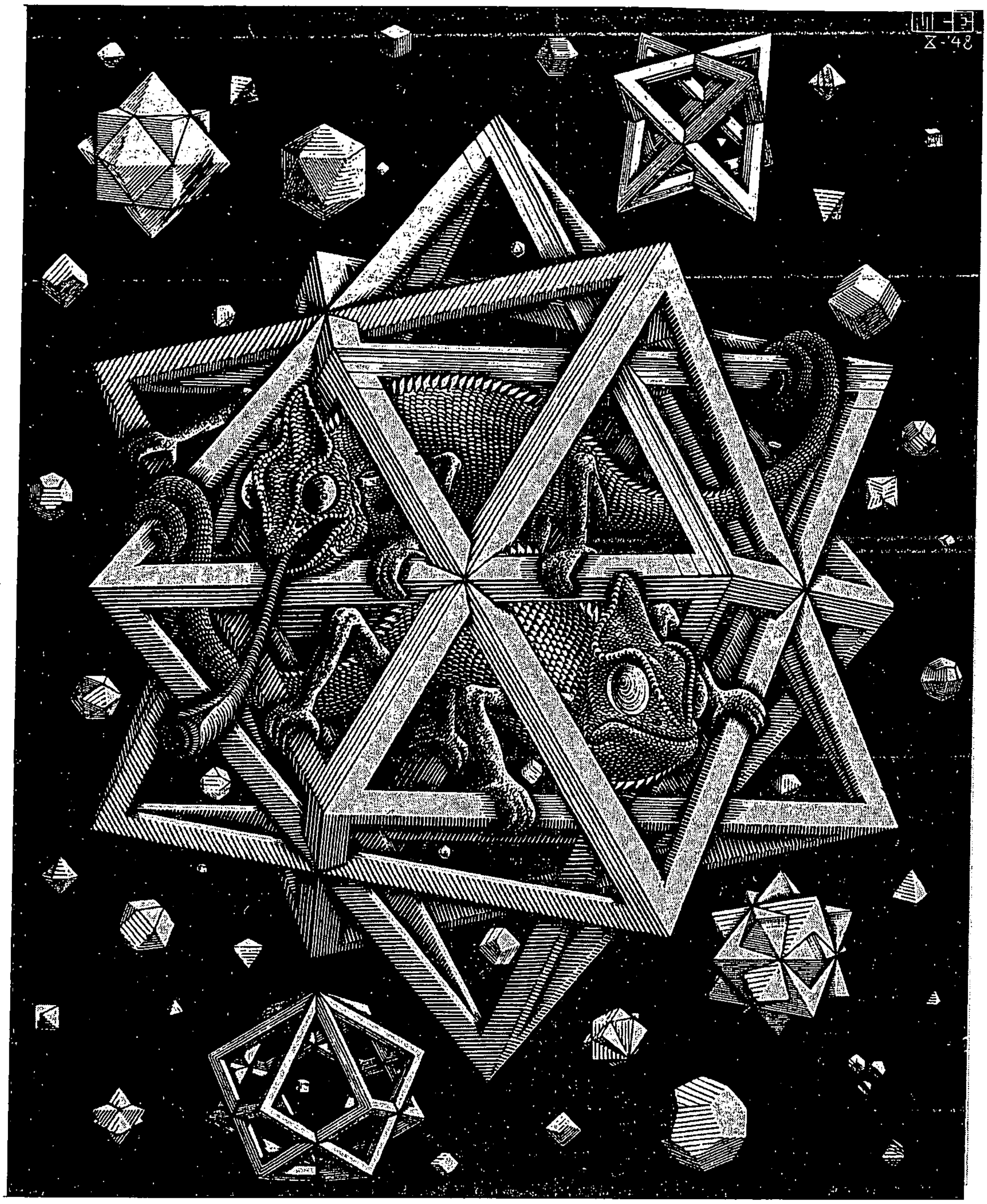
אתגר - גליונות מתמטיקה

גליון מס' 21 אדר ב' תשנ"ב - מרץ 1992



הפקולטות למתמטיקה

הטכניון
חיפה

מכון ויצמן
רחובות

בתמיכת המרכז המדעי י.ב.מ. ישראל

תוכן העניינים

אתגר - גליונות מתמטיקה ISBN = 0334-201

מוצא לאור ע"י הפקולטות למתמטיקה במכון וייצמן ובטכניון.

המערכת:

פרופ' א. ברמן וד"ר צ. הראל, הפקולטה למתמטיקה בטכניון.

פרופ' י. גיליס, המחלקה למתמטיקה שימושית, מכון וייצמן.

מען המערכת: הפקולטה למתמטיקה, הטכניון - מכון טכנולוגי לישראל

חיפה 32000, טל. 294279 - 04

דבר המערכת

אנו שמחים לחדש את הופעת "אתגר - גליונות מתמטיקה" לאחר מספר חודשי הפסקה. בהזדמנות זו אנו מחדשים את מדור הבעיות ומזמינים את קוראי העתון לנסות את כוחם ולשלח פתרונות למערכת. שמות הפותרים יפורסמו ולמצטיינים יוענקו פרסים.

