נספחים לחשבון מודולרי - 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 שלשות פיתגוריות

הגדרה 1.1. נאמר ששלשה $(a,b,c)\in\mathbb{N}^3$ היא <u>שלשה פיתגורית</u> אם מתקיים $a^2+b^2=c^2$.

הגדרה 1.2. תהא $(a,b,c)\in\mathbb{N}^3$ שלשה פיתגורית, נאמר שהיא שלשה פיתגורית <u>פרימיטיבית</u> אם $\gcd(a,b,c)=1$.

הגדרה 1.3. יהי $k\in\mathbb{Z}$ חופשי מריבועים, נאמר שפתרון $(a,b,c)\in\mathbb{N}^3$ של המשוואה $x^2+ky^2=z^2$ הוא <u>פתרון פרימיטיבי</u> אם $\gcd(a,b,c)=1$.

- ♣ ניתן להוכיח שלכל $k\in\mathbb{N}$ חופשי מריבועים ופתרון פרימיטיבי (a,b,c) מתאים המספרים a, b ו-c זרים בזוגות.
- ♣ בכל המקרים הללו אנחנו לא מתעניינים בפתרונות ב-$\mathbb{Z}^3$ מפני שהפתרונות $(0,0,0)$, $(\pm1,0,\pm1)$ ו-$(\pm1,0,\mp1)$[1] הם טריוויאליים וכל פתרון שבו כל האיברים שונים מ-0 הוא שיקוף של פתרון ב-$\mathbb{N}^3$. א"כ נרצה למצוא את כל השלשות הפיתגוריות הפרימיטיביות, נשים לב שלשם כך מספיק למצוא רק את השלשות הפרימיטיביות ושבכל שלשה כזו c[2] מוכרח להיות אי-זוגי שכן אחרת נקבל ש-$4\mid c$ וזה בלתי אפשרי מפני שהוא סכום של ריבועים ולכן הדבר יגרור ש-$a\equiv b\equiv 0 \mod 4$ (השאריות הריבועיות היחידות מודולו 4 הן 0 ו-1), מכאן שמבין a ו-b אחד זוגי (מקובל לבחור את b) והאחר אי-זוגי.

סימון: לכל $k\in\mathbb{Z}$ חופשי מריבועים ולכל $m,n\in\mathbb{N}$ נסמן:

$$d_k(m,n):=\gcd\left(m^2-kn^2,2mn,m^2+kn^2\right)$$

משפט 1.4. יהי $k\in\mathbb{Z}$ חופשי מריבועים ויהא $(a,b,c)\in\mathbb{N}^3$ פתרון פרימיטיבי למשוואה $x^2+ky^2=z^2$, קיימים $n,m\in\mathbb{N}$ יחידים כך ש-$m>n$ המקיימים[3]:

$$a=\frac{m^2-kn^2}{d_k(m,n)},\ \ b=\frac{2mn}{d_k(m,n)},\ \ c=\frac{m^2+kn^2}{d_k(m,n)}$$

ולכל $n,m\in\mathbb{N}$ כך ש-$m>n$ השלשה $\left(n^2-km^2,2nm,n^2+km^2\right)$ היא פתרון של המשוואה $x^2+ky^2=z^2$.

- ♣ שימו לב שקבוצת הפתרונות הממשיים של המשוואה היא אליפסה, ההוכחה של המשפט תשתמש במעט גאומטריה וזה פשוט יפהפה!
- ♣ אם היינו מקבלים k שאינו חופשי מריבועים היינו פועלים כך:
  יהיו $p,q\in\mathbb{N}$ כך ש-$pq=k$, q חופשי מריבועים ו-p הוא ריבוע ויהי $s\in\mathbb{N}$ כך ש-$p=s^2$.
  מכאן שהמשוואה $x^2+ky^2=z^2$ שקולה למשוואה $x^2+q(sy)^2=z^2$ ולכן כל פתרון שלה מקיים ש-(x,sy,z) הוא פתרון של המשוואה $x^2+qy^2=z^2$ ו-q חופשי מריבועים,
  ומצד שני לכל פתרון של המשוואה $x^2+qy^2=z^2$ כך ש-$s\mid y$ מקיים ש-$\left(x,\frac{y}{s},z\right)$ הוא פתרון של המשוואה $x^2+ky^2=z^2$.
- ♣ ניתן לשנות את המקדם של x^2 אולם המקדם הזה מוכרח להיות ריבוע כדי שנוכל למצוא פתרון כדוגמת $(-1,0)$ שביחס אליו נבנה את השיפועים של כל הפתרונות האחרים (ראו את ההוכחה בקובץ ההוכחות).

---

[1] כש-$k=1$ (שלשות פיתגוריות) נוספים גם הפתרונות $(0,\pm1,\pm1)$ ו-$(0,\pm1,\mp1)$.

[2] כלומר היתר, המספר שנמצא לבדו בצד אחד של המשוואה בניסוחה הקלאסי: $a^2+b^2=c^2$.

[3] השלשה $\left(n^2-km^2,2nm,n^2+km^2\right)$ אינה בהכרח פתרון פרימיטיבי: קחו כל פתרון פרימיטיבי, מצאו את ה-n וה-m שלו (יש כאלה לפי המשפט) הגדירו $m_0:=q\cdot m,\ \ n_0:=q\cdot n$ עבור $1<q\in\mathbb{N}$ כלשהו ותקבלו ש-n_0 ו-m_0 (באמצעות אותה נוסחה) יוצרים פתרון שאינו פרימיטיבי (כל האיברים בשלשה מתחלקים ב-q^2).

