התחלקות - הוכחות נבחרות

תורת המספרים האלמנטרית - 80115

מרצה: אהוד (אודי) דה-שליט

מתרגל: גיא ספיר

סוכם ע"י: שריה אנסבכר

סמסטר ב' תשפ"ג, האונ' העברית

תוכן העניינים

אשמח לקבל הערות והארות על הסיכומים על מנת לשפרם בעתיד,
כל הערה ולו הפעוטה ביותר (אפילו פסיק שאינו במקום או רווח מיותר) תתקבל בברכה;
אתם מוזמנים לכתוב לי לתיבת הדוא"ל: sraya.ansbacher@mail.huji.ac.il.

לסיכומים נוספים היכנסו לאתר:
אקסיומת השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 יחס החלוקה

טענה 1.1. יהיו $a, b, c \in \mathbb{Z}$, מתקיימים כל הפסוקים הבאים:

1. אם $a \mid b$ אז גם $-a \mid b$ וגם $a \mid -b$ (ולכן גם $-a \mid -b$).
2. אם $a \mid b$ ו-$b \neq 0$ אז $|a| \leq |b|$.
3. אם $a \mid b$ אז $a \mid bq$ לכל $q \in \mathbb{Z}$.
4. אם $a \mid b$ וגם $a \mid c$ אז $a \mid b + c$
5. אם $a \mid b$ וגם $a \mid c$ אז $a \mid bx + cy$ לכל $x, y \in \mathbb{Z}$.
6. יחס החלוקה הוא טרנזיטיבי, כלומר אם $a \mid b$ וגם $b \mid c$ אז $a \mid c$.
7. מתקיים $a \mid b$ וגם $b \mid a$ אם"ם מתקיים $a = \pm b$ (או $|a| = |b|$).
8. לכל $0 \neq m \in \mathbb{Z}$ מתקיים $a \mid b$ אם"ם $ma \mid mb$.

♣ בגלל סעיף 1 משפטים רבים שננסח עבור הטבעיים יהיו נכונים על השלמים בשינויים הקלים המתבקשים.

טענה 1.2. יהיו $a, b \in \mathbb{Z}$, a מחלק את b אם"ם $(a) \supseteq (b)$ ומתקיים שוויון בין (a) ל-(b) אם"ם $a = \pm b$.

משפט 1.3. חילוק עם שארית

יהיו $a, b \in \mathbb{Z}$ כך ש-$0 < a$ (כלומר $a \in \mathbb{N}$), קיימים ויחידים $q, r \in \mathbb{Z}$ כך ש-$a > r \geq 0$ וגם $b = q \cdot a + r$; בנוסף $a \mid b$ אם"ם $r = 0$.

♣ r זה נקרא <u>השארית</u> של חלוקת b ב-a ו-q נקרא <u>המנה</u> של חלוקה זו.

♣ יש לשים לב לכך ש-r אי-שלילי ולכן השארית של חלוקת -8 ב-3 היא 1 ולא -2 כפי שניתן היה לחשוב.

♣ לא בכל חוג קיימת חלוקה עם שארית, זהו הבדל מהותי בין חוג השלמים לחוגים אחרים, כך למשל השקילות בין אי-פריקות לראשוניות (שנגיע אליה בהמשך) נובעת ממשפט זה.

הוכחה. נסמן $q := \max\{i \in \mathbb{Z} \mid i \cdot a \leq b\}$ ו-$r := b - q \cdot a$.
מהגדרה מתקיים $b < (q+1) \cdot a = q \cdot a + a$ ומכאן ש-$a > b - q \cdot a = r$, כמו כן מהגדרה מתקיים $r = b - q \cdot a \geq 0$ ולכן r עומד בדרישות; כמובן שמתקיים:

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

א"כ הוכחנו את הקיום, נוכיח כעת את היחידות.
יהיו $q', r' \in \mathbb{Z}$ כך ש-$a > r' \geq 0$ וגם $b = q' \cdot a + r'$,

$$\Rightarrow q' \cdot a + r' = q \cdot a + r$$
$$\Rightarrow (q' - q) \cdot a + (r' - r) = 0$$

אבל בהכרח מתקיים $a > |r' - r|$ ומכאן ש-$r' - r = 0$ וממילא גם $q' - q = 0$, כלומר $r' = r$ ו-$q' = q$. ■

משפט 1.4. יהיו $a_1, a_2, \dots, a_n \in \mathbb{Z}$, מתקיימים שני הפסוקים הבאים:

- אם קיים $r \geq i \in \mathbb{N}$ כך ש-$a_i \neq 0$ אז קיים $d \in \mathbb{N}$ יחיד כך ש-$d \mid a_i$ לכל $n \geq i \in \mathbb{N}$ ובנוסף לכל $q \in \mathbb{Z}$ המחלק את כולם ($q \mid a_i$ לכל $n \geq i \in \mathbb{N}$) מתקיים $q \mid d$.
- אם $a_i \neq 0$ לכל $n \geq i \in \mathbb{N}$ אז קיים $l \in \mathbb{N}$ כך ש-$l \mid a_i$ לכל $n \geq i \in \mathbb{N}$ ובנוסף לכל $m \in \mathbb{Z}$ המתחלק בכולם ($a_i \mid m$ לכל $n \geq i \in \mathbb{N}$) מתקיים $l \mid m$.

טענה 1.5. יהי $I \subseteq \mathbb{Z}$ אידיאל, קיים $a \in \mathbb{N}_0$ יחיד כך ש-$I = (a)$.

הוכחה. אם $I = \{0\}$ אז ודאי ש-$I = (0)$ ולא קיים $0 \neq a \in \mathbb{N}_0$ כך ש-$I = (a)$.
א"כ נניח ש-$I \neq \{0\}$ ונסמן $a := \min\{i \in I \mid i > 0\}$ (מהגדרה $(a) \subseteq I$).
יהי $b \in I$, נחלק את b ב-a עם שארית: יהיו $q, r \in \mathbb{Z}$ כך ש-$0 \leq r < a$ וגם $b = q \cdot a + r$; I סגור לכפל בכל שלם ולכן $-q \cdot a \in I$, I סגור גם לחיבור ולכן $r = b - q \cdot a \in I$.
מהמינימליות של a נובע ש-$r = 0$ (אחרת $0 < r$ בסתירה לכך ש-a הוא החיובי הקטן ביותר שנמצא ב-I) ולכן $a \mid b$, כלומר $b \in (a)$; b הנ"ל היה שרירותי ומכאן ש-$I \subseteq (a)$, כלומר $I = (a)$.
היחידות נובעת גם היא מהמינימליות של a: לכל $a < c \in \mathbb{N}_0$ מתקיים $a \notin (c)$ למרות ש-$a \in I$. ■

♣ a זה נקרא <u>היוצר</u> של האידיאל והוא החיובי הקטן ביותר ששייך לאידיאל.

משפט 1.6. לכל $a, b \in \mathbb{Z}$ כך שלפחות אחד מהם שונה מאפס היוצר של האידיאל $\{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\}$ הוא $\gcd(a, b)$.

♣ כלומר לכל $d \in \mathbb{Z}$ מתקיים $d = \gcd(a, b)$ אם"ם $(d) = \{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\}$.

♣ מכאן נובע שניתן להציג את ה-gcd כצר"ל של a ו-b ושהוא המספר החיובי הקטן ביותר שניתן להציגו כך.

♣ לאפשרות להציג את ה-gcd כצר"ל של a ו-b ישנה חשיבות רבה בחשבון מודולרי: אם a ו-b זרים אז קיימים $x, y \in \mathbb{Z}$ כך ש-$1 = x \cdot a + y \cdot b$ ומכאן שלכל $c, d \in \mathbb{N}_0$ $b >$ קיים $x' \in \mathbb{Z}$ כך ש-$c \equiv d + x' \cdot a \mod b$ שהרי מתקיים $x \cdot a = 1 - y \cdot b$ ומכאן שגם:

$$d + (c - d) \cdot x \cdot a \equiv d + (c - d) \cdot (1 - y \cdot b) \equiv d + c - d - (c - d) \cdot y \cdot b \equiv c \mod b$$

טענה 1.7. יהיו $a, b \in \mathbb{Z}$.

