רבעון למתמטיקה

ללמוד ולמחקר

בעריכת דב ירדן

חוברת 4

ירושלים, אלול תש"ח, אוקטובר 1948

כרך 2

תכן

כתבת המערכת: דב ירדן, מלאכי 20, ירושלים

המחיר 200 מיל

על פתרון משוואות ליניאריות מסדימות בחוג המרפשט

פסח חברוני

§1. על הקשר בין המשוואות $a_1x_1=b$, $a_2x_2=b$ ו $a_1(a_1+a_2)^{-1}a_2x=b$ בתוך חוג בעל יחידה. יהא R איזה חוג שהוא בעל יחידה. בין הפתרונים של שלש המשוואות שבחוג

$$a_1x_1=b, \tag{1}$$

$$a_2x_2=b, \tag{2}$$

$$a_1(a_1+a_2)^{-1}a_2x=b \tag{3}$$

ישנם קשרים קבועים הנתנים ע"י המשפט הבא.

משפט 1. 1) אם x_1 ו x_2 ממלאים את 1) ו 2) אז

$$x=x_1+x_2 \tag{3'}$$

ממלא את 3).

2) ולהפך, מתוך כל פתרון x של 3) נקבל פתרונים של 1) ושל 2) ע"י הנוסחאות

$$x_1=(a_1+a_2)^{-1}a_2x, \quad x_2=(a_1+a_2)^{-1}a_1x \tag{4}$$

x_1 ו x_2 אלו ממלאים ביחד עם הפתרון x של 3) את המשויה 3').

3) אם נתן ב 3') את x_1 לעבור את כל הפתרונים של 1) ואת x_2 לעבור את כל הפתרונים של 2), אז יעבור x את כל הפתרונים של 3).

הוכחה. 1) מ 1) ו 2) יצא

$$a_1(a_1+a_2)^{-1}a_1x_1=a_1(a_1+a_2)^{-1}b, \tag{4'}$$

$$a_1(a_1+a_2)^{-1}a_2x_2=a_1(a_1+a_2)^{-1}b, \tag{5}$$

$$a_1(a_1+a_2)^{-1}(a_1+a_2)x_1=b. \tag{6}$$

נחבר את 5) ל 6) ונחסיר את 4') ונקבל $a_1(a_1+a_2)^{-1}a_2(x_1+x_2)=b$ ובזה הוכח 1).

2) יהא x איזה פתרון שהוא של 3). נגדיר את x_1 ואת x_2 ע"י 4) (מה שאפשר לאחר ההפיכות של x_1+x_2) ואז יהיה

$$x_1+x_2=(a_1+a_2)^{-1}(a_1+a_2)x=x.$$

מלבד זה יהיה בתוקף 4_1) ו 3)

$$a_1x_1=a_1(a_1+a_2)^{-1}a_2x=b$$

כלומר x_1 ממלא את 1) ולפי"ז עלינו רק להוכיח עוד כי x_2 ממלא את 2). לשם הכנה נעיר כי

$$a_1(a_1+a_2)^{-1}a_2+a_2(a_1+a_2)^{-1}a_2=(a_1+a_2)(a_1+a_2)^{-1}a_2=a_2=$$
$$=a_2(a_1+a_2)^{-1}(a_1+a_2)=a_2(a_1+a_2)^{-1}a_1+a_2(a_1+a_2)^{-1}a_2$$

וא"כ

$$a_2(a_1+a_2)^{-1}a_1=a_1(a_1+a_2)^{-1}a_2 \tag{7}$$

מ 4_2), 7) ו 3) יצא

$$a_2x_2=a_2(a_1+a_2)^{-1}a_1x=a_1(a_1+a_2)^{-1}a_2x=b \tag{8}$$

ובזה הוכחנו גם את 2).

3) יוצא מ 1) ומ 2) שהרי 1) אומר: אם x_1 ו x_2 ממלאים את 1) ואת 2), אז ה x הנתן ע"י 3') ממלא 3). ו 2) אומר: כל x הממלא את 3) אפשר לפרקו לסכום x_1+x_2 באופן ש x_1 ו x_2 ימלאו את 1) ואת 2).

§2. על משויה ליניארית מטפוס ידוע בחוג המופשט. אנו מניחים כי החוג R שבו אנו מטפלים כעת מכיל את כל המספרים (גם הממשיים וגם המרוכבים). מובן שהמספרים יהוו חלק של המרכז של R (או את כולו).

יהא a איזה אלמנט שהוא בתוך החוג. בפולינום

$$f(a)=\sum_{i=0}^{n+1}\beta_i a^{i-1} \tag{10}$$

יהיו ה β_i מספרים. תהא נתונה המשויה

$$f(a)x=c, \tag{11}$$

אשר בה c הוא איזה אלמנט שהוא ב R. בכדי לפתור את 11) נפרק את $f(a)$ לגורמים ליניאריים

$$f(a)=\prod_{k=1}^{n}(a-\alpha_k), \tag{12}$$

ופה יהיו $\alpha_1,\ldots\alpha_n$ מספרים. אם נשים את הערך של $f(a)$ (12 בתוך 11) נקבל

$$\prod_{k=1}^{n}(a-\alpha_k)x=c. \tag{13}$$

אנו מניחים כי $\alpha_1,\ldots\alpha_n$ כולם שונים זמ"ז. בכדי לפתור את 13) נתבונן למשויות העזר

$$(a-\alpha_k)x_k=I_k, \qquad 1\leq k\leq n \tag{14}$$

אשר את ה $I_1,I_2,\ldots I_n$ שבהן עתידים אנו לקבוע באופן מתאים. אנו כותבים לשם סמון