הוכחה. נסמן $x := \frac{a}{c},\ y := \frac{b}{c}$ ונזכור שאנו עוסקים במקרה שבו $b \neq 0$ ומכאן ש-$a^2 \neq c^2$ ולכן $a \neq -c$ וממילא $x \neq -1$.
יהי $l \in \mathbb{R}$ השיפוע שבין הנקודות (x,y) ו-$(-1,0)$, מהגדרה זהו $l := \frac{y}{x+1} = \frac{b}{a+c} \neq 0$ ולכן l רציונלי, א"כ יהיו $m,n \in \mathbb{N}$ כך ש-$l = \frac{n}{m}$.
x ו-y מקיימים:

$$y = l\left(x+1\right)$$

$$\Rightarrow x^2 + kl^2\left(x+1\right)^2 = x^2 + ky^2 = \left(\frac{a}{c}\right)^2 + k\left(\frac{b}{c}\right)^2 = \frac{a^2+kb^2}{c^2} = \frac{c^2}{c^2} = 1$$

לכל $-1 \neq r \in \mathbb{R}$ המקיים $r^2 + kl^2\left(r+1\right)^2 = 1$ מתקיים:

$$\begin{aligned} 0 &= r^2 + kl^2\left(r+1\right)^2 - 1 \\ &= r^2 + kl^2r^2 + 2kl^2r + kl^2 - 1 \\ &= \left(kl^2+1\right)r^2 + 2kl^2r + \left(kl^2-1\right) \end{aligned}$$

מכאן שע"פ נוסחת השורשים כל r כזה מקיים גם:

$$\begin{aligned} r &= \frac{-2kl^2 \pm \sqrt{4k^2l^4 - 4\left(kl^2+1\right)\left(kl^2-1\right)}}{2\left(kl^2+1\right)} \\ &= \frac{-2kl^2 \pm \sqrt{4k^2l^4 - 4\left(k^2l^4-1\right)}}{2\left(kl^2+1\right)} \\ &= \frac{-2kl^2 \pm 2\cdot\sqrt{k^2l^4 - \left(k^2l^4-1\right)}}{2\left(kl^2+1\right)} \\ &= \frac{-2\cdot kl^2 \pm 2}{2\left(kl^2+1\right)} = \frac{-kl^2 \pm 1}{kl^2+1} \end{aligned}$$

אבל מכיוון ש-r הוגדר להיות שונה מ--1 זה אומר שמתקיים:

$$r = \frac{-kl^2+1}{kl^2+1} = \frac{-k\cdot\left(\frac{n}{m}\right)^2+1}{k\cdot\left(\frac{n}{m}\right)^2+1} = \frac{m^2-kn^2}{m^2+kn^2}$$

אנחנו עוסקים במקרה שבו $x \neq -1$ (ראינו לעיל את הנימוק), כעת נזכור שהמשוואה הריבועית הנ"ל הוגדרה כך ש-x הוא פתרון שלה ולכן:

$$\frac{a}{c} = x = \frac{m^2-kn^2}{m^2+kn^2}$$

$$\begin{aligned} \Rightarrow \frac{b}{c} = y = l\left(x+1\right) &= \frac{n}{m}\cdot\left(\frac{m^2-kn^2}{m^2+kn^2}+1\right) \\ &= \frac{n}{m}\cdot\left(\frac{m^2-kn^2+kn^2+m^2}{m^2+kn^2}\right) \\ &= \frac{n}{m}\cdot\left(\frac{2m^2}{m^2+kn^2}\right) = \frac{2mn}{m^2+kn^2} \end{aligned}$$

השלשה $\left(m^2-kn^2,2mn,m^2+kn^2\right)$ היא פתרון של המשוואה בעצמה[4] ומכיוון שהיחסים בין איבריה זהים לאלה של (a,b,c) נדע ששתי השלשות הן כפולה של אותו פתרון פרימיטיבי, מכאן שאם נחלק את השלשה $\left(m^2-kn^2,2mn,m^2+kn^2\right)$ ב-$d_k\left(m,n\right)$ נקבל את הפתרון הפרימיטיבי המתאים, כלומר את (a,b,c). ■

♣ את הפרמטריזציה עם שיפוע הישר ניתן לעשות לכל משוואה דיופנטית מדרגה 2 בעלת שני נעלמים.

מסקנה 1.5. תהא $(a,b,c)\in\mathbb{N}^3$ שלשה פיתגורית פרימיטיבית כך ש-b זוגי; קיימים $n,m\in\mathbb{N}$ כך ש-$m>n$, אחד מהם זוגי והאחר אינו זוגי ($n\not\equiv m \mod 2$), המקיימים:

$$a=\frac{m^2-n^2}{d_1\left(m,n\right)},\ \ b=\frac{2mn}{d_1\left(m,n\right)},\ \ c=\frac{m^2+n^2}{d_1\left(m,n\right)}$$

♣ סימן לזיכרון: הפרש ריבועיהם, כפל מכפלתם וסכום ריבועיהם (תיבת האוצרות של פרופסור סטיוארט, הוצאת כינרת-זמורה ביתן, עמוד 75).

[4] מתקיים:

$$\begin{aligned}\left(m^2-kn^2\right)^2+k\left(2mn\right)^2&=m^4-2km^2n^2+k^2n^4+4km^2n^2\\&=m^4+2km^2n^2+k^2=\left(m^2+kn^2\right)^2\end{aligned}$$

2 מספרים P-אדיים

לפני שנתחיל לעסוק בנושא זה נזכיר בקצרה כמה הגדרות הקשורות למטריקה.

הגדרה. פונקציה $d:X\times X\to\mathbb{R}$ תקרא מטריקה על הקבוצה X אם היא מקיימת את שלוש התכונות הבאות:

1. חיוביות בהחלט: לכל $x,y\in X$ מתקיים $d\left(x,y\right)\geq0$ ובנוסף $x=y\Longleftrightarrow d\left(x,y\right)=0$.
2. סימטריה: $d\left(x,y\right)=d\left(y,x\right)$ לכל $x,y\in X$.
3. א"ש המשולש: מתקיים $d\left(x,z\right)\leq d\left(x,y\right)+d\left(y,z\right)$.

קבוצה שעליה מוגדרת מטריקה נקראת מרחב מטרי.

הגדרה. כדור פתוח במרחב מטרי:

יהי $\left(X,d\right)$ מרחב מטרי ויהיו $x\in X$ ו-$0<r\in\mathbb{R}$, הכדור הפתוח ברדיוס r סביב x הוא הקבוצה:

$$B_{d}\left(x,r\right):=\left\{ y\in X\mid d\left(x,y\right)<r\right\}$$

סימון: נסמן את הריבוי של ראשוני p בפירוק של שלם a גם ע"י $v_{p}\left(a\right):=\text{Ord}_{p}\left(a\right)$ ונקרא ל-$v_{p}\left(a\right)$ ההערכה ה-p-אדית של a.

