©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תשע"ט:
בר אלון, מיכאל טוויטו, שמואל שמעוני, צבי מינץ, דורון מור, אלעד חורב
נכתב ע"י צבי מינץ

קונגרואנציות

חלק 1.

נזכר כי בהרצאה דברנו על אריתמטיקה מודלרית, ראינו את הטענה הבאה:

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:

טענה:
יהיו $a,b,c \in Z$ ויהי $m \in Z^+$ ויהי $d = (c,m)$
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 הדוגמא הבאה:

ידוע כי $14 \equiv 8\ (\ mod\ 2\ )$

ולכן לפי הטענה נקבל כי $7 \equiv 4\ (\ mod\ 1\ )$

נשים לב כי לא יכלנו לחלק ב2, היות ו- $7 \not\equiv 4\ (\ mod\ 2\ )$.

אולם, נשים לב כי נוכל לרשום את $7 \cdot 2 \equiv 4 \cdot 2\ \ (\ mod\ 2\ )$ בצורה הבאה:

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

במידה ותיהיה לנו טענה עבור משוואות מהצורה $a \cdot c \equiv b \cdot c\ (\ mod\ m \cdot c)$, הדברים היו יכולים להיות הרבה יותר פשוטים.

נסתכל על הטענה הבאה:

טענה:

יהיו $\boldsymbol{a,b,c \in \mathbb{Z}}$ ויהי $\boldsymbol{m \in \mathbb{Z}^+}$

אזי $\boldsymbol{a \equiv b\ (\ mod\ m\ )\quad \Leftrightarrow \quad a \cdot c \equiv b \cdot c\ (\ mod\ m \cdot c\ )}$

הוכחה: על מנת להוכיח טענת אם"ם יש צורך להוכיח גרירה דו כיוונית.

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

נניח כי $a \cdot c \equiv b \cdot c\ (\ mod\ m \cdot c\ )$ ולכן $m \cdot c \mid ac - bc$ ולכן $m \mid c(a-b)$ ולכן $m \mid (a-b)$ ולכן $a \equiv b\ (\ mod\ m\ )$

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

בר אלון, מיכאל טוויטו, שמואל שמעוני, צבי מינץ, דורון מור, אלעד חורב

נכתב ע"י צבי מינץ

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 ב c ונקבל $ca - cb = c \cdot m \cdot k$ ולכן $m \cdot c \mid ca - cb$ ולכן

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

■

נחזור לדוגמא הקודמת, $14 \ \equiv 8\ (mod\ 2\ )$

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

ולכן $7 \equiv 4\ (mod\ 1\ )$

כעת יש לנו סיכון קל לבלבול שנפתור בעזרת הדוגמא הבאה:

ידוע כי $15 \ \equiv 9\ (mod\ 6\ )$

נוכל לרשום זאת באופן הבא $3 \cdot 5 \ \equiv 3 \cdot 3\ (mod\ 6\ )$

לפי הטענה הראשונה

$$5 \ \equiv 3\ \left(mod \frac{6}{3}\right)$$

ולכן

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

לפי הטענה השנייה

$$3 \cdot 5 \ \equiv 3 \cdot 3\ (mod\ 2 \cdot 3\ )$$

ולכן

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

<u>נשים לב כי קבלנו תשובה זהה בעזרת 2 הטענות.</u>

כעת אנחנו יכולים לשאול את השאלה הבאה:

נראה כי הטענה הראשונה יותר "מסובכת", **האם היא באמת נחוצה**?

אז התשובה היא כן, כאשר מדובר במודלו ראשוני לדוגמא, ניתן לראות הבדל מהותי בין 2 הטענות.

יהיה p ראשוני כלשהו ו $(c,p) = 1$, נסתכל על :

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

לפי הטענה הראשונה, נקבל כי $a \ \equiv b\ (mod\ p\ )$ ואילו בטענה השנייה לא נוכל להשתמש היות ו p לא מתחלק ב c, הבעיה לא נובעת רק בגלל שהמודלו הוא ראשוני, אלא עבור כל m כך ש $(m,c) = 1$, טענה 2 **לא** תוכל לתרום לנו.

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

למעשה, הטענה השנייה אינה אמורה "לבטל" או להוות טענה עבור "חילוק" אלא "**להרחבה**".

