©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש"ף:

בר אלון, איבראהים שאהין, שמואל שמעוני, מיכאל פרי, דורון מור, חיה קלר, אלעד אייגנר חורב

נכתב ע"י צבי מינץ. נערך ע"י מיכאל פרי

קונגרואנציות (שקילויות)

חלק 1.

בהרצאה דברנו על אריתמטיקה מודלרית, וראינו את הטענה הבאה (משפט 5 בהרצאת "שקילויות"):

יהיו $a,b,c,d \in \mathbb{Z}$ ויהי $m \in \mathbb{Z}^+$ כך ש $a \equiv b\ (mod\ m), c \equiv d\ (mod\ m)$. אזי:

1. חיבור: $a + c \equiv b + d\ (mod\ m)$.
2. חיסור: $a - c \equiv b - d\ (mod\ m)$.
3. הכפלה: $ac \equiv bd\ (mod\ m)$.

כעת נדבר על פעולת **"החילוק"**. נתעניין בביטוי הבא: $a \cdot c\ \equiv b \cdot c\ (mod\ m)$

ראינו בהרצאה את הטענה הבאה (משפט 6 בהרצאת "שקילויות"):

טענה (כלל הצמצום):
יהיו $a,b,c\ \in Z$, $m \in Z^+$ ו-$d = (c,m)$. אזי:

$$a \equiv b\ (mod \frac{m}{d}) \Leftrightarrow a \cdot c\ \equiv b \cdot c\ (mod\ m)$$

על מנת להבהיר את הטענה, נסתכל על התרגיל הבא:

תרגיל 1\א: נתון כי: $14\ \equiv 8\ (mod\ 2)$

כלומר נתון כי $7 \cdot 2\ \equiv 4 \cdot 2\ (mod\ 2)$

נשים לב כי לא יכלנו לחלק ב-2 את שני האגפים מבלי "לגעת" ב-$(mod\ 2)$, היות ו- $7\ \not\equiv 4\ (mod\ 2)$.

אולם, לפי כלל הצמצום נובע

$$7 \equiv 4\ \ (mod\ \frac{2}{(2,2)})$$

כלומר

$$7 \equiv 4\ \ (mod\ 1)$$

ולכן מכלל הצמצום נקבל $7 \equiv 4\ (mod\ 1)$ שזוהי שקילות נכונה (שהרי כל זוג מספרים שלמים שקולים זה לזה מודולו 1).

כעת נסתכל על הטענה הבאה שהוא כלל ההרחבה: קל יותר לזכור אותו מאשר את כלל הצמצום, אולם תכף נראה שיש מקרים בהם כלל הצמצום עוזר ואילו כלל ההרחבה אינו עוזר.

טענה (כלל ההרחבה):
יהיו $\boldsymbol{a,b,c \in \mathbb{Z}}$, $\boldsymbol{c \neq 0}$ **ויהי** $\boldsymbol{m \in \mathbb{Z}^+}$
אזי $\boldsymbol{a \equiv b\ (mod\ m) \Leftrightarrow a \cdot c \equiv b \cdot c\ (mod\ m \cdot c)}$

©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש"ף:
בר אלון, איבראהים שאהין, שמואל שמעוני, מיכאל פרי, דורון מור, חיה קלר, אלעד אייגנר חורב
נכתב ע"י צבי מינץ. נערך ע"י מיכאל פרי

<u>הוכחה: על מנת להוכיח טענת אם"ם יש צורך להוכיח גרירה דו כיוונית.</u>

צד ראשון: נוכיח כי $\boldsymbol{a \equiv b\ (mod\ m)\ \Rightarrow\ a \cdot c \equiv b \cdot c\ (mod\ m \cdot c)}$

נניח כי $a \cdot c \equiv b \cdot c\ (mod\ m \cdot c)$ ולכן $m \cdot c \mid ac - bc$. נובע כי $mc \mid c(a-b)$ ולכן קיים k שלם שעבורו מתקיים: $c(a-b) = mck$. מכיוון ש-$\boldsymbol{c}$ אינו 0 אזי נחלק ב-$\boldsymbol{c}$ ונקבל: $(a-b) = mk$ ← לפי הגדרה: $m \mid (a-b)$ ← $a \equiv b\ (mod\ m)$ כנדרש.