1. $\gcd(a, b) = \gcd(b, a)$.
2. לכל $m \in \mathbb{N}$ מתקיים $m \cdot \gcd(a, b) = \gcd(ma, mb)$.
3. אם קיים $d \in \mathbb{Z}$ כך ש-$d \mid a, b$ אז אותו d מקיים $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \cdot \gcd(a, b)$.
4. לכל $x \in \mathbb{Z}$ מתקיים $\gcd(a, b) = \gcd(a, b + ax)$.
5. אם קיים $c \in \mathbb{Z}$ כך ש-$c \mid ab$ וגם $\gcd(b, c) = 1$ אז $a \mid c$.

1.1 אלגוריתם אוקלידס

יהיו $n, m \in \mathbb{Z}$ כך שלפחות אחד מהם שונה מאפס, נרצה למצוא את $\gcd(n, m)$.
כפי שראינו בטענה 1.1 המחלקים של מספר שלם ואלו של הנגדי שלו הם אותם מחלקים ולכן הסימן אינו משנה עבור מציאת ה-gcd, א"כ נגדיר $r_0 = |n|$ ו-$r_1 = |m|$[1] ונמצא את $\gcd(r_0, r_1)$.
לאלגוריתם ישנן שתי גרסאות: האלגוריתם הבסיסי והאלגוריתם המורחב, להלן הפירוט של שניהם בפסאודו-קוד.

אלגוריתם 1 אלגוריתם אוקלידס הבסיסי

נגדיר $i := 0$.
כל עוד $r_{i+1} \neq 0$:

- נחלק את r_i ב-r_{i+1} עם שארית, נסמן ב-q_i את המנה וב-r_{i+2} את השארית (כלומר יהיו $q_i, r_{i+2} \in \mathbb{Z}$ כך ש-$0 \leq r_{i+2} < r_{i+1}$ וגם $r_i = r_{i+1} \cdot q_i + r_{i+2}$).
- נגדיר את i להיות $i + 1$ ונעבור לשלב הבא בלולאה.

כעת מתקיים $r_{i+1} = 0$, א"כ מתקיים $r_i = \gcd(n, m)$ ולכן נחזיר את r_i ונסיים.

אלגוריתם 2 אלגוריתם אוקלידס המורחב

נגדיר $i := 0$.
נגדיר $a_{-1} := 0$ ו-$b_{-1} := 1$ ומכאן שמתקיים:

$$r_1 = a_{-1} \cdot r_0 + b_{-1} \cdot r_1$$

כל עוד $r_{i+1} \neq 0$:

- נחלק את r_i ב-r_{i+1} עם שארית, נסמן ב-q_i את המנה וב-r_{i+2} את השארית.
- נחלק למקרים:
  - אם $i = 0$ אז נגדיר $a_0 := 1$ ו-$b_0 := -q_0$.
  - אחרת, נגדיר $a_i = a_{i-2} - q_i \cdot a_{i-1}$ ו-$b_i := b_{i-2} - q_i \cdot b_{i-1}$.
- נגדיר את i להיות $i + 1$ ונעבור לשלב הבא בלולאה.

כעת מתקיים $r_{i+1} = 0$ וגם:

$$\gcd(r_0, r_1) = r_i = a_{i-2} \cdot n + b_{i-2} \cdot m$$

בעמוד הבא נוכיח את הנכונות של האלגוריתם המורחב וממילא נקבל את הנכונות של האלגוריתם הבסיסי.

[1] כדאי להגדיר את r_0 להיות בעל הערך המוחלט הגדול מבין השניים משום שבשלב הראשון של האלגוריתם נחלק את r_0 ב-r_1 עם שארית.

הוכחה. נגדיר $i := 0$.

נגדיר $a_{-1} := 0$ ו-$b_{-1} := 1$ ומכאן שמתקיים:

$$r_1 = a_{-1} \cdot r_0 + b_{-1} \cdot r_1$$

כל עוד $r_{i+1} \neq 0$:

- נחלק את r_i ב-r_{i+1} עם שארית, נסמן ב-q_i את המנה וב-r_{i+2} את השארית.

$$\Rightarrow r_{i+2} = r_i - r_{i+1} \cdot q_i$$

בכל שלב נובע מסעיף 4 בטענה האחרונה (1.7) שמתקיים $\gcd(r_{i+2}, r_{i+1}) = \gcd(r_{i+1}, r_i) = \ldots = \gcd(r_0, r_1)$, וגם $0 \leq r_{i+2} < r_{i+1}$ (לכן האלגוריתם מוכרח להיעצר בשלב כלשהו שהרי מדובר במספרים שלמים).

- יהיו $a_i, b_i \in \mathbb{Z}$ כך שמתקיים:

$$r_{i+2} = a_i \cdot r_0 + b_i \cdot r_{i+1}$$

נסביר כיצד למצוא את אותם n_i ו-m_i:

  - אם $i = 0$ אז נגדיר $a_0 := 1$ ו-$b_0 := -q_0$ ואכן מתקיים $r_2 = 1 \cdot r_0 - q_0 \cdot r_1$.
  - אחרת, נזכור ש-$r_{i+1} = a_{i-1} \cdot r_0 + b_{i-1} \cdot r_1$ וגם $r_i = a_{i-2} \cdot r_0 + b_{i-2} \cdot r_1$, ומכיוון ש-$r_{i+2} = r_i - q_i \cdot r_{i+1}$ ניתן להציג את r_{i+2} כך:

$$\begin{aligned} r_{i+2} = r_i - r_{i+1} \cdot q_i &= (a_{i-2} \cdot r_0 + b_{i-2} \cdot r_1) - (a_{i-1} \cdot r_0 + b_{i-1} \cdot r_1) \cdot q_i \\ &= (a_{i-2} - q_i \cdot a_{i-1}) \cdot r_0 + (b_{i-2} - q_i \cdot b_{i-1}) \cdot r_1 \end{aligned}$$

ולכן נגדיר $a_i = a_{i-2} - q_i \cdot a_{i-1}$ ו-$b_i := b_{i-2} - q_i \cdot b_{i-1}$.

- נגדיר את i להיות $i+1$ ונעבור לשלב הבא בלולאה.

כעת מתקיים $r_{i+1} = 0$, כלומר:

$$0 = r_{i+1} = r_{i-1} - r_i \cdot q_{i-1}$$

וממילא:

$$r_i = \gcd(r_{i+1}, r_i) = \gcd(r_i, r_{i-1}) = \ldots = \gcd(r_0, r_1)$$

בנוסף מתקיים:

$$\gcd(r_0, r_1) = r_i = a_{i-2} \cdot n + b_{i-2} \cdot m$$

ולכן נחזיר את r_i, a_{i-2}, b_{i-2} ונסיים. ■

2 המספרים הראשוניים

2.1 התחלה

יהי $2 \leq n \in \mathbb{N}$, נרצה למצוא את כל המספרים האי-פריקים הקטנים או שווים ל-n. להלן פירוט של אלגוריתם "הנפה של ארטוסתנס" בפסאודו-קוד, אלגוריתם זה מבצע את המשימה (באופן בלתי יעיל בעליל), לאחר הצגתו נסביר מדוע הוא אכן עושה זאת.

אלגוריתם 3 הנפה של ארטוסתנס

נגדיר $S := \{m \in \mathbb{N} \mid 2 \leq m \leq n\}$ ו-$P := \emptyset$.

- כל עוד S אינה ריקה:
  - נגדיר $a := \min S$.
  - נגדיר את S להיות $S \setminus (a)$ (כלומר נסיר מ-S את כל הכפולות של a - כולל a) ואת P נגדיר להיות $P \cup \{a\}$.

בסיום ריצת הלולאה הקבוצה P תכיל את כל האי-פריקים הקטנים או שווים ל-n.

♣ הסיבה לכך שהאלגוריתם עובד היא שבסיום הריצה כל האיברים ב-P הם איברים שהוגדרו להיות a באיזשהו שלב ולכן לא קיים טבעי קטן מהם (שונה מ-1) המחלק אותם, מכיוון שערכו המוחלט של המחלק מוכרח להיות קטן מזה של המחולק הדבר גורר שכל האיברים ב-P הם אי-פריקים; מצד שני לכל אי-פריק הקטן או שווה ל-n אין מחלקים קטנים ממנו ולכן כל אי-פריק כזה נבחר בשלב כלשהו להיות a וממילא הוא שייך ל-P.

