קירובים דיופנטיים - 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

תודתי נתונה לאורטל פלדמן על הסיכום שכתב בשנת הלימודים תשע"ו,
נעזרתי בו רבות על מנת לכתוב את הסיכום שלפניכם.

* * *

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 התחלה

♣ "בתורת המספרים, קירוב דיופנטי של מספר ממשי נתון הוא מספר רציונלי קרוב אל המספר המבוקש. האנליזה הדיופנטית עוסקת, בין השאר, בקיומם של קירובים דיופנטיים, בטיב הקירוב האפשרי, ובהכללות של הבעיה היסודית. התחום נקרא על שמו של דיופנטוס שהציג בעיות שהפתרונות שלהן דווקא במספרים שלמים." (ציטוט מהערך "קירוב דיופנטי" בוויקיפדיה העברית)

משפט 1.1. לכל $x\in\mathbb{R}$ קיימות סדרת טבעיים עולה ממש $(q_n)_{n=1}^{\infty}$ וסדרת שלמים $(p_n)_{n=1}^{\infty}$ כך שלכל $n\in\mathbb{N}$ מתקיים:

$$\left|x-\frac{p_n}{q_n}\right|<\frac{1}{\left(q_n\right)^2}$$

♣ כלומר קיימת סדרת קירובים טובה כל כך שהיא מקרבת עד כדי ההופכי של ריבוע המכנה ולא רק עד כדי מחצית מההופכי של המכנה.

♣ כמובן ש-$(p_n)_{n=1}^{\infty}$ תהיה סדרת חיוביים אם x חיובי וסדרת שליליים אם x שלילי.

הוכחה. יהי $x\in\mathbb{R}$, אם $x\in\mathbb{Q}$ אז קיימים $a\in\mathbb{Z}$ ו-$b\in\mathbb{N}$ כך ש-$x=\frac{a}{b}$ ואותם a ו-b יקיימו שהסדרות $(n\cdot a)_{n=1}^{\infty}$ ו-$(n\cdot b)_{n=1}^{\infty}$ הן סדרות מתאימות, א"כ נניח ש-$x\notin\mathbb{Q}$.
יהי $Q\in\mathbb{N}$ ונסמן $\alpha_n:=\lfloor nx\rfloor$ ו-$\beta_n:=nx-\lfloor nx\rfloor$ לכל $Q\geq n\in\mathbb{N}$, מהגדרה מתקיים $\beta_n\in(0,1)$ לכל $Q\geq n\in\mathbb{N}$ ולכן מעקרון שובך היונים נובע שקיימים $i,j\in\mathbb{N}\geq Q$ כך ש-$i\neq j$ ומתקיים:

$$0\leq\beta_i-\beta_j\leq\frac{1}{Q}$$

יהיו i ו-j כנ"ל ונבחין כי:

$$(i-j)\cdot x=(\alpha_i+\beta_i)-(\alpha_j+\beta_j)=(\alpha_i-\alpha_j)+(\beta_i-\beta_j)$$

$$\Rightarrow\left|(i-j)\cdot x-(\alpha_i-\alpha_j)\right|=\beta_i-\beta_j\leq\frac{1}{Q}$$
$$\Rightarrow\left|x-\frac{\alpha_i-\alpha_j}{i-j}\right|\leq\frac{\beta_i-\beta_j}{|i-j|}\leq\frac{1}{Q\cdot|i-j|}<\frac{1}{\left(i-j\right)^2}$$

נסמן $p:=\alpha_i-\alpha_j$ ו-$q:=|i-j|$, א"כ מתקיים:

$$\left|x-\frac{p}{q}\right|<\frac{1}{q^2},\ \ \left|x-\frac{p}{q}\right|\leq\frac{1}{q\cdot Q}<\frac{1}{Q}$$

נסמן:

$$\varepsilon:=\min\left\{\left|x-\frac{m}{n}\right|:m\in\mathbb{Z},\ \ Q\geq n\in\mathbb{N}\right\}$$

כלומר ε הוא המרחק בין x לקירוב הטוב ביותר שלו שהמכנה שלו קטן או שווה ל-Q.
יהי $Q'\in\mathbb{N}$ כך ש-$\frac{1}{Q'}<\varepsilon$, Q הנ"ל היה שרירותי ולכן קיימים $p'\in\mathbb{Z}$ ו-$q'\in\mathbb{N}$ כך שמתקיים:

$$\left|x-\frac{p'}{q'}\right|<\frac{1}{q'^2},\ \ \left|x-\frac{p'}{q'}\right|\leq\frac{1}{q'\cdot Q'}<\frac{1}{Q'}<\varepsilon$$

כלומר $\frac{p'}{q'}$ הוא קירוב טוב יותר מכל קירוב שהמכנה שלו קטן או שווה ל-Q ומכאן שבהכרח $q<Q<q'$, מכאן שאכן ניתן לבנות סדרה עולה ממש של טבעיים $(q_n)_{n=1}^{\infty}$ וסדרת שלמים מתאימה $(p_n)_{n=1}^{\infty}$ כך שלכל $n\in\mathbb{N}$ מתקיים:

$$\left|x-\frac{p_n}{q_n}\right|<\frac{1}{(q_n)^2}$$

■

טענה 1.2. קבוצת המספרים האלגבריים היא שדה.

משפט 1.3. משפט ליוביל[1]

יהי $\alpha\in\mathbb{R}$ מספר אלגברי מדרגה $1<d\in\mathbb{N}$,[2] קיים קבוע $0<c\in\mathbb{R}$ כך שלכל $\frac{p}{q}\in\mathbb{Q}$ יתקיים:

$$\left|x-\frac{p}{q}\right|>\frac{c}{q^d}$$

♣ משפט ליוביל הוא משפט חלש למדי במובן שהוא מאפשר קירובים שבהם החזקה במכנה קטנה מ-d אבל גדולה מ-2, המשפט הבא מראה שגם זה לא אפשרי:

משפט. משפט Thue-Siegel-Roth[3]

יהי $\alpha\in\mathbb{R}$ מספר אלגברי מדרגה $1<d\in\mathbb{N}$, לכל $0<\varepsilon\in\mathbb{R}$ קיים קבוע $0<c\in\mathbb{R}$ כך שלכל $\frac{p}{q}\in\mathbb{Q}$ יתקיים:

$$\left|x-\frac{p}{q}\right|>\frac{c}{q^{2+\varepsilon}}$$

הוכחה. יהי $f\in\mathbb{Z}[x]$ פולינום כך ש-$f(\alpha)=0$ וגם $\deg f=d$, א"כ מהעובדה ש-f בעל מקדמים שלמים נובע שלכל $\frac{p}{q}\in\mathbb{Q}$ מתקיים $q^d\cdot f\left(\frac{p}{q}\right)\in\mathbb{Z}$ ולכן לכל $\frac{p}{q}\in\mathbb{Q}$ כך ש-$f\left(\frac{p}{q}\right)\neq 0$ מתקיים:

$$\left|q^d\cdot f\left(\frac{p}{q}\right)\right|\geq 1$$

וממילא גם:

$$\left|f\left(\frac{p}{q}\right)\right|\geq\frac{1}{q^d}$$

נסמן ב-m את החזקה הגדולה ביותר של הפולינום $x-\alpha$ המחלקת את $f(x)$ (מהגדרה $m\geq 1$ מפני ש-α הוא שורש של f ולכן $x-\alpha$ מחלק את $f(x)$), ויהי $g\in\mathbb{R}[x]$ המנה של חלוקת $f(x)$ ב-$(x-\alpha)^m$, כלומר מתקיים (שוויון בין פולינומים ב-$\mathbb{R}[x]$):

$$f(x)=(x-\alpha)^m\cdot g(x)$$

מהגדרה g אינו פולינום האפס[4] ובנוסף, מהגדרת m נובע ש-α אינו שורש של g.

תהא $0<\delta\in\mathbb{R}$ כך ש-$\delta<1$ ולכל $r\in B_\delta(\alpha)$ מתקיים[5]:

$$0<\frac{1}{2}\cdot|g(\alpha)|\leq|g(x)|\leq 2\cdot|g(\alpha)|$$

[1] ערך בוויקיפדיה: ז'וזף ליוביל.
[2] שקול לכך ש-$\alpha\notin\mathbb{Q}$.
[3] ערכים בוויקיפדיה האנגלית: Axel Thue, Carl Ludwig Siegel ו-Klaus Roth.
המשפט הוכח ע"י Roth ע"י שיפור תוצאות קודמות של שני האחרים ושל פרימן דייסון.
[4] אחרת גם f היה פולינום האפס בסתירה לכך שדרגתו גדולה ממש מ-1.
[5] מהרציפות של $|g(x)|$ נובע שאכן קיימת δ כזו.