$$f_k(a) = \frac{f(a)}{a-\alpha_k} \tag{14'}$$

אז נקבל מתוך 14)

$$f(a)x_k=f_k(a)(a-\alpha_k)x_k=f_k(a)I_k$$

מכאן יצא

$$f(a)\sum_{k=1}^{n}x_k = \sum_{k=1}^{n}f_k(a)I_k$$

נניח כי ה $I_1,\ldots I_n$ נבחרו באופן ש

$$\sum_{k=1}^{n}f_k(a)I_k=c \tag{15}$$

אז יהיה

$$x = \sum_{k=1}^{n}x_k \tag{15'}$$

פתרון של 11). $f_k(a)$ היא פולינום ממעלה ה $n-1$ ב a שמקדמיו הם מספרים. יהא

$$f_k(a) = \sum_{i=1}^{n}\alpha_{ik}a^{i-1} \tag{16}$$

אז תהפך המשויה 15) ל

$$\sum_{i=1}^{n}a^{i-1}\sum_{k=1}^{n}\alpha_{ik}I_k=c \tag{17}$$

נכתוב דרך סמון

$$\delta_i = \begin{cases} 1 & \text{אם } i=1 \\ 0 & \text{אם } i\neq 1 \end{cases}$$

ונבקש למלא את 17) ע"י כך שנשתדל לבחור את $I_1,\ldots I_n$ באופן שיהיה

$$\sum_{k=1}^{n}\alpha_{ik}I_k = \delta_i c \qquad 1\leq i\leq n \tag{18}$$

אם הדטרמיננטה $D=|\alpha_{ik}|$ ממלאה את התנאי

$$D \neq 0 \tag{19}$$

נוכל לקבוע את ערכם של ה I_k מתוך המשויות (18 באופן חד-משמעי. לאחר קביעתם של ה I_k יתן כל פתרון $x_1,\dots x_n$ של (14 ע"י חבורם של האלמנטים האלה, $x=\sum_{k=1}^{n} x_k$, פתרון אחד של (11.

נוכל להוכיח, כי על יסוד ההנחה ש $\alpha_1,\dots,\alpha_n$ כולם שונים זמ"ז ימלא אי-השויון (19.

אם נניח לרגע כי $\alpha_s=\alpha_t$ אז יהיה $f_s(a)=f_t(a)$ ואא"כ יהיה $\alpha_{is}-\alpha_{it}$ בשביל $1\leq i\leq n$ מתחלק על ידי $\alpha_s-\alpha_t$. ואא"כ D מתחלק על ידי מכפלת-ההפרשים D' (Differenzenprodukt) של $\alpha_1,\dots\alpha_n$. מכיון שגם D וגם D' הם פולינומים ממעלה ה $\frac{1}{2}n(n-1)$ ב $\alpha_1,\dots\alpha_n$ הרי בהכרח יהיה

$$D = kD'$$

במקום ש k הוא מספר בלתי תלוי ב $\alpha_1,\dots,\alpha_n$. k אינו יכול להיות 0 שהרי, כפי שנקל לראות, המקדם של $\alpha_1^{\,n-1}\alpha_2^{\,n-2}\dots\alpha_{n-1}$ ב D הוא שונה מ 0 ובכן לא רק D' שונה מ 0 (בתור מכפלת ההפרשים של השעורים $\alpha_1,\dots,\alpha_n$ שכולם שונים זמ"ז) כי"א גם k. ולפי"ז גם $D\neq 0$. ובכן יוצא לנו

<u>משפט 2.</u> נניח כי השרשים $\alpha_1,\dots\alpha_n$ של הפולינום (10 הם שונים זמ"ז. אם נגדיר את המספרים α_{ik} $1\leq i,k\leq n$ ע"י (14' ו (16 אז תמלא (19. בעזרת (18 נוכל לקבוע את האלמנטים I_k $1\leq k\leq n$ באפן חד-משמעי. ואז מכל פתרון $x_1,\dots x_n$ של המשויות (14 נקבל פתרון x של (11 ע"י שנשים $x=\sum_{i=1}^{n} x_i$. נכון גם ההפך של משפט זה

<u>משפט 3.</u> אם השרשים $\alpha_1,\dots\alpha_n$ של $f(a)=0$ הם שונים זמ"ז אז כל פתרון x של (11 יכול להיות מוצג בצורת (15' במקום שה x_k הם פתרונים של (14.

<u>הוכחה.</u> המטריצה (α_{ik}) היא הפיכה בשל (19. אנו כותבים דרך סמון

$$(\beta_{ik})=(\alpha_{ik})^{-1}$$

ואז יהיה $(\alpha_{ik})(\beta_{ik})=(1)$. ואא"כ

$$\sum_{k=1}^{n}\alpha_{ik}\beta_{k1}=\delta_i \tag{20}$$

במקום ש $\delta_1,\delta_2,\dots\delta_n$ מוגדרים ע"י (17'. מ (18 יצא

$$I_k = \sum_{\varrho=1}^{n}\beta_{k\varrho}\delta_\varrho c=\beta_{k1}c.$$

יהא x איזה פתרון שהוא של (11. נשים $1\leq k\leq n$ $x_k=\beta_{k1}f_k(a)x$

אז יהיה

$$(a-\alpha_k)x_k=\beta_{k1}(a-\alpha_k)f_k(a)x=\beta_{k1}f(a)x=\beta_{k1}c=I_k$$

I_k אלו ממלאים (14. נוסף לכך יהיה בשל (16 ו (20

$$\sum_{k=1}^{n}x_k=\sum_{k=1}^{n}\beta_{k1}f_k(a)x=\sum_{k=1}^{n}\beta_{k1}\sum_{i=1}^{n}\alpha_{ik}a^{i-1}x=\sum_{i=1}^{n}a^{i-1}\sum_{k=1}^{n}\alpha_{ik}\beta_{k1}x=\sum_{i=1}^{n}a^{i-1}\delta_i x=a^0x=x,$$

מה שהיה עלינו להוכיח.

