לינארית 2 הרצאה מספר 11

תזכורת: פונקציית אוילר

לכל מספר טבעי n הגדרנו $\varphi(n)$ - כמות המספרים הטבעיים מולו n. כאינו כי $\varphi(n)$ שווה גם לגם למספר המספרים הזרים ל- n (מ- 1 עד n).

כאינו כי: $\varphi(p) = p-1$, כאשר p מספר ראשוני.

כאינו כי: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(p-1)$, כאשר p מספר ראשוני ו- α מספר טבעי.

כאינו כי: $\varphi(p\cdot q) = (p-1)(q-1)$, כאשר p, q מספרים ראשוניים.

כאינו כי: $\varphi(p^\alpha q^\beta) = p^\alpha q^\beta\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$, כאשר p, q מספרים ראשוניים ו- α, β מספרים טבעיים.

אפשר גם להוכיח כי לכל $m, n \in \mathbb{N}$ כאשר m ו- n זרים מתקיים: $\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n)$

נסיק מסקנה: אם $n = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ כאשר $p_1, p_2, \ldots, p_k$ מספרים ראשוניים ו- $\alpha_1, \alpha_2, \ldots, \alpha_k$ טבעיים, אז:

$$\varphi(n) = \varphi(p_1^{\alpha_1})\cdot\varphi(p_2^{\alpha_2})\cdot\ldots\cdot\varphi(p_k^{\alpha_k})$$

$$= p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

מתקיים לפי הנתון $n = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ ולכן סך הכל נוכל לרשום:

$$\varphi(n) = \underbrace{p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}}_{n}\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right) = n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

$$\boxed{\varphi(n) = n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)}$$

דוגמה: $\varphi(1176)$

מתקיים:

1176	588	294	147	49	7	1
2	2	2	3	7	7	

נינקנו את המספר לגורמים ראשוניים כלומר $\varphi(1176) = \varphi(\underbrace{2}_{p_1}{}^3\cdot\underbrace{3}_{p_2}{}^1\cdot\underbrace{7}_{p_3}{}^2)$. לפי פי הנוסחה:

$$\boxed{\varphi(n) = n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)}$$

$$\Downarrow$$

$$\varphi(1176) = 1176\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right) = 1176\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{6}{7} = 336$$

משפט אוילר:

יהי $n \geq 1$ מספר טבעי. ויהי $a \in \mathbb{N}$ זר ל- n (כלומר $\gcd(a,n) = 1$)

אז:

$$\boxed{a^{\varphi(n)} = 1 \pmod{n}}$$

נדגים זאת: לדוגמה עבור $n = 24$ מתקיים $\varphi(24) = \varphi(2^3 \cdot 3^1)$ לכן: $\varphi(24) = 24 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 8$.
ניקח מספר זר ל- 24, לדוגמה ניקח את 5 (5 זר ל- 24 כי $\gcd(5,24) = 1$). לפי הנוסחה של משפט אוילר אנו אומרים לקבל ש- 5 בחזקת 8 שווה ל- 1 מודולו 24.

$$5^2 \equiv 25 \equiv 1 \pmod{24}$$

$$\Downarrow$$

$$(5^2)^2 \equiv 5^4 \equiv 1^2 \equiv 1 \pmod{24}$$

$$\Downarrow$$

$$\left((5^2)^2\right)^2 \equiv 5^8 \equiv 1^2 \equiv 1 \pmod{24}$$

$$5^8 \overset{?}{\equiv} 1 \pmod{24}$$

$$\downarrow$$

$$5^8 \equiv 1 \pmod{24} \checkmark$$

דוגמה: מצאו את 3 הספרות האחרונות של המספר 3^{2024}.

