<u>אלגוריתם אוקלידס המורחב</u>

לפי זהות בזו ידוע כי $(a,b) \in \mathcal{L}(a,b)$ כאשר $\mathcal{L}(a,b) \coloneqq \{ma+nb \mid m,n \in \mathbb{Z}\}$

נשקול תרגילים מהסגנון :

מצא $x,y \in \mathbb{Z}$ כך ש $36 = 252 \cdot x + 192 \cdot y$

אלגוריתם אוקלידס המורחב

<u>טענה 1 (מהרצאה):</u> למשוואה $ax+by=c$ יש פתרון בשלמים אם ורק אם $(a,b) \mid c$

<u>טענה 2 (מהרצאה):</u> יהי (x_0,y_0) פתרון למשוואה $ax+by=c$ אזי כל פתרון אחר (x,y) ל $ax+by=c$ הוא מהצורה:

$$x = x_0 + \left(\frac{b}{(a,b)}\right) \cdot t$$
$$y = y_0 - \left(\frac{a}{(a,b)}\right) \cdot t$$

עבור $t \in \mathbb{Z}$

דוגמא לשימוש באלגוריתם אוקלידס המורחב:
<u>תרגיל 3:</u>

מצא $x,y \in \mathbb{Z}$ כך ש $36 = 252 \cdot x + 192 \cdot y$

<u>פתרון:</u>

1. **<u>קודם כל נבצע את אלגוריתם אוקלידס הרגיל ונמצא את ה– (a,b)</u>**

$$252 = (198) \cdot 1 + 54$$

$$198 = (54) \cdot 3 + 36$$

$$54 = (36) \cdot 1 + \mathbf{18}$$

$$36 = (18) \cdot 2 + (0)$$

$$\Rightarrow (252,198) = 18$$

2. **<u>נבצע "הצבה הפוכה"</u>**
   - נמצא את המשוואה האחרונה שהשארית אינה 0.
     $54 = (36) \cdot 1 + \mathbf{18}$
   - נבודד את כלל השאריות:
     $\mathbf{18} = 54 - (36) \cdot 1$
     $36 = 192 - (54) \cdot 3$
     $54 = 252 - (198) \cdot 1$
   - נבצע הצבה הפוכה מהמשוואה הראשוני עד לקומבנציה לינארית של 252 ו 198

נקבל כי :

$$18 = 54 - 36 \cdot 1 =$$
$$= 54 - (192 - (54) \cdot 3) \cdot 1 =$$
$$= (54) \cdot 4 - 198 \cdot 1 =$$

$$= (252 - (198) \cdot 1) \cdot 4 - 198 \cdot 1 =$$
$$= 252 \cdot 4 - 198 \cdot 5$$

ולכן $(x, y) = (4, -5)$

3. נבצע בדיקה עבור הפלט

$18 = 252 \cdot 4 - 198 \cdot 5$ - אכן מתקיים.

4. בדיקה האם קיים פתרון

נבדוק האם קיימים $x, y \in \mathbb{Z}$ כך ש $36 = 252 \cdot x + 198 \cdot y$

לפי טענה 1, למשוואה $ax + by = c$ יש פתרון בשלמים אם ורק אם $(a, b) \mid c$, כלומר אם $(a, b) \nmid c$ אזי אין פתרון למשוואה.

במקרה שלנו, $a = 252, b = 198$ ו $(a, b) = 18, c = 36$ ואכן מתקיים כי $18 \mid 36$ ולכן קיים פתרון למשוואה $36 = 252 \cdot x + 198 \cdot y$

5. נגיע למשוואה הרצויה

נכפיל ב $\frac{c}{(a,b)}$ את המשוואה, במקרה שלנו נכפיל ב $2 = \frac{36}{18}$

ונקבל כי:

$$18 = 252 \cdot 4 - 198 \cdot 5 \quad | \quad \cdot 2 \quad \Rightarrow 36 = 252 \cdot 8 - 198 \cdot 10$$

ולכן $x_0 = 8, y_0 = -10$.