בקונגרס הבינלאומי למתמטיקה שהתקיים בשנת 1900 הציע המתמטיקאי המפורסם דויד הילברט 23 בעיות, כבעיות מרכזיות למאה העשרים. המאמר של פרופ' בנימיני עוסק בגירסא המישורית לבעיה השלישית מבין בעיות אלו. משפט ידוע של מתמטיקאי מפורסם אחר, דיריקלה, אומר שסידרה חשבונית שלאיבריה אין גורם משותף גדול מ 1 , מכילה אינסוף מספרים ראשוניים. המאמר של גיל אלון נותן הוכחה פשוטה ואלגנטית למקרה פרטי של משפט זה. המאמר השלישי בגליון, מאמרו של אליהו לוי, מראה שכבר לפני 2000 שנה ידעו הסינים להשתמש ב"נתונים מסודרים בלוח בצורת מלבן", כלומר במטריצות.

אנו מאחלים לקוראים חג פורים שמח ומקוים שהגליון הבא יצא לאור עוד לפני חופשת הפסח.

ה ו ד ע ה

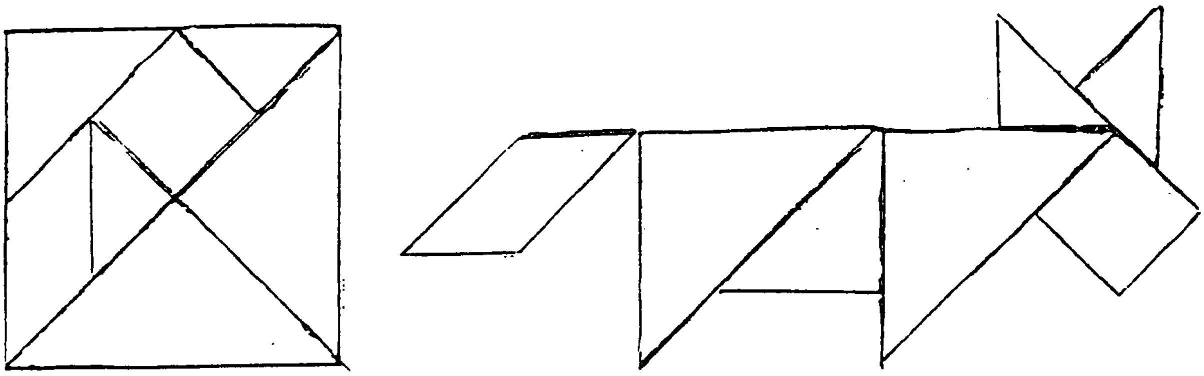
האולימפידה ה-33 ע"ש פרופ' גרוסמן תתקיים בקרית הטכניון ב 10.4.1992.
קוראי העתון מוזמנים להשתתף.

פרטים והרשמה: הפקולטה למתמטיקה בטכניון, חיפה 32000, טל. 294281(04)

פרוק והרכבה של מצולעים במישור *

מאת יואב בנימיני, הפקולטה למתמטיקה בטכניון

כולנו מכירים את המשחק "טנגרם": מחלקים ריבוע לכמה חלקים, ואנו נדרשים להרכיב מחלקים אלה צורות מסויימות אחרות:



מהן כל הצורות שאפשר להרכיב באופן כזה ? מהן הצורות שניתן להרכיב אם נרשה לחלק את הריבוע באפן אחר?

אם נקפיד שהריבוע יחולק למספר סופי של מצולעים, הרי ברור שנוכל להרכיב מחלקים אלה אך ורק מצולעים. כמו כן ברור שלצורה שנקבל בסוף תהליך הפירוק וההרכבה אותו השטח כמו לריבוע המקורי. האם יש עוד מגבלות?

זה תכנו של המשפט הבא, שהוכח באופן בלתי-תלוי ע"י המתמטיקאי ההונגרי F. Bolyai ב 1832 וע"י המתמטיקאי הגרמני P. Gerwin ב 1833:

<u>משפט:</u> כל מצולע במישור אפשר לחלק למספר סופי של מצולעים חלקיים, ולהרכיב את החלקים מחדש כך שיתקבל ריבוע.

---

* ע"פ הרצאה שניתנה בטקס חלוקת הפרסים לזוכים ב"תחרות הערים" לתלמידי חטיבת הביניים, 21/5/1991.

כדי להקל על הדיון נשתמש במינוח הבא: נאמר ששני מצולעים "שקולים זה לזה ע"י פרוק והרכבה" (או, בקיצור, ששני המצולעים שקולים), אם אפשר לפרק את המצולע האחד למספר סופי של מצולעים חלקיים, ולהרכיב את החלקים מחדש כך שיתקבל המצולע השני.

