$$1+2+2^2+\dots\dots+2^n = \frac{2^{n+1}-1}{2-1} = 2^{n+1}-1$$

$$1+q+q^2+\dots\dots+q^n = \frac{q^{n+1}-1}{q-1}$$

נוכל $\alpha = \frac{1+\sqrt{5}}{2}$

$f_n > \alpha^{n-2}$ לכל $n \geq 3$

$f_{n+2} - f_{n+1} - f_n = 0$

$x^2 - x - 1 = 0$

$\alpha = \frac{1+\sqrt{5}}{2}$ $\quad \frac{1-\sqrt{5}}{2} = \beta$ $\quad f_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$

כדי מוכיח...

הוכחה:

אינדוקציה על $n$

בס"ד: הטענה נכונה עבור $n=3$, $n=4$

$f_3 = 2 > \alpha^{3-2} = a = \frac{1+\sqrt{5}}{2}$

$f_4 = 3 > \alpha^{4-2} = \alpha^2 \approx 2.6\dots$

נניח שהטענה נכונה לכל $k$, $3 \leq k \leq n-1$. נראה את הטענה עבור $n$

$f_n = f_{n-1} + f_{n-2} > a^{n-3} + a^{n-4} = a^{n-4}(a+1)$

הנ"ל הנחת האינדוקציה

- $\alpha$ הוא אחד הפתרונות של המשוואה $x^2 - x - 1 = 0$
- כלומר $a^2 - a - 1 = 0$
- כלומר $a+1 = a^2$

$\Rightarrow f_n > a^{n-4} \cdot a^2 = a^{n-2}$

מתקיים

טענה: $f_n < 2^{n-4}$ לכל $n \geq 11$

הוכחה:
אינדוקציה על $n$

בסיס: הטענה נכונה עבור $n=11$ ! $n=12$

$$f_{11} = 89 < 2^{11-4} = 2^7 = 128$$
$$f_{12} = 144 < 2^{12-4} = 2^8 = 256$$

נניח שהטענה נכונה לכל $k$, $11 \leq k \leq n-1$,
נוכיח את הטענה עבור $n$

$$f_n = f_{n-1} + f_{n-2} \underset{\text{הנחת האינדוקציה}}{<} 2^{n-5} + 2^{n-6} = 2^{n-6}(2+1)$$
$$= 2^{n-6} \cdot 3 < 2^{n-6} \cdot 2^2 = 2^{n-4}$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} < f_n < 2^{n-4}$$

## אי שוויון קושי שוורץ

יהיו $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in \mathbb{R}$
אזי $\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right) \cdot \left(\sum_{i=1}^{n} b_i^2\right)$

הוכחה: (אינדוקציה על $n$)

בסיס: $n=1$, $(a_1 \cdot b_1)^2 \leq a_1^2 \cdot b_1^2$

נניח שהטענה נכונה עבור $k$, $1 \leq k \leq n$, נוכיח את הטענה עבור $n+1$

$$\sum_{i=1}^{n} a_i \cdot b_i + a_{n+1} \cdot b_{n+1} \underset{\text{לפי הנחת האינדוקציה}}{\leq} \sqrt{\sum_{i=1}^{n} a_i^2} \cdot \sqrt{\sum_{i=1}^{n} b_i^2} + a_{n+1} \cdot b_{n+1}$$

נסמן $\sqrt{\sum_{i=1}^{n} a_i} = \alpha$, $\sqrt{\sum_{i=1}^{n} b_i} = \beta$

$$\alpha\beta + a_{n+1} \cdot b_{n+1} \leq \sqrt{\alpha^2 + a_{n+1}^2} \cdot \sqrt{\beta^2 + b_{n+1}^2}$$

(לא טעה שלנו עבור $\alpha, a_{n+1}, \beta, b_{n+1}$ הם נכונה גם לי הנחת האינדוקציה.

$$= \alpha\beta + a_{n+1} b_{n+1} \leq \sqrt{a^2 + a_{n+1} +}$$

להשלים.

24/11/15 תורת המספרים - שיעור 6 בס"ד ובהשגחתו

(1)

רוצים להוכיח: משפט יסודי של האריתמטיקה לכל מספר טבעי $n \geq 2$ קיים פירוק יחיד למספרים ראשוניים. לדוגמה: $240 = 2\cdot2\cdot2\cdot2\cdot3\cdot5$

$2^4\cdot3\cdot5$

בכל שני דברים: (1) קיים פירוק - קל. (2) הוא יחיד - קשה

(1) הוכחה שקיים פירוק. באינדוקציה חזקה.

