הרצאה 2

כותב: איתיווייסמן, מרצה: רון אהרוני

26 באפריל 2019

בהינתן שני מספרים m,n מספר a נקרא מחלק משותף אם $a|m$ וגם $a|n$.
האם לכל 2 מספרים יש מחלק משותף? התשובה היא כן, שכן עבור 1 מתקיים $1|m$ וכן $1|n$ לכל m,n כאלה.
מעניין למצוא את המחלק המשותף הגדול ביותר, יסומן ממג"ב, או (m,n) ובסימון מלא $gcd(m,n)$.
למשל עבור: $40 = (120,80)$, עבור $3 = (2019,81)$ ניתן לגלות כי שניהם מתחלקים ב-3 לפי כלל חלוקה. עבור $1 = (1003,2018)$ שכן 1003 הוא ראשוני. $1003 = (1003,2006)$ למרות ש1003 ראשוני, הוא מתחלק בעצמו.

1 מכפלה משדותפת

מכפלה משותפת של 2 מספרים m,n הוא מספר המתחלק גם ב-m וגם ב-n.
דוגמה למכפלה משותפת של $120,80$ היא 120×80, אך מעניין למצוא את המכפלה המשותפת הקטנה ביותר שהיא 240.
נרצה למצוא את המכפלה המשותפת המינימאלית של m,n והיא מסומנת ב-$[m,n]$ ובסימון מלא $l.c.m(m,n)$.
עבור הדוגמה שלנו: $l.c.m(120,80) = 240$.

1.1 איך מוצאים את $l.c.m(m,n)$ ואת $gcd(m,n)$?

מפרקים לפירוק ראשוני: $2\cdot2\cdot2\cdot3\cdot5 = 120$ ועבור $2^4\cdot5 = 80$. כך קל למצוא את $gcd(120,80) = 5\cdot2^3$ שכן אלה נמצאים ב2 הפירוקים (החיתוך של הפירוקים).
עבור $l.c.m$: $l.c.m(120,80) = 2^4\cdot3\cdot5$, לקחנו סוג של איחוד של הפירוקים, כך שלקחנו את החזקה המקסימלית מכל מחלק בפירוקים.
פורמאלית, אם קיימים הפירוקים:

$$m = p_1^{k_1}\cdot p_2^{k_2}\cdots p_l^{k_r}$$
$$n = p_1^{l_1}\cdot p_2^{l_2}\cdots p_r^{l_r}$$

נשים לשם שחלק מה k_i וכן חלק מה-l_i יכולים להיות 0 ולכן לא יכללו בפירוק.
מתקיים:

$$gcd(m,n) = p_1^{min\{k_1 l_1\}}\cdots p_r^{min\{k_r,l_r\}}$$

$$l.c.m(m,n) = p_1^{max\{k_1 l_1\}} \cdots p_r^{max\{k_r,l_r\}}$$

טענה. מתקיים $gcd(m,n) \cdot l.c.m(m,n) = m \cdot n$

הוכחה. אם מכפילים את את המס' על פי הגדרתם לעיל, נקבל כי לכל p_i החזקה היא חיבור החזקות התואמות של כל פירוק ולכן מחוקי חזקות קל להפריד למס' m, n המקוריים. ■

למעשה זהו המחלק המשותף המקסימלי ובעזרת שיטה זו קל יחסית למצוא אותו.

1.2 אלגוריתם למציאת m, n

ראשית נוכיח משפט: (m,n) הוא צירוף לינארי של m,n, כלומר: $(m,n) = a \cdot m + b \cdot n$ כאשר $a, b \in \mathbb{Z}$

למשל מתקיים: $40 = (120, 80) = 1 \cdot 120 - 1 \cdot 80$

עבור: $1 = (19,7) = 3 \cdot 19 - 8 \cdot 7$ (לא מאוד קל למצוא את זה ישר).

האלגוריתם שנציג, ימצא לנו את a, b הללו. נשים לב כי קיימים אינסוף זוגות a, b שמתאימים לנו.

הוכחה. נוכיח בצורה שאינה קונסטרוקטיבית, דהיינו נוכיח שקיים הצירוף הזה אך לא נראה איך להשיג אותו (זה נעשה באמצעות האלגוריתם).

