20/10/15

בס"ד

ובהשגחתו!

תורת המספרים - גבריאל נבש

gabrieln@ariel.ac.il

אתר הקורס - באתר של ד"ר אלעד חורב (קישור במודל)

עבודות בית 20%

מבחן 80%

http://elad-horev.org/NT16

סימני הרצאות

- בשבל ה -

## הקדמה על קבוצות

קבוצה - אוסף של איברים. $3 \in A, 8 \notin A$ $A=\{3,4,7\}$ (אין משמעות לסדר)

$A \subseteq B$ מוכל. $A \subsetneq B$ מוכל ממש (מוכל אבל לא שווה). $\{\{2,3\}\} \subseteq F$

$A \cup B$ איחוד $A \cap B$ חיתוך

$\emptyset$ הקבוצה הריקה. תת-קבוצה של כל קבוצה.

$F=\{\{2,3\},2,\{4,5\},\emptyset\}$

$\{2\} \in F$ ? לא

$\{2\} \subseteq F$ ? כן

$\{2,3\} \in F$ ? כן

$\{2,3\} \subseteq F$ ? לא

$2 \in F$ ? כן

$3 \in F$ ? לא

$\emptyset \in F$ ? כן

$\emptyset \subseteq F$ ? כן

$\emptyset \subseteq \emptyset$ ? כן

חסר - שיעור 5 10 11

**זוג סדור** לדוגמא $(2,3)$ או $<,>$

- יש חשיבות לסדר $(3,2) \neq (2,3)$
- איבר יכול להופיע יותר מפעם אחת $(2,2)$ $(3,3)$
- יש גם שלשה סדורה, חמישיה סדורה, n-יה סדורה.

**מכפלה קרטזית**

$X \times Y$ - קבוצת כל הזוגות הסדורים עם איבר ראשון מ-X ואיבר שני מ-Y

לדוגמא: $A=\{2,3\}$ $B=\{3,4,5\}$

$A \times B = \{(2,3),(2,4),(2,5),(3,3),(3,4),(3,5)\}$

תרגיל: חשב את $(A \times B) \cap (B \times A)$.

$B \times A = \{(3,2),(3,3),(4,2),(4,3),(5,2),(5,3)\}$

$|A \times B| = 6$ $|A|=2$ $|B|=3$

משפט: לכל קבוצה שתי קבוצות סופיות $X,Y$, $|X \times Y| = |X| \cdot |Y|$

20/10/15 ג' חשון

מס' 5 והתשובות:

$A^2 = A \times A$

$A \times B \times A = \{(2,3,2),\dots,(3,4,2)\dots\}$ קבוצת כל השלשות המתקבלות עם איבר ראשון מ-A, איבר שני מ-B, ואיבר שלישי מ-A.

**מחלקים**

הגדרה: יהיו $a,b \in \mathbb{Z}$ אז אומרים ש-a מחלק את b אם $\frac{b}{a}$ (הוא) מספר שלם ($\frac{b}{a} \in \mathbb{Z}$)

הגדרה אחרת: יהיו $ab \in \mathbb{Z}$ אז אומרים ש-a מחלק את b אם קיים $c \in \mathbb{Z}$ כך ש $ac = b$

סימון: $a|b$ → "a מחלק את b".

תרגיל: האם $-2|8$ ? כן

$0|3$ ? לא

$3|3$ ? כן

$3|0$ ? כן

$0|0$ ? כן

אם $n \in \mathbb{Z}$ אז נגדיר $D(n) = \{m \in \mathbb{N} \mid m|n\}$ "כך ש"

קבוצת המחלקים של n

לדוגמא:

$D(12) = \{1,2,3,4,6,12\} = D(-12)$

$0 \notin D(12)$

**ראשוניים** מספר $n \in \mathbb{N}$ נקרא ראשוני אם:

א. $n \geq 2$

ב. המחלקים החיוביים היחידים של n הם 1, n.

משפט - כל מספר טבעי הוא מכפלה של מספרים ראשוניים.

סקיצה של הוכחה: $60 = 20 \cdot 3$, $20 = 10 \cdot 2$, $10 = 5 \cdot 2$

לכן $60 = 5 \cdot 2 \cdot 2 \cdot 3$

אם n הוא ראשוני - סיימנו.

אחרת, נפרק את n ל- $n = a \cdot b$ ונמשיך הלאה עם a ו-b. התהליך בטוח יסתיים.

**מה מינימלי** עקרון - לכל קבוצה לא ריקה יש מספר מינימלי.

27/10/15

הסדר ובהתאמה לתנו!

תורת המספרים - שיעור 2

אך על קבוצות

סימון בניית קבוצות

$A=\{1,2,3,4,5\}$ $B=\{2,3\}$

$C=\{x\in A : x<4\} \Rightarrow C=\{1,2,3\}$

כאשר

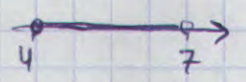
$D=\{x+2y : x\in A, y\in B\}$

$(x,y)=(1,2)\ (1,3)\ (2,2)\ (2,3)\ (3,2)\ (3,3)\ (4,2)\ (4,3)\ (5,2)\ (5,3)$

$D=\{5,7,6,8,9,10,11\}$

סימון קטעים של מספרים

$E=[4,7)$



עקרון הסדר הטוב - תרגום חופשי

Well-Ordering Principle

לכל תת-קבוצה לא ריקה של $\mathbb{N}$ (הטבעיים) יש איבר מינימלי.

