קירובים דיופנטיים

משפט דיריכלה - יהי Q טבעי $Q\geq 2$, ויהי $\theta\in\mathbb{R}$
אז יש מספר טבעי $1\leq q<Q$ ושלם p כך ש-
$$(*) \qquad |q\theta - p| \leq \frac{1}{Q}$$

בהעברת אגפים, $(*)$ שקול ל:
$$\left|\theta - \frac{p}{q}\right| \leq \frac{1}{qQ}$$

ולכן $\left(\left|\theta - \frac{p}{q}\right| \leq \frac{1}{q^2}\right)$

תזכורת מתרגול 1 - הרציונלים צפופים ב-$\mathbb{R}$. כלומר לכל $\theta\in\mathbb{R}$ ו-$\varepsilon>0$
יש $\frac{p}{q}\in\mathbb{Q}$ כך ש- $\left|\theta-\frac{p}{q}\right|<\varepsilon$

בהוכחה נקבל $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q}$

בהוכחת משפט דיריכלה נקבל קירוב הרבה יותר טוב.

הוכחה - נסמן עבור $x\in\mathbb{R}$, $\lfloor x\rfloor = \max\{k\in\mathbb{Z} \mid k\leq x\}$, $\{x\}=x-\lfloor x\rfloor$

נחלק את $[0,1)$ ל- Q קטעים באורך $\frac{1}{Q}$:
$$[0,1) = \left[0,\tfrac{1}{Q}\right)\cup\left[\tfrac{1}{Q},\tfrac{2}{Q}\right)\cup\dots\cup\left[1-\tfrac{1}{Q},1\right)$$

המספרים $i=1,2\dots Q$ $\{i\theta\}$, שמספרם $Q+1$,
מוכלים בחלוקה ל- Q תתי קטעים.
לפי עיקרון שובך היונים יש $0\leq i<j\leq Q$ כך ש- $\{i\theta\},\{j\theta\}$ שייכים לאותו תת-קטע

$$p_i = \lfloor i\theta\rfloor, \quad \{i\theta\} = i\theta - p_i$$
$$p_j = \lfloor j\theta\rfloor, \quad \{j\theta\} = j\theta - p_j, \quad p_i, p_j\in\mathbb{Z}$$

$$\frac{1}{Q} \geq |\{j\theta\}-\{i\theta\}| = |j\theta - p_j - (i\theta - p_i)| =$$
$$= |(j-i)\theta - (p_j - p_i)| = |q\theta - p|$$

נסמן $q=j-i\leq Q$, $p_j - p_i = p\in\mathbb{Z}$

מסקנה - אם $\theta\in\mathbb{R}\setminus\mathbb{Q}$, אז יש אינסוף רציונלים מצומצמים $\frac{p_k}{q_k}$ שמקיימים:
$$\left|\theta - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k^2}$$

עתה נבנה באינדוקציה אינסוף פתרונות שונים לאי-השוויון $\left|\theta - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k^2}$
את הראשון נבנה באמצעות משפט דיריכלה עם $Q=2$.
נניח שמצאנו $\frac{p_1}{q_1}\dots\frac{p_n}{q_n}$. נבחר Q ~~...~~ מספיק ~~...~~ גדול כך ש- $\frac{1}{Q}<\min|q_j\theta - p_j|$
נפעיל את משפט דיריכלה עם Q זה ונקבל פיתרון נוסף, וכו'.

דוגמה - עבור $x=\pi$, הקירובים הבאים מקיימים את המסקנה הקודמת:

$\pi \approx 3,\ 3\frac{1}{7},\ 3\frac{15}{106},\ 3\frac{16}{113}$

$3\frac{16}{113} \to 3.1415929\ldots$

$3\frac{15}{106} \to 3.14159265\ldots$

$3\frac{1}{7} \to 3.1428\ldots$

מטרתנו כעת - למצוא דרך מפורשת לכתוב קירובים כאלה
נשתמש בשברים משולבים, ביטוים מהצורה:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$$

$a_0 \in \mathbb{Z}$

$a_i \in \mathbb{N}$, $i \geq 1$

איך מגיעים לזה בכלל? לפי אלגוריתם אוקלידס.
אלגוריתם אוקלידס על p,q (בהנחה ש- $p<q$):

$$q = ap + r$$

נחלק ב- p:

$$\frac{q}{p} = a + \frac{r}{p}$$

או:

$$\frac{p}{q} = \frac{1}{a + \frac{r}{p}}$$

נמשיך לפי האלגוריתם, ונקבל:

$$\frac{p}{q} = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \frac{r_1}{p_1}}} = \ldots = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_n}}}$$

כמו כן, כל רציונלי $\frac{p}{q}$ אפשר לרשום בצורה

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots a_n}}$$

(בשני הביטוים, $n \geq 0$, $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$ $\forall i \geq 1$.)