פתרון: שלושת הספרות האחרונות של מספר הן שארית החלוקה של אותו מספר ב- 1000.
לכן צריך לחשב את:

$$3^{2024} \pmod{1000}$$

המספרים 3, 1000 זרים כי $\gcd(3,1000) = 1$, ולכן $3^{\varphi(1000)} = 1 \pmod{1000}$ לפי משפט אוילר.
כעת נצטרך לגלות מה הוא $\varphi(1000)$?

$$\varphi(1000) = \varphi(2^3 \cdot 5^3) = 1000 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400$$

לכן לפי משפט אוילר:

$$3^{400} \equiv 1 \pmod{1000}$$

מכאן נוכל להגיע ש-

$$3^{2000} = \left(3^{400}\right)^5 \equiv 1^5 \pmod{1000} = 1 \pmod{1000}$$

נשאר לחשב את $3^{24} \pmod{1000}$:

$$3^5 = 243 \pmod{1000}$$

$$3^{10} = \left(3^5\right)^2 = 243^2 \pmod{1000} = 59049 \pmod{1000} \equiv 49 \bmod (1000)$$

$$3^{20} = \left(3^{10}\right)^2 = 49^2 \pmod{1000} = 2401 \pmod{1000} \equiv 401 \pmod{1000}$$

$$3^4 = 81 \pmod{1000} \Rightarrow 3^{24} = 3^{20} \cdot 3^4 = 401 \cdot 81 \pmod{1000} = 481 \pmod{1000}$$

לכן:

$$3^{2024} = 3^{2000} \cdot 3^{24} = 1 \cdot 481 \pmod{1000} = 481 \pmod{1000}$$

שלוש הספרות האחרונות הן 481.

שימוש בחזקת במספרים להצפנה:

תיאור כללי: נתון מרחב מסרים אפשריים M.

מגדירים את המסר הנתון ע"י פונקציה $f: M \to M$.

כלומר אם $m \in M$ הוא מספר נתון אז $f(m)$ הצפנה.

פיענוח מתבצע ע"י שימוש בפונקציה נוספת $g: M \to M$, כך ש- $g(f(m)) = m$ לכל $m \in M$.

למשל: אם M הוא אוסף של מחרוזות בינאריות באורך n ו- A מטריצה בינארית הפיכה מסדר $n \times n$

אז $f: M \to M$ הנתונה ע"י $f(x) = A \cdot x$ - הצפנה.

ו- $g: M \to M$ הנתונה ע"י $g(y) = A^{-1} \cdot y$ - פיענוח.

הערה: יש מיסכון, אם יודע A (כלומר שיטת הצפנה) אז קל מאוד לגלות את A^{-1} (כלומר את שיטת הפיענוח).

הצפנה עם מפתח פומבי:

אליס (A) ובוב (B) מחליפים מסרים ביניהם.

הם רוצים לבצע הצפנה של התקשורת שלהם.

P_A - מפתח פומבי של אליס - יודע לכולם.

P_B - מפתח פומבי של בוב - יודע לכולם.

S_A - מפתח סודי של אליס - יודע רק לאליס.

S_B - מפתח סודי של בוב - יודע רק לבוב.

אליס שולחת לבוב מסר מוצפן ע"י מפתח הסודי שלה כלומר ע"י $P_B(m)$

בוב מקבל את המסר ומפענח אותו ע"י מפתח סודי שלו: $S_B(P_B(m)) = m$

הערה:

א. S_B אכן פעמם להצפנה P_B (כלומר שהמפתח הפומבי יהיה באמת רק שמאפשר לפענח את הצפנן בסודי שלו).

ב. קשה מאוד לגלות את S_B בהינתן P_B (כלומר קשה לגלות את המפתח הסודי בהינתן המפתח הפומבי).

שיטת דיפי הלמן

בוחרים מספר ראשוני P.

בוחרים מספר g בעל תכונה שבחזקות של g: $g, g^2, g^3, \dots, g^{P-1}$ מכסות את כל המספרים $1, 2, \dots, P-1$ מודולו P

(תנאי יש g כזה).

מתקיים כי (P, g) - יודע לכולם.

אליס בוחרת $2 \le a \le P-1$. a הוא המפתח הסודי של אליס $(S_A = a)$

אליס יוצרת מפתח פומבי: $P_A = g^a \pmod P$

בוב בוחר $2 \le b \le P-1$. b הוא המפתח הסודי של בוב $(S_B = a)$.