♣ לכל מספר $1<N\in\mathbb{N}$ ולכל $m\in\mathbb{Z}$ ניתן להציג את m בבסיס ספירה N בצורה יחידה ע"י $m=\text{sgn}\left(m\right)\cdot\sum_{i=0}^{k}a_{i}\cdot N^{i}$ (כאשר $N\geq a_{i}\in\mathbb{N}_{0}$ ו-$a_{k}\neq0$) כמו כן ניתן לייצג כל מספר ממשי $x\in\mathbb{R}$ ע"י טור מהצורה $x=\text{sgn}\left(x\right)\cdot\left[\sum_{i=0}^{k}b_{i}\cdot N^{i}+\sum_{i=1}^{\infty}c_{i}\cdot N^{-i}\right]$ (וזהו אכן טור מתכנס שכן מתקיים $N\geq c_{i}\in\mathbb{N}_{0}$ לכל $i\in\mathbb{N}$), לא אפרט כאן איך זה עובד מפני שאני מניח שכולנו יודעים לעבוד עם בסיסי ספירה שונים (אתם מוזמנים לקרוא על כך בוויקיפדיה: בסיס ספירה).

במספרים p-אדיים אנחנו מייצגים את המספרים השלמים[5] בבסיס ראשוני p אלא שהערך המוחלט ה-p-אדי של $n=\text{sgn}\left(n\right)\cdot\sum_{i=1}^{k}a_{i}\cdot p^{k}$ יהיה p^{-j} כאשר $j:=\min\left\{ i:0\leq i\leq k,\ \ a_{i}\neq0\right\}$, כלומר הערך המוחלט הוא ההופכי של ערך הספרה הקטנה ביותר השונה מאפס[6] ולכן בעצם זה שקול לכך שניקח את ערך הספרה הגדולה ביותר של $\sum_{i=0}^{k}a_{i}\cdot p^{-k}$; מסיבה זו דווקא הטור $\sum_{i=1}^{\infty}a_{i}\cdot p^{k}$ הוא זה שמתכנס עבור הערך מוחלט ה-p-אדי ולא הטור $\sum_{i=1}^{\infty}a_{i}\cdot p^{-k}$ (שמתכנס עבור הערך המוחלט הרגיל). בהמשך נגדיר גם את המטריקה ה-p-אדית ע"י הערך המוחלט ה-p-אדי של ההפרש בין שני מספרים ואז בעצם מה שהמטריקה תבדוק הוא את ערך הספרה הקטנה ביותר של ההפרש בניגוד למטריקה הרגילה שעבורה אם היינו רוצים לעגל את החישוב באופן דומה היינו לוקחים דווקא את ערך הספרה הגדולה ביותר של ההפרש.

---

[5] ולא רק אותם אבל זה מה שנלמד במסגרת קורס זה.

[6] בייצוג של של המספר בבסיס p.

הגדרה 2.1. הערך המוחלט ה-p-אדי

לכל $p \in \mathbb{N}$ ראשוני נגדיר הערך המוחלט ה-p-אדי ע"י (לכל $a \in \mathbb{Z}$):

$$|a|_p := \begin{cases} p^{-v_p(a)} & a \neq 0 \\ 0 & a = 0 \end{cases}$$

♣ הרעיון הוא שככל שהריבוי של p בפירוק של a גדול יותר כך a "קרוב יותר" לנקודת האפס של הערך המוחלט הזה.

♣ ניתן היה להגדיר את ההגדרה הזו לכל טבעי גדול מ-1 ולאו דווקא ראשוניים, הסיבה להגדיר זאת דווקא כך היא "כלל המכפלה" המופיע בטענה הבאה.

♣ אודי הגדיר את הערך המוחלט בצורה שונה: $|a|_p := e^{v_p(a)}$ עבור $e \in \mathbb{R}$ כלשהו המקיים $0 < e < 1$, כמובן שזה שקול (גיא בחר $e := p^{-1}$).

טענה 2.2. נוסחת המכפלה: לכל $0 \neq a \in \mathbb{Z}$ מתקיים[7] $|a| \cdot \prod_p |a|_p = 1$.

טענה 2.3. לכל $p \in \mathbb{N}$ ראשוני הערך המוחלט ה-p-אדי מקיים את שלוש התכונות הבאות[8]:

1. חיוביות בהחלט: לכל $a \in \mathbb{Z}$ מתקיים $|a|_p \geq 0$ ובנוסף $a = 0 \Longleftrightarrow |a|_p = 0$.
2. כפליות: לכל $0 \neq a, b \in \mathbb{Z}$ מתקיים $|a|_p \cdot |b|_p = |ab|_p$.
3. א"ש המשולש הלא ארכימדי: לכל $0 \neq a, b \in \mathbb{Z}$ מתקיים $\boldsymbol{|a \pm b|_p \leq \max\left\{|a|_p, |b|_p\right\}} \leq |a|_p + |b|_p$.

♣ כשמדברים על א"ש המשולש הלא ארכימדי מתכוונים לחלק המודגש של אי-השוויון, הוספתי את החלק האחר כדי להראות שמדובר בטענה חזקה יותר מא"ש המשולש הרגיל.

♣ א"ש המשולש הלא ארכימדי נובע מהעובדה שלכל $0 \neq a, b \in \mathbb{Z}$ מתקיים $v_p(a \pm b) \geq \min\{v_p(a), v_p(b)\}$.

הגדרה 2.4. המטריקה ה-p-אדית

בהינתן $p \in \mathbb{N}$ ראשוני נגדיר את המטריקה ה-p-אדית ע"י (לכל $a, b \in \mathbb{Z}$) $d_p(a, b) := |a - b|_p$.

♣ ושוב הרעיון הוא שככל שהריבוי של p בפירוק של $a - b$ גדול יותר כך a "קרוב יותר" ל-b במטריקה הזו.

טענה 2.5. המטריקה ה-p-אדית היא אכן מטריקה.

טענה 2.6. יהיו $a, b \in \mathbb{Z}$ כך ש-$v_p(a) \neq v_p(b)$, מתקיים $|a \pm b|_p = \max\left\{|a|_p, |b|_p\right\}$.

