רבעון למתמטיקה

ללמוד ולמחקר

בעריכת דב ירדן

כרך 1 ירושלים, ניסן תש"ז, אפריל 1947 חוברת 4

תכן

כתבת המערכת: דב ירדן, מלאכי 20, ירושלים

המחיר 200 מיל

פירודים מסודרים וציקליים

תאודור מוצקין

מבוא.

1. תיאור של מספר טבעי n כסכום מחוברים טבעיים (שמספרם יכול להיות גם אחת) יקרא פירוד של n. אם שני סכומים בעלי אותם המחוברים אך בסדר שונה יחשבו לשונים, נדבר על פירודים מסודרים. אך אפשר גם להסתכל בפירודים כשווים, אם הם מתהוים זה מזה על ידי תמורות ידועות המהוות חבורה.

2. אם התמורות האלה הן כל התמורות הציקליות של הפירוד, יקרא הפירוד ציקלי. בפרק א' נבנה נוסחה לספירת הפירודים הציקליים של מספר נתון. בפרקים ב' וג' נספור את הפירודים המסודרים והציקליים שמחובריהם לקוחים מקבוצת-מספרים נתונה.

3. לכל פירוד (מסודר או ציקלי) ישנו פירוד הפוך המתקבל ממנו על-ידי הפיכת סדר המחוברים. אם נסתכל בפירוד ובהפוכו כבפירוד אחד נדבר על פירוד (מסודר או ציקלי) בלי מגמה. מספר הפירודים האלה יתקבל בפרק ד'.

4. פירוד של מספר נתון n נתאר לעצמנו גם כחלוקת קטע בעל n יחידות או, אם הפירוד הוא ציקלי, כחלוקת מעגל המחובר מ n קשתות שוות. הפירוד נתן על ידי זה שמסמנים במיוחד את קצות המחוברים. כך פירוד מסודר בעל i מחוברים נתון על ידי קביעת i-1 קצוות (נקודות-הפרדה) מבין n-1 נקודות מותרות לכך. מכאן, שמספר הפירודים המסודרים של n בעלי i מחוברים הוא $\binom{n-1}{i-1}$. לכן מספר כל הפירודים המסודרים של n הוא $\sum_{i=1}^{n}\binom{n-1}{i-1}=2^{n-1}$.

5. נזכיר עוד, לשם יתר שלמות, מקרים אחרים של חבורות-תמורות במובן הנ"ל. אפשר למשל להרשות בפירוד מסודר להחליף את סדר שנים או שלושה האיברים האחרונים. אם נסמן ב s_2 ו s_3 את מספר הפירודים במובן הזה, קל לקבל כי $s_2=(r_1+r_2-1)/2$ ו $s_3=(r_1+3r_2+2r_3+2r_1^{(2)}+5)/6$, באשר r_k מסמן את מספר הפירודים המסודרים ש k מחובריהם האחרונים שוים זה לזה, ו $r_k^{(i)}$ אותו דבר בתנאי שמספר כל המחוברים שווה ל i.

6. מ $r_1=2^{n-1}$ נובע בלי קושי $r_2=[\frac{2^{n-1}}{3}+\frac{1}{2}]$ ו $r_3=[\frac{2^{n-1}}{7}+\frac{1}{2}]$. $r_1^{(2)}=n-1$ כבר היה לנו. הכנסת ערכים אלו וחשבונות פשוטים מביאים לתוצאות לתוצאות $s_2=[\frac{2^n}{3}]+1$ ו $s_3=[\frac{2^{n+2}}{21}+\frac{n}{3}]+1$.

7. אם מרשים את כל תמורות המחוברים, זאת אומרת אם רוצים לקבל את המספר $s_n(n)$ של כל הפירודים, שגודל מחובריהם עולה באופן מונוטוני במובן הרחב, נכנסים כידוע לפרק קלסי של תורת-המספרים האדיטיבית, שבו שפלו רבים מאז אוילר. אם מרשים רק את התמורות הזוגיות, באים לשאלה המקורבת על מספר הפירודים בעלי מחוברים עולים במובן המצומצם.

א. ספירת הפירודים הציקליים.

8. כדי לקבוע את המספר $z=z(n)$ של פירודים ציקליים של n צריך קודם-כל להתחשב בזה, שפירוד ציקלי בדרך-כלל מתהוה מאותו מספר של פירודים מסודרים כפי שיש בו מחוברים. נקבל אפוא כקירוב ראשון ל z את המספר

$$y=\sum_{i=1}^{n}\binom{n-1}{i-1}/i=\sum_{i=1}^{n}\binom{n}{i}/n=\frac{2^n-1}{n}.$$

9. אך יש גם להתחשב בפירודים ציקליים השייכים לפחות מ i פירודים מסודרים; הם הפירודים המחזוריים ובהם אפשר להסתכל כבפירודים ציקליים של מספר קטן מ n. על-כן יקראו פירודים ציקליים לא-אמיתיים של n.

10. כל פירוד לא-אמיתי הוא פירוד של איזה $\frac{n}{p}$, באשר p הוא גורם ראשוני של n. הוא שייך (לכל-היותר) ל i/p פירודים מסודרים וב $y(n)$ הוה איפוא במקום יחידה רק סך $1/p$. עלינו איפוא להוסיף $(p-1)/p$ בשביל כל פירוד כזה, זאת אומרת, סך-הכל $\sum_{p|n} \frac{p-1}{p} z(\frac{n}{p})$.

11. אולם פירוד ציקלי השייך רק ל n/p^2 הובא לעת-עתה בחשבון רק כ $1/p^2$ (בתוך y) וכ $(p-1)/p$ (על-ידי התיקון שבסעיף הקודם). חסר ליחידה עוד $(p-1)/p^2$ ובהתאם לכך עלינו להוסיף מחוברים מהצורה $\frac{p-1}{p^2} z(\frac{n}{p^2})$.

12. עכשיו נבדוק פירוד השייך ל n/pq, באשר q מספר ראשוני שונה מ p. במקום יחידה קבלנו, לעת-עתה, $\frac{q-1}{q} + \frac{p-1}{p} + \frac{1}{pq}$, זאת אומרת, ב $\frac{p-1}{p} \cdot \frac{q-1}{q}$ יותר מדי ועלינו איפוא לחסר: $\sum \frac{p-1}{p} \cdot \frac{q-1}{q} z(\frac{n}{pq})$, באשר $pq|n$.

13. על-ידי המשך תהליך זה נקבל בסוף נוסחה המביעה את $z(n)$ על-ידי $y(n)$ ועל-ידי מספרים $z(n/t)$ המכופלים במקדמים, התלויים רק ב t. אם נעביר את כל מחוברי התוספת לאגף השני, נוכל לכתוב

$$\sum_{t|n} \sigma(t)\ z(\tfrac{n}{t}) = y(n) \qquad (1)$$

בנוסחה זו $\sigma(1)=1$, לפי מובן התהליך, ובכלל

$$\sum_{t|n} \sigma(t) = \frac{1}{n} \qquad (2)$$

נוסחה זו דומה לקודמת ועלינו להתעכב רגע בדיון כללי בנוסחות כאלו[1].

14. אם נתונות לנו שתי פונקציות σ ו z אילו שהן, המוגדרות בשביל כל מספר טבעי, נוכל תמיד להגדיר על-ידי הנוסחה (1) פונקציה חדשה y הנקראת כידוע מכפלת דיריקלה של σ ו z; נסמנה ב $\sigma{}^\wedge z$. מכפלה זו קומוטטיבית, דיסטריבוטיבית לגבי החיבור ואסוציאטיבית. אם נתונה פונקציה $f=f(n)$ עם $f(1)\neq 0$, יהיה קיים (ובאופן יחיד) גם ההפוך של דיריקלה $f{}^{\wedge -1}$ בעל התכונה $f{}^\wedge f{}^{\wedge -1}=\hat{1}$, באשר $\hat{1}$ היא הפונקציה שערכה 1 בשביל 1 ו 0 בכל מקום אחר. יחד עם כפל זה נשתמש גם בכפל הרגיל, בהפוך הרגיל וב 1 רגיל, שיסמן (בין הפונקציות) פונקציה שערכה 1 בכל מקום.

