נספחים לחשבון מודולרי - הגדרות וטענות

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:
אקסיומות 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 שלשה פיתגורית 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 פרימיטיבית 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 פתרון פרימיטיבי 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-$n<m$ 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-$n<m$ 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, יש למשפט הוכחה גאומטרית יפהפייה שאותה נראה בקובץ ההוכחות.
- ♣ 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 $n_0:=q\cdot n,\ \ m_0:=q\cdot m$ 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).

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).

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 $d\left(x,y\right)\geq 0$ ובנוסף $x=y \iff d\left(x,y\right)=0$.
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 $v_p\left(a\right):=\mathrm{Ord}_p\left(a\right)$ 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 $m=\mathrm{sgn}\left(m\right)\cdot\sum_{i=0}^{k}a_i\cdot N^i$ (כאשר $N\geq a_i\in\mathbb{N}_0$ ו-$a_k\neq 0$) כמו כן ניתן לייצג כל מספר ממשי $x\in\mathbb{R}$ ע"י טור מהצורה $x=\mathrm{sgn}\left(x\right)\cdot\left[\sum_{i=0}^{k}b_i\cdot N^i+\sum_{i=1}^{\infty}c_i\cdot N^{-i}\right]$ (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[4] בבסיס ראשוני p אלא שהערך המוחלט ה-p-אדי של $n=\mathrm{sgn}\left(n\right)\cdot\sum_{i=1}^{k}a_i\cdot p^k$ יהיה p^{-j} כאשר $j:=\min\left\{i:0\leq i\leq k,\ \ a_i\neq 0\right\}$, כלומר הערך המוחלט הוא ההופכי של ערך הספרה הקטנה ביותר השונה מאפס[5] 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.

[4] ולא רק אותם אבל זה מה שנלמד במסגרת קורס זה.
[5] 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[6] $|a| \cdot \prod_p |a|_p = 1$.

טענה 2.3. לכל $p \in \mathbb{N}$ ראשוני הערך המוחלט ה-p-אדי מקיים את שלוש התכונות הבאות[7]:

1. חיוביות בהחלט: לכל $a \in \mathbb{Z}$ מתקיים $|a|_p \geq 0$ ובנוסף $a = 0 \iff |a|_p = 0$.
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 $|a|_p + |b|_p \geq \boldsymbol{\max\left\{|a|_p, |b|_p\right\} \geq |a \pm b|_p}$.

- ♣ 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.

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:

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

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

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

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 $\mathrm{Ord}_{p}\left(a^{p}-1\right)=\mathrm{Ord}_{p}\left(a-1\right)+1$ לכל $0\neq a\in\mathbb{Z}$.

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 $y\not\equiv 0 \mod p$[8]) כך ש-$x^{2}+y^{2}\equiv 0 \mod p$.

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 $\mathbb{Z}\left[i\right]=\mathbb{Z}+\pi\cdot\mathbb{Z}\left[i\right]$.

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: $2=1^{2}+1^{2}$.

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 $p\equiv 3 \mod 4$.

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 $\mathrm{Ord}_{p}\left(n\right)\in\mathrm{Even}$.

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

4 השיטה העשרונית

הגדרה 4.1. הספרות

נגדיר:

$$2 := 1+1 \qquad 5 := 4+1 \qquad 8 := 7+1$$
$$3 := 2+1 \qquad 6 := 5+1 \qquad 9 := 8+1$$
$$4 := 3+1 \qquad 7 := 6+1 \qquad 10 := 9+1$$

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

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[9]:

$$a_n \ldots a_2 a_1 a_0 . a_{-1}, a_{-2} \ldots a_{-m} := \sum_{k=-m}^{n} a_k \cdot 10^k$$

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

לדוגמה: $93856.7664 := 4\cdot 10^{-4} + 6\cdot 10^{-3} + 6\cdot 10^{-2} + 7\cdot 10^{-1} + 6\cdot 10^{0} + 5\cdot 10^{1} + 8\cdot 10^{2} + 3\cdot 10^{3} + 9\cdot 10^{4}$, 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.

למה 4.3. לכל $x \in \mathbb{R}$ קיימת סדרת ספרות[10] $(a_k)_{k=-\infty}^{n}$ המקיימת:

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

---

[9] הנקודה המודגשת באדום נקראת הנקודה העשרונית.

[10] הכוונה היא לסדרה המהווה פונקציה (ככל סדרה) שהתחום שלה הוא $\{k \in \mathbb{Z} \mid k \le n\}$ והטווח שלה הוא Digits.

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:

$$a_n \ldots a_2 a_1 a_0 . a_{-1}, a_{-2} \ldots := \sum_{k=-\infty}^{n} a_k \cdot 10^k$$

הצגה זו נקראת <u>ההצגה העשרונית</u> 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 <u>הפיתוח העשרוני</u> 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[11], 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 <u>מחזורי</u> אם עבור סדרת הספרות המתאימה $(a_k)_{k=-\infty}^{n}$[12] 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:

$$a_n \ldots a_2 a_1 a_0 . a_{-1}, a_{-2} \ldots a_K a_{K-1} \overline{a_{K-1} a_{K-2} \ldots a_{K-T}}$$

כמובן שאם קיימים K ו-T כאלה אז קיימים אינסוף כאלה[13], המינימלי מבין הטבעיים המקיימים את התפקיד של T בהגדרה יקרא <u>אורך המחזור</u> של הפיתוח העשרוני.

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

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.

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

[11] כלומר הראשוניים היחידים בפירוק של המכנה שלהם (בהצגה המצומצמת) הם 2 ו/או 5.
[12] בפרט הפיתוח העשרוני של x אינו סופי.
[13] כל כפולה של T תתאים לתפקיד של T וכל $K + qT$ יתאים לתפקיד של K.