רבעון למתמטיקה

ללמוד ולמחקר

בעריכת דב ירדן

כרך 4 | ירושלים, חשון תשי"א, אוקטובר 1950 | חוברת 3–4

תכן

עמוד

כתבת המערכת: דב ירדן, כנסת החדשה, ירושלים

המחיר 500 פרוטה

לבעית טארי-אסקוט המינימלית

ע"י ז'בוטינסקי

בעית טארי-אסקוט המינימלית היא למצוא, בשביל M נתון, שתי סדרות מספרים, A_m ו-B_m $(m=1,2,\dots,M)$, של M מספרים שלמים כל אחת, באופן שיהיה קיים:

$$\sum_{m=1}^{M}(A_m)^k = \sum_{m=1}^{M}(B_m)^k \qquad (A)$$

בשביל $k=0,1,\dots,(M-1)$. (אגב, במשואה (A) עלול להופיע 0^0. אנו נתנה לכתוב תמיד $0^0=1$. תנאי זה דרוש כדי שנוכל להשתמש במשפט-הבינום $(a+t)^k=\sum_{i=0}^{k}\binom{k}{i}a^{k-i}t^i$ גם במקרה ש: $k=t=0$).

בעיה זו נחקרה באופן מקיף בחמשים השנים האחרונות. בשנת 1944 הופיעה המהדורה השניה מספרו של אלברט גלודן[1], המוקדש כולו לבעיה זו ולבעיות הנובעות ממנה. בספר זה נתנים פתרונות של הבעיה בשביל $M\leqslant 10$ $(k\leqslant 9)$. אנו נותנים בחמשה המשפטים הראשונים את רב התכונות המשותפות לבעיותינו בשביל כל M. המשפטים 1 ו-2 ידועים היטב. המשפטים 3 ו-4, הנותנים נסוח מולטיפליקטיבי של הבעיה, הנם פחות ידועים, אבל אין בהם מן החדוש. משפט 5, המטפל בפתרונות פרמטריים (זאת אומרת בפתרונות בהם ה-A_m וה-B_m הם פונקציות של פרמטרים שרירותיים), הוא, כנראה, חדש. משפט זה מהוה את המכשיר העקרי למציאת פתרונות פרמטריים.

מכאן ואילך אנו מטפלים בפתרונות פרמטריים לינאריים. משפט 6 נותן אפשרות של נורמליזציה ידועה של הפתרונות הללו. הדוגמאות הידועות של פתרונות כאלה (הנתונות בעמודים 43-44, מיד אחרי משפט 2) נותנות יסוד להשערה שכל הפתרונות הפרמטריים הלינאריים יש להם עוד תכונה נוספת שנוסחה בהשערה 1. במקרה שהשערה זו איננה נכונה, יצא שדיונינו מצטמצמים לפתרונות המספקים את ההנחה שבהשערה 1 בלבד. פתרונות אלה נתנים לנורמליזציה נוספת (תוצאה 1).

משפט 7 קובע תנאי מספיק לצורות הפרמטריות הלינאריות $A_m(x,y)$ ו-$B_m(x,y)$ אחר הובאו לצורה נורמלית לפי תוצאה 1 בשביל שהן תהוינה פתרון של בעיתנו. במקרה שנכונה השערה 1, התנאי של משפט 7 הוא גם הכרחי. משפט 8 הוא משפט עזר על סדרת נסיגה מסוימת מסדר 4, שבעזרתה אנו מוצאים את כל הצורות הלינאריות המספקות את תנאי משפט 7. משפט 9 מסכם את כל הדיונים ונותן פתרון אקספליציטי לבעית מציאת פתרונות פרמטריים לינאריים בשביל כל M. אם נכונה השערה 1, ממצה משפט זה את כל הפתרונות הפרמטריים הלינאריים. בשביל $M=12$ נתנת דוגמה של פתרון מספרי בשדה $a+b\sqrt{3}$. בסוף נתנת השערה על הדרגה המינימלית של הפתרון הפרמטרי בשביל כל M.

---

[1] Albert Gloden, Mehrgradige Gleichungen, Groningen, 1944, pp. 104.

בספרו מסתמש גלודן בכתיב מקוצר ומבטא את המשואה (A) בצורה המקוצרת הבאה:

$$A_1,A_2,\dots,A_M \stackrel{M-1}{=} B_1,B_2,\dots,B_M$$

בעמוד 56 הוא נותן גם פתרונות של הבעיה בשביל המקרים $M-1=1,\dots,9$. אלה הם הפתרונות במספרים הקטנים ביותר הידועים עד הנה:

$$1,3 \stackrel{1}{=} 2,2$$

$$1,4,4 \stackrel{2}{=} 2,2,5$$

$$1,5,8,12 \stackrel{3}{=} 2,3,10,11$$

$$1,5,9,17,18 \stackrel{4}{=} 2,3,11,15,19$$

$$1,4,6,12,14,17 \stackrel{5}{=} 2,2,9,9,16,16$$

$$1,19,28,59,65,90,102 \stackrel{6}{=} 2,14,39,45,76,85,103$$

$$1,5,10,24,28,42,47,51 \stackrel{7}{=} 2,3,12,21,31,40,49,50$$

$$1,25,31,84,87,134,158,182,198 \stackrel{8}{=} 2,18,42,66,113,116,169,175,199$$

$$1,3084,3302,11894,23315,24187,35608,44200,44418,47501 \stackrel{9}{=} 13,2866,3520,11870,23739,23763,35632,43982,44636,47489$$

הערה. הקורא ישים לב שגלודן מציין בכתיב שלו לא את מספר האיברים M מכל צד המשואה, אלא את החזקה הגבוהה ביותר, שהיא $(M-1)$, שעבורה קיימת המשואה. אנו נקרא ל $(M-1)$ ח ז ק ת המשואה או הבעיה ול-M נקרא ד ר ג ת המשואה או הבעיה. להלן נראה שנוח הוא למיין את בעיות טארי-אסקוט לפי דרגת המשואות ולא לפי חזקתן. אנו נראה, למשל, שבעיות שדרגותיהן הן כפולות של אותו מספר, יש ביניהן מן הקרבה. (גלודן לא היה יכול להשתמש בדרגת המשואות, הואיל והוא מטפל גם בבעיה יותר רחבה: למצוא פתרונות לבעיה מחזקה $(M-1)$ על-ידי פתרונות בעלי M איברים ל פ ח ו ת, בה בשעה שאנו מצמצמים את עצמנו לחפוש הפתרונות בעלי M איברים ב ד י ו ק).

שני משפטים יסודיים. נוכיח כעת שני משפטים המהוים יסוד לכל המחקר (המשפטים הללו ידועים היטב):

משפט 1. אם קיים $\sum_{m=1}^{M}(A_m)^k=\sum_{m=1}^{M}(B_m)^k$ בשביל $k=0,1,\dots,(M-1)$, אזי קיים גם $\sum_{m=1}^{M}(A_m+t)^k=\sum_{m=1}^{M}(B_m+t)^k$ בשביל $k=0,1,\dots,(M-1)$ ובשביל כל t.

הוכחה. נפתח את $(A_m+t)^k$ ואת $(B_m+t)^k$ בעזרת משפט הבינום לפי החזקות של t ונוכח שהמקדמים של החזקות השוות של t שוים הם משני צדי המשואה.

משפט זה מאפשר, למשל, לבחור t כך שכל האיברים יהיו חיוביים, או כך ש $\sum_{m=1}^{m=M}(A_m+t)=\sum_{m=1}^{m=M}(B_m+t)=0$.

משפט 2. אם קיים (א) $\sum_{m=1}^{m=M'}(A_m)^k=\sum_{m=1}^{m=M'}(B_m)^k$ בשביל $k=0,1,\dots,(M-1)$ ואם (ב) $M'<M$ אזי כל ה A_m שוים ל-B_m בסדר מתאים.

הוכחה. אם קיים (א), אז כל הפונקציות הסמטריות של ה-A_m שוות הן לאותן הפונקציות של ה-B_m עד לפונקציות הסמטריות מהמעלה $(M-1)$. אולם הפונקציות הסמטריות מהמעלה M יכולות להיות שונות. עתה נתבונן במכפלות $F(z)=\prod_{m=1}^{m=M'}(z-A_m)$ ו-$G(z)=\prod_{m=1}^{m=M'}(z-B_m)$. אם $M'<M$ אזי המקדמים של החזקות השונות של z שוים הם ב-$F(z)$ וב-$G(z)$, ולכן קיים $F(z)=G(z)$. אבל לכל אחת המשואות $F(z)=0$ ו-$G(z)=0$ יש M' שרשים, ולכן ה-A_m שוים ל-B_m.

הגדרה. פתרון שבו כל האיברים מהצד האחד שוים לאיברים מהצד השני בסדר מתאים נקרא פ ת ר ו ן ט ר י ו י א ל י .

פתרונות פרמטריים. באופן מיוחד נתענין כאן בפתרונות פרמטריים של הבעיה. ליתר דיוק, נסתכל בפתרונות שעבורם $A_m=A_m(x,y)$ ו-$B_m=B_m(x,y)$, באשר x ו-y הם שני מספרים שלמים כל שהם.

בשביל השמוש להלן נתן כאן דוגמאות של פתרונות פרמטריים.

דוגמאות של פתרונות פרמטריים (בחלק מהדוגמאות הבאות מופיעים שני פרמטרים נוספים a ו-b).

א.

$M=3$	$M-1=2$	$A_1=$	$0.x+$	$0.y$	$B_1=$	$0.x+$	$(a+b).y$
		$A_2=$	$(-b).x+$	$(a).y$	$B_2=$	$(-b).x+$	$0.y$
		$A_3=$	$(a).x+$	$(a+b).y$	$B_3=$	$(a).x+$	$(a).y$
$M=4$	$M-1=3$	$A_1=$	$0.x+$	$0.y$	$B_1=$	$0.x+$	$(b).y$
		$A_2=$	$(a-b).x+$	$(a).y$	$B_2=$	$(a-b).x+$	$0.y$
		$A_3=$	$(2a).x+$	$(a+b).y$	$B_3=$	$(2a).x+$	$(a).y$
		$A_4=$	$(a+b).x+$	$(b).y$	$B_4=$	$(a+b).x+$	$(a+b).y$
$M=6$	$M-1=5$	$A_1=$	$0.x+$	$0.y$	$B_1=$	$0.x+$	$(-a+b).y$
		$A_2=$	$(2a-b).x+$	$(a).y$	$B_2=$	$(2a-b).x+$	$0.y$
		$A_3=$	$(3a).x+$	$(a+b).y$	$B_3=$	$(3a).x+$	$(a).y$
		$A_4=$	$(2a+2b).x+$	$(2b).y$	$B_4=$	$(2a+2b).x+$	$(a+b).y$
		$A_5=$	$(3b).x+$	$(-a+2b).y$	$B_5=$	$(3b).x+$	$(2b).y$
		$A_6=$	$(-a+2b).x+$	$(-a+b).y$	$B_6=$	$(-a+2b).x+$	$(-a+2b).y$

ב.

$M=5 \quad M-1=4$

$A_1 = 0x^2 + (a^2-b^2)xy + (a^2)y^2 \qquad B_1 = 0x^2 + (-a^2+b^2)xy + (-a^2)y^2$

$A_2 = a(a-b)x^2 + (a^2)xy + (ab)y^2 \qquad B_2 = a(a-b)x^2 + (a^2-b^2)xy + 0y^2$

$A_3 = b(a-b)x^2 + 0xy + (-ab)y^2 \qquad B_3 = b(a-b)x^2 + (a^2)xy + (a^2)y^2$

$A_4 = -b(a-b)x^2 + (-a^2)xy + (-a^2)y^2 \qquad B_4 = -b(a-b)x^2 + 0xy + (ab)y^2$

$A_5 = -a(a-b)x^2 + (-a^2+b^2)xy + 0y^2 \qquad B_5 = -a(a-b)x^2 + (-a^2)xy + (-ab)y^2$

$M=8 \quad M-1=7$

$A_1 = 1x^2 - 23xy + 84y^2 \qquad B_1 = 1x^2 + 5xy - 56y^2$

$A_2 = 3x^2 - 35xy + 112y^2 \qquad B_2 = 3x^2 - 23xy + 28y^2$

$A_3 = 4x^2 - 33xy + 56y^2 \qquad B_3 = 4x^2 - 35xy + 84y^2$

$A_4 = 2x^2 - 5xy - 28y^2 \qquad B_4 = 2x^2 - 33xy + 112y^2$

$A_5 = -1x^2 + 23xy - 84y^2 \qquad B_5 = -1x^2 - 5xy + 56y^2$

$A_6 = -3x^2 + 35xy - 112y^2 \qquad B_6 = -3x^2 + 23xy - 28y^2$

$A_7 = -4x^2 + 33xy - 56y^2 \qquad B_7 = -4x^2 + 35xy - 84y^2$

$A_8 = -2x^2 + 5xy + 28y^2 \qquad B_8 = -2x^2 + 33xy - 112y^2$

ג.