מקרה בסיס: (בבית)

הנחת האינדוקציה: לכל מספר $2 \leq i \leq n-1$, קיים פירוק לראשוניים.

רוצים להוכיח: למספר $n$ קיים פירוק לראשוניים.

שני מקרים: (*) אם $n$ ראשוני - סיימנו. הפירוק הוא $n=n$.

(*) אם $n$ לא ראשוני, אז $n=a\cdot b$ $\quad n>a,b\geq 2$

לפי הנחת האינדוקציה $a=$ ראשוניים, $b=$ ראשוניים

לכן ראשוניים, $n=$ ראשוניים

משפט: אם $n$ לא ראשוני אז יש לו מחלק ראשוני $\leq \sqrt{n}$

הוכחה: $n$ לא ראשוני $\Leftarrow$ $n=a\cdot b$, $a,b\geq 2$

נניח בשלילה ש- $a,b > \sqrt{n}$

אז $a,b > n$ סתירה! לכן אחד מהם הוא $\leq \sqrt{n}$.

אז הוא לא ראשוני. מ.ש.ל.

---

למה: אם $a|bc$ וגם $a,b$ זרים $(\gcd(a,b)=1)$ $\quad a,b,c\in\mathbb{Z}$

אז $a|c$.

הוכחה: קיימים $m,n\in\mathbb{Z}$ כך ש- $ma+nb=1$ (לפי אוקלידס מורחב)

נכפיל שני אגפים ב-$c$: $mac+nbc=c$

מוגדלו $a\cdot x$ לפי ההנחה $a|bc$

$a(\underbrace{mc+nx}_{\text{משהו}})=c$

כלומר $a|c$

מ.ש.ל

(2)

**מסקנה** (מתלמה סמלמוד הקודם): אם $p$ הוא ראשוני ויש $p|ab$ אז $p$ מחלק את $a$ או את $b$.

**הוכחה**: אם $p|a$ אז סיימנו.

אחרת, $p$ זר ל $a$.

אז לפי הלמה $p|b$. משל.

**מסקנה**: אם $p|a_1\cdot(a_2\cdot\ldots\cdot a_k)$

אז $p|a_i$ עבור איזשהו $1\le i\le k$. (הוכחה באינדוקציה על $k$).

---

(2) **משפט**: הפירוק לראשוניים הוא **יחיד**!

**הוכחה**: נניח בשלילה שקיים מספר שיש לו שני פירוקים שונים לראשוניים.

לפי POSW (שלכל קבוצת מספרים טבעיים יש איבר מינימלי).

ניקח את המספר הכי קטן כזה. נקרא לו $n$.

$$n=\underbrace{p_1\cdot p_2\cdot\ldots\cdot p_j}_{\text{ראשוניים}}=\underbrace{q_1\cdot q_2\cdot\ldots\cdot q_k}_{\text{ראשוניים}}$$

כל $p_i$ שונה מכל $q_l$. $1\le i\le j$, $1\le l\le k$.

כי אחרת היינו יכולים לצמצם אותו משני האגפים (נניח $p_1=q_1$)

$$\cancel{p_1}\cdot p_2\cdot\ldots\cdot p_j=\cancel{q_1}\cdot q_2\cdot\ldots\cdot q_k$$

קיבלנו מספר יותר קטן מ-$n$ עם שני פירוקים שונים.

אבל $p_1|q_1\cdot q_2\cdot\ldots\cdot q_k$.

לפי המסקנה $p_1$ מחלק איזשהו $q_l$.

לכן $p_1=q_l$ ← שלנו כבר. אז **סתירה!** משל.

כי אין מצב שראשוני מחלק ראשוני אם הם לא שווים.

(3)

**משפט (אוקלידס): יש אינסוף מספרים ראשוניים.**

**הוכחה:** (אחת מני רבות)

נניח בשלילה שיש n מספרים ראשוניים ושהם $p_1, p_2, \dots, p_n$

נגדיר $a = p_1 p_2 \cdots p_n + 1$

אם a ראשוני ← סתירה. סיימנו.