הערות: * לא בהכרח יש איבר מקסימלי

* אם במקום $\mathbb{N}$ נשים $\mathbb{R}$ (או $\mathbb{Z}$) אז ~~[illegible]~~ זה לא נכון.

דוגמאות

$A=\{n\in\mathbb{N}:$ n מסתיים ב-7 ויש לו 3 ספרות$\}$

$A=\{107,117,127,\dots 997\}$ איבר מינימלי: 107. מקס: 997

$B=\{n\in\mathbb{N}:$ n מסתיים ב-7$\}$

$B=\{7,17,27,\dots\dots\}$ מינימלי: 7, מקסי: אין.

משפט: $\sqrt{2}\notin\mathbb{Q}$ ($\sqrt{2}$ הוא אי-רציונלי)

מס שהריבוע שלו שווה ל-2 $\rightarrow \sqrt{2}=1.414\dots$

* ההוכחה הראשונה שלנו

* דוגמה לשימוש ב-WOP

מחלקת שקילות

$\frac{1}{2}$ $\frac{2}{4}$ $\frac{5}{10}$ $\frac{100}{200}$

שאלה: האם קיימים $p,q\in\mathbb{N}$ כך ש- $\frac{p}{q}=\sqrt{2}$?

לכל מספר רציונלי יש הרבה ייצוגים למשל: $0.5=\frac{1}{2}=\frac{2}{4}=\frac{3}{6}=\frac{100}{200}$

ניקח את הייצוג עם המונה הכי קטן ← מה קיים עפ"י ה-WOP.

$A=\{p\in\mathbb{N} : \exists q,\ \frac{p}{q}=\frac{1}{2}\}$

$A=\{$הקבוצות המונים של שברים ששווים ל- $\frac{1}{2}\}$

ל-A יש איבר מינימלי עפ"י ה-WOP.

~~ההוכחה לא עוקבת השאלה: נניח בשאלה ש- $\sqrt{2}$ רציונלי. ניקח את מחלקת השקילות של ל~~

27/10/15

<u>חזרה והשלמות:</u>

הוכחה על דרך השלילה: נניח בשלילה ש-$\sqrt{2}$ רציונלי. ניקח את מחלקת השקילות של כל השברים ששווים ל-$\sqrt{2}$.

ניקח את השבר עם המונה הכי קטן (עי' ה-WOP) נקרא לו $\frac{p}{q}$

$$\frac{p}{q}=\sqrt{2} \rightarrow \frac{p^2}{q^2}=2 \rightarrow p^2=2\cdot q^2$$

לכן $p^2$ הוא מס' זוגי (מתחלק ב-2)

$$p^2=2\cdot q^2 \rightarrow (2n)^2=2\cdot q^2 \rightarrow 4n^2=2q^2 \rightarrow 2n^2=q^2$$

לכן $q^2$ זוגי.

לכן $q$ בעצמו הוא זוגי. כלומר, קיים $m\in\mathbb{N}$ כך ש- $q=2m$.

$$\sqrt{2}=\frac{p}{q}=\frac{2n}{2m}=\frac{n}{m}$$

הנה שבר עם מונה יותר קטן. אבל לקחנו כבר את הכי קטן. סתירה! משלל!

<u>העבודה:</u> $a|b$ ("a מחלק את b") אם קיים $c\in\mathbb{N}$ כך ש- $a\cdot c=b$.

לדוג' $D(12)=\{1,2,3,4,6,12\}$ $\quad D(n)$ ← קבוצת כל המס' הטבעיים שמחלקים את n.

$4\nmid 7$ , $2|8$

הגדרה: $p\in\mathbb{N}$ נקרא מספר ראשוני אם $p\neq 1$ ו- $D(p)=\{1,p\}$

המשפט היסודי של האריתמטיקה

<u>משפט בסיס:</u> כל מספר טבעי הוא מכפלה של מספרים ראשוניים. דוגמא:

$$11=11 \quad , \quad 10=2\cdot 5 \quad , \quad 40=2\cdot 2\cdot 2\cdot 5=2^3\cdot 5$$

הוכחה:

נתון מספר n. אם n ראשוני - סיימנו.

אם n לא ראשוני, זה אומר שקיים $1<a<n$ כך ש- $a|n$.

לכן קיים b כך ש- $n=a\cdot b$. ממשיכים הלאה, מפרקים את a ואת b

עד שמגיעים ל- $n=\underset{\text{ראשוני}}{\circ}\cdot\underset{\text{ראשוני}}{\circ}\cdot\underset{\text{ראשוני}}{\circ}\cdot\underset{\text{ראשוני}}{\circ}\cdots\underset{\text{ראשוני}}{\circ}$ (יש כאן אינדוקציה. קשור ל-WOP)

המשפט היסודי של האריתמטיקה

<u>משפט לא כל כך בסיסי:</u> לכל $n\in\mathbb{N}$ הפירוק של n לראשוניים הוא <u>יחיד</u> (עד כדי סדר הראשוניים האיברים בכפל)

$$20=2\cdot 2\cdot 5=2\cdot 5\cdot 2=5\cdot 2\cdot 2$$

$$1261=13\cdot 97\neq \underbrace{31\cdot 41}_{1271}$$

27/10/15

בס"ד וקח שבלותינו!

