תזכורות משבוע שעבר:

- כדי להוכיח ש $(a,b)=(c,d)$ יש להראות שכל מחלק משותף של a,b הוא מחלק משותף של c,d **ולהפך**.
- כדי להוכיח ש $(a,b)=1$, כלומר a,b זרים אז ניתן להראות כי:
  1. קיימים $x,y\in\mathbb{Z}$ כך ש $1=ax+by$.
  2. להראות שכל מחלק של a,b מחלק את 1.
  3. להראות כי $d=(a,b)$ מחלק את 1 או שווה ל-1.

  נשים לב כי $\forall a,b\in\mathbb{Z}$ מתקיים כי $(a,b)\geq 1$ ולכן מספיק להראות כי הוא חסום ע"י 1 ע"י כך שהוא מחלק את 1. ולכן $(a,b)\leq 1$ ולכן $(a,b)=1$
- אם $d \mid |a-\beta b|$ אז $d \mid a-\beta b$

תרגיל 1:

יהי $p_1,p_2,\dots,p_n$ n המספרים הראשוניים ויהי $k\in[1,n]$. נגדיר :

$$Q\coloneqq p_1\cdot p_2\cdot\dots\cdot p_k$$
$$R\coloneqq p_{k+1}\cdot p_{k+2}\cdot\dots\cdot p_n$$

1. הוכיחו כי לכל $i\in[n]$ מתקיים כי $Q+R \nmid p_i$ $p_i \nmid Q+R$
2. העזרו בסעיף א' על מנת לתת הוכחה לכך שיש אינסוף ראשוניים.

פתרון: במודל [תרגול 6](#)

1. יהי p_i ראשוני כלשהו כך ש $i\in[1,n]$, נניח בה"כ כי $p_i\in[p_{k+1},p_n]$

$$p_i\nmid Q \text{ ו } p_i\mid R$$

נניח בשלילה כי $p_i\mid Q+R$ ולכן לפי תכונות חלוקה מתקיים כי $p_i\mid Q+R-R=Q$ בסתירה לכך ש $p_i\nmid Q$

2. נניח בשלילה ש $p_1,\dots,p_n$ הינם כל הראשוניים בעולם, מכוון ש 2,3 ראשוניים נקבל כי $n\geq 2$ ולכן קיים $k\in[1,n]$ כך ש :

$$Q\coloneqq p_1\cdot p_2\cdot\dots\cdot p_k$$

$$R\coloneqq p_{k+1}\cdot p_{k+2}\cdot\dots\cdot p_n$$

היות ו $Q+R$ גדול מכל הראשוניים נובע שהוא מספר פריק, כי אם אחרת, הוא דוגמא נגדית עצמאית להמצאות ראשוני נוסף.

לפי ההנחה $Q+R$ פריק ולכן קיים מחלק ראשוני q כך ש $q\mid Q+R$ ולכן לפי לפי סעיף א' מתקיים כי $q\neq p_i$ עבור כל $i\in[1,n]$ ולכן $q\notin\{p_1,\dots,p_n\}$ בסתירה לכך שהקבוצה $\{p_1,\dots p_n\}$ היא קבוצת כל הראשוניים בעולם.

תרגיל 2:

הוכיחו כי יש אינסוף ראשוניים מהצורה $4n+3$

פתרון:

נניח כי יש מספר סופי של ראשוניים מהצורה $4n+3$, נגדיר $S\coloneqq\{p_1,p_2,\dots,p_n\}$ קבוצת כל הראשוניים מהצורה $4n+3$.

נגדיר $N\coloneqq 4(p_1\cdot\ldots\cdot p_n)+3$, נשים לב כי $N>1$ ולכן קיים ל– N מחלק ראשוני כלשהו.

אבחנה: כפולה של 2 מספרים מהצורה $4n+1$ נשארת מהצורה $4m+1$.
הוכחה: נקח 2 מספרים מהצורה $4n+1$ ונכפיל בינהם, נראה כי הצורה שמתקבלת היא $4m+1$

$$(4q+1)\cdot(4k+1) = 16qk + 4q + 4k + 1 = 4(4qk + q + k) + 1 = 4m + 1$$

נשים לב כי **כל** מחלק ראשוני של N הוא מהצורה $4n+1$ **או** מהצורה $4n+3$ (שאר הצורות זוגיות),
ונשים לב כי N מהצורה $4n+3$.
לפי הטענה הקודמת, לא יכול להיות שכל המחלקים של N הם מהצורה $4n+1$, כי אם אחרת, הוא היה נשאר מהצורה $4n+1$, אך N מהצורה $4n+3$ ולכן **קיים** ל $N -$ מחלק ראשוני **אחד** לפחות מהצורה $4n+3$, נקרא למחלק הראשוני הזה q.

