<u>אלגוריתמים בתורת המספרים ויסודות בתורת ההצפנה</u>

תורת המספרים האלמנטרית היא פרק עתיק יומין במתימטיקה. במשך שנים רבות זה נראה כאחד התחומים המתימטיים הרחוקים מכל יישום, אך כל זה השתנה מאוד בשנים האחרונות כשהתברר תפקידה החשוב של תורת המספרים בהצפנת מידע. מאידך גיסא, כמה מהאלגוריתמים הקדומים ביותר המוכרים לנו שייכים לתורה זו.

<u>הצפנה במפתח פומבי</u>

הצפנה של מידע היא אמנות עתיקה וכתבי סתר למיניהם ידועים כבר אלפי שנים. יסוד משותף לכל שיטות ההצפנה העתיקות הוא עיקרון המפתח הפרטי (Private key cryptography): לצד המשדר ולצד הקולט יש מידע סודי משותף הידוע רק להם. למידע זה קוראים המפתח הפרטי שלהם, ומי שיודע אותו קל לו להצפין ולפענח. אך בלי ידיעת המפתח הפרטי קשה באופן בלתי סביר להצפין ולפענח. (למשל - ניתן לקוות כי משתמש לא מוסמך המנסה לשבור את ההצפנה, אין לו מנוס מלנסות את כל הצירופים האפשריים למפתח הסודי. זהו הסבר אינטואיטיבי בלבד. הביסוס התיאורטי המלא של רעיונות אלה מצריך מאמץ גדול, וניתן ללמוד כל זאת בקורס "שיטות הצפנה").

בשנת 1976 פרסמו Diffie and Hellman מאמר קצר שחולל מהפכה בתחום זה ומ-ציין את תחילתה של הקריפטוגרפיה המודרנית. הרעיון הבסיסי שלהם הוא המושג של הצפנה במפתח פומבי (Public-key cryptography): נניח ש-$\mathcal{D}$ הוא אוסף כל ההודעות האפשריות. את המשתמשים ברשת התקשורת אנו מסמנים ב-A, B, C וכו'. מקובל גם לקרוא למשתמשים בשמות Bob ו- Alice. לכ"א מן השחקנים מתאימים זוג פונקציות הופכיות $\mathcal{D} \to \mathcal{D}$ למשל לשחקן A מותאמות ההעתקות $s_A : \mathcal{D} \to \mathcal{D}$ ו-$p_A : \mathcal{D} \to \mathcal{D}$ כך שלכל $x \in \mathcal{D}$ מתקיים: $s_A(p_A(x)) = p_A(s_A(x)) = x$

הפונקציה p_A ידועה לכל ($p = public$) ואילו הפונקציה s_A ידועה רק לשחקן A ($s = secret$).

אבני יסוד בפיתוח השיטה הן ההנחות הבאות:

1. כל שחקן יכול ליצור באופן יעיל זוג העתקות הופכיות s_A, p_A כנ"ל.
2. אין קושי לכל שחקן שהוא B לחשב את הערך $p_A(x)$ לכל שם A של שחקן כלשהו ולכל הודעה נתונה x. הסבר: הפונקציות הפומביות p_A מופיעות ב"ספר טלפונים" וכך כש-B רוצה להעביר את ההודעה x ל-A הוא שולח אליו את ההודעה $p_A(x)$ שזו הגירסה המוצפנת (cyphertext) של x ו-A מפענח את ההודעה ומגלה מהו x ע"י חישוב $s_A(p_A(x)) = x$.

   את זאת יכול A לעשות שהרי הפונקציה s_A ידועה לו.
3. מניחים גם שאיש מלבד A לא יכול לחשב את הפונקציה s_A וזאת אפילו שהפונ-קציה ההופכית p_A ידועה לכל.

