  הכלל מפענה של צופן אפיני. אז

$$d_k(e_k(x)) = x \bmod 26$$

לכל  $\mathbb{Z}_{26} \in x$ . כמובן, צופן אפיני ניתן לפענוח.

הוכחה: נסמן  $y = e_k(x)$ .

$$\begin{aligned} d_k(e_k(x)) &= d_k(y) \\ &= a^{-1}(y - b) \bmod 26 \\ &= a^{-1}([(ax + b) \bmod 26] - b) \bmod 26 \\ &\stackrel{\text{ככל חכפי}}{=} (a^{-1} \bmod 26)(([(ax + b) \bmod 26] - b) \bmod 26) \bmod 26 \\ &\stackrel{5}{\stackrel{\text{משפט}}{=}} (a^{-1} \bmod 26)(ax \bmod 26) \bmod 26 \\ &\stackrel{\text{ככל חכפי}}{=} (a^{-1}ax \bmod 26) \bmod 26 \\ &= x \bmod 26 . \end{aligned}$$



#### משפט 7: קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך הśליליה.  
נניח כי  $\{p_1, \dots, p_n\}$  הוא הקבוצה של כל הראשוניים שקיים וקבוצה זו נוצרת סופי.  
נגידר המשפט  $M = (p_1 \cdot p_2 \cdot \dots \cdot p_n + 1)$  שלעיל או משפט 9 (ראוי משפט 18 למטה) הוא מספר ראשי או שווה למכפלה של ראשוניים.

$M$  לא מספר ראשי בಗלל ש-  $p_i < M$  לכל  $1 \leq i \leq n$ .  
אם לא קיים מספק ראשי  $p_i$  אשר מחלק את  $M$ . הרי

$$M \bmod p_i = 1 \Rightarrow p_i \nmid M .$$

הגענו לסתירה של המשפט הפירוק לראשוניים, לכן קיימים אינסוף מספרים ראשוניים.



## משפט 8: נוסחת קיילי המילטון

נניח כי  $A \in \mathbb{R}^{n \times n}$  מטריצה ריבועית. אם  $A$  הפיכה, כלומר אם  $|A| \neq 0$  אז המטריצה ההופכית נתונה ע"י  
נוסחת קיילי המילטון:

$$A^{-1} = \frac{1}{|A|} \text{adj}(A) ,$$

כאשר  $\text{adj}(A)$  המטריצה המצורפת של  $A$ .

## משפט 9: משפט הפירוק לראשוניים

המשפט היסודי של האריתמטיקה או **משפט הפירוק לראשוניים** קובע כי כל מספר טבעי ניתן לרשום כמכפלה ייחודית של מספרים ראשוניים.  
ז"א, יהיו  $a \in \mathbb{N}$  כל מספר טבעי. אז

$$a = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_n^{e_n} .$$

כאשר  $p_1, \dots, p_n$  מספרים ראשוניים ו-  $e_1, \dots, e_n \in \mathbb{N}$ , והפירוק זהה ייחיד.

## משפט 10: הפירוק לראשוניים של פונקציית אוילר

נתון מספר טבעי  $m$ . נניח כי הפירוק למספרים ראשוניים שלו הוא

$$m = \prod_{i=1}^n p_i^{e_i} ,$$

כאשר  $p_i$  מספרים ראשוניים שונים ו-  $0 < e_i < n$  מספרים שלמים ו-  $1 \leq i \leq n$ . אז

$$\phi(m) = \prod_{i=1}^n (p_i^{e_i} - p_i^{e_i-1}) .$$

## משפט 11: שיטה לחישוב gcd

נתונים השלמים  $a, b$  כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} , \quad b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

וללא הגבלה כללית נתון כי  $n \leq k$ . אז gcd נתון על ידי

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$

## משפט 12: שיטה לחישוב lcm

נתונים השלמים  $a, b$  כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} , \quad b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

וללא הגבלה כללית נתון כי  $n \leq k$ . אז lcm נתון על ידי

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}$$

## משפט 13:

$$\gcd(a, b) \text{lcm}(a, b) = ab .$$

הוכחה:

$$\min(a, b) + \max(a, b) = a + b .$$

#### משפט 14: משפט חילוק של אוקלידס

יהיו  $a, b$  מספרים שלמים  $0 \neq b$ . קיימים מספרים שלמים  $q, r$  ייחדים כך ש-  

$$a = qb + r$$
  
 כאשר  $0 \leq r < |b|$

- $b$  נקרא **מודולו**,
- $q$  נקראת **המנה**
- ואילו  $r$  נקרא **השארית**.
- במקרה ש-  $r = a \bmod b$  אז  $a, b > 0$

#### משפט 15: האלגוריתם של אוקלידס

יהיו  $a, b$  מספרים שלמים חיוביים. קיים אלגוריתם אשר נותן את  $d = \gcd(a, b)$  כדלקמן. ראשית מתחילהים  $r_0 - 1$  ו-  $r_0$ :

$$r_0 = a , \quad r_1 = b .$$

אם  $r_1 = b \neq 0$  אז מתחילהים את הלולאה. בשלב  $i = 1$  מחשבים את  $q_1$  ו-  $r_2$  כך:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor , \quad r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor .$$

אם  $r_2 \neq 0$  ממשיכים לשלב  $i = 2$  שבו מחשבים את  $q_2$  ו-  $r_3$  כך:

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor , \quad r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor .$$

התהליך ממשיך עד שנקבל  $r_{n+1} = 0$  בשלב ה-  $n$ -ית. כל השלבים של התהליך הם כדלקמן:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor \quad r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor r_1 \quad : i = 1$$

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor \quad r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor r_2 \quad : i = 2$$

$$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor \quad r_4 = r_2 - q_3 r_3 = r_2 - \left\lfloor \frac{r_2}{r_3} \right\rfloor r_3 \quad : i = 3$$

⋮

$$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor \quad r_n = r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} - \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor r_{n-1} \quad : i = n-1$$

$$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor \quad r_{n+1} = 0 \quad : i = n$$

התהליך מסתיים בשלב ה-  $n$ -ית אם  $r_{n+1} = 0$ . ואז הפלט של האלגוריתם הוא  $r_n = \gcd(a, b)$ . למטה

רשום ייצוג פסאודו-קוד של האלגוריתם של אוקלידס:

---

### האלגוריתם של אוקלידס 1

---

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a$ 
3:  $r_1 \leftarrow b$ 
4:  $n \leftarrow 1$ 
5: while  $r_n \neq 0$  do
6:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
7:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
8:    $n \leftarrow n + 1$ 
9: end while
10:  $n \leftarrow n - 1$ 
11: Output:  $r_n = \gcd(a, b)$ 

```

---

### משפט 16: משפט בז'ו (Bezout's identity)

יהיו  $a, b$  שלמים ויהי  $d = \gcd(a, b)$ . קיימים שלמים  $s, t$  כך שנitinן לרשום ה-  $\gcd(a, b) = c\pi r\alpha f$  לינארי של  $a$  ו-  $b$ :

$$sa + tb = d .$$

### משפט 17: האלגוריתם המוכפל של אוקלידס

יהיו  $a, b$  שלמים חיוביים. קיים אלגוריתם אשר נותן שלמים  $s, t, d$  עבורם

$$d = sa + tb$$

כאשר  $d = \gcd(a, b)$ , כدلקמן. ראשית מאתחלים:

$$r_0 = a , \quad r_1 = b , \quad s_0 = 1 , \quad s_1 = 0 , \quad t_0 = 0 , \quad t_1 = 1 .$$

אם  $q_1, r_2, s_2, t_2$  מוצאים האיטרציה הראשונה של הלולאה. בשלב  $i = 1$  מחשבים את  $r_1 = b \neq 0$  כך:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor , \quad r_2 = r_0 - q_1 r_1 , \quad s_2 = s_0 - q_1 s_1 , \quad t_2 = t_0 - q_1 t_1 .$$

אם  $r_2 \neq 0$  אז עוברים לאיטרציה  $i = 2$  שבה מחשבים את  $r_3, s_3, t_3$  כך:

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor , \quad r_3 = r_1 - q_2 r_2 , \quad s_3 = s_1 - q_2 s_2 , \quad t_3 = t_1 - q_2 t_2 .$$

התהlik ממשיך עד השלב ה-  $n$  שבו מקבלים  $r_{n+1}$ , ו-  $s, t$  פולטים. כל השלבים של האלגוריתם הם כدلקמן:

$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor$	$r_2 = r_0 - q_1 r_1$	$s_2 = s_0 - q_1 s_1$	$t_2 = t_0 - q_1 t_1$	שלב 1
$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor$	$r_3 = r_1 - q_2 r_2$	$s_3 = s_1 - q_2 s_2$	$t_3 = t_1 - q_2 t_2$	שלב 2
				⋮
$q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$	$r_{i+1} = r_{i-1} - q_i r_i$	$s_{i+1} = s_{i-1} - q_i s_i$	$t_{i+1} = t_{i-1} - q_i t_i$	שלב $i$
				⋮
$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor$	$r_n = r_{n-2} - q_{n-1} r_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$t_n = t_{n-2} - q_{n-1} t_{n-1}$	שלב $n-1$
$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$	$r_{n+1} = r_{n-1} - q_n r_n$	$s_{n+1} = s_{n-1} - q_n s_n$	$t_{n+1} = t_{n-1} - q_n t_n$	שלב $n$

$$d = \gcd(a, b) = r_n , \quad s = s_n , \quad t = t_n .$$

למטה רשום ייצוג פסאודו-קוד של האלגוריתם:

---

### האלגוריתם המוכפל של אוקלידס

---

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a$ 
3:  $r_1 \leftarrow b$ 
4:  $s_0 \leftarrow 1$ 
5:  $s_1 \leftarrow 0$ 
6:  $t_0 \leftarrow 0$ 
7:  $t_1 \leftarrow 1$ 
8:  $n \leftarrow 1$ 
9: while  $r_n \neq 0$  do
10:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
11:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
12:    $s_{n+1} \leftarrow s_{n-1} - q_n s_n$ 
13:    $t_{n+1} \leftarrow t_{n-1} - q_n t_n$ 
14:    $n \leftarrow n + 1$ 
15: end while
16:  $n \leftarrow n - 1$ 
17: Output:  $r_n, s_n, t_n$                                  $\triangleright d = r_n = \gcd(a, b)$  and  $d = sa + tb$  where  $s = s_n, t = t_n.$ 

```

---

### משפט 18: משפט הפירוק לראשוניים

(ראו משפט 9) לכל מספר טבעי  $n$  קיימים שלמים  $e_i$  וראשוניים  $p_i$  כך ש-

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

**הוכחה:** אינדוקציה.

### משפט 19: נוסחת פונקציית אוילר

(ראו משפט 10) לכל מספר שלם  $n$  בעל פירוק לראשוניים

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

פונקציית אוילר ניתנת על ידי

$$\phi(n) = \prod_{i=1}^k (p_i^{e_i} - p_i^{e_i-1}) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

### משפט 20: נוסחת השארית

נתונים  $a, b > 0$  מספר שלמים.

$$a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor \quad \text{(א)}$$

$$.(-a) \bmod b = b - (a \bmod b) = b \left\lceil \frac{a}{b} \right\rceil - a \quad \text{(ב)}$$

**הוכחה:**

**א)** לפי משפט החילוק של אוקלידס 14, קיימים שלמים  $r, q, r \leq q$  ש-

$$a = qb + r \quad \text{(*)1}$$

כאשר  $0 \leq r < b$ . נחלק ב-  $b$ . ונקבל

$$\frac{a}{b} = q + \frac{r}{b} \quad \text{(*)2}$$

נשים לב כי  $0 < \frac{r}{b} < 1$ , לכן לפי (\*)2

$$\left\lfloor \frac{a}{b} \right\rfloor = q .$$

נציב זה ב- (\*)1 ונקבל

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + r \Rightarrow r = a - b \left\lfloor \frac{a}{b} \right\rfloor . \quad \text{(*)3}$$

**ב)** לפי משפט החילוק של אוקלידס 14, קיימים שלמים  $r' \leq 0$  כ-  $q'$  ש-

$$-a = q'b + r'$$

כאשר  $b \mid r'$ . מכאן

$$a = -q'b - r' = -q'b - b + b - r' = -(q' + 1)b + (b - r') . \quad \text{(*)4}$$

נשים לב כי  $0 \leq b - r' \leq b$ . אבל לפי (\*)1  $a \bmod b = qb + r$  כאשר  $a = qb + r$  ייחיד. לכן

$$r = b - r' \Rightarrow r' = b - r \stackrel{\text{(*)3}}{=} b - a + b \left\lfloor \frac{a}{b} \right\rfloor = b - \left( a - b \left\lfloor \frac{a}{b} \right\rfloor \right) = b - (a \bmod b) . \quad \text{(*)5}$$

לכן  $r' = (-a) \bmod b = b - (a \bmod b)$

זהות שני מנווע מ- (\*)5

$$r = b - r' \Rightarrow r' = b - r \stackrel{\text{(*)3}}{=} b - a + b \left\lfloor \frac{a}{b} \right\rfloor - a + \left\lceil \frac{a}{b} \right\rceil .$$

$$\text{לכן } r' = (-a) \bmod b = -a + \left\lceil \frac{a}{b} \right\rceil$$

### משפט 21: זהויות של הפונקציה אoilר

(1) אם  $p$  מספר ראשוני אז  $\phi(p) = p - 1$ .

(2) אם  $p$  מספר ראשוני אז  $\phi(p^n) = p^n - p^{n-1}$ .

(3) אם  $s, t$  שלמים זרים (כלומר  $\gcd(s, t) = 1$ ) אז  $\phi(s \cdot t) = \phi(s) \cdot \phi(t)$ .

(4) אם  $p$  ו- $q$  מספרים ראשוניים שונים אז  $\phi(p \cdot q) = (p - 1)(q - 1)$ .

### משפט 22: משפט עזר למשפט הקטן של פרמה

אם  $p$  מספר ראשוני אז

$$p \mid \binom{p}{k}.$$

הוכחה:

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} \Rightarrow k!(p-k)!\binom{p}{k} = p!$$

מכיוון ש-  $p \mid p!$  ו-  $p \mid k!(p-k)!$  אז  $p \mid \binom{p}{k}$ .  
מכיוון ש:  $p$  מספר ראשוני אז  $p \nmid k!(p-k)!$  לכן בהכרח:  
 $p \mid \binom{p}{k}$ .