♣ טענה זו שקולה לכך שמתקיים $\mathrm{Ord}_p(a \pm b) = \min\{\mathrm{Ord}_p(a), \mathrm{Ord}_p(b)\}$.

טענה 2.7. יהיו $a \in \mathbb{Z}$, $p \in \mathbb{N}$ ראשוני ו-$b \in B_{d_p}(a, r)$; מתקיים $B_{d_p}(b, r) = B_{d_p}(a, r)$.

♣ בתרגול ראינו יותר מזה שאם $a \neq 0$ אז $B_{d_p}(a, r)$ הוא בעצם הקבוצה $\{a + k \cdot p^t \mid k \in \mathbb{Z}\}$ כאשר $t := \lceil \log_p(r) \rceil$, זוהי קבוצת האיברים של סדרה חשבונית אינסופית (בשני הכיוונים) ולכן ברור מניין הסימטרייה בין a ל-b וממילא השוויון הנ"ל.

הוכחה. יהי $x \in B_{d_p}(a, r)$.

$$\Rightarrow |b - x|_p \leq |b - a + a - x|_p \leq \max\left\{|b - a|_p, |a - x|_p\right\} < r$$

$$\Rightarrow B_{d_p}(a, r) \subseteq B_{d_p}(b, r)$$

באותה צורה נוכיח ש-$B_{d_p}(b, r) \subseteq B_{d_p}(a, r)$ (נחליף תפקידים בין a ל-b) ומכאן ש-$B_{d_p}(b, r) = B_{d_p}(a, r)$. ■

[7] כאשר $|a|$ הוא הערך המוחלט הרגיל של a והמכפלה עוברת על כל הראשוניים.

[8] היינו מצפים מכל ערך מוחלט שיהיה אי-שלילי, כפלי ויקיים את א"ש המשולש.

למה 2.8. יהי $p \in \mathbb{N}$ ראשוני ויהיו $a, b \in \mathbb{Z}$ כך ש-$a \equiv b \not\equiv 0 \mod p$, מתקיים:

$$\sum_{k=0}^{p-1} a^{p-1-k} \cdot b^k \equiv 0 \mod p$$

הוכחה. ע"פ המשפט הקטן של פרמה לכל $p - 1 \geq k \in \mathbb{N}_0$ מתקיים:

$$a^{p-1-k} \cdot b^k \equiv a^{p-1} \equiv 1 \mod p$$

$$\Rightarrow \sum_{k=0}^{p-1} a^{p-1-k} \cdot b^k \equiv \sum_{k=0}^{p-1} 1 \equiv p \equiv 0 \mod p$$

■

טענה 2.9. יהיו $p, t \in \mathbb{N}$ כך ש-p ראשוני ויהיו $a, b \in \mathbb{Z}$ כך ש-$a \equiv b \mod p^t$, מתקיים $a^p \equiv b^p \mod p^{t+1}$.

♣ בפרט, אם $p \neq 2$, נציב $b = 1$ ונקבל שמתקיים $\text{Ord}_p\left(a^p - 1\right) = \text{Ord}_p\left(a - 1\right) + 1$ לכל $0 \neq a \in \mathbb{Z}$.

הוכחה. <u>הוכחה 1 - באמצעות הלמה</u>

נניח ש-$a \equiv b \mod p^t$ עבור $t \in \mathbb{N}$ כלשהו ויהי t כנ"ל.

נשים לב שאם $a \equiv b \equiv 0 \mod p^t$, כלומר a ו-b הם כפולות של p^t, אז ודאי ש-$p^{t+1} \mid p^{2t} \mid a^2 \mid a^p$ (נזכור ש-t טבעי ו-$p \geq 2$) וכנ"ל לגבי b, ומכאן ש-$a^p \equiv b^p \equiv 0 \mod p^{t+1}$, לכן נעסוק במקרה שבו $a \equiv b \not\equiv 0 \mod p$.

מהלמה (2.8) נובע שמתקיים:

$$p \mid \sum_{k=0}^{p-1} a^{p-1-k} \cdot b^k$$

נזכור ש-$p^t \mid a - b$ ומכאן שמתקיים:

$$p^{t+1} = p^t \cdot p \mid (a - b) \cdot \sum_{k=0}^{p-1} a^{p-1-k} \cdot b^k = a^p - b^p$$

כלומר $a^p \equiv b^p \mod p^{t+1}$. ■

הוכחה. <u>הוכחה 2 - באמצעות הבינום של ניוטון</u>

נניח ש-$a \equiv b \mod p^t$ עבור $t \in \mathbb{N}$ כלשהו ויהי t כנ"ל, א"כ קיים $k \in \mathbb{Z}$ כך ש-$a = b + k \cdot p^t$, יהי k כנ"ל.

$$\Rightarrow a^p = \left(b + k \cdot p^t\right)^p = \sum_{i=0}^{p} \binom{p}{i} \cdot b^{p-i} \cdot \left(k \cdot p^t\right)^i$$

$$= b^p + p \cdot b^{p-1} \cdot k \cdot p^t + \sum_{i=2}^{p} \binom{p}{i} \cdot b^{p-i} \cdot k^i \cdot p^{t \cdot i}$$

כעת נשים לב לכך ש-p^{t+1} מחלק את $p^t \cdot k \cdot a^{p-1} \cdot p$ וגם את $p^{t \cdot i}$ לכל $2 \leq i \in \mathbb{N}$ ומכאן שמתקיים $a^p \equiv b^p \mod p^{t+1}$. ■

מסקנה 2.10. לכל $a, b \in \mathbb{Z}$, אם $d_p\left(a, b\right) < 1$ אז $d_p\left(a^p, b^p\right) < d_p\left(a, b\right)$.

3 הצגת מספר כסכום של שני ריבועים

הגדרה 3.1. נאמר שמספר $n\in\mathbb{Z}$ ניתן להצגה כסכום של שני ריבועים אם קיימים $x,y\in\mathbb{Z}$ כך ש-$n=x^2+y^2$.

- ♣ כמובן שמהגדרה א"א להציג שלמים שליליים כסכום של שני ריבועים.
- ♣ כמובן שניתן לדרוש ש-x ו-y יהיו אי-שליליים.