6. פתרון

לפי טענה 2, אם יש פתרון כללי למשוואה $ax + by = c$ אזי יש **אינסוף** פתרונות.
כי אם (x_0, y_0) פתרון למשוואה $ax + by = c$ אזי כל פתרון אחר (x, y) ל $ax + by = c$ הוא מהצורה:

$$x = x_0 + \left(\frac{b}{(a, b)}\right) \cdot t$$

$$y = y_0 - \left(\frac{a}{(a, b)}\right) \cdot t$$

עבור $t \in \mathbb{Z}$

ולכן במקרה שלנו, $(x_0, y_0) = (8, -10)$ ולכן פתרון כללי למשוואה $36 = 252 \cdot x + 198 \cdot y$ הוא מהצורה:

$$x = 8 + 11 \cdot t$$
$$y = -10 - 14 \cdot t$$

עבור $t \in \mathbb{Z}$

הערה: נשים לב כי עבור $t = 1$ בפרט מתקיים כי $36 = 252 \cdot 19 + 198 \cdot (-24)$

שקליות מודלריות:

חשבון מודלרי – שיטה מתמטית בה מחליפים מספרים בשארית החלוקה במספר קבוע, הדוגמא הידועה ביותר לחשבון מודלרי היא החשבון על פני שעון. שעון הוא חשבון מודלרי מודלו 24, האם השעה כעת היא 20:00 ואנו רוצים לדעת מה תהיה השעה 9 שעות מאוחר יותר הפעולה שאנחנו עושים היא $20 + 9 \equiv 5 (mod\ 24)$

הגדרה: $a \equiv b\ (mod\ m)$ אם"ם $m \mid a - b$ אם"ם $a - b = km$ אם"ם $a = b + km$ עבור $k \in \mathbb{Z}$

במילים אחרות, $a \equiv b\ (mod\ m)$ אם a ו– b משאירים את **אותה שארית** בחלוקה ב– m.

הגדרה: מספרים a,b נקראים שקולים מודלו m אם $a \equiv b \ (mod\ m)$

משפט 1: היחס השקילות מודלו הוא **יחס שקילות.**
כלומר, יהיו $a,b,c \in \mathbb{Z}$ אזי התכונות הבאות מתקיימות:

- **רפלקסיבי Reflexive:** $a \equiv a \ (mod\ m\ )$
- **סימטרי Symmetric:** אם $a \equiv b \ (mod\ m\ )$ אזי $b \equiv a \ (mod\ m\ )$
- **תורשתי/טרנזטיבי Transitive:** אם $a \equiv b \ (mod\ m)$ ו $b \equiv c \ (mod\ m\ )$ אזי $a \equiv c \ (mod\ m\ )$

הוכחה (תורשתי): ידוע כי $a \equiv b \ (mod\ m)$ ו $b \equiv c \ (mod\ m\ )$ ולכן $m \mid a-b$ ו $m \mid b-c$
ולכן $a-b = mk_1$ ו $b-c = mk_2$ ולכן אם נחבר את 2 המשוואות נקבל כי
$a-c = m(k_1+k_2)$ ולכן $m \mid a-c$ ולכן $a \equiv c \ (mod\ m)$

אריתמטיקה מודלרית :

0. כל כפולה של המודלו שקולה ל-0

עבור כל $k \in \mathbb{Z}$ מתקיים כי $km \equiv 0 \ (mod\ m)$

לדוגמא $14 \equiv 0 \ (\ mod\ 7)$

לתכונה זו יש שימוש מרכזי בצימצום משוואת.

תרגיל: מצאו מהו x עבור השקילות הבאה:

$$1925141221 \equiv x \ (\ mod\ 10)$$

פתרון: נשים לב כי $1925141221 = 1925141220 \cdot 10 + 1$

ולכן $1925141221 \equiv 1925141220 \cdot 10 + 1 \equiv 1 \ (\ mod\ 10)$

1. מותר להוסיף כפולה של המודלו לכל אחד מהאגפים.