בעזרת המינוח החדש, ניסוח המשפט יהיה, אם כך, שכל מצולע שקול לריבוע. ברור שניתן להשתמש גם במשפט "בכיוון ההפוך": בהנתן מצולע במישור, אפשר לפרק את הריבוע בעל אותו השטח למספר סופי של מצולעים חלקיים, ולהרכיב מחלקים אלה את המצולע הנתון. יתר על כן, לריבוע אין שום תפקיד מיוחד: בהנתן שני מצולעים שווי שטח כלשהם, אפשר לפרק את האחד ולהרכיב מחלקיו את השני. דרך פשוטה להסיק זאת היא להשתמש במשפט פעמיים: נפרק את המצולע הראשון ונרכיב מחלקיו ריבוע, ואח"כ נפרק את הריבוע ונרכיב מחלקיו את המצולע השני.

ניסוח אחר למשפט יהיה לכן: תנאי הכרחי ומספיק לכך ששני מצולעים יהיו שקולים זה לזה ע"י פרוק והרכבה הוא שיהיה להם אותו שטח.

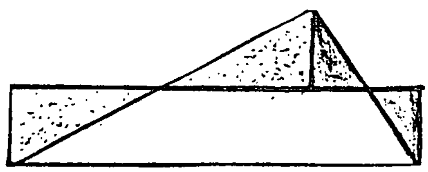
הוכחת המשפט תעשה בכמה שלבים:

א. כל מצולע ניתן לפרוק למספר סופי של משולשים.

למרות שהטענה היא מאד אינטואיטיבית, הרי שהוכחה מדוייקת ומלאה איננה כה קלה. האם תוכלו לתת הוכחה כזו? (שימו לב שהמצולע הנתון איננו צריך להיות קמור!)

ב. כל משולש שקול למלבן.

אם נקח את הצלע הארוכה של המשולש כבסיס, ונבנה על אותו בסיס מלבן שגבהו חצי מגבה המשולש, נוכל לצייר את הפרוק וההרכבה המתאימים:

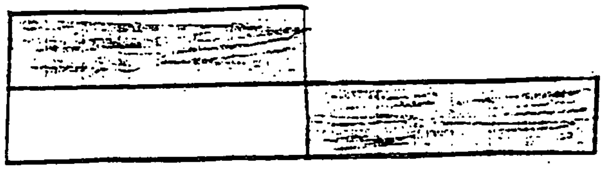


ונשאיר לקוראים את הבדיקה הפשוטה שהחלקים המותאמים אכן חופפים זה לזה.

ג. כל מלבן שקול למלבן שיחס ארכי צלעותיו קטן מ-4:1.

נסמן ב-a את ארך הבסיס של המלבן וב-b את גבהו, ונניח כי $b \le a$.

אם $a \ge 4b$, נפרק את המלבן לשני חצאים, ונרכיב אותם מחדש עפ"י התרשים הבא:



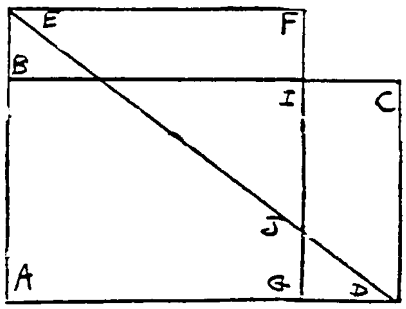
באפן זה נקבל מלבן חדש שבסיסו $a_1 = \frac{a}{2}$ וגבהו $b_1 = 2b$.

היות והנחנו כי $a \ge 4b$ הרי שגם במלבן החדש יתקיים $b_1 \le a_1$, אך יחס ארכי הצלעות בו הוא רבע מהיחס הקודם.

נמשיך ונחזור על פעולה זו מספר פעמים עפ"י הצורך: בכל פעם נקטין את יחס ארכי הצלעות פי ארבעה, עד שנגיע למלבן שבו היחס יהיה קטן מ-4:1.

ד. כל מלבן שקול לריבוע.

ע"ס צעד ג' נוכל להניח שארכו של בסיס המלבן a וגבהו b כאשר $b < a < 4b$, ונתבונן בשרטוט הבא:



המלבן ABCD הוא המלבן הנתון, ונתון כי $|AD| = a$, $|AB| = b$.

AEFG הוא ריבוע שווה-שטח למלבן הנתון, וצלעו היא, לכן $|AE|=|AG|=\sqrt{ab}$.

נחשב את הארך של JG:

עפ"י דמיון משולשים $\frac{|JG|}{|GD|} = \frac{|AE|}{|AD|}$

אך $|AE| = \sqrt{ab}$, $|AD| = a$ ו $|GD| = a - \sqrt{ab}$, לכן:

$$|JG| = \sqrt{ab}(a - \sqrt{ab})/a = \sqrt{ab} - b$$

כמסקנה ראשונה וחשובה מחישוב זה נקבל שהשרטוט אכן "אמיתי", והישר ED עובר מ"תחת" ל-I: עפ"י הנתון $a < 4b$, ולכן

$$|JG| = \sqrt{ab} - b < \sqrt{4b^2} - b = b = |GI|$$

כעת נוכל לראות איך לפרק את המלבן ABCD:

- המחומש ABHJG יהיה החלק הראשון, והוא יישאר במקומו בהרכבת החלקים לריבוע.