שאלה: מתי ניתן להציג מספר טבעי כסכום של שני ריבועים?

למה 3.2. יהי $2<p\in\mathbb{N}$ ראשוני, התנאים הבאים שקולים:

1. $p\equiv 1 \mod 4$.
2. קיים $x\in\mathbb{F}_p$ כך ש-$x^2=-1$ (בשדה).
3. קיימים $x,y\in\mathbb{Z}$ לא טריוויאליים (כלומר $x\not\equiv 0 \mod p$ וגם $y\not\equiv 0 \mod p$)[9] כך ש-$x^2+y^2\equiv 0 \mod p$.

הוכחה. את השקילות בין שני הסעיפים הראשונים כבר ראינו, נוכיח את השקילות בין שני הסעיפים האחרונים: יהי $2<p\in\mathbb{N}$ ראשוני, מצד אחד אם קיים $x\in\mathbb{F}_p$ כך ש-$x^2\equiv -1 \mod p$ אז אותו x מקיים $x^2+1^2\equiv 0 \mod p$ (ובוודאי שיקיים גם $x\not\equiv 0 \mod p$), ומצד שני אם קיימים $x,y\in\mathbb{Z}$ לא טריוויאליים כך ש-$x^2+y^2\equiv 0 \mod p$ אז $\gcd(p,y)=1$ ולכן קיימים $a,b\in\mathbb{Z}$ כך ש-$1=a\cdot p+b\cdot y$, כלומר $b\cdot y=1-a\cdot p\equiv 1 \mod p$ ומכאן שגם:

$$(b\cdot x)^2+1^2\equiv(b\cdot x)^2+(b\cdot y)^2\equiv b^2\cdot\left(x^2+y^2\right)\equiv b^2\cdot 0\equiv 0 \mod p$$

וממילא $(b\cdot x)^2\equiv -1 \mod p$. ■

טענה 3.3. יהיו $q\in\mathbb{N}$ ו-$r,s\in\mathbb{Z}$ כך ש-$q=r^2+s^2$ ו-q ראשוני, נסמן $\pi:=r+si$, מתקיים $\mathbb{Z}[i]=\mathbb{Z}+\pi\cdot\mathbb{Z}[i]$.

הוכחה. נסמן $R:=\mathbb{Z}+\pi\cdot\mathbb{Z}[i]$ ונשים לב לכך ש-$R\subseteq\mathbb{Z}[i]$ וש-R סגורה לחיבור ולכפל.
בוודאי ש-$si=-r+\pi\cdot 1\in R$, בנוסף מכיוון ש-$\overline{\pi}\cdot i\in\mathbb{Z}[i]$ נדע שגם $qi=\pi\cdot\overline{\pi}\cdot i\in\pi\cdot\mathbb{Z}[i]\subseteq R$; מהגדרה $\gcd(q,s)=1$ ולכן קיימים $n.m\in\mathbb{Z}$ כך ש-$1=n\cdot q+m\cdot s$, א"כ מהסגירות של R לחיבור ולכפל נובע ש-$i\in R$ שהרי $i=n\cdot qi+m\cdot si$; כמובן ש-$1\in R$ ולכן $\mathbb{Z}[i]\subseteq R$ ומכאן ש-$R=\mathbb{Z}[i]$. ■

משפט 3.4. יהי $2<p\in\mathbb{N}$ מספר ראשוני, p ניתן להצגה כסכום של שני ריבועים אם"ם $p\equiv 1 \mod 4$.

- ♣ כמובן ש-2 ניתן להצגה כסכום של שני ריבועים: $2=1^2+1^2$.

הוכחה. נוכיח את הטענה באינדוקציה שלמה.
בסיס האינדוקציה הוא הראשוני 5 ($5=1^2+2^2$), א"כ יהי $5<p\in\mathbb{N}$ ראשוני המקיים $p\equiv 1 \mod 4$ ונניח שלכל ראשוני $p>q\in\mathbb{N}$ המקיים $p\equiv 1 \mod 4$ ניתן להציג את q כסכום של שני ריבועים.
נגדיר:

$$S:=\left\{1\leq N\in\mathbb{N}\mid \exists x,y\in\mathbb{Z}:x^2+y^2=N\cdot p\wedge p\nmid x,y\right\}$$

כלומר S היא קבוצת הטבעיים שהמכפלה שלהם ב-p ניתנת להצגה כסכום של שני ריבועים לא טריוויאליים; מסעיף 3 בלמה נובע ש-S לא ריקה ולכן אם נצליח להוכיח שלכל $N\in S$ קיים $N>N'\in S$ נדע ש-$1\in S$ ולכן p ניתן להצגה כסכום של שני ריבועים (זהו רעיון הירידה של פרמה).
יהי $1<N\in S$ ויהיו $x,y\in\mathbb{Z}$ כך ש-$N\cdot p=x^2+y^2$ ובנוסף x ו-y אינם כפולות של p.
יהיו $a,b\in\mathbb{Z}$ כך ש-$a\equiv x \mod p$ ו-$b\equiv y \mod p$ ובנוסף $-\frac{p}{2}<a,b<\frac{p}{2}$ (מהגדרה $a,b\neq 0$), אנחנו יכולים להניח את התנאי

[9] העובדה שאחד מהם אינו טריוויאלי גוררת שגם האחר אינו טריוויאלי.

האחרון מפני שלכל מחלקה ב-$\mathbb{Z}/p\mathbb{Z}$ יש נציג בטווח המדובר. מהגדרה מתקיים $a^2+b^2 \equiv 0 \mod p$, א"כ קיים $N_0 \in \mathbb{N}$ כך ש-$N_0 \cdot p = a^2+b^2$, נשים לב לכך שמתקיים $\frac{p^2}{2} = \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 > a^2+b^2$ ומכאן ש-$N_0 < \frac{p}{2}$.
נניח ש-$N_0 > 1$ (אחרת סיימנו) ויהי $q \in \mathbb{N}$ ראשוני כך ש-$q \mid N_0$.
נעסוק תחילה בשני המקרים הקלים יותר:

- אם $q = 2$ אז נשים לב לכך ש-$a^2+b^2 \in \text{Even}$ (שהרי $N_0 \cdot p \in \text{Even}$) ולכן a ו-b הם מאותה זוגיות (או ששניהם זוגיים או ששניהם אי-זוגיים) ומכאן שסכומם והפרשם זוגיים וממילא $\frac{a+b}{2}, \frac{a-b}{2} \in \mathbb{Z}$. כעת נשים לב לכך שמתקיים:
$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 = \frac{a^2+b^2}{2} = \frac{N_0}{2} \cdot p$$
והרי N_0 זוגי ולכן $\frac{N_0}{2} = \frac{N_0}{q} \in S$.