צד שני: נוכיח כי $\boldsymbol{a \equiv b\ (\ mod\ m\ )\ \Leftarrow\ a \cdot c \equiv b \cdot c\ (\ mod\ m \cdot c\ )}$

נניח כי $a \equiv b\ (mod\ m)$ ולכן $m \mid a-b$ ולכן קיים $k \in \mathbb{Z}^+$ כך ש $a - b = m \cdot k$

נכפיל את 2 האגפים פי c ונקבל $ca - cb = c \cdot m \cdot k$ ולכן $m \cdot c \mid ca - cb$ ולכן

$$ac\ \equiv bc\ (mod\ m \cdot c)$$

■

נחזור לתרגיל הקודם:

<u>דוגמא:</u> $14\ \equiv 8\ (mod\ 2)$.

כלומר $7 \cdot 2\ \equiv 4 \cdot 2\ \ (mod\ 2 \cdot 1)$

ולכן לפי כלל ההרחבה נגיע לאותה מסקנה אליה הגענו באמצעות כלל הצמצום:

$7 \equiv 4\ (mod\ 1)$.

נראה כעת דוגמה נוספת בה אפשר הן באמצעות כלל ההרחבה והן באמצעות כלל הצמצום להגיע לאותה מסקנה:

<u>דוגמא:</u> ידוע כי $15\ \equiv 9\ (mod\ 6)$ ננסה להגיע לשקילות מתאימה באמצעות כלל ההרחבה ובאמצעות כלל הצמצום.

נוכל לרשום זאת באופן הבא $3 \cdot 5\ \equiv 3 \cdot 3\ (mod\ 6)$ ומכיוון ש- $gcd(3,6) = 3$

לפי כלל הצמצום
$5\ \equiv 3\ (mod\ \ 6/3)$
ולכן
$5\ \equiv 3\ (mod\ 2)$

לפי כלל ההרחבה
$3 \cdot 5\ \equiv 3 \cdot 3\ (mod\ 2 \cdot 3)$
ולכן
$5\ \equiv 3\ (mod\ 2)$

<u>קיבלנו שקילות זהה בעזרת 2 הכללים</u>

אז מדוע צריך את כלל הצמצום? כאשר מדובר במודלו ראשוני, ניתן לראות הבדל מהותי בין כלל הצמצום לכלל ההרחבה. במקרה זה (ובמקרים נוספים) מוכרחים להשתמש בכלל הצמצום ואילו כלל ההרחבה לא מספיק.

בר אלון, איבראהים שאהין, שמואל שמעוני, מיכאל פרי, דורון מור, חיה קלר, אלעד אייגנר חורב

נכתב ע"י צבי מינץ. נערך ע"י מיכאל פרי

יהי p ראשוני כלשהו ויהי c כך ש-$(c,p)=1$, נסתכל על השקילות

$$a\cdot c\ \equiv b\cdot c\,(\,mod\; p\,)$$

לפי כלל הצמצום, נקבל כי $a\ \equiv b\ (mod\ p)$ ואילו בכלל ההרחבה לא נוכל להשתמש היות ו-p לא מתחלק ב-c! הבעיה לא נובעת רק בגלל שהמודלו הוא ראשוני, אלא עבור כל m שאינו כפולה של c, כלל ההרחבה לא יעזור.

נשים לב כי בכלל הצמצום **תמיד** נוכל להשתמש, היות ו-(c,m) מוגדר היטב עבור כל $m,c\in\mathbb{Z}$, ואילו בכלל ההרחבה נשתמש אם אנחנו רואים כי m הוא כפולה של c.

לדוגמא:

$$7\ \equiv 3\,(\,mod\;4\,)\ \Leftrightarrow\ \underbrace{7\cdot 3}_{21}\ \equiv\ \underbrace{3\cdot 3}_{9}\ \underbrace{mod\ (4\cdot 3)}_{12}$$

חלק 2.

