קירובים דיופנטיים - טענות בלבד

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:

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

♣ 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.

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:

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

למה 1.4. יהי $x\in\mathbb{R}$, אם קיימים $0<a\in\mathbb{R}$, 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:

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

אז 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:

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

[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.

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 קבוע ליוביל המוגדר ע"י (כאן $s=10$ ו-$(n_k)_{k=1}^{\infty}=(k!)_{n=1}^{\infty}$):

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

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:

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

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.

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 $\max\{q,q'\}\leq n<q+q'$.

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 $\max\{q,q'\}\leq N$), 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.

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:

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

♣ ישנו שיפור קטן לטענה זו:

משפט. משפט הורוויץ[4]

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).

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 $k \in \mathbb{N}$):

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

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

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

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

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

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

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 $k \in \mathbb{N}_0$).

[4] ערך בוויקיפדיה: אדולף הורוויץ.

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:

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

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.

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

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

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 $a^2-D\cdot b^2=\pm1$.

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.

טענה 4.6. למשוואת פל $x^2-Dy^2=1$ יש פתרון לא טריוויאלי (כלומר לא מתקיים $x=\pm1$ 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[5] 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.

[5] לא ייתכן שאחד מהם הוא 0 מפני שהפתרון לא טריוויאלי (כלומר $y\neq0$) ו-$-Dy^2<0<1$ (כלומר $x\neq0$).

משפט 4.7. יהיו $x,y\in\mathbb{N}$ כך ש-(x,y) הוא הפתרון היסודי[6], 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 $a,b<0$.

[6] כפי שאמרנו לעיל הכוונה היא שלכל $a,b\in\mathbb{N}$ המקיימים $a^{2}-Db^{2}=1$ מתקיים $x+\sqrt{D}y\leq a+\sqrt{D}b$.