בנאמר לעיל מובלע רעיון עמוק ורב ערך. בניגוד למחשבה הקדומה על הצפנה, איננו מקווים עוד למערכת צופן <u>שכלל</u> לא ניתן לשבור. אנו מניחים תחת זאת שליריב שלנו יש <u>רק</u> משאבים חישוביים סבירים ("זו מכונת טיורינג המחשבת בזמן פולינומי") ואנו "מסתפקים" בכך שבהנחה זו יידרש היריב לזמן חישוב ענקי (למשל כגיל היקום) ע"מ לשבור את הצופן שלנו. זו נקודת מבט המובילה למסקנות עמוקות ומפתיעות, אך כאמור הביסוס התיאורטי המלא של תורה זו מצריך קורס סמסטריאלי שלם. אנו נציג כאן בהמשך זוגות כאלה של פונקציות הופכיות שתכונותיהן מבוססות על תורת המספרים - שיטת ההצפנה RSA.

אנו נראה כי מערכת פונקציות כזו מאפשרת גם <u>לחתום</u> על מסמכים. נניח שהחתימה הגלויה ש-A רוצה לשלוח היא w (זה עשוי להיות כל מידע המזהה את A באופן חד-ערכי). על מנת "לחתום" את החתימה w, אמור A לשלוח את זוג ההודעות $(w, s_A(w))$. נניח שהוא שולח את הזוג (w, z). כל שחקן אחר יכול לאמת שזו חתימה תקפה ע"י בדיקה ש: $p_A(z) = w$ אין קושי לעשות זאת שהרי p_A מפורסם באופן ציבורי. מאידך גיסא, שחקן אחר אינו יכול "לזייף את החתימה" שהרי אינו יכול לחשב את $s_A(w)$ בהינתן w.

<u>אלגוריתמים בסיסיים בתורת המספרים</u>

נפתח בכמה עובדות ומושגים יסודיים: אומרים שהמספר הטבעי a מחלק את המספר הטבעי b אם $b = ax$ כש-x שלם. מסמנים זאת ע"י: $a|b$. אומרים שהמספר $p \geq 2$ ראשוני אם 1 ו-p הם המספרים הטבעיים היחידים המחלקים את p. המספרים הראשוניים הראשונים הם 2,3,5,7,11,13,17,19,23

יחידות הפירוק: עובדה קלה להוכחה שלא נוכיח כאן היא שלכל מספר טבעי n יש הצגה אחת ויחידה כמכפלת חזקות של מספרים ראשוניים $n = p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k}$ כש-p_i מספרים ראשוניים שונים ו-e_i מספרים טבעיים חיוביים.

עוד עובדה פשוטה שנצטט ללא הוכחה היא שאם $n = p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k}$ אז $m|n$ אם"ם $m = p_1^{f_1} p_2^{f_2} \cdot p_k^{f_k}$ כש-$e_i \geq f_i$ לכל i.

מסקנה: יהיו $a = q_1^{e_1} q_2^{e_2} \cdot q_k^{e_k}$ ו-$b = q_1^{f_1} q_2^{f_2} \cdot q_k^{f_k}$ כש-q_i ראשוניים ו-$e_i, f_i \geq 0$. אז c מחלק הן את a והן את b אם"ם $c = q_1^{r_1} q_2^{r_2} \cdot q_k^{r_k}$ ולכל i מתקיים $r_i \leq e_i, f_i$ בפרט המספר $z = q_1^{\min(e_1, f_1)} \cdot q_k^{\min(e_i, f_i)}$ הוא המחלק המשותף המקסימלי של a, b כלומר $z|a, z|b$ וכן כל מחלק אחר y של a, b מקיים $y|z$ מסמנים $z = \gcd(a, b)$ או $z = (a, b)$.

כדאי להדגיש שוב את הנקודה האחרונה. מראש אנו מגדירים את $\gcd(a,b)$ כשלם הגדול ביותר המחלק את a,b. אולם מתברר שיש לו תכונה חזקה יותר והיא, שכל מחלק משותף של a,b הוא לא רק $\leq gcd\left(a,b\right)$ אלא אף מחלק את $\gcd(a,b)$.

את המחלק המשותף המקסימלי ניתן לאפיין גם כך:

משפט: יהיו a, b מספרים טבעיים חיוביים אז המחלק המשותף המקסימלי שלהם z הוא המספר הטבעי החיובי הקטן ביותר מהצורה $z = ax + by$ כש-x, y מספרים שלמים.

