

מבוא לתורת המספרים האלמנטרית

תורת המספרים האלמנטרית עוסקת במספרים שלמים, \mathbb{Z} .

הגדרה

a מחלק את b , ומסמנים $a|b$, אם קיים c כך ש:

$$b = ac$$

תרגיל

$\cdot | \cdot$ הוא יחס טרנזיטיבי ורפלקסיבי.

תרגיל

$$a|b|a \Leftrightarrow b = \pm a$$

הגדרה

יהיו $a, b \in \mathbb{Z}$, לא שניהם 0.

d הוא המחלק המשותף המקסימלי של a, b , ונסמן (a, b) , אם $d|a, b$, והוא הגדול ביותר כנ"ל.

טענה

לכל a ולכל $b \neq 0$, קיימים q, r כך ש:

$$a = q \cdot b + r$$

:ו

$$0 \leq r < |b|$$

הוכחה

נניח כי $0 < b$, ונוכיח עבור $0 \leq a$.

נוכיח באינדוקציה על a .

בסיס: $a = 0$

מתקיים:

$$0 = 0 \cdot b + 0$$

צעד: $0 < a$

נניח כי:

$$a = q \cdot b + r$$

כאשר:

$$0 \leq r < b$$

אם $r < b - 1$:

$$a + 1 = q \cdot b + (r + 1)$$

ואכן:

$$0 \leq r + 1 < b$$

אם $r \geq b - 1$:

$$a + 1 = (q + 1) \cdot b + 0$$

ואכן:

$$0 \leq 0 < b$$

■

משפט

יהיו $a, b \in \mathbb{Z}$, לא שניהם 0.

אז קיימים $\alpha, \beta \in \mathbb{Z}$, כך ש:

$$(a, b) = \alpha a + \beta b$$

הוכחה

נתבונן בקבוצה:

$$I = \{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\}$$

נסמן:

$$I^+ = \{x \in I \mid 0 < x\}$$

$$e = \min I^+$$

$d|e$, לכן $d|a, b$.

נצבע חלוקה עם שארית של a ב- e :

$$a = q \cdot e + r$$

כאשר:

$$0 \leq r < e$$

לכן, $r \in I$.

$r \notin I^+$, שכן:

$$r < e = \min I^+$$

לכן:

$$r = 0$$

לכן $e|a$.

באופן דומה, $e|b$.

לכן:

$$e \leq d$$

לכן:

$$d = e$$

■

למה

אם $(a, b) = 1$ ו- $a|bc$ אז $a|c$.

הוכחה

עפ"י המשפט, קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש:

$$\alpha a + \beta b = 1$$

לכן: $a | \alpha ac + \beta bc$.

לכן: $a | c$.



הגדרה

a אי פריק אם מתקיים: אם $b | a$, אז $b = \pm 1, \pm a$.

p ראשוני אם מתקיים: אם $p | bc$, אז $p | b$ או $p | c$.