<u>דוגמה.</u> יהא n=2 $\quad f(a)=a(a+1)$

במקרה זה יהיה $\quad f_1(a)=a+1\ ,\ \ f_2(a)=a$

$$(\alpha_{ik})=\begin{pmatrix}1,0\\1,1\end{pmatrix}\ ,\quad (\beta_{ik})=\begin{pmatrix}1,0\\-1,1\end{pmatrix}\ ,$$

$$I_1=\beta_{11}c=c\ ,\quad I_2=\beta_{21}c=-c$$

ולפי"ז הנושא שלנו במקרה זה הוא פתרון המשויות

$$a(a+1)x=c, \tag{21}$$

22) $ax_1=c,$

23) $(a+1)x_2=-c.$

ונקבל מן האמור לעיל: אם x_1 ו x_2 הם אי-אלו פתרונים שהם של (22 ו (23 אז יהיה $x=x_1+x_2$ פתרון של (21. ולהפך: כל פתרון של (21 יכול להיות מוצג כסכום של שני פתרונים של (22 ושל (23 כלומר $x=x_1+x_2$, וכאן יהיה

$$x_1=(a+1)x\ ,\quad x_2=-ax.$$

פתרון של מערכת קונגרואנציות

נתן קבקר

1. נתונות שתי מערכות של מספרים שלמים $a_1,\dots,a_n$; $m_1,\dots,m_n$. רוצים לפתור את מערכת הקונגרואנציות

$$x\equiv a_1 \bmod m_1\ ;\ x\equiv a_2 \bmod m_2;\ \dots;\ x\equiv a_n \bmod m_n. \qquad (\text{א})$$

נסמן ע"י $(m_1,\dots,m_n)$ את המחלק המשותף הגדול ביותר של $m_1,\dots,m_n$.

אם $(m_1,\dots,m_n)=1$ יש למערכת (א) פתרון יחיד $\bmod\ m_1\dots m_n$. את הפתרון הזה קל לחשב (ראה למשל:

Hardy-Wright: An Introduction to the Theory of Numbers, 1938, §8.1).

מטרת המאמר הזה הוא למצוא תנאי הכרחי ומספיק לכך שלמערכת (א) יהיה פתרון, ולמצוא את הפתרון במקרה שהוא קיים.

2. להלן נסמן ע"י m את הכפולה המשותפת הקטנה ביותר של ה m_i-ים.

3. נניח לרגע כי למערכת (א) יש פתרון, וננסה לחשב אותו. נסמן את הפתרון באות x.

נכפיל את הקונגרואנציה $x\equiv a_i \bmod m_i$, $(i=1,\dots,n)$ במספר m/m_i. ע"כ תתקבל הקונגרואנציה:

$$(m/m_i)x \equiv a_i(m/m_i) \bmod m_i(m/m_i)$$

כלומר:

$$(m/m_i)x \equiv a_i(m/m_i) \bmod m. \qquad (\text{ב})$$

ברור כי

$$((m/m_1),\dots,(m/m_n)) = 1$$

ע"כ אפשר למצוא מספרים שלמים $s_1,\dots,s_n$ כך שיתקיים:

$$(m/m_1)s_1+\dots+(m/m_n)s_n = 1 \qquad (\text{ג})$$

נכפיל את הקונגרואנציה (ב) ע"י s_i:

$$(m/m_i)s_ix \equiv a_i(m/m_i)s_i \bmod m.$$

נחבר את כל הקונגרואנציות האלה:

$$x\sum_{i=1}^{n}(m/m_i)s_i \equiv \sum_{i=1}^{n}a_i(m/m_i)s_i \bmod m.$$

לכן, עפ"י (ג):

$$x \equiv \sum_{i=1}^{n}a_i(m/m_i)s_i \bmod m. \qquad (\text{ד})$$

משפט 1. אם יש למערכת (א) פתרון, הפתרון הוא יחיד $\bmod m$, ונתון ע"י (ד).

4. משפט 2. תנאי הכרחי ומספיק לכך שיהיה פתרון למערכת הקונגרואנציות

$$x\equiv a_1 \bmod m_1;\ x\equiv a_2 \bmod m_2 \qquad (ה)$$

הוא כי: $a_1\equiv a_2 \bmod (m_1,m_2)$.

הוכחה: פה $x=a_1+m_1u$ מהקונגרואנציה הראשונה, $x=a_2+m_2v$ מהשניה. לכן המערכת (ה) אקויולנטית למשואה הדיופנטית:

$$m_1u-m_2v=a_2-a_1$$

כדי שלמשואה זו יהיה פתרון שלם, הכרחי ומספיק כי (m_1,m_2) יחלק את a_2-a_1 (ראה למשל §5.4 בספר המצוטט ב 1). וזה מה שהיה עלינו להוכיח.

5. בתור מסקנה מידית ממשפט 2 נקבל:

משפט 3. תנאי הכרחי לכך שלמערכת (א) יהיה פתרון, הוא כי

$$a_i\equiv a_j \bmod (m_i,m_j) \quad i,j=1,\dots,n \qquad (ו)$$

יש עוד לברר אם תנאי זה הוא מספיק.