$M=7 \quad M-1=6$

$A_1 = 1x^5 - 1x^4y - 2x^3y^2 + 4x^2y^3 - 4xy^4 + 1y^5 \qquad B_1 = -1x^5 + 1x^4y + 2x^3y^2 - 4x^2y^3 + 4xy^4 - 1y^5$

$A_2 = 0x^5 + 1x^4y - 3x^3y^2 + 0x^2y^3 + 3xy^4 - 1y^5 \qquad B_2 = 0x^5 - 1x^4y + 3x^3y^2 + 0x^2y^3 - 3xy^4 + 1y^5$

$A_3 = 0x^5 - 2x^4y + 3x^3y^2 + 1x^2y^3 - 1xy^4 + 0y^5 \qquad B_3 = 0x^5 + 2x^4y - 3x^3y^2 - 1x^2y^3 + 1xy^4 + 0y^5$

$A_4 = -1x^5 + 2x^4y + 2x^3y^2 - 5x^2y^3 + 2xy^4 + 0y^5 \qquad B_4 = 1x^5 - 2x^4y - 2x^3y^2 + 5x^2y^3 - 2xy^4 + 0y^5$

$A_5 = -1x^5 + 1x^4y + 1x^3y^2 + 1x^2y^3 - 3xy^4 + 1y^5 \qquad B_5 = 1x^5 - 1x^4y - 1x^3y^2 - 1x^2y^3 + 3xy^4 - 1y^5$

$A_6 = 1x^5 - 2x^4y - 1x^3y^2 + 4x^2y^3 - 1xy^4 + 0y^5 \qquad B_6 = -1x^5 + 2x^4y + 1x^3y^2 - 4x^2y^3 + 1xy^4 + 0y^5$

$A_7 = 0x^5 + 1x^4y + 0x^3y^2 - 5x^2y^3 + 4xy^4 - 1y^5 \qquad B_7 = 0x^5 - 1x^4y + 0x^3y^2 + 5x^2y^3 - 4xy^4 + 1y^5$

הערה. נתנו את הדוגמאות בסדר זה, מכיון שבפתרונות המקרים M=3,4,6 הפרמטרים x ו-y מופיעים בצורה לינארית, בשני המקרים M=5,8 הפרמטרים מופיעים בצורה רבועית ובמקרה M=7 בצורה ממעלה חמישית. כפי שיתברר להלן (ראה את הסעיף האחרון במאמר זה) יש לצפות למצוא בשביל המקרה M=7 בטוי ממעלה שלישית בלבד. כמו כן יש לצפות למצוא בטויים ממעלה שניה למקרים M=10,12 (במקרה M=10 ידועים אין-סוף פתרונות, אך אין עדיין בטוי פרמטרי אלגברי; במקרה M=12 אין ידוע שום פתרון). במקרה M=9 נראה שיש לצפות לבטוי פרמטרי שגם הוא ממעלה שלישית (במקרה זה ידועים רק שני פתרונות בודדים). במקרה M=11, שבו אין ידוע שום פתרון, נראה שיש לצפות למצוא פתרונות ממעלה חמישית. בארבע הדוגמאות הראשונות נתונים הפתרונות למעשה על-ידי 4 פרמטרים, הואיל ושם מופיעים לשני הפרמטרים נוספים a ו-b. במקרה M=8 יש לנו פתרון שנדמה כי הוא נובע מפתרון יותר כללי על-ידי קביעת שני הפרמטרים a ו-b.

הדוגמאות למקרים M=3,4,6 חושבו על ידי לפי שיטה שנלמד אותה להלן. הדוגמה למקרה M=5 חושבה על ידי מתוך מקרה מיוחד הנתן על-ידי גלודן (עמוד 42). המקרה של גלודן מתקבל, אם נשים a=1, b=2. הדוגמה למקרה M=8

אקויולנטית לדוגמאות שנתנו על-ידי גלודן (עמוד 54). הדוגמה למקרה $M=7$ מחושבת לפי שיטה שנתנה על-ידי גלודן (עמודים 42-44). שם אמנם מתקבל פתרון פרמטרי מהמעלה התשיעית, אבל לכל המספרים A_m ו-B_m יש גורם משותף ממעלה רביעית, לכן אפשר לחלק את כולם בגורם זה.

צורה מולטיפליקטיבית של הבעיה. בשביל חפוש פתרונות פרמטריים יהיה לנו נוח לנסח את בעית טארי-אסקוט בצורה מולטיפליקטיבית. לשם כך נחזור לפולינומים $F(z)=\prod_{m=1}^{M}(z-A_m)$ ו-$G(z)=\prod_{m=1}^{M}(z-B_m)$ אשר שפלנו בהם בהוכחה למשפט 2 ונוכיח את שני המשפטים הבאים, הנכונים גם עבור פתרונות פרמטריים.

משפט 3. יהי M נתון. אם המספרים A_m ו-B_m $(m=1,2,\dots,M)$ מהוים פתרון מספרי של בעית טארי-אסקוט, זאת-אומרת אם קיים

$$\sum_{m=1}^{M}(A_m)^k=\sum_{m=1}^{M}(B_m)^k \qquad (k=0,1,\dots,(M-1)\ \text{בשביל})$$

אזי קיים גם:

$$\prod_{m=1}^{M}(B_n-A_m)=C \qquad (n=1,2,\dots,M\ \text{בשביל})$$

באשר C איננו תלוי ב-n. הערך של C נתן על-ידי:

$$(-1)^M C=\prod_{m=1}^{M}A_m-\prod_{m=1}^{M}B_m$$

הוכחה. המקדמים של מעלות שוות של z ב-$F(z)$ וב-$G(z)$ שוים פרט לאיבר החפשי, הואיל והפונקציות הסמטריות של ה-A_m שוות לאותן הפונקציות הסמטריות של ה B_m עד לפונקציות ממעלה $(M-1)$ ועד בכלל. לכן קיים $F(z)-G(z)=(-1)^M\left(\prod_{m=1}^{M}A_m-\prod_{m=1}^{M}B_m\right)$. לכן

$$\prod_{m=1}^{M}(B_n-A_m)=F(B_n)=G(B_n)+(-1)^M\left(\prod_{m=1}^{M}A_m-\prod_{m=1}^{M}B_m\right)$$

אבל ברור ש- $G(B_n)=0$.

הערה. ממשפט זה נובע שאם נסדר את ה A_m ואת ה B_m בשורה אחת לפי סדר גדלם, יצא שבין כל שני A_m יש מספר זוגי $(0,2,4\dots)$ B_m ולהפך, בין כל שני B_m יש מספר זוגי של A_m. בעובדה זו לא נשתמש להלן.

משפט 4. יהי M נתון. אם המספרים A_m ו-B_m $(m=1,2,\dots,M)$ ממלאים את

$$\prod_{m=1}^{M}(B_n-A_m)=C$$

בשביל $n=1,2,\dots,M$, באשר C אינו תלוי ב-n, אזי המספרים A_m ו-B_m מהוים פתרון של בעית טארי-אסקוט וקיים:

$$\sum_{m=1}^{M}(A_m)^k=\sum_{m=1}^{M}(B_m)^k \qquad (k=0,1,\dots,M-1)$$

$$(-1)^M C=\prod_{m=1}^{M}A_m-\prod_{m=1}^{M}B_m$$

הוכחה. M המספרים B_n הם השרשים של המשואה $\prod_{m=1}^{M}(x-A_m)=C$. הפונקציות הסמטריות של השרשים הללו מהמעלות $k=0,1,2,\dots,(M-1)$ שוות לאותן הפונקציות הסמטריות של A_n. לכן קיים

$$\sum_{m=1}^{M}(B_n)^k=\sum_{m=1}^{M}(A_m)^k \qquad (\text{בשביל } k=0,1,2,\dots,(M-1))$$

ובאשר לפונקציות הסמטריות ממעלה M, קיים:

$$(-1)^M\prod_{n=1}^{M}B_n=-C+(-1)^M\prod_{m=1}^{M}A_m$$

המשפטים 3 ו 4 היו בודאי ידועים באפן עקרוני לגלודן.

משפט 4 נותן נסוח מולטיפליקטיבי של בעית טארי-אסקוט שהוא זהה עם הנסוח האדיטיבי הרגיל. הנוחיות של נסוח זה לחדוש פתרונות פרמטריים נובעת מכך שאם ה-A_m וה-B_m הם פולינומים באיזה פרמטרים שהם, הרי כן הוא גם C ולכן הגדלים B_n-A_m, שגם הם פולינומים (יש M^2 גדלים כאלה), הם כולם גורמים של הפולינום האחד C. ננסח כעת ביתר דיוק את הבעיה הפרמטרית.

נסוח הבעיה הפרמטרית. בטפולנו להלן נקפיא את כל הפרמטרים פרט ל-x ול-y. לפנינו עומדת אפוא הבעיה:

למצוא M צורות אלגבריות $A_m(x,y)$ ו-M צורות אלגבריות $B_m(x,y)$ באפן שיהיה קיים:

$$\sum_{m=1}^{M} A_m(x,y)^k=\sum_{m=1}^{M} B_m(x,y)^k \qquad (B)$$

בשביל $k=1,2,\dots,(M-1)$

משפחת הצורות האלגבריות $A_m(x,y)$ ו-$B_m(x,y)$ המספקת את (B) תקרא פ ת ר ו ן פ ר מ ט ר י של בעיתנו. הערכים שמקבלות הצורות הללו בשביל ערכים נתונים של x ו-y מהוים אז פ ת ר ו ן מ ס פ ר י של הבעיה. להלן נבדיל תמיד בין פתרון פרמטרי לפתרון מספרי.

פתרונות טריויאליים. אם נתונים ה-$A_m(x,y)$ אפשר לבחור בתור ה-$B_m(x,y)$ את ה-$A_m(x,y)$ באיזה סדר שהוא. ברור שהואיל ומשני צדי שויון (B) נמצאים אותם הבטויים, יהיה השויון נכון באפן זהותי בשביל כל k, אפילו בשביל $k>(M-1)$.

הערה. אנו נראה שאם קיים פתרון פרמטרי בלתי טריויאלי, אפשר לבחור את הערכים של x ו-y כך שהפתרון המספרי בשביל הערכים הללו יהיה טריויאלי.

פתרונות פרמטריים אקויולנטיים. נניח שלפנינו פתרון פרמטרי של המשואה (B). אזי:

א) אפשר לשנות את סדר ה-A_m וה-B_m באפן שרירותי.

ב) אפשר להכפיל את ה-A_m ואת ה-B_m במקדם משותף s.

ג) אפשר לחבר ל-$A_m(x,y)$ ול-$B_m(x,y)$ את אותה הצורה האלגברית $T(x,y)$. (זה נובע ממשפט 1).

ד) במקום x ו-y אפשר לבחור כפרמטרים u ו-v הקשורים ב-x וב-y על-ידי שתי המשואות $x=au+bv$, $y=cu+dv$ בתנאי שהן בלתי תלויות.

שני פתרונות פרמטריים שאפשר לעבור מן האחד לשני בכמה פעולות מהמינים א' עד ד' בזו אחר זו יקראו פתרונות פרמטריים אקויולנטיים. כך, לדוגמה, שני הפתרונות הפרמטריים למקרה $M=8$, הנתנים על-ידי גלודן בעמוד 54 הם, למעשה, אקויולנטיים במובן ההגדרה שלמעלה.

התכונה היסודית של הפתרונות הפרמטריים. נבחר במשואה (B) את x ו-y כך שיהיה קיים $A_i(x,y)=B_j(x,y)$. אזי אפשר למחוק את A_i משמאל ואת B_j מימין ותשארנה משואות עם $(M-1)$ איברים בלבד (במקום M איברים) הנכונות בשביל $k=1,2,\ldots,(M-1)$. משפט 2 אומר שבתנאים אלה כל ה-A_m הנותרים שוים ל-B_m הנותרים בסדר מתאים. בשביל שהדבר יהיה ברור, נתבונן בדוגמה מיוחדת במקרה $M=6$. קיים:

$$\begin{aligned}&(x+y)^k+(2x+3y)^k+(7x+6y)^k+(11x+7y)^k+(10x+5y)^k+(5x+2y)^k=\\&=(x+2y)^k+(2x+y)^k+(7x+3y)^k+(11x+6y)^k+(10x+7y)^k+(5x+5y)^k\end{aligned}\qquad (C)$$

בשביל $k=0,1,2,3,4,5$.