יהי x שלם מהצורה $12n+5$, אזי x מקיים:

$$x\ \equiv 5\,(\,mod\;12\,)$$

כל השלמים מהצורה הזאת הם אי זוגיים, היות $x=12n+5$ אז $x=2(6n+2)+1$,

ולכן נוכל להגיד כי כל השלמים מהצורה $12n+5$ נמצאים ב $[1]_2$ **כלומר**, משאירים שארית 1 בחלוקה ב-2. כלומר, קיבלנו צורה חדשה להסתכלות על משפט החלוקה: כאשר המחלק הוא b, משפט החלוקה מחלק את העולם ל b שאריות אפשריות. כאשר $b=2$ נקבל שכל הזוגיים נמצאים ב-$[0]_2$, וכל האי זוגיים נמצאים ב-$[1]_2$. כאשר $b=12$ נקבל שש מחלקות שמתאימות לזוגיים ושש מחלקות שמתאימות לאי זוגיים. לכן יש שש מחלקות מודולו 12 שאיחוד כולן הוא המחלקה $[0]_2$, ויש שש מחלקות מודולו 12 שאיחוד כולן הוא המחלקה $[1]_2$.

נראה זאת באופן ציורי: (סטודנטים המדפיסים את הדף – שימו לב שיש כאן צבעים שונים!)

נסתכל על מערכת שאריות שלמה מודולו 12:

0	1	2	3	4	5	6	7	8	9	10	11

ונסתכל על מערכת שאריות שלמה מודולו 2

0	1

קל לראות כיצד כל מערכת השאריות מודולו 12 "משתלבת" אל תוך מערכת השאריות מודולו 2, וגם באופן ההפוך, כיצד מערכת השאריות מודולו 2 "משתלבת" אל תוך מערכת השאריות מודולו 12.

אבל האם זה תמיד כל כך פשוט?

ננסה להחליף את 2 עם 3 ונראה כיצד אותה "תמונה" תראה.

ובאופן יותר כללי,

אם $x \in [r]_{12}$ אז נרצה להשלים את האמירה הבאה:

אז $x \in [\ ?\ ]_3$?

למשל, אם $x \in [5]_{12}$, כלומר x משאיר שארית 5 במודולו 12, לכן איזה שארית x נותן בחלוקה ב-3? כלומר, $x \in [\ ?\ ]_3$?

אם $x \in [5]_{12}$ אז $x \in \{\dots,5,17,29,41,\dots\}$. נתבונן על מספרים אלו מודולו 3 ונקבל:
$[5\ ]_3 = 2$, $[17\ ]_3 = 2$, $[29\ ]_3 = 2$ וכן הלאה...

אחרי שהתרשמנו מדוגמאות מסוימות, ננסה להוכיח באופן גורף.

נשים לב כי $12 \mid 3$ ולכן נוכל לרשום כי לפי משפט החלוקה, קיימים $q, r \in \mathbb{Z}$ כך ש:

$$x = 12 \cdot q + r = 3 \cdot (4 \cdot q) + r$$

נשים לב כי החלק ■ הוא תמיד כפולה של 3. כעת נוכל להפעיל שוב את משפט החלוקה על r ולכן לפי משפט החלוקה, קיימים $k, l \in \mathbb{Z}$ כך ש :

$$\begin{aligned} x &= 3 \cdot (4 \cdot q) + r \\ &= 3 \cdot (4 \cdot q) + 3 \cdot k + l \\ &= 3 \cdot (4 \cdot q + k) + l \end{aligned}$$

ולכן אם $x \in [r]_{12}$ אז $x \in [l]_3$

כלומר r- שארית של x במודולו 12

ו-l שארית של x במודולו 3.

ולכן ה"תמונה" תראה באופן הבא: (שימו לב לצבעים השונים!)

מערכת שאריות שלמה מודולו 12

0	1	2	3	4	5	6	7	8	9	10	11

מערכת שאריות שלמה מודולו 3

0	1	2

נציין כי משהו פה נראה "קל מדי". אם ניקח כל זוג של שאריות זהות מ-"הקבוצה הגדולה" אז נקבל גם כן **אותה** שארית ב"קבוצה הקטנה".