- המשולש GJD יהיה החלק השני מהמלבן, והוא יועבר לתפוס את מקומו של המשולש BEH. שני משולשים אלה אכן חופפים כי ברור שהם דומים - ויש להם אותו גבה: $|EB| = |AE|-|AB| = \sqrt{ab} - b$, וזה גם הגבה $|JG|$ במשולש GJD, כפי שחישבנו למעלה.

- החלק השלישי מהמלבן יהיה המשולש HCD שיועבר לתפוס את מקומו של המשולש EFJ. שוב ברור שמשולשים אלה דומים ויש להם אותו גבה:
$$|FJ| = |FG|-|JG| = \sqrt{ab} - (\sqrt{ab} - b) = b = |CD|$$
(נעיר שהחישוב האחרון למעשה מיותר. המשולשים חופפים כי הם דומים ושווי שטח: שטחם הוא השטח המקורי ab, כשמפחיתים את שטחי החלקים שכבר הוכחנו שהם חופפים זה לזה).

ה. כל שני מלבנים שווי שטח שקולים זה לזה.

כי שניהם שקולים לריבוע בעל אותו שטח!

בפרט, נקבל כי כל מלבן שקול למלבן שאורך בסיסו 1, וגבהו כשטח המלבן הנתון.

<u>סיום ההוכחה:</u>

נצא מהמצולע הנתון ונפרקו למשולשים. כל משולש כזה שקול למלבן, וע"ס ההערה בסוף שלב ה' נוכל להניח כי אורך בסיס המלבן הוא 1. כעת נשים את כל המלבנים המתקבלים ב"ערימה", זה מעל זה, ונקבל שהמצולע המקורי שקול למלבן שאורך בסיסו 1. שימוש נוסף בשלב ד' ייתן שהמלבן הזה שקול לריבוע.

מ.ש.ל.

מה קורה בשלושה ממדים? הצורות המרחביות האנלוגיות למצולעים במישור הן "פאונים" (פאון הוא גוף מרחבי המוגבל ע"י מספר סופי של פאות, שכל אחת מהן היא מצולע מישורי המוכל באיזשהו מישור במרחב.)

האם נכון שכל שני פאונים שווי נפח שקולים זה לזה ע"י פרוק והרכבה, כאשר אנחנו מרשים פרוק למספר סופי של פאונים חלקיים?

זו היתה השאלה השלישית בין 23 השאלות ששאל D. Hilbert בהרצאתו המפורסמת בקונגרס המתמטי הבינלאומי בפריס בשנת 1900.

מתברר שהתשובה היא שלילית, ודוגמא נגדית ניתנה ע"י M. Dehn כבר באותה שנה!

מתברר, למשל, כי קוביה וטטראדר משוכלל עם אותו נפח כמו הקוביה אינם שקולים ע"י פירוק והרכבה!

כדי להוכיח שפאונים אלה אינם שקולים, Dehn התאים, בצורה מסויימת, מספר $f(P)$ לכל פאון P. הוא הראה שאם שני פאונים P ו-Q שקולים זה לזה אז, בהכרח, $f(P) = f(Q)$. אח"כ הוא חישב במפורש את f(קוביה) ו- f(טטראדר משוכלל) והראה כי הם שונים זה מזה!

פרטים נוספים על משפט Bolyai-Gerwin, על משפט Dehn, על הרקע ההיסטורי והחשיבות המתמטית שלהם ועל בעיות דומות אפשר לקרוא בספר:

V.G.Boltianskii: Hilbert's Third Problem

זהו ספר מאוד קריא, ומיועד לקהל רחב של חובבי מתמטיקה ולאו דוקא למתמטיקאים מקצועיים.

* * * * * *

משפט בתורת המספרים

מאת גיל אלון, ירושלים

יהי p מספר ראשוני.

<u>למה 1</u>: אם a מספר טבעי, p , q מספרים ראשוניים כך ש- $q \mid a^p-1$, אבל $q \nmid a-1$, אז $q \equiv 1 \pmod p$.

($m \mid n$ הוא סימון ל: m מחלק את n)

הוכחה: $a^p \equiv 1 \pmod q$, אבל $a \not\equiv 1 \pmod q$. היות ו-p ראשוני, נובע ש-p הוא הטבעי הקטן ביותר המקיים $a^p \equiv 1 \pmod q$. לכן לכל t המקיים $a^t \equiv 1 \pmod q$ מתקיים $p \mid t$. אבל לפי המשפט הקטן של Fermat , $a^{q-1} \equiv 1 \pmod q$ ולכן $p \mid q-1$, כנדרש.

(תנאי משפט Fermat מתקיימים כי $q \nmid a$, היות ו- $q \mid a-1$)

למה 2: אם a טבעי כך ש- $p \nmid a-1$, אז המספרים $\frac{a^p-1}{a-1}$ ו $a-1$ זרים.

מסקנה: אם $p \nmid a-1$ יש ל- a^p-1 גורם ראשוני שאינו מחלק את $a-1$.