טענה 2.1. לכל $n \in \mathbb{N}$ קיים $m \in \mathbb{N}$ כך ש-$m \mid n$ וגם $m \leq \sqrt{n}$.

♣ טענה זו מראה לנו שניתן לעצור את האלגוריתם לאחר שעוברים את $\sqrt{n}$ שהרי השורשים של כל המספרים האחרים קטנים מ-$\sqrt{n}$ ולכן בהכרח אם הם פריקים כבר מחקנו אותם מן הרשימה.

2.2 חוג השלמים של גאוס

טענה 2.2. הנורמה ב-$\mathbb{Z}[i]$ היא כפלית: לכל $a, b \in \mathbb{Z}[i]$ מתקיים $N(ab) = N(a) \cdot N(b)$.

מסקנה 2.3. האיברים ההפיכים היחידים ב-$\mathbb{Z}[i]$ הם ± 1 ו-$\pm i$.

משפט 2.4. חילוק עם שארית

לכל $a, b \in \mathbb{Z}[i]$ (כאשר $b \neq 0$) קיימים $q, r \in \mathbb{Z}[i]$ כך ש-$a = bq + r$ ו-$N(r) < N(b)$.

♣ לא למדנו את ההוכחה בתרגול אך גיא אמר שהשיטה היא לחלק את a ב-b ללא שארית (כלומר לבצע את החילוק ב-$\mathbb{C}$) ואז לבחור בתור q את האיבר הכי קרוב לתוצאה ב-$\mathbb{Z}[i]$, זו גם הסיבה לכך שאין כאן יחידות: ייתכן ששניים או ארבעה נמצאים באותו מרחק (אך לא יכולים להיות שלושה בלבד באותו מרחק).

טענה 2.5. למספר ראשוני $p\in\mathbb{N}$ יש לכל היותר הצגה אחת כסכום של ריבועים עד כדי שינוי סדר ועד כדי שינוי סימן, כלומר אם ישנן שתי הצגות $p=a^2+b^2$ ו-$p=c^2+d^2$ (כאשר $a,b,c,d\in\mathbb{Z}$) אז מתקיימת אחת משמונה האפשרויות: $a=\pm c$ ו-$b=\pm d$ או ש-$a=\pm d$ ו-$b=\pm d$.[2]

הוכחה. יהי $p\in\mathbb{N}$ ראשוני כך שקיימים $a,b\in\mathbb{Z}$ המקיימים $a^2+b^2=p$.
יהיו $s,t,u,v\in\mathbb{Z}$ כך שמתקיים:

$$a=s\cdot u-t\cdot v,\ \ b=s\cdot v+t\cdot u$$

כלומר:

$$a+b\cdot i=\left(s+t\cdot i\right)\left(u+v\cdot i\right)$$

$$\begin{aligned}\Rightarrow p=a^2+b^2&=N\left(a+b\cdot i\right)\\&=N\left(\left(s+t\cdot i\right)\left(u+v\cdot i\right)\right)\\&=N\left(s+t\cdot i\right)\cdot N\left(u+v\cdot i\right)\\&=\left(s^2+t^2\right)\left(u^2+v^2\right)\end{aligned}$$

השוויון $p=\left(s^2+t^2\right)\left(u^2+v^2\right)$ הוא כבר שוויון בשלמים ולכן מאי-הפריקות של p נובע ש-$s^2+t^2=\pm p$ (ו-$u^2+v^2=\pm 1$) או ש-$s^2+t^2=\pm 1$ (ו-$u^2+v^2=\pm 1$).

נניח בהג"כ ש-$s^2+t^2=\pm p$ ו-$u^2+v^2=\pm 1$, והרי $0\leq u^2+v^2$ ולכן בהכרח $u^2+v^2=1$; בנוסף ניתן להסיק מכאן ש-$u=\pm 1$ (ו-$v=0$) או ש-$u=0$ (ו-$v=\pm 1$).

נניח בהג"כ ש-$u=\pm 1$ ו-$v=0$, מכאן ש-$s=\pm a$ ו-$t=\pm b$.

מכאן ש-$a+b\cdot i$ הוא מספר אי-פריק ב-$\mathbb{Z}\left[i\right]$ וממילא גם הצמוד שלו אי-פריק, נזכור שב-$\mathbb{Z}\left[i\right]$ אי-פריקות שקולה לראשוניות ולכן הם גם ראשוניים.

יהיו $c,d\in\mathbb{Z}$ כך ש-$c^2+d^2=p$, a ו-b היו שרירותיים ולכן גם $c+d\cdot i$ והצמוד שלו הם אי-פריקים וראשוניים, בנוסף מתקיים:

$$\left(c+d\cdot i\right)\left(c-d\cdot i\right)=c^2+d^2=p=a^2+b^2=\left(a+b\cdot i\right)\left(a-b\cdot i\right)$$

מהראשוניות של $a+b\cdot i$ נובע ש-$c\pm d\cdot i\mid a+b\cdot i$ ולכן מאי-הפריקות של $c\pm d\cdot i$ נובע ש-$a+b\cdot i=\pm\left(c+d\cdot i\right)$ או ש-$a+b\cdot i=\pm\left(c-d\cdot i\right)$;[3]

כלומר מתקיים אחד מהשניים: $a=\pm c$ ו-$b=\pm d$. ∎

---

[2] מבחינה פורמלית הביטוי "$a=\pm c$ ו-$b=\pm d$" אומר פירושו "$\left(a=c\wedge b=d\right)\vee\left(a=-c\wedge b=-d\right)$", למרות זאת כאן הכוונה היא גם לאפשרויות '$a=c\wedge b=-d$' ו-'$a=-c\wedge b=d$' וכנ"ל לגבי הביטוי "$b=\pm d$ או ש-$a=\pm d$".

[3] לא ייתכן ש-$a+b\cdot i$ הוא איבר הפיך מפני שההפיכים היחידים ב-$\mathbb{Z}\left[i\right]$ הם ± 1 ו-$\pm i$ ולכן שם $a+b\cdot i$ היה איבר הפיך היינו מקבלים ש-$p=1$.

2.3 המשפט היסודי של האריתמטיקה

טענה 2.6. יהי $p\in\mathbb{Z}$ מספר אי-פריק, ויהי $I\subseteq\mathbb{Z}$ אידיאל המקיים $(p)\subseteq I$, מתקיימת אחת משתי האפשרויות: $I=\mathbb{Z}$ או ש-$I=(p)$.

משפט 2.7. יהי $p\in\mathbb{Z}$, p אי-פריק אם"ם p ראשוני.

♣ שקילות זו אינה נכונה בכל חוג והיא נובעת מהיכולת לחלק עם שארית בחוג השלמים, נביא דוגמה לחוג שבו השקילות אינה מתקיימת.
נסמן $\mathbb{Z}\left[\sqrt{-5}\right]:=\left\{x+y\cdot\sqrt{-5}\mid x,y\in\mathbb{Z}\right\}\subseteq\mathbb{C}$[4], זהו חוג חילופי (הקורא מוזמן לבדוק זאת) ומתקיים בו:

$$6=2\cdot 3=\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$$

2 הוא אי-פריק בחוג זה[5] אך כפי שניתן לראות בבירור מהפירוק שלעיל הוא אינו ראשוני מפני שהוא מחלק את המכפלה $\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$ אך אינו מחלק אף אחד ממרכיביה[6].

♣ בגלל משפט זה נוכל להתייחס לראשוניות ואי-פריקות כתכונה אחת ולכן בכל פעם שנאמר על מספר שהוא ראשוני נתכוון גם לכך שהמספר אי-פריק.

הוכחה. יהי $p\in\mathbb{Z}$.

- $\Leftarrow$
נניח ש-p אי-פריק ויהיו $a,b\in\mathbb{Z}$ כך ש-$p\mid ab$.
נסמן $d:=\gcd(a,p)$, מהגדרה $d\mid p$ ולכן מהעובדה ש-p אי-פריק נובע ש-$d=1$ או ש-$d=\pm p$.
אם $d=1$ אז p ו-a זרים ולכן מסעיף 5 בטענה 1.7 נובע ש-$p\mid b$, ואם $d=\pm p$ אז מהגדרת ה-gcd p מחלק את a.
- $\Rightarrow$
נניח ש-p ראשוני ויהי $a\in\mathbb{Z}$ כך ש-$a\mid p$.
יהי $q\in\mathbb{Z}$ כך ש-$p=aq$, א"כ מתקיים $p\mid aq$ ולכן מהראשוניות של p נובע ש-$p\mid a$ או ש-$p\mid q$.
אם $p\mid a$ אז מכיוון שגם $a\mid p$ נדע ש-$a=\pm p$ ואם $p\mid q$ אז מאותה סיבה ($q\mid p$) נדע ש-$q=\pm p$ וממילא $a=\pm 1$.