- אם $q \equiv 3 \mod 4$ אז מהלמה נוכל להניח בהג"כ ש-$a \equiv 0 \mod q$, כלומר $q \mid a$ ולכן גם $q \mid a^2$ ומכיוון ש-$q \mid a^2+b^2$ נדע ש-$q \mid b^2$ ומכיוון ש-q ראשוני מתקיים גם $q \mid b$, א"כ $q^2 \mid a^2, b^2$ ולכן גם $q^2 \mid a^2+b^2$, כלומר $q^2 \mid N_0 \cdot p$ אבל $\gcd\left(p, q^2\right) = 1$ ולכן מטענה שלמדנו נובע ש-$q^2 \mid N_0$; כעת נשים לב לכך שמתקיים:
$$\left(\frac{a}{q}\right)^2 + \left(\frac{b}{q}\right)^2 = \frac{N_0}{q^2} \cdot p$$
והרי $\frac{a}{q}, \frac{b}{q}, \frac{N_0}{q^2} \in \mathbb{Z}$ ולכן $\frac{N_0}{q^2} \in S$.

- כעת נעסוק במקרה שבו $q \equiv 1 \mod 4$, q מחלק את N_0 ולכן $q \le N_0 < \frac{p}{2} < p$ ומכאן שניתן להשתמש לגביו בהנחת האינדוקציה, א"כ יהיו $r, s \in \mathbb{Z}$ כך ש-$q = r^2+s^2$ ונסמן $\pi := r + si \in \mathbb{Z}[i]$.
נרצה להוכיח ש-$\pi \mid a+bi$ וגם $\pi \mid a-bi$.

מהטענה נובע שניתן להציג את חוג השלמים של גאוס כך: $\mathbb{Z}[i] = \mathbb{Z} + \pi \cdot \mathbb{Z}[i]$, א"כ יהיו $n_1, n_2 \in \mathbb{Z}$ ו-$z_1, z_2 \in \mathbb{Z}[i]$ כך ש-$a+bi = n_1 + \pi \cdot z_1$ ו-$a-bi = n_2 + \pi \cdot z_2$.
כעת נניח בשלילה ש-π אינו מחלק את $a \pm bi$ (ב-$\mathbb{Z}[i]$!) ומכאן ש-π אינו מחלק את n_1 ו-n_2 ומכיוון ש-$q = \pi \cdot \overline{\pi}$ גם אינו מחלק אותם (ב-$\mathbb{Z}[i]$! ...ובפרט ב-$\mathbb{Z}$), אבל $q \mid a^2+b^2$ (ב-$\mathbb{Z}$ וקל וחומר שב-$\mathbb{Z}[i]$) ומכאן שגם π מחלק את a^2+b^2 (ב-$\mathbb{Z}[i]$), כלומר π מחלק את $a^2+b^2 = (a+bi)(a-bi) = n_1 \cdot n_2 + \pi \cdot (m_1 + m_2 + m_1 \cdot m_2 \cdot \pi)$ ולכן גם את $n_1 \cdot n_2$, א"כ $\overline{\pi}$ מחלק את $\overline{n_1 \cdot n_2} = n_1 \cdot n_2$ ולכן $q = \pi \cdot \overline{\pi} \mid (n_1)^2 \cdot (n_2)^2$ וזאת בסתירה לכך ש-q ראשוני! מכאן שבהג"כ ניתן להניח ש-$\pi \mid a+bi$, כלומר קיים $\omega \in \mathbb{Z}[i]$ כך ש-$a+bi = \pi \cdot \omega$ ומכאן שמתקיים:
$$a^2+b^2 = (a+bi) \cdot (a-bi) = \pi \cdot \overline{\pi} \cdot \omega \cdot \overline{\omega} = q \cdot (\omega \cdot \overline{\omega})$$
יהיו $u, v \in \mathbb{Z}$ כך ש-$\omega = u + vi$ ומכאן ש-$a^2+b^2 = q \cdot \left(u^2+v^2\right)$ ולכן מתקיים גם:
$$u^2+v^2 = \frac{a^2+b^2}{q} = \frac{N_0}{q} \cdot p$$
ומכאן ש-$\frac{N_0}{q} \in S$.

■

טענה 3.5. לכל $n, m \in \mathbb{N}$ שניתן להציגם כסכום של שני ריבועים ניתן להציג גם את $n \cdot m$ כמכפלה של שני ריבועים.

♣ כמובן שלכל $n \in \mathbb{Z}$ ניתן להציג n^2 כסכום של שני ריבועים ($n^2 = n^2 + 0^2$) ובפרט עבור $2 < p \in \mathbb{N}$ ראשוני המקיים $p \equiv 3 \mod 4$.

הוכחה. יהיו $n,m\in\mathbb{N}$ כנ"ל ויהיו $a,b,c,d\in\mathbb{Z}$ כך ש-$n=a^2+b^2$ ו-$m=c^2+d^2$, א"כ מתקיים (ב-$\mathbb{Z}[i]$):

$$\begin{aligned}n\cdot m&=(a+bi)(a-bi)(c+di)(c-di)\\&=(a+bi)(c+di)(a-bi)(c-di)\\&=[(ac-bd)+(ad+bc)i]\cdot[(ac-bd)-(ad+bc)i]\\&=(ac-bd)^2+(ad+bc)^2\end{aligned}$$

והרי $(ac-bd),(ad+bc)\in\mathbb{Z}$ ומכאן שמצאנו הצגה של $n\cdot m$ כסכום של שני ריבועים. ■

מסקנה 3.6. יהי $n\in\mathbb{N}$ ניתן להציג את n כסכום של שני ריבועים אם"ם לכל $p\in\mathbb{N}$ המקיים $p\equiv 3 \mod 4$ מתקיים $\mathrm{Ord}_p(n)\in\mathrm{Even}$.