סימון - הפיתוח לשברים משולבים של $\frac{p}{q}$ הוא $\frac{p}{q} = [a_0, a_1, \ldots a_n]$

טענה - אם $a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_n}} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\ddots\, b_m}}$, $m \geq n$, התנאים על a_i, b_i מתקיימים.

אז או שמתקיים $m=n$, $a_i = b_i$ $\forall i$
או שמתקיים $n=m+1$, $a_m = b_m - 1$, $b_{m+1} = 1$, $a_0 = b_0, \ldots, a_{m-1} = b_{m-1}$

דוגמה -

$$3 + \cfrac{1}{5 + \frac{1}{2}} = 3 + \cfrac{1}{5 + \cfrac{1}{5 + \frac{1}{1}}}$$

הוכחה - נניח שהמקרה הראשון לא מתקיים ((a_i), (b_i) לא זהות)
ונוכיח שהמקרה השני מתקיים, באינדוקציה על m

המשך בעמוד הבא.

המשך הוכחה - אם $m=0$, מקבלים

$$a_0 = b_0 + \underbrace{\cfrac{1}{b_1 + \cfrac{1}{b_2 \ddots \cfrac{1}{b_n}}}}_{B}$$

$B \in (0,1]$

אם הביטויים שווים אז $a_0 = b_0 + 1$, ואז בהכרח $B = 1$

כלומר $n=1$, $b_1 = 1$

אם $m \geq 1$, רושמים

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 \ddots \cfrac{1}{a_m}}} = b_0 + \underbrace{\cfrac{1}{b_1 + \cfrac{1}{b_2 \dots \cfrac{1}{b_n}}}}_{B}$$

$B \in (0,1)$ ← הביטוי אינו 1 כי ובנוסף $n \geq m \geq 1$ כלומר המכנה גדול מ-1.

קיבלנו $b_0 = \lfloor x \rfloor$ ובאותו אופן $a_0 = \lfloor x \rfloor$.

בפרט $a_0 = b_0$, ולכן $A = B$.

את $A=B$ ניתן לרשום גם בתור:

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots \cfrac{1}{a_m}}} = b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \dots \cfrac{1}{b_n}}}$$

זהו שוויון בין שני ביטויים קטנים יותר, וממשיכים באינדוקציה.

מסקנה - נגדיר

$$cf: \left\{ [a_0, a_1, \dots, a_n] \;\middle|\; \begin{array}{l} n \in \mathbb{N} \cup \{0\} \\ a_0 \in \mathbb{Z} \\ a_i \in \mathbb{N} \ (i \geq 1) \end{array} \right\} \to \mathbb{Q}$$

ההעתקה שמעבירה את $[a_0 \dots a_n]$ למספר $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 \dots \cfrac{1}{a_n}}}$

העתקה ט היא ב 1-ל-1, ועל.

cf - continued fractions, שברים משולבים.

טענה - נסמן $q_{-1} = 0$, $q_{-2} = 1$, $p_{-2} = 0$, $p_{-1} = 1$.

בהינתן $[a_0, a_1 \dots a_n]$ נגדיר נוסחאות נסיגה:

$$p_{k+1} = a_{k+1} p_k + p_{k-1}$$
$$q_{k+1} = a_{k+1} q_k + q_{k-1} \qquad (k = 1, 2 \dots n-1)$$

בכתיבה מטריצית:

$$\begin{bmatrix} p_{k+1} & p_k \\ q_{k+1} & q_k \end{bmatrix} = \begin{bmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{bmatrix} \begin{bmatrix} a_{k+1} & 1 \\ 1 & 0 \end{bmatrix}$$

אזי $\frac{p_n}{q_n} = [0, a_1, \dots, a_n]$

ושבר זה מצומצם הוא $gcd(p_n, q_n)$

הוכחה - באינדוקציה על n. (בסיס תעשו לבד, עצלנים)

נסמן $[a_1; a_2 \dots a_n] = \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}$ (שבר מצומצם מנוסחאות שברים משולבים)

נשים לב -
$$\frac{\tilde{p}_n}{\tilde{q}_n} = a_0 + \frac{1}{\frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}}} = a_0 + \frac{\tilde{q}_{n-1}}{\tilde{p}_{n-1}} = \frac{a_0 \tilde{p}_{n-1} + \tilde{q}_{n-1}}{\tilde{p}_{n-1}}$$

כלומר:
$$\begin{bmatrix} \tilde{p}_n \\ \tilde{q}_n \end{bmatrix} = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \tilde{p}_{n-1} \\ \tilde{q}_{n-1} \end{bmatrix}$$

אם היה ~~מחלק~~ מחלק משותף לא טריוויאלי של $\tilde{p}_{n-1}$, $a_0 \tilde{p}_{n-1} + \tilde{q}_{n-1}$
אז הוא היה מחלק משותף של $\tilde{p}_{n-1}, \tilde{q}_{n-1}$. סתירה.