יהי $\frac{u}{v} \in B_{\delta}\left(\alpha\right)$ מספר רציונלי, מהשורה הקודמת נובע שמתקיים $g\left(\frac{u}{v}\right) \neq 0$ ומכיוון שבהכרח $\alpha \neq \frac{u}{v}$ [6] נדע שגם $\left(\frac{u}{v}-\alpha\right)^{m} \neq 0$ וממילא:

$$f\left(\frac{u}{v}\right)=\left(\frac{u}{v}-\alpha\right)^{m}\cdot g\left(\frac{u}{v}\right)\neq0$$

כפי שראינו בתחילת ההוכחה נובע מזה שמתקיים:

$$\frac{1}{v^{d}}\leq\left|f\left(\frac{u}{v}\right)\right|=\left|\left(\frac{u}{v}-\alpha\right)^{m}\cdot g\left(\frac{u}{v}\right)\right|=\left|\frac{u}{v}-\alpha\right|^{m}\cdot\left|g\left(\frac{u}{v}\right)\right|$$

ומהגדרת δ נקבל שמתקיים גם:

$$\frac{1}{v^{d}}\cdot\frac{1}{2\cdot\left|g\left(\alpha\right)\right|}\leq\frac{1}{v^{d}}\cdot\frac{1}{\left|g\left(\frac{u}{v}\right)\right|}\leq\left|\frac{u}{v}-\alpha\right|^{m}$$

בנוסף, הגדרנו את δ כך ש-$\delta<1$ ולכן מתקיים:

$$\left|\frac{u}{v}-\alpha\right|^{m}<\left|\frac{u}{v}-\alpha\right|=\left|\alpha-\frac{u}{v}\right|$$

$$\Rightarrow\left|\alpha-\frac{u}{v}\right|>\frac{1}{v^{d}}\cdot\frac{1}{2\cdot\left|g\left(\alpha\right)\right|}$$

א"כ נגדיר $c_{1}:=\frac{1}{2\cdot\left|g\left(\alpha\right)\right|}$ ומכיוון ש-$\frac{u}{v}$ היה שרירותי הרי שלכל מספר רציונלי $\frac{p}{q}\in B_{\delta}\left(\alpha\right)$ יתקיים:

$$\left|\alpha-\frac{p}{q}\right|>\frac{c_{1}}{q^{d}}$$

נעבור להוכיח את המשפט עבור רציונליים ב-$\mathbb{Q}\setminus B_{\delta}\left(\alpha\right)$.

הקבוצה $B:=\left\{ n\in\mathbb{N}\mid\frac{1}{n^{d}}>\delta\right\}$ היא קבוצה סופית ולכן קיים $0<c_{2}\in\mathbb{R}$ כך שלכל $b\in B$ ולכל $a\in\mathbb{Z}$ מתקיים:

$$\left|\alpha-\frac{a}{b}\right|>\frac{c_{2}}{b^{d}}$$

יהי c_{2} כנ"ל ומכאן שלכל $\frac{a}{b}\in\mathbb{Q}\setminus B_{\delta}\left(\alpha\right)$: אם $b\in B$ אז c_{2} מקיים את הרצוי ואם $b\notin B$ אז קיים מספר רציונלי $\frac{s}{t}\in B_{\delta}\left(\alpha\right)$ כך ש-$t=b$ ואז ממה שהוכחנו לעיל נובע שמתקיים:

$$\left|\alpha-\frac{a}{b}\right|>\left|\alpha-\frac{s}{t}\right|>\frac{c_{1}}{t^{d}}=\frac{c_{1}}{b^{d}}$$

ולכן c_{2} מקיים את הרצוי. נגדיר $c:=\min\left\{ c_{1},c_{2}\right\} >0$ ומכאן שלכל $\frac{p}{q}\in\mathbb{Q}$ מתקיים:

$$\left|\alpha-\frac{p}{q}\right|>\frac{c}{q^{d}}$$

■

למה 1.4. יהי $x\in\mathbb{R}$, אם קיימים $0<a\in\mathbb{R}$, סדרת טבעיים עולה ממש $\left(q_{n}\right)_{n=1}^{\infty}$ וסדרת שלמים $\left(p_{n}\right)_{n=1}^{\infty}$ המקיימים שלכל $e\in\mathbb{N}$ קיים $n\in\mathbb{N}$ מתקיים:

$$\left|x-\frac{p_{n}}{q_{n}}\right|<\frac{a}{\left(q_{n}\right)^{e}}$$

אז x טרנסצנדנטי.

[6] שהרי $1<d$ ולכן α אינו רציונלי.

הוכחה. נניח שקיימים $0 < a \in \mathbb{R}$, סדרת טבעיים עולה ממש $(q_n)_{n=1}^{\infty}$ וסדרת שלמים $(p_n)_{n=1}^{\infty}$ המקיימים שלכל $e \in \mathbb{N}$ קיים $n \in \mathbb{N}$ מתקיים:

$$\left|x - \frac{p_n}{q_n}\right| < \frac{a}{(q_n)^e}$$

ויהיו $a, (q_n)_{n=1}^{\infty}, (p_n)_{n=1}^{\infty}$ כנ"ל.
כעת נניח בשלילה ש-x אלגברי ונסמן ב-d את דרגתו.
יהי $0 < c \in \mathbb{R}$.
יהי $m \in \mathbb{N}$ כך ש-$\frac{a}{2^m} < c$ ויהי $n \in \mathbb{N}$ כך שמתקיים:

$$\left|x - \frac{p_n}{q_n}\right| < \frac{a}{(q_n)^{m+d}}$$

$$\Rightarrow \left|x - \frac{p_n}{q_n}\right| < \frac{a}{(q_n)^{m+d}} = \frac{a}{(q_n)^m \cdot (q_n)^d} \leq \frac{a}{2^m \cdot (q_n)^d} < \frac{c}{(q_n)^d}$$

c הנ"ל היה שרירותי ולכן הנ"ל נכון לכל $0 < c \in \mathbb{R}$ וזאת בסתירה למשפט ליוביל.
מכאן שהנחת השלילה אינה נכונה ו-x אינו אלגברי, כלומר x טרנסצנדנטי. ■

למה 1.5. יהי $1 < s \in \mathbb{R}$ ותהא $(n_k)_{k=1}^{\infty}$ סדרת טבעיים עולה ממש, לכל $m \in \mathbb{N}$ מתקיים:

$$\sum_{k=m}^{\infty} \frac{1}{s^{n_k}} \leq \frac{1}{s^{n_m}} \cdot \frac{1}{1 - \frac{1}{s}} = \frac{1}{s^{n_m}} \cdot \frac{s}{s-1} = \frac{1}{s^{n_m - 1}} \cdot \frac{1}{s-1}$$

טענה 1.6. יהי $1 < s \in \mathbb{N}$ ותהא $(n_k)_{k=1}^{\infty}$ סדרת טבעיים עולה ממש המקיימת:

$$\lim_{k \to \infty} \frac{n_{k+1}}{n_k} = \infty$$

ונסמן:

$$\alpha := \sum_{k=1}^{\infty} \frac{1}{s^{n_k}}$$

α הוא מספר טרנסצנדנטי.

♣ הדוגמה הקלאסית היא <u>קבוע ליוביל</u> המוגדר ע"י (כאן $s = 10$ ו-$(n_k)_{k=1}^{\infty} = (k!)_{n=1}^{\infty}$):

$$c := \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$$

הוכחה. תהיינה $(p_m)_{m=1}^{\infty}$ו-$(q_m)_{m=1}^{\infty}$ שתי סדרות המוגדרות ע"י (לכל $m \in \mathbb{N}$):

$$p_m = \sum_{k=1}^{m} s^{n_m - n_k},\ \ q_m = s^{n_m}$$

נשים לב ש-$(p_m)_{m=1}^{\infty}$ היא אכן סדרת טבעיים משום שלכל $n \geq k \in \mathbb{N}$ מתקיים $n_m \geq n_k$ וודאי ש-$(q_m)_{m=1}^{\infty}$ גם היא סדרת טבעיים.
נשים לב לכך שלכל $m \in \mathbb{N}$ מתקיים:

$$\frac{p_m}{q_m} = \sum_{k=1}^{m} \frac{1}{s^{n_k}}$$

ומכאן שע"פ למה 1.5 לכל $m \in \mathbb{N}$ מתקיים:

$$\left|\alpha - \frac{p_m}{q_m}\right| = \left|\sum_{k=1}^{\infty} \frac{1}{s^{n_k}} - \sum_{k=1}^{m} \frac{1}{s^{n_k}}\right| = \sum_{k=m+1}^{\infty} \frac{1}{s^{n_k}}$$
$$\leq \frac{1}{s^{n_{m+1}}} \cdot \frac{1}{1-\frac{1}{s}}$$