בוב יוצר מפתח פומבי: $P_B = g^b \pmod P$

אליס ובוב יכולים לייצר מפתח משותף (סודי) משלהם:

$$\underbrace{(g^b)^a = g^{ab} \pmod P}_{\text{מה שאליס יכולה לעשות עם המפתח הפומבי של בוב}}$$

$$\underbrace{(g^a)^b = g^{ab} \pmod P}_{\text{מה שבוב יכול לעשות עם המפתח הפומבי של אליס}}$$

הם משתמשים ב- g^{ab} להצפנה: $g^{ab} \cdot m \pmod P$ ומשתמשים ב- $(g^{ab})^{-1}$ לפיענוח: $(g^{ab})^{-1}(g^{ab} \cdot m) = m \pmod P$

3^α	3^1	3^2	3^3	3^4	3^5	3^6	
תוצאה mod 17	3	9	10	13	5	15	....

דוגמה: $g=3$, $P=17$

עבור אליס: $a=4$

עבור בוב: $b=3$

מפתח פומבי של אליס: $3^4 \pmod{17} = 13 \pmod{17}$

מפתח משותף (סוד) של בוב ואליס: $13^3 \pmod{17} = 4 \pmod{17}$ (לוקח מפתח פומבי של אליס ומעלה בחזקת b)

נניח כי בוב שולח לאליס מסר $m=10$.

הוא מצפן אותו ע"י כפל במפתח משותף 4.

כלומר אליס מקבלת: $6 \pmod{17} = 10 \cdot 4 \pmod{17}$

אליס רוצה לבטח את המסר $6 \pmod{17}$ שהיא קיבלה מבוב.

כדי לעשות זאת אליס צריכה למצוא את ההופכי של $4 \pmod{17}$ כלומר אם נסמן ב- x את המפתח ההופכי אזי:

צריך להתקיים: $4 \cdot x = 1 \pmod{17}$ (ניתן למצוא זאת ע"י אלגוריתם אוקלידס) ולקבל: $x = 13 \pmod{17}$.

אליס רוצה לבטח את המסר $6 \pmod{17}$ שהיא קיבלה, היא צריכה להכפיל אותו ב- x:

$$m = 6 \pmod{17} \cdot 13 \pmod{17} = 78 \pmod{17} = 10 \pmod{17}$$

שיטת RSA:

בוחרים $n = p \cdot q$ כאשר p, q מספרים ראשוניים גדולים.

$\varphi(n) = (p-1)(q-1)$.

בוחרים מספר e המקיים e זר ל- $\varphi(n)$. מחשבים f כך שמתקיים: $ef = 1 \pmod{\varphi(n)}$

(e,n) - יצוא לכולם.

בהינתן מסר m, הצפנה היא: $m^e \pmod{n}$ <= הצפנה

פיענוח:

$$(m^e)^f = m^{ef} = m^{\varphi(n)\cdot k + 1} \pmod{n} = \left(\underbrace{m^{\varphi(n)}}_{\substack{1 \text{ לפי} \\ \text{משפט אויילר} \\ \text{כאשר } n,m \text{ זרים.}}}\right)^k \cdot m \pmod{n} = m \pmod{n}$$

ef - שארית חלוקה 1 ב- $\varphi(n)$

לכן:

$$ef = \varphi(n) \cdot k + 1$$

לסיכום, בשיטה זו הצפנה זה לעלות בחזקת e ופיענוח זה לעלות את המסר שקיבלנו בחזקת f.

דוגמה: $p=11$, $q=29$ (קיים למען הבמחשב).

מתקיים: $n = pq = 319$. בנוסף נתון $e=3$.

לכן המפתח הפומבי שלנו הוא $(319,3)$ והוא יצוא לכולם.