הוכחה: יהיה $s = ax + by$ המינימום הנ"ל ויהיה $q = \lfloor \frac{a}{s} \rfloor$ אז

$$a \bmod s = a - s \cdot q = a(1 - q \cdot x) - bq \cdot y$$

לכן גם $a \bmod s$ הוא צירוף של a, b במקדמים שלמים. בגלל המינימליות של s בהכרח $a \bmod s = 0$ כלומר $s|a$. כיו"ב $s|b$. מאידך גיסא, מכיון ש-s צירוף בשלמים של a, b מתקיים גם $\gcd(a, b)|s$ ולכן $s = \gcd(a, b)$ כפי שטענו. אומרים שהמספרים a, b הם זרים אם $\gcd(a, b) = 1$.

אלגוריתם אוקלידס ל-gcd: זהו אחד האלגוריתמים הלא טריביאליים הקדומים ביותר הידועים לנו. כבר ראיתם אותו בתרגיל ונסכם את עיקרי הדברים.

מוכיחים תחילה:

משפט: יהיו $a \geq b$ טבעיים אז: $\gcd(a, b) = \gcd(a \bmod b, b)$.

משתמשים בטענה זו ממש באלגוריתם, דהיינו:

$Euclid(a, b)$

אם $b = 0$, החזר a

אחרת, החזר $Euclid(b, a \bmod b)$

ומראים שתוך $O(\log(a + b))$ איטרציות האלגוריתם הזה מחשב את $\gcd(a, b)$. כמו כן מראים שבהתאמה קלה של האלגוריתם מתקבל אלגוריתם אוקלידס המורחב אשר בהינתן לו שני מספרים טבעיים a, b מוצא x, y שלמים כך ש: $ax + by = \gcd(a, b)$.

מדוע: נדרשות כאן מספר טענות

טענה 1: לכל $a > b \geq 0$ טבעיים $gcd\left(a,b\right) = gcd\left(b, amodb\right)$ (זו הטענה המוכיחה את נכונות האלגוריתם).

טענה 2: אם אלגוריתם אוקלידס בקלט (a, b) כש- $a > b \geq 0$ אורך k איטרציות אז $a \geq F_{k+1}, b \geq F_k$ כאשר F_j הוא מספר פיבונאצי ה- j (זו הסידרה המוגדרת ע"י $F_1 = F_2 = 1$ ו- $F_{j+1} = F_j + F_{j-1}$).

טענה 3: $F_j = \frac{1}{\sqrt{5}}(\Phi^j - \overset{\wedge}{\Phi^j}$ כאשר $\Phi = \frac{1+\sqrt{5}}{2}, \hat{\Phi} = \frac{1-\sqrt{5}}{2}$ (Φהוא "חתך הזהב").

(טענות אלה מספקות את ההערכה על זמן הריצה של האלגוריתם).

טענה 4: מתוך סידרת הזוגות a_i ,b_i המהווים קלט באיטרציות של האלגוריתם ניתן לבנות מספרים שלמים x,y כך ש- ax+by=gcd(a,b) (זוהי התוספת המסבה את אלגוריתם אוקלידס לאלגוריתם אוקלידס המורחב).

הוכחת טענה 1: נראה שהמספר שבאגף ימין וזה שבאגף שמאל מחלקים זה את זה ולכן הם שווים. ואכן, אם d מחלק את a,b אז הוא מחלק גם את a mod b שהרי a mod b=a-qb כאשר $q=\left\lfloor \frac{a}{b}\right\rfloor$.

מאידך גיסא, אם f מחלק את b, a mod b אז הוא מחלק גם את a=(a mod b)+qb.

הוכחת טענה 2: באינדוקציה. בסיס האינדוקציה (k=1) מובן מאליו. צעד האינדוקציה: נדרשות k-1 אינטרציות כשהקלט הוא b, a mod b ולכן ע"פ הנחת האינדוקציה $b \geq F_k$, a mod b$\geq F_{k-1}$ ואולם $a \geq (a\ mod\ b)+b \geq F_{k-1}+F_k = F_{k+1}$.