יהי $e \in \mathbb{N}$ ויהי $m \in \mathbb{N}$ כך ש-$\frac{n_{m+1}}{n_m} > e$ (מהנתון $\frac{n_{k+1}}{n_k} \xrightarrow[k\to\infty]{} \infty$ נובע שאכן קיים m כזה), מכאן ש-$n_{m+1} > n_m \cdot e$ ולכן גם $s^{n_{m+1}} > s^{n_m \cdot e}$ וממילא:

$$\frac{1}{s^{n_{m+1}}} < \frac{1}{s^{n_m \cdot e}} = \frac{1}{(s^{n_m})^e}$$

$$\Rightarrow \left|\alpha - \frac{p_m}{q_m}\right| < \frac{1}{s^{n_{m+1}}} \cdot \frac{1}{1-\frac{1}{s}} < \frac{1}{(s^{n_m})^e} \cdot \frac{1}{1-\frac{1}{s}} = \frac{1}{(q_m)^e} \cdot \frac{1}{1-\frac{1}{s}}$$

e הנ"ל היה שרירותי ולכן הנ"ל נכון לכל $e \in \mathbb{N}$ ומכאן שע"פ למה 1.4 α טרנסצנדנטי. ■

2 סדרות פרי (Farey)

למה 2.1. יהיו $\frac{p}{q}, \frac{p'}{q'} \in \mathbb{Q}$ שברים מצומצמים כך ש-$0 \leq \frac{p}{q} < \frac{p'}{q'} \leq 1$, לכל $r \in \mathbb{Q}$ המקיים $\frac{p}{q} < r < \frac{p'}{q'}$ קיימים $u, v \in \mathbb{N}$ יחידים כך ש-$\gcd(u,v) = 1$ ומתקיים:

$$r = \frac{v \cdot p + u \cdot p'}{v \cdot q + u \cdot q'}$$

הוכחה. תהא $f : (0,\infty) \to \mathbb{R}$ פונקציה המוגדרת ע"י (לכל $t \in (0,\infty)$):

$$f(t) = \frac{p + t \cdot p'}{q + t \cdot q'}$$

מהגדרה מתקיים $\mathrm{Im}(f) = \left(\frac{p}{q}, \frac{p'}{q'}\right)$.

יהיו $t_1, t_2 \in (0,\infty)$ כך ש-$t_1 < t_2$, מתקיים:

$$t_2 \cdot \frac{p}{q} + t_1 \cdot \frac{p'}{q'} < t_1 \cdot \frac{p}{q} + t_2 \cdot \frac{p'}{q'}$$

$$\Rightarrow \frac{t_2 \cdot p \cdot q' + t_1 \cdot p' \cdot q}{q \cdot q'} < \frac{t_1 \cdot p \cdot q' + t_2 \cdot p' \cdot q}{q \cdot q'}$$
$$\Rightarrow t_2 \cdot p \cdot q' + t_1 \cdot p' \cdot q < t_1 \cdot p \cdot q' + t_2 \cdot p' \cdot q$$

$$\Rightarrow p \cdot q + t_2 \cdot p \cdot q' + t_1 \cdot p' \cdot q + t_1 \cdot t_2 \cdot p' \cdot q' < p \cdot q + t_1 \cdot p \cdot q' + t_2 \cdot p' \cdot q + t_1 \cdot t_2 \cdot p' \cdot q'$$
$$\Rightarrow (p + t_1 \cdot p')(q + t_2 \cdot q') < (p + t_2 \cdot p')(q + t_1 \cdot q')$$
$$\Rightarrow f(t_1) = \frac{p + t_1 \cdot p'}{q + t_1 \cdot q'} < \frac{p + t_2 \cdot p'}{p + t_2 \cdot p'} = f(t_2)$$

א"כ f היא פונקציה עולה ממש ולכן היא חח"ע.
יתרה מזאת, לכל $t \in (0, \infty)$ מתקיים:

$$(q + t \cdot q') \cdot f(t) = p + t \cdot p'$$

ומכאן שגם:

$$q \cdot f(t) - p = t \cdot (p' - q' \cdot f(t))$$

וממילא:

$$t = \frac{q \cdot f(t) - p}{p' - q' \cdot f(t)}$$

ולכן מתקיים $f(t) \in \mathbb{Q}$ אם"ם $t \in \mathbb{Q}$ ומכאן ש-f מהווה התאמה חח"ע ועל בין הרציונליים החיוביים לבין הרציונליים בקטע $\left(\frac{p}{q}, \frac{p'}{q'}\right)$.
נבחין כי לכל $u, v \in \mathbb{N}$ מתקיים:

$$f\left(\frac{u}{v}\right) = \frac{p + \frac{u}{v} \cdot p'}{q + \frac{u}{v} \cdot q'} = \frac{v \cdot p + u \cdot p'}{v \cdot q + u \cdot q'}$$

ומכאן שלכל $r \in \left(\frac{p}{q}, \frac{p'}{q'}\right)$ רציונלי קיימים $u, v \in \mathbb{N}$ יחידים[7] כך ש-$\gcd(u, v) = 1$ ומתקיים:

$$r = f\left(\frac{u}{v}\right) = \frac{v \cdot p + u \cdot p'}{v \cdot q + u \cdot q'}$$

■

למה 2.2. יהיו $\frac{p}{q}, \frac{p'}{q'} \in \mathbb{Q}$ שברים מצומצמים כך ש-$0 \leq \frac{p}{q} < \frac{p'}{q'} \leq 1$, יהי $r \in \mathbb{Q}$ המקיים $\frac{p}{q} < r < \frac{p'}{q'}$ ויהיו $u, v \in \mathbb{N}$ כך ש-$\gcd(u, v) = 1$ וגם:

$$r = \frac{v \cdot p + u \cdot p'}{v \cdot q + u \cdot q'}$$

אם $p' \cdot q - q' \cdot p = 1$ אז ההצגה הנ"ל היא ההצגה המצומצמת של r.

הוכחה. נניח כי $p' \cdot q - q' \cdot p = 1$, א"כ מתקיים:

$$p' \cdot (v \cdot q + u \cdot q') - q' \cdot (v \cdot p + u \cdot p') = v \cdot (p' \cdot q - q' \cdot p) + u \cdot (p' \cdot q' - q' \cdot p') = v$$
$$-p \cdot (v \cdot q + u \cdot q') + q \cdot (v \cdot p + u \cdot p') = v \cdot (-p \cdot q + q \cdot p) + u \cdot (-p \cdot q' + q \cdot p') = u$$

מכאן שכל מחלק משותף של $v \cdot p + u \cdot p'$ ו-$v \cdot q + u \cdot q'$ יחלק גם את u ו-v ולכן העובדה ש-$\gcd(u, v) = 1$ אומרת שההצגה הנ"ל היא ההצגה המצומצמת של r. ■

טענה 2.3. יהיו $\frac{p}{q}, \frac{p'}{q'} \in \mathbb{Q}$ שברים מצומצמים כך ש-$0 \leq \frac{p}{q} < \frac{p'}{q'} \leq 1$, אם $p' \cdot q - q' \cdot p = 1$ אז $\frac{p}{q}$ ו-$\frac{p'}{q'}$ הם איברים עוקבים ב-$\mathcal{F}_n$ לכל $n \in \mathbb{N}$ המקיים $\max\{q, q'\} \leq n < q + q'$.

הוכחה. <u>הוכחה 1 - שימוש בלמות</u>
יהי $r \in \left(\frac{p}{q}, \frac{p'}{q'}\right)$ מספר רציונלי, משתי הלמות האחרונות נובע שהמכנה של r בהצגתו המצומצמת הוא צר"ל של q ו-q' שמקדמיו טבעיים[8] ולכן אותו מכנה גדול או שווה ל-$q + q'$ וממילא $\frac{p}{q}$ ו-$\frac{p'}{q'}$ הם איברים עוקבים ב-$\mathcal{F}_n$ לכל $n \in \mathbb{N}$ המקיים $\max\{q, q'\} \leq n < q + q'$. ■

[7] היחידות נובעת מיחידות ההצגה המצומצמת של מספר רציונלי.
[8] כלומר לכל קיימים $a, b \in \mathbb{N}$ כך שההצגה המצומצמת של r היא:

$$\frac{a \cdot p + b \cdot p'}{a \cdot q + b \cdot q'}$$

הוכחה. <u>הוכחה 2 - אלגברה פשוטה</u>
יהי $n \in \mathbb{N}$ כך ש-$\max\{q,q'\} \le n < q+q'$.
נניח ש-$p' \cdot q - q' \cdot p = 1$ ונניח בשלילה ש- $\frac{p}{q}$ ו-$\frac{p'}{q'}$ אינם מספרים עוקבים ב-$\mathcal{F}_n$, א"כ קיים $\frac{a}{b} \in \mathbb{Q}$ ($a, b \in \mathbb{N}$) כך ש-$\frac{p}{q} < \frac{a}{b} < \frac{p'}{q'}$ וגם $b \le n$.
מהגדרה מתקיים:

$$0 < \frac{a}{b} - \frac{p}{q} = \frac{aq - bp}{bq}$$
$$0 < \frac{p'}{q'} - \frac{a}{b} = \frac{p'b - q'a}{bq'}$$