15. מלבד מכפלת דיריקלה עלינו להזכיר במיוחד את הפונקציות הכפליות. פונקציה $f=f(n)$ נקראת כפלית, אם $f(1)=1$ ואם $f(mn)=f(m)f(n)$ בשביל m ו n זרים זה לזה. לגבי מכפלת דיריקלה מהוות פונקציות אלו חבורה, זאת אומרת מכפלת דיריקלה והפוך דיריקלה של פונקציות כפליות הן גם-כן כפליות. מובן שהן גם חבורה לגבי הכפל הרגיל, אם מתנים $f(n)\neq 0$.

16. אחת הפשוטות בין הפונקציות האלה היא n, זאת אומרת הפונקציה שבשבילה הערך שווה תמיד למקור. כן n^k היא פונקציה כפלית ובשביל $k=0$ ו $k=-\infty$ מקבלים את הפונקציות הנ"ל 1 ו $\hat{1}$. $1^{\wedge -1}$ היא הפונקציה μ של מביוס[2], ו $n{}^\wedge/1=n{}^\wedge\mu$ היא הפונקציה φ של אוילר. $\frac{1}{n}{}^\wedge/1 = \frac{1}{n}{}^\wedge\mu$ היא לפי המשוואה (2) בסעיף 13 הפונקציה σ, מה שנותן לנו עבור הערך של σ את הנוסחה

$$\sigma(\prod p_i^{\alpha_i}) = \prod (1-p_i)/p_i^{\alpha_i}$$

17. קל לאשר את הזהות $fn^k{}^\wedge gn^k=(f{}^\wedge g)n^k$ ומכאן במיוחד $\frac{\varphi}{n}{}^\wedge\sigma = \frac{1}{n}(\varphi{}^\wedge 1{}^\wedge n\mu)=\hat{1}$, זאת אומרת $\sigma{}^{\wedge -1}=\varphi/n$. במקום המשוואה (1) נוכל איפוא לכתוב

$$z = y{}^\wedge\sigma{}^{\wedge -1} = \frac{2^n-1}{n} {}^\wedge \frac{\varphi}{n} = \frac{1}{n}\ (2^n{}^\wedge\varphi) - 1$$

1) ביתר פרוט ראה דב ירדן ותאודור מוצקין, צרוף דירכלה ותורת המספרים, רבעון למתמטיקה 1 (תש"ו, 1946) ע' 1-7.
2) $1{}^{\wedge 2}$ ו $1{}^\wedge n$ הם מספר מחלקי n וסכומם.

או ביתר פירוש

$$z(n) = \frac{1}{n}\sum_{t|n} 2^t \varphi\left(\frac{n}{t}\right) - 1$$

18. כדי לחשב גם את מספר הפירודים האמיתיים בלבד, עלינו לחסר מ $z(n)$ את המספר $z(n/p)$ של אותם הפירודים, שעליהם אפשר להביט גם כעל פירודים ציקליים של n/p, באשר p הוא מספר ראשוני; אבל פירודים השייכים ל n/pq, באשר q הוא מספר ראשוני שונה מ p, חסרנו על-ידי-כך פעמים ועל-כן עלינו להוסיף את מספרם $z(n/pq)$ מחדש, וכן הלאה. מקבלים כך, בעליל, $z\hat{}\mu$, זאת אומרת $y\hat{}\frac{\mu}{n}$, מה ששווה בשביל $n>1$ ל $\frac{1}{n}\sum_{t|n} 2^t \mu(n/t)$.

19. באופן דומה רואים ש $z\hat{}\mu_2$ הוא גם מספר הפירודים הציקליים הזרים, זאת אומרת בעלי מחוברים זרים, וש $z\hat{}\mu\hat{}{}^2$ נותן את מספר הפירודים האמיתיים הזרים[1]. אם נסמן ב μ' פונקציה כפלית השווה ל $-(p+1)$ בשביל p, ל p בשביל p^2 ול 0 בשביל כל חזקה יותר גבוהה של המספר הראשוני p, תשורה התוצאה ל $y\hat{}\frac{\mu'}{n}$ ולכן ל $\frac{1}{n}\sum_{t|n} 2^t \mu'(n/t) - \mu(n)$.

ב. פירודים שמחובריהם לקוחים מקבוצת - מספרים נתונה.

20. אפשר לשאול מהו המספר $u_A(n)$ של אותם הפירודים של מספר טבעי n שכל מחובריהם שייכים לקבוצה נתונה A של מספרים טבעיים. תהי הקבוצה $A=(a_1,a_2,\dots)$, באשר סדר האיברים אינו חשוב ומספרם סופי (≥ 1) או אין-סופי.

21. לכאורה צריך לדרוש שהאיברים $a_1,a_2,\dots$ יהיו שונים ביניהם. אך כדאי לכלול גם את המקרה של איברים שוים אך נתנים להבחנה. זאת אומרת גם אם $a_1=a_2$, צריך להיות ידוע ביחס לכל מחובר של פירוד האם הוא בא כ a_1 או כ a_2. ואולם לא נרשה מציאות של אין-סוף איברים שוים ב A; מכאן שהמערכת (לא "קבוצה") A תהיה לכל היותר נתנת להמנות.

22. כל פירוד קובע את התדירויות, שבהן השתמשו באותו פירוד באיברים $a_1,a_2,\dots$; נסמנם ב $x_1,x_2,\dots$. יהיה איפוא $\sum a_k x_k = n$; מכאן ש $\sum x_k \leq n$ ושמספר ה x ים השונים מ 0 גם הוא $\leq n$.

23. אם נתונים x ים שבשבילם $\sum a_k x_k = n$, נוכל ליצור מהם פירודים כמספר התמורות של $\sum x_k$ עצמים שביניהם $x_1,x_2,\dots$ שוים, זאת אומרת $(\sum x_k)!/\Pi x_k!$ פירודים. אם נסמן את המקדם הפולינומילי הזה ב (x) (קרא: מעל x)[2], נקבל אפוא $u_A(n)=\sum (x)$, באשר הסכום משתרע על כל הצירופים x_k שבשבילם קים $\sum a_k x_k = n$.

24. את הפירודים של n הלקוחים מ A נוכל לחלק למחלקות לפי המחובר הראשון. אם נספור את הפירודים שבכל מחלקה, נקבל את נוסחת-הנסיגה $u_A(u)=\sum_k u_A(n-a_k)$. רואים, מה שגם נובע מהנוסחה בסעיף הקודם, שעלינו לשים $u_A(0)=1$ ו $u_A(n)=0$ בשביל n שלילי. על-פי-זה יש להוסיף יחידה בנוסחת-הנסיגה אם $n=0$, כך שנכתבה:

$$u_A(n) = \sum_k u_A(n-a_k) + 1_{n=0}$$

---

1) פירודים אלו מתאימים לריתמוסים הפרימיטיביים השייכים למחזור n.

2) בשביל A בעל שני איברים נותן איפוא u_A (וכן הנוסחה בסוף סעיף 29) את סכומי המספרים הנמצאים על ישרים מקבילים, החותכים את משולש-פסקל.

25. בשביל מערכת סופית A תכיל נוסחה זו מספר חסום של מחוברים. במקרה זה אפשר גם להגדיר פונקציה $\acute{u}(n)$ המתלכדת ב $u(n)$ בשביל n אי-שלילי והממלאת את נוסחת-הנסיגה בלי תוספת האיבר $1_{n=0}$, זאת אומרת המגדירה סידרת-נסיגה רגילה (של מספרים שלמים, אם A מכיל רק איבר מכסימלי אחד).

26. על סידרות-נסיגה אלו יש כידוע ספרות רחבה עד למאד. במקרה $A=(1,2)$ יתן $\acute{u}_A(n)$ את מספרי פיבונצ׳י שנוהגים לסמנם ב u_{n+1}[1]. סידרות-הנסיגה $u(n)$ וגם הפונקציות הכלליות $\acute{u}(n)$ עולות ממקום ידוע באופן מונוטוני אם לאיברי A אין מחלק משותף; אחרת מופיעים אין-סוף אפסים. רק $\acute{u}_1(n)=1$.