6. נניח אפוא כי התנאים (ו) מתקימים.

באופן דומה להוכחת משפט 2, עלינו לראות אם יש פתרון למערכת המשואות הדיופנטיות:

$$x=a_1+m_1u_1=a_2+m_2u_2=\dots=a_n+m_nu_n$$

לשם זה די להסתכל במערכת המשואות הדיופנטיות (את השאר אפשר לקבל ע"י חסור שתים מאלה המסומנות להלן)

$$\begin{matrix} m_1u_1-m_2u_2=a_2-a_1 \\ m_1u_1-m_3u_3=a_3-a_1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ m_1u_1-m_nu_n=a_n-a_1 \end{matrix} \qquad (ז)$$

מספר המשואות כאן הוא $n-1$.

כיון שקימים התנאים (ו), נובע כי לכל משואה דיופנטית ב (ז) בפני עצמה יש פתרון (משפט 2). יש לראות האם יש פתרון הדדי לכלן.

נניח כי $u_1=U_2;\ u_1=U_3;\ \dots;\ u_1=U_n$ פותרים בהתאמה את משואות המערכת (ז). הפתרונות הכלליים ב (ז) נתונים ע"י

$$u_1=U_2+\frac{m_2}{(m_1,m_2)}v_2;\ u_1=U_3+\frac{m_3}{(m_1,m_3)}v_3;\ \dots;\ u_n=U_n+\frac{m_n}{(m_1,m_n)}v_n \qquad (ח)$$

(פה ה v_i-ים רצויים).

יש לראות האם אפשר למצוא מספרים שלמים $v_2,\dots,v_n$ כך שעבורם יתקבל אותו ערך בשביל u_1 מכל $n-1$ המשואות.

יש לנו אפוא לפתור את מערכת הקונגרואנציות הבאה:

$$u_1\equiv U_2 \bmod m_2/(m_1,m_2);\ \dots;\ u_1\equiv U_n \bmod m_n/(m_1,m_n) \qquad (ט)$$

כלומר, עלינו לפתור מערכת מהסוג (א) כשמספר הקונגרואנציות הוא $n-1$.

משפט 4. אם קימים התנאים (ו) ויש פתרון למערכת (ט), יש פתרון למערכת (א).

7. נפנה כעת למערכת (ט), ונוכיח כי היא מקימת את התנאים (ו).

לפי הגדרת ה U_i-ים:

$$m_1U_i-m_iu_i'=a_i-a_1$$

$$m_1U_j-m_ju_j'=a_j-a_1$$

ע"י חסור נקבל:

$$m_1(U_i-U_j)-m_iu_i'+m_ju_j'=a_i-a_j$$

ע"ס (ו):

$$a_i\equiv a_j \mod (m_i,m_j)$$

ולכן:

$$m_1(U_i-U_j)\equiv 0 \mod (m_i,m_j)$$

או בכתיב אחר:

$$U_i\equiv U_j \mod \frac{(m_i,m_j)}{(m_1,(m_i,m_j))} \qquad (\text{י})$$

ברור כי:

$$\frac{(m_i,m_j)}{(m_1,(m_i,m_j))}=\left(\frac{m_i}{(m_1,m_i)},\frac{m_j}{(m_1,m_j)}\right)$$

ע"כ במקום (י) נכתוב:

$$U_i\equiv U_j \mod \left(\frac{m_i}{(m_1,m_i)},\frac{m_j}{(m_1,m_j)}\right)$$

אם נסתכל ב (ט) נראה כי אלה הם בדיוק התנאים (ו) עבור מערכת קונגרואנציות זו.

<u>משפט 5.</u> המערכת (ט) מקימת את התנאים מספוס (ו).

8. <u>משפט 6.</u> אם תנאים מהספוס (ו) מתקימים עבור מערכת קונגרואנציות, יש למערכת פתרון.

<u>הוכחה.</u> אם n, מספר הקונגרואנציות במערכת, הוא 2, המשפט נכון (משפט 2).

נניח כי המשפט נכון עבור $n-1$. אז, ע"ס משפט 5, יש למערכת (ט) פתרון. מכאן, ע"ס משפט 4, יש פתרון עבור המערכת (א); כלומר המשפט נכון עבור n. המשפט 6 הוכח אפוא בדרך האינדוקציה.

9. סכום.

<u>משפט 7.</u> תנאי הכרחי ומספיק לכך שלמערכת קונגרואנציות (א) יהיה פתרון, הוא (ו). אם יש פתרון, הוא יחיד $\mod m$, ונתון ע"י (ד).

<u>הערה:</u> משפט 7 מכיל כמקרה פרטי את המשפט המצוטט ב §1.

על פרוק מספרי פבונצ׳י

דב ירדן

1. <u>מבוא.</u> מטרת המאמר הנכחי היא לקבע צורות ליניאריות שלהן שיכים המחלקים הראשוניים הקדומים של מספרי פבונצ׳י. השמוש בצורות ליניאריות מצמצם במדה נכרת את מספר הנסיונות הדרושים לפרוק[1]. בשיטה זו השתמש כבר E. Lucas[2], אלא שלא הסדיר את תוצאותיו וקבל צורות ליניאריות חלשות יותר מהנתנות להלן בלוחות I, II.

2. <u>הסדרות (u_n) ו (v_n).</u> יהי u_n המספר ה n-י של פבונצ׳י, קים

$$u_1=u_2=1,\ u_n=u_{n-1}+u_{n-2}$$

יהי v_n המספר ה n-י של סדרה דומה המגדרת ע"י $v_1=1,\ v_2=3,\ v_n=v_{n-1}+v_{n-2}$.
קים $u_{2n}=u_nv_n$ [3].