הוכחת למה 2:

$$\frac{a^p-1}{a-1} = a^{p-1} + \dots + a + 1 \equiv \underbrace{1+ \dots +1}_{\text{פעמים } p} \equiv p \pmod q$$

כלומר, יש k שלם כך ש-

$$\frac{a^p-1}{a-1} - p = k(a-1)$$

לכן, כל מספר טבעי d שמחלק את $a-1$ ואת $\frac{a^p-1}{a-1}$ מחלק בהכרח גם את p , אבל $p \nmid a-1$, ולכן אין מחלק משותף.

משפט: יהא p ראשוני. אזי יש אינסוף מספרים ראשוניים q המקיימים $q \equiv 1 \pmod p$.

הוכחה: נוכיח באינדוקציה. ראשית, אם q מחלק ראשוני של 2^p-1 , אז לפי למה 1, $q \equiv 1 \pmod p$.

כעת נניח ש- $q_1, \dots, q_n$ מספרים ראשוניים שונים כך ש- $q_i \equiv 1 \pmod p$ לכל $1 \le i \le n$. נגדיר $a = q_1 \cdot \ldots \cdot q_n + 1$. $a-1 \equiv 1 \pmod p$, ולכן $p \nmid a-1$, ולפי המסקנה מלמה 2, קיים ל- a^p-1 גורם ראשוני q שלא מחלק את $a-1$.

כעת, ראשית, $q \nmid a-1 = q_1 \cdot \ldots \cdot q_n$ ולכן q מספר ראשוני השונה מ- $q_1, \dots, q_n$. שנית, לפי למה 1, היות ו $q-1$ מחלק של a^p-1 , $q \equiv 1 \pmod p$.

מ.ש.ל.

* * * * * *

המטריצות והמתמטיקה הסינית הקדומה *

מאת אליהו לוי, חיפה

בשם מטריצה קוראים פשוט למספרים רשומים בתבנית מלבנית. למשל: את כל האינפורמציה שבמערכת 2 משוואות ב 2 נעלמים, כגון:

$$\begin{aligned} 2x - y &= 3 \\ x + 3y &= 19 \end{aligned} \qquad (*)$$

אפשר לכתוב בצורת מטריצה של המקדמים:

$$\begin{bmatrix} 2 & -1 & 3 \\ 1 & 3 & 19 \end{bmatrix} \qquad (**)$$

ברור שכל מטריצה מתפרקת ל"שורות" אפקיות, או ל"עמודות" אנכיות, שכל אחת מהן היא סידרת מספרים. למשל במטריצה (**) יש 2 שורות, בכל אחת 3 מספרים, ויש בה 3 עמודות, בכל אחת 2 מספרים. מטריצה כזו נקראת מטריצת 2x3 .

נוכל לפתור את המשוואות (*) ע"י "משחק" במטריצות, שבו מותר לנו לבצע פעולות ממעלה ראשונה בשורות. נסביר זאת: מותר לנו למשל להחליף במטריצה (**) את השורה הראשונה בשורה שבה במקום הראשון (משמאל) יהיה $2 - 1 = 1$, במקום השני $-1 - 3 = -4$ ובמקום השלישי $3 - 19 = -16$. כלומר: בדיוק מה שאנו עושים במקום הראשון (מחליפים את המספר שבמקום הראשון בשורה הראשונה באותו מספר ממנו מחסירים את המספר שבמקום הראשון בשורה השניה) עלינו לעשות גם במקום השני וכן הלאה. למה שעשינו קוראים בקיצור: החלפת השורה הראשונה בשורה הראשונה פחות השניה. בדומה לכך נוכל, למשל, להכפיל את השורה הראשונה ב 2, לחבר לשניה ואת התוצאה לשים במקום השניה. השורה השניה החדשה תהיה אז 5 1 25 , כי $2\cdot3 + 19 = 25$, $2\cdot(-1) + 3 = 1$, $2\cdot2 + 1 = 5$ פעולה מותרת אחרת: להכפיל (או לחלק) שורה מסויימת במספר קבוע שונה מאפס. למשל מותר לנו להחליף את השורה הראשונה בשורה 4 -2 6 (הכפלה ב 2). נדגיש שמותרות רק פעולות "ממעלה ראשונה": אסור, למשל, להעלות את כל אברי שורה בריבוע או להכפיל שתי שורות זו בזו. אחרי שביצענו פעולה אחת בשורות, אנו יכולים לבצע עוד פעולות כאלה, כאוות נפשנו. נקרא למשחק: משחק הפעולות בשורות.

---

* כל מה שייכתב בלשון זכר (כמו: פתור וכדי) - הכוונה גם ללשון נקבה.