ומכאן שגם:

$$0 < aq - bp$$
$$0 < p'b - q'a$$

וממילא (מדובר במספרים טבעיים):

$$1 \le aq - bp$$
$$1 \le p'b - q'a$$

נשים לב לכך שמתקיים:

$$\begin{aligned}\frac{1}{qq'} = \frac{p'}{q'} - \frac{p}{q} &= \left(\frac{p'}{q'} - \frac{a}{b}\right) + \left(\frac{a}{b} - \frac{p}{q}\right)\\ &= \frac{p'b - q'a}{bq'} + \frac{aq - bp}{bq}\\ &\ge \frac{1}{bq'} + \frac{1}{bq} = \frac{q+q'}{bqq'}\end{aligned}$$

$$\Rightarrow \frac{b}{bqq'} \ge \frac{q+q'}{bqq'}$$
$$\Rightarrow b \ge q + q'$$

בסתירה לכך ש-$b \le n < q+q'$.
מכאן שהנחת השלילה אינה נכונה ואלו איברים עוקבים. ■

משפט 2.4. לכל $\frac{p}{q}, \frac{p'}{q'} \in \mathbb{Q}$ ו-$N \in \mathbb{N}$ כך ש-$\frac{p}{q}$ ו-$\frac{p'}{q'}$ הם שברים מצומצמים המהווים איברים עוקבים ב-$\mathcal{F}_N$ (בפרט $\max\{q,q'\} \le N$), מתקיימים שני הפסוקים הבאים:

1. $p' \cdot q - q' \cdot p = 1$.
2. ב-$\mathcal{F}_{q+q'}$ קיים איבר יחיד בין $\frac{p}{q}$ ל-$\frac{p'}{q'}$ והוא $\frac{p+p'}{q+q'}$.

♣ הטענה הקודמת וסעיף 2 במשפט זה מאפשרים לבנות את סדרות פרי באופן אינדוקטיבי.

הוכחה.

בסיס האינדוקציה

עבור $\mathcal{F}_1$ האיברים היחידים בסדרה הם $\frac{0}{1}$ ו-$\frac{1}{1}$ ואלו אכן מקיימים ש-$1 \cdot 1 - 1 \cdot 0 = 1$, כמו כן האיבר היחיד ב-$\mathcal{F}_2$ ($2 = 1 + 1$) שנמצא בין $\frac{0}{1}$ ל-$\frac{1}{1}$ הוא $\frac{0+1}{1+1} = \frac{1}{2}$, א"כ שני סעיפי המשפט נכונים עבור $\mathcal{F}_1$.

צעד האינדוקציה

יהי $N \in \mathbb{N}$ ונניח באינדוקציה ששני סעיפי המשפט מתקיימים עבור $\mathcal{F}_N$.

יהיו $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ שברים מצומצמים המהווים איברים עוקבים ב-$\mathcal{F}_{N+1}$ ($\frac{a}{b} < \frac{c}{d}$) ונחלק למקרים:

- נניח ש-$\frac{a}{b}$ ו-$\frac{c}{d}$ הם איברים עוקבים גם ב-$\mathcal{F}_N$, א"כ שני הסעיפים נובעים ישירות מהנחת האינדוקציה.
- נניח ש-$\frac{a}{b}$ ו-$\frac{c}{d}$ אינם איברים עוקבים ב-$\mathcal{F}_N$ ויהיו $\frac{p}{q}, \frac{p'}{q'} \in \mathbb{Q}$ כך ש-$\frac{p}{q}$ הוא האיבר הכי גדול ב-$\mathcal{F}_N$ שקטן או שווה ל-$\frac{a}{b}$ ו-$\frac{p'}{q'}$ הוא האיבר הכי קטן ב-$\mathcal{F}_N$ שגדול או שווה ל-$\frac{c}{d}$. א"כ מתקיים:

$$\frac{p}{q} \leq \frac{a}{b} < \frac{c}{d} \leq \frac{p'}{q'}$$

נוכיח ש-$\frac{p}{q}$ ו-$\frac{p'}{q'}$ הם איברים עוקבים ב-$\mathcal{F}_N$: אם היה קיים איבר $\frac{x}{y}$ ב-$\mathcal{F}_N$ כך ש-$\frac{p}{q} < \frac{x}{y} < \frac{p'}{q'}$ אז מהגדרת $\frac{p}{q}$ ו-$\frac{p'}{q'}$ נובע ש-$\frac{a}{b} < \frac{x}{y} < \frac{c}{d}$ בסתירה לכך ש-$\frac{a}{b}$ ו-$\frac{c}{d}$ הם איברים עוקבים ב-$\mathcal{F}_{N+1}$.

מסעיף 2 בהנחת האינדוקציה נובע ש-$N < q + q'$ ומטענה 2.3 נובע ש-$q + q' \leq N + 1$, א"כ $N + 1 = q + q'$.

בנוסף, מהשורה הקודמת ומסעיף 2 בהנחת האינדוקציה נובע שמתקיים אחד מהשניים:

  - $\frac{a}{b} = \frac{p}{q}$ ו-$\frac{c}{d} = \frac{p+p'}{q+q'}$, ובנוסף $\frac{p}{q}$ ו-$\frac{c}{d}$ הם איברים עוקבים ב-$\mathcal{F}_{N+1}$ וגם $\frac{c}{d}$ ו-$\frac{p'}{q'}$ הם איברים עוקבים ב-$\mathcal{F}_{N+1}$.
  - $\frac{a}{b} = \frac{p+p'}{q+q'}$ ו-$\frac{c}{d} = \frac{p'}{q'}$, ובנוסף $\frac{p}{q}$ ו-$\frac{a}{b}$ הם איברים עוקבים ב-$\mathcal{F}_{N+1}$ וגם $\frac{a}{b}$ ו-$\frac{p'}{q'}$ הם איברים עוקבים ב-$\mathcal{F}_{N+1}$.

ע"פ הסעיף הראשון בהנחת האינדוקציה מתקיים $p' \cdot q - q' \cdot p = 1$ ולכן גם:

$$(p + p') \cdot q - (q + q') \cdot p = p \cdot q + p' \cdot q - q \cdot p - q' \cdot p = 1$$
$$p' \cdot (q + q') - q' \cdot (p + p') = p' \cdot q + p' \cdot q' - q' \cdot p - q' \cdot p' = 1$$

ומכאן שלא משנה איזה משני המקרים הנ"ל הוא הנכון, בכל מקרה מתקיים:

$$c \cdot b - d \cdot a = 1$$

מכאן שהסעיף הראשון במשפט נכון גם עבור $\frac{a}{b}$ ו-$\frac{c}{d}$.

בנוסף, בנוסף מלמה 2.2 נובע שלכל מספר רציונלי $r \in \left(\frac{a}{b}, \frac{c}{d}\right)$ קיימים $u, v \in \mathbb{N}$ כך שההצגה המצומצמת של r היא:

$$\frac{v \cdot a + u \cdot c}{v \cdot b + u \cdot d}$$

מכאן שב-$\mathcal{F}_{b+d}$ קיים איבר יחיד בין $\frac{a}{c}$ ל-$\frac{b}{d}$ והוא:

$$\frac{1 \cdot a + 1 \cdot c}{1 \cdot b + 1 \cdot d}$$

משום שהצר"ל היחיד שמקיים $v \cdot b + u \cdot d \leq b + d$ הוא זה שבו $u = v = 1$, א"כ גם הסעיף השני במשפט נכון עבור $\frac{a}{b}$ ו-$\frac{c}{d}$. $\frac{a}{b}$ ו-$\frac{c}{d}$ הנ"ל היו שרירותיים ומכאן שהמשפט נכון עבור $\mathcal{F}_{N+1}$. ■

מסקנה 2.5. לכל שני שברים מצומצמים $\frac{p}{q}, \frac{p'}{q'} \in \mathbb{Q}$ המהווים איברים עוקבים בסדרת פרי כלשהי ($\frac{p}{q} < \frac{p'}{q'}$) מתקיים:

$$\frac{p'}{q'} - \frac{p}{q} = \frac{p' \cdot q - q' \cdot p}{q \cdot q'} = \frac{1}{q \cdot q'}$$

טענה 2.6. יהי $x\in\mathbb{R}$, קיימת סדרת טבעיים עולה ממש $(q_n)_{n=1}^{\infty}$ וסדרת שלמים $(p_n)_{n=1}^{\infty}$ כך שלכל $n\in\mathbb{N}$ מתקיים:
$$\left|x-\frac{p_n}{q_n}\right|\le\frac{1}{2\left(q_n\right)^2}$$

♣ ישנו שיפור קטן לטענה זו:

משפט. משפט הורוויץ[9]

יהי $\alpha\in\mathbb{R}$, קיימת סדרת טבעיים עולה ממש $(q_n)_{n=1}^{\infty}$ וסדרת שלמים $(p_n)_{n=1}^{\infty}$ כך שלכל $n\in\mathbb{N}$ מתקיים:
$$\left|x-\frac{p_n}{q_n}\right|<\frac{1}{\sqrt{5}\cdot\left(q_n\right)^2}$$
ובנוסף לא קיים $\sqrt{5}<r\in\mathbb{R}$ המקיים זאת, כלומר זהו הקירוב הטוב ביותר (עבור מספר כללי שלא ידוע עליו דבר).