4 השיטה העשרונית

הגדרה 4.1. הספרות

נגדיר:

$$\begin{aligned}2&:=1+1 & 5&:=4+1 & 8&:=7+1\\3&:=2+1 & 6&:=5+1 & 9&:=8+1\\4&:=3+1 & 7&:=6+1 & 10&:=9+1\end{aligned}$$

$$\mathrm{Digits}:=\{0,1,2,3,4,5,6,7,8,9\}$$

הגדרה 4.2. הצגה עשרונית סופית

לכל סדרה סופית $(a_n,\ldots,a_2,a_1,a_0,a_{-1},a_{-2},\ldots,a_{-m})$ שכל איבריה ב-Digits נזהה את הסדרה עם המספר:

$$\sum_{k=-m}^{n}a_k\cdot 10^k$$

ונכתוב אותה ברצף (ללא פסיקים), כך[10]:

$$a_n\ldots a_2a_1a_0.a_{-1},a_{-2}\ldots a_{-m}:=\sum_{k=-m}^{n}a_k\cdot 10^k$$

הצגה זו נקראת <u>ההצגה העשרונית</u> של המספר $\sum_{k=-m}^{n}a_k\cdot 10^k$, וכשנרצה לכתוב את הנגדי שלו נוסיף סימן "$-$" בקצה השמאלי של המחרוזת.

לדוגמה: $93856.7664:=4\cdot10^{-4}+6\cdot10^{-3}+6\cdot10^{-2}+7\cdot10^{-1}+6\cdot10^{0}+5\cdot10^{1}+8\cdot10^{2}+3\cdot10^{3}+9\cdot10^{4}$, קיים מנהג מקובל להוסיף "מפריד אלפים" בין כל שלישיית ספרות (החל מהנקודה העשרונית), כך: $93,856.7664$.

♣ ניתן להציג בצורה זו כל מספר טבעי וכל שבר מצומצם $\frac{p}{q}\in\mathbb{Q}$ כך שהראשוניים היחידים בפירוק של q הם 2 ו/או 5.

[10] הנקודה המודגשת באדום נקראת <u>הנקודה העשרונית</u>.

למה 4.3. לכל $x\in\mathbb{R}$ קיימת סדרת $(a_k)_{k=-\infty}^{n}$ ספרות[11] המקיימת:

$$x=\operatorname{sgn}(x)\cdot\sum_{k=-\infty}^{n}a_k\cdot 10^k$$

הגדרה 4.4. הצגה עשרונית אין-סופית

לכל סדרה סופית $(a_k)_{k=-\infty}^{n}$ שכל איבריה ב-Digits נזהה את הסדרה עם המספר:

$$\sum_{k=-\infty}^{n}a_k\cdot 10^k$$

ונכתוב אותה ברצף (ללא פסיקים), כך:

$$a_n\ldots a_2a_1a_0.a_{-1},a_{-2}\ldots:=\sum_{k=-\infty}^{n}a_k\cdot 10^k$$

הצגה זו נקראת ההצגה העשרונית של המספר $\sum_{k=-\infty}^{n}a_k\cdot 10^k$, וכשנרצה לכתוב את הנגדי שלו נוסיף סימן "$-$" בקצה השמאלי של המחרוזת.

- ♣ הצגה כזו נקראת הפיתוח העשרוני של x והיא יחידה עד כדי התחכמויות מהצורות הבאות:

$$\frac{1}{2}=0.5=0.49999999\ldots=0.5000000\ldots$$

- ♣ התחכמות זו אפשרית רק עבור רציונליים שהפיתוח העשרוני שלהם סופי[12], א"כ נאמר שאם יש למספר פיתוח עשרוני סופי אז זהו הפיתוח העשרוני שלו למרות שניתן להציגו גם אחרת.
- ♣ כמובן שכל מה שנאמר בפרק זה על השיטה העשרונית נכון לכל בסיס ספירה אחר (עם ההתאמות הנדרשות: יש להחליף את 2 ו-5 בראשוניים המופיעים בפירוק של בסיס הספירה).

הגדרה 4.5. יהי $x\in\mathbb{R}$, נאמר שהפיתוח העשרוני של x הוא מחזורי אם עבור סדרת הספרות המתאימה[13] $(a_k)_{k=-\infty}^{n}$ להצגה העשרונית של x קיים $0\geq K\in\mathbb{Z}$ וקיים $T\in\mathbb{N}$ כך שלכל $K>k\in\mathbb{Z}$ מתקיים $a_k=a_{k-T}$ ובמקרה נכתוב את ההצגה העשרונית של בצורה מקוצרת כך:

$$a_n\ldots a_2a_1a_0.a_{-1},a_{-2}\ldots a_Ka_{K-1}\overline{a_{K-1}a_{K-2}\ldots a_{K-T}}$$

כמובן שאם קיימים K ו-T כאלה אז קיימים אינסוף כאלה[14], המינימלי מבין הטבעיים המקיימים את התפקיד של T בהגדרה יקרא אורך המחזור של הפיתוח העשרוני.

[11] הכוונה היא לסדרה המהווה פונקציה (ככל סדרה) שהתחום שלה הוא $\{k\in\mathbb{Z}\mid k\leq n\}$ והטווח שלה הוא Digits.
[12] כלומר הראשוניים היחידים בפירוק של המכנה שלהם (בהצגה המצומצמת) הם 2 ו/או 5.
[13] בפרט הפיתוח העשרוני של x אינו סופי.
[14] כל כפולה של T תתאים לתפקיד של T וכל $K+qT$ יתאים לתפקיד של K.

טענה 4.6. יהי $x \in \mathbb{R}$, הפיתוח העשרוני של x הוא סופי ו/או מחזורי אם"ם $x \in \mathbb{Q}$.

הוכחה.

- $\Leftarrow$

נניח שהפיתוח העשרוני של x הוא סופי ו/או מחזורי, אם הפיתוח סופי אז הטענה טריוויאלית ולכן נעסוק רק במקרה שהוא מחזורי.