לָמה זה טוב ? כי יש לנו שמורות שלא ישתנו ע"י משחק כזה. למשל אם x ו y פותרים את מערכת המשוואות של מטריצה, הם ימשיכו לפתור את מערכת המשוואות של המטריצות החדשות שהתקבלו ממשחק הפעולות בשורות (הוכח זאת לגבי הדוגמאות לפעולות בשורות שניתנו לעיל - כאן חשוב מאוד שלא מרשים פעולות שאינן ממעלה ראשונה). כדי לפתור את המשוואות עלינו רק לשחק במשחק, מתוך מטרה להגיע למטריצה שנותנת משוואות בעלות פתרון מיידי. נדגים זאת לגבי (**) (רשמנו גם את הפעולות שהתבצעו: $ש_1$ מסמן את השורה הראשונה ו $ש_2$ את השניה):

$$\begin{bmatrix} 2 & -1 & 3 \\ 1 & 3 & 19 \end{bmatrix} \xrightarrow[\text{במקום } ש_1]{ש_1 - 2\cdot ש_2} \begin{bmatrix} 0 & -7 & -35 \\ 1 & 3 & 19 \end{bmatrix} \xrightarrow[\text{במקום } ש_1]{(-1/7)\cdot ש_1} \begin{bmatrix} 0 & 1 & 5 \\ 1 & 3 & 19 \end{bmatrix} \xrightarrow[\text{במקום } ש_2]{ש_2 - 3\cdot ש_1} \begin{bmatrix} 0 & 1 & 5 \\ 1 & 0 & 4 \end{bmatrix}$$

המשוואות של המטריצה האחרונה מימין הן $x = 4$, $y = 5$, והפתרון מיידי.

שאלה: האם שיטה זו שונה באמת משיטת החילוץ שנלמדת בבית הספר ?

באותה צורה אפשר לפתור מערכות של מספר כלשהו של משוואות ממעלה ראשונה במספר נעלמים.

וכאן נכנסת לַתמונה המתמטיקה הסינית הקדומה. השימוש במטריצות היה נושא בו הצטיינו הסינים, אולי בהשפעת השימוש שלהם במקלות חישוב (מעין קדַם-חשבוניות). הסינים לא נהגו לבצע חישובים ע"י כתיבה, אלא השתמשו במקלות על לוח. קבוצות של מקלות סימנו את סיפרת היחידות, העשרות, המאות וכו' והחישובים בוצעו ע"י העברת המקלות. כאשר קבוצות המקלות שסימנו מספרים הונחו בסדר מלבני - יש לנו מטריצה, והסינים פתרו בעזרת מטריצות כאלה מערכות משוואות ממעלה ראשונה, בדרך כמו זו שתארנו. דרך זו מתוארת כבר בספר הקלאסי של המתמטיקה הסינית: Jiu-zhang suan-shu (קרא: ג'יו-ג'אנג סואן-שו), שפירושו: "תשעה פרקים על אומנות המתמטיקה" (ראה תמונה בגב החוברת). ספר זה נערך בצורתו הסופית בתקופת שושלת האן, לפני כ-2000 שנה, ומתמטיקאים סיניים מאוחרים יותר כתבו לו פירושים. מעניין שהמונח בו קוראים לַמשוואות בסין, fang cheng, אינו אלא השם המסורתי של שיטת הפתרון ע"י מטריצות, שנקראה: fang-cheng shui שפירושו בערך: "שיטה (אלגוריתם) של חישוב צעד-צעד בנתונים מסודרים על לוח המקלות בצורת ריבוע (או מלבן)".

באירופה הוכנסה המטריצה לראשונה כמושג מתמטי עצמאי באמצע המאה ה 19 ע"י המתמטיקאי הבריטי-יהודי סילבסטר (J. J. Sylvester), שהיה מחשובי מפתחי האלגברה "הגבוהה", אם כי שיטת החילוץ לפתרון מערכת משוואות, וכן מושג הדטרמיננטה (ששייך למעשה לתורת המטריצות ושאולי חלק מהקוראים מכיר אותו),

היו מוכרים לפני כן. עד מהרה פותחה תורה עשירה של המטריצות, כעצמים מתמטיים לכל דבר, וגם כיום עדיין חוקרים אותן וכן משתמשים בהן למטרות מגוונות שחלקן רחוקות מבעיית פתרון מערכת משוואות.

אבל נחזור לפתרון משוואות. באותו רעיון אפשר להשתמש גם עבור משוואות דיופנטיות, כלומר שבהן מחפשים פתרונות שלמים בלבד. כל ההבדל בשיטה הוא שבמשחק מותר רק לחבר או לחסר שורות מוכפלות במספרים שלמים או להכפיל שורה במספר שלם שאינו אפס (לפעולות כאלה נקרא: פעולות שלמות). גם בכך עסקו המתמטיקאים הסיניים, ובעיות מסוג זה ופתרונן בעזרת מטריצות מופיעים בספרו של המתמטיקאי Qin Jiu-shao (קרא: צִ'ין גְ'ייו-שאו) משנת 1247 לספירת הנוצרים, ספר שגם הוא מחולק לתשעה פרקים (לפי צו המסורת ?)

צ'ין מטפל בבעיה שאפשר לנסחה כך (יש להדגיש שהסינים לא הכירו את הסימון האלגברי באותיות, שהוכנס לשימוש רק במאה ה 16 באירופה ע"י המתמטיקאי Vieta. בדומה למה שהיו עושים כל אלה שעסקו במשוואות בעולם עד Vieta, גם הסינים היו מנסחים בעיות מספריות ומראים כיצד לפתור אותן, והיה ברור ללומד ששיטת הפתרון אינה תלויה כלל בבחירת הנתונים):

נתונים מספרים טבעיים m ו a . מצא מספר שלם x כך שיתקיים $ax \equiv 1 \pmod m$ (זה סימון לקונגרואנציה מודולו m, שמשמעותה שההפרש בין שני האגפים מתחלק ב m, או, בלשון אחרת: שניהם נותנים אותה שארית בחלוקה ל m - הוכח שזה באמת אותו דבר!). כאן אם x פתרון יהיה כל מספר קונגרואנטי ל x מודולו m גם הוא פתרון (מדוע ?). משוואה זו היא דוגמא ל"משוואת קונגרואנציה".