זה מתרחש כי לקחנו מערכת שאריות אשר מתחלקת באחרת, כלומר $12 \mid 3$. כעת ננסה לענות על אותה שאלה, אך נחליף את 3 ב-5.

אם $x \equiv r \ (\,mod\ 12\,)$ אז $x \ \equiv ?\ (\,mod\ 5\,)$

נתחיל בכך שנשים לב ש $12 \nmid 5$.

לפי משפט החלוקה, קיימים $q, r \in \mathbb{Z}$ כך ש :

$$x = 12q + r = 5 \cdot (2q) + 2q + r$$

כעת, כל מה שקבלנו זה ש $x \in [2q + r]_5$

אנחנו מקבלים את התחושה **שהאלגנטיות** של $x \in [r]_{12} \Rightarrow x \in [r]_3$ נעלמה.

זה שונה מהמקרה הקודם (של 3 ו-12), היות וקיים מצב שעבור 2 מספרים זרים

$x_1, x_2 \in [r]_{12}$ נקבל 2 תשובות שונות עבור $[2q + r]_5$.: לדוגמה:

$$x_1 \ = 12 \cdot 1 + 3 \ \in \ [3]_{12}$$

ומתקיים

$$x_1 = \ \ 5 \cdot 2 + 2 \cdot 1 + 3 \in \ [0]_5$$

לעומת זאת:

$$x_2 := 12 \cdot 2 + 3 \ \in \ [3]_{12}$$

אבל

$$x_2 = \ \ 5 \cdot 4 + 2 \cdot 2 + 3 \ \in \ [2]_5$$

כלומר עבור $x_1, x_2 \in [3]_{12}$ נקבל כי $x_1 \in [0]_5$ ו $x_2 \in [2]_5$, כלומר הם נותנים 2 שאריות <u>**שונות**</u> בחלוקה ב-5.

באופן יותר כללי:

- אם $(m_1, m_2) = 1$ אז $[c]_{m_1}$ יכול להתפצל על כמה שאריות שונות במודולו m_2 (בהנחה ש-$m_2 < m_1$).
- ואם $m_1 \mid m_2$ אז נוכל ישר להגיד כי אם $a \ \equiv c \ (mod\ m_1)$ אז $a \ \equiv c \ (mod\ m_2)$.

ומה עם הכיוון ההפוך?

קודם לקחנו $a \in [r]_{12}$ ושאלנו לאיזה מחלקה מודולו 3 אנחנו שייכים, כעת אם נהפוך את השאלה, כלומר, נניח כי $a \in [r]_3$, צריך למצוא עבור איזה $k \in [0{,}11]$ מתקיים:

$a \equiv k\ (mod\ 12)$ כלומר לאיזה מחלקה מודולו 12, a שייך.

כאן לא ניתן לענות על השאלה בלי לקבל עוד מידע על a .

לדוגמא: a=7 , a=4 שייכים למחלקות שונות מודולו 12 אבל לאותה מחלקה מודולו 3.

<u>חלק 3.</u>

טענה:
יהיו $m_1, m_2, \dots, m_k$ מספרים שלמים עבור $k \in \mathbb{Z}^+$.
אם $a \ \equiv b\ (mod\ m_i)$ עבור כל $i \in [1, k]$ **אז**:

$$a \ \equiv b\ \left(mod\ lcm(m_1, m_2, \dots, m_k)\right)$$

<u>הוכחה:</u>

לפי ההנחה, $m_i | a-b$ ולכן $a-b$ הינו כפולה של m_i עבור כל $i \in [1,k]$. לכן $lcm(m_1,\dots,m_k) | a-b$ ומכאן הטענה נובעת. (שימו לב שהשתמשנו כאן בכך שכל כפולה משותפת של n מספרים היא כפולה של ה-lcm של n המספרים. הוכחתם זאת עבור n=2 בתרגול LCM כחלק מהוכחת המשפט בעמוד 2 שם, והמעבר לערכי n גדולים יותר מושאר לקורא להוכחה באינדוקציה.)