הוכחת טענה 3: מן הסתם ראיתם זאת בקורס "מתימטיקה דיסקרטית". אם לא ראיתם זאת, ההוכחה באינדוקציה קלה. בודקים תחילה את שני מקרי הבסיס k=1,2 צעד האינדוקציה מתבסס על כך ש $\Phi, \hat{\Phi}$ הם שני השורשים של המשוואה הריבועית $x^2 = x+1$.

מסקנה: מספר האיטרציות של אלגוריתם אוקלידס בקלט $a > b \geq 0$ הוא O(log a).

הוכחת המסקנה: יהיה k מס' האיטרציות של האלגוריתם. אז כפי שראינו $a \geq F_{k+1} \geq \Omega\left(\Phi^k\right)$ כש- $\Phi \simeq 1.6$ - חתך הזהב. לכן $k \leq$ O(log a) כפי שטענו. לפני שנוכיח את טענה 4 נדגים כיצד פועל האלגוריתם.

נחשב

$gcd\left(175,49\right) = gcd\left(49,28\right) = gcd\left(28,21\right) = gcd\left(21,7\right) = gcd\left(7,0\right) = 7$ אנו מחפשים x,y שלמים כך ש- $175x+49y=7$. נמצא x,y ע"י סריקת הסידרה הנ"ל מן הסוף להתחלה. קל למצוא u_1, v_1 כך ש-$7u_1+0v_1=7$ כמובן $u_1=1$,$v_1=0$. ממשיכים ובונים טבלה כדלקמן:

		u	v
175	49	2	-7
49	28	-1	2
28	21	1	-1
21	7	0	1
7	0	1	0

על מנת להמחיש איך היא נבנתה נתבונן בצעד האחרון שבו עברנו מהייצוג $49\cdot(-1)+28\cdot 2=7$ לייצוג $175\cdot 2+49\cdot(-3)=7$, כלומר ידוע לנו כי $u_4=-1, v_4=2$ הוא פתרון ל-

$$49u_4+28v_4=7 \qquad (1)$$

ואנו מחפשים פתרון ל- $175u_5+49v_5=75$. ואכן החישוב של $175\ mod\ 49$ נותן $175=3\cdot 49+28$

יוצא שרצוננו לפתור

$\left(3\cdot 49+28\right)u_5+49v_5=7$

נסדר את המחוברים כדלקמן:

$49\left(3u_5+v_5\right)+28u_5=7$ לכן, עפ"י המשוואה 1 אם נבחר $u_5=v_4$ ו- $3u_5+v_5=u_4$ כלומר $v_5=u_4-3v_4$ נקבל את מבוקשנו. נסכם:

$u_5=v_4=2$,$v_5=u_4-3v_4=-1-3\cdot 2=-7$.

כך נראה גם הפתרון הכללי: נניח שידוע לנו כי $b\cdot u+\left(a\ mod\ b\right)v=d$ ואנו מחפשים u',v' שלמים כך ש- $a\cdot u'+bv'=d$.

אם $q=\left\lfloor \frac{a}{b}\right\rfloor$ אז קל לראות שהפתרון הוא

$$\begin{cases} u'=v \\ v'=u-qv \end{cases}$$

ואכן:

$$au' + bv' = av + b\,(u - qv) = bu + (a - bq)\,v = bu + (a\; mod\; b)\cdot v = d$$

ממה שכבר נאמר נובעת השקילות בין התנאים הבאים:

- a, b זרים.
- יש שלמים x, y כך ש: $ax + by = 1$
- אין להם גורם ראשוני משותף במילים אחרות:

אם $a = p_1^{e_1}p_2^{e_2}\cdot p_k^{e_k}$ ו- $b = p_1^{f_1}p_2^{f_2}\cdot p_k^{f_k}$
הצגות של a, b כחזקות של ראשוניים, אז לכל אינדקס j מתקיים $e_j = 0$ או $f_j = 0$
תזכורת קצרה באלגברה:
חבורה $(S, \bullet)$ מורכבת מקבוצה S ומפעולה $\bullet$.
פעולה זו העתקה $\bullet : S \times S \to S$.
בניגוד למקובל בסימוני העתקות אנו מסמנים את הפעולה כ- $x \bullet y$ (ולא $\bullet(x, y)$)
הדרישות מחבורה הן כדלקמן:

1. קיום איבר יחידה $e \in S$ המקיים $e \bullet x = x \bullet e = x$ לכל $x \in S$.
2. אסוציאטיביות של הפעולה: $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ לכל $x, y, z \in S$.
3. קיום הופכי: לכל $x \in S$ יש $y \in S$ המקיים $x \bullet y = y \bullet x = e$. לאיבר y קוראים ההופכי של x, ומסמנים $y = x^{-1}$.