בר אלון, מיכאל טוויטו, שמואל שמעוני, צבי מינץ, דורון מור, אלעד חורב

נכתב ע"י צבי מינץ

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

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 $x = 2(6n+2)+1$

אשר זוהי צורה אי זוגית, ולכן נוכל להגיד כי כל השלמים מהצורה $12n+5$ נמצאים ב $[1]_2$ **כלומר**, משאירים שארית 1 בחלוקה ב2.

וזה הודות לכך שמודולו 2 מחלק את קבוצת המספרים השלמים ל2 קבוצות, קבוצה של מספרים זוגיים אשר נמצאים ב $[0]_2$, וכל המספרים האי זוגיים אשר נמצאים ב $[1]_2$.

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

אנחנו יכולים לראות כיצד כל אותה מערכת שאריות מודולו 12 "משתלבת" אל תוך מערכת שאריות מודולו 2, וגם באופן ההפוך, כיצד כל מערכת השאריות מודולו 2 "משתלבת" אל תוך מערכת שאריות שלמה 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 $x \in [\,?\,]_3$?

למזלנו, 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 :

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

בר אלון, מיכאל טוויטו, שמואל שמעוני, צבי מינץ, דורון מור, אלעד חורב

נכתב ע"י צבי מינץ

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

ולכן ה"תמונה" תראה באופן הבא:

מערכת שאריות שלמה מודלו 12

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

מערכת שאריות שלמה מודלו 3

0	1	2

נציין כי משהו פה נראה "קל מדי", נראה שאם נקח כל זוג של שאריות זהות מה-"קבוצה הגדולה" אז נקבל גם כן **אותה** שארית ב"קבוצה הקטנה".

נשים לב כי זה קרה בגלל שלקחנו מערכת שאריות אשר מתחלקת באחרת, כלומר $3 \mid 12$.
כעת ננסה לענות על אותה שאלה, אך שכעת נחליף את 3 ב5, ונשאל את אותה שאלה:

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

נתחיל בכך שנשים לב ש $12 \nmid 5$.

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

$$x = 12q + r =$$
$$= (5l + r_1)q + 5k + r_2$$
$$= 5(lq + k) + r_1 q + r_2$$

- כאשר המעבר הראשון לשני זה להפעיל את משפט החלוקה עבור 5 על 12 ו- r.

כעת, כל מה שקבלנו זה ש $x \in [r_1 q + r_2]_5$

ניתן לראות כי עם קצת מאמץ נוכל לבצע חישוב זה לכל x, m כל עוד אנחנו יודעים ש $q = \left[\frac{12}{x}\right]$.

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

האם יש דרך להחזיר את אותה אלגנטיות עבור $x = 5$?

אנחנו מרגישים כי משהו שונה הולך לקרות היות ויכל להיות מצב שעבור 2 מספרים זרים $x_1, x_2 \in [r]_{12}$ נקבל 2 תשובות שונות עבור $[r_1 q + r_2]_5$:

$$x_1 := 12 \cdot 1 + 3 \ \in [3]_{12} = 5 \cdot 2 + 2 + 3 = 5 \cdot 3 \in [0]_5$$
$$x_2 := 12 \cdot 2 + 3 \ \in [3]_{12} = 4 \cdot 5 + 4 + 3 = 4 \cdot 5 + 7 =$$
$$= 4 \cdot 5 + 5 + 2$$
$$= 5 \cdot 5 + 2 \in [2]_5$$

אז עבור $x_1, x_2 \in [3]_{12}$ נקבל כי $x_1 \in [0]_5$ ו $x_2 \in [2]_5$, כלומר 2 שאריות **<u>שונות</u>**!

בר אלון, מיכאל טוויטו, שמואל שמעוני, צבי מינץ, דורון מור, אלעד חורב
נכתב ע"י צבי מינץ

באופן יותר כללי:

- ראינו את התשובה לשאלה :
  בהינתן $a \equiv c \ (mod\ m_1)$ מצאו את x כך ש $a \equiv x \ (mod\ m_2)$

- בנוסף, ראינו כי אם $(m_1, m_2) = 1$ אז $[c]_{m_1}$ יכול להתפצל על כמה שאריות שונות במודלו m_2 , בהנחה ש $m_2 < m_1$

- אם $(m_1, m_2) \neq 1$, כלומר עבור $m_2 < m_1$ ראינו כי $m_2 \mid m_1$ אז נוכל ישר להגיד כי אם $a \equiv c \ (mod\ m_1)$ אז $a \equiv c \ (mod\ m_2)$.