### משפט 23: המשפט הקטן של פרמה

אם  $p$  מספר ראשוני ו-  $a \in \mathbb{Z}_p$ . אז התנאים הבאים מתקיימים:

$$a^p \equiv a \pmod{p}. \quad .1$$

$$a^{p-1} \equiv 1 \pmod{p}. \quad .2$$

$$a^{-1} \equiv a^{p-2} \pmod{p}. \quad .3$$

הוכחה:

**טענה 1.** נוכיח באינדוקציה.

שלב הבסיס:

עבור  $a = 0$  הטענה  $0^p \equiv 0 \pmod{p}$  מתקיימת.

שלב המעבר:

נניח כי הטענה מתקיימת עבור  $a$  (שזה ההנחה האינדוקציה).

nocich כי היא מתקיימת גם עבור  $a + 1$  באופן הבא.

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{k}a^{p-k} + \cdots + \binom{p}{1}a + 1 .$$

לכל  $1 \leq k \leq p-1$  טבבי לפि משפט 22:  $p \mid \binom{p}{k}$  ולכן

$$(a+1)^p \equiv a^p + 1 \pmod{p}$$

על פי ההנחה האינדוקציה:  $a^p \equiv a \pmod{p}$  לכן

$$(a+1)^p \pmod{p} \equiv a^p + 1 \pmod{p} \equiv (a+1) \pmod{p} .$$

כנדרש.

**טענה 2.** לכל מספר ראשוני ושלם  $a$  מקיימים  $\gcd(a, p) = 1$  לפיכך קיים איבר הופכי

נכפיל את היחס שקיים בסעיף הקודם ב-  $a^{-1}$ :

$$a^{-1}a^p \equiv a^{-1} \cdot a \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p} .$$

**טענה 3.**

$$a^{p-1} \equiv 1 \pmod{p} \Leftrightarrow 1 \equiv a^{p-1} \pmod{p} \Rightarrow a^{-1} \equiv a^{p-2} \pmod{p} .$$



#### משפט 24: משפט אוילר

אם  $\gcd(a, n) = 1$  אז  $a$  שלמים ו-

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad (1)$$

$$a^{-1} \equiv a^{\phi(n)-1} \pmod{n} \quad (2)$$

#### משפט 25: משפט השאריות הסיני

יהיו  $m_1, m_2, \dots, m_r$  שלמים אשר זרים בזוגות ויהיו  $a_1, a_2, \dots, a_r$  שלמים. למערכת של יחסים שקיים

$$x = a_1 \pmod{m_1},$$

$$x = a_2 \pmod{m_2},$$

⋮

$$x = a_r \pmod{m_r},$$

קיים פתרון ייחיד מודולו  $M = m_1 m_2 \cdots m_r$  שנitin על ידי

$$x = \sum_{i=1}^r a_i M_i y_i \pmod{M}$$

$$\text{כאשר } 1 \leq i \leq r \text{ לכל } y_i = M_i^{-1} \pmod{m_i} \rightarrow M_i = \frac{M}{m_i}$$

#### משפט 26:

יהיו  $a, b, m$  שלמים. אז

$$(a \pmod{m})(b \pmod{m}) \equiv ab \pmod{m} .$$

**הוכחה:** לפי משפט החילוק של אטקלידס קיימים שלמים  $r_1, r_2$  כך ש:  $a = q_1m + r_1$  וכך  $a \mod m = a - q_1m$ .  
באותה מידה כך ש:  $b = q_2m + r_2$  וכך  $b \mod m = b - q_2m$  וכך  $b = b - q_2m + r_2$ . לפיכך:  
 $(a \mod m)(b \mod m) = (a - q_1m)(b - q_2m) = ab + (-aq_2 - bq_1 + q_1q_2m)m \equiv ab \pmod{m}$ .

### משפט 27:

יהיו  $a, b, m$  שלמים. אז  
 $(a \mod m)(b \mod m) \mod m = ab \mod m$ .

### הוכחה:

### משפט 28:

אם  $a, b, m$  שלמים חיוביים אז:  
 $a \equiv b \pmod{m} \iff b \equiv a \pmod{m} \iff a \mod m = b \mod m$ .

**הוכחה:**  
נניח ש-  $a \equiv b \pmod{m}$ . נוכיח כי  $b \equiv a \pmod{m}$  באופן הבא.

$a = qm + b$   $\Rightarrow$   $b = -qm + a$   $\Rightarrow$   $b = Qm + b$ ,  
 $b = Qm + a - q$  ולכן  
 $b \equiv a \pmod{m}$ .  
כנדרש.

נניח ש-  $b \mod m = a \mod m$ . נוכיח כי  $b \equiv a \pmod{m}$  באופן הבא.

$a = qm + b$  :  

- קיימים שלם  $q$  כך ש:  $a \equiv b \pmod{m}$
- על פי ההגדרה של השארית:

 $a \mod m = a - \left\lfloor \frac{a}{m} \right\rfloor m$ .

$$\begin{aligned} a \mod m &= qm + b - \left\lfloor \frac{qm + b}{m} \right\rfloor m \\ &= qm + b - \left\lfloor q + \frac{b}{m} \right\rfloor m \\ &= qm + b - qm - \left\lfloor \frac{b}{m} \right\rfloor m \\ &= b - \left\lfloor \frac{b}{m} \right\rfloor m \\ &= b \mod m. \end{aligned}$$

**משפט 29:**

יהיו  $a, m$  שלמים. אזי

$$(a \bmod m)^{-1} \bmod m = a^{-1} \bmod m$$

**הוכחה:**

נסמן  $x \equiv (a \bmod m)^{-1} \pmod{m}$ . אזי, מכיוון ש-  $x$  הוא האיבר החופשי של  $a \bmod m$  מודולר  $m$  אזי  $(a \bmod m)x \equiv 1 \pmod{m}$ .

מכאן קיימים שלם  $q_1$  כך ש:  $(a \bmod m)x = q_1m + 1$ . נציב  $a \bmod m = a - q_2m$  ונקבל  $(a - q_2m)x = q_1m + 1$ . לכן  $ax = (q_2x + q_1)m + 1$  ולבסוף

$$ax \equiv 1 \pmod{m}$$

ולכן

$$x \equiv a^{-1} \pmod{m} \Rightarrow (a \bmod m)^{-1} \bmod m = a^{-1} \bmod m.$$

■

**משפט 30:**

צופן El-Gamal ניתן לפענוח. קלומר

$$d_k(e_k(x)) = x \bmod p.$$

**הוכחה:**

**שיטת 1**

לפי ההגדרה של צופן El-Gamal, הכלל מצפין הוא

$$e_k(x) = (y_1, y_2) \quad y_1 \alpha^d \bmod p, \quad y_2 = \beta^d x \bmod p,$$

כאשר  $p$  ראשוני ו-  $d$  שלם, והכלל מעונח הוא

$$d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \bmod p.$$

לפי כן:

$$d_k(e_k(x)) = d_k(y_1, y_2)$$

$$= (y_1^a)^{-1} y_2 \bmod p$$

$$= [(\alpha^d \bmod p)^a]^{-1} (x \beta^d \bmod p) \bmod p$$

$$= (\alpha^{da} \bmod p)^{-1} (x \beta^d \bmod p) \bmod p \quad (\text{כלל הכפל של יחס מודולרים})$$

$$= ((\alpha^{da})^{-1} \bmod p) (x \beta^d \bmod p) \bmod p \quad (\text{משפט 29})$$

$$= (\alpha^{da})^{-1} (x \beta^d) \bmod p \quad (\text{משפט 27})$$

$$= (\alpha^{da})^{-1} (x (\alpha^a)^d) \bmod p \quad (\text{הגדרה של צופן El-Gamal})$$

$$= (\alpha^{da})^{-1} (x \alpha^{ad}) \bmod p$$

$$= (\alpha^{da})^{-1} \alpha^{ad} x \bmod p$$

$$= x \bmod p.$$

## שיטת 2

לפי ההגדרה של צופן El-Gamal, הכלל מצפיעו הוא

$$e_k(x) = (y_1, y_2) \quad y_1 = \alpha^d \pmod{p}, \quad y_2 = \beta^d x \pmod{p},$$