אם a לא ראשוני אז יש לו פירוק לראשוניים, אבל בכל אופן הוא לא מתחלק בכל אחד מ- $p_1, \dots, p_n$.

אם a היה מתחלק ב- $p_i$.

$$\underbrace{a}_{p_i x} = \underbrace{p_1 \cdot p_2 \cdots p_n}_{\text{נסביר אח"כ}} + 1$$

$$* \quad p_i(x - p_1 p_2 \cdots p_n) = 1$$

לא הגיוני. (כפל של שני מספרים שלמים שווה 1).

**מ.ש.ל**

**מספרים ראשוניים:**
- זוגיים - רק 2
- אי זוגיים $4n+1$ $(\dots, 13, 8)$
- $4n+3$ $(\dots, 11, 7)$

משפט 1: יש אינסוף ראשוניים מהצורה $4n+1$ ← יותר קשה. לא נוכיח עכשיו.

משפט 2: יש אינסוף ראשוניים מהצורה $4n+3$ ← נוכיח עכשיו.

(אבל, לא כל המס' מהצורה הזאת ראשוניים לדוגמא: $4 \cdot 22 + 3 = 91 = 7 \cdot 13$)

**הוכחת משפט 2** **לעזרה:** אם a,b הם מהצורה $4n+1$.

אז גם $a \cdot b$ הוא מאותה הצורה.

**הוכחה:** $a = 4m+1 \quad b = 4n+1$

$$a \cdot b = 16mn + 4m + 4n + 1$$

$$= 4(\underbrace{4mn + m + n}_{\text{משתנה}}) + 1$$

**מ.ש.ל** לעזרה.

## הוכחת משפט 2

נניח בשלילה ש- $p_1, p_2, \dots, p_k$ . הם כל המספרים הראשוניים מהצורה $4n+3$ שיש.

נגדיר $a = 4 \cdot p_1 \cdot p_2 \cdots p_k - 1$ (נשים לב ש-$a$ הוא מהצורה $4n+3$)

לדוגמה: $79 = 4 \cdot 20 - 1 = 4 \cdot 19 + 3$ .

ל-$a$ יש פירוק לראשוניים. הראשוניים בפירוק הם לא כולם מהצורה $4n+1$ .

$a = q_1^{4n+1} \cdot q_2^{4n+3} \cdots q_l$ (כי אם $a$ היה מהצורה $4n+1$, אפשר הלימה)

=> לפחות אחד מהראשוניים בפירוק של $a$ הוא ברשימה $p_1, \dots, p_k$ .

לא ייתכן כי $a+1$ מתחלק ב $p_i$ (הסברת אגפים $a = 4 \cdot p_1 \cdot p_2 \cdots p_k - 1$, $a+1 = 4 p_1 p_2 \cdots p_k$)

לכן $a$ עצמו לא מתחלק ב-$p_i$. סתירה. מ.ש.ל

---

**משפט:** קיימים רצפים בכל האורכים של מספרים לא ראשוניים.

לדוגמא: $24, 25, 26, 27, 28$, רצף באורך 5.

**הוכחה:** הנה רצף באורך $n-1$ :

$$\underbrace{n!+2}_{\text{מתחלק ב-2}}, \underbrace{n!+3}_{\text{מתחלק ב-3}}, \underbrace{n!+4}_{\text{מתחלק ב-4}}, \dots, \underbrace{n!+n}_{\text{מתחלק ב-n}}$$

תזכורת: $n! = n(n-1)(n-2) \cdots 2 \cdot 1$

"n עצרת": $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$

מ.ש.ל

---

**משפט:** נסמן את המספרים הראשוניים $\underset{2}{p_1}, \underset{3}{p_2}, \underset{5}{p_3}, \underset{7}{p_4}, \dots$

**טענה:** $p_n \le 2^{2^n}$

טענה שאוכיחים בתרגול: $(p_{n+1})^2 \le p_1 \cdot p_2 \cdots p_n$ $(n \ge 5)$

**משפט:** (Bertrand) (לא נוכיח) אבל נשתמש כדי להוכיח את המשפט.

לכל $n$ קיים לפחות מספר ראשוני אחד בין $n$ לבין $2n$ .

מסקנה (לתרגיל): $p_n \le 2^n$

**משפט:** (Dirichlet) (לא נוכיח)

לכל $a, b$ זרים יש אינסוף ראשוניים $an+b$ . לדוג: $4n+1$, $4n+3$, $7n+9$, $20n+13$ .