אבל מה עם הכיוון ההפוך?

קודם לכן לקחנו $a \in [r]_{12}$ ושאלנו את עצמנו לאיזה מחלקה מודלו 3 אנחנו שייכים, כעת אם נהפוך את השאלה, כלומר, נניח כי $a \in [r]_3$, צריך למצוא עבור איזה $k \in [0,11]$ נקבל כי $a \equiv k \ (mod\ 12)$

העבודה ש $[r]_3$ מתפצל, רומז שאנחנו לא יכולים לקוות לטענה שתעזור לנו לא לעשות שום חישובים (כמו שהיה לנו בצד השני במקרה ש m_1 ו m_2 אינם זרים)

אז כאן נצטרך להפעיל את משפט החלוקה עבור a ו 12 באופן ישיר.

חלק 3.

טענה:
יהיו $a_1, a_2, \dots, a_n$ מספרים שלמים **זרים** עבור $n \in \mathbb{Z}^+$
אזי:
$$lcm(a_1, a_2, \dots, a_n) = a_1 \cdot a_2 \cdot \dots \cdot a_n$$

על מנת להוכיח טענה זו יש צורך בכמה טענות מוקדמות.

נגדיר את הקבוצה הבאה : $\mathcal{D}_a = \{n \in \mathbb{Z}^+ : a \mid n\}$

כלומר, הקבוצה $\mathcal{D}_a$ מכילה את כל המספרים השלמים אשר מתחלקים ב a, או בניסוח שונה, כל המספרים השלמים אשר הינם כפולה של a.

טענה:
יהיו a, b שני מספרים שלמים זרים
אזי $\mathcal{D}_a = \mathcal{D}_b \Leftrightarrow a = b$

הוכחה:

על מנת להוכיח טענת אם"ם נוכיח גרירה דו כיוונית

כיוון ראשון: $\boldsymbol{\mathcal{D}_a = \mathcal{D}_b \Leftarrow a = b}$

מתקיים באופן טרוואלי. היות ואם $a = b$ אז כמובן ש $\mathcal{D}_a = \mathcal{D}_b$.

כיוון שני: $\boldsymbol{\mathcal{D}_a = \mathcal{D}_b \Rightarrow a = b}$

נניח כי $\mathcal{D}_a = \mathcal{D}_b$, נוכיח כי $a = b$.

בר אלון, מיכאל טוויטו, שמואל שמעוני, צבי מינץ, דורון מור, אלעד חורב

נכתב ע"י צבי מינץ

נניח בשלילה כי $a \neq b$ ונניח בה"כ (בלי הגבלת הכלליות) כי $a < b$.

נשים לב כי לפי הגדרת הקבוצה $\mathcal{D}_a$, אזי $a \in D_a$, אבל בטוח כי $a \notin D_b$ כי $a < b$

ולכן הגענו לסתירה להנחה ש $\mathcal{D}_a = \mathcal{D}_b$. ■

טענת נוספת שנעזר בה היא הטענה הבאה:

> **טענה:**
> יהיו $a_1, a_2, \ldots, a_n$ מספרים שלמים זרים עבור $n \in \mathbb{Z}^+$, אזי:
> $$lcm(a_1, a_2, \ldots, a_n) = lcm\,(lcm\,(a_1, a_2, \ldots a_{n-1}), a_n)$$

<u>הוכחה:</u>

נגדיר $\alpha = lcm(a_1, \ldots, a_n)$

נגדיר $\beta = lcm(lcm(a_1, \ldots, a_{n-1}), a_n)$

נגדיר $\gamma = lcm(a_1, \ldots, a_{n-1})$.

נראה כי $\mathcal{D}_\alpha = \mathcal{D}_\beta$ ולכן $\alpha = \beta$ לפי הטענה הקודמת, נוכיח זאת ע"י הכלה דו כיוונית.