כאשר  $p$  ראשוני ו-  $d$  שלם, והכלל מעונח הוא

$$d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \pmod{p}.$$

לפיכך:

$$d_k(e_k(x)) = d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \pmod{p} = [(\alpha^d \pmod{p})^a]^{-1} (x \beta^d \pmod{p}) \pmod{p}. \quad (*1)$$

זהות הבאה מתקיימת. אם  $z, m, n$  שלמים חיוביים אז

$$(z \pmod{m})^n \equiv z^n \pmod{m}. \quad (*2)$$

הוכחה: לפי משפט החלוק של אטקלידס קיימים שלמים  $r, q$  כך ש-  $z = qm + r$ , וכך  $(z \pmod{m})^n = z^n + \sum_{k=1}^n \binom{n}{k} (-qm)^k z^{n-k} \equiv z^n \pmod{m}$ . לכן  $z \pmod{m} = z - qm$

משמעותו  $(*)$ , לכל  $y, z, m, n$  שלמים חיוביים:  $y(z \pmod{m})^n \equiv yz^n \pmod{m}$  ולכן  $y(z \pmod{m})^n \pmod{m} = yz^n \pmod{m}$ .  $(*)3$

בנוסף להזאות הבאה מתקיימת. לכל שלמים חיוביים  $b, c, m$

$$b \equiv c \pmod{m} \Rightarrow b^{-1} \equiv c^{-1} \pmod{m}. \quad (*4)$$

הוכחה: נניח  $cb^{-1} \equiv bb^{-1} \pmod{m} \equiv 1 \pmod{m}$  ו-  $bb^{-1} \equiv 1 \pmod{m}$ . מכיוון ש-  $b \equiv c \pmod{m}$  ולכן  $b^{-1} \equiv c^{-1} \pmod{m}$

מן  $(*)$  ו-  $(*)4$ , לכל  $z, m, n$  שלמים חיוביים:

$$[(z \pmod{m})^n]^{-1} \equiv z^{-n} \pmod{m}. \quad (*5)$$

מכאן, לכל  $y$  שלם:

$$[(z \pmod{m})^n]^{-1} \equiv z^{-n} \pmod{m} \Rightarrow [(z \pmod{m})^n]^{-1} y \equiv z^{-n} y \pmod{m}. \quad (*6)$$

ולכן

$$[(z \pmod{m})^n]^{-1} y \pmod{m} = z^{-n} y \pmod{m}. \quad (*7)$$

לפי משמעות  $(*)$ , אם נציב  $y = x\beta^d \pmod{p}$ ,  $m = p$ ,  $z = \alpha^d \pmod{p}$  נקבל:

$$[(\alpha^d \pmod{p})^a]^{-1} (x\beta^d \pmod{p}) \pmod{p} = \alpha^{-ad} (x\beta^d \pmod{p}) \pmod{p}, \quad (*8)$$

ולכן לפי משווה  $(*)$ :

$$d_k(e_k(x)) = \alpha^{-ad} (x\beta^d \pmod{p}) \pmod{p}. \quad (*9)$$

לכל שלמים  $b, c, m$  מתקיים:

$$b(c \pmod{m}) \pmod{m} = bc \pmod{m} \quad (*10)$$

ולכן

$$d_k(e_k(x)) = \alpha^{-ad} x \beta^d \pmod{p}. \quad (*11)$$

נציב את ההגדרה של  $\beta = \alpha^a \pmod{p}$

$$d_k(e_k(x)) = \alpha^{-ad} x (\alpha^a \pmod{p})^d \pmod{p}.$$

ואז לפי משווה  $(*)$  אנחנו מקבלים:

$$d_k(e_k(x)) = \alpha^{-ad} x \alpha^{ad} \pmod{p} = x \pmod{p}.$$



**משפט 31:**

יהיו  $a, b, c, d$  מספרים ממשיים כך ש-  $c \geq d \wedge a \geq b$ . אז  $ac + bd \geq ad + bc$ .

**הוכחה:**

$$a \geq b \Rightarrow (a - b) \geq 0$$

-1

$$c \geq d \Rightarrow (c - d) \geq 0.$$

לכן

$$(a - b)(c - d) \geq 0 \Rightarrow ac + bd - bc - ad \geq 0 \Rightarrow ac + bd \geq bc + ad.$$

**משפט 32:**

יהי  $X = \{x_1, x_2, \dots, x_k\}$  קבוצת אוטיות בעלת פונקציית ההסתברות  $p_i = P_X(x_i)$  כך ש-

$$p_1 \geq p_2 \geq \dots \geq p_k$$

$$|f(x_i)| = n_i$$

ונתונה הצפנה בינהarity  $f : X \rightarrow \{0, 1\}^*$ . כלומר,  $x_i$  מוצפן ע"י  $n_i$  ספרות בינהירות. אוריינט היצפנת הבינהarity של  $x_i$  הוא  $n_i$ . במלים אחרות, האות  $x_i$  מוצפן על ידי היצפנת שמיימת

$$n_1 \leq n_2 \leq \dots \leq n_k.$$

**הוכחה:** נניח בשלילה שקיים תמורה  $\{n_{i_1}, \dots, n_{i_k}\}$  של  $\{n_1, \dots, n_k\}$  כך שהתווחלה

$$E = n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_{i_j}p_j + \dots + n_{i_k}p_k.$$

היא מינימלית.

לא הגבלת הכלליות נניח כי  $n_1 = n_{i_j}$ . אז

$$E = n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_1p_j + \dots + n_{i_k}p_k.$$

( $n_{i_{j-1}} \geq n_1$  אז בהכרח  $n_1 = \min(n_1, \dots, n_k)$ )

בנוסף  $p_{j-1} \geq p_j$  לכן  $p_1 \geq p_2 \geq \dots \geq p_k$

לכן לפי משפט 31:

$$n_{i_{j-1}}p_{j-1} + n_1p_j \geq n_1p_{j-1} + n_{i_{j-1}}p_j. \quad (1*)$$

לכן אם נחליף  $n_1$  עם  $n_{i_{j-1}}$  ב-  $E$  קיבל את התוחלת החדשה

$$E' = n_{i_1}p_1 + \dots + n_1p_{j-1} + n_{i_{j-1}}p_j + \dots + n_{i_k}p_k$$

כך שלפי (1\*):

$E' = n_{i_1}p_1 + \dots + n_1p_{j-1} + n_{i_{j-1}}p_j + \dots + n_{i_k}p_k \leq n_{i_1}p_1 + \dots + n_{i_{j-1}}p_{j-1} + n_1p_j + \dots + n_{i_k}p_k = E$   
ו"א בסתיו לכך כי  $E'$  התוחלת המינימלית.