■

[4] לשם העניין נגדיר $\sqrt{-5}:=i\cdot\sqrt{5}$ למרות שבניגוד לשורש הממשי במרוכבים אין דרך להפריד בין $i\cdot\sqrt{5}$ ל-$-i\cdot\sqrt{5}$ - הריבוע של שניהם הוא -5 ואין ביניהם חיובי ושלילי כי $\mathbb{C}$ אינו שדה סדור.

[5] נניח שקיים פירוק $2=\left(a+b\cdot\sqrt{-5}\right)\left(c+d\cdot\sqrt{-5}\right)$, א"כ:

$$4=|2|^2=2\cdot\overline{2}=\left(a+b\cdot\sqrt{-5}\right)\left(a-b\cdot\sqrt{-5}\right)\left(c+d\cdot\sqrt{-5}\right)\left(c-d\cdot\sqrt{-5}\right)=\left(a^2+5b^2\right)\left(c^2+5d^2\right)$$

וזה כבר פירוק ב-$\mathbb{Z}$, אבל אנחנו יודעים שהפירוק היחיד של 4 ב-$\mathbb{Z}$ ולכן נקבל ש-$2=a^2+5b^2$ כעת אם $b\neq 0$ אז $a^2+5b^2\geq 5>2$ ואם $b=0$ נקבל שקיים $a\in\mathbb{Z}$ כך ש-$a^2=2$.

[6] $\frac{1}{2}\pm\frac{\sqrt{-5}}{2}\notin\mathbb{Z}[-5]$.

למה 2.8. יהי $p\in\mathbb{Z}$ מספר ראשוני ויהיו $a_1,a_2,\ldots,a_n\in\mathbb{Z}$ כך שמתקיים $p\mid a_1\cdot a_2\cdot\ldots\cdot a_n$, קיים $n\geq i\in\mathbb{N}$ כך ש-$p\mid a_i$.

משפט 2.9. המשפט היסודי של האריתמטיקה (פריקות חד-ערכית)

יהי $n\in\mathbb{Z}\setminus\{-1,1,0\}$, קיימים $p_1,p_2,\ldots p_r\in\mathbb{Z}$ ראשוניים יחידים (עד כדי שינוי סדר ועד כדי שינוי סימן) אך לאו דווקא שונים זה מזה כך שמתקיים:

$$n=\prod_{i=1}^{r}p_i$$

כלומר אם מתקיים גם $n=q_1\cdot q_2\cdot\ldots\cdot q_s$ (כאשר $q_1,q_2,\ldots q_s\in\mathbb{Z}$ ראשוניים) אז קיימת פונקציה הפיכה $f:\{i\in\mathbb{N}\mid i\leq r\}\to\{i\in\mathbb{N}\mid i\leq s\}$ כך שלכל $r\geq i\in\mathbb{N}$ מתקיים $q_{f(i)}=\pm p_i$.

- ♣ זו אחת הסיבות לכך שאיננו רוצים להגדיר את 1 כראשוני, אחרת לא תהיה לנו פריקות חד-ערכית.
- ♣ קל יותר לנסח את המשפט כך: לכל $0\neq n\in\mathbb{Z}$ [7] קיימת הצגה יחידה בצורה הבאה:

$$n=\operatorname{sgn}(n)\cdot\prod_{i=1}^{r}p_i^{e_i}$$

כאשר $p_1,p_2,\ldots,p_r\in\mathbb{N}$ הם מספרים ראשוניים המקיימים $p_1<p_2<\ldots<p_r$ ו-$e_1,e_2,\ldots,e_r\in\mathbb{N}$.

הוכחה. יהי $n\in\mathbb{Z}\setminus\{-1,1,0\}$.
ניתן להוכיח באינדוקציה שניתן להציג כל מספר שלם כמכפלה של אי-פריקים[8], א"כ יהיו $p_1,p_2,\ldots p_r,q_1,q_2,\ldots q_s\in\text{Prime}$ כך שמתקיים:

$$\prod_{i=1}^{r}p_i=n=\prod_{j=1}^{s}q_j$$

נגדיר פונקציה $f:\{i\in\mathbb{N}\mid i\leq r\}\to\{i\in\mathbb{N}\mid i\leq s\}$ באופן אינדוקטיבי.
נסמן $i:=1$

- לכל $r\geq i\in\mathbb{N}$:
  - מהלמה האחרונה נובע שקיים $s\geq j\in\mathbb{N}$ כך ש-$q_j=\pm p_i$, יהי j כנ"ל ונסמן $f(i):=j$.
  - כעת נסיר מהמכפלה באגף שמאל את p_i ומאגף ימין נסיר את q_j ושוב נקבל שוויון עד כדי סימן כך ש-q_j כבר אינו מופיע מופיע במכפלה הימנית ומכאן שהפונקציה שנגדיר תהיה חח"ע.
  - נעבור לשלב הבא בלולאה.
- כעת אגף שמאל הוא המכפלה הריקה השווה ל-1 ולכן גם אגף ימין שווה ל-1, כלומר $s=r$ ומכאן ש-f על ומכיוון שהיא חח"ע הרי שהיא הפיכה.

■

- ♣ שימו לב: בשלב הראשון של ההוכחה (לפני ההגדרה האינדוקטיבית של f) השתמשנו בתכונת ה**אי-פריקות** ובשלב השני השתמשנו בלמה שמבוססת על תכונת ה**ראשוניות**, ההוכחה לא הייתה עובדת אלמלא השקילות בין שתי התכונות הללו וכפי שכבר הזכרנו קיימים חוגים שבהם הן אינן שקולות.

[7] את 1 ניתן לייצג באמצעות במכפלה הריקה $\prod_{i=1}^{0}p_i:=1$ ואת -1 באמצעות הנגדי שלה $-\prod_{i=1}^{0}p_i=-1$.
[8] מפרקים לגורמים עד שכבר א"א לחלק מפני שכל הגורמים אי-פריקים.

למה 2.10. יהיו $0 \neq a,b \in \mathbb{Z}$, נסמן $n := ab$ ויהי $p \in \mathbb{Z}$ מספר ראשוני, מתקיים $\mathrm{Ord}_p(a) + \mathrm{Ord}_p(b) = \mathrm{Ord}_p(n)$.

טענה 2.11. יהיו $0 \neq a,b \in \mathbb{Z}$, מתקיים $a \mid b$ אם"ם $\mathrm{Ord}_p(a) \leq \mathrm{Ord}_p(b)$ לכל $p \in \mathbb{Z}$ ראשוני.

מסקנה 2.12. יהיו $0 \neq a,b \in \mathbb{Z}$ ויהיו $p_1,p_2,\ldots,p_r \in \mathbb{N}$ מספרים ראשוניים ו-$e_1,e_2,\ldots,e_r,f_1,f_2,\ldots,f_r \in \mathbb{N}_0$ כך שמתקיים:

$$a = \mathrm{sgn}(a) \cdot \prod_{i=1}^{r} p_i^{e_i}$$
$$b = \mathrm{sgn}(b) \cdot \prod_{i=1}^{r} p_i^{f_i}$$

במקרה כזה מתקיים:

$$\gcd(a,b) = \prod_{i=1}^{r} p_i^{\min\{e_i,f_i\}}$$
$$\mathrm{lcm}(a,b) = \prod_{i=1}^{r} p_i^{\max\{e_i,f_i\}}$$

♣ מכאן נובע שמתקיים גם:

$$\mathrm{lcm}(a,b) = \frac{|a \cdot b|}{\gcd(a,b)}$$

שהרי לכל $r \geq i \in \mathbb{N}$ מתקיים $\max\{e_i,f_i\} + \min\{e_i,f_i\} = e_i + f_i$.

מסקנה 2.13. יהיו $0 \neq a,b \in \mathbb{Z}$ כך ש-a חופשי מריבועים ו-$a \mid b^2$, מתקיים גם $a \mid b$.