הוכחה. יהיו $\frac{p}{q},\frac{p'}{q'}\in\mathbb{Q}$ שני שברים מצומצמים המהווים איברים עוקבים בסדרת פרי כלשהי.
לכל $0<r\in\mathbb{R}$ המקיים:
$$\left[\frac{p}{q},\frac{p}{q}+\frac{1}{r\cdot q^2}\right]\cap\left[\frac{p'}{q'}-\frac{1}{r\cdot q'^2},\frac{p'}{q'}\right]\neq\emptyset$$
מתקיים:
$$\frac{p}{q}+\frac{1}{r\cdot q^2}\ge\frac{p'}{q'}-\frac{1}{r\cdot q'^2}$$
$$\begin{aligned}&\iff\frac{1}{r}\cdot\left(\frac{1}{q'^2}+\frac{1}{q^2}\right)\ge\frac{p'}{q'}-\frac{p}{q}=\frac{1}{q\cdot q'}\\&\iff\frac{q}{q'}+\frac{q'}{q}=q\cdot q'\cdot\left(\frac{1}{q'^2}+\frac{1}{q^2}\right)\ge r\end{aligned}$$
נרצה למצוא את ה-r המינימלי המקיים זאת ולשם כך נגדיר את הפונקציה $f:(0,\infty)\to\mathbb{R}$ ע"י $f(x):=x+\frac{1}{x}$ לכל $0<x\in\mathbb{R}$, מכאן שלכל $0<x\in\mathbb{R}$ מתקיים $f'(x)=1-\frac{1}{x^2}$ וגם $f''(x)=\frac{2}{x^3}$. א"כ ע"פ מה שלמדנו באינפי' 1 יש ל-f נקודת קיצון יחידה והיא $x=1$ וזוהי נקודת מינימום, מהגדרה $f(1)=2$ ולכן מתקיים:
$$\frac{q}{q'}+\frac{q'}{q}\ge 2$$
וממילא ע"פ מה שראינו לעיל מתקיים גם:
$$\left[\frac{p}{q},\frac{p}{q}+\frac{1}{2q^2}\right]\cap\left[\frac{p'}{q'}-\frac{1}{2q'^2},\frac{p'}{q'}\right]\neq\emptyset$$
ולכן לכל $x\in\left[\frac{p}{q},\frac{p'}{q'}\right]$ מתקיים $\left|x-\frac{p}{q}\right|\le\frac{1}{2q^2}$ ו/או $\left|x-\frac{p'}{q'}\right|\le\frac{1}{2q'^2}$.
$\frac{p}{q}$ ו-$\frac{p'}{q'}$ היו שרירותיים ולכן הנ"ל מתקיים לכל שני איברים עוקבים בסדרת פרי כלשהי.
נסמן $a:=\lfloor x\rfloor$ ו-$b:=x-\lfloor x\rfloor$, א"כ מהגדרה מתקיים $x=a+b$, $b\in\mathbb{Z}$ ו-$0\le a<1$; מכאן שלכל $n\in\mathbb{N}$ יש ב-$\mathcal{F}_n$ איבר המקיים את הנדרש עבור $\lfloor\alpha\rceil$, יתרה מזאת: מטענה 2.3 ומסעיף 2 במשפט 2.4 נובע שלכל $n\in\mathbb{N}$ יש ב-$\mathcal{F}_{3n}$ איבר שלא מופיע ב-$\mathcal{F}_n$ ומקיים גם הוא את הנדרש עבור $\lfloor\alpha\rceil$[10]. המכנים המצומצמים של איברים המופיעים ב-$\mathcal{F}_{3n}$ ואינם ב-$\mathcal{F}_n$ גדולים ממש מ-n

[9] ערך בוויקיפדיה: אדולף הורוויץ.

[10] המכנים המצומצמים של האיברים ב-$\mathcal{F}_n$ מוכרחים להיות קטנים או שווים ל-n, מכאן שע"פ הטענה והמשפט הנ"ל שלכל שני איברים עוקבים ב-$\mathcal{F}_n$ יש בקטע הפתוח שביניהם יותר משני איברים שמופיעים ב-$\mathcal{F}_{3n}$ ואינם נמצאים ב-$\mathcal{F}_n$, ובין אלו יש שני איברים עוקבים (ב-$\mathcal{F}_{3n}$) כך ש-$\lfloor\alpha\rceil$ שייך לקטע הסגור שביניהם.

ולכן קיימת סדרת טבעיים עולה ממש $(q_n)_{n=1}^{\infty}$ וסדרת טבעיים $(p_n)_{n=1}^{\infty}$ כך שלכל $n \in \mathbb{N}$ מתקיים:

$$\left|a - \frac{p_n}{q_n}\right| = \left|\lfloor x \rfloor - \frac{p_n}{q_n}\right| \leq \frac{1}{2\left(q_n\right)^2}$$

מכאן שלכל $n \in \mathbb{N}$ מתקיים:

$$\left|x - \frac{p_n + b \cdot q_n}{q_n}\right| = \left|a + b - \frac{p_n + b \cdot q_n}{q_n}\right| = \left|a + b - b - \frac{p_n}{q_n}\right| \leq \frac{1}{2\left(q_n\right)^2}$$

ולכן אם נחליף את $(p_n)_{n=1}^{\infty}$ ב-$(p_n + b \cdot q_n)_{n=1}^{\infty}$ נקבל את הסדרות המבוקשות. ■

3 שברים משולבים

טענה 3.1. יהי $\alpha \in \mathbb{R}$, קיים שבר משולב סופי השווה ל-α אם"ם α רציונלי.

יהי $n \in \mathbb{N}$ ותהא $(a_k)_{k=0}^{\infty}$ סדרה המקיימת $0 \leq a_0 \in \mathbb{R}$ ו-$0 < a_k \in \mathbb{R}$ לכל $k \in \mathbb{N}$, נגדיר שתי סדרות חדשות $(P_k)_{k=-1}^{\infty}$ ו-$(Q_k)_{k=-1}^{\infty}$ ע"י (לכל $k \in \mathbb{N}$):

$$P_{-1} := 1 \qquad P_0 := a_0 \qquad P_k := P_{k-1} \cdot a_k + P_{k-2}$$
$$Q_{-1} := 0 \qquad Q_0 := 1 \qquad Q_k := Q_{k-1} \cdot a_k + Q_{k-2}$$

למה 3.2. לכל $0 < x \in \mathbb{R}$ ולכל $k \in \mathbb{N}_0$ מתקיים:

$$a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +}\frac{1}{a_3 +}\cdots\frac{1}{a_{k-1} +}\frac{1}{a_k + \frac{1}{x}} = \frac{P_k \cdot x + P_{k-1}}{Q_k \cdot x + Q_{k-1}}$$

הוכחה. נוכיח את הטענה באינדוקציה.

<u>בסיס האינדוקציה</u>

מהגדרה מתקיים (לכל $0 < x \in \mathbb{R}$):

$$\frac{P_0 \cdot x + P_{-1}}{Q_0 \cdot x + Q_{-1}} = \frac{a_0 \cdot x + 1}{1 \cdot x + 0} = a_0 + \frac{1}{x}$$

<u>צעד האינדוקציה</u>

יהי $k \in \mathbb{N}_0$ ונניח שלכל $0 < y \in \mathbb{R}$ מתקיים:

$$a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +}\frac{1}{a_3 +}\cdots\frac{1}{a_{k-1} +}\frac{1}{a_k + \frac{1}{y}} = \frac{P_k \cdot y + P_{k-1}}{Q_k \cdot y + Q_{k-1}}$$

יהי $0<x\in\mathbb{R}$ ונסמן $y:=a_{k+1}+\frac{1}{x}$, א"כ $y>0$ ולכן ע"פ הנחת האינדוקציה מתקיים:

$$\begin{aligned}
a_0+\frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k-1}+}\frac{1}{a_k+}\frac{1}{a_{k+1}+\frac{1}{x}} &= a_0+\frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k-1}+}\frac{1}{a_k+\frac{1}{a_{k+1}+\frac{1}{x}}}\\
&=\frac{P_k\cdot\left(a_{k+1}+\frac{1}{x}\right)+P_{k-1}}{Q_k\cdot\left(a_{k+1}+\frac{1}{x}\right)+Q_{k-1}}\\
&=\frac{P_k\cdot a_{k+1}+P_{k-1}+P_k\cdot\frac{1}{x}}{Q_k\cdot a_{k+1}+Q_{k-1}+Q_k\cdot\frac{1}{x}}\\
&=\frac{P_{k+1}+P_k\cdot\frac{1}{x}}{Q_{k+1}+Q_k\cdot\frac{1}{x}}\\
&=\frac{P_{k+1}+P_k\cdot\frac{1}{x}}{Q_{k+1}+Q_k\cdot\frac{1}{x}}\cdot\frac{x}{x}\\
&=\frac{P_{k+1}\cdot x+P_k}{Q_{k+1}\cdot x+Q_k}
\end{aligned}$$