צד ראשון: נראה כי $\mathcal{D}_a \subseteq \mathcal{D}_b$

יהי $m \in D_\alpha$, ולכן $m \mid \alpha$, היות ולכל a_i מתקיים ש $\alpha \mid a_i$, נובע כי $m \mid a_i$ עבור כל $i \in [n]$

בגלל ש $m \mid a_i$ עבור כל $i \in [n]$ נובע כי $m \mid \gamma$, בוסף $m \mid a_n$ ולכן $m \mid \beta$

נשים לב כי הוכחנו שעבור כל $m \in \mathcal{D}_\alpha$ מתקיים כי $m \mid \beta$ ולכן $\mathcal{D}_\alpha \subseteq \mathcal{D}_\beta$

צד שני: נראה כי $\mathcal{D}_\alpha \supseteq \mathcal{D}_\beta$

יהי $m \in D_\beta$ ולכן $m \mid \beta$, כלומר $m \mid a_n$ וגם $m \mid \gamma$, מכאן נובע כי לכל $i \in [1, n-1]$ מתקיים ש $m \mid a_i$, בצירוף עם כך ש $m \mid a_n$ נקבל כי $m \mid a_i$ עבור כל $i \in [1, n]$ ולכן $m \mid \alpha$ ולכן $m \in \mathcal{D}_\alpha$.

נשים לב כי הוכחנו שעבור כל $m \in D_\beta$ מתקיים כי $m \mid \alpha$ ולכן $D_\alpha \supseteq D_\beta$

הוכחנו הכלה דו כיוונית ולכן $\mathcal{D}_\alpha = \mathcal{D}_\beta$ ולכן $\alpha = \beta$ לפי הטענה הקודמת, זאת אומרת

$$lcm(a_1, a_2, \ldots, a_n) = lcm\,(lcm\,(a_1, a_2, \ldots a_{n-1}), a_n)$$

■

לאחר שסיימנו להוכיח את טענות העזר, נתקדם בהוכחה של הטענה המקורית.

נזכר בטענה אותה נרצה להוכיח:

> **טענה:**
> יהיו $a_1, a_2, \ldots, a_n$ מספרים שלמים **זרים** עבור $n \in \mathbb{Z}^+$
> אזי:
> $$lcm(a_1, a_2, \ldots, a_n) = a_1 \cdot a_2 \cdot \ldots \cdot a_n$$

<u>הוכחה:</u>

נוכיח באינדוקציה על n

בסיס: עבור $n=2$ נקבל כי צ"ל ש $lcm(a_1,a_2)=a_1*a_2$.

הוכחנו בתרגולים הקודמים כי $lcm(a_1,a_2)=\frac{a_1\cdot a_2}{(a_1,a_2)}$, מההנחה כי a_1 ו a_2 זרים נקבל כי $lcm(a_1,a_2)=a_1\cdot a_2$.

צעד: נניח כי הטענה עבור כל $n\geq 2$, כלומר $lcm(a_1,a_2,\dots,a_n)=a_1\cdot a_2\cdot\ldots\cdot a_n$ ונוכיח נכונות עבור $n+1$, כלומר צ"ל כי $lcm(a_1,a_2,\dots,a_n,a_{n+1})=a_1\cdot a_2\cdot\ldots\cdot a_n\cdot a_{n+1}$.

נשים לב כי:

$$lcm(a_1,a_2,\dots,a_n,a_{n+1})=lcm(lcm(a_1,\dots,a_n),a_{n+1})$$

בגלל הטענה הקודמת, בנוסף לפי הנחת האינדוקציה מתקיים:

$$lcm(a_1,a_2,\dots,a_n)=a_1\cdot a_2\cdot\ldots\cdot a_n$$

ולכן לפי הנחת האינדוקציה מתקיים :

$$lcm(lcm(a_1,\dots,a_n),a_{n+1})=lcm(a_1\cdot a_2\cdot\ldots\cdot a_n,a_{n+1})$$

לפי ההנחה, עבור כל $i\neq j:\ i,j\in[1,n]$ מתקיים כי $(a_i,a_j)=1$ ולכן היות ואף אחד מהאיברים לא חולק ראשוניים משותפים, נקבל כי :

$$(a_1\cdot a_2\cdot\ldots\cdot a_n,a_{n+1})=1$$

ולכן $lcm(a_1\cdot a_2\cdot\ldots\cdot a_n,a_{n+1})=a_1\cdot a_2\cdot\ldots\cdot a_n\cdot a_{n+1}$.

