

הערה: חלק מהסימונים לא עשיתי בצורה כל כך טובה, אתקן את זה מתישהו, אם מישהו יודע איך אשמח אם הוא יצור קשר איתי.

## הרצאה 5

### משפט ווילסון – Wilson

מספר טבעי  $n > 1$  הוא מספר ראשוני אם  $(n-1)! \equiv (-1) \pmod{n}$

#### הוכחה

$\Leftarrow$  עבור  $n = p$  ראשוני כלשהו, חבורת אוילר היא  $U_p = \{1, 2, \dots, p-1\}$ .

כיוון שהחבורה אבלית, מכפלת כל האיברים היא  $m = (p-1)!$ , ומקיימת  $m^2 = 1 \pmod{p}$  ע"י הצבת כל איבר ליד ההופכי שלו הודות לקומוטטיביות.

כל איבר  $a$  ההפוך לעצמו:  $0 = a^2 - 1 = (a-1)(a+1)$ , כיוון שאין מחלקי אפס ב  $U_p$ , האיברים ההופכיים לעצמם הם רק  $\pm 1$  (כי אחד הגורמים צריך להתאפס), מכאן שלכל איבר אחר יש איבר הופכי אחר, לכן במכפלת כל האיברים פעם אחת האיבר היחיד שלא מצטמצם הוא  $-1$  ולכן  $m \equiv (-1) \pmod{p}$

$\Rightarrow$  נניח בשלילה כי  $n$  אינו ראשוני, אם  $n=4$  קל לבדוק ש:  $(4-1)! = 6 \equiv 2 \pmod{4}$

עבור  $n > 4$  כיוון ש- $n$  אינו ראשוני ב  $\mathbb{Z}_n^*$  (לגבי כפל) יש בהכרח לפחות איבר אחד  $a$  מחלק אפס. אם  $a = \sqrt{n}$  אז  $a^2 = n < 2a < a^2 = n$  ולכן  $4 < n \Rightarrow 2 < a \Rightarrow 2a < a^2 = n$  ולכן  $2a^2$  מאפס אותה (מודולו  $n$ ).

אחרת  $(n \neq \sqrt{n}) \Rightarrow \exists 1 < a, b < n \quad ab \equiv 0 \pmod{n}$

### תרגיל (מועד א 2007)

הוכח או הפרך:

$1 + 70! \mid 71$  נכון כי  $71$  ראשוני ולכן ע"פ משפט ווילסון.

$1 + 116! \mid 117$  לא נכון כי  $117 = 9 * 13$  ולכן  $117 \mid 116! + 1 \Rightarrow 13 \mid 116! + 1$ .

### קוסטים ומשפט לגרנז'

#### הגדרה

תהא חבורה  $G$  ות"ח  $H$ , שני איברים  $x, y \in G$  יקראו קונגורוארטים משמאל מודולו  $H$  אם:

$$x \sim^L y \Leftrightarrow \exists h \in H : x = yh$$

( $x$  הוא הזזה של  $y$  ע"י איבר  $H$ )

#### טענה

היחס  $\sim^L$  הוא יחס שקילות

### הוכחה

רפלקסיביות:  $x \sim^L x : x = xe$

סמטריות:  $x \sim^L y \Rightarrow x = yh \Rightarrow xh^{-1} = y \Rightarrow y \sim^L x$

טרנזיטיביות:  $x \sim^L y, y \sim^L z \Rightarrow x = yh_1, y = zh_2 \Rightarrow x = zh_2h_1 = zh_3 \Rightarrow x \sim^L z$