■

מסקנה 3.3. לכל $k\in\mathbb{N}_0$ מתקיים:

$$\frac{P_k}{Q_k}=a_0+\frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k-1}+}\frac{1}{a_k}$$

הוכחה. מהגדרה מתקיים:

$$\frac{P_0}{Q_0}=\frac{a_0}{1}=a_0$$

יהי $k\in\mathbb{N}$, מהגדרה $\frac{1}{a_k}>0$ ולכן מהלמה האחרונה (??) נובע שמתקיים:

$$a_0+\frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k-1}+\frac{1}{a_k}}=\frac{P_{k-1}\cdot a_k+P_{k-2}}{Q_{k-1}\cdot a_k+Q_{k-2}}=\frac{P_k}{Q_k}$$

■

טענה 3.4. לכל $k\in\mathbb{N}$ מתקיים $P_k\cdot Q_{k-1}-Q_k\cdot P_{k-1}=(-1)^{k-1}$.

הוכחה. גם את הטענה הזו נוכיח באינדוקציה.

<u>בסיס האינדוקציה</u>

מהגדרה מתקיים:

$$\begin{aligned}
P_0\cdot Q_{-1}-Q_0\cdot P_{-1}&=a_0\cdot 0-1\cdot 1=-1=(-1)^{-1}\\
P_1\cdot Q_0-Q_1\cdot P_0&=(P_0\cdot a_1+P_{-1})\cdot Q_0-(Q_0\cdot a_1+Q_{-1})\cdot P_0\\
&=(a_0\cdot a_1+1)\cdot 1-(1\cdot a_1+0)\cdot a_0=1=(-1)^0
\end{aligned}$$

<u>צעד האינדוקציה</u>

יהי $k\in\mathbb{N}$ ונניח שמתקיים $P_k\cdot Q_{k-1}-Q_k\cdot P_{k-1}=(-1)^{k-1}$ וגם $P_{k-1}\cdot Q_{k-2}-Q_{k-1}\cdot P_{k-2}=(-1)^{k-2}$, א"כ מהגדרה מתקיים:

$$\begin{aligned}
P_{k+1}\cdot Q_k&=(P_k\cdot a_{k+1}+P_{k-1})\cdot(Q_{k-1}\cdot a_k+Q_{k-2})\\
&=P_k\cdot a_{k+1}\cdot Q_{k-1}\cdot a_k+P_k\cdot a_{k+1}\cdot Q_{k-2}+P_{k-1}\cdot Q_{k-1}\cdot a_k+P_{k-1}\cdot Q_{k-2}
\end{aligned}$$

$$\begin{aligned}Q_{k+1}\cdot P_k &= \left(Q_k\cdot a_{k+1}+Q_{k-1}\right)\left(P_{k-1}\cdot a_k+P_{k-2}\right)\\ &= Q_k\cdot a_{k+1}\cdot P_{k-1}\cdot a_k+Q_k\cdot a_{k+1}\cdot P_{k-2}+Q_{k-1}\cdot P_{k-1}\cdot a_k+Q_{k-1}\cdot P_{k-2}\end{aligned}$$

$$\begin{aligned}\Rightarrow P_{k+1}\cdot Q_k-Q_{k+1}\cdot P_k &= a_k\cdot a_{k+1}\cdot(-1)^{k-1}+P_k\cdot a_{k+1}\cdot Q_{k-2}-Q_k\cdot a_{k+1}\cdot P_{k-2}+(-1)^{k-2}\\ &= a_k\cdot a_{k+1}\cdot(-1)^{k-1}+a_{k+1}\cdot\left(P_k\cdot Q_{k-2}-Q_k\cdot P_{k-2}\right)+(-1)^{k-2}\end{aligned}$$

כמו כן מהגדרה מתקיים:

$$\begin{aligned}P_k\cdot Q_{k-2} &= \left(P_{k-1}\cdot a_k+P_{k-2}\right)\cdot Q_{k-2}\\ &= P_{k-1}\cdot a_k\cdot Q_{k-2}+P_{k-2}\cdot Q_{k-2}\\ Q_k\cdot P_{k-2} &= \left(Q_{k-1}\cdot a_k+Q_{k-2}\right)\cdot P_{k-2}\\ &= Q_{k-1}\cdot a_k\cdot P_{k-2}+Q_{k-2}\cdot P_{k-2}\end{aligned}$$

$$\Rightarrow P_k\cdot Q_{k-2}-Q_k\cdot P_{k-2}=a_k\cdot(-1)^{k-2}$$

$$\begin{aligned}\Rightarrow P_{k+1}\cdot Q_k-Q_{k+1}\cdot P_k &= a_k\cdot a_{k+1}\cdot(-1)^{k-1}+a_{k+1}\cdot a_k\cdot(-1)^{k-2}+(-1)^{k-2}\\ &= a_k\cdot a_{k+1}\cdot\left((-1)^{k-1}+(-1)^{k-2}\right)+(-1)^{k-2}\\ &= a_k\cdot a_{k+1}\cdot 0+(-1)^{k-2}=(-1)^k=(-1)^{k+1-1}\end{aligned}$$

■

מסקנה 3.5. אם $(a_k)_{k=0}^{\infty}$ היא סדרה שכל איבריה שלמים אז $\frac{P_k}{Q_k}$ היא הצגה מצומצמת של המספר הרציונלי המתאים (לכל $k\in\mathbb{N}_0$).

טענה 3.6. לכל $n-1>k\in\mathbb{N}_0$ מתקיים:

- אם $k\in\text{Odd}$ אז:

$$a_0+\frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k-1}+}\frac{1}{a_k}=\frac{P_k}{Q_k}>\frac{P_{k+2}}{Q_{k+2}}=a_0+\frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k+1}+}\frac{1}{a_{k+2}}$$

- אם $k\in\text{Even}$ אז:

$$a_0+\frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k-1}+}\frac{1}{a_k}=\frac{P_k}{Q_k}<\frac{P_{k+2}}{Q_{k+2}}=a_0+\frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k+1}+}\frac{1}{a_{k+2}}$$

הוכחה. מטענה 3.4 נובע שמתקיים:

$$\begin{aligned}\frac{P_{k+2}}{Q_{k+2}}-\frac{P_k}{Q_k} &= \left(\frac{P_{k+2}}{Q_{k+2}}-\frac{P_{k+1}}{Q_{k+1}}\right)+\left(\frac{P_{k+1}}{Q_{k+1}}-\frac{P_k}{Q_k}\right)\\ &= \frac{P_{k+2}\cdot Q_{k+1}-Q_{k+2}\cdot P_{k+1}}{Q_{k+2}\cdot Q_{k+1}}+\frac{P_{k+1}\cdot Q_k-Q_{k+1}\cdot P_k}{Q_{k+1}\cdot Q_k}\\ &= \frac{(-1)^{k+1}}{Q_{k+2}\cdot Q_{k+1}}+\frac{(-1)^k}{Q_{k+1}\cdot Q_k}=(-1)^k\cdot\frac{Q_{k+2}-Q_k}{Q_{k+2}\cdot Q_{k+1}\cdot Q_k}\end{aligned}$$

מהגדרתה $(Q_k)_{k=0}^{\infty}$ היא סדרת חיוביים עולה ממש ולכן ההפרש הנ"ל שלילי כאשר $k \in \text{Odd}$ וחיובי כאשר $k \in \text{Even}$, ומכאן שאם $k \in \text{Odd}$ אז $\frac{P_{k+2}}{Q_{k+2}} > \frac{P_k}{Q_k}$ ואם $k \in \text{Even}$ אז $\frac{P_{k+2}}{Q_{k+2}} < \frac{P_k}{Q_k}$. ■

טענה 3.7. לכל $k \in \text{Odd}$ ולכל $m \in \text{Even}$ מתקיים:

$$a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{m-1}+}\frac{1}{a_m} = \frac{P_m}{Q_m} < \frac{P_k}{Q_k} = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_{k-1}+}\frac{1}{a_k}$$

ואם השבר המשולב מתכנס למספר אי-רציונלי אז מתקיים גם (נסמן את הגבול ב-x):

$$\frac{P_m}{Q_m} < x < \frac{P_k}{Q_k}$$

♣ כלומר:

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \cdots < x < \cdots < \frac{P_5}{Q_5} < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}$$

והשבר המשולב מתכנס אם האינפימום של קבוצת האיברים האי-זוגיים שווה לסופרמום של קבוצת האיברים הזוגיים.