3. מחלקים קדומים. מחלק $d>1$ של u_n (או v_n) נקרא קדום, אם הוא זר לכל u_m (או v_m) בעל $m<n$. קימים כללים פשוטים הנותנים את כל המחלקים הבלתי קדומים של u_n, אם רק ידוע הפרוק של כל ה u_m בעלי $m|n$. פרוק מספרי פבונצ׳י מצטמצם אפוא לפרוק מחלקיהם הקדומים המכסימליים. נוסף לזה קים המשפט הבא:

A. המחלקים הקדומים המכסימליים של u_{2n} ו v_n מתלכדים [4]. הפרוק של u_{2n} שקול אפוא כנגד הפרוק של v_n.

4. צורות ליניאריות. קימים המשפטים הבאים:

I. הצורה הליניארית של כל מחלק ראשוני קדום p של u_n נתונה בשביל $n>5$ אי-זוגי ע״י הלוח הבא:

$n\equiv$	1	(mod 10), $p\equiv$	1,8n+1,14n-1,18n-1	(mod 20n)
	3		1,6n-1,16n+1,18n-1	
	7		1,2n-1, 4n+1,14n-1	
	9		1,2n-1, 6n-1,12n+1	
	5		1	(mod 4n)

II. הצורה הליניארית של כל מחלק ראשוני קדום p של u_{2n} (ושל v_n) נתונה ע״י הלוח הבא:

$n\equiv$	1	(mod 10)	$p\equiv$	1,8n+1	(mod 10n)
	3			1,6n+1	
	7			1,4n+1	
	9			1,2n+1	
	5			1	(mod 2n)
	0	(mod 20)		1	
	10			1	(mod 4n)
	2			1,2n-1, 4n+1,14n-1	(mod 20n)
	6			1,8n+1,14n-1,18n-1	
	14			1,2n-1, 6n-1,12n+1	
	18			1,6n-1,16n+1,18n-1	
	4			1,2n-1, 2n+1, 6n-1	(mod 10n)
	8			1,6n-1, 6n+1, 8n-1	
	12			1,2n-1, 4n-1, 4n+1	
	16			1,4n-1, 8n-1, 8n+1	

הוכחת I מתבססת על שתי ההצעות הבאות:

B. בשביל n אי-זוגי כל מחלק ראשוני אי-זוגי של u_n הוא $\equiv 1$ (מודולו 4)[5].

C. כל מחלק ראשוני קדום p של u_n הוא $\equiv (5/p)$ (מודולו n), באשר $(5/p)$ הוא סמל לג׳נדר [6].

ע״י צרוף B ו C ובשים לב לכך כי $(5/p)=1$ בשביל $p\equiv\pm1 \pmod{10}$ ו $(5/p)=-1$ בשביל $p\equiv\pm3 \pmod{10}$, שמכאן בשביל $n>5$ אי-זוגי $p\equiv(5/p) \pmod{2n}$, נקבל את הלוח I.

הוכחת II מתבססת על שתי ההצעות הבאות:

D. בשביל n אי-זוגי, כל מחלק ראשוני אי-זוגי של v_n הוא $\equiv \pm1$ (מודולו 10). בשביל $n\equiv2 \pmod 4$, כל מחלק ראשוני אי-זוגי של v_n הוא $\equiv 1, 3, 9, 27$ (מודולו 40). בשביל $n\equiv0 \pmod 4$, כל מחלק ראשוני אי-זוגי של v_n הוא $\equiv 1, 7, 9, 23$ (מודולו 40)[7].

E. כל מחלק ראשוני קדום של v_n הוא $\equiv (5/p)$ (מודולו $2n$) (זה נובע מיד מ A ו C).

ע״י צרוף D ו E נקבל את הלוח II.

---

1) השוה: דב ירדן, השלמות ללוח מספרי פבונצ׳י, רבעון למתמטיקה 2(תשי״ח),22; דב ירדן ואלכסנדר כץ, גורמים חדשים של מספרי פבונצ׳י, שם, 35.

2) C.R.82 (1876),167. 3) E.Lucas, Amer.Jour.Math. 1(1878),185.

Niedere Zahlentheorie II (1910), 83. 7) l.c. 201,212.

על סכום הרבועים של הפונקציות המספריות U_n ו V_n של Lucas

זבולון טוכמן ודב ירדן

בנושא הנזכר בכותרת טפל
Edouard Lucas, Théorie des Fonctions Numériques Simplement Périodiques, American Journal of Mathematics 1 (1878), 204-206
וקבל את הנוסחות (62)-('64) המובאות להלן. אכן, הדרך שבה הגיע Lucas לנוסחותיו אינה מסתברת מתוך הרצאתו הקצרה, הלקויה גם בטעויות דפוס. נרצה כאן את הדברים מחדש בהרצאה מפורטת יותר, בשמרנו עד כמה שאפשר על סמוניו של Lucas.