**משפט 33: קריפטו-מערכת RSA ניתן לפענוח**

יהי  $p, q$  מספרים ראשוניים שונים,  $a, b \in \mathbb{Z}$  שלמים חיוביים כך ש-  $ab = 1 \pmod{\phi(n)}$

אם  $x \in \mathbb{Z}_n$

$$(x^b)^a = x \pmod{n}.$$

**הוכחה:** נתון כי  $.ab \equiv 1 \pmod{\phi(n)}$   
**לפי משפט 21:**  $\phi(n) = \phi(pq) = (p-1)(q-1)$  ז"א

$$ab \equiv 1 \pmod{\phi(n)} \equiv 1 \pmod{(p-1)(q-1)}$$

לכן קיימים  $t \in \mathbb{Z}$  כך ש-

$$ab - 1 = t(p-1)(q-1).$$

לכל  $z \in \mathbb{Z}$  לפי משפט 23  $.z^{p-1} \equiv 1 \pmod{p}$  בפרט

$$x^{ab-1} = x^{t(p-1)(q-1)} = (x^{t(q-1)})^{p-1} = y^{p-1}$$

כasher  $x^{ab-1} \equiv 1 \pmod{p}$  מכאן  $y = x^{t(q-1)}$

באותה מידת אפשר להראות כי  $x^{ab-1} \equiv 1 \pmod{q}$

$$x^{ab-1} - 1 = 0 \pmod{q} \text{ ו- } x^{ab-1} - 1 = 0 \pmod{p}$$

מכיוון ש-  $p \text{ ו- } q$  זרים אז

$$x^{ab-1} - 1 = 0 \pmod{pq}.$$

לפיכך

$$x^{ab-1} = 1 \pmod{pq}.$$

נכפיל ב-  $x$  ונקבל

$$(x^a)^b \equiv x \pmod{(pq)},$$

ולכן

$$(x^a)^b = x \pmod{(pq)} = x \pmod{n}.$$

ז"א הוכחנו כי לכל טקסט גליי  $x$ , אם נצפין אותו ואז אחר כך נפענה את הטקסט מוצפן המתබל מאלגוריתם RSA, נקבל אותו טקסט גליי המקורי בחזרה.  
■

### משפט 34:

יהיו  $p, q$  מספרים ראשוניים ויהי  $pq = n$ . יי

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

נגיד צוף חדש אשר זהה ל- RSA אלא  $\phi(n)$  הוחלף עם  $\lambda(n)$  כך ש- (ז"א) אזי הкриיפטו-מערכת ניתנת לפענה.

**הוכחה:**

**שלב 1)** רושמים את הצופן:

$$\left. \begin{array}{l} e_k(x) = x^b \pmod{n} \\ d_k(y) = y^a \pmod{n} \end{array} \right\} \quad \begin{aligned} n &= pq, & ab &\equiv 1 \pmod{\lambda(n)}. \end{aligned}$$

**שלב 2)** נתון כי  $(p-1)(q-1) \equiv 1 \pmod{d}$  ז"אקיימים  $p'$  שולם כך ש-

$$p-1 = p'd \iff \frac{p-1}{d} = p' \iff d = \frac{p-1}{p'} \quad (\#1)$$

באותה מידה קיימן  $q'$  שלם כך ש-

$$q - 1 = q'd \Leftrightarrow \frac{q - 1}{d} = q' \Leftrightarrow d = \frac{q - 1}{q'}.$$
(#2)

**שלב 3**

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} = \frac{(p-1)(q-1)}{d}.$$

$$\lambda(n) \stackrel{(\#1)}{=} \frac{(p-1)(q-1)}{\left(\frac{p-1}{p'}\right)} = p'(q-1). \Leftrightarrow d = \frac{p-1}{p'}.$$
(1\*)

$$\lambda(n) \stackrel{(\#2)}{=} \frac{(p-1)(q-1)}{\left(\frac{q-1}{q'}\right)} = q'(p-1). \Leftrightarrow d = \frac{p-1}{p'}.$$
(2\*)

**שלב 4** (נתו) לכן קיימן  $t$  שלם כך ש-  
 $ab \equiv 1 \pmod{\lambda(n)}$

$$ab = 1 + t\lambda(n) \stackrel{(2*)}{=} 1 + t(p-1)q'.$$

לכן

$$ab - 1 = t(p-1)q'.$$

מכאן

$$x^{ab-1}x^{tq'(p-1)} = y^{p-1} \stackrel{\text{פרמייה}}{\equiv} 1 \pmod{p}$$

כאשר  $y = x^{tq'}$  והשווין השני מתקיים בגלל ש-  $p$  מספר ראשוני. לפיכך  
 $x^{ab-1} \equiv 1 \pmod{p}$ .

**שלב 5** (נתו) לכן קיימן  $t$  שלם כך ש-  
 $ab \equiv 1 + t\lambda(n) \stackrel{(1*)}{=} 1 + t(q-1)p'$ .

לכן

$$ab - 1 = t(q-1)p'.$$

מכאן

$$x^{ab-1}x^{tp'(q-1)} = z^{q-1} \stackrel{\text{פרמייה}}{\equiv} 1 \pmod{q}$$

כאשר  $z = x^{tp'}$  והשווין השני מתקיים בgalל ש-  $q$  מספר ראשוני. לפיכך  
 $x^{ab-1} \equiv 1 \pmod{q}$ .

**שלב 6** מכיוון ש-  $p, q$  ראשוניים אז

$$\left. \begin{array}{l} x^{ab-1} \equiv 1 \pmod{q} \\ x^{ab-1} \equiv 1 \pmod{p} \end{array} \right\} \Rightarrow x^{ab-1} \equiv 1 \pmod{pq}$$

לפי

$$x^{ab-1} \equiv 1 \pmod{n} \Rightarrow (x^b)^a \equiv x \pmod{n}$$

כנדרש.

**משפט 35:**

$$a \equiv b \pmod{m} \text{ אם ורק אם } a \pmod{m} = b \pmod{m}$$

**הוכחה:** נניח כי  $a \bmod m = b \bmod m$ . אז  $r = a \bmod m = b \bmod m$

$$a = mq_1 + r, \quad b = mq_2 + r$$

כasher  $q_1, q_2$  מספרים שלמים. ז"א  
 $a - b = mq_1 - mq_2 = m(q_1 - q_2)$ .

$a - b$  מספר שלם שכן  $b \bmod m \mid a - b$  כנדרש.

כעת נניח כי  $a \equiv b \pmod{m}$ . קיימים  $q$  שלם כך ש-

$$a - b = mq$$

נסמן  $m \mid a - b$ . קיימים  $q_1$  שלם כך ש-  
 $a = q_1m + r$ .

מכאן

$$b = a - qm = q_1m + r - qm = (q_1 - q)m + r.$$

ז"א  $b \bmod m = r$  כנדרש.

### משפט 36:

אם  $p$  מספר ראשוני ו-  $n$  מספר שלם חיובי אז

$$\phi(pn) = \begin{cases} (p-1)\phi(n), & p \nmid n \\ p\phi(n), & p \mid n \end{cases}.$$

**הוכחה:** אם  $n \nmid p$  לא מופיע בפירוק לראשוניים של  $n$ . ז"א אם הפירוק לראשוניים של  $n$  הוא

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

ז"א  $p \neq p_i$  לכל  $1 \leq i \leq k$ . לכן הפיקור לראשוניים של  $pn$  הוא  
 $pn = p^1 p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ .

מכאן הfonקציית אוילר עבור  $pn$  היא

$$\phi(pn) = (p^1 - p^0)(p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}).$$

אבל הfonקציית אוילר של  $p$  היה  $\phi(p) = p-1$  והfonקציית אוילר של  $n$  הוא  $\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$ .

$$\phi(pn) = (p-1)\phi(n).$$

אם  $n \mid p$  מופיע בפירוק לראשוניים של  $n$ . ז"א אם הפירוק לראשוניים של  $n$  הוא

$$n = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_i^{e_i} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k}$$

ז"א קיימים  $i, j$  עבורי  $p_i = p_j$ . לכן  
 $np = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_i^{e_i+1} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k}$ .

מכאן הפונקציה אוילר של  $np$  היא

$$\begin{aligned}\phi(np) &= (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_i^{e_{i-1}-1}) (p^{e_i+1} - p^{e_i}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_i^{e_{i-1}-1}) p (p^{e_i} - p^{e_i-1}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_i^{e_{i-1}-1}) (p^{e_i} - p^{e_i-1}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p\phi(n)\end{aligned}$$

### משפט 37:

יהיו  $a$  ו-  $b$  מספרים ראשוניים.

$$\phi(a) = a - 1 \quad .1$$

$$\phi(ab) = (a - 1)(b - 1) \quad .2$$

הוכחה:

1.  $a$  ראשוני לכן הפירוק לראשוניים שלו הוא  $p_1^{e_1}$  כאשר  $p_1 = a$  ו-  $e_1 = 1$ .

לכן הפונקציה אוילר של  $a$  הינה

$$\phi(a) = (p_1^{e_1} - p_1^{e_1-1}) = a - 1$$

2.  $a, p_1 = a, p_2 = b$  ראשוניים לכן הפירוק לראשוניים של  $ab$  הוא  $p_1^{e_1}p_2^{e_2}$  כאשר  $ab = p_1^{e_1}p_2^{e_2}$  ו-  $e_1 = 1, e_2 = 1$ .

לכן הפונקציה אוילר של  $ab$  הינה

$$\phi(ab) = (p_1^{e_1} - p_1^{e_1-1}) (p_2^{e_2} - p_2^{e_2-1}) = (a - 1)(b - 1)$$

### משפט 38:

יהיו  $a, b$  מספרים שלמים.

אם קיימים שלמים  $s, t$  כך ש-  $sa + tb = 1$  אז  $a$  ו-  $b$  זרים.

הוכחה: יהיו  $d$  וה-  $\gcd(a, b) = 1$ . לכן  $d = 1$  או  $d \neq 1$ . אם  $d \neq 1$  בchner  $d$  מחלק  $1$ . לכן  $d \mid 1$  ו-  $d \mid a$  ו-  $d \mid b$ .

### משפט 39:

יהיו  $a, b, n$  שלמים חיוביים. אז  $\gcd(a^n, b^n) = \gcd(a, b)^n$

הוכחה: יהיו  $a, b$  שלמים חיוביים. נסמן  $d = \gcd(a, b)$ . נוכיח  $d \mid a^n$  ו-  $d \mid b^n$ .  
נניח  $a = q_1d$  ו-  $b = q_2d$ .  
נוכיח  $d \mid a^n$  ו-  $d \mid b^n$ .

מכאן

$$\gcd(q_1, q_2) = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) \stackrel{\text{משפט 2}}{=} 1$$

ז"א  $q_1, q_2$  לא חולקים גורמים משותפים (לפי פירוק לגורמים הראשוניים) ולכן גם  $\gcd(q_1^n, q_2^n) = 1$ .

נשים לב:

$$\begin{aligned} \gcd(a^n, b^n) &= \gcd(q_1^n d^n, q_2^n d^n) \\ &= d^n \gcd(q_1^n, q_2^n) \\ &= d^n \\ &= \gcd(a, b)^n. \end{aligned}$$

#### משפט 40:

יהיו  $a, b$  שלמים.

$.c | d : b \rightarrow c$  אם ורק אם לכל מחלק משותף  $c$  של  $a$  ו-  $b$   $d = \gcd(a, b)$

הוכחה:

כיוון  $\Leftarrow$

יהי  $d = \gcd(a, b)$ . נניח כי  $c | a$  וגם  $c | b$ . אזי קיימים שלמים  $a' = a/c$  ו-  $b' = b/c$  שאינם שלמים  $s, t$  עבורם  $d = sa + tb = sca' + tcb' = c(sa' + tb')$ . לכן לכל מחלק משותף  $c$  של  $a$  ו-  $b$  מתקיים  $c | d$ .

כיוון  $\Rightarrow$

נניח שעבור כל מחלק משותף  $c$  של  $a$  ו-  $b$  מתקיים  $c | d$ .

$$d' \leq c \Leftrightarrow d' = qc \Leftrightarrow$$

מכיוון ש-  $c | d$  אז  $c | a$  ו-  $c | b$  ( $\gcd(a, b) \leq c$ , בגלל ש-  $c$  מחלק  $a$  ו-  $b$ )

$$d' \leq \gcd(a, b) \Leftrightarrow d' \leq c \leq \gcd(a, b) \Leftrightarrow$$

מצד שני, הוא עצמו מחלק משותף של  $a$  ו-  $b$ , לכן לפי ההנחה התחלהית,  $\gcd(a, b) \leq d'$  ( $\gcd(a, b) \leq d' \Leftrightarrow d' = Q \gcd(a, b)$ ).

ז"א קיבלנו ש-  $d' = \gcd(a, b)$  ו-  $d' \leq \gcd(a, b)$  ולכן  $d' = \gcd(a, b)$ .

#### משפט 41: האלגוריתם של אוקלידס

אם  $a, b$  שלמים ו-  $b \neq 0$  אז  $\gcd(a, b) = \gcd(b, a \bmod b)$

הוכחה:

$$\text{רأشית נוכיח כי } \gcd(a, b) \mid \gcd(b, a \bmod b).$$

לפי המשפט החילוק של אוקלידיים (משפט קיימים שלמים  $r, q$  עוברים  $a = qb + r = \left\lfloor \frac{a}{b} \right\rfloor b + (a \bmod b)$   $\Rightarrow a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor b$ .  
לכן אם  $d \mid \gcd(b, a \bmod b) \Leftrightarrow d \mid (a \bmod b) \Leftrightarrow d \mid b - d \mid a$  אז  $d = \gcd(a, b)$

$$\text{כעת נוכיח כי } \gcd(b, a \bmod b) \mid \gcd(a, b)$$

נסמן  $(q, r)$   $d \mid (a \bmod b)$  ו-  $d \mid b$   $\Rightarrow d = \gcd(b, a \bmod b)$  קיימים שלמים  $r, q$  עוברים  $a = qb + r = \left\lfloor \frac{a}{b} \right\rfloor b + (a \bmod b)$   
 $d \mid \gcd(a, b) \Leftrightarrow d \mid b$  וגם  $d \mid a$   $\Rightarrow d \mid a$ .

הוכחנו כי  $\gcd(a, b) \mid \gcd(b, a \bmod b) \wedge \gcd(b, a \bmod b) \mid \gcd(a, b)$   
 $\gcd(a, b) = \gcd(b, a \bmod b)$ .



#### משפט 42: הקשר בין יחס שקלות מודולרי והשארית

יהיו  $a, b, m$  שלמים חיוביים.

הוכחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:  
 $a \bmod m = b \bmod m$  אם ורק אם  $a \equiv b \pmod{m}$

הוכחה:

כיוון  $\Leftarrow$

נניח ש-  $a \equiv b \pmod{m}$ . אז קיים שלם  $Q$  כך ש:  $a = qm + b$ .