27. אם במערכת A נמצאים לפחות שני איברים, נוכל לגזור ממנה מערכת אחרת $B=(\dots,b_{k,l},\dots)$, באשר $b_{k,l}=a_k+la_1$, $k>1$, $l\geqslant 0$. כל פירוד של n מתוך B יתן גם פירוד של n מתוך A, אם במקום $b_{k,l}$ נכניס את הסכום המגדיר מספר זה. וגם להיפך, נוכל בכל פירוד מתוך A לצרף את המחוברים a_1 למחובר הקודם להם וכך לקבל פירוד מסוים מתוך B, אם הפירוד מתוך A איננו מתחיל ב a_1. כך נקבל את הנוסחה

$$u_B(n) = u_A(n) - u_A(n-a_1)$$

28. נוסחה זו מראה שגם u_B הוא בעל נוסחת-נסיגה חסומה, אם דבר זה נכון לגבי u_A, למשל אם A הוא סופי. מעבר כמו מ A ל B אפשר להוציא לפועל פעמים רצופות. נציין גם את המקרה ש B מכיל את כל המספרים בעלי שאריות נתונות לפי מודולוס נתון.

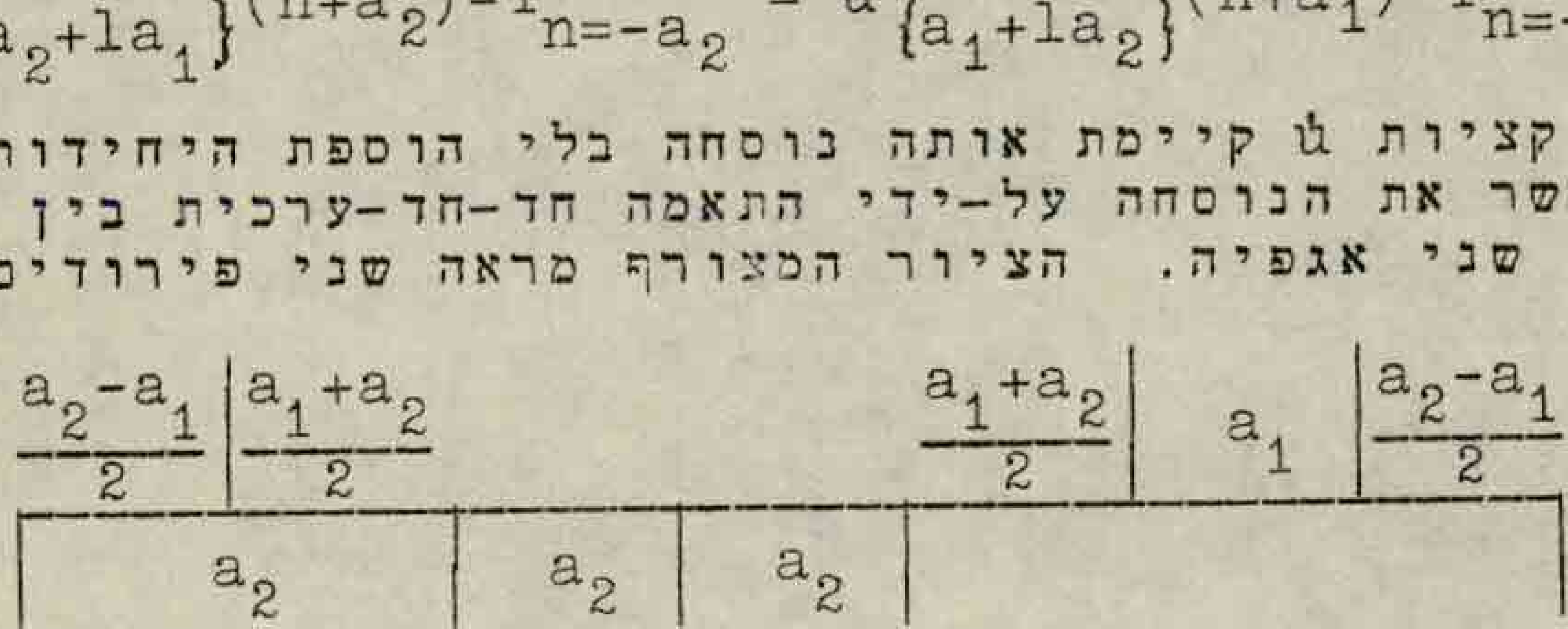
29. אם $A=(a_1,a_2)$, יכיל B את האיברים של סידרה אריתמטית a_2+la_1. יהיה $u_{\{a_2+la_1\}}(n)=u_A(n)-u_A(n-a_1)=u_{a_1,a_2}(n-a_2)+1_{n=0}$, כמו שנובע מהסעיפים 27 ו 24. ה u הימני יכול, לפי סעיף 23, גם להכתב

$$\sum_{a_1x_1+a_2x_2=n} \binom{x_1+x_2-1}{x_1} \quad , \quad x_1\geqslant 0 \quad , \quad x_2\geqslant 1 \; .$$

30. מהסעיף הקודם מקבלים גם נוסחת-סימטריות מעניינת

$$u_{\{a_2+la_1\}}(n+a_2)-1_{n=-a_2} = u_{\{a_1+la_2\}}(n+a_1)-1_{n=-a_1}$$

בשביל הפונקציות $\acute{u}$ קיימת אותה נוסחה בלי הוספת היחידות עם ציונים. אפשר גם לאשר את הנוסחה על-ידי התאמה חד-חד-ערכית בין הפירודים הנמנים בין שני אגפיה. הציור המצורף מראה שני פירודים המתאימים זה לזה:



ג. פירודים ציקליים מתוך קבוצת-מספרים נתונה.

31. אם נחפש את המספר $z_A(n)$ של הפירודים הציקליים של n שמחובריהם לקוחים ממערכת נתונה A, יתקבל קירוב ראשון $y_A(n)$, כמו בסעיף 8, על-ידי חלוק של כל מקדם פולינומילי (x) (בסעיף 23) במספר $\sum x_k$ של מחוברי הפירודים המתאימים. יהיה איפוא $y=\sum_x \frac{(x)}{\sum x_k}$.

32. נסמן ב $x-\mathcal{E}_1$ מערכת השונה מ x רק בזה שמ x_1 (>0) חסרו יחידה. אז

---

1) על מספרים אלו ראה ד. יורז׳ק (ירדן), "תכונות סדרות פבונצ׳י ושימושיהן", ירושלים תשי"א (עבודת-גמר), עם ביבליוגרפיה ספורטת.

ברור כי $(x-\xi_l) = (x)x_l / \sum x_k$. בגלל $\sum_{x_k>0} a_k x_k = n$ יהיה איפוא $\sum a_l (x-\xi_l) = \frac{n(x)}{\sum x_k}$. מכאן $y = \frac{1}{n}\sum_l a_l \sum_x (x-\xi_l)$. הסכום השני לקוח בשביל כל x שבשבילו לא-שליליים איברי $x'=x-\xi_l$ ומתקיים $\sum a_k x_k = n$, זאת אומרת $\sum a_k x'_k = n-a_l$. לכן סכום זה עצמו שווה ל $u_A(n-a_l)$, ו $y = \frac{1}{n}\sum_l a_l u_A(n-a_l)$.

33. נכניס פונקציה חדשה v המוגדרת על-ידי נוסחה דומה לנוסחה שבסעיף 24

$$v_A(n) = \sum_k a_k u_A(n-a_k)$$

בשביל כל n שלם. $y_A(n)$, המוגדר רק בשביל $n>0$, ישווה ל $\frac{1}{n} v_A(n)$.

34. המעבר מקירוב ראשון זה לנוסחה המדויקת נעשה בדיוק באותם השלבים כמו בפרק א' ומתקבלת התוצאה

$$z_A(n) = y\hat{}\sigma\hat{}^{-1} = \frac{1}{n}(v\hat{}\varphi) = \frac{1}{n}\sum_{t|n} v_A(t)\,\varphi\left(\frac{n}{t}\right).$$

35. כמו בסעיף 18 אפשר לקבל את מספר הפירודים האמיתיים כ $z\hat{}\mu$, מה ששווה ל $v\hat{}\mu = \frac{1}{n}\sum_{t|n} v_A(t)\,\mu\left(\frac{n}{t}\right)$. אך אין זה כבר שווה למספר הפירודים הזרים, כי המעבר ליחידה אחרת משנה את גודל המחוברים.