<u>דוגמה:</u>

אם

$$x \equiv 1\ (mod\ 2)$$
$$x \equiv 1\ (mod\ 4)$$
$$x \equiv 1\ (mod\ 6)$$

אז

$x \equiv 1\ \big(mod\ lcm(2,4,6)\big)$ כלומר: $x \equiv 1\ (mod\ 12)$

כעת ניתן לשאול את השאלה, מה קורה עבור $m_1, m_2, \dots, m_k$ מספרים **שלמים** זרים?
נסתכל על הטענה הבאה:

טענה:
יהיו $m_1, m_2, \dots, m_k$ מספרים שלמים **זרים** עבור $k \in \mathbb{Z}^+$
אזי אם $a\ \equiv b\ (mod\ m_i)$ עבור כל $i \in [1,k]$ אזי:

$$a\ \equiv b\ (mod\ m_1 \cdot m_2 \cdot \dots \cdot m_k)$$

<u>הוכחת הטענה:</u> נובע מיידית מהטענה הקודמת, כי אם $m_1, m_2, \dots, m_k$ מספרים **זרים** אז: $lcm(m_1, m_2, \dots, m_k) = m_1 \cdot m_2 \cdot \dots \cdot m_k$.

<u>דוגמא:</u>

אם

$$x \equiv 1\ (mod\ 2)$$
$$x \equiv 1\ (mod\ 3)$$
$$x \equiv 1\ (mod\ 5)$$

אז $x \equiv 1\ (mod\ 2 \cdot 3 \cdot 5)\ \equiv 1\ (mod\ 30)$

נראה כי זה נכון גם לכיוון השני:

טענה:

יהיו $m_1, m_2, \dots, m_k$ מספרים שלמים עבור $k \in \mathbb{Z}^+$.

אם

$$a\ \equiv b\ \big(mod\ lcm(m_1, m_2, \dots, m_k)\big)$$

אז:

בר אלון, איבראהים שאהין, שמואל שמעוני, מיכאל פרי, דורון מור, חיה קלר, אלעד אייגנר חורב
נכתב ע"י צבי מינץ. נערך ע"י מיכאל פרי

$a \equiv b \ (mod\ m_i)$ עבור כל $i \in [1,k]$

הוכחה: עבור כל $i \in [1,k]$ קיים $k_i \in \mathbb{Z}$ כך ש $lcm(m_1, m_2, \dots, m_k) = k_i m_i$

העובדה ש $a - b \mid lcm(m_1, m_2, \dots, m_k)$ גוררת ש $a - b \mid k_i m_i$ עבור כל $i \in [1,k]$

ולכן עבור כל i נקבל כי קיים l_i כך ש $a - b = l_i k_i m_i$, ומכאן $a - b \mid m_i$.

ולכן קבלנו כי לכל $i \in [k]$: $a - b \mid m_i$ כלומר $a \equiv b \ (mod\ m_i)$ כנדרש.

נסכם את הדיון במשפט הבא:

יהיו $m_1, m_2, \dots, m_k$ מספרים שלמים עבור $k \in N$, אזי:

1. $a \equiv b \ (mod\ m_i), \forall i \in [1,k] \Leftrightarrow a \equiv b \ \big(mod\ lcm(m_1, m_2, \dots, m_k)\big)$

2. במידה $m_1, m_2, \dots, m_k$ מספרים שלמים **זרים** אזי:
$a \equiv b \ (mod\ m_i), \forall i \in [1,k] \Leftrightarrow a \equiv b \ (mod\ m_1 \cdot m_2 \cdot \ldots \cdot m_k)$

שימו לב כי הוכחנו את שני הכיוונים של 1 ואילו 2 נובע ישירות מ-1 כי אם $m_1, m_2, \dots, m_k$ מספרים זרים אז: $lcm(m_1, m_2, \dots, m_k) = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

<u>דוגמא:</u>

עבור $m_1 = 4, m_2 = 6$ **לא זרים** נקבל:

$(4,6) = 2$ ו- $lcm(4,6) = 12$ ולכן:

$$\begin{matrix} x \equiv 1 \ (\ mod\ 4\ ) \\ x \equiv 1 \ (\ mod\ 6\ ) \end{matrix} \quad \Leftrightarrow \quad x \equiv 1 \ (\ mod\ 12\ )$$

