משפט החלוקה

משפט החלוקה:
אם a ו-b שלמים כך ש- $b>0$, אז קיימים: q ו– $0\le r<b$ שלמים יחידים כך ש $a=bq+r$.

דוגמה: (נעשתה בהרצאה)
יהי a שלם. אזי $3|a^3-a$.

כדי לראות זאת, קודם נשים לב כי מתקיים:
$$a^3-a=a(a^2-1)=(a-1)a(a+1)$$

לפי משפט החלוקה, קיים $k\in\mathbb{Z}$ כך ש:
$$a=3k \quad \text{או} \quad a=3k+1 \quad \text{או} \quad a=3k+2.$$

נבדוק את כל שלושת המקרים :

1. אם $a=3k$: אז
$$a^3-a=a(a^2-1)=3k(a^2-1)$$
מתחלק ב-3.

2. אם $a=3k+1$: אז $a-1=3k$ ולכן
$$a^3-a=a(a-1)(a+1)=a\cdot 3k\cdot(a+1)$$
מתחלק ב-3.

3. אם $a=3k+2$: אז $a+1=3k+3=3(k+1)$ ולכן
$$a^3-a=a(a-1)(a+1)=a(a-1)\cdot 3\cdot(k+1)$$
מתחלק ב-3.

באופן דומה ניתן להסיק את הטענה הבאה.

<u>טענה</u>:
יהי $b \in \mathbb{N}$. מבין כל b שלמים עוקבים, לפחות אחד מהם כפולה של b.

<u>תרגיל</u>:
הוכיחו כי המכפלה של כל שלושה מספרים שלמים עוקבים מתחלקת ב-6.

<u>פתרון</u>:
יהי $n \in \mathbb{Z}$. נראה כי מתקיים $6|(n-1)\cdot n\cdot(n+1)$.

<u>תזכורת</u>: אם $n_1,..,n_r$ טבעיים זרים בזוגות, m טבעי ו- $n_i|m$ לכל $1 \le i \le r$ אז $n_1\cdot..\cdot n_r|m$. (בהרצאה הוכחנו את זה עבור $r=2$, ואנחנו גם עומדים להשתמש בתזכורת הזו רק במקרה של $r=2$. יחד עם זאת, התזכורת אכן נכונה גם לכל r טבעי וניתן להוכיח זאת באינדוקציה, תוך שימוש במקרה $r=2$ שהוכח בהרצאה.)

מכיוון ש- $2,3$ זרים, לפי התזכורת, די שנראה כי $2|(n-1)\cdot n\cdot(n+1)$ וכי $3|(n-1)\cdot n\cdot(n+1)$.

אם n זוגי: אזי $2|(n-1)\cdot n\cdot(n+1)$ כי $2|n$
אחרת (n אי זוגי): אז $2|n+1$ וגם $2|n-1$ ומכאן $2|(n-1)n(n+1)$.
לגבי $3|(n-1)\cdot n\cdot(n+1)$: נשתמש בדוגמה מהעמוד הקודם שהוכחה בהרצאה, בה הראינו כי מכפלת כל שלושה שלמים עוקבים מתחלקת ב-3. לכן $3|(n-1)\cdot n\cdot(n+1)$.

קיבלנו כי גם 2 וגם 3 מחלקים את $(n-1)\cdot n\cdot(n+1)$. לכן מהתזכורת נובע ש 6 גם מחלק את המכפלה הזו.

<u>תרגיל</u>:
הוכיחו כי אם a,b ו- c שלמים שונים מ 0 אזי: $a|b \leftrightarrow ac|bc$.

<u>הוכחה</u>:
<u>כיוון א</u>: נתון $a|b$ צ"ל $ac|bc$.
<u>הוכחה</u>: $a|b \leftarrow$ קיים $k \in \mathbb{Z}$ כך ש - $b=ak$ לכן $bc=ack$ ונובע $ac|bc$.

<u>כיוון ב:</u> נתון $ac|bc$ צ"ל $a|b$.

<u>הוכחה:</u> $ac|bc$ ולכן קיים $k\in\mathbb{Z}$ כך ש $bc=kac$. לכן $b=ka$ ונובע כי $a|b$.

<u>תרגיל:</u>
יהיו a ו- b שלמים חיוביים אי-זוגיים המקיימים $b\nmid a$. הראו שקיימים שלמים q ו- p כך ש $a=bq+p$ כאשר p אי זוגי המקיים $|p|<b$.

<u>אינטואיציה :</u>

נתבונן בדוגמא $a=23, b=3$ ונקבל $23=3\cdot 7+2$ כלומר, קיבלנו לצערנו שארית זוגית במקום שארית אי זוגית. איך נתחכם כדי לקבל p זוגי? נהפוך את ה 7 ל 8 ואז ה"שארית" תהיה **שלילית ואי זוגית** $23=3*8+(-1)$.

<u>הוכחה</u>

על פי משפט החלוקה, ניתן לכתוב $a=bs+t$, כאשר s ו- t שלמים וגם $0\le t<b$.

