## תזכורת

* משפט החילוק: לכל $a,b$ $b\neq 0$ קיימים $q,r\in\mathbb{Z}$ הבודדים יחידים כך ש $a=bq+r$ כאשר $r\in[0,b-1]$

* יחס חילוקה: נאמר ש $a|b$ אם $\exists k\in\mathbb{Z}$ כך ש $b=a\cdot k$

* מחלק משותף מקסימלי: נאמר ש $a,b\in\mathbb{Z}$ אזי $d=(a,b)$ מקיים: (1) $d|a$ ו $d|b$

(2) $\forall c\in\mathbb{Z}$ כך ש $c|a$ ו $c|b$ אזי $c\leq d$

דוג': $(12,6)=6$ $(18,14)=2$ $(24,36)=12$

* תכונות חילוקה: (1) $a|b \Rightarrow a|bk$ $\forall k$, (2) $a|b$, $a|c \Rightarrow a|b\pm c$

(3) $a|b$, $b|c \Rightarrow a|c$

## נכיל 1: מבוא לאלגוריתם אוקלידס:

הגדרה: $(a,b)=(b,r)$

כאשר $r=a-bq$

פירוש: נוכיח כי כל מחלק משותף של $a,b$ מחלק גם גם את $r,b$ ולהפך.

צד ראשון: יהי $e$ מחלק משותף של $a,b$ ונראה כי $e$ מחלק את $b$ ואת $a-bq$

לפי הנחה, $e|a$ ו $e|b$ ולכן $e|bq$ (1)

ולכן $e|a-bq$ (2) כנדרש (לפי תכונות חילוקה)

צד שני: יהי $e$ מחלק של $b$, $a-bq$ ונראה $e$ מחלק את $a$ ו $b$.

לפי הנחה, $e|b$ ו $e|a-bq$, ולכן $e|bq$ (1) ולכן $e|a-bq+bq=a$ (2) כנדרש.

Scanned with CamScanner

אלגוריתם אוקלידס:

```
Euclid (a,b):
if b = 0 then:
        return a
else
        return (b, a-bq)
```

בוא נראה כיצד (לצורך, נכונות ויעילות האלג' תוכח בהרצאה)

נחשב (426,324)

$(426,324) = (324,102) = (102,18) = (18,12) = (12,6) = (6,0) = 6$

בדק אחרת:

$426 = 324 \cdot 1 + 102$

$324 = 102 \cdot 3 + 18$

$102 = 18 \cdot 5 + 12$

$18 = 12 \cdot 1 + 6$

$12 = 6 \cdot 2 + 0$

← לשם הרא הדבק

---

הגדרה: מספר ראשי $n$ וקרא מספר משני אם $n>1$ ואם $n$ מתחלק רק ב 1 ובעצמו

הגדרה: מספר ראשי $n$ יקרא מספר פריק אם קיימים $a,b$ כך ש $2 \le a,b \le n-1$ כך ש $n=a \cdot b$

**הגדרה:** יהיו $a,b$ מספרים שלמים אז הקומבינציה הלינארית היא הקבוצה:

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

**טענה ביזו:** אם $a,b \in \mathbb{Z}$ ו $(a,b)=d$ אז קיימים $n,m \in \mathbb{Z}$ כך ש $a\cdot n + m\cdot b = d$

**דוג:** אם $(18,12)=6$ אז

$$6 = 18\cdot n + 12\cdot m$$

כאשר $n=1$, $m=-1$

**תרגיל:** יהיו $a,b,c \in \mathbb{Z}$ אז אם $a \mid bc$ ו $(b,a)=1$ אז $a \mid c$

**פתרון:** נשים לב כי

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

לפי ביזו

$$= cma + cnb$$

נקבל כי $a \mid a$ ולכן $a \mid cma$

ו $a \mid cbc$ לפי ההנחה ולכן $a \mid c$.

* זה תרגיל חשוב!!

**למה:** לכל מספר $n$ שלם גדול מ-1 קיים מחלק ראשוני.

הוכחה: נניח בשלילה שהטענה אינה נכונה, ויהי $n$ בדיוק מ נבחר להיות מינימלי (לפי עקרון ה-WOP) אם $n$ ראשוני אז $n$ חוא בסתירה לכך שאין לו מחלקים ראשוניים

אם $n$ לא ראשוני, אז $n$ פריק ולכן קיימים $1-n \geq a,b \geq 2$ כך ש $n=a\cdot b$.

הוו $n$ הוא בדיוק מינימלי, קיים $a$ ראלב מחלק ראשוני, נקרא לו $p$ ולכן $p|a$ לפי הגדרת $p|a$ ו $p|a$ אז $p$ חוא סתירה.

**משפט:** אם $n$ פריק אז יש לו מחלק ראשוני $\leq \sqrt{n}$

הוכחה: $n$ פריק ולכן $n=a\cdot b$ עבור $a,b \in [2,n-1]$ נניח כי $a \leq b$ בלב. נשים לב כי $a \leq \sqrt{n}$ כי אם אחרת $a\cdot b > n$. לפי הלמה הקודמת קיים $a$ מחלק ראשוני ולכן גם $n$. (מחלק $\leq \sqrt{n}$)

מסקנה: כדי לבדוק אם מספר $n$ הוא ראשוני או לא, נוכל לבדוק אם קיים לו מחלק עד $\sqrt{n}$ אם לא, אזי $n$ ראשוני

---

תרגיל*: הוכיחו כי כל מחלק ראשוני צרים $a,b \in \mathbb{Z}$ שונה ב-1 משלם של $a^2+b^2$

**בתרגיל:** ידוע כי $p|a+b$ ולכן $p|(a+b)^2$ בנוסף $p|a^2+b^2$ ולכן מתקבלת חלוקה

$$p|(a+b)^2-a^2-b^2 = 2ab$$

בדיוק מחלק לגורמים.

מקרה I: אם $p|a$ ו $p|a+b$ אזי $p|a+b-a$
$=b$

ידוע כי $(a,b)=1$ ולכן קיבלנו סתירה להנחה
כי אם $p|a$ אזי $(a,b)=p>1$.

מקרה II: אם $p|b$ (סימטרי)

מקרה III: $p \nmid a$ ו $p \nmid b$
ידוע כי $p|2ab$ ולכן $p$ בוא ולכן $p=2$ בהכרח

לפי הנחת התרגיל אם $a|bc$
ו $(a,b)=1$ אזי $a|c$.