נסמן ב a ו b את שני שרשי המשואה

$$x^2=Px-Q \tag{1}$$

שמקדמיה P ו Q הם מספרים שלמים, חיוביים או שליליים, וראשוניים ביניהם. נתבונן בשתי הפונקציות המספריות U ו V המגדרות על ידי השויונות

$$U_n = (a^n-b^n)/(a-b), \qquad V_n = a^n+b^n. \tag{2}$$

קימות הנוסחות הבאות:

$$U_nV_m = U_{m+n}-Q^nU_{m-n} \tag{52}$$

$$V_mV_n = V_{m+n}+Q^nV_{m-n} \tag{53}$$

$$\Delta U_mU_n = V_{m+n}-Q^nV_{m-n}, \qquad \Delta = (a-b)^2 \tag{53'}$$

$$\sum_{k=0}^{n} V_{m+kr}/Q^{kr/2} = V_{(2m+nr)/2}U_{(n+1)r/2}/Q^{nr/2}U_{r/2} \tag{54}$$

$$\sum_{k=1}^{n} V_{m+kr} = (V_{m+r}+Q^rV_{m+nr}-V_{m+(n+1)r}-Q^rV_m)/(1+Q^r-V_r) \tag{57}$$

בעזרת הנוסחות שלמעלה נוכל להוכיח את הנוסחות הבאות:

$$\Delta\sum_{k=1}^{n} U_{kr}^2/Q^{kr} = (U_{(2n+1)r}/Q^{nr}U_r)-2n-1 \tag{62}$$

$$\Delta\sum_{k=0}^{n-1} U_{(2k+1)r}^2/Q^{(2k+1)r} = (U_{4nr}/Q^{2nr}U_{2r})-2n \tag{62'}$$

$$\sum_{k=1}^{n} V_{kr}^2/Q^{kr} = (U_{(2n+1)r}/Q^{nr}U_r)+2n-1 \tag{63}$$

$$\sum_{k=0}^{n-1} V_{(2k+1)r}^2/Q^{(2k+1)r} = (U_{4nr}/Q^{nr}U_{2r})+2n \tag{63'}$$

$$\Delta\sum_{k=0}^{n} U_{m+kr}^2 = \frac{V_{2m+2(n+1)r}-V_{2m}-Q^{2r}(V_{2m+2nr}-V_{2m-2r})}{V_{2r}-Q^{2r}-1} - 2Q^m\,\frac{Q^{(n+1)r}-1}{Q^r-1} \tag{64}$$

$$\sum_{k=0}^{n} V_{m+kr}^2 = \frac{V_{2m+2(n+1)r}-V_{2m}-Q^{2r}(V_{2m+2nr}-V_{2m-2r})}{V_{2r}-Q^{2r}-1} + 2Q^m\,\frac{Q^{(n+1)r}-1}{Q^r-1} \tag{64'}$$

<u>הוכחת (62).</u> אם נשים ב ('53) m=n=kr, נקבל:

$$\Delta U_{kr}^2=V_{2kr}-Q^{kr}2, \quad \Delta U_{kr}^2/Q^{kr}=(V_{2kr}/Q^{kr})-2, \quad \Delta\sum_{k=1}^{n} U_{kr}^2/Q^{kr}=\sum_{k=1}^{n}(V_{2kr}/Q^{kr})-2n$$

אם נשים ב ('54) (לאחר שנכפילו ב $Q^{-r/2}$) 2r במקום m וכן במקום r, נקבל הלאה:

$$= (V_{(n+1)r}U_{nr}/Q^{nr}U_r)-2n$$

ולפי (52') נקבל

$$= ((U_{(2n+1)r}-Q^{nr}U_r)/Q^{nr}U_r) -2n=(U_{(2n+1)r}/Q^{nr}U_r)-2n-1.$$

<u>הוכחת (62').</u> אם נשים ב (53') $m=n=(2k+1)r$, נקבל:

$$\Delta U^2_{(2k+1)r}=V_{(2k+1)2r}-Q^{(2k+1)r}2,\ \Delta U^2_{(2k+1)r}/Q^{(2k+1)r}=(V_{(2k+1)2r}/Q^{(2k+1)r})-2,$$

$$\Delta \sum_{k=1}^{n} U^2_{(2k+1)r}/Q^{(2k+1)r} = \sum_{k=1}^{n}(V_{(2k+1)2r}/Q^{(2k+1)r})-2n$$

אם נשים ב (54) (לאחר שנכפילו ב $Q^{-r/4}$) $2r$ במקום m ו $4r$ במקום r, נקבל הלאה:

$$= (V_{2nr}U_{2nr}/Q^{2nr}U_{2r})-2n$$

ולפי (52) נקבל:

$$= (U_{4nr}/Q^{2nr}U_{2r})-2n.$$

באפן דומה נקבל את (63) ואת (63') לפי (53), (54) ו (52).

<u>הוכחת (64).</u> אם נשים ב (53') $m+kr$ במקום m ו n, נקבל:

$$\Delta U^2_{m+kr} = V_{2m+2kr}-Q^{m+kr}2,\ \Delta \sum_{k=0}^{n} U^2_{m+kr} = \sum_{k=0}^{n} V_{2m+2kr}-Q^m 2\sum_{k=0}^{n} Q^{kr}$$

ומכאן, בעזרת (57) נקבל, בשימנו $2m$ במקום m ו $2r$ במקום r:

$$= \frac{V_{2m+2r}+Q^{2r}V_{2m+2nr}-V_{2m+2(n+1)r}-Q^{2r}V_{2m}}{1+Q^{2r}-V_{2r}} + V_{2m} - Q^m 2\ \frac{Q^{(n+1)r}-1}{Q^r-1}$$

מכאן, לפי (53) נקבל את (64).

באפן דומה נקבל את (64') לפי (53) ו (57).

סדרות - נסיגה

(המשך מעמוד 21)

דב ירדן

על ידי שטיחת סומציה על נוסחת-הנסיגה, נקבל:

<u>משפט 10.</u>

$$(a_0+\dots+a_s)\sum_{i=1}^{n} W_i=a_1(W_1-W_{n+1})+\dots+a_s(W_1+\dots+W_s-W_{n+1}-\dots-W_{n+s}).$$

בשימנו $n=m$, נקבל ממשפט 10:

<u>משפט 11:</u> סכום השאריות של המחזור מודולו m ב W, בשביל $(m,\ a_0+\dots+a_s)=1$, מתחלק ב m.