הוכחה. נחלק למקרים:

- אם $k > m$ אז מטענה 3.4 נובע שמתקיים:

$$\frac{P_k}{Q_k} - \frac{P_m}{Q_m} = \sum_{i=m}^{k-1}\left(\frac{P_{i+1}}{Q_{i+1}} - \frac{P_i}{Q_i}\right) = \sum_{i=m}^{k-1}\frac{P_{i+1}\cdot Q_i - Q_{i+1}\cdot P_i}{Q_{i+1}\cdot Q_i} = \sum_{i=m}^{k-1}\frac{(-1)^i}{Q_{i+1}\cdot Q_i}$$

כעת מכיוון ש-$(Q_k)_{k=1}^{\infty}$ היא סדרת חיוביים עולה ממש נדע שלכל $i \in \text{Even}$ כך ש-$m \le i \le k-3$ מתקיים $\frac{1}{Q_{i+1}\cdot Q_i} > \frac{1}{Q_{i+2}\cdot Q_{i+1}}$ ומכאן שגם:

$$\frac{(-1)^i}{Q_{i+1}\cdot Q_i} + \frac{(-1)^{i+1}}{Q_{i+2}\cdot Q_{i+1}} > 0$$

וממילא גם:

$$\frac{P_k}{Q_k} - \frac{P_m}{Q_m} = \sum_{i=m}^{k-1}\frac{(-1)^i}{Q_{i+1}\cdot Q_i} > \sum_{i=m}^{k-2}\frac{(-1)^i}{Q_{i+1}\cdot Q_i} > 0$$

- אם $m > k$ אז מנימוקים דומים נובע שמתקיים:

$$\begin{aligned}\frac{P_m}{Q_m} - \frac{P_k}{Q_k} &= \sum_{i=k}^{m-1}\left(\frac{P_{i+1}}{Q_{i+1}} - \frac{P_i}{Q_i}\right) = \sum_{i=k}^{m-1}\frac{P_{i+1}\cdot Q_i - Q_{i+1}\cdot P_i}{Q_{i+1}\cdot Q_i}\\ &= \sum_{i=k}^{m-1}\frac{(-1)^i}{Q_{i+1}\cdot Q_i} < \sum_{i=k}^{m-2}\frac{(-1)^i}{Q_{i+1}\cdot Q_i} < 0\end{aligned}$$

■

טענה 3.8. לכל $k \in \mathbb{N}$ מתקיים:

$$\left|\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}}\right| = \frac{1}{Q_{k-1} \cdot Q_k}$$

הוכחה. נובע ישירות מטענה 3.4, לכל $k \in \mathbb{N}$ מתקיים:

$$\left|\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}}\right| = \left|\frac{P_k \cdot Q_{k-1} - Q_k \cdot P_{k-1}}{Q_k \cdot Q_{k-1}}\right| = \left|\frac{(-1)^{k-1}}{Q_k \cdot Q_{k-1}}\right| = \frac{1}{Q_{k-1} \cdot Q_k}$$

■

מסקנה 3.9. אם השבר המשולב מתכנס למספר אי-רציונלי אז לכל $k \in \mathbb{N}$ מתקיים גם (נסמן את הגבול ב-x):

$$\left|x - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k \cdot Q_{k+1}} < \frac{1}{(Q_k)^2}$$

♣ כלומר השבר המשולב שנבנה ע"י הפרדת החלק השלם מהחלק השברי נותן את קירוב מהסדר הגבוה ביותר שניתן לתת (עבור מספר כללי שלא ידוע עליו דבר).

4 משוואות פל (Pell)

♣ הסיבה היחידה לכך שפרק זה מופיע בקבצים העוסקים בקירובים דיופנטיים היא שההוכחה ללמה 4.5 (להלן) משתמשת בטענה שלמספר ממשי יש אינסוף קירובים שונים מסדר שני (טענה 2.6).

יהי $D \in \mathbb{N}$ שאינו ריבוע ונסמן $R := \mathbb{Z}\left[\sqrt{D}\right] := \left\{x + \sqrt{D}y \mid x, y \in \mathbb{Z}\right\}$ ו-$F := \mathbb{Q}\left[\sqrt{D}\right] := \left\{r + \sqrt{D} \cdot s \mid r, s \in \mathbb{Q}\right\}$.

למה 4.1. הנורמה (ב-R וב-F) כפלית.

מסקנה 4.2. לכל $a, b \in \mathbb{Z}$ מתקיים: $a + \sqrt{D} \cdot b$ הפיך ב-R אם"ם $a^2 - D \cdot b^2 = \pm 1$.

הוכחה.

- $\Leftarrow$

  נניח ש-$a + \sqrt{D} \cdot b$ הפיך ב-R ויהי $c + \sqrt{D} \cdot d$ ההופכי שלו, א"כ מתקיים:

  $$1 = N(1) = N\left(\left(a + \sqrt{D} \cdot b\right) \cdot \left(c + \sqrt{D} \cdot d\right)\right) = N\left(a + \sqrt{D} \cdot b\right) \cdot N\left(c + \sqrt{D} \cdot d\right)$$

  נזכור ש-$N\left(a + \sqrt{D} \cdot b\right), N\left(c + \sqrt{D} \cdot d\right) \in \mathbb{Z}$ ומכאן שמתקיים $N\left(a + \sqrt{D} \cdot b\right) = \pm 1 = N\left(c + \sqrt{D} \cdot d\right)$.

- $\Rightarrow$

  נניח ש-$a^2 - D \cdot b^2 = \pm 1$, א"כ מתקיים:

  $$\begin{aligned} 1 = \left(a^2 - D \cdot b^2\right)^2 &= \left(a + \sqrt{D} \cdot b\right) \cdot \left[\left(a - \sqrt{D} \cdot b\right) \cdot \left(a^2 - D \cdot b^2\right)\right] \\ &= \left(a + \sqrt{D} \cdot b\right) \cdot \left[a \cdot \left(a^2 - D \cdot b^2\right) - \sqrt{D} \cdot b \cdot \left(a^2 - D \cdot b^2\right)\right] \end{aligned}$$

  כלומר מצאנו את ההופכי של $a + \sqrt{D} \cdot b$ ב-F והוא אכן איבר ב-R.

■

מסקנה 4.3. יהיו $0 \neq N_1, N_2 \in \mathbb{Z}$ ונניח שקיימים $a,b,c,d \in \mathbb{Z}$ כך ש-$a^2 - Db^2 = N_1$ ו-$c^2 - Dd^2 = N_2$, מתקיים גם:

$$\begin{aligned} N_1 \cdot N_2 &= N\left(a+\sqrt{D}b\right) \cdot N\left(c+\sqrt{D}d\right) \\ &= N\left([ac+Dbd] + \sqrt{D} \cdot [bc+ad]\right) \\ &= \left([ac+Dbd] + \sqrt{D} \cdot [bc+ad]\right)\left([ac+Dbd] - \sqrt{D} \cdot [bc+ad]\right) \\ &= (ac+Dbd)^2 - D\,(bc+ad)^2 \end{aligned}$$

♣ כלומר אם למשוואות פל $x^2 - Dy^2 = N_1$ ו-$x^2 - Dy^2 = N_2$ יש פתרון אז גם למשוואה $x^2 - Dy^2 = N_1 \cdot N_2$ יש פתרון.

מסקנה 4.4. אם למשוואת פל $x^2 - D \cdot y^2 = 1$ יש פתרון אחד אז יש לה אינסוף פתרונות.

למה 4.5. קיים $0 \neq N \in \mathbb{Z}$ כך שלמשוואת פל $x^2 - Dy^2 = N$ קיימים אינסוף פתרונות.