משפט 2.14. לכל $1 < n \in \mathbb{N}$ חופשי מריבועים מתקיים $\sqrt{n} \notin \mathbb{Q}$.

הוכחה. יהי $1 < n \in \mathbb{N}$ חופשי מריבועים ונניח בשלילה ש-$\sqrt{n} \in \mathbb{Q}$.
יהיו $p,q \in \mathbb{N}$ כך ש-$\frac{p}{q}$ היא ההצגה המצומצמת של $\sqrt{n}$ (כלומר $\gcd(p,q) = 1$).

$$\Rightarrow \frac{p^2}{q^2} = \left(\frac{p}{q}\right)^2 = n$$
$$\Rightarrow p^2 = nq^2$$
$$\Rightarrow n \mid p^2$$

כעת, מכיוון ש-n חופשי מריבועים נדע שמתקיים $n \mid p$, א"כ קיים $k \in \mathbb{N}$ כך ש-$p = nk$, יהי k כנ"ל.

$$\Rightarrow n^2k^2 = p^2 = nq^2$$
$$\Rightarrow k^2 n = q^2$$
$$\Rightarrow n \mid q^2$$

ושוב מאותה סיבה נקבל ש-$n \mid q$, כלומר n מחלק הן את p והן את q בסתירה לכך ש-$\gcd(p,q) = 1$ ו-$1 < n$.
מכאן שהנחת השלילה אינה נכונה ו-$\sqrt{n} \notin \mathbb{Q}$. ■

מסקנה 2.15. לכל $n \in \mathbb{N}$ שאינו מספר ריבועי מתקיים $\sqrt{n} \notin \mathbb{Q}$.

הוכחה. יהי $n \in \mathbb{N}$ שאינו מספר ריבועי ויהיו $a,b,s \in \mathbb{N}$ כך ש-$n = ab$, b חופשי מריבועים, a הוא מספר ריבועי[9] ו-$s = \sqrt{a}$.

[9] ניתן בהכרח לפרק את n בצורה זו משום שלכל ראשוני p בפירוק של n כך ש-$\mathrm{Ord}_p(n) = 1$ "נכניס" ל-b; ועבור כל ראשוני q בפירוק של n כך ש-$\mathrm{Ord}_q(n) \geq 2$ "נכניס" את q בחזקת הזוגי הגדול ביותר שקטן או שווה ל-$\mathrm{Ord}_q(n)$ ל-a (נגדיר $t := 2 \cdot \left\lfloor \frac{\mathrm{Ord}_q(n)}{2} \right\rfloor$ ואת q^t "נכניס" ל-a"), ואת השאר (q^1 או q^0) "נכניס" ל-b.

נשים לב לכך שמתקיים $\sqrt{n}=\sqrt{ab}=\sqrt{a}\cdot\sqrt{b}=s\cdot\sqrt{b}$, אנחנו יודעים ש-$s\in\mathbb{Q}$ ומהמשפט נובע ש-$\sqrt{b}\notin\mathbb{Q}$, מכאן שגם $s\cdot\sqrt{b}\notin\mathbb{Q}$ שהרי $\mathbb{Q}$ הוא שדה[10]. ■

טענה 2.16. לכל $0\neq a,b\in\mathbb{Z}$ ולכל $p\in\mathbb{Z}$ ראשוני מתקיים $\mathrm{Ord}_p\left(a+b\right)\geq\min\left\{\mathrm{Ord}_p\left(a\right),\mathrm{Ord}_p\left(b\right)\right\}$.

2.4 שכיחות המספרים הראשוניים

משפט 2.17. קיימים אינסוף ראשוניים, כלומר קבוצת המספרים הראשוניים היא קבוצה אינסופית.

הראשון שהוכיח את המשפט היה אוקלידס, אנחנו נראה שתי הוכחות: הראשונה היא ההוכחה של אוקלידס והיא פשוטה יחסית והאחרת (של אוילר) מערבת כלים כבדים של חשבון אינפיניטסימלי.

הוכחה. הוכחה 1 - אוקלידס

נניח בשלילה שקבוצת הראשוניים היא קבוצה סופית ויהיו $p_1,p_2,\ldots,p_r\in\mathbb{Z}$ כל הראשוניים הללו.

נתבונן במספר:

$$a:=1+\prod_{i=1}^{r}p_i$$

מהמשפט היסודי של האריתמטיקה יש ל-a הצגה כמכפלה של ראשוניים ולכן בהכרח קיים ראשוני המחלק אותו, אבל ראשוני כזה אינו יכול להיות אחד מאלו שמופיעים במכפלה שלעיל בסתירה לכך שאלו כל הראשוניים בכלל.

מכאן שהנחת השלילה אינה נכונה וקבוצת הראשוניים היא אינסופית. ■

הוכחה. הוכחה 2 - אוילר

נניח שקבוצת הראשוניים היא קבוצה סופית ויהיו $p_1,p_2,\ldots,p_r\in\mathbb{N}$ כל הראשוניים הטבעיים בקבוצה.

ע"פ הנוסחה לסכום של סדרה הנדסית מתכנסת מתקיים:

$$\prod_{i=1}^{r}\frac{1}{1-\frac{1}{p_i}}=\prod_{i=1}^{r}\left(\sum_{n=0}^{\infty}\frac{1}{\left(p_i\right)^n}\right)$$

תהא $\left(a_n\right)_{n=1}^{\infty}$ סדרה המוגדרת ע"י (לכל $n\in\mathbb{N}$):

$$a_n:=\prod_{i=1}^{r}\left(\sum_{j=0}^{m_n}\frac{1}{\left(p_i\right)^j}\right)$$

כאשר $\left(m_n\right)_{n=1}^{\infty}$ היא סדרה המוגדרת ע"י $m_n:=\max\left\{\mathrm{Ord}_{p_i}\left(n\right)\mid r\geq i\in\mathbb{N}\right\}$ לכל $n\in\mathbb{N}$, כלומר m_n הוא החזקה הגדולה ביותר שבה ראשוני כלשהו מחלק את n.

$$\Rightarrow\lim_{n\to\infty}a_n=\prod_{i=1}^{r}\left(\sum_{n=0}^{\infty}\frac{1}{\left(p_i\right)^n}\right)=\prod_{i=1}^{r}\frac{1}{1-\frac{1}{p_i}}$$

בנוסף, לכל $N\in\mathbb{N}$ ולכל $N\geq n\in\mathbb{N}$, $\frac{1}{n}$ מופיע במכפלה:

$$a_N:=\prod_{i=1}^{r}\left(\sum_{j=0}^{m_N}\frac{1}{\left(p_i\right)^j}\right)=\sum_{\forall i\leq r:\ 0\leq e_i\leq m_n}\prod_{i=1}^{r}\frac{1}{\left(p_i\right)^{e_i}}$$

ומזה נובע שלכל $N\in\mathbb{N}$ מתקיים[11]:

$$a_N\geq\sum_{n=1}^{N}\frac{1}{n}$$

[10] מהסגירות לחילוק באיבר שונה מאפס נובע שאם $s\cdot\sqrt{b}\in\mathbb{Q}$ אז גם $\sqrt{b}=\frac{s\cdot\sqrt{b}}{s}\in\mathbb{Q}$ ($s\neq0$ שכן $s^2\cdot b=n\neq0$).

[11] נזכור שכל האיברים במכפלה חיוביים ושלכל $N\in\mathbb{N}$ מתקיים $m_N\leq N$.

כעת נזכור ש-$\left(a_n\right)_{n=1}^{\infty}$ היא סדרה מתכנסת ושהטור ההרמוני הוא טור חיובי ולכן אי-השוויון הנ"ל גורר את התכנסות הטור ההרמוני בסתירה לכך שאנו יודעים שאינו מתכנס.

מכאן שהנחת השלילה אינה נכונה וקבוצת הראשוניים היא אינסופית. ■

♣ זוהי הגרסה המפורמלת של ההוכחה שכתב אוילר:

$$\sum_{n=1}^{\infty}\frac{1}{n}=\prod_{p\in\text{Prime}}\left(\sum_{n=0}^{\infty}\frac{1}{p^n}\right)$$

משפט 2.18. לכל $n\in\mathbb{N}$ קיימים שני ראשוניים עוקבים[12] $p,p'\in\mathbb{N}$ (כך ש-$p<p'$) כך ש-$p'-p>n$, כלומר קיימים מרווחים גדולים כרצוננו בין שני ראשוניים עוקבים.