ואילו עבור $m_1 = 3, m_2 = 4$ **<u>זרים</u>** נקבל:

$$\begin{matrix} x \equiv 1 \ (\ mod\ 4\ ) \\ x \equiv 1 \ (\ mod\ 3\ ) \end{matrix} \quad \Leftrightarrow \quad x \equiv 1 \ (\ mod\ 12\ )$$

דוגמא נוספת:

אם $x \equiv 9 \ (mod\ 12)$ **אזי** $x \equiv 9 \ (mod\ 4)$ **ו** $x \equiv 9 \ (mod\ 3)$

ולכן נקבל כי

$$\begin{matrix} x \equiv 1 \ (mod\ 4) \\ x \equiv 0 \ (mod\ 3) \end{matrix}$$

טענה

יהיו m_1, m_2 מספרים שלמים כלשהם

אם $x \equiv r \left(mod\ lcm(m_1, m_2)\right)$

אז

$$x \equiv (r\ mod\ m_1)\ (mod\ m_1)$$
$$x \equiv (r\ mod\ m_2)\ (mod\ m_2)$$

דוגמא:

נחזור לדוגמא הקודמת: $lcm(4,3) = 12$ ולכן:

אם $x \equiv 9\ (\ mod\ 12\ )$ **אזי** לפי הטענה נקבל כי

$$x \equiv (9\ mod\ 4)\ (mod\ 4) \quad \rightarrow \quad x \equiv 1\ (\ mod\ 4\ )$$
$$x \equiv (9\ mod\ 3)\ (mod\ 3) \quad \rightarrow \quad x \equiv 0\ (\ mod\ 3\ )$$
.

הוכחה: (למה 2 מהרצאת "משפט השאריות הסיני")

ידוע כי m_1, m_2 הם שני מספרים שלמים כך ש $x \equiv r\ \left(\ mod\ lcm(m_1, m_2)\right)$ ולכן

$x = lcm(m_1, m_2) \cdot n + r$ כאשר $n \in \mathbb{Z}$.

ידוע כי

$$m_1\ |\ lcm(m_1, m_2)$$
$$m_2\ |\ lcm(m_1, m_2)$$

ולכן קיימים $k_1, k_2 \in \mathbb{Z}$ כך ש $x = k_1 m_1 + r$ וגם $x = k_2 m_2 + r$

כעת נוכל לרשום את r באופן הבא :

$$r = l_1 m_1 + (r\ mod\ m_1)$$
$$r = l_2 m_2 + (r\ mod\ m_2)$$

עבור $l_1, l_2 \in \mathbb{Z}$ ולכן נקבל:

$$x = (k_1 + l_1)m_1 + (\ r\ mod\ m_1)$$

וגם

$$x = (k_2 + l_2)m_2 + (\ r\ mod\ m_2)$$

ולכן

$$x \equiv (r\ mod\ m_1)\ (\ mod\ m_1)$$
$$x \equiv (r\ mod\ m_2)\ (\ mod\ m_2)$$

חלק 4.

חשבון את $2^{644}\ (\,mod\ 645\,)$.

בטוח שלחשב את 2^{644} זה לא עבודה קלה, ולכן ישנם אלגורתמים אשר עוזרים לנו בחישובים אלה, נסתכל על האלגוריתם הרקרוסיבי הבא ונוכיח שהוא מספק פתרון לבעיה.

קלט: מספרים שלמים a, e, n כאשר $e \geq 0, n \geq 2$ ובנוסף $0 \leq a < n$

הוכיחו כי האלגוריתם הבא מחשב את $a^e\ (mod\ n\,)$

$F(a, e, n)$:

1. If $e = 0$ return 1.
2. Else if e mod $2 = 0$ then:
   (a) $t = F(a, e/2, n)$.
   (b) return t^2 mod n.
3. Else:
   (a) $t = F(a, e-1, n)$.
   (b) return at mod n.

