תזכורת

שדה

1. יש שתי פעולות - חיבור וכפל.
2. שדה סגורה ביחס לחיבור וכפל.
3. החיבור והכפל קיבוציים בשדה
4. יש איבר ניטרלי לחיבור ויש איבר ניטרלי לכפל
5. החיבור והכפל חילופיים בשדה
6. חוק הפילוג מקשר בין החיבור לכפל.

מספרים טבעיים - חלק 1: מבוא לתורת המספרים

הגדרה

יהי $a \in \mathbb{N}$. נאמר כי $b \in \mathbb{N}$ מחלק את a אם קיים $c \in \mathbb{N}$ כך ש $a = b \cdot c$.

נסמן $b | a$.

תרגיל

יהיו $a,b,c\in\mathbb{Z}$,

הוכיחו את הפריט:

① אם $a|b$ וגם $a|c$ אז $a|b+c$.

תשובה

נ"ח $a|b$ וגם $a|c$.

$a|b$ ולכן קיים $d\in\mathbb{Z}$ כך ש $b=a\cdot d$

$a|c$ ולכן קיים $e\in\mathbb{Z}$ כך ש $c=a\cdot e$

נתבונן ב $d+e$,

$d,e\in A$ ו A סגורה לחיבור. לכן $d+e\in A$.

כמו כן:

$$a\cdot(d+e)=a\cdot d+a\cdot e=b+c$$

לכן $a|b+c$.

מש"ל.

2. אם $a|c$ וגם $b|c$ אז $a+b|c$.

<u>תשובה</u>

נבחון את 12, 4, 6.

$6|12$ וגם $4|12$ וגם $10\nmid 12$.

לכן הטענה אינה נכונה.

3. $a|a$ (רפלקסיביות יחס החלוקה)

<u>תשובה</u>

נתון a ב-$\mathbb{Z}$.

$1 \in \mathbb{Z}$ וגם $a = a \cdot 1$

ולכן $a|a$.

4. אם $a|b$ וגם $b|a$ אז $a=b$.

(אנטיסימטריות יחס החלוקה)

<u>תשובה</u>

נניח $a|b$ וגם $b|a$.

$a|b$ ולכן קיים $d\in\mathbb{N}$ כך ש $b=a\cdot d$.

$d\in\mathbb{N}$ ולכן $1\geq d$. נכפול את שני האגפים

ב a (שהוא חיובי) ונקבל $ad\geq a$ כלומר $b\geq a$.

באופן דומה $a\geq b$ ולכן $a=b$.

מש"ל.

5. אם $a|b$ וגם $b|c$ אז $a|c$.

(טרנזיטיביות יחס החלוקה)

<u>תשובה</u>

נניח $a|b$ וגם $b|c$.

$a|b$ ולכן קיים $d\in\mathbb{N}$ כך ש $b=ad$.

$b|c$ ולכן קיים $e\in\mathbb{N}$ כך ש $c=b\cdot e$.

נתבונן ב $e\cdot d$.

$d,e\in\mathbb{N}$ מסגירות לכפל $de\in\mathbb{N}$.

כמו כן: $a\cdot(de)=(ad)e=be=c$

ולכן $c|a$.

מש"ל.

6. אם $c|a$ וגם $c|b$ אז $c|a\cdot b$.

<u>תשובה</u>

נתבונן ב $12, 6, 4$.

$12|4$ וגם $12|6$ וגם $12 \nmid 24$.

לכן הטענה איננה נכונה.

מש"ל.

7. אם $a|c$ וגם $b|c$ וגם a,b ראשוניים

אז $ab|c$.

תשובה

נתבונן ב $a=b=c=7$.

$7|7$ וגם 7 ראשוני וגם $49 \nmid 7$.

לכן הטענה אינה נכונה

מש"ל.

הגדרה

$p \in \mathbb{N}$ "נקרא ראשוני" אם:

1. p אינו הפיך ביחס לכפל.
2. לכל $q \in \mathbb{N}$. אם $q|p$ אז קיים $u \in \mathbb{N}$ הפיך ביחס לכפל כך ש $q = u \cdot p$ או $q = u \cdot 1$.