נחשב את $\varphi(n)$:

$$\varphi(n=319) = (p-1)(q-1) = 10 \cdot 28 = 280$$

אנחנו צריכים למצוא את f כאשר $e=3$ כלומר את $3f$:

$$3f = 1 \pmod{\varphi(n)} \equiv 1 \pmod{280}$$

$$\Downarrow$$

$$3f = 1 \pmod{280} \longrightarrow f = 187 \pmod{280}$$

נתון מספר $m = 100$:

הבנת: $100^3 \pmod{319} \equiv 254 \pmod{319}$

נשאלת:

$$(254)^{187} \bmod (319) \equiv \underbrace{???\ldots}_{\text{צריך להיות שיטה יעילה למציאת חזקות מודולו}} = 100 \pmod{319}$$

מציאת הופכי מודולו מספר נתון בעזרת אלגוריתם אוקלידס:

רוצים למצוא x כאשר מתקיים השוואה $4 \cdot x = 1 \pmod{17}$ כלומר למצוא את ההופכי של 4 (כאשר אנחנו עובדים תחת מודולו 17). נחלק את 17 ב- 4 עם שארית:

$$17 = 4 \cdot 4 + \underset{\text{שארית}}{1} \Rightarrow 1 = 17 - 4 \cdot 4$$

$$4 = 1 \cdot 4 + 0 \qquad 4 \cdot \underbrace{(-4)}_{x} = 1 \pmod{17}$$

$$x = -4 \pmod{17} = 13 \pmod{17}$$

דוגמה נוספת: $3x = 1 \pmod{280}$. נחלק את 280 ב- 3 עם שארית:

$$280 = 3 \cdot 93 + \underset{\text{שארית}}{1} \qquad 1 = 280 - 3 \cdot 93 \pmod{280}$$

$$1 \pmod{280} = -3 \cdot 93 \pmod{280}$$

$$3 = 3 \cdot 1 + \underset{\text{שארית}}{0} \qquad x = -93 \pmod{280} = 187 \pmod{280}$$

דוגמה נוספת: $11 \cdot x \equiv 1 \pmod{280}$

$$280 \equiv 11 \cdot 25 + \underset{\text{שארית}}{5}$$

$$11 = 5 \cdot 2 + 1 \longrightarrow 1 = 11 - 5 \cdot 2 = 11 - (\underbrace{280 - 11 \cdot 25}_{5}) \cdot 2 = 51 \cdot 11 - 2 \cdot 280$$

$$5 = 1 \cdot 5 + 0$$

$$51 \cdot 11 = 1 + 2 \cdot 280$$

$$51 \cdot 11 = 1 \pmod{280}$$

$$11 \cdot x \equiv 1 \pmod{280}$$

$$280 = 11 \cdot 25 + 5 \qquad 1 \pmod{280} = 11 - 5 \cdot 2 = 11 - 2(280 - 11 \cdot 25) \pmod{280}$$

$$11 = 5 \cdot 2 + 1 \qquad 1 \pmod{280} = 11 - 2 \cdot 280 + 50 \cdot 11 \pmod{280}$$

$$1 \pmod{280} = 51 \cdot 11 - 2 \cdot 280 \pmod{280}$$

$$5 = 1 \cdot 5 + 0 \qquad 1 \pmod{280} = 51 \cdot 11 - 2 \cdot 280 \pmod{280}$$

$$1 \pmod{280} = 51 \cdot 11 \Rightarrow \underbrace{51}_{x = 51} \cdot 11 = 1 \pmod{280}$$

$4 \cdot x = 1 \pmod{17}$

$17 = 2^4 + 1$

$4 = 1 \cdot 2^2 + \underline{\underline{0}}$

$1 \pmod{17} = 17 - 2^4 \pmod{17}$

$1 \pmod{17} = 17 - (17-1) \mod 17$

$1 \pmod{17} = 17 - 16 \mod 17$

$1 \pmod{17} = 17 - 4 \cdot 4 \pmod{17}$

$4x = 1 \pmod{17}$

$4x = 18 \pmod{17}$

$4x = 35 \pmod{17}$

$4x = 52 \pmod{17}$

$x = 13 \pmod{17}$

$11x = 1 \pmod{280}$

$11x = 281 \pmod{280}$

$11x = 561 \pmod{280}$

$11x = \frac{561}{11} \pmod{280} = 51 \pmod{280}$

$3x = 1 \pmod{280}$

$3x = 281 \pmod{280}$

$3x = 561 \pmod{280}$

$x = \frac{561}{3} \pmod{280} = 187 \pmod{280}$