אם $a \equiv b \ (mod\ m)$ ויהי $k \in \mathbb{Z}$ אזי:

א. $a + km \equiv b \ (mod\ m\ )$
ב. $a \equiv b + km (mod\ m\ )$
ג. $a + km \equiv b + km (mod\ m\ )$

2. ניתן להוסיף ולהחסיר את האגפים בכל מספר שלם

אם $a \equiv b \ (mod\ m)$ ו $c \in \mathbb{Z}$ אזי:

א. $a + c \equiv b + c \ (mod\ m\ )$
ב. $a + c \equiv b + c \ (mod\ m\ )$
ג. $a \cdot c \equiv b \cdot c \ (mod\ m\ )$

בנוסף אם $c \equiv d \ (mod\ m\ )$ וכן $a \equiv b \ (mod\ m\ )$, אזי:

א. $a + c \equiv b + d \ (mod\ m\ )$
ב. $a + c \equiv b + d \ (mod\ m\ )$
ג. $a \cdot c \equiv b \cdot d \ (mod\ m\ )$

3. ניתן לעלות בחזקה אי שלילית

אם $a \equiv b\ (mod\ m)$ ו $k \in \mathbb{Z}^+$ אזי: $a^k \equiv b^k\ (mod\ m)$

4. **אסור לחלק!**

משפט 2: יהיו $a,b,c \in \mathbb{Z}$ ויהי $m \in \mathbb{Z}^+$ כך ש $d = (c,m)$ אזי
$$ac \equiv bc\ (mod\ m) \Leftrightarrow a \equiv b\ (mod \frac{m}{d})$$

אבחנה: אם $(c,m) = 1$ אזי מתקיים כי ניתן לצמצם ב-c מבלי לשנות את המודלו.
לדוגמא:
אם $14 \equiv 35\ (mod\ 3)$ אזי $2 \equiv 5\ (mod\ 3)$ כי $(7,3) = 1$
אם $4 \equiv 2\ (mod\ 2)$ אזי $2 \not\equiv 1\ (mod\ 2)$ אלא $2 \equiv 1\ (mod\ 1)$ כי $(2,2) = 2$
הוכחה:
יש צורך להוכיח 2 כיוונים
כיוון ראשון: נניח כי $ac \equiv bc\ (mod\ m)$, כלומר $m \mid ac - bc$ ולכן קיים $k \in \mathbb{Z}$ כך ש:
$$mk = c(a-b)$$
לפי הגדרת gcd ניתן לרשום $\substack{c=dr \\ m=ds}$ עבור $(r,s) = 1$ ולכן נציב במשוואה הקודמת ונקבל:
$$dsk = dr(a-b)$$
ידוע כי $d \geq 1$ ולכן נוכל לצמצם את 2 האגפים ב d ולכן:
$$sk = r(a-b)$$
ולכן:
$$s \mid r(a-b)$$
כעת, ידוע כי $(s,r) = 1$ ולכן לפי **טענת עזר** $s \mid a-b$ ולכן $a \equiv b\ (mod\ s = \frac{m}{d})$
טענת עזר: אם $a \mid bc$ ו $(a,b) = 1$ אזי $a \mid c$ (הוכחנו זאת בתרגולים קודמים)

כיוון שני: כיוון זה זהה לכיוון הראשון, רק שעובדים "מלמטה למעלה".