מההנחה ש– $b\nmid a$ נובע ש $t>0$. נשים לב:

אם t **אי-זוגי**, אז סיימנו. שכן נוכל לקחת $q=s$ ו- $p=t$.

נניח אם כן ש- t **זוגי** מכך ש- $t<b$ ומההנחה ש- b אי-זוגי,
מתקיים ש - $t-b$ אי-זוגי ושלילי.
ניתן לכתוב : (שימו לב שזה בדיוק מה שעשינו באינטואיציה דלעיל...)

$$a=bs+t=(bs+b)+(t-b)=b(s+1)+(t-b)$$

כעת נגדיר $p=t-b, q=s+1$

עלינו להראות כי : $|p|=|t-b|<b$. אכן, $t-b$ שלילי ולכן : $|t-b|=b-t$
ומכיוון ש- $t>0$ נובע כי $|p|=b-t<b$..

(כאן השתמשנו בכך ש=$|x|=\begin{cases}x, & if\ x\ge 0\\ -x & if\ x<0\end{cases}$**. זו פשוט ההגדרה של ערך מוחלט.)**

<u>תרגיל</u>
יהיו $1 \leq b < a$ שלמים. הוכיחו כי מתקיים $a\ mod\ b < \frac{a}{2}$.

<u>הערה:</u> $a\ mod\ b$ מסמן את שארית החלוקה של a ב- b.
ניתן שתי הוכחות שונות.

<u>הוכחה 1</u>
נכתוב $a = bk + r$ כאשר $0 \leq r < b$, על פי משפט החלוקה.
כלומר $r = a\ mod\ b$
נניח בשלילה ש - $r \geq \frac{a}{2}$, מכיוון ש- $r = a - bk$ נובע כי $a - bk \geq \frac{a}{2}$.
כלומר $2a - 2bk \geq a$ ולכן $a \geq 2bk$. לכן מתקיים $bk + r = a \geq 2bk$..
כלומר קיבלנו $r \geq bk$ ומכיוון ש$k \geq 1$ קבלנו $r \geq b$ בסתירה לכך ש- $r < b$.

<u>הוכחה 2</u>
נכתוב $a = bk + r$, כאשר $0 \leq r < b$ שלם. על פי משפט החלוקה, נחלק לשני מקרים:
מקרה ראשון : $b \leq \frac{a}{2}$.
מקרה שני: $b > \frac{a}{2}$.
במקרה הראשון מתקיים : $r \leq b - 1 \leq \frac{a}{2} - 1 < \frac{a}{2}$ ולכן סיימנו.
במקרה השני, אנו מחלקים את a במספר הגדול מ- $a/2$. אך קטן מ-a.
לכן $k = 1$ ונובע $a = b + r$. לכן $r = a - b$ ונובע $r < a/2$ (מכיוון ש $b > \frac{a}{2}$). קיבלנו כי $r = (a\ mod\ b) < \frac{a}{2}$. כנדרש.

<u>תרגילי בית</u>:
<u>שאלה 1</u>:

א. הוכיחו כל מספר ריבועי (כלומר מספר שניתן להצגה כריבוע של מספר טבעי m) הוא מהצורה $4k$ או $4k+1$.

<u>הוכחה</u>: אם המספר m הוא זוגי : אזי הוא מהצורה $m=2j$ אם נעלה אותו בריבוע : $m^2=(2j)^2=4j^2$ וקיבלנו מספר מהצורה $4k$.
אם המספר m הוא אי זוגי : אזי הוא מהצורה $m=2j+1$ אם נעלה אותו בריבוע : $(2j+1)^2=4j^2+4j+1=4(j^2+j)+1$ נקבל מספר מהצורה $4k+1$.

ב. הסיקו מסעיף א' כי אף אחד מהמספרים הבאים אינו ריבועי
:11,111,1111,11111...

<u>הוכחה:</u> הסדרה הנ"ל מוגדרת ע"י הנוסחה הבאה:

$$a_1=11$$
$$a_n=4\cdot 25\cdot 10^{n-2}+a_{n-1}\qquad \forall n\geq 2$$

נראה באינדוקציה כי כל אברי הסדרה הם מהצורה $4k+3$ ולכן לפי הסעיף הקודם אף אחד מהם אינו ריבוע.

בדיקה עבור $n=1$: האיבר הראשון a_1 אינו מהצורה $4k+1$ אלא הוא מהצורה $4\cdot 2+3$.
נניח כי עבור n כלשהו, a_n הוא מהצורה $a_n=4k+3$.
עלינו להוכיח כי a_{n+1} הוא מהצורה $4k'+3$. (כמובן $k'\neq k$).
אכן,

$$a_{n+1}=4\cdot 25\cdot 10^{n-1}+a_n=4\cdot\ 25\cdot 10^{n-1}+(4k+3)=$$
$$=4\cdot(25\cdot 10^{n-1}+k)+3=4k'+3$$

כאשר השוויון השני משמאל משתמש בהנחת האינדוקציה.

קבלנו כי כל אברי הסדרה הם מהצורה $4k+3$ ולכן לפי הסעיף הקודם אף אחד מהם אינו ריבועי.