הוכחה. יהי $n\in\mathbb{N}$, נסמן $m:=n+1$ ונתבונן בסדרת המספרים העוקבים הבאה:

$$\left(m!+2,m!+3,\ldots,m!+m\right)$$

זוהי סדרה באורך n שכל איבריה פריקים שכן האיבר הראשון מתחלק ב-2, השני ב-3 וכן הלאה עד האיבר האחרון שמתחלק ב-$n+1$. ■

טענה 2.19. לכל $n\in\mathbb{N}$ פריק גם $M_n=2^n-1$ (מספר מרסן ה-n-י) הוא מספר פריק.

הוכחה. יהי $n\in\mathbb{N}$ פריק ויהיו $1<a,b\in\mathbb{N}$ כך ש-$a\cdot b=n$.

$$\begin{aligned}\Rightarrow M_n&=2^{a\cdot b}-1=\left(2^a\right)^b-1^b\\&=\left(2^a-1\right)\cdot\left(2^{0\cdot a}+2^{1\cdot a}+2^{2a}+\ldots+2^{(b-1)\cdot a}\right)\end{aligned}$$

והרי $a>1$ ולכן הגורם השמאלי גדול מ-1 ו-$b-1>0$ ולכן הגורם הימני גדול מ-1, כלומר מצאנו פירוק לא טריוויאלי של M_n ועל כן M_n פריק. ■

טענה 2.20. יהי $n\in\mathbb{N}$, אם $F_n=2^n+1$ (מספר פרמה ה-n-י) ראשוני אז קיים $m\in\mathbb{N}_0$ כך ש-$n=2^m$.

הוכחה. נניח ש-F_n ראשוני, כמו לכל טבעי גם ל-n קיימים $m\in\mathbb{N}_0$ ו-$k\in\text{Odd}$ כך ש-$n=2^m\cdot k$, יהיו m ו-k כנ"ל ונסמן $u:2^m$.

$$\begin{aligned}\Rightarrow F_n&=2^{u\cdot k}+1=\left(2^u\right)^k-(-1)^k\\&=\left(2^u-(-1)\right)\cdot\sum_{j=0}^{k-1}\left(2^u\right)^j\cdot(-1)^{k-1-j}\\&=\left(2^u+1\right)\cdot\sum_{j=0}^{k-1}\left(2^u\right)^j\cdot(-1)^{k-1-j}\end{aligned}$$

כעת, אם $k>1$ אז $k-1>1$ (נזכור ש-k אי-זוגי) ולכן הגורם הימני שונה מ-±1 ומכיוון שהגורם השמאלי ודאי שונה מ-±1 הרי שמצאנו פירוק לא טריוויאלי של F_n בסתירה להיות F_n אי-פריק, א"כ בהכרח מתקיים $k=1$, כלומר $n=2^m\cdot k=2^m$. ■

לכל $x\in[0,\infty)$ נסמן ב-$\pi\left(x\right)$ את כמות המספרים הראשוניים בקטע $[0,x]$ (כלומר הגדרנו פונקציה $\pi:[0,\infty)\to\mathbb{N}_0$).

למה 2.21. לכל $m\in\mathbb{N}$ מתקיים:

$$1+\sum_{k=1}^{m}\frac{2^k}{\ln\left(2^k\right)}\leq3\cdot\frac{2^m}{\ln\left(2^m\right)}$$

---

[12] לכל ראשוני q שונה מהם מתקיים $q<p$ או ש-$p'<q$.

הוכחה. נוכיח את הלמה באינדוקציה על m.

- עבור $m \in \{1,2,3\}$ נשים לב לכך שמתקיים:

$$1 < \frac{2}{\ln(2)} = \frac{2 \cdot 2}{2 \cdot \ln(2)} = \frac{2^2}{\ln(2^2)}$$

ולכן גם:

$$1 + \frac{2}{\ln(2)} < 3 \cdot \frac{2}{\ln(2)}$$

וכמו כן גם:

$$1 + \frac{2}{\ln(2)} + \frac{2^2}{\ln(2^2)} = 1 + 2 \cdot \frac{2}{\ln(2)} < 3 \cdot \frac{2}{\ln(2)} = 3 \cdot \frac{2^2}{\ln(2^2)}$$

בנוסף מתקיים:

$$\begin{aligned} 1 \leq \frac{4}{3 \cdot \ln(2)} &= \frac{4}{3} \cdot \frac{1}{\ln(2)} = \frac{1}{2} \cdot \frac{2^3}{3 \cdot \ln(2)} \\ \frac{2}{\ln(2)} + \frac{2^2}{\ln(2^2)} &= 2 \cdot \frac{2}{\ln(2)} = \frac{3}{2} \cdot \frac{2^3}{3 \cdot \ln(2)} \end{aligned}$$

וממילא:

$$1 + \frac{2}{\ln(2)} + \frac{2^2}{\ln(2^2)} + \frac{2^3}{\ln(2^3)} \leq 3 \cdot \frac{2^3}{3 \cdot \ln(2)}$$

- כעת יהי $3 \leq m \in \mathbb{N}$, נניח באינדוקציה שהטענה נכונה עבור m ונוכיח עבור $m+1$:

$$\begin{aligned} 1 + \sum_{k=1}^{m+1} \frac{2^k}{\ln(2^k)} &= \frac{2^{m+1}}{\ln(2^{m+1})} + 1 + \sum_{k=1}^{m} \frac{2^k}{\ln(2^k)} \leq \frac{2^{m+1}}{\ln(2^{m+1})} + 3 \cdot \frac{2^m}{\ln(2^m)} \\ &= 2 \cdot \frac{2^m}{(m+1) \cdot \ln(2)} + 3 \cdot \frac{2^m}{m \cdot \ln(2)} \\ &= \frac{2^m}{\ln(2)} \cdot \left(\frac{2}{m+1} + \frac{3}{m} \right) = \frac{2^m}{\ln(2)} \cdot \frac{2m + 3m + 3}{m \cdot (m+1)} \\ &\leq \frac{2^m}{\ln(2)} \cdot \frac{2m + 3m + 3}{m \cdot (m+1)} \leq \frac{2^m}{\ln(2)} \cdot \frac{6m}{m \cdot (m+1)} \\ &\leq \frac{2^m}{\ln(2)} \cdot \frac{6}{m+1} = 3 \cdot \frac{2^{m+1}}{(m+1) \cdot \ln(2)} = 3 \cdot \frac{2^{m+1}}{\ln(2^{m+1})} \end{aligned}$$

■

למה 2.22. לכל $n \in \mathbb{N}$ מתקיים:

$$\mathrm{Ord}_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

♣ אמנם מבחינה פורמלית זהו סכום אינסופי אך לכל $k \in \mathbb{N}$ כך ש-$\log_p n < k$ מתקיים $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$.

משפט 2.23. משפט צ'בישב[13]

קיימים $A,B\in\mathbb{R}$ כך ש-$A<B$ ולכל $2\le x\in\mathbb{R}$ מתקיים:

$$A\cdot\frac{x}{\ln x}\le\pi\left(x\right)\le B\cdot\frac{x}{\ln x}$$

♣ צ'בישב הראה באמצע המאה ה-19 ש-$A=\frac{7}{8}$ ו-$B=\frac{9}{8}$ מקיימים את הנדרש, בכיתה הוכחנו את המשפט עבור $A=\frac{1}{2}\cdot\ln 2$ ו-$B=6\cdot\ln 2$.

♣ בנוסף, צ'בישב הוכיח שאם הגבול $\lim_{x\to\infty}\frac{\pi\left(x\right)}{\frac{x}{\ln x}}$ קיים אז הוא שווה ל-1[14] אולם ההוכחה של משפט זה, הלא הוא משפט המספרים הראשוניים, נאלצה לחכות עד לשנת 1896 שאז הוכחה בכלים אנליטיים (אני מנחש שזו הסיבה לכך שמקובל להגדיר את הפונקציה π על $[0,\infty)$ ולא על $\mathbb{N}$).