נבחר את x ו-y כך למשל שהאיבר השני משמאל יהיה שוה לאיבר הרביעי מימין. זאת אומרת כך ש: $5x+2y=11x+6y$ או $6x+4y=0$. בשביל כך מספיק לקחת $x=-2$, $y=3$. המשואה הנזכרת הופכת בשביל ערכים אלה של x ו-y ל:

$$1^k+5^k+4^k+(-1)^k+(-5)^k+\cancel{(-4)}^k=4^k+(-1)^k+(-5)^k+\cancel{(-4)}^k+1^k+5^k$$

מחקנו את האיבר השני משמאל ואת האיבר הרביעי מימין, אולם נמצא (כפי שצפינו) כי גם האיברים הנותרים שוים הם משני הצדדים של המשואה. מכאן:

משפט 5. אם במשואה (B) נבחר את x ו-y כך ש: $A_i(x,y)=B_j(x,y)$, אזי גם שאר האיברים מצד שמאל יהיו שוים לשאר האיברים מצד ימין בסדר מתאים.

זוהי התכונה היסודית של הפתרונות הפרמטריים. אנו ננסה להשתמש בה בשביל לחקור את התכונות של הפתרון הכללי של בעיתנו.

אולם נתחיל מהמקרה הפשוט ביותר, כשקיים פתרון פרמטרי ליניארי והומוגני, זאת-אומרת, נחפש בשביל M נתון פתרונות מהצורה:

$$A_m(x,y)=p_mx+q_my;\quad B_m(x,y)=r_mx+s_my\quad (m=1,2,\ldots,M)$$

באשר קיימים m ו-n כאלה ש $\begin{vmatrix}p_m & q_m\\ r_n & s_n\end{vmatrix}\neq 0$ (אחרת יהיה הפתרון הפרמטרי תלוי למעשה רק בפרמטר אחד ויקרא פתרון פרמטרי ד ג נ ר ט י ב י).

פתרונות פרמטריים ליניאריים והומוגניים. בכל הדוגמאות של פתרונות ליניאריים והומוגניים שנתנו (בעמודים 43-44) אנו יכולים לבדוק את העובדה הבאה: המקדמים של x ושל y ב-$A_m(x,y)$ הם שוים למקדמים של x ו-y ב-$B_m(x,y)$, אם כי בסדר אחר. למשל, במשואה (C) המקדמים של ה-y-ים מצד שמאל הם 1,3,6,7,5,2 ומצד ימין 2,1,3,6,7,5 וכיוצא בו בשביל מקדמי ה-x-ים. זוהי תכונה כללית. ביתר דיוק קיים המשפט:

משפט 6. אם קיים פתרון פרמטרי בלתי דגנרטיבי ליניארי והומוגני של שני פרמטרים, אזי אפשר תמיד לבנות פתרון פרמטרי אקויולנטי אשר בו המקדמים של x ושל y ב-$A_m(x,y)$ יהיו שוים למקדמים של x ו-y ב-$B_m(x,y)$ בסדר מתאים.

הוכחה. יהי $A_m(u,v)\overset{M-1}{=}B_m(u,v)$ הפתרון הפרמטרי, באשר ה-$A_m(u,v)$ וה-$B_m(u,v)$ הן צורות ליניאריות הומוגניות ב-u ו-v. נכתוב:

$$x=A_1(u,v)-B_1(u,v) \qquad y=A_1(u,v)-B_2(u,v)$$

ונבטא את u ו-v כפונקציות ליניאריות של x ו-y. זה אפשרי, הואיל וכשהפתרון הפרמטרי הנתון איננו טריויאלי או דגנרטיבי אזי המשואות הליניאריות הנותנות את x ו-y הן בלתי תלויות. נקבל $A_m(u,v)=A'_m(x,y)$ ו- $B_m(u,v)=B'_m(x,y)$. ברור ש-$A'_m(x,y)$ ו-$B'_m(x,y)$ מהוים פתרון פרמטרי ליניארי חדש (אם המקדמים אינם שלמים אפשר להכפיל את ה-A'_m וה-B'_m במקדם משותף מתאים), האקויולנטי לראשון. נניח עתה ש- x=0. אזי $A'_1=B'_1$, כי כך בחרנו את x. לכן, לפי משפט 5, גם שאר האיברים מצד שמאל שוים לשאר האיברים מצד ימין בסדר מתאים. אם עתה נבחר y=1, האיברים משני הצדדים יהיו דוקא המקדמים של y ב-$A'_m(x,y)$ וב-$B'_m(x,y)$. לכן המקדמים של y מצד שמאל שוים בסדר ידוע למקדמים של y מצד ימין. באותו אפן, אם נכתוב y=0 ו- x=1, נראה כי גם המקדמים של x שוים הם משני צדי המשואה.

התרכבות פרמטריים ליניאריים וחבורות. נחזור למשואה (C) ונחפש להשוות כל איבר משמאל לכל איבר מימין. נתחיל מזה שנבחר את האיבר הראשון משמאל, (x+y), ונשוה אותו בזה אחר זה לכל אחד מששת האיברים מימין, נקבל שש משואות:

$$x+y=x+2y,\quad x+y=2x+y,\quad x+y=7x+3y,\quad x+y=11x+6y,\quad x+y=10x+7y,\quad x+y=5x+5y$$

או:

$$y=0,\quad x=0,\quad 2(3x+y)=0,\quad 5(2x+y)=0,\quad 3(3x+2y)=0,\quad 4(x+y)=0$$

את המקדמים שמחוץ לסוגרות אפשר למחוק ולבסוף מקבלים אנו את שש המשואות:

$$y=0,\quad x=0,\quad 3x+y=0,\quad 2x+y=0,\quad 3x+2y=0,\quad x+y=0$$

אם נרצה להשוות עתה כל שני איברים אחרים, מן ההכרח הוא שנקבל שוב את אחת משש המשואות הנזכרות לעיל. בלוח הבא סכמנו את התוצאות. כל שורה מיצגת איבר מצד שמאל וכל עמודה איבר מצד ימין. בהצטלבות השורה והעמודה רשמנו כל פעם את הבטוי ב-x ו-y שעליו להתאפס בשביל ששני האיברים הללו יהיו שוים. נמצא:

לוח I:

	1	2	3	4	5	6
1	y	x	3x+y	2x+y	3x+2y	x+y
2	x+y	y	x	3x+y	2x+y	3x+2y
3	3x+2y	x+y	y	x	3x+y	2x+y
4	2x+y	3x+2y	x+y	y	x	3x+y
5	3x+y	2x+y	3x+2y	x+y	y	x
6	x	3x+y	2x+y	3x+2y	x+y	y

אותה התופעה אפשר להציג על-ידי לוח ממין אחר: נקדיש כל שורה לאחד מששת הבטויים ב-x ו-y שעליהם להתאפס ובגוף הלוח נרשום את המספר הסדורי של האיבר מצד שמאל שעליו להיות שוה לאיבר שמצד ימין שלו מוקדשת העמודה. נקבל:

לוח II.

	1	2	3	4	5	6
y	1	2	3	4	5	6
x+y	2	3	4	5	6	1
3x+2y	3	4	5	6	1	2
2x+y	4	5	6	1	2	3
3x+y	5	6	1	2	3	4
x	6	1	2	3	4	5

זהו לוח שהנו זהה עם לוח הכפל של חבורה ציקלית ממעלה ששית. להלן נצמצם בפתרונות פרמטריים המביאים ללוח II מטפוס לוח-הכפל של חבורה ציקלית.

השערה. נעלה כעת השערה המבוססת על הדוגמה שנותחה בסעיף הקודם. ההשערה היא שאם, בשביל M איזה שהוא, קיים פתרון פרמטרי לינארי הומוגני בלתי דגנרטיבי ובלתי טריויאלי, אזי אפשר לבחור את סדר האיברים משני הצדדים באפן שאם נבנה לוח מטפוס לוח II, יהיה זה לוח מכפלה של חבורה ציקלית.

זאת אומרת, אנו מניחים כי קיימת:

השערה 1. יהי M נתון. אם קיים פתרון פרמטרי לינארי הומוגני בלתי דגנרטיבי, אזי אפשר לסדר את האיברים בסדר כזה שאם בוחרים את x ו-y כך ש

$$A_i(x,y)=B_j(x,y)$$

אזי קיים:

$$A_{i+h}(x,y)=B_{j+h}(x,y)$$

בשביל כל h, באשר אנו קובעים כי $A_{m+M}(x,y)=A_m(x,y)$ ו-$B_{m+M}(x,y)=B_m(x,y)$.

השערה 1 קובעת ש כ ל פתרון לינארי מביא ללוח II מטפוס לוח הכפל של חבורה ציקלית. אם יתברר שההשערה איננה צודקת ושקיימים פתרונות לינאריים הומוגניים אשר לוח II שלהם איננו מהטפוס הזה, הרי על-ידי הנחת השערה 1 והשמוש בה פירוש צמצמנו את משפחת הפתרונות הפרמטריים שאנו מסתכלים בהם. במקום השערה 1 היינו יכולים לאמור, כמו שעשינו למעלה, שאנו מסתכלים אך ורק בפתרונות הפרמטריים הלינאריים שכלפיהם נכונה השערה 1 (הדוגמאות שנתנו בעמוד 43 מוכיחות שהמשפחה זו איננה ריקה).

אולם סבור אני שאת השערה 1 אפשר להוכיח. נסתכל איך בנוי לוח II. לפי משפט 5, כל מספר צריך להופיע בלוח זה פעם אחת בכל שורה ופעם אחת בכל עמודה. הלוח הוא אפוא "רבוע לטיני". בשביל להוכיח שזה גם לוח כפל של חבורה צריך להוכיח שהוא מקיים את חוק האסוציאטיביות: $a(bc)=(ab)c$. בדרך נסיונית ראיתי שרבועים לטיניים (אלה שנסיתי אותם) אינם נובעים מפתרונות פרמטריים של בעיתנו. נסיתי גם לוחות כפל של חבורות לא ציקליות וראיתי שלוחות אלו נובעים אמנם מפתרונות פרמטריים של בעיתנו, אולם מפתרונות טריויאליים (ה-$A_m(x,y)$ זהים ל-$B_m(x,y)$ בסדר ידוע).

משפט 6 לאור השערה 1. ממשפט 6 נובע שאם יש פתרון פרמטרי, לינארי, הומוגני ובלתי דגנרטיבי, אזי קיים גם פתרון פרמטרי אקוילנטי שאיבריו מסודרים באפן ש:

$$A_m(x,y)=p_mx+q_my; \qquad B_m(x,y)=p_mx+q_{f(m)}y$$

כאשר $f(m)$ היא פונקציה של m המעתיקה את הסדרה $m=1,2,\dots,M$ על עצמה בסדר מתאים.

הערה 1 אומרת בין היתר שאפשר תמיד לסדר את האיברים כך שיהיה $f(m)=m-1$. זאת אומרת שמתקבלת:

תוצאה 1. אם קיים פתרון פרמטרי, ליניארי והומוגני, בלתי דגנרטיבי, אזי אפשר תמיד לבנות פתרון פרמטרי אקויולנטי מהצורה:

$$A_m(x,y)=p_mx+q_my; \qquad B_m(x,y)=p_mx+q_{m-1}y$$

(אנו מגדירים $p_{m+M}=p_m$ ו- $q_{m+M}=q_m$).

הערה. תוצאה 1 נותנת אפשרות של נורמליזציה ידועה של פתרונות פרמטריים ליניאריים אקויולנטיים. נדמה לי שקיימת אותה האפשרות של נורמליזציה של פתרונות פרמטריים ממעלות יותר גבוהות. כך למשל, הדוגמאות שנתנו בעמוד 44 עבור $M=5$ ו- $M=8$ הנן בנויות בצורה הבאה:

$$A_m(x,y)=p_mx^2+q_mxy+r_my^2; \quad B_m(x,y)=p_mx^2+q_{m-1}xy+r_{m-2}y^2$$

אולם טרם הצלחתי לברר אם התכונה הזאת כללית היא לכל הפתרונות הפרמטריים ממעלה הגבוהה מהראשונה.

משפט יסודי לפתרונות הפרמטריים הליניאריים. להלן נניח תמיד $A_{m+M}=A_m$, $B_{m+M}=B_m$, $p_{m+M}=p_M$ ו- $q_{m+M}=q_m$. קיים המשפט:

משפט 7. יהי M נתון. נניח שקיים:

א': $A_m(x,y)=p_mx+q_my;\ B_m(x,y)=p_mx+q_{m-1}y$ (בשביל $m=1,2,\dots,M$).