**השערות:**

1) יש אינסוף תאומות של ראשוניים ראשונים. לדוג: $(11,13), (17,19), (p, p+2)$

2) (Goldbach) כל מספר זוגי הוא סכום של שני ראשוניים. $20 = 13+7$, $22 = 11+11 = 17+5$

3) יש אינסוף ראשוניים מהצורה $n^2+1$ .

24/11/15

**משפט:** קיים מספר אינסופי של מספרים ראשוניים.

**הוכחה:** נבנה סדרת מספרים $\mathbb{Z}^+$: $n_1=2,\ n_2=n_1+1,\ n_3=n_1\cdot n_2+1,\ n_4=n_1n_2n_3+1,\ \dots,\ n_k=n_1\cdots n_{k-1}+1$

$2,3,7,43,\dots$

כל $n_k$, $n_k>1$, מתחלק בלפחות מספר אחד ראשוני.

לא יתכן שלשני $n_k$ יש אותו מחלק ראשוני. (כלומר כל שאין גורם שלשני מספרים מה-n שהם גדול מ 1).

נסמן $d=\gcd(n_i,n_k)_{i<k}$

$d\mid n_i \Rightarrow d\mid n_1\cdot n_2\cdots n_i\cdots n_{k-1}$

$d\mid n_k$

$(a\mid -b \Leftrightarrow a\mid b)$ (לבדוק)

**משפט:** יהיו $a,b,c\in\mathbb{Z}$. אם $a\mid b$ ו- $a\mid c$ אז $a\mid(b\pm c)$

$\Leftarrow d\mid n_k-n_1\cdot n_2\cdots n_{k-1}$

$\Leftarrow d\mid 1$ (כי $n_k=n_1n_2n_3\cdots n_{k-1}+1$)

$\Leftarrow d=1$ (השפרות אגפים: $n_k-n_1n_2n_3\cdots n_{k-1}=1$)

$n_k$ זרים בעזרות. לכל $n_k$ יש מחלק ראשוני.

מיפוי: כמו שקיים אינסוף מספרים טבעיים $\mathbb{Z}^+$ קיים אינסוף מספרים ראשוניים.

מסכנה למשפט הבא:

אם $p_n$-מספר $n$ ראשוני. $p_{n+1}<p_1p_2\cdots p_n+1$ (לדוגמא: $p_5<2\cdot3\cdot5\cdot7+1=210$, $p_5=11$)

**משפט 2:** (Bonse's inequality) 1907 בשנת: $(p_{n+1})^2<p_1p_2\cdots p_n$, $n\geq5$

**הוכחה:** נגדיר: $x\geq5$ (שלם)

(הקשר היותר שמקיים את הראשוניות)
$$\begin{cases} r_x\geq4 & \text{מה ראשוני} \\ x-r_x+1\leq p_{r_x} \end{cases}$$

$s\in\{1,2,\dots,p_{r_x}\}$

$N_s=(s\cdot p_1\cdot p_2\cdots p_{r_x-1})-1$

**למה (2.3):** לכל מספר שלם $x\geq5$ קיים $j\in[1,p_{r_x}]$ כך שלכל $i\in[1,x]$ $p_i\nmid N_j$ (לא מחלק)

ההוכחה באתר של הקורס.

שיעור 7

# יחסי שקילות מודולו Congruences

**הגדרה 1:** $a,b\in\mathbb{Z}$ , $m\in\mathbb{Z}^+$

אם $a$ ו $b$ יש לו שארית כאשר מחלקים ב $m$ שקול ל $a$ מודולו $m$.

$a\equiv b \pmod m$ אם $a \bmod m = b \bmod m$.

דוגמא: $a=17$, $b=38$, $m=7$ $\quad a \bmod m=3$, $b \bmod m=?$

לכן $17\equiv 38 \pmod 7$

**הגדרה ב:**

אומרים $a\equiv b \pmod m$ אם $m \mid a-b$.

דוגמא $17-38=-21$ , $7\mid(-21)$

**משפט:** שתי ההגדרות הן שקולות.

**הוכחה:** אם נניח ש $a=b \pmod m$ לפי הגדרה 1.

נראה $a=b \pmod m$ לפי הגדרה ב.