א"כ תהא $(a_k)_{k=-\infty}^{n}$ סדרת הספרות המתאימה לפיתוח של $|x|$, יהי $0 > K \in \mathbb{Z}$ ויהי $T \in \mathbb{N}$ כך שלכל $K > k \in \mathbb{Z}$ מתקיים $a_k = a_{k-T}$.

נסמן:

$$y := \frac{1}{10^K} \cdot 0.\overline{a_{K-1}a_{K-2}\dots a_{K-T}}$$

כלומר y הוא החלק המחזורי בפיתוח של x, נשים לב לכך שמתקיים:

$$0.\overline{a_{K-1}a_{K-2}\dots a_{K-T}} = \frac{1}{10^T} \cdot \left[a_{K-1}a_{K-2}\dots a_{K-T} + 0.\overline{a_{K-1}a_{K-2}\dots a_{K-T}}\right]$$

$$\Rightarrow \frac{10^T - 1}{10^T} \cdot 0.\overline{a_{K-1}a_{K-2}\dots a_{K-T}} = \frac{a_{K-1}a_{K-2}\dots a_{K-T}}{10^T}$$
$$\Rightarrow 0.\overline{a_{K-1}a_{K-2}\dots a_{K-T}} = \frac{a_{K-1}a_{K-2}\dots a_{K-T}}{10^T - 1}$$

מכאן ש-$y \in \mathbb{Q}$ ומכיוון שמתקיים:

$$x = a_n \dots a_2 a_1 a_0.a_{-1}, a_{-2} \dots a_K a_{K-1} + \frac{1}{10^K} \cdot 0.\overline{a_{K-1}a_{K-2}\dots a_{K-T}} = \sum_{k=K-1}^{n} a_k + y$$

נדע שגם x רציונלי.

- $\Rightarrow$

נניח ש-x רציונלי ויהיו $a, b \in \mathbb{N}$ כך ש-$|x| = \frac{a}{b}$.

הטענה נובעת מתכונות החילוק הארוך:

1. בשלב הראשון אנחנו מחלקים את a ב-b עם שארית, המנה היא החלק השלם של $|x|$ והשארית (תסומן ב-r_0) היא החלק השברי.
2. נסמן $i = 0$ וכעת כל עוד $r_i \neq 0$:
   - נסמן $n_i := \min\{n \in \mathbb{N} \mid (r_i)^n \geq b\}$ ונחלק את b ב-$(r_i)^{n_i}$ עם שארית, המנה המתקבלת היא n_i הספרות הבאות בפיתוח העשרוני של x והשארית (תסומן ב-r_{i+1}) מקיימת $r_{i+1} < b$.
   - נגדיר את i להיות $i + 1$.
3. כעת נובע מעקרון שובך היונים שקיים $k \in \mathbb{N}_0$ כך ש-$r_k = 0$ (ואז הפיתוח העשרוני של $|x|$ סופי) או שקיימים $j, k \in \mathbb{N}_0$ כך ש-$j \neq k$ ו-$r_j = r_k$, ואז מכיוון שלכל $i \in \mathbb{N}_0$ הערך של r_{i+1} תלוי אך ורק ב-r_i וב-b נדע שהחל משלב זה תוצאות החילוק תחזורנה על עצמן בקביעות.

■

טענה 4.7. יהי $\frac{a}{b}\in\mathbb{Q}$ שבר מצומצם הפיתוח העשרוני של $\frac{a}{b}$ סופי אם"ם קיימים $n,m\in\mathbb{N}_0$ כך ש-$b=2^n\cdot 5^m$.

טענה 4.8. יהי $\frac{a}{b}\in\mathbb{Q}$ שבר כך ש-b זר ל-10 ותהא $(a_k)_{k=-\infty}^{n}$ סדרת הספרות המתאימה להצגה העשרונית של $\frac{a}{b}$, קיים $T\in\mathbb{N}$ כך שלכל $0>k\in\mathbb{Z}$ מתקיים $a_k=a_{k-T}$.

♣ כלומר אם המכנה זר ל-10 אז המחזוריות מתחילה מיד לאחר הנקודה העשרונית.

הוכחה. נסמן $r:=a-\left\lfloor\frac{a}{b}\right\rfloor\cdot b$, כלומר r הוא השארית של חלוקת a ב-b.
יהי $T\in\mathbb{N}$ כך ש-$10^T\equiv 1 \mod b$ (ממשפט אוילר נובע שאכן קיים כזה T), יהי T כנ"ל ויהי $q\in\mathbb{Z}$ כך ש-$10^T=1+b\cdot q$.

$$\Rightarrow b=\frac{10^T-1}{q}$$

$$\Rightarrow \frac{a}{b}=\left\lfloor\frac{a}{b}\right\rfloor\cdot b+\frac{r}{b}=\left\lfloor\frac{a}{b}\right\rfloor\cdot b+\frac{r\cdot q}{10^T-1}$$

מהגדרה מתקיים:

$$\frac{r\cdot q}{10^T-1}<1$$

מדרך ההוכחה של הכיוון הראשון בטענה 4.6 ניתן לראות שבמקרה כזה מתקיים:

$$\frac{a\cdot q}{10^T-1}=\frac{d_{-1}d_{-2}\ldots d_{-T}}{10^T-1}=0.\overline{d_Td_{T-1}\ldots d_0}$$

כאשר $(d_k)_{k=0}^{T}$היא סדרת הספרות של $r\cdot q$, כלומר:

$$r\cdot q=\sum_{k=0}^{T}d_k\cdot 10^k=d_Td_{T-1}\ldots d_0$$

■

טענה 4.9. יהי $p\in\mathbb{N}$ ראשוני שאינו 2 או 5, אורך המחזור של הפיתוח העשרוני של $\frac{1}{p}$ הוא $e_p(10)$.

הוכחה. מהגדרה p זר ל-10 ולכן מדרך ההוכחה של הטענה הקודמת (4.8) נובע שכל $T\in\mathbb{N}$ המקיים $10^T\equiv 1 \mod p$ מקיים את הגדרת המחזוריות של פיתוח עשרוני, $e_p(10)$ מוגדר להיות המינימלי מביניהם ולכן הוא אורך המחזור. ■