36. ראינו כי $v=ny$ כמו u מתבטא על-ידי מקדמים פולינומיליים. כן הוא מקיים את נוסחת-הנסיגה. כי, לפי 33 ו 24,

$$v_A(n) = \sum_k a_k u_A(n-a_k) = \sum_{k,l} a_k u_A(n-a_k-a_l) + \sum_{a_k=n} a_k = \sum_l v_A(n-a_l) + \sum_{a_k=n} a_k$$

37. בשביל A סופי נוכל גם עתה להגדיר פונקציה נסיגתית ϑ השווה ל v בשביל כל n חיובי. גם עליה חלות ההערות שבסעיפים 25 ו 26. נציין עוד $\vartheta_1(n)=1$, $\vartheta_{1,1}(n)=u_{1,1}(n)=2^n$, $\vartheta_{1,2}(n)=v_n$, באשר ה v_n ים הם המספרים המסומנים כך בדיונים על-דבר מספרי פבונצ'י.

38. גם הפונקציה v נשארת נסיגתית אם במקום v_A מסתכלים ב v_B, באשר v_A היתה נסיגתית והמערכת B נגזרת מ A כמו בסעיף 27. זאת מראה החשבון הבא, אם נניח כידוע כי סכום שתי פונקציות נסיגתיות הוא נסיגתי בעצמו.

39. לפי הגדרת v ו B יהיה $v_B(n) = \sum_{k>1, l\geq 0} (a_k+la_1)u_B(n-a_k-la_1)$.

מכאן, בעזרת 27,

$$v_B(n) = \sum_{l\geq 0}(a_k+la_1)u_A(n-a_k-la_1) - \sum_{l>0} a_k+(l-1)a_1u_A(n-a_k-la_1).$$

אחרי צמצום איברים מתבטלים נקבל

$$v_B(n) = \sum_{k>1} a_k u_A(n-a_k) + \sum_{l>0,k>1} a_1 u_A(n-a_k-la_1)$$

ולכן, לפי הגדרת v ונוסחת-הנסיגה שבסעיף 24,

$$v_B(n) = v_A(n) - a_1u_A(n-a_1) + a_1\sum_{l>0}u_A(n-la_1) - a_1\sum_{l>0}u_A(n-(l+1)a_1) - a_1\cdot 1_{n=la_1}$$

המחוברים האמצעיים מתבטלים והאחרון שווה בעליל ל $v_{a_1}(n)$, כך שמצאנו $v_B(n)=v_A(n)-v_{a_1}(n)$.

40. מהנוסחה האחרונה נובעות בקלות נוסחות דומות בשביל y ו z (לפי 33 ו 34), והן $y_B(n)=y_A(n)-y_{a_1}(n)$ ו $z_B(n)=z_A(n)-z_{a_1}(n)$. אפשר גם לכתבן $y_B(n)=y_A(n)-\frac{1}{n}v_{a_1}(n)$ ו $z_B(n)=z_A(n)-u_{a_1}(n)$. באמת $u_{a_1}(n)$ שווה ל 1 אם n מתחלק ב a_1 ואחרת ל 0, ולכן הקשר שנתנו בין $z_B(n)$ ו $z_A(n)$ הוא המתקבל גם ישר כמו הקשר בין $u_B(n)$ ו $u_A(n)$ לפי ההוכחה שבסעיף 27.

41. מה שנוגע לפונקציה z_B^{μ} (בשביל סעיף 35), רואים בנקל, כי היא שווה ל z_A^{μ}, חוץ מאשר בשביל $n=a_1$ ואז ב 1 פחות. – בשביל $A=(1,1)$, $B=(1,2,3,...)$ מקבלים שוב את התוצאות של פרק א'.

ד. פירודים בלי מגמה.

42. פירוד (מסודר או ציקלי) המתלכד בהיפוכו נקרא סימטרי. מכיון שמספר הפירודים בלי מגמה שווה לממוצע האריתמטי של מספר הפירודים עם מגמה ושל מספר הפירודים הסימטריים, דיינו לחשב את זה האחרון.

43. אם נתאר לנו שוב כל פירוד כחלוקת קטע, יכיל פירוד סימטרי אותם המחוברים בהתחלת הקטע כמו בסופו ורק באמצע יכול להופיע מחובר a_k יחיד שלא בכפילות. אם סכום הפירוד הוא n, אם a_k נתון ואם גם שאר המחוברים צריכים להלקח מתוך המערכת הנתונה A, יהיה איפוא לפרד $n-a_k$ למחוברים $2a_l$. בסמננו את המערכת $(2a_1,2a_2,\dots)$ ב 2A, את מספר הפירודים הסימטריים של n מתוך A ב $\overset{2}{u}_A(n)$ ואת 0 ב a_0, נקבל

$$\overset{2}{u}_A(n)=\sum_{k\geq 0} u_{2A}(n-a_k)$$

44. באופן דומה נחשב את המספר $\overset{2}{z}_A(n)$ של פירודים ציקליים סימטריים. לפירוד כזה מתואר על גבי מעגל יש בודאי מחובר אמצעי a_k או 0 שלגביו הוא סימטרי. יחד עם מחובר כזה מופיע גם מחובר אמצעי נגדי. יכולים להופיע באותו פירוד גם יותר מחוברים אמצעיים.

45. אחרי מחיקת המחובר האמצעי a_k נשאר פירוד מסודר סימטרי של $n-a_k$, השייך למחובר זה. אם לשני מחוברים אמצעיים שייך אותו פירוד, מראה עובדה זו על מציאות מחובר אמצעי נוסף ביניהם. מצד שני, אם מסתכלים בסידור המחוברים האמצעיים על המעגל, רואים שכל אחד שייך לאותו פירוד כמו העוקב לעוקבו.

46. לכן שייכים באופן זה לכל פירוד ציקלי סימטרי של n שני פירודים מסודרים סימטריים של $n-a_k$, $k\geq 0$. מכל אחד מבין האחרונים מקבלים את הפירוד הציקלי באופן חד-ערכי על-ידי הוספת a_k. יהיה איפוא

$$\overset{2}{z}_A(n)=\frac{1}{2}\sum_{k\geq 0}\overset{2}{u}_A(n-a_k)=\frac{1}{2}\sum_{k\geq 0,\,l\geq 0}u_{2A}(n-a_k-a_l).$$

47. קל לחשב את נוסחות-הנסיגה בשביל $\overset{2}{u}$ ו $\overset{2}{z}$. ודהיינו

$$\overset{2}{u}_A(n)=\sum_{k\geq 0}u_{2A}(n-a_k)=\sum_{k\geq 0,\,l>0}u_{2A}(n-a_k-2a_l)+\sum_{k\geq 0}1_{n=a_k}=\sum_{l>0}\overset{2}{u}_A(n-2a_l)+u_A^{(1)}(n),$$

כאשר $u_A^{(i)}(n)$ מסמן את מספר הפירודים בעלי לכל היותר i מחוברים. באותו אופן יהיה

$$.\ \overset{2}{z}_A(n)=\sum_{l>0}\overset{2}{z}_A(n-2a_l)+\frac{1}{2}u_A^{(2)}(n)$$

48. לפונקציות $\overset{2}{u}$ ו $\overset{2}{z}$ יש תכונות דומות לפונקציה u (לא z). הן שלמות

בשביל כל n שלם, רק $\overset{2}{z}_A(0) = \frac{1}{2}$. בשביל A סופי אפשר להגדיר פונקציות נסיגתיות מתאימות $\overset{(2)}{u}$ ו $\overset{(2)}{z}$. נעיר גם כי $\overset{2}{z}^{\wedge}\mu$ נותן את מספר הפירודים הציקליים הסימטריים האפיתיים.

49. המעבר מ A ל B (השווה בסעיפים 27 ו 38) קל בשביל $\overset{2}{u}$. אנו מקבלים, אם נביא בחשבון כי 2B מתיחס ל 2A כמו B ל A,

$$\overset{2}{u}_B(n) = \sum_{k=l=0,\,k>1,\,l\geq 0} u_{2B}(n-a_k-la_1) = \sum u_{2A}(n-a_k-la_1) -$$
$$- \sum u_{2A}(n-a_k-(l+2)a_1) = \sum_{k\neq 1} u_{2A}(n-a_k) +$$
$$+ \sum_{k>1} u_{2A}(n-a_k-a_1) - u_{2A}(n-2a_1) = \overset{2}{u}_A(n) +$$
$$+ \overset{2}{u}_A(n-a_1) - 2u_{2A}(n-a_1) - 2u_{2A}(n-2a_1) .$$

החשבון המתאים בשביל $\overset{2}{z}$ איננו מביא לקשר פשוט.