ב': ה-p_m וה-q_m הם כאלה שאם בוחרים x ו-y כך ש:

$$A_m(x,y)=B_n(x,y)$$

אזי קיים בשביל כל h:

$$A_{m+h}(x,y)=B_{n+h}(x,y)$$

אז ה-$A_m(x,y)$ וה-$B_m(x,y)$ מהוים פתרון פרמטרי של בעית טארי–אסקוט.

הוכחה. לשם הוכחת משפט 7 נשתמש במשפט 4. נסתכל במכפלה:

$$\prod_{m=1}^{M}[B_n(x,y)-A_m(x,y)]=C_n(x,y)$$

עלינו להוכיח שהפולינום $C_n(x,y)$, שהוא מכפלה של M גורמים ליניאריים, אינו תלוי ב-n. אם נחליף את n ב-$(n+h)$ נוכל לכתוב:

$$C_{n+h}(x,y)=\prod_{m=1}^{M}[B_{n+h}(x,y)-A_m(x,y)]=\prod_{m=1}^{M}[B_{n+h}(x,y)-A_{m+h}(x,y)]$$

מפני שעלינו לעבור באפן ציקלי על כל ה-A_m. אבל לאור ההנחה ב' שבמשפט 7 נראה שקיים:

$$B_{n+h}(x,y)-A_{m+h}(x,y)=l\,[B_n(x,y)-A_m(x,y)]$$

כאשר l הוא גורם מספרי בלתי תלוי ב-x ו-y. לכן קיים:

$$C_{n+h}(x,y)=L\cdot C_n(x,y)$$

כאשר גם L הוא גורם מספרי בלתי תלוי ב-x ו-y. עלינו עתה להוכיח ש- $L=1$

בשביל כל h. זה ינבע מהקשר המיוחד הקיים בין מקדמי ה-x וה-y ב-A_m וב-B_m. נחשב את האיברים בעלי המעלה הכי גבוהה ב-x ב-$C_n(x,y)$ וב-$C_{n+h}(x,y)$ ונראה שהם שוים. די יהיה להראות זאת במקרה $h=1$. המקרה הכללי ינבע מכאן על-ידי אינדוקציה לפי h.

לאור הנחה א' של משפט 7 קיים:

$$B_n(x,y)-A_m(x,y)=(p_n-p_m)x+(q_{n-1}-q_m)y$$

לכן, לאור הנחה ב' של אותו משפט:

$$1[(p_n-p_m)x+(q_{n-1}-q_m)y]=(p_{n+h}-p_{m+h})x+(q_{n+h-1}-q_{m+h})y$$

באשר 1 הוא גורם מספרי בלתי תלוי ב-x ו-y. ומכאן:

$$\frac{p_{n+h}-p_{m+h}}{q_{n+h-1}-q_{m+h}}=\frac{p_n-p_m}{q_{n-1}-q_m} \qquad (ג')$$

לכל m,n ו-h. (ג') אקויולנטית להנחות א' ו-ב'.

את (ג') יכולים אנו לכתוב:

$$\frac{p_n-p_m}{q_{n-1}-q_m}=f_{n-m}$$

באשר f_{n-m} הוא מספר אשר איננו תלוי אלא בהפרש n-m. מכאן:

$$p_{n+1}-p_m=f_{n+1-m}(q_n-q_m)$$

$$p_{m+1}-p_n=f_{m+1-n}(q_m-q_n)$$

או:

$$\frac{p_{n+1}-p_m}{p_n-p_{m+1}}=\frac{f_{n+1-m}}{f_{m+1-n}} \qquad (ד')$$

מכאן:

$$\prod_{\substack{m=1\\ m\neq n+1,n,n-1}}^{M}\frac{p_{n+1}-p_m}{p_n-p_{m+1}}=\prod_{\substack{m=1\\ m\neq n+1,n,n-1}}^{M}\frac{f_{n+1-m}}{f_{m+1-n}}$$

אבל כש-m עובר על הערכים מ-1 עד M, פרט לערכים n-1,n,n+1, הגדלים n+1-m ו- m+1-n עוברים שניהם על כל המספרים מודולו M, פרט למספרים 0,1 ו-2. לכן המכפלה הנזכרת לעיל שוה ל-1. מכאן:

$$\prod_{\substack{m=1\\ m\neq n+1,n-1}}^{M}\frac{p_{n+1}-p_m}{p_n-p_{m+1}}=\frac{p_{n+1}-p_n}{p_n-p_{n+1}}=-1$$

ועתה יכולים אנו לסיים את ההוכחה. קיים:

$$C_n(x,y)=\prod_{m=1}^{M}[(p_n-p_m)x+(q_{n-1}-q_m)y]$$

הגורם של $C_n(x,y)$ עבור m=n איננו מכיל את x ולכן האיבר בעל המעלה הגבוהה ביותר ב-x הוא $x^{M-1}y$. המקדם של איבר זה הוא

$$(q_{n-1}-q_n)\prod_{\substack{m=1\\ m\neq n}}^{M}(p_n-p_m)$$

ועלינו להוכיח שקיים:

$$(q_{n-1}-q_n)\prod_{\substack{m=1\\m\neq n}}^{M}(p_n-p_m)=(q_n-q_{n+1})\prod_{\substack{m=1\\m\neq n+1}}^{M}(p_{n+1}-p_n)$$

אבל:

$$\frac{\prod\limits_{\substack{m=1\\m\neq n}}^{M}(p_n-p_m)}{\prod\limits_{\substack{m=1\\m\neq n+1}}^{M}(p_{n+1}-p_m)}=\frac{\prod\limits_{\substack{m=1\\m\neq n-1}}^{M}(p_n-p_{m+1})}{\prod\limits_{\substack{m=1\\m\neq n+1}}^{M}(p_{n+1}-p_m)}=\frac{(p_n-p_{n+2})}{(p_{n+1}-p_{n-1})}\prod_{\substack{m=1\\m\neq n\pm1}}^{M}\frac{p_n-p_{m+1}}{p_{n+1}-p_m}=\frac{p_n-p_{n+2}}{p_{n+1}-p_{n-1}}$$

לכן, בסופו של דבר, עלינו להוכיח שקיים:

$$(q_{n-1}-q_n)(p_n-p_{n+2})=-(q_n-q_n-q_{n+1})(p_{n+1}-p_{n-1})$$

אבל, לפי (ג'), קיים:

$$f_2=\frac{p_{n+2}-p_n}{q_{n+1}-q_n}=\frac{p_{n+1}-p_{n-1}}{q_n-q_{n-1}}$$

ועל-ידי כך מסתיימת ההוכחה של משפט 7.

חישוב פתרונות פרמטריים ליניאריים. ממשפט 7 נובע כי בשביל למצוא פתרון פרמטרי ליניארי הומוגני בשביל M נתון, עלינו למצוא M מספרים p_m ו-M מספרים q_m $(m=1,2,\dots,M)$ באופן ש:

$$A_m(x,y)=p_mx+q_my;\qquad B_m(x,y)=p_mx+q_{m-1}y \tag{D}$$

(אנו מגדירים $p_{m+M}=p_m$ ו- $q_{m+M}=q_m$) ובאופן שאם x ו-y מספקים את המשואה $p_ix+q_iy=p_jx+q_{j-1}y$, אז אותם הערכים של x ו-y מספקים גם את המשואה: $p_{i+h}x+q_{i+h}y=p_{j+h}x+q_{j+h-1}y$, בשביל כל h. זאת אומרת שבשביל כל h קיים שוויון:

$$\frac{p_i-p_j}{q_i-q_{j-1}}=\frac{p_{i+h}-p_{j+h}}{q_{i+h}-q_{j+h-1}}\quad\left(=-\frac{y}{x}\right) \tag{E}$$

או:

$$(p_i-p_j)/(q_i-q_{j-1})=f_{(i-j)}$$

באשר $f_{(i-j)}$ הוא מספר התלוי רק בהפרש $(i-j)$. (קיים כמובן $f_{(m+M)}=f_m$). במשואה האחרונה נחליף את i ב-j ואת j ב-i ונקבל:

$$(p_j-p_i)/(q_j-q_{i-1})=f_{(j-i)}$$

אם נחלק זו בזו את שתי המשואות נמצא: $(q_i-q_{j-1})/(q_{i-1}-q_j)=g_{(i-j)}$, באשר $g_{(i-j)}=f_{(j-i)}/f_{(i-j)}$. נכתוב עתה:

$$q_2-q_1=D_1;\ q_3-q_2=D_2;\ \dots;\ q_{m+1}-q_m=D_m;\ \dots;\ q_1-q_M=D_M.$$

ברור שקיים

$$\sum_{m=1}^{m=M}D_m=0$$

נבחר עכשו את i ו-j כך ש: $i-j=2$. אזי קיים:

$$\frac{q_{j+2}-q_{j-1}}{q_{j+1}-q_j} = \frac{D_{j+1}+D_j+D_{j-1}}{D_j} = g_2$$

באשר g_2 אינו תלוי ב-j. קיים: $D_{j+1}=(g_2-1)D_j-D_{j-1}$. אם ידוע g_2, זו היא משואה המגדירה את ה-D_j כסדרת-נסיגה מסדר 2. אם נקבע באפן שרירותי את D_1 ואת D_2 נוכל לחשב את כל ה-D_j. לשם צמצום הכתיבה נכתוב $z=g_2-1$. נוסחת הנסיגה נכתבת:

$$D_{j+1}=zD_j-D_{j-1} \qquad (F)$$

יהיו a ו-b שני מספרים כל שהם. נכתוב: $D_1=a$ ו- $D_2=b$. נוסחת הנסיגה נותנת לנו בזה אחר זה: $D_3=-a+zb$, $D_4=-za+(z^2-1)b$, $D_5=-(z^2-1)a+(z^3-2z)b$ וכו'. אולם עלינו לבחור את z, את a ואת b באפן שיהיה $\sum_{m=1}^{m=M} D_m=0$. לשם כך נחשב את המספרים $E_m=\sum_{j=1}^{j=m} D_j$. נקבל בזה אחר זה:

$E_0=0$ $E_1=a$ $E_2=a-b$ $E_3=(z-1)b$ $E_4=-za-(z^2-z)b$ $E_5=(z^2-z-1)a-(z^3-z^2-z)b$

אנו רואים שקיים $E_m=R_m(z)a+S_m(z)b$ באשר $R_m(z)$ ו-$S_m(z)$ הם פולינומים ב-z. אם נבחר $q_1=0$ אזי $q_m=E_{m-1}$ וקיים:

$$q_m=R_{m-1}(z)a+S_{m-1}(z)b \qquad (G)$$

בעיתנו היא לבחור את z, a ו-b באפן ש $E_M=0$. יש שתי אפשרויות:

(א) אנו בוחרים את z כך שיהיה בבת אחת

$$R_M(z)=0, \quad S_M(z)=0 \qquad (H)$$

(ב) אם לא, אזי נבחר z איזה שהוא ונניח

$$a=1S_M(z); \quad b=-1R_M(z)$$

אפשר להראות שאפשרות (ב) מביאה רק לפתרונות טריויאליים. באשר לאפשרות (א) הרי נראה שתמיד יש ערכים של z המאפסים את שתי המשואות (H) בבת אחת. מבין הערכים הללו של z, נלמד לברור ערכים המביאים לפתרונות לא טריויאליים. אולם יתברר שערכים אלה של z הם לרב בלתי רציונליים.

לכן נניח לעת עתה שהצלחנו לבחור a, b ו-z כאלה שקיים $E_M=0$ ונחפש לחשב את ה-p_m וה-q_m מבלי לדאוג לשאלת שלמות המספרים הללו אלא אך ורק לכך שהצורות הלינאריות (D) תספקנה את המשואה (E).

הואיל ו-z, a ו-b ידועים, נוכל לחשב את ה-D_j בזה אחר זה. נעשה עתה את ההנחות הנוספות הבאות: $q_1=0$, $p_1=0$ ו- $f_1=1$. הנחות אלו, כמוהן כבחירה באחד מבין פתרונות אקויולנטיים.

מההנחה $q_1=0$ נקבל, הודות לידיעת ה-D_j את כל ה-q_m, הואיל ואז:

$$q_m=\sum_{j=1}^{j=m-1} D_j=E_{m-1}$$

מההנחה $f_1=1$ אנו מקבלים $(p_{j+1}-p_j)/(q_{j+1}-q_{j-1})=1$ או: $p_{j+1}-p_j=q_{j+1}-q_{j-1}$. ההנחה $p_1=0$ מאפשרת עתה לחשב גם את כל ה-p_m.