**נתון:** $a \bmod m=r$, $b \bmod m=r$

I $a=x\cdot m+r$ $\quad$ II $b=y\cdot m+r$ $\quad$ I - II $\Rightarrow a-b=(x-y)m$

$m\mid a-b \Leftarrow$ מ.ש.ל (1)

ב. נניח ש $a=b \pmod m$ לפי הגדרה ב. } **תרגיל**

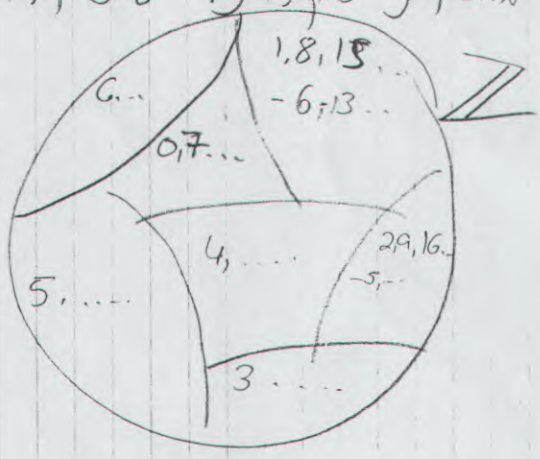
נראה $a=b \pmod m$ לפי הגדרה 1.

**משפט:** יחס השקילות מודולו $m$ הוא בעל יחס שקילות כלומר הוא:

* רפלקסיבי - $a\equiv a \pmod m$ לכל $a$.
* סימטרי - אם $a\equiv b \pmod m$ אז $b\equiv a \pmod m$
* טרנזיטיבי - אם $a\equiv b \pmod m$ ו $b\equiv c \pmod m$ אז $a\equiv c \pmod m$

מחלקת שקילות:

דוגמא: מחלקת שקילות. לשקילות מודולו 7




בלוקן כללי - לשקילות מודולו m יש m מחלקות שקילות.

הגדרה: קבוצה של m מס' אחד מכל יחס שקילות מודולו m נקראת מערכת שלמה מודולו m

(Complete System of residues modulo m)

דוגמאות למערכת שלמה מודולו 7:

א. $\{0,1,2,3,4,5,6\}$ ← קנונית.

ב. $\{14,1,-5,-11,74,705,-17\}$

משפט: אם $a \equiv b \pmod m$ וגם $c \equiv d \pmod m$

אז גם:

1. $a+c \equiv b+d \pmod m$
2. $a-c \equiv b-d \pmod m$
3. $a \cdot c \equiv b \cdot d \pmod m$

דוגמא: $13 \equiv -22 \pmod 7$, $3 \equiv 24 \pmod 7$

תיקון - $-10 \equiv 46 \pmod 7$ , תיקון - $16 \equiv 2 \pmod 7$

$39 \equiv -528 \pmod 7$

הוכחה של ג: (עפ"י הגדרה ב)

נתון $m|(a-b)$ , $m|(c-d)$ $(a-b=xm,\ c-d=ym)$

צ"ל $m|(ac-bd)$

$ac-bd \Rightarrow (xm+b)(ym+d)-bd$

$a=xm+b \quad c=ym+d$

$xym^2+xmd+bym+bd-bd = m(\overbrace{xym+xd+by}^{\text{משהו}})=ac-bd$

$m|(ac-bd)$ . ש.ל.מ

מסקנה מ-ג: אם $a\equiv b \pmod m$

אז $a^k\equiv b^k \pmod m$ לכל $k\in\mathbb{N}$

סקיצה של הוכחה: $k\begin{cases} a\equiv b \\ a\equiv b \\ a\equiv b \end{cases}$

$a\cdot a\cdot a\equiv b\cdot b\cdot b$

לפעמים אסור לצמצם:

אם $ac\equiv bc \pmod m$

אז לא בהכרחית: $a\equiv b \pmod m$

דוגמא: $14\equiv 8 \pmod 6$ $\xleftarrow{\text{נחלק ב-2}}$ $7\overset{?}{\equiv}4 \pmod 6$ לא.