תזכורת: הראנו שאם $S \subseteq \mathbb{Z}$ סגורה לחיבור ולחיסור אז $S = k \cdot \mathbb{Z}$ כלומר כל המס' המתחלקים בk.

(הערה: אם S סגורה לחיסור אז היא סגורה גם לחיבור).

תהא S קבוצת כל הצירופים של m,n, דהיינו: $S = \{a \cdot n + b \cdot m | a, b \in \mathbb{Z}\}$.

טענה: S סגורה לחיסור. נוכיח על פי ההגדרה: יהיו $x = a_1 m + b_1 n \in S$ וכן $y = a_2 m + b_2 n \in S$ אזי מתקיים: $x - y = (a_1 - a_2)m - (b_1 - b_2)n$ ולכן $x - y \in S$ עפ"י הגדרת S. באופן דומה S סגורה לחיבור. לכן $k \in S$.

טענה: $k = (m,n)$, אם נוכיח זאת אזי יתקיים $k = am + bn$ כי הוא בS וסיימנו.

נוכיח: $k|m, k|n$ ולאחר מכן נוכיח שהוא הגדול ביותר. $m = 1 \cdot m + 0 \cdot n$ ולכן $m \in S$. באותו אופן $n = 0 \cdot m + 1 \cdot n$ ולכן $n \in S$. מכך ש $S = k\mathbb{Z}$, אזי מתקיים $m = q \cdot k$ ולכן $k|m$ ובאופן דומה $k|n$, ולכן k מחלק משותף. נוכיח מקסימליות: כלומר לכל מחלק משותף l אז $l \leq k$. נראה ש: $l|k$. נתון לנו כי $l|m$ וגם $l|n$ ולכן מתקיים: $l|am$ וכן $l|bn$ ולכן גם $l|am + bn$ כלומר $l|k$, ולכן $l \leq k$. ■

1.2.1 אלגוריתם אוקלידס - מציאת a, b

הראנו $(19,7) = 1$ (נדבר בהמשך על המקרה המיוחד הזה בו ה$gcd(m,n) = 1$, כלומר המספרים זרים).

מתקיים: $19 = 2 \cdot 7 + 5$. ולכן $5 = 19 - 2 \cdot 7$ ולכן לאחר הצבה חוזרת מהמשפט שהראנו $k|5$.

מתקיים: $7 = 1 \cdot 5 + 2$ ולכן $2 = 7 - 1 \cdot 5$ ולכן $k|2$.

נמשיך: $5 = 2 \cdot 2 + 1$ ולכן $1 = 5 - 2 \cdot 2$ ולכן $k|1$

ולכן $k = 1$.

טענה. יהיו m,n,a$\in \mathbb{N}$. מספר k מחלק את m וגם מחלק את n אם ורק אם k מחלק את n ואת $m - na$.

הוכחה. נניח ש k מחלק את m ואת n, אז $k|n$ ולכן $k|na$ ולכן $k|m-na$. באופן דומה בכיוון ההפוך. ■

מסקנה. $(m,n)=1$ אם ורק אם 1 הוא צירוף שלהם, כלומר קיימים a,b כך ש-$am+bn=1$.

הוכחה. כיוון ראשון, אם $(m,n)=1$ אזי כמו שהראנו קודם $am+bn=1$. בכיוון השני, נניח ש$am+bn=1$, נראה ש $(m,n)=1$. יהא x מחלק משותף, נראה כי $x=1$.
$x|a \wedge x|b \Rightarrow x|am+bn=1$ ולכן $x=1$. ■

טענה. אם p ראשוני, וכן $p|mn$ אזי $p|m$ או $p|n$.

הוכחה. נניח בשלילה כי הנ"ל לא מתקיים, כלומר p לא מחלק את m ולא מחלק את n, כלומר $gcd(p,m)=1$ $gcd(p,n)=1$. לפי הטענה לעיל מתקיים $ap+bm=1$ וכן $cp+dn=1$. נכפול את המשוואות ונקבל $1=(cp+dn)(ap+bm)=p(acp+bmc+adn)+bdmn$ אך ממשוואה זו נשים לב כי $p|mn$ ולכן $p|1$ בסתירה לכך של-1 מחלק יחיד, הוא עצמו. ■