♣ החסמים של צ'בישב היו כה טובים עד שאפשרו לו להוכיח לראשונה את נכונותה של **השערת ברטראן**[15] **(הנקראת מאז גם "משפט ברטראן-צ'בישב):**
לכל $3<n\in\mathbb{N}$ קיים $p\in\mathbb{N}$ ראשוני המקיים $n\le p\le 2n$, ההוכחה מסתמכת על משפט צ'בישב ולמעשה ממשפט המספרים הראשוניים נובעת טענה חזקה יותר האומרת שלכל $0<\varepsilon\in\mathbb{R}$ קיים $N\in\mathbb{N}$ כך שלכל $N<n\in\mathbb{N}$ יש לפחות ראשוני אחד בקטע $(n,n+\varepsilon\cdot n)$.

הוכחה. נסמן $A:=\frac{1}{2}\cdot\ln 2$ ו-$B:=6\cdot\ln 2$ ונוכיח שלכל $1<x\in\mathbb{R}$ מתקיים:

$$A\cdot\frac{x}{\ln x}\le\pi\left(x\right)\le B\cdot\frac{x}{\ln x}$$

נזכור בכל שלב של ההוכחה שהפונקציה $\frac{x}{\ln x}$ עולה ממש בתחום $[e,\infty)$ ויורדת בתחום $(1,e]$.
נוכיח תחילה עבור החסם מלעיל (B).
יהי $n\in\mathbb{N}$, נסמן $N:=\begin{pmatrix}2n\\n\end{pmatrix}$.

$$\Rightarrow N\le\sum_{k=0}^{2n}\begin{pmatrix}2n\\k\end{pmatrix}=\left(1+1\right)^{2n}$$

$$\Rightarrow N\le 2^{2n}$$

נסמן $P:=\left\{p\in\text{Prime}\mid n<p\le 2n\right\}$, לכל ראשוני $p\in P$ מתקיים $p\mid N$ ו-$\text{Ord}_p\left(N\right)=1$ וזאת משום ש-p מחלק את המכפלה $\prod_{i=n+1}^{2n}i$ אך p^2 אינו מחלק את המכפלה ובנוסף p אינו מחלק אף אחד מהאיברים ב-$n!$.

$$\Rightarrow\prod_{p\in P}p\le N\le 2^{2n}$$

$$\Rightarrow\sum_{p\in P}\ln\left(p\right)\le\ln\left(N\right)\le\ln\left(2^{2n}\right)=2n\cdot\ln\left(2\right)$$

נניח כרגע ש-$n>1$,

$$\Rightarrow\ln\left(n\right)\cdot\left(\pi\left(2n\right)-\pi\left(n\right)\right)=\ln\left(n\right)\cdot\left|P\right|\le\sum_{p\in P}\ln\left(p\right)\le 2n\cdot\ln\left(2\right)$$

$$\Rightarrow\pi\left(2n\right)-\pi\left(n\right)=\frac{2n\cdot\ln\left(2\right)}{\ln\left(n\right)}=2\cdot\ln\left(2\right)\cdot\frac{n}{\ln n}$$

---

[13] ערך בוויקיפדיה: פפנוטי צ'בישב.
[14] כלומר שאם מוכנים לוותר על הדרישה שאי-השוויונות יתקיימו לכל $1<x\in\mathbb{R}$ ומוכנים להסתפק בדרישה שקיים $M\in\mathbb{R}$ כך שאי-השוויונות יתקיימו החל מ-M, אז ניתן להשתמש בכל שני קבועים המקיימים $A<1<B$ (כמובן שככל ש-A ו-B יהיו קרובים יותר ל-1 נזדקק ל-M גדול יותר).
[15] ערך בוויקיפדיה: ז'וזף ברטראן.

n הנ"ל היה שרירותי ולכן הנ"ל נכון לכל $1 < n \in \mathbb{N}$, בפרט לכל $k \in \mathbb{N}$ מתקיים:

$$\pi\left(2^{k+1}\right) - \pi\left(2^{k}\right) = 2 \cdot \ln(2) \cdot \frac{2^k}{\ln\left(2^k\right)}$$

ומכאן ע"פ למה 2.21 שלכל $m \in \mathbb{N}$ מתקיים:

$$\pi\left(2^{m+1}\right) = \sum_{k=0}^{m}\left(\pi\left(2^{k+1}\right) - \pi\left(2^{k}\right)\right) = 2 \cdot \ln(2) \cdot \left(1 + \sum_{k=1}^{m} \frac{2^k}{\ln\left(2^k\right)}\right) \leq 6 \cdot \ln(2) \cdot \frac{2^m}{\ln\left(2^m\right)}$$

כעת נשים לב לכך שלכל $e \leq x \in \mathbb{R}$ קיים $m \in \mathbb{N}$ כך ש-$2^m \leq x \leq 2^{m+1}$ ולכן עבור אותו m יתקיים גם:

$$\pi(x) \leq \pi\left(2^{m+1}\right) \leq 6 \cdot \ln(2) \cdot \frac{2^m}{\ln\left(2^m\right)} \leq 6 \cdot \ln(2) \cdot \frac{x}{\ln(x)}$$

ועבור $x \in (1, e)$ מתקיים:

$$\pi(x) \leq 1 \leq 6 \cdot \ln(2) \cdot e = 6 \cdot \ln(2) \cdot \frac{e}{\ln(e)} \leq 6 \cdot \ln(2) \cdot \frac{x}{\ln(x)}$$

כעת נעבור להוכחה עבור החסם מלרע (A) ונעבוד אם $n \in \mathbb{N}$ כללי שאינו בהכרח גדול ממש מ-1.

נזכור שמתקיים $\binom{2n}{k} \leq \binom{2n}{n}$ לכל $2n \geq k \in \mathbb{N}_0$.

$$\Rightarrow \sum_{k=1}^{2n-1} \binom{2n}{k} \leq \binom{2n}{n} \cdot (2n-1)$$

ומכאן שגם:

$$\sum_{k=0}^{2n} \binom{2n}{k} = \binom{2n}{0} + \sum_{k=1}^{2n-1} \binom{2n}{k} + \binom{2n}{2n} = 1 + \sum_{k=1}^{2n-1} \binom{2n}{k} + 1 \leq \binom{2n}{n} \cdot (2n-1) + \binom{2n}{n} = 2n \cdot \binom{2n}{n}$$

$$\Rightarrow \frac{2^{2n}}{2n} = \frac{(1+1)^{2n}}{2n} = \frac{1}{2n} \cdot \sum_{k=0}^{2n} \binom{2n}{k} \leq \binom{2n}{n} = N = \prod_{2n \geq p \in \text{Prime}} p^{\text{Ord}_p(N)}$$

$$\Rightarrow 2n \cdot \ln(2) - \ln(2n) = \ln\left(\frac{2^{2n}}{2n}\right) \leq \ln\left(\prod_{2n \geq p \in \text{Prime}} p^{\text{Ord}_p(N)}\right) = \sum_{2n \geq p \in \text{Prime}} \text{Ord}_p(N) \cdot \ln(p)$$

נזכור ש-N הוגדר להיות $\frac{(2n)!}{(n!)^2} = \binom{2n}{n}$ ולכן לכל $2n \geq p \in \text{Prime}$ מתקיים:

$$\text{Ord}_p(N) = \text{Ord}_p((2n)!) - \text{Ord}\left((n!)^2\right) = \text{Ord}_p((2n)!) - 2 \cdot \text{Ord}(n!)$$

ולכן מלמה 2.22 נובע כי (לכל $2n \geq p \in \text{Prime}$):

$$\text{Ord}_p(N) = \sum_{k=1}^{\infty} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \cdot \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - \left\lfloor 2 \cdot \frac{n}{p^k} \right\rfloor \right)$$

לכל $x \in \mathbb{R}$ מתקיים $\lfloor 2x \rfloor - 2 \cdot \lfloor x \rfloor \in \{0, 1\}$[16], לכן (לכל $2n \geq p \in \text{Prime}$) כל המחוברים בטור הם 1 או 0 ובנוסף יש לכל היותר $\left\lfloor \log_p(2n) \right\rfloor = \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor$ מחוברים שונים מאפס, מכאן שלכל $2n \geq p \in \text{Prime}$ מתקיים:

$$\text{Ord}_p(N) \leq \frac{\ln(2n)}{\ln(p)}$$

[16] אם $0 \leq \lfloor x \rfloor < \frac{1}{2}$ אז $\lfloor 2x \rfloor - 2 \cdot \lfloor x \rfloor = 0$ ואם $\frac{1}{2} \leq \lfloor x \rfloor < 1$ אז $\lfloor 2x \rfloor - 2 \cdot \lfloor x \rfloor = 1$.