מתי מותר לצמצם, ואיך:

משפט: נניח ש- $ac\equiv bc \pmod m$ ונסמן $d=\gcd(c,m)$

אז $a\equiv b \pmod{\frac{m}{d}}$ עפ"י

הוכחה: נתון: $m|(ac-bc) \rightarrow ac-bc=mx$

$d=\gcd(c,m) \rightarrow c=yd \quad m=zd$

$\gcd(z,y)=1$ (אחרת היה מחלק משותף יותר גדול מ-d)

$ayd-byd=zdx \rightarrow (a-b)y=zx \Rightarrow z|(a-b)y$

{תזכורת: אם $h|jk$ ו- $\gcd(j,k)=1$ אז $h|k$}

במקרה שלנו: $z|(a-b) \Rightarrow a\equiv b \pmod{\underset{\frac{m}{d}}{z}}$

ש.ל.מ

**מסקנות:**

① אם $ac \equiv bc \pmod m$
ואם $\gcd(c,m)=1$
אז $a \equiv b \pmod m$

דוגמא: $6 \equiv 36 \pmod{10}$, $2 \equiv 12 \pmod{10}$

② אם $ac \equiv bc \pmod p$ ($p$ ראשוני)
ואם $p \nmid c$
אז $a \equiv b \pmod p$

**בעיה:** מצא $x$ כך ש $9x \equiv 12 \pmod{15}$ **פתרון:** $x=3$, $x=18$

לאיזו פתרון כ $3 \equiv 18 \pmod{15}$

**בעיה כללית:**

מצא $x$ כך ש $ax \equiv b \pmod m$ $[a,b,m$ מספרים נתונים$]$.

**למה:**
אם $x_1$ הוא פתרון ואם $x_1 \equiv x_2 \pmod m$
אז גם $x_2$ הוא פתרון.

**הוכחה:** נתון $ax_1 \equiv b \pmod m \leftarrow m \mid ax_1 - b \leftarrow ax_1 - b = my_1$

צ"ל: $ax_2 \equiv b \pmod m$

נתון $x_2 \equiv x_1 \pmod m \leftarrow x_2 - x_1 = zm \leftarrow x_1 = x_2 - zm$

$\Rightarrow a(x_2 - zm) - b = my_1 = ax_2 - b = m(y_1 + az)$

$m \mid ax_2 - b \Rightarrow ax_2 \equiv b \pmod m$ (נ.ש.ל)

נמצא לינארי פתרונות לכל שקילות ראשית כי לדוגמא $9x \equiv 12 \pmod{15}$

תשובה לשאלה:
① פתרון ל: $x=3$ $(3, 18, 33 \ldots)$
② פתרון ב: $x=8$ $(8, 23, 38 \ldots)$
③ פתרון ג: $x=13$ (או $y=-2$) $(13, 28, 43 \ldots)$

**משפט:** נתונה משוואה $ax \equiv b \pmod m$

כאשר $x$ הוא הנעלם! $a, b, m$ הם מס' נתונים.

נסמן $d = \gcd(a, m)$ אז:

(1) אם $d \nmid b$ אין פתרון.

(2) אם $d \mid b$ אז יש $d$ פתרונות שונים מודולו $m$.

**הוכחה:** נרצה $x$ כך ש $m \mid (ax-b)$

לומר נרצה $x, y$ כך ש $ax - b = m(-y) \Leftarrow ax + my = b$

**תזכורת:** למשוואה $js + kt = c$ ($s, t$ שלמים)

יש פתרון אם ורק אם $d \mid c$ כאשר $d = \gcd(j, k)$

במקרה שיש פתרון, הפתרון הכללי הוא $s = s_0 + \left(\frac{k}{d}\right)r$, $t = t_0 - \left(\frac{j}{d}\right)r$ לכל $r \in \mathbb{Z}$

**דוגמא:**

$45 + 10t = 6 \xrightarrow{\text{אוקלידס}} 45 + 10t = 2 \Leftarrow s = -2, t = 1$

$-24 + 30 = 6$ $\boxed{s_0 = -6, t_0 = 3}$ כבר יודעים

**הפתרון הכללי:** $\begin{cases} s = -6 + 5r \\ t = 3 - 2r \end{cases}$ $r$ - כל מס' שלמים נרצה.

נסמן $d = \gcd(a, m)$

**הפתרון הכללי:** $\begin{cases} x = x_0 + \left(\frac{m}{d}\right) \cdot r \\ y = y_0 - \left(\frac{m}{d}\right) \cdot r \end{cases}$ לכל $r \in \mathbb{Z}$ כאשר $r$ הוא פתרון שמצאנו $(x_0, y_0)$ ע"י אוקלידס.