שיטת הפתרון, שהיא בעיקרה השיטה המתוארת בספרו של צ'ין (אם כי אולי אינה מנומקת כמו שננמק אותה להלן) תהיה: לרשום את המטריצה $\begin{bmatrix} 1 & a \\ 0 & m \end{bmatrix}$ ולנסות לבצע פעולות שלמות בשורות עד שנקבל מטריצה שתהיה בה שורה מהצורה: 1 b .
(הנחיה כיצד לעשות זאת: בכל שלב בחר פעולה שלמה בשורות כך שאחד המספרים שיהיו בעמודה הימנית יהיה קטן בערכו המוחלט משני המספרים שהיו בה בשלב הקודם - הבהר זאת). אז b יהיה פתרון. הוכחה: אם x פתרון, אזי $1 \equiv ax \pmod m$ וכן $0 \equiv mx \pmod m$ (מדוע ?) ותכונה זו - שהאיבר הראשון בכל שורה קונגרואנטי מודולו m לאיבר השני מוכפל ב x , לא תתקלקל ע"י המשחק שלנו. לכן במטריצה הסופית, בה יש שורה 1 b , יתקיים $b \equiv 1 \cdot x \pmod m$, וכיון ש x פתרון, גם b פתרון (וכן כל מספר קונגרואנטי ל b מודולו m).

נביא דוגמא פשוטה מספרו של צ'ין, שבלשוננו תיכתב כ $14 \cdot x \equiv 1 \pmod{19}$. דרך הפתרון תהיה (אצל צ'ין כתובה דרך הפתרון בצורה קצת שונה, בגלל שאין הוא משתמש בה במספרים שליליים) - אילו פעולות (שלמות) בשורות בוצעו כאן ?

$$\begin{bmatrix} 1 & 14 \\ 0 & 19 \end{bmatrix} \dashrightarrow \begin{bmatrix} 1 & 14 \\ -1 & 5 \end{bmatrix} \dashrightarrow \begin{bmatrix} 3 & 4 \\ -1 & 5 \end{bmatrix} \dashrightarrow \begin{bmatrix} 3 & 4 \\ -4 & 1 \end{bmatrix} \dashrightarrow \begin{bmatrix} 15 & 1 \\ -4 & 1 \end{bmatrix}$$

והפתרון הוא $x = 15$ (אין צורך בצעד האחרון: $x = -4$ הוא פתרון).

שאלות:

1. פתור בשיטה זו: א) $8x \equiv 1 \pmod{13}$ ב) $9x \equiv 1 \pmod{11}$ ג) $256x \equiv 1 \pmod{337}$. (כדאי לבדוק את הפתרונות)

2. נניח שמצאת פתרון x למשוואה $ax \equiv 1 \pmod{m}$. נסה לפתור בעזרתו משוואה כללית יותר: $ay \equiv b \pmod{m}$.

3. האם לכל משוואה $ax \equiv 1 \pmod{m}$ יש פתרון ? נסה למצא דוגמא בה אין פתרון. מה תוכל להגיד, אם מצאת פתרון x, על הצורה הכללית של כל הפתרונות ?

4. האם אתה רואה קשר בין השיטה שלעיל לבין האלגוריתם הידוע (של אוקלידס) למציאת המחלק המשותף הגדול ביותר של שני מספרים ? נסה להיעזר בכך כדי למצוא תנאי שצריכים לקיים m ו a שיהיה הכרחי ומספיק לכך שיש פתרון למשוואה $ax \equiv 1 \pmod{m}$.

5. צ'ין עוסק בבעיה אחרת, שבלשוננו תנוסח כך: יש למצוא y שלם שיקיים את מערכת משוואות הקונגרואנציה הבאות (כל המקדמים שלמים):

$$(***) \quad y \equiv b_1 \pmod{m_1}, \quad y \equiv b_2 \pmod{m_2}, \quad \ldots \quad y \equiv b_n \pmod{m_n}$$

אשר את השיטה הבאה למצוא פתרון (שהיא השיטה שבספרו של צ'ין): תהי m המכפלה $m_1 m_2 \ldots m_n$, ויהיו $a_1 = m/m_1,\ a_2 = m/m_2, \ldots,\ a_n = m/m_n$ (ה a ים שלמים!). נניח שמצאנו פתרונות $x_1, x_2, \ldots x_n$ למשוואות:

$$a_1 x_1 \equiv 1 \pmod{m_1}, \quad a_2 x_2 \equiv 1 \pmod{m_2}, \quad \ldots \quad a_n x_n \equiv 1 \pmod{m_n}$$

אז המספר y הבא ייתן פתרון למערכת (***):

$$y = b_1 a_1 x_1 + b_2 a_2 x_2 + \ldots + b_n a_n x_n$$

(שים לב שהצלחת השיטה תלויה באפשרות לפתור את המשוואות עבור ה x ים !)