<u>משפט 12.</u> מספר הפרודים המסודרים של מספר טבעי n למחוברים $1,2,3,\dots,s$ $(s\geqslant 2)$ הוא $P_n^{(s)}$, באשר

$$P_1^{(s)}=1,P_2^{(s)}=2,P_3^{(s)}=2^2,\dots,P_s^{(s)}=2^{s-1},\quad P_n^{(s)}=P_{n-1}^{(s)}+P_{n-2}^{(s)}+\dots+P_{n-s}^{(s)}\quad (n>s).$$

<u>הוכחה.</u> פרודי $n\geqslant s$ השונים מ s פותחים ב 1 או ב 2 ... או ב s והם מתלכדים אפוא בפרודי $n-1$ אם מחברים להם 1 בראשם או בפרודי $n-2$ אם מחברים להם 2 בראשם... או בפרודי $n-s$ אם מחברים להם s בראשם. מספר פרודי $n>s$ הוא אפוא סכום מספרי הפרודים של $n-1$, $n-2$, ... , $n-s$. הפרודים של $n<s$ למחוברים $1,\dots,s$ מתלכדים בפרודים של n למחוברים $1,\dots,s-1$. קל לבדק אפוא באנדוקציה לפי s כי הפרודים של $1,\dots,s$ (למחוברים $1,\dots,s$) שוים בהתאמה ל $1,2,2^2,\dots,2^{s-1}$ מה שמוכיח את משפטנו.

השוה: תאודור מוצקין. פרודים מסודרים

לוח התחלקות האפסים במחזור מודולו p של סדרת-נסיגה מסדר 3

דב ירדן

הלוח מתיחס לסדרות U, V, $\bar U$, $\bar V$ המגדרות ע"י:

$$U_0=U_1=\bar U_0=\bar U_1=0,\quad U_2=\bar U_2=1,\qquad U_n=U_{n-3}+U_{n-2},\qquad \bar U_n=\bar U_{n-3}-U_{n-2},$$
$$V_0=\bar V_0=3,\quad V_1=\bar V_1=0,\quad V_2=-\bar V_2=2,\qquad V_n=V_{n-3}+V_{n-2},\qquad \bar V_n=\bar V_{n-3}-\bar V_{n-2}.$$

השוה: דב ירדן ואלכסנדר כץ, לוח סדרות-נסיגה לינאריות בינריות מסדר 3, לעיל, 54-55. להלן יצין p מספר ראשוני, P את ארך המחזור מודולו p, N את מספר האפסים במחזור מודולו p, a את הציון הטבעי הראשון שבשבילו U_a, U_{a+1} ($\bar U_a$, $\bar U_{a+1}$) מתחלקים ב p. המחזורים מודולו p של U,V ($\bar U$, $\bar V$) שוים, פרט ל $p=23$ ($p=31$). $a|P$. $V_{p^\alpha}\equiv\bar V_{p^\alpha}\equiv\bar V_{11p^\alpha}\equiv 0 \pmod p$ (α שלם אי-שלילי).
כל מחלק משותף של U_n, U_{n+1} מחלק גם ל U_{kn}, U_{kn+1}, U_{kn+3}, U_{kn-4}, V_{kn+1};
- של $\bar U_n$, $\bar U_{n+1}$ מחלק גם ל $\bar U_{kn}$, $\bar U_{kn+1}$, $\bar U_{kn+3}$, $\bar U_{kn-8}$, $\bar V_{kn+1}$, $\bar V_{kn+11}$;
- של V_n, V_{n+1} מחלק גם ל V_{n+3}, V_{n-5}, V_{n-13}; - של $\bar V_n$, $\bar V_{n+1}$ מחלק גם ל $\bar V_{n+3}$, $\bar V_{n+8}$. האפסים חושבו כאן ע"י חשוב ישיר של המחזורים. בגלל $V_{kp}\equiv V_k \pmod p$ ($\bar V_{kp}\equiv\bar V_k \pmod p$) טוב לכתב את המחזור מודולו p של V ($\bar V$) בעמודות בעלות ארך p. אז מזדהה השורה התחתונה בעמודה השמאלית הראשונה, מה שמאפשר לבדק כל p צעדים אם לא נפלה טעות. בשביל V, עד $p=23$, נתן הלוח ע"י E. Malo, L'interméd. des Math. 7 (1900), 313

p	2		3	5		7		11		13		17		19		23		29		31	
P	7		13	24		48		120		183		288		180		22	506	871		993	
	V	U		V	U	V	U	V	U	V	U	V	U	V	U	V	U	V	U	V	U
N	3		4	5		6	12	11		9	21	17		6	18	1	22	30	31	36	
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2	3	3	5	3	7	3	11	3	13	3	10	3	19	3		3	12	3	31	3
	4	7	9	6	11	17	12	19	28	47	20	14	29	61	22		30	29	79	40	27
			13	8	20	23	16	40	38	62	26	15	82	79	47		36	47	85	44	89
				16	24	33	17	63	46	74	48	17	117	121	56		68	72	100	45	107
						39	19	74	67	108	57	43	141	139	60		83	102	108	47	171
							28	80	90	123	61	96	156		61		94	165	147	71	203
							32	89	101	135	62	131	165		63		142	222	166	133	255
							33	93	107	169	64	155	178		82		202	276	188	151	288
							35	94	116		81	170	186		107		219	296	214	215	318
							44	96	120		87	180	197		116		227	308	241	247	327
							48				109	192	218		120		239	332	294	299	331
											118	200	224		121		258	341	305	332	332
											122	211	241		123		328	345	356	362	334
											123	232	275		142		379	346	366	371	358
											125	238	284		167		389	348	400	375	420
											142	255	288		176		407	424	496	376	438
											148				180		431	430	527	378	502
											170						452	445	538	402	534
											179						493	453	555	464	586
											183						502	492	573	482	619
																	506	511	598	546	649
																		533	628	578	658
																		559	691	630	662
																		586	748	663	663
																		650	802	693	665
																		701	822	702	689
																		711	834	706	751
																		745	858	707	769
																		841	867	709	833
																			871	733	865
																				795	917
																				813	950
																				877	980
																				909	989
																				961	993