החבורות שתופענה כאן הן כולן קומוטטיביות (נקראות גם אבליות ע"ש N. Abel). כלומר הן מקיימות גם $x \bullet y = y \bullet x$ לכל $x, y \in S$. התורה של חבורות קומוטטיביות היא פשוטה בהרבה מן התורה הכללית של חבורות. הערה נוספת: לעיתים מקצרים ואומרים "החבורה S", זה כאשר ברור מהי הפעולה.

דוגמאות: חיבור מודולו n. כאן $S = \{0, 1, \ldots, n-1\}$ והפעולה $\bullet$ היא חיבור מודולו n, שאנו מסמנים ב-$+$, כרגיל.

מה בדבר כפל מודולו n? אם n אינו ראשוני יש בעיה בהגדרת הכפל. כך למשל אם $n = 30$ אז קל לבדוק שלאיבר 25 אין הופכי. לכן אנו נאלצים לצמצם את הדיון רק למספרים שהם זרים ל-n.

טענה: לכל n טבעי, המספרים הקטנים מ-n וזרים ל-n ביחד עם פעולת הכפל מודולו n מהווים חבורה אבלית. הסימון המקובל לחבורה זו הוא Z_n^*, ואת הפעולה אנו מסמנים ב-$\cdot$ ולפעמים פשוט משמיטים שת סימון הפעולה כמקובל בכפל רגיל.

הוכחה: רוב התכונות של חבורה קלות לבדיקה, ונוותר לכן על כך. תכונה לא טריביאלית אחת שיש לוודא היא קיום ההפיך: ואכן אם $a < n$ זר ל-n אז מאלגוריתם אוקלידס המוכלל יש x, y שלמים כך ש-$ax + ny = 1$ יוצא ש-x הוא ההופכי הכפלי של a מודולו n כלומר $ax \equiv 1 \pmod{n}$.

תכונה נוספת שיש לאמת היא שאם $a, b < n$ וזרים ל-n אז גם $ab \bmod n$ זר ל-n.
כפי שראינו: המספרים הטבעיים u, v זרים אם"ם יש שלמים x, y כך ש-$ux + vy = 1$.
נעזר בזאת לשם הוכחת הטענה. מכיוון ש-a זר ל-n יש x_1, y_1 שלמים כך ש-$ax_1 +$ $ny_1 = 1$ כיו"ב יש שלמים x_2, y_2 כך ש-$bx_2 + ny_2 = 1$. נכפיל את שני הביטויים ונרשום זאת כך: $(x_1x_2)ab + (ax_1y_2 + bx_2y_1 + y_1y_2n)n = 1$ מכאן מתקבל ש-ab זר ל-n ולכן גם $ab \bmod n$ זר ל-n.

מומלץ לכם לחשב דוגמה מספרית קטנה, למשל לחשב את "לוח הכפל" של החבורה הכפלית של המספרים הזרים ל 12 מודולו 12.

הוכחנו אם כן שהמספרים הקטנים מ-n וזרים ל-n ביחד עם פעולת הכפל מודולו n מהווים חבורה Z_n^*. מה גודלה של חבורה זו? שימוש פשוט בנוסחת ההכלה וההדחה מספק את התשובה.

משפט (Euler): יהיה n מספר טבעי ויהיה $n = p_1^{e_1}p_2^{e_2}\cdot p_k^{e_k}$ כש-$e_i \geq 1$ הייצוג של n כמכפלה של חזקות ראשוניים. אז מספר המספרים הקטנים מ-n וזרים לו הוא $\phi(n) = n(1 - \frac{1}{p_1})\cdots(1 - \frac{1}{p_k})$.