## תורת מספרים "איברים"

gcd = greatest common divisor

מחלק משותף מקסימלי.

הגדרה:

$$\gcd(a,b) = \max\big(\underbrace{D(a)\cap D(b)}_{\text{קבוצת המחלקים המשותפים של } a,b}\big)$$

דוגמא: נמצא את $\gcd(36,60)$

$D(36) = \ldots$

$D(60) = \ldots$

$D(36)\cap D(60) =$

$\gcd(36,60) = 12$

חישוב gcd עפ"י פירוק לראשוניים

$36 = 2^2\cdot 3^2\cdot 5^0$

$60 = 2^2\cdot 3^1\cdot 5^1$

$\gcd = 2^2\cdot 3^1\cdot 5^0$

לוקחים חזקה מינימלית של כל מספר ראשוני בפירוק.

## משפט החילוקה עם שארית

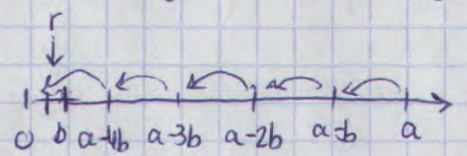
$100 \quad \frac{3}{33} \quad 100 = 33\cdot 3 + 1$ שארית

אם $a\in\mathbb{Z}$, $b\in\mathbb{N}$ אז קיימים מספרים יחידים $q, r\in\mathbb{Z}$ כך ש: $a = qb + r$ (שארית, מנה)

$0\le r\le b-1$ ( q=quatient r=remanider)

הוכחה: מחסרים מ-a כפלות של b עד שמגיעים למספר בין 0 ל-(b-1).

רושמים $r = a-qb$




הוכחה ע"י שימוש ב- WOP. נגדיר את הקבוצה

קבוצת כל השארות הפוטנציאליות $A=\{a-kb : k\in\mathbb{Z},\ a-kb\ge 0\}$

שייך ל: $A\subseteq\mathbb{N}$ בגלל: $A\ne\emptyset$

למה A לא ריקה? אם $a>0$ אז אפשר לקחת $k=0$ ⇐ $a\in A$ (אם סלב תיאל)

לכן עפ"י ה- WOP יש איבר מינימלי ב-A. נקרא לו r. $r = a-kb$

צריך רק להוכיח $0\le r\le b-1$ (כבר יודעים)

נניח בשלילה ש- $r\ge b$

ניתן למקום ש- r הוא לא באמת האיבר המינימלי ב-A. סתירה!

$$\underbrace{a-(k+1)b}_{\text{המספר הזה יותר קטן מ-r ועדיין שייך ל-A. סתירה.}} = \underbrace{a-kb}_{r} - b = r-b \ge 0$$

כי $r\ge b$

27/10/15

יהלי ובהשלמתו!

נשאר להוכיח: יש רק דרך אחת לכתוב $a=qb+r$ $\quad 0\le r\le b-1$

נניח שיש שתי דרכים: $a=q_1\cdot b+r_1$

$a=q_2\cdot b+r_2$

נוכיח ש- $q_1=q_2$ , $r_1=r_2$ (אז שתי הדרכים הן בעצם אותה הדרך).

$q_2b+r_2=a=q_1\cdot b+r_1$

$q_1b+r_1=q_2b+r_2$

$(q_1-q_2)b=r_2-r_1$

$b\mid(r_2-r_1)$ לכן

אבל

$-(b-1)\le r_2-r_1\le b-1$

אלו מספרים מתחלקים ב-b

בין $-(b-1)$ לבין $b-1$? רק 0!

$r_2-r_1=0$ לכן

$\Downarrow$

$r_1=r_2$

תרגיל: סיים את ההוכחה הראה ש $q_1=q_2$

$\mathbb{N}\subseteq S$ $\quad$ $\mathbb{Z}^+\subset\mathbb{N}$ $\quad$ **WOP**

נוכיח כי $\sqrt{2}$ לא מספר רציונלי.

$\sqrt{2}=\frac{a}{b}$ $\quad a\in\mathbb{Z}^+,\ b\in\mathbb{Z},\ b\neq0 \iff \sqrt{2}\in\mathbb{Q} \iff$ ① נניח בשלילה שהטענה לא נכונה

$\iff a=b\sqrt{2}$

$\in\mathbb{Z}^+$

נגדיר: $k$

$\in$ - איברים. $\subseteq$ - קבוצות

3/11/15 (4 שע') תורת המספרים - שיעור 3 בס"ד ובהשגחתו

(*) הערה: $\gcd(n,0)=n$

## אלגוריתם של אוקלידס (Euclid) לחישוב gcd

~~gcd(69677, 18~~

$\gcd(69677, 8108) = \gcd(8108, 4813) = \gcd(4813, 3295) =$

$\gcd(3295, 1518) = \gcd(1518, 259) =$

$= \gcd(36, 7) = \gcd(7, 1)$

$= \gcd(1, 0) = 1$

לוקחים כל פעם את המס' הקטן ושימים בצד שמאל של המאגרים ובצד ימין שמים את $a \bmod b$.