50. מתוצאות מיוחדות נציין $\overset{2}{u}_{1,1}(n)=2^{[\frac{n+1}{2}]}$, $\overset{2}{z}_{1,1}(n)=2^{[\frac{n}{2}]}+2^{[\frac{n-1}{2}]}$,

$\overset{2}{u}(n) = 2^{[\frac{n}{2}]}$, $\overset{2}{z}(n) = 2^{[\frac{n}{2}]} + 2^{[\frac{n-1}{2}]} -1$, כאשר $n>0$

והעדר הציון התחתון בא במקום $B=(1,2,3,\ldots)$.

הערות נוספות.

51. בנוגע לפונקציות f כמו u_A ו v_A המקיימות נוסחת-נסיגה ביחס למערכת (A) (כפי שהגדרנוה גם אין-סופית) בעלת שני איברים לפחות ובלי מחלק משותף לכל האיברים, אפשר להראות כי היחס $f(n)/f(n-1)$ שואף בשביל $n \longrightarrow +\infty$ לגבול מסוים λ שהוא השורש החיובי של המשוואה $\sum_k \lambda^{a_k} = 1$

52. במקום על פירודי מספר אפשר לשאול על פירודי וקטור טבעי (זאת אומרת, בעל שיעורים אי-שליליים שלא כולם 0) לוקטורים טבעיים. אם יש לבחור את המחוברים האלה מבין העמודות של מטריצה נתונה A, ישווה מספר פירודי הוקטור n ל $\sum_{xA=n} (x)$. אם A היא מטריצת היחידה, מקבלים את המקדמים הפולינומיליים, אך המקרה הכללי כולל פונקציות נסיגתיות של משתנים אחדים; בנוגע לקושי הטיפול בהן מתיחסות פונקציות אלו לפונקציות הנסיגתיות של משתנה אחד כמו המשוואות הדיפרנציאליות החלקיות לרגילות.

תוכן.

הוכחה חדשה למשפט ההדדיות של גאוס

שמואל ביסטריצקי

להוכחה זו הגעתי לפני שנים מספר, ואם כי לא מצאתי דוגמתה בספרות, שמתי אל לב שיש קשר פנימי אמיץ בין הוכחה זו לבין ההוכחה הנתנת למשפט ע"י סכומי גאוס (דהיינו הסכומים $\sum_{\ell=0}^{p-1} e^{2\pi i \ell^2/p}$). אף על פי כן יש ענין בהוכחה כשלעצמה, הואיל ומבחינת שיטתה היא אלמנטרית לגמרי, בעוד שההוכחה בעזרת סכומי גאוס מסתמכת על תכונות שרשי היחידה והפולינום הבלתי פריק השייך להם. – משפט ההדדיות של גאוס, כידוע, נסוחו המתימטי הוא הבא:

<u>משפט 1.</u> יהיו p,q שני מספרים ראשוניים אי-זוגיים שונים. אזי קיים: $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, כאשר $(\frac{a}{p})$, p ראשוני, $a\not\equiv 0(p)$, הוא הסמל הידוע של לג'נדר, דהיינו: $(\frac{a}{p})=1$ אם a הוא שארית רבועית מודולו p ו $(\frac{a}{p})=-1$ אם a הוא אי-שארית רבועית מודולו p. למשפט זה נוהגים לצרף את "משפט התוספת".

<u>משפט 2.</u> יהי p מספר ראשוני אי-זוגי, אזי קיים: $(\frac{2}{p})=(-1)^{(p^2-1)/8}$.

לפני שניגש להוכחת שני המשפטים המנוסחים לעיל נעיר את ההערות הפשוטות הבאות. יהי p מספר ראשוני אי-זוגי. משקולים אלמנטריים ביותר מתקבל ש $p-1$ השאריות מודולו p מתחלקות ל $(p-1)/2$ שאריות רבועיות ול $(p-1)/2$ אי-שאריות רבועיות. ואם $m\not\equiv 0(p)$ כל שהוא, נותן מבחן אוילר לגבי טפוסר הרבועי של m: $(\frac{m}{p})\equiv m^{(p-1)/2} \pmod p$. ל $m\equiv -1(p)$ נקבל מיד: $(\frac{-1}{p})=(-1)^{(p-1)/2}$. דהיינו: $(\frac{-1}{p})=1$ כאשר $p\equiv 1(4)$ ו $(\frac{-1}{p})=-1$ כאשר $p=3(4)$.

לצרכי הוכחתנו נוכיח שני משפטי-עזר.

<u>משפט-עזר 1.</u> יהי q מספר ראשוני. יהי $A=(x_1,\dots,x_q)$, $B=(y_1,\dots,y_q)$, $A=B$ אם $x_i=y_i$, $i=1,2,\dots,q$. על ידי תמורה ציקלית על A נקבל את: $A_k=(x_k.x_{k+1},\dots,x_q,x_1,\dots,x_{k-1})$. אם $1\leqslant k<q$ ואם $A=A_k$, קיים $x_1=x_2=\dots=x_q$.

<u>הוכחה:</u> לכל l שלם נגדיר את x_l ע"י השויון $x_l=x_j$, באשר $1\leqslant j\leqslant q$ ו $l\equiv j(q)$. בעזרת הרחבה זו נוכל לתאר את השויון בין התמורות A ו A_k ע"י השויון: $x_i=x_{i+k}$, i שלם כל שהוא. מכאן נקבל $x_i=x_{i+mk}$, m מספר שלם כל שהוא. הואיל ו $1\leqslant k<q$, q ראשוני, נקבל ש k זר ל q. לכן יש פתרון m_o (i,k קבועים) לקונגרואנציה $i-1+mk\equiv 0(q)$, מכאן נקבל $x_i=x_{1+i-1+m_ok}=x_1$ והשויון האחרון נכון לכל i. מכאן התוצאה.

משפט-העזר השני יטפל בשאלת מספר הפתרונות של הקונגרואנציה

$$x^2-ay^2 \equiv d(p) \qquad (1)$$

כאשר d, $a\not\equiv 0(p)$ קבועים וכאשר $0\leqslant x\leqslant p-1$, $0\leqslant y\leqslant p-1$. קל לראות שמספר זה של פתרונות תלוי רק באופי הרבועי של a ו d. ראשית עלינו להבדיל אפוא בין המקרים $(\frac{a}{p})=1$ ו $(\frac{a}{p})=-1$ וכל אחד משני מקרים אלה מתפצל לשלושת המקרים $d\equiv 0(p)$, $(\frac{d}{p})=1$, $(\frac{d}{p})=-1$.

<u>משפט-עזר 2.</u> אם נסמן ב $u(a)$ את מספר הפתרונות של (1) כאשר $(\frac{d}{p})=1$,

ב $v(a)$ כאשר $(\frac{d}{p})=-1$ וב $w(a)$ כאשר $d\equiv 0(p)$, נקבל: א. אם $(\frac{a}{p})=1$,
$u(a)=v(a)=p-1$, $w(a)=2p-1$. ב. אם $(\frac{a}{p})=-1$, $u(a)=v(a)=p+1$, $w(a)=1$.

<u>הוכחה.</u> מ ק ר ה א. קיים $(\frac{a}{p})=1$. יש אפוא k הממלא $k^2=a(p)$.
לכן נוכל לכתוב את (1) בצורה:

$$x^2-ay^2 \equiv k^2-k^2y^2 \equiv (x-ky)(x+ky) \equiv d(p) \qquad (2)$$

אם $d\not\equiv 0(p)$, נוכל לקבוע את מספר הפתרונות (x,y) ע"י זוג הקונגרואנציות: $x+ky\equiv f(p)$, $x-ky\equiv f'(p)$, כאשר $1\leq f\leq p-1$ ו f' נקבע ע"י $f'f\equiv d(p)$. פתרונות אלה נקבעים באופן חד ערכי לכל f. מכאן: $u(a)=v(a)=p-1$ ל $d\equiv 0(p)$ נוכל לקבל את מספר הפתרונות $w(a)$ מ (2) למשל בדרך הבאה: מספר הפתרונות (x,y) של $x+ky\equiv 0(p)$ הוא p. כן מספר הפתרונות של $x-ky\equiv 0(p)$ הוא p. מזה עלינו לנכות פעם אחת את הפתרון $(0,0)$ המשותף ל $x+ky\equiv 0(p)$ ול $x-ky\equiv 0(p)$. בסה"כ נקבל: $w(a)=2p-1$.