ציוני האפסים (קו משורטט בין שני אפסים עוקבים)

p	2		3	5		7		11		13		17		19		23		29		31	
P	7		8	31		57		60		168		288		381		528		840		30	427
	$\bar V$	$\bar U$		$\bar V$	$\bar U$	$\bar V$	$\bar U$	$\bar V$	$\bar U$	$\bar V$	$\bar U$	$\bar V$	$\bar U$	$\bar V$	$\bar U$	$\bar V$	$\bar U$	$\bar V$	$\bar U$	$\bar V$	$\bar U$
N	3			6		9	12	5	6	18		17		27		23		29		3	12
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2	3	3	5	3	7	3	11	3	10	3	11	3	11	3	11	3	11	3	11	3
	4	7	8	11	8	11	8	20	8	11	8	17	8	12	8	23	8	29	8	21	8
				24	12	20	19	24	35	13	21	26	29	14	23	27	39	30	43		92
				25	18	26	20	40	46	18	47	96	64	19	71	90	52	32	59		109
				27	31	30	22		60	31	56	110	68	34	90	91	58	37	159		135
						39	27			57	57	142	81	82	96	93	86	72	172		167
						45	38			66	59	154	105	101	117	98	146	88	184		196
						49	39			67	64	165	115	107	127	129	163	188	204		274
							41			69	77	184	121	128	128	142	181	201	251		313
							46			74	103	185	130	138	130	148	208	213	257		391
							57			87	112	187	200	139	135	176	222	233	268		427
										113	113	192	214	141	150	236	237	280	290		
										122	115	213	246	146	198	253	262	286	305		
										123	120	248	258	161	217	271	335	297	314		
										125	133	252	269	209	223	298	396	319	379		
										130	159	265	288	228	244	312	419	334	383		
										143	168			234	254	327	428	343	417		
														255	255	352	439	408	487		
														265	257	425	449	412	531		
														266	262	486	461	446	606		
														268	277	509	465	516	655		
														273	325	518	528	560	678		
														288	344			635	705		
														336	350			684	746		
														355	371			707	760		
														361	381			734	812		
																		775	822		
																		789	840		

ציוני האפסים (קו משורטט בין שני אפסים עוקבים)

הערות: P מחלק ל p^2+p+1 (כל ה P אי-הזוגיים בלוח) או ל p^2-1, זולת p=23 (p=31). מספר האפסים במחזור מודולו p של V ($\bar V$) אינו עולה על מספר האפסים במחזור מודולו p של U ($\bar U$). אם (כמו בשביל p=31 (p=13, 19)) מספר האפסים במחזורים מודולו p של V, U ($\bar V$, $\bar U$) שוים ואם a<P, שוים מספרי האפסים גם עד ka+1 (ועד בכלל) בשביל כל ka<P. לאיזה מודולים p יש במחזורים של V זוג אפסים עוקבים?

תקונים לכרך 1

ע' 4 בהוכחת משפט 17: $g=\mu^f$. ע' 51 ש' אחרונה: -כמותנה. ע' 52 5 שורות לפני הציור $y_1/y_2=-1$ (ולא: ≢). ע' 53, §4, ש' 5: $|\sum$. ע' 53 קצת אחרי אמצע העמוד: מספיק להראות ש. ע' 86 ש' 6 מלמטה: האות המטושטשת היא b. ע' 87 ש' 18: $=2a+(a,b+c)+b+c$. ע' 88 ש' 13 מלמטה: $x_1=a_1^{-1}$. ע' 90 ש' 5 מלמטה: $a|y_0$. ש' 10 מלמטה: $\sigma_2(y_0|a)$. 11 מלמטה: $\sigma_1(a|y_0)$.

תקונים לכרך 2

ע' 34 במאמר הכללת משפט לנדאו ש' 6: שבה P מספר ממשי חיובי כלשהו שונה מאפס. ע' 44 שנת 1941: H. Gupta. שנת 1943: Lehmer*. סוף שנת 1947:

*מוצקין ת., פירודים מסודרים וציקליים, רבעון למתמטיקה 1, 61-67. ע' 47 ש' 3: פירוש התנאי שהאבר (1) יהיה חפשי מה t ים, ה y ים וה z ים. ע' 54 שורות 5-6: גורם ראשוני של $\bar V_{-62}/2=9803919989$ גדול מ 51721.

ע' 54:

n	U_{-n} פרוק	U_{-n}
56	$2^4.3.43$	−2064
57	19.59	1121
58	13.59	767
59	19.149	−2831
60	$2^4.13.19$	3952
61	$5.7^2.13$	−3185
62	2.3.59	354
63	2.7.257	3598
64	3.7.17.19	−6783

תכן כרך 2

Contents of Volume 2