תרגיל 1:
הוכיחו כי $2^{20} \equiv 1\ (mod\ 41)$
פתרון: נציג 2 דרכים לפתרון

דרך א'

שלב ראשון: נציג את הביטוי ע"י שקליות כלומר צ"ל כי $2^{20} \equiv 1\ (mod\ 41)$

שלב שני: העלה בחזקות שקרובות למודלו
$$2^{20} \equiv (2^5)^4 \equiv (32)^4 \equiv (-9)^4 \equiv ((-9)^2)^2 \equiv (81)^2 \equiv (-1)^2 \equiv 1\ (mod\ 41)$$

דרך ב'

שלב ראשון: נציג את הביטוי ע"י שקליות כלומר צ"ל כי $2^{20} \equiv 1\ (mod\ 41)$
שלב שני: נגיע ל 2^{20} ע"י העלאה של כפולות של הבסיס
שלב שלישי: ידוע כי $2^{20} = 2^{16} \cdot 2^4$ (פירוק של 20 לבינארי)
כעת נחשב את $2^{16}, 2^4$
$$2 \equiv 2\ (mod\ 41)$$
$$2^2 \equiv 2^2 \equiv 4\ (mod\ 41)$$
$$2^4 \equiv 4^2 \equiv 16\ (mod\ 41)$$
$$2^8 \equiv 16^2 \equiv 256 \equiv 10\ (mod\ 41)$$
$$2^{16} \equiv 10^2 \equiv 100 \equiv 18\ (mod\ 41)$$
שלב רביעי: נבצע מכפלה
$$2^{20} \equiv 2^{16} \cdot 2^4 \equiv 18 \cdot 16 \equiv 288 \equiv 1\ mod\ (41)$$

תרגיל 2:
א. נתון ש- $n \equiv 3 \pmod 7$. מה ניתן להסיק על $n \bmod 14$? (8 נק')
ב. נתון ש- $t \equiv 3 \pmod{14}$. מה ניתן להסיק על $t \bmod 7$? (7 נק')

פתרון:

סעיף א' : ידוע כי $n \equiv 3 \ (mod\ 7\ )$ ולכן $7 \mid n-3$ ולכן $k \in \mathbb{Z} : n-3=7k$ ולכן

$n=7k+3$. כעת נחלק ל2 מקרים

מקרה ראשון: k זוגי ולכן $t \in \mathbb{Z} : k=2t$

ולכן מתקיים כי $n=14t+3$ ולכן $n \equiv 3 \ (mod\ 14)$

מקרה שני: k אי זוגי ולכן $t \in \mathbb{Z} : k=2t+1$

ולכן מתקיים כי $n=14t+10$ ולכן $n \equiv 10 \ (mod\ 14)$ ולכן התשובה היא

$n \equiv 3 \ (mod\ 14)$ או $n \equiv 10 \ (mod\ 14)$

סעיף ב' : ידוע כי $t \equiv 3 \ (\ mod\ 14\ )$ ולכן $14 \mid t-3$ ולכן $k \in \mathbb{Z} : t-3=14k$ ולכן

$$t \equiv 14k+3 \equiv 7(2k)+3 \equiv 3 \ (mod\ 7)$$

תרגיל 3:

הוכיחו כי $27 \mid 2^{5n+1}+5^{n+2}$

פתרון:

דרך מחשבה בתרגילים כאלה הוא קודם כל להעביר לשקליות, ולאחר מכן לנסות להגיע לאותו בסיס ע"י הוספה או החסרה של כפליות של המודלו.

צריך להוכיח כי $2^{5n+1}+5^{n+2} \equiv 0 \ (mod\ 27)$

- חשוב מאוד לשים לב כי זו אינה משוואה אלה שקילות, יש להגיע מאגף שמאל אל אגף ימין כלומר לצאת מ $2^{5n+1}+5^{n+2} \ (mod\ 27)$ ולהגיע ל $0 \ (mod\ 27)$

$$2^{5n+1}+5^{n+2} \equiv 2 \cdot 2^{5n} + 25 \cdot 5^n \equiv 2 \cdot (32)^n + 25 \cdot 5^n \equiv$$

$$\equiv 2 \cdot (32-27=5)^n + 25 \cdot 5^n \equiv 27 \cdot 5^n \equiv 0 \ (mod\ 27)$$