מ ק ר ה ב. $(\frac{a}{p})=-1$. רואים מיד שלקונגרואנציה (1) כאשר $d\equiv 0(p)$ יש הפתרון היחיד $(0,0)$ לכן: $w(a)=1$. כאשר $d\not\equiv 0(p)$ ו $(\frac{d}{p})=1$ יש ל (1) זוג פתרונות שבהם $y\equiv 0(p)$. יהי (x,y) פתרון השונה מהזוג האמור, $y\not\equiv 0$. יש אפוא y' הממלא $y'y\equiv 1(p)$. ע"י כפל של (1) ב y'^2 וסדור האגפים נקבל:

$$x_1^2-dy_1^2 \equiv a(p) \qquad (3)$$

כאשר $1\leq y_1\leq p-1$, $0\leq x_1\leq p-1$ ו $y_1\equiv y'(p)$, $x_1\equiv xy'(p)$. ולהפך, כל פתרון של (3) מקיים בהכרח $y\not\equiv 0(p)$ ולו מתאים ע"י הטרנספורמציה ההפוכה פתרון יחיד של (1) עם $y\not\equiv 0(p)$. אולם הקונגרואנציה (3) (הואיל ו $(\frac{d}{p})=1$) היא טפוס שטפלנו בו בחלק א של משפט-העזר, מכאן: $u(a)=v(d)+2=p-1+2=p+1$. כדי לחשב את $v(a)$ נשתמש בנוסחת הקשר:

$$[u(a)+v(a)]\frac{p-1}{2} + w(a) = p^2 \qquad (4)$$

האגף השמאלי ב (4) מבטא את המספר הכללי של פתרונות של (1) ל $0\leq d\leq p-1$. אולם מספר זה כולל את כל הזוגות (x,y) שמספרם הוא p^2. מכאן השויון (4). אם נציב עכשיו $u(a)=p+1$, $w(a)=1$, נקבל: $v(a)=u(a)=p+1$, מש"ל.

בשלב זה נוכל כבר להוכיח את משפט 2, משפט התוספת, דהיינו שקיים: $(\frac{2}{p})=(-1)^{(p^2-1)/8}$.

<u>הוכחה:</u> בקונגרואנציה (1) נבחר $a=-1$. אם קיים (א) $(\frac{2}{p})=1$, נסתכל בפתרונות של $x^2+y^2\equiv d(p)$ כאשר $(\frac{d}{p})=-1$. מספרם הוא $v(-1)$, ולפי משפט-עזר 2, $v(-1)=p\pm 1$ (כפי שרואים בנקל: $p-1$, אם $p\equiv 1(4)$ ו $p+1$, אם $p\equiv 3(4)$). פתרון כזה (x,y) מקיים גם (א) $xy\not\equiv 0(p)$. כי אם למשל $y\equiv 0(p)$ תתקבל הסתירה $(\frac{d}{q})=1$ וכו'. (ב) $x\not\equiv y(p)$. כי אם $x\equiv y$ תתקבל הסתירה $1=(\frac{2}{p})=(\frac{d}{p})=-1$. נוכל אפוא לערוך את הפתרונות בקבוצות בנות שמונה אברים. בכל קבוצה יהיו הפתרונות השונים המתקבלים מ (x,y) ע"י שנויי הסימן והסדר (דהיינו: $(x,y),\dots,(p-x,y),\dots,(y,x)$ וכו'). נובע מכאן $v(-1)=p\pm 1\equiv 0(8)$, דהיינו: $p\equiv \pm 1(8)$. אם קיים (ב) $(\frac{2}{p})=-1$, נתבונן בקונגרואנציה $x^2+y^2\equiv d(p)$ כאשר $(\frac{d}{p})=1$. אף מספר פתרונותיה הוא: $u(-1)=p\pm 1$. כי אם (x,y) הוא פתרון, גם כאן כמו במקרה הקודם $x\not\equiv y(p)$. אולם במקרה זה יש לקונגרואנציה האחרונה זוג פתרונות מהטפוס $(x,0)$ וזוג פתרונות מהטפוס $(0,y)$. אם נוציא ארבעה פתרונות אלה, נוכל שוב לערוך את שאר הפתרונות, ע"י שנויי הסימן והסדר, בקבוצות בנות שמונה אברים. נקבל מכאן: $u(-1)-4=p\pm 1-4\equiv 0(8)$ ומכאן נובע: $p\equiv 4\pm 1(8)$. הואיל וארבעת המקרים ב (א) ו (ב) הם שונים ומכילים את כל האפשרויות, נקבל את התוצאה המנוסחת במשפט.

כדי להוכיח את משפט ההדדיות נטפל במספר הפתרונות של הקונגרואנציה הכללית:

$$x_1^2+x_2^2+\dots+x_m^2 \equiv d \pmod p \tag{5}$$

כאשר $2\leq m$, $0\leq x_i\leq p-1$. גם כאן רואים בקלות שמספר הפתרונות הנ"ל תלוי רק באופי הרבועי של d. נגדיר אפוא $Z(m)$ כמספר הפתרונות של (5) כאשר $d\equiv 0(p)$, $R(m)$ כאשר $(\frac{d}{p})=1$, $N(m)$ כאשר $(\frac{d}{p})=-1$. ברור שכאשר $m=2$ קיים: $Z(2)=w(-1)$, $N(2)=v(-1)$, $R(2)=u(-1)$. כמו כן קיימות נוסחאות הנסיגה הבאות בין $2\leq m$ ל $m+1$.

$$R(m+1) = 2Z(m) + \frac{R(m)}{2}(u(-1)-2) + \frac{N(m)}{2}(u(-n)-2)$$

$$\left\{\begin{aligned} N(m+1) &= \frac{R(m)}{2}v(-1) + \frac{N(m)}{2}v(-n) \\ Z(m+1) &= Z(m) + (p-1)S(m) \end{aligned}\right. \tag{6}$$

אם נגדיר $S(m)=R(m)$ כאשר $p\equiv 1(4)$; $S(m)=N(m)$ כאשר $p\equiv 3(4)$.
כמו כן נגדיר: $T(m)=N(m)$, $p\equiv 1(4)$; $T(m)=R(m)$ כאשר $p\equiv 3(4)$.
ל u,v יש המובן של משפט-עזר 2. n הוא אי-שארית רבועית מסוימת: $(\frac{n}{p})=-1$.
כמו כן קיימת נוסחת הקשר:

$$\left\{R(m)+N(m)\right\}\frac{p-1}{2} + Z(m) = p^m \tag{7}$$

כדאי להעיר שע"י בדיקה פשוטה מתאשרות (6) ו (7) גם במקרה $m=1$.

הנוסחאות (6) מתקבלות באופן פשוט ביותר. נראה למשל איך מתקבלת הנוסחה הראשונה ב (6). יהי אפוא d שארית רבועית. נחשב את מספר הפתרונות של

$$x_1^2+x_2^2+\dots+x_{n+1}^2 \equiv d(p) \tag{8}$$

נעתיק את (8) בצורה $x_{m+1}^2+Q(x_1,\dots,x_m)\equiv d(p)$, כאשר Q הוא סכום m הרבועים הראשונים. את הפתרונות $(x_1,x_2,\dots,x_{m+1})$ של (8) נחלק לשלוש מחלקות שסכומן יתן לנו את מספר הפתרונות הכללי. (א) המחלקה הראשונה בה מתמלא $Q\equiv 0(p)$. לקונגרואנציה האחרונה יש $Z(m)$ פתרונות. לכל הפתרונות של $Q\equiv 0(p)$ מתאימים אנו שני x_{m+1} הממלאים $x_{m+1}^2\equiv d(p)$. לכן תתרום מחלקה זו $2Z(m)$ פתרונות. (ב) המחלקה השניה בה מתמלא $(\frac{Q}{p})=1$. אולם לכל שארית רבועית r יש ל $Q\equiv r(p)$ $R(m)$ פתרונות. מכאן מקבלים אנו שבמחלקה הזאת עוברים ה Q-ים $\frac{R(m)}{2}$ פעמים (קל לראות ש $R(m)$ זוגי) את כל הרבועים x^2 מודולו p. כאשר $1\leq x\leq p-1$ נקבל אפוא בסה"כ שבמחלקה זו נמצאים $\frac{R(m)}{2}$ פעמים מספר הפתרונות של $x_{m+1}^2+x^2\equiv d(p)$ (כאשר $0\leq x_1\leq p-1$, $1\leq x\leq p-1$) אברים. אולם לקונגרואנציה האחרונה יש לפי משפט-עזר 2, כנקל לראות, $u(-1)-2$ פתרונות. תרומת המחלקה (ב) למספר הפתרונות הכללי היא אפוא $\frac{R(m)}{2}(u(-1)-2)$.