**משפט:** יהיו $a,b \in \mathbb{Z}$ ונסמן $d = \gcd(a,b)$

אז ניתן לכתוב את $d$ בצורה $d = ma + nb$ עבור $m,n \in \mathbb{Z}$

אלגוריתם מורחב של "אוקלידס".

"הוכחה" ע"י דוגמה: $a=60$ $b=35$

(1) $\gcd(60,35)$ $\quad 60 = 1\cdot 35 + 25$

(2) $\gcd(35,25)$ $\quad 35 = 1\cdot 25 + 10$

(3) $\gcd(25,10)$ $\quad 25 = 2\cdot 10 + 5$

(4) $\gcd(10,5)$ $\quad 10 = 2\cdot 5 + 0$

$\gcd(5,0) = 5$

$5 = \_\_\_\cdot 60 + \_\_\_\cdot 35$

$5 = 25 + (-2)10$ $\quad 5 = 25 - 20$

(2) $\boxed{10 = 35 + (-1)\cdot 25}$

$5 = 25 + (-2)35 + 2\cdot 25$

$5 = (-2)35 + 3\cdot 25$

$5 = (-2)35 + 3\cdot 25$

(1) $\boxed{25 = 60 + (-1)35}$

$5 = (-2)35 + 3\cdot 60 + (-3)35$

(3) $\boxed{5 = 3\cdot 60 + (-5)\cdot 35}$

---

**תרגיל** $x,y \in \mathbb{Z}$

① $\underbrace{172}_{a}x + \underbrace{20}_{b}y = \underbrace{1000}_{c}$ ← למשוואה זו קיים פתרון אמ"מ $\gcd(a,b)|c$

$\gcd(172,20) = 4$ ← $172x_1 + 20y_1 = 4$ ← נמצא את $x_1, y_1$ ואז נהכפיל ב-250 (כי $\frac{1000}{4} = 250$)

② כמה מס' טבעיים שלא גדולים מ-1,000 ולא מתחלקים ב-3 או 5.

תשובה: $1{,}000 - \underbrace{[1000/3]}_{\text{מס' טבעיים}} - [1{,}000/5] + [1{,}000/15] = 533$ ← בדלה והלאה

③ **בג'**: אם $a$ ו-$b$ באותה זוגיות (או שניהם זוגיים או שניהם לא) אז $a^2+b^2$ זוגי.

הוכחה: $a=2n+1$, $b=2n+1$ או $a=2n$, $b=2n$

$4n^2 + 4n^2 = 4(n^2+n^2)$ $(+2)$

## משפט החילוק עם שארית

לכל $a,b$ ניתן לכתוב $a=qb+r$ בצורה יחידה מקיימת כאשר $0\le r\le b-1$

**הגדרה:** $a \bmod b = r$

**תרגיל:** $100 \bmod 3 = 1$ , $300 \bmod 3 = 0$ , $3 \bmod 100 = 3$ , $20 \bmod 7 = 6$ , $(-20) \bmod 7 = \frac{1}{\cancel{-6}}$

$-20 = (-3)\cdot 7 + 1$

**הערה:** ב-C (ואולי בג'אווה) $20\%7=6$ ! $(-20)\%7=(-6)$

**תרגיל:** הוכח - לכל $a\in\mathbb{Z}$, $3 \mid a^3-a$

הבנת התרגיל ע"י דוגמא $a=3 \to 24$ , $a=4 \to 60$ , $a=0 \to 0$ , $a=2 \to -6$

**הוכחה:** $a^3-a = a(a^2-1)$

$= a(a+1)(a-1)$

$= \underbrace{(a-1)\cdot a\cdot(a+1)}$

שלושה מספרים, אחד מהם מתחלק ב-3.

למה? $a$ יכול להיות מהצורה

$a=3q$ או $a=3q+1$ או $a=3q+2$

אם $a=3q$ אז $3\mid a$ (סיימנו)

אם $a=3q+1$ אז $3\mid(a-1)$

אם $a=3q+2$ אז $3\mid(a+1)$

בכל מקרה $3 \mid \underbrace{(a-1)\,a\,(a+1)}$

מ.ש.ל

**תרגיל** הוכח - הריבוע של כל מספר אי-זוגי הוא מהצורה $8k+1$

דוגמה $1^2=1=0\cdot 8+1$ , $17^2=289=36\cdot 8+1$ , $15^2=225=28\cdot 8+1$ , $7^2=49=6\cdot 8+1$

**הוכחה:** תהי $n$ מספר אי-זוגי. כלומר $n=2q+1$ לכן

$n^2=(2q+1)^2 = 4q^2+4q+1 = 4q(q+1)+1$

אם $q$ זוגי אז $q=2t$ ואז $n^2=4\cdot 2t(q+1)+1$

$= 8t(q+1)+1$ סיימנו.