הערה. מפני הסמטריות המיוחדת של הצורות הלינאריות (D), אפשר היה להתחיל מחישוב ה-p_m. בדרך כלל יש לצפות למצוא בטויים דומים עבור ה-p_m וה-q_m.

לאחר שידועים ה-p_m וה-q_m, נותנות הנוסחאות (D) את ה-$A_m(x,y)$ וה-$B_m(x,y)$.

בשביל להוכיח שהצורות הליניאריות $A_m(x,y)$ ו-$B_m(x,y)$ הללו מספקות את ההנחות של משפט 7, עלינו עוד להוכיח שה-p_m וה-q_m מספקים את המשואה (E) בשביל כל $(i-j)$. זאת אומרת, עלינו להוכיח שאם $(p_{j+1}-p_j)/(q_{j+1}-q_{j-1})=1$ ו- $(q_{j+2}-q_{j-1})/(q_{j+1}-q_j)=z+1$, באשר z הוא מספר קבוע (אלה היו ההנחות מהן יצאנו לחישוב ה-q_m וה-p_m), אזי גם נכון (E) באפן כללי. הדבר נכון ואני משאיר את ההוכחה לקורא.

מתוך כך עלינו עתה לחקור את הפולינומים $R_m(z)$ ו-$S_m(z)$.

קיים:

$$D_{m+1}=[R_{m+1}(z)-R_m(z)]a+[S_{m+1}(z)-S_m(z)]b$$

מהמשואה (F) יוצא (לשם קצור נותר על כתיבת הארגומנט z):

$$(R_{m+1}-zR_m+zR_{m-1}-R_{m-2})a+(S_{m+1}-zS_m+zS_{m-1}-S_{m-2})b=0$$

דבר זה צריך להיות קיים עבור כל a ו-b ולכן צריך להיות באפן זהותי:

$$R_{m+1}-zR_m+zR_{m-1}-R_{m-2}=0$$

$$S_{m+1}-zS_m+zS_{m-1}-S_{m-2}=0$$

עם התנאים הראשוניים:

$$R_0=0,\quad R_1=1,\quad R_2=1$$

$$S_0=0,\quad S_1=0,\quad S_2=1$$

$S_m(z),R_m(z)$ הם איברים של סדרת נסיגה מסדר 3. בקשר לפולינומים $R_m(z)$ ו-$S_m(z)$ יש לנו המשפט הבא:

משפט 8. יהי $T_m(z)$ מוגדר על-ידי משואת נסיגה מסדר 2:

$$T_{m+1}(z)=zT_m(z)-T_{m-1}(z)$$

עם תנאי המוצא:

$$T_0(z)=0,\quad T_1(z)=1$$

נגדיר את $P_m(z)$ על-ידי המשואות

$$P_{2m}(z)=T_m(z);\quad P_{2m+1}(z)=T_m(z)+T_{m+1}(z)$$

ה-$P_n(z)$ מספקים את משואת הנסיגה מסדר 4:

$$P_{m+2}(z)=zP_m(z)-P_{m-2}(z)$$

עם תנאי המוצא:

$$P_0(z)=0,\quad P_1(z)=1,\quad P_2(z)=1,\quad P_3(z)=z+1$$

אזי קיים:

(א) $R_m(z)=-P_m(z)P_{m-3}(z);\qquad S_m(z)=P_m(z)P_{m-1}(z)$

(ב) ל-$P_{m-3}(z)$ ול-$P_{m-1}(z)$ אין שרשים משותפים והשרשים המשותפים ל-$R_m(z)$ ול-$S_m(z)$ הם השרשים של $P_m(z)$.

(ג) אם n מחלק את m אז הפולינום $P_n(z)$ מחלק את הפולינום $P_m(z)$. לכן לפולינום $P_m(z)$ יש גורמים אשר הופיעו כבר בפולינומים $P_n(z)$ אשר עבורם $n|m$ וגם גורם חדש, הנקרא הגורם הפרימיטיבי של $P_m(z)$. הגורם הפרימיטיבי של $P_M(z)$ הוא הפולינום $Q_M(z)$ המאפין את בעית טארי–אסקוט מסדר M.

ההוכחה של משפט 8 היא טפוסית לטפול בסדרות נסיגה והנני משאיר גם אותה לקורא. בסוף המאמר אני נותן לוח של הפולינומים $P_n(z)$ הראשונים ומציין על-ידי הדגשה את הגורמים הפרימיטיביים.

הערה. המספרים $P_n(z)$ נותנים, בשביל $z=-3$, את מספרי סדרת פ י ב ו נ צ ' י U_n, בסימן מסוים (U מוגדר על-ידי משואת הנסיגה $U_{n+1}=U_n+U_{n-1}$ ו: $U_1=1$,$U_0=0$). באפן מדויק יותר קיים:

$$P_n(-3)=(-1)^{(n-1)/2}\,U_n$$

אולם לא נשתמש בעובדה זאת להלן.

בטוי אקספליציטי של המתרגנת הפרמטריים הלינאריים. מהמשואה (G) ומסעיף (א) של משפט 8 נובע שקיים:

$$q_m=P_{m-1}(z)\left[-P_{m-4}(z)a+P_{m-2}(z)b\right]$$

מטעמי סמטריות רואים שקיים גם

$$p_m=P_{m-1}(z)\left[-P_{m-4}(z)a'+P_{m-2}(z)b'\right]$$

באשר a' ו-b' הם שני פרמטרים הקשורים ב-a ו-b. בשביל למצוא את a' ו-b' נכתוב, כפי שעשינו זאת לעיל, שבמשואה (E) קיים $f_1=1$, זאת אומרת שקיים:

$$p_{i+1}-p_i=q_{i+1}-q_{i-1}$$

אם במשואה זו נכתוב $i=2$ ואחר כך $i=3$ ונציג בתוכה את p_m ו-q_m על-ידי הבטויים דלעיל, נמצא שתי משואות לינאריות ב-a' ו-b' שמהן נקבל:

$$a'=(z+1)a-b;\quad b'=a+b$$

אפשר בקלות להוכח שבשביל ערכים אלה של a' ו-b', נכונה המשואה $p_{i+1}-p_i=q_{i+1}-q_i$ בשביל כל ערך של i. זו היא תוצאה של תכונות הפולינומים $P_n(z)$.

עתה יכולים אנו לסכם את כל הנזכר לעיל על-ידי המשפט הבא, המכיל את כל התוצאות שהוכחנו עד הנה:

משפט 9. יהי M נתון. יהיו x, y, a ו-b פרמטרים ו-z משתנה. יהיו $P_n(z)$ פולינומים המוגדרים על-ידי משואת הנסיגה:

$$P_{2n+2}(z)=zP_{2n}(z)-P_{2n-2}(z)$$

עם התנאים הראשוניים:

$$P_0(z)=0,\ P_1(z)=1,\ P_2(z)=1,\ P_3(z)=z+1$$

יהיו a' ו-b' מוגדרים על-ידי המשואות:

$$a'=(z+1)a-b,\quad b'=a+b$$

ויהיו p_m ו-q_m מוגדרים על-ידי המשואות:

$$p_m=P_{m-1}(z)\left[-P_{m-4}(z)a'+P_{m-2}(z)b'\right]$$

$$q_m=P_{m-1}(z)\left[-P_{m-4}(z)a+P_{m-2}(z)b\right]$$

תהיינה $A_m(x,y)$ ו-$B_m(x,y)$ שתי צורות לינאריות המוגדרות על-ידי המשואות:

$$A_m(x,y)=p_mx+q_my;\quad B_m(x,y)=p_mx+q_{m-1}y$$

אזי קיים:

$$\sum_{m=1}^{m=M}[A_m(x,y)]^k=\sum_{m=1}^{m=M}[B_m(x,y)]^k \pmod{P_M(z)[-P_{M-3}(z)a+P_{M-1}(z)b]}$$

בשביל $k=0,1,\dots,(M-1)$.

אם z הוא שורש של המשואה

$$P_M(z)[-P_{M-3}(z)a+P_{M-1}(z)b]=0$$

אז ה-$A_m(x,y)$ וה-$B_m(x,y)$ מהוים פתרון פרמטרי של הבעיה. אם z הוא שורש של הגורם הפרימיטיבי של $P_M(z)$ אזי הפתרון הפרמטרי הוא לא טריויאלי. בכל מקרה אחר הפתרון הפרמטרי הוא טריויאלי.

אם לגורם הפרימיטיבי של $P_M(z)$ יש שורש רציונלי אזי הפתרון הפרמטרי הנזכר לעיל נותן פתרונות מספריים במספרים שלמים. זה קורה בשביל $M=3,4,6$.

אם נכונה השערה 1 אז אין לבעית טארי-אסקוט פתרונות פרמטריים לינאריים מלבד אלה הנתונים על ידי משפט זה.

דוגמה למקרה $M=12$, $M-1=11$. הגורם הפרימיטיבי של $P_{12}(z)$ הוא (z^2-3). לכן נבחר $z=\sqrt{3}$. נכתוב: $P_m(\sqrt{3})=P_m$. קיים:

$P_{-2}=-1,\ P_{-1}=-1,\ P_0=0,\ P_1=1,\ P_2=1,\ P_3=1+\sqrt{3},\ P_4=\sqrt{3},\ P_5=2+\sqrt{3},\ P_6=2,$

$P_7=2+\sqrt{3},\ P_9=1+\sqrt{3},\ P_{10}=1,\ P_{11}=1,\ P_{12}=0,\dots$

נבחר $a=1,b=2$ ואף $x=y=1$. נקבל: $a'=\sqrt{3}-1,b'=3$. ומכאן הפתרון המספרי:

$A_1=0$	$A_7=14+8\sqrt{3}$	$B_1=2-\sqrt{3}$	$B_7=12+9\sqrt{3}$
$A_2=\sqrt{3}$	$A_8=14+7\sqrt{3}$	$B_2=-1+\sqrt{3}$	$B_8=15+7\sqrt{3}$
$A_3=5+\sqrt{3}$	$A_9=9+7\sqrt{3}$	$B_3=3+\sqrt{3}$	$B_9=11+7\sqrt{3}$
$A_4=5+5\sqrt{3}$	$A_{10}=9+3\sqrt{3}$	$B_4=6+3\sqrt{3}$	$B_{10}=8+5\sqrt{3}$
$A_5=12+5\sqrt{3}$	$A_{11}=2+3\sqrt{3}$	$B_5=3+6\sqrt{3}$	$B_{11}=6+2\sqrt{3}$
$A_6=12+8\sqrt{3}$	$A_{12}=2$	$B_6=14+6\sqrt{3}$	$B_{12}=2\sqrt{3}$

סכום. הצלחנו למצוא את כל הפתרונות הפרמטריים הלינאריים, אולם ראינו שלא תמיד המקדמים הם רציונליים. כנראה של-$P_M(z)$ יש גורמים פרימיטיביים לינאריים רק בשביל $M=3,4,6$. אני משער שבכל מקרה יש לבעיה פתרון פרמטרי על-ידי צורות אלגבריות הומוגניות עם מקדמים רציונליים ממעלה שוה לזו של הגורם הפרימיטיבי של $P_M(z)$, זאת אומרת של הפולינום המאפין $Q_M(z)$. העובדות הידועות אינן סותרות את ההשערה הזאת. מענין היה לערוך תיאוריה של פתרונות פרמטריים ממעלות 2, 3 וכולי, דוגמת התיאוריה הנתנת כאן. יתכן כי הדבר ידרוש טפול ברב-חבורות (מולטי-גרופס, בלעז). ברצוני לנסח את ההשערה הזאת באפן פורמלי:

השערה 2. לבעית טארי-אסקוט מסדר M יש פתרון פרמטרי בצורת פולינומים הומוגניים בשני פרמטרים עם מקדמים רציונליים, ממעלה השוה למעלת הגורם הפרימיטיבי של $P_M(z)$.