(ג) כאן יכנסו הפתרונות הממלאים $(\frac{Q}{p})=-1$. דוגמת (ב) נסיק בקלות שמחלקה זו תורמת $\frac{N(m)}{2}(u(-n)-2)$ פתרונות. סכום הפתרונות של שלוש המחלקות יביאנו לנוסחה הראשונה ב (6). שתי הנוסחאות האחרות ב (6) מתקבלות באופן דומה. אשר לנוסחת הקשר (7), דוגמת הנוסחה (4), הרי האגף השמאלי נותן לנו את מספר הפתרונות הכללי של (5) ל-$d=0,1,\dots,p-1$, אולם מספר זה נותן לנו את כל הקומפלכסים האפשריים $(x_1,x_2,\dots,x_m)$ כאשר $0\leq x_i\leq p-1$, אולם מספר אלה הוא p^m. מכאן הנוסחה.

בהתחשב עם (6), (7), עם $u(a)$, $v(a)$ כפי שהם מופיעים במשפט-עזר 2 ובהתחשב עם הגדרות $S(m)$, $T(m)$, נקבל את הנוסחאות (9):

(9) $R(m+1)=p^{m}+Z(m)-S(m),\ N(m+1)=p^{m}-Z(m)+T(m),\ Z(m+1)=Z(m)+(p-1)S(m)$

ע"י שימוש פעמיים ב (9) ושימוש ב (7) לפי הצורך, נקבל את הנוסחאות (10) ו (11) במקרים:

(א) $p\equiv 1(4)$

(10) $R(m+2)=p^{m+1}-p^{m}+pR(m),\ N(m+2)=p^{m+1}-p^{m}+pN(m),\ Z(m+2)=p^{m+1}-p^{m}+pZ(m)$

(ב) $p\equiv 3(4)$

(11) $R(m+2)=p^{m+1}+p^{m}-pR(m),\ N(m+2)=p^{m+1}+p^{m}-pN(m),\ Z(m+2)=p^{m+1}+p^{m}-pZ(m)$

אם נשתמש עכשיו בעובדה $R(1)=2$, $N(1)=0$, $Z(1)=1$, נקבל בקלות מנוסחאות הנסיגה האחרונות ל q אי-זוגי:

(א) $p\equiv 1(4)$

(12) $R(q)=p^{q-1}+p^{(q-1)/2},\ N(q)=p^{q-1}-p^{(q-1)/2},\ Z(q)=p^{q-1}$

(ב) $p\equiv 3(4)$

(13) $R(q)=p^{q-1}+(-1)^{(q-1)/2}p^{(q-1)/2},\ N(q)=p^{q-1}-(-1)^{(q-1)/2}p^{(q-1)/2},\ Z(q)=p^{q-1}$

בעזרת הנוסחאות (12) ו (13) נוכל להוכיח עכשיו את משפט 1, משפט ההדדיות של גאוס, האומר: אם p,q הם שני מספרים ראשוניים אי-זוגיים שונים, קיים $(\frac{p}{q})(\frac{q}{p})=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

<u>הוכחה:</u> אם אחד לפחות מבין p,q הוא מהצורה $4c+1$, נוכל, מטעמי סימטריות, להניח ש $p\equiv 1(4)$. אם $(\frac{q}{p})=1$, נתבונן במספר הפתרונות של

$$x_1^2+x_2^2+\dots+x_q^2\equiv d(p) \qquad (14)$$

כאשר $(\frac{d}{p})=-1$. מספר פתרונות אלה הוא $N(q)$. כל תמורה ציקלית של פתרון כזה עם k המופיע במשפט-עזר 1 המקיים $0\leq k\leq q-1$ אף היא פתרון. שתי תמורות שונות נותנות פתרונות שונים. כי משויון התמורות, לפי משפט-עזר 1, היה נובע: $x_1=x_2=\dots=x_q$ ומכאן: $qx_1^2=d(p)$, מה שהיה מביא לסתירה: $-1=(\frac{d}{p})=(\frac{q}{p})=1$. לכן נוכל לערוך את כל הפתרונות $N(q)$ במחלקות בנות q אברים כל אחת. מכאן נקבל: $N(q)\equiv 0(q)$ אולם מ (12) נסיק: $p^{(q-1)/2}(p^{(q-1)/2}-1)\equiv 0(q)$. מכאן נקבל: $p^{(q-1)/2}\equiv 1(q)$. אולם לפי מבחן אוילר פירוש השויון האחרון הוא ש $(\frac{p}{q})=1$. לכן קיבלנו במקרה זה את המסקנה הדרושה: $(\frac{p}{q})=1=(\frac{q}{p})$.

אם $(\frac{q}{p})=-1$ נתבונן באופן דומה במספר הפתרונות $R(q)$ של (14) כאשר $(\frac{d}{p})=1$. גם כאן נקבל: $R(q)\equiv 0(q)$ ולפי (12) נקבל: $p^{(q-1)/2}(p^{(q-1)/2}+1)\equiv 0(q)$, ז"א: $p^{(q-1)/2}\equiv -1(q)$ ומכאן שוב לפי מבחן אוילר $(\frac{p}{q})=-1$. קיבלנו שוב $(\frac{p}{q})=-1=(\frac{q}{p})$. קיבלנו בסה"כ כאשר $\frac{p-1}{2}\cdot\frac{q-1}{2}\equiv 0(2)$ את התוצאה: $(\frac{p}{q})(\frac{q}{p})=1=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

נשאר עוד המקרה שגם p וגם q הם מהצורה $4c+3$. כאן אפשר יהיה לכתוב את משפט ההדדיות בצורה $(\frac{p}{q})=-(\frac{q}{p})$. את ההוכחה של חלק זה נקבל מ (13) בהתחשב עם $(-1)^{(q-1)/2}=-1$. אם $(\frac{q}{p})=1$, נתבונן ב (14) כאשר $(\frac{d}{p})=-1$. נקבל כמו במקרים הקודמים $N(q)\equiv 0(q)$. אולם מ (13) נקבל: $p^{(q-1)/2}(p^{q-1}+1)\equiv 0(q)$, ז"א $p^{(q-1)/2}\equiv -1(q)$, לכן: $(\frac{p}{q})=-1=-(\frac{q}{p})$. אם $(\frac{q}{p})=-1$, נתבונן ב (14) כאשר $(\frac{d}{p})=1$. נקבל שוב: $R(q)\equiv 0(q)$. ומ (13) נקבל: $p^{(q-1)/2}(p^{(q-1)/2}-1)\equiv 0(q)$, לכן $p^{(q-1)/2}\equiv 1(q)$, ז"א: $(\frac{p}{q})=1=-(\frac{q}{p})$. ובזאת הושלמה הוכחת משפט ההדדיות.

על הכדורים המשיקים לארבעה כדורים נתונים

שמואל שריבר

ידועה לנו מן הזמן העתיק השאלה שהציג אפולוניוס: למצא את כל המעגלים המשיקים לשלשה מעגלים נתונים במישור. שאלה זו נתנה דחיפה למחקרים רבים בגיאומטריה של המעגלים, ובמחצית הראשונה של המאה הקודמת טופל בה הרבה ביחוד באסכולותיהם של מונג' (Monge) ומביוס (Möbius). יש לציין שבתקופה ההיא החלה הגיאומטריה של המעגל והכדור להתפתח באופן יותר ויותר עצמאי, ואף הסימונים שוכללו באופן שהקל על חקר השאלות בתחום זה.

בכדי לרמוז על התפתחות הסימון והנוחיות שזו הביאה בעקבותיה, אביא כאן בקצרה את ענין השיעורים הפנטספריים שהוכנסו לספרות במחצית הראשונה של המאה הקודמת.