לפי המשפט החילוק של אוקלידיים,  
 $b = \bar{q}m = r_1$ ,  $r_1 = b \bmod m$ .

לכן

$$a = (q + \bar{q})m + r_1 = Qm + r_1$$

כאשר  $\bar{q}$  שלם ו-  $0 \leq r_1 < b$  הוא השארית  $r_1 = b \bmod m$ . מכאן נובע ש:

$$a \bmod m = a - m \left\lfloor \frac{a}{m} \right\rfloor = Qm + r_1 - Qm = r_1$$

$$a \bmod m = r_1 = b \bmod m$$

ז"א

כיוון  $\Rightarrow$

נניח ש-  $a \bmod m = b \bmod m$

$$a - m \left\lfloor \frac{a}{m} \right\rfloor = b - m \left\lfloor \frac{b}{m} \right\rfloor \Rightarrow a = \left( \left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor \right) m + b \Rightarrow a = qm + b$$

כלומר קיים שלם  $q = \left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor$

**משפט 43:**

יהיו  $a, m$  מספרים זרים.

הוכחה:

כיוון

נניח כי  $.ab \equiv ac \pmod{m}$

$$ab \equiv ac \pmod{m} \Rightarrow ab = ac + qm \Rightarrow ab - ac = qm \Rightarrow a(b - c) = qm .$$

מכאן  $qm | a$ .

$.q = ak$  זרים לכך  $a \nmid q$  לכן  $q | a$ .

לפיכך  $m | k$  שלם עבורו  $k = km$

$$a(b - c) = qm \Rightarrow a(b - c) = akm \Rightarrow b - c = km \Rightarrow b = c + km \Rightarrow b \equiv c \pmod{m} .$$

כיוון

נניח כי  $.b \equiv c \pmod{m}$

$$b = qm + c \Rightarrow ab = aqm + ac \Rightarrow ab \equiv ac \pmod{m} .$$

**משפט 44:**

יהיו  $a, m$  מספרים (לא בהכרח זרים).

$.b \equiv c \pmod{\frac{m}{\gcd(a, m)}}$  אם ורק אם  $ab \equiv ac \pmod{m}$

הוכחה:

כיוון

נניח כי  $.ab \equiv ac \pmod{m}$

$$ab = ac + qm \Rightarrow ab - ac = qm \Rightarrow m | a(b - c) \Rightarrow \frac{m}{\gcd(a, m)} | \frac{a}{\gcd(a, m)}(b - c) .$$

מכיוון ש-  $\frac{a}{\gcd(a, m)}$  ו-  $\frac{m}{\gcd(a, m)}$  זרים, אז

$$\frac{m}{\gcd(a, m)} | (b - c) .$$

לכן

$$b \equiv c \pmod{\left(\frac{m}{\gcd(a, m)}\right)}.$$

#### משפט 45:

יהיו  $a, b, c$  שלמים.  
אם  $a^n \equiv b^n \pmod{c}$  אז  $a \equiv b \pmod{c}$   $\forall n > 1$ .

**הוכחה:** אם  $a \equiv b \pmod{c}$  אז קיים שלם  $q$ :

$$a = qc + b.$$

לכן

$$a^n = (qc + b)^n = \left( \sum_{k=1}^n \binom{n}{k} q^k c^{k-1} b^{n-k} \right) c + b^n = Qc + b^n$$

כאשר  $Q$  שלם. לכן קיים שלם  $Q$  כך ש:

$$a^n = Qc + b^n \Rightarrow a^n \equiv b^n \pmod{c}.$$

#### משפט 46: מחזור בחזקת האורך שלה הוא תמורה זהה

תהי  $\Sigma \rightarrow \Sigma : \pi$  תמורה מעל אלפבית  $\Sigma$ . אם  $\pi$  היא מחזור של אורך  $k$  אז  $\pi^k = \text{id}$ .

**הוכחה:** נניח כי  $\Sigma \rightarrow \Sigma : \pi$  מחזור באורך  $k$ . ז"א הפירוק למחזוריים של  $\pi$  הוא:  
 $\pi = (a_1 \ a_2 \ \dots \ a_{k-1} \ a_k)$ ,

או, כפונקציה מעל  $\Sigma$ :

$$\pi(a_1) = a_2, \quad \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \quad \pi(a_k) = a_1.$$

אפשר לרשום את זה בביטוי ייחיד:

$$\pi(a_i) = a_{(i \bmod k)+1}.$$

עבור  $\pi^2$ :

$$\pi^2(a_1) = a_3, \quad \pi^2(a_2) = a_4, \quad \dots \quad \pi^2(a_{k-2}) = a_k, \quad \pi^2(a_{k-1}) = a_1, \quad \pi^2(a_k) = a_2.$$

ובאותה מידה אפשר לרשום  $\pi^2$  בביטוי ייחיד:

$$\pi^2(a_i) = a_{((i+1) \bmod k)+1}.$$

באופן כללי לכל  $j \geq 0$  טבעי:

$$\pi^j(a_i) = a_{((i+j-1) \bmod k)+1}.$$

מכאן נציב  $j = k$ :

$$\pi^k(a_i) = a_{((i+k-1) \bmod k)+1} = a_{((i-1) \bmod k)+1} = \begin{cases} a_i & : i < k \\ a_k & : i = k \end{cases}.$$

ז"א לכל  $1 \leq i \leq k$

$$\pi^k(a_i) = a_i \Rightarrow \pi^k = \text{id}$$

#### משפט 47: תנאי סודיות מושלמת של צופן קיסר

אם לכל מפתח  $K \in K$  בצופן קיסר יש הסתברות שווה, כלומר

$$P(K = k) = \frac{1}{26} .$$

אז לצופן קיסר יש סודיות מושלמת.

**הוכחה:** תחילה נחשב את ההסתברות  $P(Y = y)$  באמצעות (??). הקבוצה מפתחות בצופן קיסר היא  $K = \{0, 1, \dots, 25\} = \mathbb{Z}_{26}$ .

לכן

$$P(Y = y) = \sum_{k \in \mathbb{Z}_{26}} P(K = k) P(X = d_k(y)) .$$

אם ההסתברות של כל מפתח שווה אז  $P(K = k) = \frac{1}{26}$  ולכן

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = d_k(y)) .$$

הכלל מצפין והכלל מפענח של צופן קיסר מוגדרים

$$e_k(x) = x + k \pmod{26}, \quad d_k(y) = y - k \pmod{26} .$$

כאשר  $k \in \mathbb{Z}_{26}$ . לכן  $P(X = d_k(y)) = P(X = y - k \pmod{26})$ . לפיכך

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = y - k \pmod{26}) .$$

הסכום בצד ימין הוא רק סכום של  $P(X = k)$  מעל כל האיברים ב- $\mathbb{Z}_{26}$ . לכן

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = k) = \frac{1}{26} \cdot 1 = \frac{1}{26} .$$

כאשר בשווין השני השתמשנו בתכונת הנרמול של הפונקציית הסתברות של המ"מ  $X$ .