לוח ה- $P_n(z)$ בשביל $-3\leq n\leq 20$

הגורמים הפרימיטיביים מודגשים. (הגורם הפרימיטיבי של $P_M(z)$ הוא הפולינום המאפין $(Q_M(z)$.

$$P_n(z)=z\cdot P_{n-2}(z)-P_{n-4}(z)$$

n	
-3	$-z-1$
-2	-1
-1	-1
0	0
1	$\underline{1}$
2	$\underline{1}$
3	$\underline{z+1}$
4	$\underline{z}$
5	$\underline{z^2+z-1}$
6	$z^2-1=(\underline{z-1})(z+1)$
7	$\underline{z^3+z^2-2z-1}$
8	$z^3-2z=z(\underline{z^2-2})$
9	$z^4+z^3-3z^2-2z+1=(z+1)(\underline{z^3-3z+1})$
10	$z^4-3z^2+1=(\underline{z^2-z-1})(z^2+z-1)$
11	$\underline{z^5+z^4-4z^3-3z^2+3z+1}$
12	$z^5-4z^3+3z=z(z-1)(z+1)(\underline{z^2-3})$
13	$\underline{z^6+z^5-5z^4-4z^3+6z^2+3z-1}$
14	$z^6-5z^4+6z^2-1=(\underline{z^3-z^2-2z+1})(z^3+z^2-2z-1)$
15	$z^7+z^6-6z^5-5z^4+10z^3+6z^2-4z-1=(z+1)(z^2+z-1)(\underline{z^4-z^3-4z^2+4z+1})$
16	$z^7-6z^5+10z^3-4z=z(z^2-2)(\underline{z^4-4z^2+2})$
17	$\underline{z^8+z^7-7z^6-6z^5+15z^4+10z^3-10z^2-4z+1}$
18	$z^8-7z^6+15z^4-10z^2+1=(z-1)(z+1)(\underline{z^3-3z-1})(z^3-3z+1)$
19	$\underline{z^9+z^8-8z^7-7z^6+21z^5+15z^4-20z^3-10z^2+5z+1}$
20	$z^9-3z^7+21z^5-20z^3+5z=z(z^2-z-1)(z^2+z-1)(\underline{z^4-5z^2+5})$

THE MINIMAL TARRY-ESCOTT PROBLEM

(Summary)

Eri Jabotinsky

The main result is contained in Theorems 8 and 9, which may be summarized as follows:

Let $P_n(z)$ be polynomials in z defined by the recurrence relation: $P_{n+2}(z)=z.P_n(z)-P_{n-2}(z)$, with the initial conditions: $P_0(z)=0$, $P_1(z)=P_2(z)=1$, $P_3(z)=z+1$. If $n|m$, then $P_n(z)$ divides $P_m(z)$. $P_m(z)$ is the product of factors appearing in the $P_n(z)$ for which $n|m$ and of a new factor $Q_n(z)$, called the n-th characterstic polynomial of the Tarry-Escott problem.

Let a,b,x,y be four parameters. Then the following algebraic congruence holds: (I) $\sum_{m=1}^{M}[A_m(x,y;z)]^k \equiv \sum_{m=1}^{M}[B_m(x,y;z)]^k \text{ Mod } P_M(z)$, where $A_m(x,y;z)=p_m(z).x+q_m(z).y$, $B_m(x,y;z)=p_m(z).x+q_{m-1}(z).y$, with: $p_m(z)=P_{m-1}(z)[-P_{m-4}(z).a'+P_{m-2}(z).b']$, $q_m(z)=P_{m-1}(z)[-P_{m-4}(z).a+P_{m-2}(z).b]$, and: $a'=(z+1)a-b$; $b'=a+b$.

The above proposition is established after ~~assuming~~ proving the following Lemma contained in Theorem 7:

Lemma. Let M be given. Then, if there exist homogeneous linear forms $A_m(x,y)$ and $B_m(x,y)$ defined for $m=1,2,\dots,M$ and for $m>M$ by the relations $A_{m+M}(x,y)=A_m(x,y)$ and $B_{m+M}(x,y)=B_m(x,y)$, such that: if, for arbitrary i and j, x and y are chosen to satisfy the equation $A_i(x,y)=A_j(x,y)$, then these same values of x and y satisfy the equations $A_{i+h}(x,y)=A_{j+h}(x,y)$ for any h, then these homogeneous linear forms satisfy the equation $\sum_{m=1}^{M}[A_m(x,y)]^k=\sum_{m=1}^{M}[B_m(x,y)]^k$ for $k=0,1,\dots,(M-1)$, provided $A_m(x,y)=p_m x+q_m y$ and $B_m(x,y)=p_m x+q_{m-1} y$.

The main instrument used is the following quite general

Theorem 5. If $\sum_{m=1}^{M}[A_m(x,y)]^k=\sum_{m=1}^{M}[B_m(x,y)]^k$ for $k=0,1,\dots,(M-1)$, A_m, B_m being any polynomials in x,y and if x,y are so chosen that $A_i(x,y)=B_j(x,y)$, then all the A_m are equal to the B_m in some order.

By chosing z to be the root of the characteristic polynomial $Q_M(z)$, equation (I) yields a non-trivial parametric solution in four parameters a,b,x,y of the minimal Tarry-Escott problem of the order (M-1) in integers belonging to the ring of the roots of $Q_M(z)$ over that of the rational integers. An example for M=12 is given.

Two hypotheses are formulated. The first hypothesis asserts that the solutions obtained from our main theorem for values of z for which $Q_M(z)=0$, are the only linear parametric solutions of the problem. The second hypothesis asserts that for every M there exists a parametric solution where the $A_m(x,y)$ and $B_m(x,y)$ are polynomials of the degree of the polynomial $Q_M^m(z)$.

הערות למאמרי „משפט Wolstenholme והכללותיו"

נתן אליוסף (קבקר)

1. במאמרי „משפט Wolstenholme והכללותיו" (יצויין להלן על-ידי W) שהופיע ב„רבעון למתמטיקה" כרך 4 עמ' 9-14 השתמשתי בתכונות מספרי Bernoulli כדי להוכיח משפטים שבנסוחם הסופי לא הופיעו מספרים אלה. יתר-על-כן הייתי נאלץ לנצל משפט עמוק כמשפט Clausen-Staudt מספר רב של פעמים. במאמר זה אראה כיצד להגיע לאותן התוצאות כמו ב-W בלי שמוש במספרי Bernoulli.

2. ב-W השתמשתי במספרי Bernoulli רק בשני סעיפים והם §§6,10.

3. המשפט W,§6. א) אם $p-1\nmid k$ יהיה $T_k(p^e)\equiv 0 \mod p^e$.

ב) אם $p-1|k$ יהיה $T_k(p^e)\equiv\varphi(p^e) \mod p^e$.

כאן מסמן $T_k(m)$ את $\sum_t t^k$ כאשר t עובר על כל המספרים הטבעיים הקטנים מ-m וזרים לו.

הוכחה. א) הוכח ב-W,§7 בלי שמוש במספרי Bernoulli.

ב) נחלק את ההוכחה לכמה מקרים, בהתאם לתכונות k.

אם $\varphi(p^e)|k$ המשפט ברור כי אז $t^k\equiv 1 \mod p^e$.

נניח אפוא כי $\varphi(p^e)\nmid k$.

מאחר ש- $T_k(p^e)\equiv T_{k'}(p^e) \mod p^e$ כאשר $k\equiv k' \mod \varphi(p^e)$, אפשר להניח, בלי הגבלת הכלליות, כי $0<k<\varphi(p^e)$.

נכתוב אפוא $k=(p-1)p^s u$ כאשר $p\nmid u$, $s\geq 0$, וכמו-כן $s<e-1$ בגלל ההגבלה על ה-k.

4. נמצא עתה את פתרונות הקונגרואנציה:

$$x^k\equiv 1 \mod p^e \dots\dots\dots\dots (1)$$

יהי g שרש פרימיטיבי $\mod p^e$. הפתרונות של (1) הם $1=g^0, g^r, g^{r'}, \dots$ ונניח כי $0<r<r'<\dots$. נוכיח כי $r|r'$. ואמנם אם $r'=ar+b$ כאשר $0\leq b<r$ נקבל כי g^b פותר את (1) ולכן $b=0$. מכאן רואים כי הפתרונות השונים של (1) הם:

$$A=\{1,g^r,g^{2r},\dots\}$$

נוכיח כי $r=p^{e-1-s}$. ואמנם, נסמן $R=p^{e-1-s}$. מצד אחד: $kR=(p-1)p^{e-1}u\equiv 0 \mod \varphi(p^e)$ ולכן $g^{kR}\equiv 1 \mod p^e$, ועל כן g^R מופיע בקבוצה A, ו- $r|R$. או $r|p^{e-1-s}$. מכאן $r=p^j$ כאשר $0\leq j\leq e-1-s$. מתוך $g^{kr}\equiv 1 \mod p^e$ ומהעובדה ש- g הוא שרש פרימיטיבי נקבל: $kr\equiv 0 \mod \varphi(p^e)$ ולכן $j\geq e-1-s$. בסך-הכל $j=e-1-s$ ועל כן $r=R$.

בסך-הכל רואים כי:

$$A=\{1,g^r,g^{2r},\dots,g^{(n-1)r}\} \dots\dots\dots\dots (2)$$

כאשר $n=p^s(p-1)$.

משפט-עזר. מספר הפתרונות של (1) הוא $p^s(p-1)$ בתנאי ש- $p-1|k$ ו-p^s היא החזקה הגבוהה ביותר של p המחלקת את k ובתנאי נוסף כי $0\le s\le e-1$.

5. נחזור להוכחת החלק ב' של המשפט ב- §3.

יהי t^k אחד המחוברים בסכום המגדיר את $T_k(p^e)$. אם x פותר את הקונגרואנציה (1) הרי $(tx)^k\equiv t^k \mod p^e$ ולכן $\mod p^e$ יופיע אותו מחובר בסכום $\sum t^k$ בדיוק $p^s(p-1)$ פעמים. לכן:

$$T_k(p^e)\equiv p^s(p-1)\sum{}' t^k \mod p^e$$

כאשר $\sum{}'$ מסמן את הסכום על כל ה-t כך שה-t^k שייכים למחלקות שאריות שונות $\mod p^e$. מתוך (2) רואים שאפשר לכתוב:

$$T_k(p^e)\equiv p^s(p-1)\sum_{j=0}^{r-1}(g^j)^k \mod p^e \text{............}(3)$$

נניח לרגע כי $s+1\ge e-s$ כלומר $s\ge\frac{e-1}{2}$. כאן $g^{p-1}\equiv1 \mod p$ ולכן $g^{(p-1)p^s}\equiv 1 \mod p^{s+1}$ ועל כן $g^k\equiv1 \mod p^{s+1}$. מאחר שאנו מניחים כי $s+1\ge e-s$ נקבל (לא-כל-שכן) $g^k\equiv1 \mod p^{e-s}$ ולכן $\sum_{j=0}^{r-1}(g^j)^k\equiv\sum_{j=0}^{r-1}1=r=p^{e-s-1} \mod p^{e-s}$. על-ידי הצבה ל- (3) יהיה:

$$T_k(p^e)\equiv p^s(p-1)p^{e-s-1}=p^{e-1}(p-1)=\varphi(p^e) \mod p^e$$

מה שרצינו להוכיח.

6. נבאר המקרה ש- $s<\frac{e-1}{2}$.

נכתוב: $k'=\varphi(p^e)-k=(p-1)p^{e-1-s}(p^s-u)=(p-1)p^{s'}u'$ כאשר $p\nmid u$. כאן $s'>\frac{e-1}{2}$ לכן לפי מה שהוכח ב- §5 נובע כי

$$T_{k'}(p^e)\equiv\varphi(p^e) \mod p^e$$

אולם (אם נסמן $p^e=P$) $\{t_1,\dots,t_{\varphi(P)}\}\equiv\{\frac{1}{t_1},\dots,\frac{1}{t_{\varphi(P)}}\} \mod P$ ולכן:

$$T_{k'}(P)\equiv\sum_t\frac{1}{t^{k'}}\equiv\sum_t\frac{1}{t^{\varphi(P)-k}}\equiv\sum_t\frac{t^{\varphi(P)}}{t^{\varphi(P)-k}}\equiv\sum t^k\equiv T_k(P) \mod P$$

ובזה הוכח המשפט בשלמותו.

7. ב- W, §9 הוכח, בלי שמוש במספרי Bernoulli כי:

$$T_k(m)\equiv p^eT_k(m_1)(1-p^{k-1})+\sum_{j=1}^{k}\binom{k}{j}m_1{}^jT_{k-j}(m_1)T_j(p^e)\text{....}(4)$$

כאשר $m=m_1p^e$ בתנאי שקיים $p\nmid m_1$.

8. המשפט W, §10. אם p^e היא החזקה הגבוהה ביותר של p המחלקת את m אז:

א) אם $p-1\nmid k$ יהיה $T_k(m)\equiv0 \mod p^e$.

ב) אם $p-1|k$ יהיה $T_k(m)\equiv\varphi(m) \mod p^e$.