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$

משפט החלוקה בשארית

43, 9

$$43 = 4 \cdot 9 + 7$$

$$(43, 9) \longrightarrow (4, 7)$$

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}_0 \times \mathbb{N}_0$$

משפט

מחלק

מחולק   מנה

יהיו $a,b\in\mathbb{N}$. אזי קיים $q\in\mathbb{N}_0$ יחיד

שארית

וקיים $r\in\mathbb{N}_0$ יחיד כך ש:

1. $a=q\cdot b+r$
2. $0\leq r<b$

תרגיל

הוכיחו או הפריכו:

קיימים טבעיים $m,n,k\in\mathbb{N}$ כך ש:

$$21m+49n+23=35k+18$$

תשובה

יהיו $m,n,k\in\mathbb{N}$.

$$35k+18=7\cdot(5k+2)+4$$

$$21m+49n+23=7(3m+7n+3)+2$$

מיחידות ההצגה של $35k+18$ כחלוקה עם שארית ב-7

נובע כי שארית החלוקה של $35k+18$ ב-7 היא 4 ובפרט

אינה 2 ולכן

$$35k+18 \neq 7(3m+7n+3)+2$$

כלומר

$$35k+18 \neq 21m+49n+23.$$

לכן הטענה אינה נכונה.

מש"ל.

תרגיל

תהיו G קבוצה ותהא $*$ פעולה בינארית על G.

נתון: 1. G סגורה ביחס ל $*$.

2. $*$ קיבוצית ב G.

3. קיים $e\in G$ ניטרלי ביחס ל $*$.

יהי $a\in G$, ויהי $n\in\mathbb{N}$.

נסמן $$a^n=\underbrace{a*a*\dots*a}_{n \text{ פעמים}}.$$

יהי $n_0 \in \mathbb{N}$ הטבעי המינימלי כך ש $a^{n_0}=e$.

ג. הראו כי לכל $m \in \mathbb{N}$.

אם $n_0 | m$ אז $a^m = e$.

<u>תשובה</u>

יהי $m \in \mathbb{N}$,

נ.ח $n_0 | m$.

$a^{mn} = (a^m)^n$
באינדוקציה

לכן קיים $z \in \mathbb{N}$ כך ש $m = n_0 \cdot z$.

$$a^m = \underbrace{\underbrace{(a * a * \dots * a)}_{n_0 \text{ פעמים}} * \underbrace{(a * a * \dots * a)}_{n_0 \text{ פעמים}} * \dots * \underbrace{(a * a * \dots * a)}_{n_0 \text{ פעמים}}}_{z \text{ פעמים}}$$

מהנתון: $\underbrace{a*a*\dots*a}_{m \text{ פעמים}} = e$ לכן:

$$a^m = \underbrace{e*e*e*\dots*e}_{m \text{ פעמים}} = e$$

(הוכחה באינדוקציה)

עבשים

2. הראו כי לכל $m \in \mathbb{N}$. אם $a^m = e$ אז $n_0 | m$.

תשובה

יהי $m \in \mathbb{N}$.

נניח $a^m = e$.

ממשפט החלוקה בשארית, קיימים $x, y \in \mathbb{N}$ יחידים כך ש:

$$m = n_0 x + y$$

וגם

$$0 \le y < n_0$$

נניח בשלילה ש $y \neq 0$. לכן $0 < y < n_0$.

מה הנחה:

$$e = a^{n_0 x + y} = \underbrace{(a * a * \dots * a)}_{n_0 x \text{ פעמים}} * \underbrace{(a * a * \dots * a)}_{y \text{ פעמים.}} =$$

$$= a^{n_0 x} * a^{y}$$

מהסעיף הקודם $e = a^{n_0 x}$.

ונקבל:

$$e = e * a^{y} = a^{y}.$$

$y < n_0$ יתבע בסתירה לכך ש n_0 הוא הטבעי המינימלי.

המקיים $a^{n_0} = e$.

לכן $y = 0$ ומכאן $m = n_0 x$ ולכן

$m \mid n_0$.

מש״ל.

תרגיל

הראו כי לכל $n \in \mathbb{N}$. שארית החלוקה של n^2 ב 3 אינה 2.

תשובה

יהי $n \in \mathbb{N}$.

אז קיימים $q, r \in \mathbb{N}_0$ יחידים כך ש

$$n = 3q + r$$

וגם

$$0 \leq r < 3$$

מקרה 1: $r=0$

נובע: $n^2=(3q)^2=9q^2=3(3q^2)+0$

לכן מיחידות ההצגה של n^2 כחלוקה ב 3 עם שארית
נובע כי שארית החלוקה של n^2 ב 3 היא 0 ובפרט
אינה 2.