מכאן הטענה נובעת. ■

<u>חלק 4.</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 $i\in[1,k]$

ולכן $lcm(m_1,\dots,m_k)\mid a-b$ ומכאן הטענה נובעת.

<u>דוגמא:</u>

אם $x\equiv 1\ (mod\ 2)$, $x\equiv 1\ (mod\ 4)$, $x\equiv 1\ (mod\ 6)$ **אז** $x\equiv 1\left(mod\ lcm(2,4,6)\right)\equiv 1\ (mod\ 12)$

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>דוגמא:</u>

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

אבל האם זה נכון גם לכיוון השני ?

כלומר אם $a \equiv b \ (mod\ m_1 \cdot m_2 \cdot \dots \cdot m_k)$ אז $a \equiv b \ (mod\ m_i)$ עבור כל $i \in [1, k]$?

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 לכך ש $a - b \mid k_i m_i$ עבור כל $i \in [1, k]$

ולכן עבור כל i שכזה 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 $i \in [k]$: $lcm(m_1, m_2, \dots, m_k) \Leftrightarrow m_i \mid a - b$.

נחזק את 2 הטענות הקודמות באופן הבא:

יהיו $m_1, m_2, \dots, m_k$ מספרים שלמים עבור $k \in \mathbb{Z}^+$, 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:
$a \equiv b \ (mod\ m_i), \forall i \in [1, k] \Leftrightarrow a \equiv b \ (mod\ m_1 \cdot m_2 \cdot \dots \cdot m_k)$

<u>**דוגמא:**</u>

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

נשים לב כי $(4,6) = 2$ וכי $lcm(4,6) = 12$ 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:

נשים לב כי $(3,4) = 1$ ולכן:

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

בר אלון, מיכאל טוויטו, שמואל שמעוני, צבי מינץ, דורון מור, אלעד חורב

נכתב ע"י צבי מינץ

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 $x \equiv r\ \big(\,mod\ lcm(m_1,m_2)\big)$

אז $\begin{matrix} x\ \equiv r\ (\,mod\ m_1)\ (\,mod\ m_1) \\ x\ \equiv r\ (\,mod\ m_2)(\,mod\ m_2) \end{matrix}$

הוכחה:

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

$x = lcm(m_1,m_2)\cdot n + r$ כאשר $n \in \mathbb{Z}$, ידוע כי $\begin{matrix} m_1 \mid lcm(m_1,m_2) \\ m_2 \mid lcm(m_1,m_2) \end{matrix}$ 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 :

$\begin{matrix} r = l_1 m_1 + r(mod\ m_1) \\ r = l_2 m_2 + r(mod\ m_2) \end{matrix}$ 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

$$\begin{matrix} x\ \equiv r\ (\,mod\ m_1)\ (\,mod\ m_1) \\ x\ \equiv r\ (\,mod\ m_2)(\,mod\ m_2) \end{matrix}$$

דוגמא:

נחזור לדוגמא הקודמת

אם $x \equiv 9\ (\,mod\ 12\,)$ **אזי** לפי הטענה נקבל כי $\begin{matrix} x \equiv 1\ (\,mod\ 4\,) \\ x \equiv 0\ (\,mod\ 3\,) \end{matrix}$.

חלק 5.

תרגיל:

חשבו 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 הרקורסיבי הבא ונוכיח שהוא מספק פתרון לבעיה.

קלט: מספרים שלמים a, e, n כאשר $n \geq 2$, $e \geq 0$ 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 $e \bmod 2 = 0$ then:
   (a) $t = F(a, e/2, n)$.
   (b) return $t^2 \bmod n$.
3. Else:
   (a) $t = F(a, e - 1, n)$.
   (b) return $at \bmod n$.

הוכחה:

קודם כל נשים לב כי

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

נוכיח נכונות באינדוקציה על e

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

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 האלגורים מכפיל את התוצאה ב a ולכן נקבל כי נקבל פתרון נכון עבור $a^e \equiv a^{2k+1} (mod\ n)$

מקרה ב' - e זוגי:

בר אלון, מיכאל טוויטו, שמואל שמעוני, צבי מינץ, דורון מור, אלעד חורב

נכתב ע"י צבי מינץ

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

■

חשיבות:

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

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

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

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

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

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

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