אם $q$ אי-זוגי אז $q+1$ הוא זוגי. כלומר $q+1=2t$ ואז $n^2=4q\cdot 2t+1$

$= 8qt+1$ מ.ש.ל

**הוכחה אחרת:** כל מס' אי-זוגי הוא מהצורה $4q+1$ או $4q+3$.

אם $n=4q+1$ אז $n^2=(4q+1)^2=16q^2+8q+1=8\underbrace{(2q^2+q)}_{k}+1$ סיימנו

אם $n=4q+3$

$n^2=(4q+3)^2=16q^2+24q+3=16q^2+24q+8+1=8\underbrace{(2q^2+3q+1)}_{k}+1$ סיימנו

3/11/15 עמוד 2 תורת המספרים - שיעור 3 מבוא והתפלגות

מטרה: להוכיח את המשפט היסודי של האריתמטיקה (הפירוק לראשונים הוא יחיד).

נלמד: איך לחשב gcd? מחלק משותף מקסימלי greatest common divisor

תזכורת הגדרה: $D(n)=\{k\in\mathbb{N} : k|n\}$

$$\gcd(a,b)=\max(D(a)\cap D(b))$$

סימון אחר $(a,b)=\gcd(a,b)$

הגדרה: אם $\gcd(a,b)=1$ אז אומרים ש-a ו-b הם זרים (relatively prime)

לדוג': 6,35 הם זרים, 7,100 זרים, 18 זרים.

משפט: יהיו $a,b\in\mathbb{Z}$ ונסמן $d=\gcd(a,b)$. אז $\frac{a}{b}=\frac{b}{a}$ מספרים שלמים

דוגמה: $a=6, b=8$ $d=2$. 3,4 זרים.

דוגמה 2: $b=10$ $a=10$ $d=10$. 1,8 זרים.

הוכחת המשפט: ניקח שני מספרים $a,b$

ניקח את $d=\gcd(a,b)$

ניקח את המספרים $\frac{a}{d},\frac{b}{d}$

ניקח את $e=\gcd\left(\frac{a}{d},\frac{b}{d}\right)$. (רוצים להוכיח $e=1$)

$e|\frac{a}{d}$ כלומר קיים מס' שלם k כך ש- $ek=\frac{a}{d}$ כלומר $\boxed{a=dek}$

$e|\frac{b}{d}$ כלומר קיים מס' שלם j כך ש- $ej=\frac{b}{d}$ כלומר $\boxed{b=dej}$

ל- a,b יש מחלק משותף de. אבל קודם אמרנו

המחלק המשותף המקסימלי שלהם הוא d. $de\le d$ $e\le 1$.

מכך שגם e לא יכול להיות פחות מ-1 לכן $e=1$. מש.

3/11/15 תורת המספרים - שיעור 3 בס"ד ובהשגחתו!

עמוד 3

משפט: לכל $a,b,c \in \mathbb{Z}$ מתקיים $\gcd(a,b)=\gcd(a+cd,b)$

דוגמה: $a=42$ , $b=24$ , $\gcd(a,b)=6$ ניקח $c=-1$

$\gcd(42-24,24)=\gcd(18,24)=6$

ניקח $c=10$ $\gcd(42+240,24)=\gcd(282,24)=6$

הוכחה: נוכיח שהמחלקים המשותפים של $a,b$

הם בדיוק המחלקים המשותפים של $a+cb,b$

צריך שני כיוונים ① כל מחלק משותף של $a,b$ הוא גם מחלק משותף של $a+c,b$ הכיוון

② כל מחלק משותף של $a+cb,b$ הוא גם מחלק משותף של $a,b$. נוכיח

הוכחה של ②: נניח ש- $k|(a+cb)$ וגם $k|b$. (רוצים $k|a$).

קיים $d$ כך ש- $kd=a+cd$

קיים $c$ כך ש- $ke=b$ $\quad (\times c)$

$kd-kec=a$

מלומר $a=k(d-ec)$ לכן $k|a$. מ.ש.ל

הוכחה: עפ"י משפט החילוק עם שארית $a=qb+\underbrace{r}_{a \bmod b}$ לכן $a \bmod b = a-qb$

לכן $\gcd(a,b)=\gcd(a-qb,b)=\gcd(a \bmod b,b)$

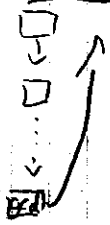
עפ"י המשפט (*)

(*) משפט: לכל $a,b,c \in \mathbb{Z}$ מתקיים $\gcd(a,b)=\gcd(a+bc,b)$

מסקנה: $\gcd(a,b)=\gcd(b,a \bmod b)$

שיעור 4

הוכחה:



## אלגוריתם אוקלידס המורחב

**למידון** נתון $a,b\in\mathbb{Z}$ נשמן $d=\gcd(a,b)$

ניתן לכתוב $d=ma+nb$ כאשר $m,n\in\mathbb{Z}$

**חסר בהוכחה:** למה התהליך תמיד נגמר? קשה.

**הוכחה פורמלית:**

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

**דוגמה:** $L(4,6)$ $\quad 2\in L(4,6) \Rightarrow 2\cdot 4+(-1)\cdot 6$ , $10\in L(4,6) \Rightarrow 1\cdot 4+1\cdot 6$

$L(4,6)=\{\dots,-6,-4,-2,0,2,4,6,\dots\}$

**משפט:** לכל $a,b\in\mathbb{Z}$ הקבוצה $L(a,b)$ מכילה בדיוק את הכפולות של $\gcd(a,b)$.

**במילים אחרות** $L(a,b)=\{\dots,-3d,-2d,-d,0,d,2d,3d,\dots\}$ כאשר $d=\gcd(a,b)$

**הוכחה:** **ביון א:** כל מספר ב $L(a,b)$ הוא כפולה של $d$.

**ביון ב:** כל כפולה של $d$ נמצאת ב $L(a,b)$.

**הוכחת ביון א:**

**נניח** ש $k\in L(a,b)$ (נרצה להוכיח: קיים $q\in\mathbb{Z}$ כך $k=q\cdot d$)

**נתון יודעים** $k=ma+nb$ , $a=x\cdot d$ $\quad b=y\cdot d$ עבור $x,y\in\mathbb{Z}$

**לכן** $k=mxd+nyd \Rightarrow k=d(mx+ny) \Rightarrow mx+ny=q$ מ.ש.ל

**הוכחת ביון ב:**

**נניח קודם:** $d$ הוא האיבר החיובי המינימלי ב $L(a,b)$ *

(קשה: יש בכלל איבר חיובי מינימלי)

**הוכחה של *:**

$\boxed{f=ma+nb}$ יהי $f$ האיבר החיובי המינימלי של $L(a,b)$ **נכיח:** $f|a$

נניח בשלילה ש $f$ אינו מחלק את $a$ אז קיים משפט החילוק עם שארית

שארית שונה מ-0: $a=qf+r$, $f>r>0$. לכל $f$ גם שייך ל $L(a,b)$:

$r=a-qf=a-q(ma+nb)=a(1-qm)+b(-qn)$

$r=a(\text{משהו})+b(\text{משהו})$ $\Leftarrow$ לכן $r\in L(a,b)$ ויש סתירה

למינימליות של $f$. $\Leftarrow$ $\boxed{f|a}$ מ.ש.ל

**נכיח:** $f|b$ באותו דבר כמו $f|a$.

לכן: f הוא מחלק משותף של a,b (רצה להוכיח: f המחלק המשותף המקסימלי של a,b)

אבל לפי ביזו'ת f היא כפולה של d.

רוצה: f המחלק המשותף המקסימלי של ab.

יש מחלק משותף כלשהו של ab נקרא לו c. נרצה: $f \geq c$

יודעים: $f = ma+nb$ , $a = x\cdot c,\ b = y\cdot c \Rightarrow f = c(mx+ny)$

לכן $c|f$ לכן $c \leq f \Rightarrow \boxed{f=d}$

**מסקנה הנלמדת:** הגדר החיובי הכי קטן ב $L(a,b)$ הוא $d$.

נראה שכל הכפולות של $d$ נמצאות ב $L(a,b)$ ע"י שנכפיל את $m,n$. $(d=ma+nb)$

## אינדוקציה

$S(n) \leftarrow$ טענה התלויה במספר $n$. (יכולה להיות נכונה/לא נכונה)

דוגמא: "$n$ הוא זוגי" $\leftarrow S(n)$. "הוא מוזר" $= S(1)$ , $S(2)$ לא נכון $S(2)$ נכון וכו'

**נכונה טענה $S(n)$**

רוצים להוכיח ש- $S(n)$ נכונה לכל $n \in \mathbb{N}$

שיטה: להוכיח $*$ $S(0)$ נכונה (נבדיקה בשורה)

$*$ לכל $n$ אם $S(n)$ נכונה אז גם $S(n+1)$ נכונה

אחרי שהוכחנו את שתי ה $*$ יוצא $S(0) \to S(1) \to S(2) \to \dots$

**תזכורת:** איך מוכיחים טענה מהצורה "אם X אז Y" **הוכחה:** נניח X ... מסקנה Y.

דוגמא: הוכח באינדוקציה שלכל $n \in \mathbb{N}$ מתקיים $\sum_{i=1}^{n}(2i-1) = n^2$

דוגמא: $n=5 \leftarrow 1+3+5+7+9 = 5^2$

**הוכחה:** עבור $n=0$ (מקרה בסיס)

$\text{שמאל} = \sum_{i=1}^{0} \leftarrow$ סכום ריק (אפס הגדרה $= 0$) $\Rightarrow 0=0$ [הצלחת מוצר]

נעשה מקרה בסיס $n=1$ $\quad \text{שמאל} = 1^2 = \text{ימין}$ ✓

**אינדוקציה:** נניח שהנוסחא נכונה עבור $n$. כלומר נניח

ש- $\sum_{i=1}^{n}(2i-1) = n^2$.