הערה: לפונקציה $\phi(\cdot)$ קוראים פונקציית אוילר.

סקירת ההוכחה: מספר b אינו זר ל-n אם"ם b מתחלק באחד המספרים הראשוניים $p_1, \ldots, p_k$. תהיה S_i קבוצת המספרים הקטנים מ-n ומתחלקים ב-p_i.קבוצת המספרים הקטנים מ-n וזרים לו היא בדיוק $[n] \setminus \cup_1^k S_i$.

את עוצמתה של קבוצה זו מחשבים באמצעות עיקרון ההכלה וההדחה. שמים לב כי $|S_i| = \frac{n}{p_i}$ וכן $|S_i \cap S_j| = \frac{n}{p_i p_j}$ וכו'. המשפט נובע, בעזרת נוסחת ההכלה וההדחה.

אנו זקוקים עתה לעובדה הפשוטה הבאה מתורת החבורות שתוכח בסוף הפרק.

טענה: תהיה G חבורה, ויהיה גודלה ("הסדר של G") $r = |G|$ אזי לכל איבר $a \in G$ מתקיים ש-$a^r = a \bullet a \bullet \ldots a = e$ כאשר במכפלה יש r מופעים של a, ו-e איבר היחידה ב-G.

מסקנה: לכל n טבעי ולכל $1 \leq a < n$ הזר ל-n מתקיים $a^{\phi(n)} \equiv 1 \pmod n$ בפרט אם p ראשוני אז $a^{p-1} \equiv 1 \pmod p$, לכל $p > a \geq 1$.

עתה ניתן להציג את אלגוריתם RSA ומערכת ההצפנה הנגזרת ממנו.

1. בחר שני מספרים ראשוניים גדולים שונים p, q. בטכנולוגיה הנוכחית "גדול" פירושו מספר בן כמה מאות ביטים.
2. הגדר $n = pq$.
3. בחר e אי זוגי קטן הזר ל-$\phi(n) = (p-1)(q-1)$.
4. חשב את d, ההופכי של e מודולו $\phi(n)$.
5. פרסם את מפתח ההצפנה הפומבי $P = (e, n)$.
6. שמור בסוד את המפתח הסודי d ואת p, q.

כאן מרחב ההודעות האפשריות הוא $\{1, \ldots, n\}$ וההעתקות הן כדלקמן: $P(M) = M^e \bmod n \quad S(C) = C^d \bmod n$

נראה תחילה שזוג ההעתקות הללו הופכיות זל"ז: עלינו להראות כי $S(P(M)) = P(S(M)) = M$ כלומר, ש-$M^{de} \equiv M \pmod n$ ואכן, מכיוון ש-d, e הפיכים מודולו $\phi(n) = (p-1)(q-1)$ ניתן לרשום $de = 1 + k(p-1)(q-1)$ ל-k טבעי כלשהו. אנו נראה כי $M^{de} \equiv M \pmod n$ ע"י שנראה כי $M^{de} \equiv M \pmod p$ וכן $M^{de} \equiv M \pmod q$ ואכן

$$M^{de} = M \cdot (M^{p-1})^{k(q-1)} \pmod p$$
$$\equiv M \cdot 1^{k(q-1)} \equiv M \pmod p$$

וכיו"ב ב-q כלומר $M^{de} - M$ מתחלק הן ב-p והן ב-q ולכן ב-n.

יש לציין גם שדרושים מספר מרכיבים אלגוריתמיים על מנת לממש את שיטת RSA באופן יעיל. חלק מהאלמנטים הללו הוצגו בתרגיל וחלקם יוצגו להלן. נתחיל בהעלאה בחזקה:

טענה: יהיו $M \leq n$ ו-e מספרים טבעיים. אז ניתן לחשב את $M^e \bmod n$ באמצעות $O(\log e)$ פעולות כפל מודולו n.

הרעיון: רושמים את e בבסיס 2 ומממשים את ההעלאה בחזקה ע"י סידרה של כפלים והעלאות בריבוע מתאימות.