$$\Rightarrow 2n\cdot\ln(2)-\ln(2n)\leq\sum_{2n\geq p\in\text{Prime}}\frac{\ln(2n)}{\ln(p)}\cdot\ln(p)=\sum_{2n\geq p\in\text{Prime}}\ln(2n)=\ln(2n)\cdot\pi(2n)$$

$$\Rightarrow\frac{2n}{\ln(2n)}\cdot\ln(2)-1\leq\pi(2n)$$

נניח כעת ש-$n\geq 4$ ונשים לב לכך שמתקיים:

$$\begin{aligned}&\left(\frac{2n}{\ln(2n)}\cdot\ln(2)-1\right)-\left(\frac{2n+2}{\ln(2n+2)}\cdot\frac{\ln(2)}{2}\right)\\&=\left(\frac{2n}{\ln(2n)}-\frac{n+1}{\ln(2n+2)}\right)\cdot\ln(2)-1\\&\geq\left(\frac{2n}{\ln(2n)}-\frac{n+1}{\ln(2n)}\right)\cdot\ln(2)-1\\&\geq\frac{n-1}{\ln(2n)}\cdot\ln(2)-1\geq\frac{4-1}{\ln(2\cdot 4)}\cdot\ln(2)-1\\&=\frac{3}{\ln(2^3)}\cdot\ln(2)-1=\frac{3}{3\cdot\ln(2)}\cdot\ln(2)-1=0\end{aligned}$$

$$\Rightarrow\frac{2n+2}{\ln(2n+2)}\cdot\frac{\ln(2)}{2}\leq\frac{2n}{\ln(2n)}\cdot\ln(2)-1\leq\pi(2n)$$

ושוב n הנ"ל היה שרירותי ולכן הנ"ל נכון לכל $4\leq n\in\mathbb{N}$. לכל $8\leq x\in\mathbb{R}$ קיים $n\in\mathbb{N}$ כך ש-$2n\leq x\leq 2n+2$ ולכן עבור אותו n יתקיים גם:

$$\frac{x}{\ln(x)}\cdot\frac{\ln(2)}{2}\leq\frac{2n+2}{\ln(2n+2)}\cdot\frac{\ln(2)}{2}\leq\pi(2n)\leq\pi(x)$$

בנוסף, מהעובדה ש-$\frac{x}{\ln x}$ עולה בקרן $[e,\infty)$ נקבל שלכל $x\in[e,3)$ מתקיים:

$$\frac{x}{\ln(x)}\cdot\frac{\ln(2)}{2}<\frac{4}{\ln(2^2)}\cdot\frac{\ln(2)}{2}=\frac{4}{2\cdot\ln(2)}\cdot\frac{\ln(2)}{2}=1=\pi(x)$$

ולכל $x\in[3,8)$ נקבל שמתקיים:

$$\frac{x}{\ln(x)}\cdot\frac{\ln(2)}{2}\leq\frac{8}{\ln(8)}\cdot\frac{\ln(2)}{2}=\frac{4}{\ln(2^3)}\cdot\ln(2)=\frac{4}{3\cdot\ln(2)}\cdot\ln(2)<2\leq\pi(x)$$

כמו כן מהעובדה ש-$\frac{x}{\ln x}$ יורדת בקטע $[2,e]$ נקבל שלכל $x\in[2,e)$ מתקיים:

$$\frac{x}{\ln(x)}\cdot\frac{\ln(2)}{2}\leq\frac{2}{\ln(2)}\cdot\frac{\ln(2)}{2}=1=\pi(2)\leq\pi(x)$$

■

2.5 הערה: משפטים והשערות אודות המספרים הראשוניים

♣ **השערת הראשוניים התאומים:** שני ראשוניים עוקבים יקראו תאומים אם ההפרש שלהם הוא 2, השערת הראשוניים התאומים טוענת שקיימים אינסוף כאלה וזוהי בעיה פתוחה במתמטיקה; עם זאת בעשור האחרון הצליחו המתמטיקאים Yitang Zhang, James Maynard וטרנס טאו להוכיח שקיימים אינסוף זוגות ראשוניים שהמרווח ביניהם קטן או שווה ל-246[17]. ממילא קיים מספר $246 \geq n \in \mathbb{N}$ כך שקיימים אינסוף זוגות ראשוניים שזהו ההפרש שלהם (עיקרון שובך היונים).

♣ כמות הראשוניים מהצורה $4n+1$ וזו של הראשוניים מהצורה $4n+3$ משתוות אסימפטוטית בשאיפה לאינסוף, כלומר אם נסמן ב-$f(x)$ את מספר הראשוניים מהצורה $4n+1$ שקטנים או שווים ל-$0 \leq x \in \mathbb{R}$ וב-$g(x)$ אז כמות הראשוניים מהצורה $4n+3$ שקטנים או שווים ל-$0 \leq x \in \mathbb{R}$ נקבל:

$$\lim_{x\to\infty}\frac{f(x)}{g(x)}=1$$

♣ **משפט דיריכלה[18]:** לכל $a,d \in \mathbb{N}$ הזרים זה לזה קיימים אינסוף איברים ראשונים שהם איברים בסדרה החשבונית $(a+dn)_{n=0}^{\infty}$[19].

♣ **משפט גרין-טאו[20]:** לכל $n \in \mathbb{N}$ קיימת סדרה חשבונית באורך n שכל איבריה ראשוניים.

♣ **משפט גרין-טאו-ציגלר[21]:** לכל ממ"ל במקדמים שלמים שאינה תלויה ליניארית שבה מספר הנעלמים עולה על מספר המשוואות ב-2 (לפחות) יש פתרון בו כל הנעלמים מקבלים ערכים ראשוניים.

♣ **משפט טאו-ציגלר[22]:** לכל $P_1,P_2,\ldots,P_n \in \mathbb{Z}[x]$ המקיימים $P_k(0)=0$ לכל $n \geq k \in \mathbb{N}$ קיימים אינסוף זוגות $(x,m) \in \mathbb{Z}^2$ כך ש-$x+P_1(m), x+P_2(m), \ldots, x+P_n(m)$ כולם ראשוניים.

♣ **השערת גולדבך[23]:** לכל $2 < n \in \text{Even}$ קיימים שני ראשוניים שסכומם הוא n.

♣ **הגרסה החלשה של השערת גולדבך[24]:** לכל $5 < n \in \text{Odd}$ קיימים שלושה ראשוניים שסכומם הוא n.
בשנת 2013 הוכחה הגרסה החלשה, כמעט אחרי 300 שנה מאז שהועלתה בהתכתבות בין כריסטיאן גולדבך ללאונרד אוילר, פירוט ניתן למצוא בערך "השערת גולדבך החלשה" (ויקיפדיה).

♣ **משפט Chen[25]:** לכל $2 < n \in \text{Even}$ קיימים $p,q,r \in \mathbb{N}$ ראשוניים כך ש-$n=p+q$ או ש-$n=p+qr$.

---

[17] ז'אנג הוכיח את הטענה עבור 70 מליון ולאחר מכן הורידו שני האחרים את החסם ל-246.
ראו גם: Twin prime conjecture, Polymath8 (ויקיפדיה האנגלית) והשערת המספרים הראשוניים התאומים (ויקיפדיה העברית).

[18] ערך בוויקיפדיה: לז'ן גוסטב פטר יוהאן דיריכלה.

[19] קל מאד להוכיח את הכיוון ההפוך (שאם יש אינסוף ראשוניים בסדרה חשבונית אז הבסיס וההפרש זרים).

[20] ערכים בוויקיפדיה: ראו בהערה הבאה.

[21] ערכים בוויקיפדיה: בן גרין, טרנס טאו ותמר ציגלר.

[22] ערכים בוויקיפדיה: ראו בהערה הקודמת.

[23] ערך בוויקיפדיה: כריסטיאן גולדבך

[24] נקראת גם "השערת גולדבך החלשה", "השערת גולדבך האי-זוגית", "השערת גולדבך המשולשת" ו-"בעיית שלושת הראשוניים"; זוהי הגרסה ה"חלשה" משום שהיא נובעת ישירות מהשערת גולדבך עצמה.

[25] ערך בוויקיפדיה האנגלית: Chen Jingrun.