©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש"פ: בר אלון, מיכאל פרי, שמואל שמעוני, איברהים שאהין, דורון מור, חיה קלר, אלעד אייגנר-חורב. נכתב ע"י דורון מור

מחלק משותף מקסימלי

__הגדרה__: (מחלק משותף מקסימלי): יהיו $0 \neq a, b \in \mathbb{Z}$. נאמר כי $d \in \mathbb{Z}$ הינו המחלק המשותף המקסימלי (מכאן ואילך נקרא לו- **gcd**) של a ו-b אם מתקיים:

I. $d|a$ וגם $d|b$. ובנוסף,
II. אם קיים מספר c כך ש $c|a$ וגם $c|b$ אזי $c \leq d$.

נרשום $\gcd(a, b)$ או (a, b) לציון מספר זה.

__הגדרה חלופית__: נרשום $D(a) = \{m \in \mathbb{Z} : m|a\}$, כלומר, קבוצת כל המחלקים של a. אזי נקבל:

$$(a, b) = \max\{D(a) \cap D(b)\}.$$

__למה 1__: יהיו a, b מספרים ויהי $d = (a, b)$. אזי $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. כלומר, המספרים $\frac{a}{d}, \frac{b}{d}$ הם זרים.

__הוכחה__: יהי $e > 0$ מחלק משותף של a ו-b. אזי מתקיים $a = edl, b = edk$ עבור k, l שלמים כלשהם. לכן ed הוא מחלק משותף של a ו-b. אלא שלפי ההגדרה בהכרח $ed \leq d$ שכן $d = (a, b)$ ולכן $e = 1$. ■

__הגדרה__: יהיו a, b מספרים שלמים. אזי אוסף הקומבינציות הליניאריות של a, b הוא הקבוצה

$$L(a, b) \coloneqq \{ma + nb : m, n \in \mathbb{Z}\}.$$

__דוגמה__: יהיו $a = 5, b = 7$. אזי אוסף הקומבינציות הליניאריות של a, b הוא הקבוצה

$$L(5,7) = \{5m + 7n : m, n \in \mathbb{Z}\}$$

(כל זוג מספרים שלמים שתציבו ב m, n יתן מספר כלשהו שהוא קומבינציה ליניארית של 5,7.)

__למה 2__ (*Bezout*): לכל שני שלמים a, b מתקיים $(a, b) \in L(a, b)$.

__הוכחה__: יהיו a, b שלמים. נבחר $m = a, n = b$ ונקבל $ma + nb = a^2 + b^2 \in \mathbb{Z}^+$ ולכן $L(a, b) \cap \mathbb{Z}^+$ לא ריק, ובפרט יש לו איבר מינימלי לפי WOP. נראה כי איבר זה הינו (a, b). יהי $d = ma + nb$ האיבר המינימלי ב $L(a, b) \cap \mathbb{Z}^+$. נראה ש $d \in D(a) \cap D(b)$. לפי משפט החלוקה אפשר לרשום $a = dq + r$ עבור $0 \leq r < d$. אם $r = 0$ אזי $d|a$. נניח בשלילה כי $r > 0$ ולכן מתקיים

$$0 < r = a - qd = a - q(ma + nb) = (1 - qm)a - qnb$$

לכן $r \in L(a, b) \cap \mathbb{Z}^+$ וגם $r < d$ בסתירה למינימליות של d. לכן, $d|a$. טיעון זהה מראה ש $d|b$.

נותר להראות כי d הינו המחלק המשותף המקסימלי. יהי c מחלק משותף של a, b. היות ומתקיים $d = ma + nb$, נובע ש-$c|d$ ולכן $c \leq d$.

__למה 3__ (*Euclid*) אם $a|bc$ וגם $(a, b) = 1$ אזי $a|c$.

__הוכחה__: לפי *Bezout*, ניתן לרשום $1 = ma + nb$ עבור $m, n \in \mathbb{Z}$. נשים לב שמתקיים

$$c = c \cdot 1 = c(ma + nb) = cma + cnb$$

באופן טריוויאלי, $a|cma$. בנוסף, לפי ההנחה ש $a|bc$ מתקיים גם ש $a|cnb$. לכן $a|c$.

<u>למה 4</u>: יהיו $a,b>0$ ויהי $c\in\mathbb{Z}^+$ אזי $(ca,cb)=c(a,b)$.

<u>הוכחה</u>: יהי $d=(a,b)$. לפי ההוכחה של *Bezout*, ראינו כי d הוא המספר החיובי המינימלי מהצורה $ma+nb$. לכן, cd הוא המספר החיובי המינימלי מהצורה $c(ma+nb)$ (עבור m,n שלמים) שזהה ל $(ca)m+(cb)n$, ולכן נקבל ש $cd=(ca,cb)$ כנדרש. ■