באופן דומה מגדירים גם את  $x \sim^R y$

### הגדרה

הקוסט השמאלי של  $a \in G$  לגבי  $H$  הוא אוסף כל האיברים השקולים משמאל ל- $a$  מודולו  $H$ , כלומר

$$aH = \{ah : h \in H\}$$

נשים לב כי  $a \in H \Leftrightarrow aH = H$

אכן  $\Rightarrow$  נובע מתוך סגירות

$\Leftarrow$  אם  $a \notin H$  אזי  $a^{-1} \notin H$  אז  $aH$  אינן  $e$

באופן כללי יחס השקילות מחלק את איברי  $G$  למחלקות שקולות זרות  $aH$

### דוגמאות

$$H = \{0,2,4\} = 2\mathbb{Z}_6 \leq \mathbb{Z}_6$$

$$0 + H = H$$

$$2 + H = H$$

$$4 + H = H$$

כלומר  $\{0,2,4\}$  נציגים של אותו קוסט.

$$H = \{0,3\} = 3\mathbb{Z}_6 \leq \mathbb{Z}_6$$

כאן יש 3 קוסטים,  $0 + H = H, 1 + H = \{1,4\}, 2 + H = \{2,5\}$

באותו אופן מגדירים קוסט ימני  $H \cdot a$ .

### הגדרה

קבוצת המנה של החלוקה משמאל ב- $H$  היא קבוצת הקוסטים השמאליים:

$$G/H = \{aH : a \in G\}$$

אפשר גם להגדיר את קבוצת הקוסטים הימניים:  $H \backslash G = \{Ha : a \in G\}$

### טענה

תהא  $G$  חבורה ו  $H \leq G$  אזי  $|G/H| = |G \setminus H|$

### הוכחה

נגדיר את ההעתקה  $\varphi: \frac{G}{H} \rightarrow H \setminus G$

$$gH \rightarrow Hg^{-1}$$

$$Hg_1^{-1} = Hg_1^{-1} \Rightarrow H \underbrace{g_1^{-1}g_2}_{\in H} = H \Rightarrow g_2H = g_1H : \text{חח"ע}$$

ברור ש  $\varphi$  על שכן לכל תמונה  $Hg^{-1}$  יש מקור  $gH$

נקרא לגודל של קבוצת המנה ה"אינדקס של  $H$  ב- $G$ ".

$$[G:H] = |G/H|$$

### משפט לגרנז'

תהא  $G$  חבורה סופית, אזי לכל ת"ח  $H \leq G$  מתקיים  $[G:H] = \frac{|G|}{|H|}$

### הוכחה

לכל  $a \in G$  נגדיר את ההעתקה  $\varphi_a = H \rightarrow Ha$

ההעתקה חח"ע שכן  $h_1a = h_2a \Rightarrow h_1 = h_2$

וברור שהיא על (מעצם הגדרתו) ולכן  $|H| = |Ha|$ .

כיוון שהקוסטים הם מחלקות שקילות,  $G$  הוא איחוד זר שלהם ולכן  $|G| = [G:H]|H|$

מסקנות מיידיות (עבור  $G$  סופית,  $H \leq G$ )

$$(1) \quad [G:H], |H| \mid |G|$$

$$(2) \quad \forall a \in G: o(a) = |\langle a \rangle| \mid |G|$$

$$(3) \quad \forall a \in G: a^{|G|} = e$$

## משפט אוילר

$$\forall a \in \mathbb{Z}^*, n \in \mathbb{N} : (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

הוכחה

$$(a, n) = 1 \Rightarrow a \equiv a' \in U_n \Rightarrow a^{\varphi(n)} \equiv a'^{|U_n|} = 1$$

תרגיל

חשב את  $9^{121} \pmod{100}$

$$(9, 100) \Rightarrow 9^{\varphi(100)} = 1 \pmod{100}$$

$$\varphi(100) = \varphi(4)\varphi(25) = 2 * 20 = 40$$

$$9^{40} = 1 \pmod{100} \Rightarrow 9^{121} = (9^{40})^3 g' = 9 \pmod{100}$$

מקרה פרטי של משפט אוילר:

$$\forall a \in \mathbb{Z}^*, p \text{ ראשוני} : a^{p-1} \equiv 1 \pmod{p}$$

## אלגוריתם ההצפנה RSA (ריבסט-שמיר-אדלמן) 1977

אליס מעוניינת שבוט ישלח לה הודעה חסויה באמצעות תקשורת פומבית.