מרכיב חשוב נוסף הוא אלגוריתם יעיל לפתרון משוואות מודולריות שהוצג בתרגיל.

כמה השלמות בתורת החבורות

תהיה G חבורה ו- $H \subseteq G$. אומרים ש- H תת חבורה של G אם H עצמה מהווה חבורה. פירוש הדבר הוא שהיא סגורה לפעולה ולהופכי ז"א לכל $x_1 y \in H$ מתקיים גם $xy \in H$ וכן $x^{-1} \in H$. אנו זקוקים לטענה הבסיסית הבאה:

משפט (לגרנז'): יהיה $H \subseteq G$ חבורה סופית ותת חבורה שלה אז המספר $|H|$מחלק את המספר $|G|$.

הוכחה: ההוכחה מסתמכת על מושג הקוסט . יהיו G,H כנ"ל ויהיה $a \in G$. נסמן ב-aH את הקבוצה הבאה:

$aH \langle ax \mid x \in H \rangle$ לקבוצה כזו קוראים קוסט של H ב- G. שימו לב שגם H היא קוסט כי אם $h \in H$ אז hH=H.

טענה: יהיה G,H כנ"ל אז כל שני קוסטים של H הם זהים או זרים.

הוכחה: במילים אחרות אנו אומרים שאם $aHnbH \neq \phi$ אז aH=bH. ואכן, נניח כי $x \in aHnbH$ יוצא שניתן להציג את x כ- $x = ah_1$ וכן כ- $x = bh_2$ כש- $h_1, h_2 \in H$. נרשום זאת $ah = ah_1h_2^{-1}h = ah_3 \in aH$ שהרי $h_1h_2^{-1}h$ שייך ל- H.

נובעת המסקנה שהקוסטים $\langle aH \rangle$ (כש-a עובר על איברי G) מהווים חלוקה של G שהרי כל איבר בחבורה נמצא בדיוק באחד מהקוסטים (שימו לב שלכל איבר $a \in G$ מתקיים $a \in aH$ שהרי $e \in H$) כמובן לכל קוסט aH יש עוצמה $|aH| = |H|$ וקל להשלים עתה את הוכחת משפט לגרנז' כי הקבוצה G מתחלקת ל- $|G| / |H|$ קבוצות בגודל $|H|$ כל אחת.

מכיוון שאנו משתמשים בכתיב כפלי לציון הפעולה בחבורה, אך טבעי שנסמן את $a \cdot a.....a$ בכתיב חזקתי כ- a^r. הדיון הנ"ל נותן גם מסקנה מועילה נוספת.

טענה: לכל חבורה סופית G ולכל $a \in G$ יש מס' טבעי k כך ש- $a^k = 1$. המספר k מחלק את $|G|$.

הוכחה: נביט בקבוצת האיברים $\langle a^j \mid j \rangle$. קל לוודא שזוהי תת חבורה של G. (מדוע?) היא קרויה התת חבורה הציקלית הנוצרת ע"י a. נתבונן באיברים $1, a, a^2.......$ מכיוון ש- G סופית גם הקבוצה הזו סופית. בפרט יש שני אינדקסים שונים $\alpha > \beta$ כך ש: $a^\alpha = a^\beta$. נובע ש- $a^{\alpha-\beta} = e$, הבחירה $k = \alpha - \beta$ מוכיחה את הטענה הראשונה.

יהיה r השלם החיובי הקטן ביותר כך ש- $a^r = e$. אנו טוענים שהחבורה הציקלית הנוצרת ע"י a כוללת את האיברים $\langle e, a, ..., a^{r-1} \rangle$ ואכן, מהנאמר לעיל נובע שלכל t מתקיים $a^t = a^{tmodr}$. יוצא שלתת חבורה הזו יש r איברים ולפי הנ"ל r מחלק את $|G|$.

מסקנה: תהיה G חבורה סופית ו- $a \in G$ אז $a^{|G|} = e$ אם נפעיל את המסקנה של .... - החבורה הכפלית מודולו n נקבל:

משפט פירמה: לכל n ולכל $1 \leq a < n$ מתקיים: $a^{\phi(n)} = 1 \pmod{n}$.