6. בהשפעת עיסוקם של הסינים בבעייה שבשאלה 5, נקרא כיום בספרות המתמטית בשם "משפט השאריות הסיני" המשפט הבא: אם $m_1\ m_2\ \ldots\ m_n$ מספרים טבעיים זרים כלומר לכל שניים מהם אין מחלק משותף גדול מ 1 , אזי עבור המשוואות (***) יתקיים: א) יש תמיד פתרון, ו ב) פתרון זה יחיד עד כדי קונגרואנציה מודולו המכפלה m , כלומר: אם y פתרון כלשהו, אזי כל מספר קונגרואנטי ל y זה מודולו m הוא פתרון (זה קל) וגם ההפך: כל פתרון אחר הוא קונגרואנטי ל y זה מודולו m . האם תוכל להוכיח משפט זה ?

פרטים על הישגי הסינים הקדמונים במתמטיקה אפשר למצוא בספר:

Li Yan: Chinese Mathematics, Oxford University Press, 1987

* * * * * *

תחרות הבעיות

את הפתרונות יש לשלוח למערכת עד 30.4.92

1. א) כיצד תבנה מ-6 גפרורים 4 משולשים שווי צלעות באותו גודל בלי לקפל, לשבור ולהצליב את הגפרורים?

   ב) כיצד תבנה מ-6 גפרורים 8 משולשים שווי צלעות בלי לפגוע בגפרורים?

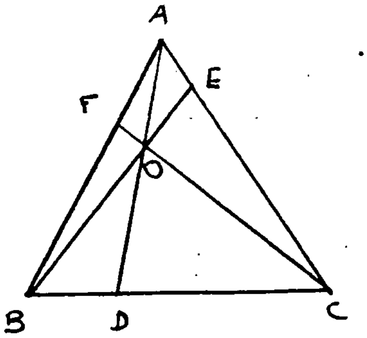
2. נתונה סידרה של n^2+1 מספרים שונים. הוכח: אפשר לבחור מהם $n+1$ מספרים (לאו דוקא עוקבים) שיהוו תת-סידרה מונוטונית עולה או יורדת.

3. נתונה קבוצה סופית של n נקודות במישור, לא כולן על ישר אחד. הוכח כי יש ישר העובר בדיוק דרך שתיים מהן.

4. "שלשה פיתגוראית" הם שלושה מספרים שלמים a, b, c המקיימים $a^2 + b^2 = c^2$, כמו למשל 3, 4, 5 או 6, 8, 10 .

   שלשות פיגוראיות ייחשבו לשונות אם הן אינן כפולות של אותה שלשה. למשל 12, 16, 20 ו 9, 12, 15 אינן שונות כי שתיהן כפולה של 3, 4, 5 , אך 5, 12, 13 שונה מהן.

   הוכח כי יש אינסוף שלשות פיתגוראיות שונות.

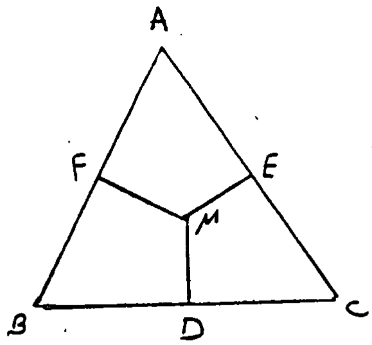


5. (הצעה ע"י אבי ב. סיגלר, נהריה): במשולש ABC, הישרים AD, BE, CF נפגשים בנקודה O.

הוכח: הקטעים $\frac{AO \cdot OD}{AD}$, $\frac{BO \cdot OE}{BE}$, $\frac{CO \cdot OF}{CF}$

מקיימים את אי-שוויון המשולש.

(כלומר הממוצעים ההרמוניים של [AO,OD], [BO,OE], [CO,OF] מקיימים את אי-שוויון המשולש).



6. (הוצעה ע"י אבי ב. סיגלר, נהריה):
יהי ABC משולש. נתבונן בשלושת מעגלי אפולוניוס, שהם המקומות הגאומטריים של הנקודות שמרחקיהן משני קדקדים של המשולש נמצאים ביחס קבוע, השווה ליחס של מרחקי שני הקדקדים מהקדקד השלישי.

א) הוכח ששלושת המעגלים נפגשים בנקודה אחת M.

ב) יהיו D,E,F הטלי M על BC, AC, AB בהתאמה. הוכח: המשולש DEF שווה צלעות.

פתיחת פרק 1 של "תשעה פרקים על אומנות המתמטיקה"

九章筭經卷第一

魏劉徽注

唐朝議大夫行太史令上輕車都尉臣李淳風等奉勑注釋

方田 以御田疇界域

今有田廣十五步從十六步問爲田幾何

荅曰一畝

又有田廣十二步從十四步問爲田幾何

百六十八步 圖從十四廣十二