**צ"ל:** הנוסחא נכונה עבור $n+1$ (נציב $n+1$ במקום $n$)

$$\underbrace{\sum_{i=1}^{n+1}(2i-1)}_{\text{צד שמאל}} = \underbrace{(n+1)^2}_{\text{צד ימין}}$$

**שיטה:** $\boxed{\text{צד ימין}} = \dots = \dots = \dots = \boxed{\text{צד שמאל}}$

$$\text{צד שמאל} = \sum_{i=1}^{n+1}(2i-1) = \underbrace{\left(\sum_{i=1}^{n}(2i-1)\right)}_{n^2} + (2(n+1)-1) = n^2+2n+1 = (n+1)^2 = \boxed{\text{צד ימין}}$$

**דוגמא ב':** $\sum_{i=1}^{n} i^2 \geq \frac{1}{3}\cdot n^3$ לכל $n \in \mathbb{N}$ נוסחא לסכום $\boxed{1^2+2^2+\dots+n^2 \geq \frac{1}{3}n^3}$

**דוגמא:** $n=4 \Rightarrow 1+4+9+16 \geq \frac{1}{3}\cdot 64 \Rightarrow 30 \geq 21.33$

**הוכחה:** **מקרה בסיס:** $n=1$ $1 \geq \frac{1}{3}\cdot 1$

**אינדוקציה:** נניח ש- $1^2+2^2+\dots+n^2 \geq \frac{1}{3}n^3$

**צריך להוכיח:** $1^2+2^2+\dots+n^2+(n+1)^2 \geq \frac{1}{3}(n+1)^3$

$$\boxed{\text{צד שמאל}} = \underbrace{1^2+2^2+\dots+n^2}_{\geq \frac{1}{3}n^3}+(n+1)^2 \underset{\text{הנחת האינדוקציה}}{\geq} \frac{1}{3}n^3+(n+1)^2 = \frac{1}{3}n^3+n^2+2n+1 > \frac{1}{3}n^3+n^2+n+\frac{1}{3} = \frac{1}{3}(n+1)^3 = \boxed{\text{צד ימין}}$$

$\{n \geq 2 \text{ לכל } 1 > \frac{1}{3}\}$

## עקרון האינדוקציה (החלשה)

תהי $P(n)$ טענה שמקיימת את התנאים הבאים:

1. $P(1)$ נכונה.
2. לכל $n$, אם $P(n)$ נכונה אז גם $P(n+1)$ נכונה

אז $P(n)$ נכונה לכל $n \in \mathbb{N}$.

## הוכחה של עקרון האינדוקציה עפ"י ה- Wop

נגדיר קבוצה $B = \{n \in \mathbb{N} \mid P(n) \text{ לא נכונה}\}$ (נרצה להוכיח $B=\emptyset$)

נניח בשלילה ש- $B$ לא ריקה, עפ"י ה- Wop יש ל- $B$ איבר מינימלי נקרא לו $a$. אחרון יודעים ש- $P(a)$ (כי $P(1)$ נכונה - נתון).

מכיוון ש- $a$ הוא מינימלי ב- $B$ אז $P(a-1)$ כן נכונה.

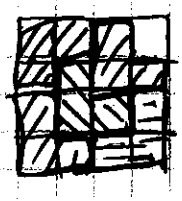
אבל סתירה להנחה ② (לכל $n$ אם $P(n)$ נכונה אז גם $P(n+1)$ נכונה).

לכן $B$ חייבת להיות הקבוצה הריקה כלומר $P$ נכונה לכל $n$.

הוכח באינדוקציה לכל $n\in\mathbb{N}$ אפשר לשלם לוח שחמט $2^n*2^n$

עם עותקים של הצורה  כך שנשארת

רק פינה אחת ריקה.



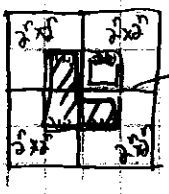
דוגמאות: $n=1$ לוח $2\times2$  $n=2$ לוח $4\times4$

$n=0$ לוח $1\times1$ □

הוכחה באינדוקציה:

נניח באינדוקציה שהטענה נכונה עבור לוח $2^n\times2^n$

צ"ל: ניתן לשלם לוח $2^{n+1}\times2^{n+1}$ ולהשאיר רק פינה אחת ריקה



נמסיל בתור עזר □

וסיימנו (נשאר רק פינה אחת)

לפעמים צריך להוכיח באינדוקציה טענה חזקה יותר

דוגמא: הוכח באינדוקציה שלכל $n\in\mathbb{N}$ $\sum_{i=1}^{n}\frac{1}{i^2}<2$

דוגמא: $n=3$ $1+\frac{1}{4}+\frac{1}{9}<2$

ננסה להוכיח באינדוקציה:

מקרה בסיס: $n=1$ $1<2$

אינדוקציה: נניח: $1+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{n^2}<2$

צ"ל: $\underbrace{1+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{n^2}+\frac{1}{(n+1)^2}}_{\text{Left Hand Side } LHS}<\underbrace{2}_{\text{RHS (Right Hand Side)}}$

$LHS=\underbrace{1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{n^2}}_{<2}+\frac{1}{(n+1)^2}<2+\frac{1}{(n+1)^2}$ (הערה בה כבר גדול מ 2) $<2$ תיר

לפי הנחת האינדוקציה

נוכיח באינדוקציה טענה יותר חזקה

$$\sum_{i=1}^{n}\frac{1}{i^2}\le 2-\frac{1}{n}$$

מקרה בסיס: $\frac{1}{1^2}\le 2-\frac{1}{1}$

אינדוקציה: נניח: $1+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{n^2}\le 2-\frac{1}{n}$