מצד שני, לפי (??),

$$P(Y = y|X = x) = \sum_{\substack{k \in \mathbb{Z}_{26} \\ x = d_k(y)}} P(K = k)$$

האילוץ על הסכום  $x = d_k(y)$  אומר ש-

$$x = k - y \pmod{26} \Rightarrow k = x + y \pmod{26} .$$

לכל  $X \in x$  ולכל  $Y \in y$  קיים רק מפתח אחד אשר מקיים תנאי זה. זו"א רק איבר אחד של הסכום נשאר ולפיכך

$$P(Y = y|X = x) = \sum_{\substack{k \in \mathbb{Z}_{26} \\ x = d_k(y)}} P(K = k) = P(K = y - x \pmod{26}) .$$

אם ההסתברות של כל מפתח שווה, כלומר  $P_K(k) = \frac{1}{26}$  אז

$$P(Y = y|X = x) = P(K = y - x \pmod{26}) = \frac{1}{26} .$$

לכן

$$P(Y = y) = \frac{1}{26} = P(Y = y|X = x)$$

■ "א' לצופן קיסר יש סודיות מושלמת.  
במילים פשוטות צופן קיסר אינו ניתן לפענה בתנאי שימושים בפתח מקרי חדש כל פעם שמצפינים אותו אחד של טקסט גלי.

#### משפט 48: תנאי חילופי לסודיות מושלמת

לפי נוסחת בייס אם לкриpto-מערכת יש סודיות מושלמת אז מתקיים גם  $P(Y = y|X = x) = P(Y = y)$ . (1)

#### משפט 49:

נתונה קריpto-מערכת בעלת סודיות מושלמת.

אם  $P(Y = y) > 0$  אז

1) קיימים לפחות מפתח אחד  $k \in K$  כך שה-

$$. |K| \geq |Y| \quad (2)$$

הוכחה:

1) לפי (1), (#1)

$$P(Y = y|X = x) = P(Y = y) > 0$$

נציב (?) בצד שמאל ונקבל

$$\sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) = P(Y = y) > 0 \quad (\#2)$$

א"

$$\sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) > 0 \quad (\#3)$$

לכן קיימים לפחות מפתח אחד,  $k$  עבורו

"א' קיימים לפחות מפתח אחד,  $k$  עבורו  $y = e_k(x)$ .

2) לפי (#1) ו- (#3), לכל  $Y \in Y$  קיימים לפחות מפתח אחד,  $k$  עבורו  $y = e_k(x)$ , לכן בהכרח  $|K| \geq |Y|$ . (#4)

#### משפט 50: משפט שאנו

נתונה קריpto-מערכת  $(X, Y, K, E, D)$  כך שה-  $|K| = |X| = |Y|$  ולמערכת יש סודיות מושלמת אם ורק אם

1) לכל  $x \in X$  ולכל  $y \in Y$  קיים מפתח  $k$  ייחיד עבורו  $y = e_k(x)$

2) לכל מפתח יש הסתברות שווה, כלומר  $P(K = k) = \frac{1}{|K|}$

הוכחה:

1) נניח כי  $|K| = |Y|$ . כלומר

$$|\{e_k(x) | x \in X\}| = |K| .$$

ז"א לא קיימים שני מפתחות  $k_1 \neq k_2$  כך ש-  $e_{k_1}(x) = y = e_{k_2}(x)$ .

לכן לכל  $x \in X$  ולכל  $y \in Y$  קיים מפתח  $k$  ייחיד עבורו  $y$ .

2) נסמן אורך של קבוצת מפתחות ב-  $n = |K|$ . נרשום את הקבוצת טקטים גלויים כ-

$$X = \{x_i | 1 \leq i \leq n\} .$$

נתון  $y \in Y$  קבוע. נמספר את המפתחות  $i$  כך ש-  $e_{k_i}(x_i) = y$ . לפי נוסחת בייס,

$$\begin{aligned} P(X = x_i | Y = y) &= \frac{P(Y = y | X = x_i)P(X = x_i)}{P(Y = y)} \\ &\stackrel{\text{לפי (??)}}{=} \frac{P(K = k_i)P(X = x_i)}{P(Y = y)} \end{aligned}$$

אם המערכת יש סודיות מושלמת אז  $P(X = x_i | Y = y) = P(X = x_i)$  לכן

$$P(X = x_i) = \frac{P(K = k_i)P(X = x_i)}{P(Y = y)} \Rightarrow P(K = k_i) = P(Y = y)$$

לכל  $1 \leq i \leq n$ . ז"א לכל מפתח יש הסתברות שווה

$$P(K = k_i) = \frac{1}{|K|} .$$

### משפט 51: אנטרופיה של שאנון

נתון משתנה מקרי  $X$  בעל פונקציית ההסתברות  $P_X(x)$ . התוחלת המינימלית של אורך ההצפנה של  $X$  מסומן ב-  $H[X]$  ונתונה על ידי הנוסחה

$$H[X] = - \sum_{x \in X} P_X(x) \log_2 P_X(x) .$$

נקרא **האנטרופיה** של  $X$   $H[X]$

הוכחה: נניח כי  $X = Y \cap Z$ , כאשר  $Y, Z$  משתנים מקרים בלתי תלויים. לפי משווואה (??):

$$\ell_Q(x) = f(p_x) .$$

$$H[X] = \sum p_x \ell_Q(x) = \sum p_x f(p_x) .$$

תהיינה  $P_Z(z)$  ו-  $P_Y(y)$  פונקציות ההסתברות של  $Z$  ושל  $Y$  בהתאם.

$$p_z = P_Z(z) \text{ ו- } p_y = P_Y(y)$$

מכיוון ש-  $Y$  ו-  $Z$  משתנים בלתי תלויים אז

$$P(X = Y \cap Z) = P_Y(y)P_Z(z) = p_y p_z .$$

נשים לב שידיעה של  $Y$  לא נותנת שום מידע על הערך של  $Z$ , שכן  
 $\ell_Q[Y \cap Z] = \ell_Q[Y] + \ell_Q[Z]$  .

לפיכך

$$H[X] = \sum p_x \ell_Q(x) = \sum p_y p_z [\ell_Q(y) + \ell_Q(z)]$$

מכאן

$$H[X] = \sum p_y p_z f(p_y p_z) = \sum p_y p_z [f(p_y) + f(p_z)]$$

$$f(p_y p_z) = f(p_y) + f(p_z) .$$

$$\text{לכל } p_y \text{ ו- } p_z. \text{ שכן} . f(p) = C \log(p)$$

כעת נניח כי יש לנו משתנה מקרי  $X = \{a, b\}$  בעל פונקציית ההסתברות  $P_X(a) = \frac{1}{2}, P_X(b) = \frac{1}{2}$ . ההצפנה של  $X$  צריכה ספרה אחת, שכן  $f(p) = -\log_2(p)$  ונקבל  $f(\frac{1}{2}) = 1$ . לכן נשים  $f(Q^*(a)) = \ell_Q^*(b) = 1$ .

■

### משפט 52:

נתון מ"מ בדיד  $X$  אשר מקבל  $N$  ערכים שונים

$$X = \{x_1, \dots, x_N\}$$

בהתשובות שווה, כולם

$$P(X = x_i) = \frac{1}{N}$$

אז האנטרופיה מקבלת ערך מקסימלי שניתנת על ידי

$$H_{\max}(X) = \log_2 N .$$

ערך זה הוא הערך המקסימלי האפשרי של האנטרופיה.

### משפט 53: אי שוויון האפמן

נתון קבוצת אובייקטים של טקסט גליי  $X$  והצפנה האפמן  $f$ . נניח כי  $l(f)$  תוחלת האורך של ההצפנה ו-  $H(X)$  האנטרופיה של הטקסט גליי. מתקיים

$$H(X) \leq l(f) \leq H(X) + 1 .$$