הוכחה. ראינו בטענה 2.6 שקיימים אינסוף זוגות $(x,y) \in \mathbb{N}^2$ כך שמתקיים:

$$\left|\sqrt{D} - \frac{x}{y}\right| < \frac{1}{y^2}$$

לכל זוג כזה מתקיים:

$$\left|x - \sqrt{D} \cdot y\right| = \left|\sqrt{D} \cdot y - x\right| < \frac{1}{y}$$

ומא"ש המשולש נובע שמתקיים גם:

$$\left|x + \sqrt{D} \cdot y\right| = \left|x - \sqrt{D} \cdot y\right| + \left|2 \cdot \sqrt{D} \cdot y\right| < \frac{1}{y} + 2 \cdot \sqrt{D} \cdot y$$

וממילא גם:

$$\left|x^2 - D \cdot y^2\right| = \left|x - \sqrt{D} \cdot y\right| \cdot \left|x + \sqrt{D} \cdot y\right| < \frac{1}{y^2} + 2 \cdot \sqrt{D} < 1 + 2 \cdot \sqrt{D}$$

א"כ קיימים אינסוף זוגות $(x,y) \in \mathbb{N}^2$ המקיימים:

$$-1 - 2 \cdot \sqrt{D} < x^2 - D \cdot y^2 < 1 + 2 \cdot \sqrt{D}$$

נשים לב לכך שלכל זוג כזה מתקיים $x^2 - D \cdot y^2 \in \mathbb{Z}$ ולכן מהעובדה שבקטע $\left(-1 - 2 \cdot \sqrt{D}, 1 + 2 \cdot \sqrt{D}\right)$ יש מספר סופי של שלמים נובע שקיים $N \in \mathbb{Z}$ שעבורו יש למשוואת פל $x^2 - D \cdot y^2 = N$ אינסוף פתרונות שונים, אותו N אינו יכול להיות 0 מפני ש-D אינו ריבוע ולכן מקיים את הנדרש. ■

טענה 4.6. למשוואת פל $x^2-Dy^2=1$ יש פתרון לא טריוויאלי (כלומר לא מתקיים $x=\pm 1$ ו-$y=0$).

♣ בגלל ש-x ו-y מופיעים במשוואה כשהם מועלים בחזקת 2 ניתן להניח שקיים פתרון לא טריוויאלי שבו x ו-y חיוביים[11] ומבין כל הפתרונות הללו קיים פתרון שעבורו הביטוי $x+\sqrt{D}y$ מקבל ערך מינימלי, לפתרון הזה נקרא הפתרון היסודי משום שכפי שנראה בטענה הבאה כל הפתרונות האחרים מתקבלים ממנו בצורה פשוטה.

הוכחה. יהי $0\neq N\in\mathbb{Z}$ כך שלמשוואת פל $x^2-Dy^2=N$ קיימים אינסוף פתרונות ויהיו $(a,b),(c,d)\in\mathbb{N}^2$ שני פתרונות שונים של משוואה זו כך ש-$a\equiv c\mod N$[12] ו-$b\equiv d\mod N$ (מהעובדה ש-$(\mathbb{Z}/N\mathbb{Z})^2$ סופית ואילו $\mathbb{N}^2$ אינה סופית נובע שאכן קיימים שני פתרונות כאלו).

$$\begin{aligned}\Rightarrow\frac{a-\sqrt{D}\cdot b}{c-\sqrt{D}\cdot d}&=\frac{\left(a-\sqrt{D}\cdot b\right)\left(c+\sqrt{D}\cdot d\right)}{\left(c-\sqrt{D}\cdot d\right)\left(c+\sqrt{D}\cdot d\right)}=\frac{(ac-D\cdot bd)+\sqrt{D}\cdot(ad-bc)}{c^2-D\cdot d^2}\\&=\frac{(ac-D\cdot bd)+\sqrt{D}\cdot(ad-bc)}{N}\end{aligned}$$

מהגדרה מתקיים $ac-D\cdot bd\equiv a^2-D\cdot b^2\equiv N\equiv 0\mod N$ וגם $ad-bc\equiv a\cdot b-b\cdot a\equiv 0\mod N$ ומכאן שקיימים $s,t\in\mathbb{Z}$ כך שמתקיים:

$$\frac{a-\sqrt{D}\cdot b}{c-\sqrt{D}\cdot d}=\frac{N\cdot s+\sqrt{D}\cdot N\cdot t}{N}=s+\sqrt{D}\cdot t$$

וממילא גם:

$$1=\frac{N}{N}=\frac{N\left(a-\sqrt{D}\cdot b\right)}{N\left(c-\sqrt{D}\cdot d\right)}=N\left(s+\sqrt{D}\cdot t\right)=s^2-D\cdot t^2$$

א"כ קיים פתרון למשוואת פל $x^2-Dy^2=1$ ולכן ע"פ מסקנה 4.4 יש לה אינסוף פתרונות ובפרט אחד מהם אינו טריוויאלי. ■

משפט 4.7. יהיו $x,y\in\mathbb{N}$ כך ש-(x,y) הוא הפתרון היסודי[13], לכל פתרון לא טריוויאלי $(a,b)\in\mathbb{N}\times\mathbb{Z}$ קיים $0\neq n\in\mathbb{Z}$ כך שמתקיים:

$$a+\sqrt{D}\cdot b=\left(x+\sqrt{D}\cdot y\right)^n$$

וכמו כן לכל $(a,b)\in\mathbb{N}\times\mathbb{Z}$, אם קיים $0\neq n\in\mathbb{Z}$ כך שמתקיים $a+\sqrt{D}\cdot b=\left(x+\sqrt{D}\cdot y\right)^n$ אז (a,b) הוא פתרון.

♣ הסימנים של n ו-b זהים וזאת משום שמתקיים:

$$\left(x+\sqrt{D}\cdot y\right)^{-1}=\frac{1}{x+\sqrt{D}\cdot y}=\frac{x-\sqrt{D}\cdot y}{x^2-D\cdot y^2}=\frac{x-\sqrt{D}\cdot y}{1}=x-\sqrt{D}\cdot y$$

♣ א"כ כל הפתרונות מתחלקים לארבע קבוצות:

1. אלו שעבורם $1<a+\sqrt{D}\cdot b$ - מתקבלים ע"י חזקה חיובית של $x+\sqrt{D}y$ ומקיימים $0<a,b$.
2. אלו שעבורם $0<a+\sqrt{D}\cdot b<1$ - מתקבלים ע"י חזקה חיובית של $x+\sqrt{D}y$ ומקיימים $b<0<a$.
3. אלו שעבורם $-1<a+\sqrt{D}\cdot b<0$ - מתקבלים ע"י לקיחת הנגדיים של הפתרונות בסעיף 2 ולפיכך מקיימים $a<0<b$.
4. אלו שעבורם $a+\sqrt{D}\cdot b<-1$ - מתקבלים ע"י לקיחת הנגדיים של הפתרונות בסעיף 1 ולפיכך מקיימים $a,b<0$.

---

[11] לא ייתכן שאחד מהם הוא 0 מפני שהפתרון לא טריוויאלי (כלומר $y\neq 0$) ו-$-Dy^2<0<1$ (כלומר $x\neq 0$).
[12] אם $N<0$ אז הכוונה היא לשקילות מודולו $-N$.
[13] כפי שאמרנו לעיל הכוונה היא שלכל $a,b\in\mathbb{N}$ המקיימים $a^2-Db^2=1$ מתקיים $x+\sqrt{D}y\leq a+\sqrt{D}b$.

הוכחה. נסמן $\alpha := x + \sqrt{D} \cdot y$ ויהי $(a,b) \in \mathbb{N} \times \mathbb{Z}$ כך ש-$b \neq 0$.

- נניח ש-(a,b) הוא פתרון ויהי $k \in \mathbb{N}$ כך שמתקיים:

$$\alpha^k \leq a + \sqrt{D} \cdot |b| \leq \alpha^{k+1}$$

$$\Rightarrow 1 \leq \frac{a + \sqrt{D} \cdot |b|}{\alpha^k} \leq \alpha$$

אבל:

$$N\left(\frac{a + \sqrt{D} \cdot |b|}{\alpha^k}\right) = \frac{N\left(a + \sqrt{D} \cdot |b|\right)}{N\left(\alpha^k\right)} = \frac{a^2 - D \cdot b^2}{N^k(\alpha)} = 1$$

ומכאן ש-$\left(a + \sqrt{D} \cdot |b|\right) \cdot \alpha^{-k}$ גם הוא פתרון ולכן מהמינימליות של α נובע שמתקיים:

$$\frac{a + \sqrt{D} \cdot |b|}{\alpha^k} = \alpha$$

$$\Rightarrow a + \sqrt{D} \cdot |b| = \alpha^{k+1}$$

אם $b > 0$ אז סיימנו, אחרת נשים לב לכך שמתקיים:

$$\begin{aligned} a + \sqrt{D} \cdot b &= \frac{a - \sqrt{D} \cdot |b|}{1} = \frac{a - \sqrt{D} \cdot |b|}{a^2 - D \cdot b^2} \\ &= \frac{a - \sqrt{D} \cdot |b|}{\left(a - \sqrt{D} \cdot |b|\right)\left(a + \sqrt{D} \cdot |b|\right)} \\ &= \left(a + \sqrt{D} \cdot |b|\right)^{-1} = \alpha^{-k-1} \end{aligned}$$

- נניח שקיים $0 \neq n \in \mathbb{Z}$ כך שמתקיים $a + \sqrt{D} \cdot b = \left(x + \sqrt{D} \cdot y\right)^n = \alpha^n$.

$$\Rightarrow a^2 - D \cdot b^2 = N\left(a + \sqrt{D} \cdot b\right) = N\left(\alpha^n\right) = N^n(\alpha) = 1^n = 1$$

ומכאן שזהו אכן פתרון.

■