מקרה 2: $r=1$

נובע: $n^2=(3q+1)^2=9q^2+6q+1=3(3q^2+2q)+1$

מיחידות ההצגה של n^2 כחלוקה ב 3 עם שארית נובע
כי שארית החלוקה של n^2 ב 3 היא 1 ובפרט אינה 2.

מקרה 3 : $r=2$

נובע:

$$n^2=(3q+2)^2=9q^2+12q+4=3(3q^2+4q+1)+1$$

מיחידות ההצגה של n^2 כחלוקה ב 3 עם שארית

נובע כי שארית החלוקה של n^2 ב 3 היא 1 ובפרט

שונה 2.

מש"ל

המשפט היסודי של האריתמטיקה

$$
\begin{array}{r|l}
1485 & 3 \\
495 & 3 \\
165 & 3 \\
55 & 5 \\
11 & 11 \\
1 & =
\end{array}
$$

$$1485 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 11$$

$$= 3^3 \cdot 5 \cdot 11$$

משפט

לכל טבעי השונה מ 1 קיימת הצגה כמכפלת ראשוניים.

הצגה זו יחידה עד כדי סדר הגורמים הראשוניים.

$$6 = 2 \cdot 3 = 3 \cdot 2$$

מבחינתי זו אותה הצגה.

תרגיל

יהי $n \in \mathbb{N}$.

הוכיחו או הפריכו:

1. אם $12 | n^2$ אז $12 | n$.

תשובה

נתבונן ב 6.

$12 | 36$ אבל $12 \nmid 6$.

לכן הטענה אינה נכונה.

מ.ש.ל.

2. אם $15|n^2$ אז $15|n$.

<u>תשובה</u>

נניח $15|n^2$.

אז $n^2\neq 1$ ולכן $n\neq 1$.

אז קיימים $p_1,p_2,\dots,p_k\in\mathbb{N}$ ראשוניים כך ש

$$n=p_1\cdot p_2\cdot\ldots\cdot p_k$$

ולכן מחוקי חזקה:

$$(*)\qquad n^2=p_1p_1p_2p_2\cdot\ldots\cdot p_kp_k$$

$15 | n^2$ לכן קיים $a\in\mathbb{N}$ כך ש $n^2=15a$

$n^2\neq 15$ לכן $a\neq 1$.

לכן קיימים $q_1,q_2,\dots,q_m\in\mathbb{N}$ ראשוניים כך ש

(**) $$n^2=3\cdot 5\cdot q_1\cdot q_2\cdot\ldots\cdot q_m$$

מיחידות ההצגה כמכפלת ראשוניים נובע שהצגת (*)

ו-(**) זהות עד כדי סדר.

ללא הגבלת כלליות

$p_1=3$

$p_2=5$

לכן $n = 3\cdot 5\cdot p_3\cdot\ldots\cdot p_k$; $n = 15\cdot(p_3\cdot\ldots\cdot p_k)$.

ומכאן $15 \mid n$.

מש"ל.

תרגיל

הראו כי לכל $x \in \mathbb{Q}$. $x^2 \neq 15$.

תשובה

יהי $x \in \mathbb{Q}$.

נניח בשלילה ש $x^2 = 15$.

$x \in \mathbb{Q}$ לכן קיימים $m \in \mathbb{Z}$, $n \in \mathbb{N}$ כך ש $x = \frac{m}{n}$.

$x^2 \neq 0$ לכן $x \neq 0$.

ללא הגבלת הכלליות $x > 0$ (אחרת נתבונן ב $-x$
$(-x)^2 = 15$)

$x>0$ גם $n>0$ לכן $m>0$ לכן גם $m\in\mathbb{N}$.

ללא הגבלת כלליות $\frac{m}{n}$ שבר מצומצם

(אחרת נצמצם).

מההנחה: $x^2=15$

לכן: $\left(\frac{m}{n}\right)^2=15$

ולכן: $\frac{m^2}{n^2}=15$ מכאן $m^2=15n^2$.

לכן $15|m^2$.

מהוכחה קודמת נובע כי $15|m$. (1)

לכן קיים $k\in\mathbb{N}$ כך ש $m=15k$.

כעת: $m^2=15n^2$

$$(15k)^2=15n^2$$

$$225k^2=15n^2 \quad /:15$$

$$15k^2=n^2$$

לכן $15|n^2$ ולכן מתרגיל קודם $15|n$. (2)

(1) ו (2) עומדים בסתירה להנחה שהשבר מצומצם.

לכן $x^2 \neq 15$.

מש"ל.

לשבוע הבא

יחידה 12 - לחזור.

* קבוצות יוצרים.
* אינדוקציה.