אז אפשר לרשום:
$$\begin{bmatrix} \tilde{p}_n \\ \tilde{q}_n \end{bmatrix} = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \underbrace{\begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_2 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{n-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_n \\ 1 \end{bmatrix}}_{\text{"מהנחת האינדוקציה"} \begin{bmatrix} \tilde{p}_{n-1} \\ \tilde{q}_{n-1} \end{bmatrix}}$$

לכן, ~~מבדיקת~~ מבדיקת עמודה ימנית ושמאלית בנפרד:
$$\begin{bmatrix} \tilde{p}_n & p_{n-1} \\ \tilde{q}_n & q_{n-1} \end{bmatrix} = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \left(\frac{p_{n-1}}{q_{n-1}} = [a_0; a_1 \dots a_{n-1}] \right)$$
$$= \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}$$
מנוסחאות הנסיגה

מסקנה - לכל n, $\det \begin{bmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{bmatrix} = \pm 1$

וגם: קיים $\lambda > 1$, $C > 0$ כך שלכל n, $q_n \geq C\lambda^n$

הוכחה - א - ראינו
$$\begin{bmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{bmatrix} = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{n+1} & 1 \\ 1 & 0 \end{bmatrix}$$

זו היא מכפלת דטרמיננטות של -1, ולכן $\det \begin{bmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{bmatrix} = (-1)^{n+2}$

ב - נבחר λ כך ש- $\lambda^2 < \lambda + 1$, $\lambda > 1$. נמשיך באינדוקציה.

נבחר קבוע C כך ש- $q_n \geq C\lambda^n$ עבור $n = 0, 1$

אז $q_{n+1} = a_{n+1} q_n + q_{n-1} \geq q_n + q_{n-1} \geq C(\lambda^n + \lambda^{n-1})$

מסקנה - נניח $a_0 \in \mathbb{Z}$, ולכל $i \in \mathbb{N}$, $a_i \in \mathbb{N}$ קיים הגבול:

$$[a_0 a_1 \dots] = \lim_{n \to \infty} [a_0, a_1 \dots a_n]$$

הוכחת המסקנה בעמוד הבא.

הוכחה - נסמן $\frac{p_n}{q_n} = [a_0; a_1, \ldots a_n]$

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}}\right| \underset{\text{מהמסקנה}}{=} \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} \le \frac{1}{q_n^2} \underset{\text{מסקנה קודמת}}{\le} \frac{1}{c^2\lambda^{2n}}$$

$$\left|\frac{p_{n+k}}{q_{n+k}} - \frac{p_n}{q_n}\right| \le \left|\frac{p_{n+k}}{q_{n+k}} - \frac{p_{n+k-1}}{p_{n+k-1}}\right| + \ldots + \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \le \frac{1}{c^2}\left(\frac{1}{\lambda^{2n}} + \frac{1}{\lambda^{2n+2}} + \ldots + \frac{1}{\lambda^{2(n+k-1)}}\right) \le$$

$$\le \frac{1}{c^2} \cdot \underbrace{\sum_{i=n}^{\infty}\left(\frac{1}{\lambda^2}\right)}_{\text{זנב של סכום אינסופי מתכנס}} \xrightarrow{n\to\infty} 0$$

קיבלנו העתקה (נמשיך לקרוא לה CF), ששולחת כל סדרה (סופית או אינסופית) למספר ממשי. נראה מייד שכל המספרים האי-רציונלים הם התמונה תחת CF של הסדרות האינסופיות, וש- CF חח"ע על סדרות אינסופיות.
כלומר נוכיח:

משפט - לכל $\alpha \in \mathbb{R}/\mathbb{Q}$ יש סדרה $a_0, a_1, \ldots$ כך ש- $a_0 \in \mathbb{Z}$ ו- $a_i \in \mathbb{N}$ $\forall i \ge 1$ המקיימת:

א - אם $\frac{p_n}{q_n} = [a_0; a_1, \ldots a_n]$ אז לכל k:

$$\ldots < \frac{p_{2k}}{q_{2k}} < \frac{p_{2k+2}}{q_{2k+2}} < \ldots < \alpha < \ldots < \frac{p_{2k+1}}{p_{2k-1}} < \frac{p_{2k-1}}{q_{2k-1}} < \ldots$$

(בפרט, מאחר שקיים $\lim_{n\to\infty} \frac{p_n}{q_n}$ אז $\frac{p_n}{q_n} \to \alpha$.

ב - לכל n, $\frac{1}{(a_{n+1}+2)q_n^2} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{a_{n+1}q_n^2}$