צ"ל: $1+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{n^2}+\frac{1}{(n+1)^2}\le 2-\frac{1}{n+1}$

$LHS=\underbrace{1+\frac{1}{2^2}+\frac{1}{3^2}+\dots+\frac{1}{n^2}}_{\le 2-\frac{1}{n}}+\frac{1}{(n+1)^2}\le 2-\frac{1}{n}+\frac{1}{(n+1)^2}\le 2-\frac{n^2+n-1}{n(n+1)^2}=2-\frac{n^2+n}{n(n+1)^2}=2-\frac{n(n+1)}{n(n+1)^2}=2-\frac{1}{n+1}=RHS$

לפי הנחת האינדוקציה

נצריך את ה-1 ובכך נקטין את המעלה

# שיעור 5

אם $d=\gcd(a,b)$ אז קיימים $x,y\in\mathbb{Z}$ כך ש: $ax+by$

אם $a,b,c\in\mathbb{Z}$, $c\mid ab$ ו: $a$ זר ל $c$ אזי $c\mid b$

**הוכחה:**

נתון ש $1=\gcd(a,c)$ לכן קיימים $x,y\in\mathbb{Z}$ כך ש $ax+cy$

נכפול את שני האגפים ב $b$ $b=abx+cby$

$c\mid cby$, $c\mid abx$ לפי הנתון, לכן $c\mid b=abx+cby$

**מסקנה:**

אם $p\in\mathbb{N}$ ראשוני, $a,b\in\mathbb{Z}$, $p\mid ab$ אזי $p\mid a$ או $p\mid b$

$p\in\mathbb{N}$ ראשוני $p\mid ab \Rightarrow p\mid a$ או $p\mid b$

**אבחנת לאינדוקציה חלשה:**

1) $S(0)$ אמת

2) $S(n)$ אמת $\leftarrow$ $S(n+1)$ אמת $\Leftarrow$ הטענה נכונה עבור כל $n$ טבעי

**אבחנת להוכחת עקרון האינדוקציה:**

1,2) מתקיים נניח בשלילה קיים $A\subseteq\mathbb{N}$ כך שעבור $a\in A$ שקר, $S(a)$

$a_0\geq 0$ כי $S(0)$ אמת.

$S(a_0-1)$ אמת כי $a_0$ מינימלי

אבל מצד ש $S(a_0-1)$ אמת נובע ש $a_0$ אמת ולכן זו סתירה להנחה.

~~אינדוקציה חזקה (שלמה):~~

$n_0,n_1\in\mathbb{N}$ $n_0\leq n_1$

אם 1) $S(n_0),S(n_0+1),\dots,S(n_1)$ אמת

2) $S(n_0),S(n_0+1),\dots,S(k-1),S(k)$ אמת אזי $S(k+1)$ אמת.

אז $S(n)$ אמת עבור כל $n\geq n_0$

## משפט קיום פירוק לראשוניים

לכל $2 \le n \in \mathbb{N}$ קיימים מספרים ראשוניים $p_1, p_2 \dots p_k$

כך ש: $n = p_1 \cdot p_2 \cdots p_k$

**הוכחה:** עבור $n = 2$ הטענה נכונה כי 2 ראשוני (דטיס אינדוקציה)

נניח שהטענה נכונה לכל מספר טבעי $2$ עד $n$

נוכיח את הטענה עבור $n+1$.

אם $n+1$ ראשוני סיימנו.

אם $n+1$ איננו ראשוני אז קיימים $a, b \in \mathbb{N}$ $2 \le a, b \le n$

כך ש: $n+1 = a \cdot b$

לפי הנחת האינדוקציה קיימים ראשוניים $p_1, p_2 \dots p_m$

כך ש: $a = p_1 p_2 \cdots p_m$

וקיימים ראשוניים $p_{m+1}, p_{m+2} \dots p_k$

כך ש: $b = p_{m+1} \cdot p_{m+2} \cdots p_k$

(הנחת האינדוקציה היא שהטענה מתקיימת לכל המספרים $2$ עד $n$, $a, b$ גם כאלה)!

$$n+1 = a \cdot b = p_1 \cdot p_2 \cdots p_m \cdot p_{m+1} \cdot p_{m+2} \cdots p_k$$

**פיבונצ'י**

$f_1 = 1 \quad f_2 = 1$

$f_n = f_{n-1} + f_{n-2}$

$$\sum_{i=1}^{n} f_i = f_{n+2} - 1$$

↓

**הוכחה:**

$n = 1$: $n = f_1 = f_{1+2} - 1 = f_3 - 1 = 2 - 1 = 1$

נניח ש: $\sum_{i=1}^{n} = f_{n+2} - 1$

נוכיח ש: $\sum_{i=1}^{n+1} f_i = f_{n+3} - 1$ (המקרה עבור $n+1$)

$$\sum_{i=1}^{n+1} f_i = \underbrace{\sum_{i=1}^{n} f_i}_{\text{לפי הנחת האינדוקציה}} + f_{n+1} = \underline{f_{n+2} - 1} + f_{n+1} = f_{n+3} - 1$$

לפי הגדרת המספר

פיבונצ'י $f_{n+2} + f_{n+1} = f_{n+3}$