הוכחה. על-סמך (4) נקבל בעזרת המשפט ב- §3 כי

$$T_k(m)\equiv\varphi(p^e)\sum_{p-1|j,\,j\ge1}\binom{k}{j}m_1{}^jT_{k-j}(m_1) \mod p^e\text{.....}(5)$$

מאחר ש- $\varphi(p^e)$ מתחלק על-ידי p^{e-1} די לטפל בסכום אשר ב- (5) רק $\mod p$.

מאחר ש- $p-1 | j$ על כן $m_1^{\,j} \equiv 1 \mod p$.

אם $j \neq k$ נקבל: $T_{k-j}(m_1) = \sum{}' t^{k-j} = \sum{}' t^k - \sum_{p|t} t^k = T_k(m_1) \mod p$.

אם $j=k$ (דבר כיתכן רק אם $p-1|k$) אז $T_0(m_1) = \varphi(m_1)$.

לכן:

א) אם $p-1 \nmid k$ יהיה $T_k(m) \equiv \varphi(p^e) T_k(m_1) B(p,k) \mod p^e$.

...(6) ב) אם $p-1|k$ יהיה $T_k(m) \equiv \varphi(p^e) T_k(m_1) C(p,k) + \varphi(p^e)\varphi(m_1) \mod p^e$.

כאן $B(p,k), C(p,k)$ הם מספרים התלויים ב- p,k אבל בלתי תלויים ב- m_1.

לכן נקח, למשל, $m_1=1$ ונקבל:

א) אם $p-1 \nmid k$, $T_k(p^e) \equiv \varphi(p^e) B(p,k) \mod p^e$. ועל-סמך המקרה א' במשפט אשר ב- §3 יהיה: $\varphi(p^e) B(p,k) \equiv 0 \mod p^e$. נציב לתוך א) אשר ב- (6) ונקבל את החלק א' של המשפט.

ב) אם $p-1|k$, $T_k(p^e) \equiv \varphi(p^e) C(p,k) + \varphi(p^e) \mod p^e$. על-סמך המקרה ב' במשפט אשר ב- §3 יהיה: $\varphi(p^e) C(p,k) \equiv 0 \mod p^e$. נציב לתוך ב) אשר ב- (6) ונקבל: $T_k(m) \equiv \varphi(p^e)\varphi(m_1) = \varphi(p^e m_1) = \varphi(m) \mod p^e$. קבלנו את החלק ב' של המשפט.

REMARKS ON MY PAPER "EXTENSIONS OF WOLSTENHOLME'S THEOREM" (Summary)

Nathan Eljoseph

In the above-named paper which has appeared in this Riveon, vol. 4, pp. 9-14, I made extensive use of the properties of the numbers of Bernoulli. In this paper I show how to prove all the theorems of that paper only with use of the concept of primitive root mod p^e.

METHOD OF PROOF. If $k=(p-1)p^s u$ where $0 \leq s < e-1$, $p \nmid u$ I prove that a l l the solutions of the congruence $x^k \equiv 1 \mod p^e$ are $A=\{1, g^r, \ldots, g^{(n-1)r}\}$ where g is a primitive root mod p^e, $r=p^{e-1-s}$ and $n=p^s(p-1)$. Hence if $T_k(p^e)=\sum{}' t^k$ where t is smaller than and coprime to p^e then $T_k(p^e) \equiv p^s(p-1)\sum{}' t^k$, the sum for all the t^k belonging to different residue classes mod p^e. Hence:

$T_k(p^e) \equiv p^s(p-1)\sum_{j=0}^{r-1}(g^j)^k \mod p^e$. It is easily seen that the sum is congruent to $p^{e-1-s} \mod p^{s+1}$ when $s \geq \frac{e-1}{2}$. If $s < \frac{e-1}{2}$ put $k' = \varphi(p^e)-k$ and $T_{k'}(p^e) \equiv T_k(p^e) \mod p^e$.

הוכחה ודוגמאות לכך שמשואת משפט הגדול של פרמה נתנת לפתרון בקוטרניונים שלמים

אברהם בירמן

לקוטרניון $q_1=a_0+a_1j_1+a_2j_2+a_3j_3$ נקרא "שלם" כאשר מקדמיו, כלומר a_0 וכו', הנם מספרים רציונליים שלמים. הקוטרניון $q_2=a_0-a_1j_1-a_2j_2-a_3j_3$ נקרא "צמוד" ל-q_1.

נוכיח להלן כי לגבי כל p, סכום החזקות ה-p-יות של שני קוטרניונים צמודים ושלמים הנו מספר רציונלי שלם, וכמו-כן נראה כי בתנאים מסוימים יכול סכום זה להיות הוא עצמו חזקה p-ית, וכך תתקים במובן ידוע משואתו המפורסמת של פרמה (Fermat): $q_1^p+q_2^p=d^p$, בעוד d מספר רציונלי שלם.

נציין באות s את החלק ה"על-דמיוני" של הקוטרניון, כלומר את $a_1j_1+a_2j_2+a_3j_3$. בהתאם לסמון זה יהיו: $q_1=a_0+s;\ q_2=a_0-s$.

נזכר-נא כי בשדה זה שרירה וקימת מערכת כל חוקי האלגברה הרגילה, פרט לאחד: החוק הקומוטטיבי של הכפל קים אמנם בין המקדמים ובין האלמנטים j_1, j_2, j_3 וכמובן גם בין המקדמים לבין עצמם, אך כדי שיתקים בין האלמנטים דרוש ל ה פ ו ך את הסימן: $j_1j_2=-j_2j_1$ וכו'. לפיכך נקל לראות כי: $s^2=-(a_1^2+a_2^2+a_3^2)$ כלומר מספר רציונלי שלם ושלילי.

אך היות והחוק הקומוטטיבי קים בין המקדמים, רשאים אנו לפתח את הבטוי $q_1^p=(a_0+s)^p=a_0^p+\binom{p}{1}a_0^{p-1}s+\dots$ בדרך הבינומית הרגילה. הוא הדין לגבי q_2^p, ולפיכך, בחברנו את הסכום $q_1^p+q_2^p$, תתבטלנה כל החזקות האי-זוגיות של s. הוי אומר, יתקבל מספר רציונלי שלם. הבה נראה אם ומתי יכול מספר זה להיות חזקה p-ית שלמה.

לתכלית זו נבחר תחלה את המקדמים באופן ש:

$$3a_0^2=a_1^2+a_2^2+a_3^2 \tag{1}$$

שהיא משואה דיופנטית הנתנת לפתרון. במקרה זה נקבל: $s^2=-3a_0^2$, ועל-כן:

$$q_1^p+q_2^p=a_0^p\cdot[(1+i\sqrt{3})^p+(1-i\sqrt{3})^p] \tag{2}$$

על-פי משפטו הידוע של דה-מואבר: $(\cos A+i\,snA)^p=\cos(pA)+i\,sn(pA)$ נקבל:

$$q_1^p+q_2^p=(2a_0)^p\,2\cos\frac{\pi\cdot p}{3} \tag{3}$$

אם p הוא מספר אי-זוגי ש א י נ ו מ ת ח ל ק ב - 3 (אך אין הוא צריך להיות ראשוני דוקא), אזי: $\cos\frac{\pi p}{3}=\frac{1}{2}$, ולכן:

$$q_1^p+q_2^p=(2a_0)^p \tag{4}$$

נציג, למשל, $a_0=a_1=a_2=a_3=1$ ונקבל קשר "פרמאי" בין י ח י ד ו ת בשדה זה:

$$(1+j_1+j_2+j_3)^p+(1-j_1-j_2-j_3)^p=2^p \tag{5}$$

או נציג, למשל, $a_0=11;\ a_1=17;\ a_2=7;\ a_3=5$ ונקבל: $3.11^2=17^2+7^2+5^2$ ואז תהיה המשואה המבוקשת:

$$(11+17j_1+7j_2+5j_3)^p+(11-17j_1-7j_2-5j_3)^p=22^p \qquad (6)$$

אם p מתחלק ב-3, שוב אין תוקף לנוסחאות הללו. לא קשה להוכיח כי אין התוצאה (3) אלא שנוי-צורה של המשואה הציקלוטומית $1+w^p+w^{2p}=0$, במקום שם יהא w שורש מעוקב של יחידה. ואם $3|p$ א י ן משואה זו נכונה!

ולא עוד אלא שבשביל $p=3$, למשל, הוכח כי למשואה (Hardy-Wright, Theory of Numbers, Ch. XIII, p. 192) $a^3=b^3+c^3$ א י ן פתרונות בתחום (השלם) $K(w)$. מאידך אפשר לנסח את התוצאות דלעיל בצורה זו: לכל מקרה של חזקה p שאינה מתחלקת ב-3, י ש פתרונות בתחום $K(w)$.

נחזור עתה למקרה $p=3$ וננסה למצוא פתרונות א ח ר י ם בקוטרניונים שלמים, ובסופו של דבר נגיע לפתרון ש ל ם של האפשרויות בקוטרניונים צ מ ו ד י ם . נכתוב:

$$K.a_0^2=a_1^2+a_2^2+a_3^2 \qquad (7)$$

במקום שם יהא K מספר רציונלי (לאו-דוקא שלם), וננסה לקבוע את ערכי K אשר יספקו את (7) ואשר יקימו גם את (4), כלומר:

$$(1+i\sqrt{K})^3+(1-i\sqrt{K})^3=d^3 \qquad (8)$$

d מספר רציונלי ש ל ם.

אחרי בטול החזקות האי-זוגיות נקבל: $2-6K=d^3$ ולכן

$$K=\frac{2-d^3}{6} \qquad (9)$$

מתברר אפוא כי K יכול להיות רק מספר רציונלי שמכנהו 6. נכתוב $K=g/6$. כדי שתתקיים המשואה (7) דרוש ומספיק כי את $6g$ אפשר יהיה לבטא כסכום של ש ל ו ש ה ר ב ו ע י ם ש ל מ י ם . כלומר, לפי משפט ידוע של גאוס, אם ורק אם ל א יהיה $6g$ בעל הצורה: $4^t(8N-1)$, במקום שם $t\geq 0$.

נציג $d=-4$ ונקבל $K=11$. אם נציג, למשל, $a_0=1;\ a_1=3;\ a_2=1;\ a_3=1$ נקבל:

$$(1+3j_1+j_2+j_3)^3+(1-3j_1-j_2-j_3)^3=(-4)^3 \qquad (10)$$

ננסה עתה למצוא באילו תנאים יכול סכום שתי חזקות ר ב י ע י ו ת של קוטרניונים צמודים להיות $\pm d^4$. שוב נגיע למשואה: $(1+i\sqrt{K})^4+(1-i\sqrt{K})^4=\pm d^4$. אחרי הפתוח נקבל: $2-12K+2K^2\mp d^4=0$. נפתור זאת כמשואה רבועית בנעלם K, ונזכור כי הדיסקרימיננטה חיבת להיות רבוע מלא: $128\pm 8d^4=v^2$. נציג $D=2d$ ונקבל: $4^4\pm D^4=2v_1^2$. ואולם לפי משפט ידוע של אוילר (עין Dickson, History of the Theory of Numbers II, page 628) אין פתרונות למשואה זו אלא אם כן $d=2;\ D=4$. לכן $K=3$, כלומר מקרה פרטי של הזהות (4). הגענו אפוא למסקנה כי זהו הפתרון ה י ח י ד בקוטרניונים צ מ ו ד י ם , ויש לשער (אף כי לא עלה בידי להוכיח) כי הוא הדין לגבי חזקות גבוהות יותר.

PROOF AND EXAMPLES THAT THE EQUATION OF FERMAT'S LAST THEOREM IS SOLVABLE IN INTEGRAL QUATERNIONS

Abraham Birman

(Summary)

First it is proved that the sum of the p^{th} powers of two quaternion c o n j u g a t e s is a real number.

If q_1 and q_2 are quaternion conjugates with rational integral coefficients:

$$q_1=a_0+a_1j_1+a_2j_2+a_3j_3; \quad q_2=a_0-a_1j_1-a_2j_2-a_3j_3$$

and if we choose the coefficients so as to satisfy the (solvable) Diophantine equation:

$3a_0^2=a_1^2+a_2^2+a_3^2$, we have: $q_1^p+q_2^p=a_0^p\left[(1+i\sqrt{3})^p+(1-i\sqrt{3})^p\right]=(2a_0)^p.2\cos\frac{\pi.p}{3}$.