אלגוריתם:

- 1) אליס בוחרת באקראי שני מספרים ראשוניים גדולים  $p, q$  שישארו חסויים אצלה, ומחשבת את  $n = pq$  ואת  $\varphi(n) = (p-1)(q-1)$ .
- 2) אליס בוחרת  $d$  כך ש  $(d, \varphi(n)) = 1$  ומחשבת את  $e \equiv d^{-1} \pmod{\varphi(n)}$  באמצעות אלגוריתם אוקלידס.
- 3) אליס שולחת לבוב את המפתח הציבורי  $(n, e)$ .
- 4) בוב מצפין הודעה  $M$  המקיימת  $(M, n) = 1$  ע"י  $E = m^e \pmod{n}$  ושולח לאליס.
- 5) אליס משחזרת את  $M$ :  $E^d = M^{ed} = M^{1+\varphi(n)k} = M(M^{\varphi(n)})^k = M$

הערות:

- אם ימצאו אלגוריתם יעיל למצוא את הפירוק  $n = pq$  יוכלו לחשב את  $\varphi(n)$  ואת  $d \equiv e^{-1}$ .
- זוהי שיטה אסימטרית: המצפין לא יודע לפענח.

## תת-חבורה נורמלית וחבורת המנה

הגדרה:

אם  $H \leq G$  מקיימת:  $\forall g \in G : gH = Hg$

אזי  $H \triangleleft G$  נקראת תת-חבורה נורמלית, ונסמן  $H \triangleleft G$

אם  $H \triangleleft G$  אזי קבוצת המנה  $H \backslash G$  היא חבורה עם פעולת הכפל המוגדרת ע"י  $Hx * Hy = Hxy$   
 אכן, אם  $H \triangleleft G$  אזי  $Hx = xH$  ובהתאם לכך  $(Hx)^{-1} = Hx^{-1}$  שכן  $HHx^{-1} = HHx^{-1} = HH = H$ .  
 $H$  הוא איבר היחידה.

הפעולה \* שבאמצעותה הגדרנו את הכפל היא הפעולה המקורית המוגדרת ב- $G$ !

לכן רק באמצעות הנורמליות של  $H \leq G$  מתקיים  $HxHy = Hxy$

דוגמא

$$G = GL_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

$$a^2 = 1, b^3 = 1$$

$$GL_2(\mathbb{Z}_2) = \langle a, b \rangle \text{ rank}(GL_2\mathbb{Z}_2) = 2$$

$$[G : \langle a \rangle] = \frac{|G|}{|\langle a \rangle|} = \frac{6}{2} = 3, [G : \langle b \rangle] = \frac{6}{3} = 2$$

$$\langle b \rangle \backslash G = \{ \langle b \rangle = \{1, b, b^2\}, a \langle b \rangle = \{a, ab, ab^2\} \}$$

$$G / \langle b \rangle = \{ \langle b \rangle = \{1, b, b^2\}, \langle b \rangle a = \{a, ba, b^2a = ab\} \}$$

נשים לב כי  $a \langle b \rangle = \langle b \rangle a$

$$G / \langle a \rangle = \{ \langle a \rangle = \{1, a\}, b \langle a \rangle = \{b, ba\}, b^2 \langle a \rangle = \{b^2, b^2a\} \}$$

$$\langle a \rangle \backslash G = \{ \langle a \rangle = \{1, a\}, \langle a \rangle b = \{b, ab\}, \langle a \rangle b^2 = \{b^2, ab^2\} \}$$

שלא שווים!

$G / \langle b \rangle \cong \mathbb{Z}_2$  חבורת המנה.

$G / \langle a \rangle$  קבוצת מנה!