הוכחה:

טרם נתחיל בהוכחה, כדאי לנו לשים לב כי הביטוי הבא מהווה הסבר אינטואיטיבי לפעולת האלגוריתם:

$$a^e = \begin{cases} a \cdot a^{e-1}, & e \text{ אי זוגי} \\ \left(a^{\frac{e}{2}}\right)^2, & e \text{ זוגי} \end{cases}$$

כעת נוכיח נכונות באינדוקציה על e:

בסיס: עבור $e = 0$ נקבל כי האלגוריתם יחזיר 1 ואכן $a^0 \equiv 1\ (mod\ n\,)$

צעד: נניח כי האלגוריתם מספק תוצאה נכונה עבור כל $f < e$ ונוכיח נכונות עבור e.

נחלק ל2 מקרים:

מקרה א' - e אי זוגי:

אם e אי זוגי נוכל לרשום ש $e = 2k + 1$ עבור $k \in \mathbb{Z}^+$, נשים לב כי לפי ההנחה עבור כל $f < e$ האלגוריתם מספק תוצאה נכונה עבור $a^f\ (mod\ n\,)$, ולכן לפי ההנחה, האלגוריתם מספק את הפתרון עבור $a^{2k}\ (\,mod\ n)$ בצורה נכונה, לאחר מכן האלגוריתם מכפיל את התוצאה ב a ולכן נקבל כי נקבל פתרון נכון עבור $a^e \equiv a^{2k+1}(mod\ n)$.

מקרה ב' - e זוגי:

אם e זוגי נוכל לרשום ש $e = 2k$ עבור $k \in N$. נשים לב כי לפי ההנחה עבור כל $f < e$ האלגוריתם מספק פתרון נכון עבור $a^f \ (mod\ n\ )$, ולכן לפי ההנחה האלגוריתם מספק פתרון נכון עבור $a^k\ (\ mod\ n)$. לאחר מכן האלגוריתם מעלה את התוצאה בריבוע ולכן נקבל כי הפתרון נכון עבור $a^e \equiv (a^k)^2 \equiv a^{2k}(mod\ n)$

חשיבות האלגוריתם:

נרצה להשתמש באלגוריתם זה על מנת לחשב את $2^{644}\ (\ mod\ 645\ )$.

אלגוריתם זה הוא רקרוסיבי, אנחנו "נתחיל" מסוף האלגוריתם.

שלב ראשון: נציג את 644 כסכום של חזקות של 2:

נשים לב כי $644 = 512 + 128 + 4$ ולכן $2^{644} = 2^{512} \cdot 2^{128} \cdot 2^4$

שלב שני: נחשב את $2^0, 2^1, 2^2, 2^4, 2^8, 2^{16}, 2^{32}, 2^{64}, 2^{128}, 2^{256}, 2^{512}\ mod(645)$

על אף שאנו זקוקים רק לשלוש חזקות של 2, כדי לחשב אותן אנו מוכרחים לעבור גם דרך כל היתר.

$2^{32} \equiv (2^{16})^2 \equiv 391^2 \equiv 16\ (mod\ 645)$ $2^{64} \equiv (2^{32})^2 \equiv 16^2 \equiv 256\ \ (mod\ 645)$ $2^{128} \equiv (2^{64})^2 \equiv 256^2 \equiv 391\ (mod\ 645)$ $2^{256} \equiv (2^{128})^2 \equiv 391^2 \equiv 16\ (mod\ 645)$ $2^{512} \equiv (2^{256})^2 \equiv 16^2 \equiv 256\ (mod\ 645)$	$2^0 \equiv 1\ (mod\ 645)$ $2^1 \equiv 2^0 \cdot 2 \equiv 2\ (mod\ 645)$ $2^2 \equiv (2^1)^2\ \ \equiv 2^2 \equiv 4(mod\ 645)$ $2^4 \equiv (2^2)^2 \equiv 4^2 \equiv 16\ (mod\ 645)$ $2^8 \equiv (2^4)^2 \equiv 16^2 \equiv 256\ (mod\ 645)$ $2^{16} \equiv (2^8)^2 \equiv 256^2\ \ \equiv 391(mod\ 645)$

עדיין היינו צריכים לבצע חישובים, אבל זה עדיין קל יותר מלחשב את 2^{644} ישירות.

סה"כ נקבל כי $2^{644} = 2^{512} \cdot 2^{128} \cdot 2^4 \equiv 16 \cdot 391 \cdot 256 \equiv 1\ (mod\ 645)$