קבלנו כי $N \mid q$, בנוסף היות ו q מהצורה $4n+3$ אזי לפי ההנחה $q \in S$ ולכן $q \mid \prod_{i \in S} p_i$
ולכן מתכונות חלוקה נקבל כי $q \mid 4 \cdot (\prod_{i\in S} p_i)$ ולכן גם כן מתכונות חלוקה נקבל כי:

$$q \mid N - 4\cdot\left(\prod_{s\in S} s\right) = 3$$

נשים לב כי היינו רוצים להגיד שהגענו לסתירה (כמו בהוכחות הקודמות) ולכן $q \notin S$ ולכן מצאנו ראשוני חדש מהצורה $4n+3$ <u>**אבל**</u> יכול להיות ש $q = 3$

הוכחה מהצורה הזאת לא תעבוד, ולכן נשים לב כי הוכחנו בתרגול הראשון כי :

$$\{4n+3 \mid n \in \mathbb{Z}\} = \{4n-1 \mid n \in \mathbb{Z}\}$$

ולכן מספיק להוכיח כי יש אינסוף ראשוניים מהצורה $4n-1$

הוכחה:
נניח כי יש מספר סופי של ראשוניים מהצורה $4n-1$, נגדיר $S \coloneqq \{p_1, p_2, \dots, p_n\}$ קבוצת כל הראשוניים מהצורה $4n-1$.

נגדיר $N \coloneqq 4(p_1 \cdot \ldots \cdot p_n) + 1$, נשים לב כי $N > 1$ ולכן קיים ל– N מחלק ראשוני כלשהו. הוכחנו כי כל מכפלה של גורמים מהצורה $4n+1$ נשארת באותה צורה, ולכן חייב להיות מחלק ראשוני ל– N מהצורה $4n-1$, יהא q מחלק זה.

קבלנו כי $N \mid q$, בנוסף היות ו q מהצורה $4n-1$ אזי לפי ההנחה $q \in S$ ולכן $q \mid \prod_{i \in S} p_i$
ולכן מתכונות חלוקה נקבל כי $q \mid 4 \cdot (\prod_{i\in S} p_i)$ ולכן גם כן מתכונות חלוקה נקבל כי:

$$q \mid N - 4\cdot\left(\prod_{s\in S} s\right) = -1$$

אך $q \geq 3$ ולכן $q \nmid -1$ בסתירה להנחה.

<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 :

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

אלגוריתם אוקלידס המורחב

EXT-EUCLID(a,b)

1. if $b = 0$ then return $(a, 1, 0)$.
2. $(d', x', y') = EXT - EUCLID(b, a \bmod b)$.
3. $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$.
4. return (d, x, y).

<u>**קלט:**</u> מקבל כקלט $a \geq b > 0$ שלמים
<u>**פלט:**</u> מחזיר כפלט את השלשה (d, x, y) כאשר $d = (a,b)$ ו x, y הם הפתרונות לקומבנציה הלינארית $d = ax + by$.

<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>

מצאו $x,y\in\mathbb{Z}$ 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 :

$$\begin{aligned}18 &= 54-36\cdot 1=\\ &= 54-(192-(54)\cdot 3)\cdot 1=\\ &=(54)\cdot 4-198\cdot 1=\\ &=(252-(198)\cdot 1)\cdot 4-198\cdot 1=\\ &=252\cdot 4-198\cdot 5\end{aligned}$$

ולכן $(x,y)=(4,-5)$

3. **<u>נבצע בדיקה עבור הפלט</u>**
   $18=252\cdot 4-198\cdot 5$ - אכן מתקיים.
4. **<u>בדיקה האם קיים פתרון</u>**

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 $c \nmid (a, b)$ 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. <u>**נגיע למשוואה הרצויה**</u>

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. <u>**פתרון**</u>

לפי טענה 2, אם יש פתרון כללי למשוואה $ax + by = c$ אזי יש <u>**אינסוף**</u> 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 $t \in \mathbb{Z}$

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