If p is an odd rational integer not divisible by 3 (but not necessarily a prime), $\cos\frac{\pi.p}{3}$ will be equal to $\frac{1}{2}$, so that:

$$q_1+q_2=(2a_0)^p$$

If we set, for example, $a_0=a_1=a_2=a_3$, we shall obtain a relation between UNITIES of the field:

$$(1+j_1+j_2+j_3)^p+(1-j_1-j_2-j_3)^p=2^p$$

Setting $a_0=11$, $a_1=17$, $a_2=7$, $a_3=5$, we obtain a definitely non-trivial result:

$$(11+17j_1+7j_2+5j_3)^p+(11-17j_1-7j_2-5j_3)^p=22^p$$

If p is divisible by 3, these results are no longer correct. But it is possible to find other solutions for the case p=3. In fact, setting:

$$k.a_0^2=a_1^2+a_2^2+a_3^2 \text{ (solvable for certain values of k)}$$

we find that our basic equation is solvable,in cubes, for such values of k as 11, 85, etc.

For $k=11$, $a_0=1$, $a_1=3$, $a_2=1$, $a_3=1$, we have:

$$(1+3j_1+j_2+j_3)^3+(1-3j_1-j_2-j_3)^3=(-4)^3$$

For biquadrates it is proved that the only solution in integral quaternion conjugates is k=3, which has already been discussed. It is conjectured that the same result holds for higher powers. Therefore the number of solutions is rather limited.

מציאות אין-סוף מספרים פריקים n שבשבילם $2^{n-1} \equiv 1 \bmod n$

דב ירדן

ברשימה בשם
Remarque sur une hypothèse des Chinois concernant les nombres $(2^n-2)/n$
(Colloquium Mathematicum I (1947), p. 9) הוכיח W. Sierpiński את
מציאותם של אין-סוף מספרים פריקים n שבשבילם מתקימת הקונגרואנציה של
פרמה: $2^{n-1} \equiv 1 \bmod n$. נביא את הדברים בהרצאתו של שרפינסקי, בתרגום:

"המתמטיקאים הסיניים חשבו כי המספר $(2^n-2)/n$ איננו יכול להיות שלם כאשר n הוא מספר פריק.

מר ב נ ח ו י ץ ‎[1]‎ מצא ב-1909 חמשה מספרים טבעיים $n \leq 2000$ שההשערה הסינית איננה שרירה לגביהם ‎[2]‎. קטן המספרים האלה הוא $341=11.31$.

אקבע כאן את <u>מציאותם של אין-סוף מספרים פריקים n שבשבילם $(2^n-2)/n$ הוא מספר שלם</u>.

לשם כך, הואיל וקים

(*) <u>מספר פריק אי-זוגי אחד n שבשבילו $(2^n-2)/n$ הוא מספר שלם</u>,

די להוכיח כי, לכל n שיש לו התכונה (*), קים מספר k גדול מ-n שיש לו גם כן אותה תכונה. ואמנם, די להניח:

$$k=2^n-1.$$

ובאמת, יהי q מחלק של n ו- $1<q<n$. אז יש לנו קדם-כל $1<2^q-1<2^n-1=k$ ורואים בלי קשי כי 2^q-1 הוא מחלק של המספר k, שהוא אפוא פריק ולפי ההגדרה אי-זוגי. לבסוף, בהיות n אי-זוגי לפי ההנחה, $(2^n-2)/n$ הוא בעליל זוגי וחציו $m=(2^{n-1}-1)/n$ הוא כתוצאה מכך מספר שלם; והואיל ו- $2^{n-1}-1=mn$, יהיה לנו:

$2^{k-1}=2^{2(2^{n-1}-1)}=2^{2mn}=(2^n)^{2m}$, ומכאן $2^{k-1}-1=(2^n)^{2m}-1$, כך ש-$2^{k-1}-1$ מתחלק ב- $2^n-1=k$ וברור מאליו כי המספר $2(2^{k-1}-1)=2^k-2$, כלומר $(2^k-2)/k$ הוא מספר שלם. ובכן, ל-k ישנה התכונה (*), מה שהיה להוכיח."

עד כאן דברי שרפינסקי.

"1) T. B a n a c h i e w i c z , Comptes rendus de la Soc. des Sc. et de Lettres de Varsovie, Classe III, Année 2 (1909), p.9."

"2) המערכת למדה מתוך מכתב בא-מקרוב של מר ב נ ח ו י ץ ׳ שיש בדיוק שבעה (אלא שהוא לא מצא את השלישי ואת הרביעי כי-אם בזמן מאוחר יותר), והם:

$341=11.31$, $561=3.11.17$, $645=3.5.43$, $1105=5.13.17$, $1387=19.73$, $1729=7.13.19$, $1905=3.5.127$."

מטרת הרשימה הנכחית היא להוכיח את התוצאה של שרפינסקי על-יסוד שתי התכונות הפשוטות מאד של מספרי-פרמה $F_m=2^{2^m}+1$, הבאות:

(1) $2^{n-1}\equiv 1 \bmod n$ לכל $n=F_m$.[1]

(2) $2^{n-1}\equiv 1 \bmod n$ לכל $n=F_mF_{m+1}$, אם F_m, F_{m+1} הם מספרים ראשוניים ו- $m>1$.[2]

באמת, על-יסוד הזהות $a^2-1=(a-1)(a+1)$, יהיה לנו:

$$2^{2^{2^m}}-1=(2^{2^{2^m-1}}-1)(2^{2^{2^m-1}}+1)$$

$$2^{2^{2^m-1}}-1=(2^{2^{2^m-2}}-1)(2^{2^{2^m-2}}+1)$$

$$2^{2^{2^m-2}}-1=(2^{2^{2^m-3}}-1)(2^{2^{2^m-3}}+1)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$2^{2^{m+1}}-1=(2^{2^m}-1)(2^{2^m}+1)$$

ועל-ידי כפל אגף-אגף וחלוק בגורמים המשותפים נקבל:

$$2^{2^{2^m}}-1=(2^{2^{2^m-1}}+1)(2^{2^{2^m-2}}+1)(2^{2^{2^m-3}}+1)\dots(2^{2^{m+1}}+1)(2^{2^m}+1)(2^{2^m}-1) \quad (3)$$

באשר שלושת הגורמים האחרונים מופיעים תמיד, שכן $m>1$. ביניהם נמצא הגורם $2^{2^m}+1$, מה שמוכיח את (1).

לשם הוכחת (2) נשים אל לב, כי אם p ו-q הם מספרים ראשוניים שונים ו- $2^q\equiv 2 \pmod p$, $2^p\equiv 2 \pmod q$, אז $2^{pq}\equiv 2 \pmod{pq}$. באמת, $2^{pq}\equiv 2^q\equiv 2 \pmod p$ לפי משפט פרמה, וכיוצא בו $2^{pq}\equiv 2^p\equiv 2 \pmod q$. מכאן $2^{pq}\equiv 2 \pmod{pq}$.[3] הקונגרואנציה $2^x\equiv 2$ (M) נובעת מן $2^{x-1}\equiv 1$ (M), ולכן די להוכיח את האחרונה. ואמנם (אם נשים: $p=2^{2^m}+1$, $q=2^{2^{m+1}}+1$)

$$2^{2^{2^{m+1}}}=(2^{2^{2^m}})^{2^{2^m}}\equiv 1 \pmod{2^{2^m}+1}$$

ואילו, הואיל והגורם $2^{2^{m+1}}+1$ מופיע תמיד ב-(3), נקבל גם:

$$2^{2^{2^m}}\equiv 1 \pmod{2^{2^{m+1}}+1}$$

מה שמוכיח את (2).

---

1) L. E. Dickson, History of the theory of numbers I, p. 94.

2) משפט זה הוא מקרה מיוחד ממשפט M. Cipolla המובא בדקסון, שם, ציון 229.

3) Hardy-Wright, An introduction to the theory of numbers, second edition (1945), p.71-72.

לשם הוכחת מציאות אין-סוף מספרים פריקים n שבשבילם $2^{n-1} \equiv 1 \mod n$ נשתמש עכשיו בדרך "ממה-נפשך": מספר המספרים הפריקים F_m הוא או אין-סופי או סופי. במקרה הראשון מוכיח (1) את תוצאת סרפינסקי. במקרה השני יוצא כי, בשביל מספר טבעי מסוים $m>1$, כל המספרים F_k, $k=m, m+1, m+2, \ldots$ הם ראשוניים. בהניחנו $n=F_iF_{i+1}$, באשר $i \geq m$, נקבל אפוא את תוצאת סרפינסקי על-יסוד (2).

EXISTENCE OF AN INFINITUDE OF COMPOSITE n FOR WHICH $2^{n-1} \equiv 1$ MOD n

Dov Jarden

(Summary)

In Colloquium Mathematicum I (1947), p. 9, W. Sierpiński proved the existence of an infinitude of composite numbers n satisfying the congruence $2^{n-1} \equiv 1 \mod n$, using the fact that, if $2^{n-1}-1$ is divisible by n, then $2^{2^n-2}-1$ is divisible by 2^n-1. The aim of the present note is to prove Sierpiński's result by the following two very simple properties of the Fermat-numbers $F_m = 2^{2^m}+1$:

(1) $2^{n-1} \equiv 1 \mod n$ for every $n=F_m$.

(2) $2^{n-1} \equiv 1 \mod n$ for $n=F_mF_{m+1}$ if F_m, F_{m+1} are primes and $m>1$ (Compare Dickson, History of the Theory of Numbers I, p. 94).

Now, the number of composite F_m is either infinite, or finite. In the first case, (1) proves Sierpiński's result. In the second case, it follows that, for a certain positive integer $m>1$, all the numbers F_k, $k=m, m+1, m+2, \ldots$, are primes. Then, supposing $n=F_iF_{i+1}$, where $i \geq m$, we obtain Sierpiński's result by (2).

תקונים לכרכים 2-3

כרך 2 עמוד 21 בהמשך שורה 9 מלמטה צריך לומר:
באגף הימני של DW_n רשום במקום כל k שרשים שוים לפי הסדר את נגזרותיהם האפסיות, הראשונות, השניות עד הנגזרות מסדר $k-1$.

כרך 3 עמוד 4 שורה ראשונה לפני הנוסחה (16) צריך לומר: $\xi_2, \xi_3, \ldots, \xi_{n-1}$ (במקום $\xi_1, \xi_2, \ldots, \xi_n$).

כרך 3 עמוד 37 שורות 2,5 מלמטה צריך לומר: .T.-F (במקום .T.-B).

כרך 3 עמוד 40 שורה 18 צריך לומר: (3.232) (במקום (3.231)).

כרך 3 עמוד 40 שורה 20 צריך לומר: $\sum_{n=s+1}^{\infty} |a_{un}|$ (במקום $\sum_{n=s}^{\infty} |a_{un}|$).

כרך 3 עמוד 41 שורה אחרונה צריך לומר: (3.21) (במקום (3.22)).

כרך 3 עמוד 59 שורה 3 צריך לומר: $\equiv B_1 \pmod p$ (במקום $=B_1$).

כרך 3 עמוד 59 שורה 4 צריך לומר: $3B \equiv \ldots \pmod p$ (במקום $3B = \ldots$).

כרך 3 עמוד 59 שורה 5 צריך לומר: $B \equiv \ldots \pmod p$ (במקום $B = \ldots$).

כרך 3 עמוד 62 שורה 2 של משפט-עזר ב" צריך לומר: $m=2^a$ (במקום $m=2$).

כרך 3 עמוד 62 שורה 3 מלמטה צריך לומר: $r_2 \equiv (2^{a-1}+1)$ (במקום $r_2 \equiv (2^{a-1}+)$).

כרך 3 עמוד 63 שורה 6 של §14 צריך לומר: $t \neq t'$ (במקום $t \neq t_0$).

כרך 3 עמוד 63 בהערה בסוף §14 צריך לומר: $m \neq p$ (במקום $m=p$).

כרך 3 עמוד 64 שורה 6 של הסכום האנגלי צריך לומר: 1/A (במקום L/A).

תכן כרך 4

Contents of Volume 4

ר ב ע ו ן ל מ ת מ ט י ק ה

ללמוד ולמחקר

בעריכת

דב ירדן

כרך 4

תש"י-י"א

ירושלם

R I V E O N L E M A T E M A T I K A

A Quarterly Journal
Intended to Promote Mathematical Research
Among Students of Mathematics

Dov Jarden
Editor

Volume 4
1950

Jerusalem
Israel

RIVEON LEMATEMATIKA

A QUARTERLY JOURNAL

INTENDED TO PROMOTE MATHEMATICAL RESEARCH
AMONG STUDENTS OF MATHEMATICS

DOV JARDEN, EDITOR

Volume 4 — Jerusalem, October 1950 — Number 3—4

CONTENTS

Editor's address: Dov Jarden, Kneset Hachadasha, Jerusalem, Israel