תהי נתונה נקודה P וכדור S. החזקה של P לגבי S היא כידוע הריבוע של אורך המשיק מ P אל S. נסמן את החזקה באות H ואת רדיוס הכדור S ב r (יש כאן חופש בחירה בנוגע לסימנו של r), ואז נקרא לגודל $\rho=H/r$ החזקה המצומצמת של P לגבי S. - נבחר לנו כעת במרחב חמשה כדורים S_1, S_2, S_3, S_4, S_5 מאונכים זה לזה (אגב, את זאת נוכל להגשים רק בעזרת 4 כדורים ממשיים וכדור חמישי בעל מרכז ממשי ורדיוס מדומה טהור), ותהיינה p_1, p_2, p_3, p_4, p_5 החזקות המצומצמות של נקודה P כלשהי לגבי חמשת הכדורים. מוכיחים שחמשת הגדלים p_i (שאחד מהם הוא מדומה טהור) מקימים את הזהות:

$$(pp) \equiv \sum_{1}^{5} p_i^2 = 0 \tag{1}$$

נוכל לראות את כל החמישיות המתכונתיות של מספרים p_i המקימים את הזהות (1) בתור שיעורים הומוגניים של נקודה במרחב ולקרא להן השיעורים הפנטספריים של הנקודה. - יהיו כעת q_i, $1\leqslant i\leqslant 5$, חמשה מספרים כלשהם, אז אפשר להוכיח על נקלה שהמשואה

$$(qp) \equiv \sum_{1}^{5} q_i p_i = 0 \tag{2}$$

היא המשואה הכללית של כדור בשיעורים פנטספריים. נוכל, יתר על כן, לראות כל חמשיה של מספרים המתכונתיים ל q_i בתור שיעורים הומוגניים של כדור Q. - מוכיחים, שאם שני הכדורים Q,R נפגשים בזוית φ, מתקים

$$\cos\varphi = (qr)/[\sqrt{(qq)}\sqrt{(rr)}] \tag{3}$$

במיוחד, בכדי ששני כדורים Q,R יהיו מאונכים, דרוש ומספיק

$$(qr) = 0 \tag{3'}$$

(תנאי בילינארי בשיעורים; אנלוגיה לוקטורים מאונכים, בסימון הרגיל!). ע"ס זה אפשר להגיד שכדור, אשר שיעוריו מקימים את השויון

$$(qq) = 0 \tag{3''}$$

הוא מאונך לעצמו, אולם התנאי הזה הוא בדיוק אותו שהצגנו לחמישית מספרים בכדי שתהוה מערכת שיעורים פנטספריים של נקודה (1). יוצא שמוצדק לקרא לנקודה בשם כדור המאונך לעצמו. - אם P נקודה ו Q כדור, רואים שהמשואה (2) מתארת את התנאי בכדי שהנקודה P תמצא על הכדור Q, אך גם את התנאי שה"כדור" P יהיה מאונך לכדור Q, ומכאן ששני התנאים הנ"ל מזדהים. - בעזרת הכתיב המתואר לעיל ובעזרת זהויות שונות בין דטרמיננטות (החשובה ביניהן - זהותו של קליפורד (Clifford)) הביא קולידג' (Coolidge) פתרון אלגנטי ביותר לאנלוגון של שאלת אפולוניוס: למצא את כל הכדורים המשיקים לארבעה כדורים נתונים (ראה, למשל, בספרו A History of Geometrical Method, p.168f.). אולם, על אף היופי והכלליות שבשיטת הפתרון של קולידג', שלא אפרט אותה כאן, הרי הביטויים המופיעים בפתרון הם מכפלות דטרמיננטות די מסובכות וביטויים אירציונליים רבים התלויים בשיעורי ארבעת הכדורים הנתונים, ולכן חשבתי לנכון להביא לפני הקורא שיטה יותר אלמנטרית של פתרון השאלה.

יהיו נתונים ארבעה כדורים ע"י משואותיהם הקרטזיות הרגילות

(4) $$S_\nu \equiv (\xi-x_\nu)^2+(\eta-y_\nu)^2+(\zeta-z_\nu)^2 = r_\nu^2\ , \qquad 1\leq\nu\leq 4$$

לפי משפטים ידועים בגיאומטריה אנליטית יש לפחות נקודה אחת (ובדרך כלל רק אחת) אשר החזקות שלה לגבי כל אחד מארבעת הכדורים שוות. נקודה זו היא, אגב, מרכז הכדור המאונך לארבעת הכדורים הנתונים. אם ישנה רק נקודה אחת כזאת, נסמן אותה ב 0 ונבחין בין שני מקרים: I. 0 נקודה סופית; II. 0 נמצאת באין-סוף. הבחנה זו היא לשם נוחיות בלבד, כי מבחינת הגיאומטריה של הכדורים אין הבדל עקרוני בין שני המקרים.

I. נעביר את ראשית הצירים לנקודה 0. המשואות (4) תקבלנה את הצורה

(4') $$S_\nu \equiv \xi^2+\eta^2+\zeta^2-2\xi x_\nu-2\eta y_\nu-2\zeta z_\nu+Q=0$$

(4") באשר $$Q = x_\nu^2+y_\nu^2+z_\nu^2-r_\nu^2$$

באופן בלתי תלוי ב ν, מאחר שהצד הימני של (4") מסמן את חזקת ראשית הצירים כלפי הכדור S_ν. יהי כעת S כדור המשיק לכל אחד מארבעת הכדורים S_ν,

(5) $$(\xi-x)^2+(\eta-y)^2+(\zeta-z)^2-r^2=0$$

אזי צריך להתקיים

(6) $$(x-x_\nu)^2+(y-y_\nu)^2+(z-z_\nu)^2=(r-\varepsilon_\nu r_\nu)^2,\ \varepsilon_\nu=\pm1$$

או, אם נשים לשם סימטריה $s=ir,\ s_\nu=ir$:

(6') $$(x-x_\nu)^2+(y-y_\nu)^2+(z-z_\nu)^2+(s-\varepsilon_\nu s_\nu)^2=0$$

וביתר פרוטרוט

(6") $$x^2+y^2+z^2+s^2-2xx_\nu-2yy_\nu-2zz_\nu-2s\varepsilon_\nu s_\nu+Q=0$$

לפנינו אפוא 4 משואות ריבועיות עם 4 נעלמים. נשים

(7) $$x^2+y^2+z^2+s^2=P$$

ונניח לרגע ש P הוא גודל ידוע. המשואות (6") עוברות עתה לצורה הבאה

(8) $$x_\nu x+y_\nu y+z_\nu z+\varepsilon_\nu s\ s = \tfrac{1}{2}(P+Q)$$

נסתכל כעת במטריצה שארבע שורותיה הן

(9) $$|1,x_\nu,y_\nu,z_\nu,\varepsilon_\nu s_\nu|$$

ונסמן את הדטרמיננטות המתקבלות ע"י מחיקת העמודות של (9) החל מהשמאלית וכלה בימנית ב a,b,c,d,e. רואים על נקלה שהפתרונות של המשואות (8) נתונים ע"י הביטויים הבאים:

(10) $$x = (P+Q)\frac{b}{2a}\ ,\ y = (P+Q)\frac{-c}{2a}\ ,\ z = (P+Q)\frac{d}{2a}\ ,\ s = (P+Q)\frac{-e}{2a}$$

עלינו כעת למלא את התנאי (7), הנותן

(11) $$(P+Q)^2(b^2+c^2+d^2+e^2)-4a^2(P+Q)+4a^2Q = 0$$

(12) ומכאן $$\tfrac{1}{2}(P+Q)=(b^2+c^2+d^2+e^2)^{-1}\left[a^2\pm a\sqrt{a^2-Q(b^2+c^2+d^2+e^2)}\right]$$

(10) ו (12) נותנות את מרכז הכדור המבוקש ואת הרדיוס שלו. רואים שלכל בחירה של רביעיה ε_ν נקבל שני פתרונות, ולכן ישנם לכאורה 2.16=32 פתרונות לשאלה. אולם אפשר לראות מתוך המשואות (6), למשל, שאם x,y,z,r היו פתרון למערכת אחת של ε_ν, אזי x,y,z,-r, ז.א. נתוני אותו הכדור, יתאימו למערכת ε_ν מוכפלת ב 1-. <u>ישנם אפוא 16 כדורים, המשיקים לארבעת הכדורים הנתונים.</u>

II. הנקודה 0 באין סוף, ז.א. קים כדור בעל מרכז באין-סוף ורדיוס אינסופי המאונך לארבעת הכדורים שלנו או, במלים אחרות, מרכזי ארבעת הכדורים נמצאים במישור אחד. נקח את המישור הזה בתור z=0 ואת ראשית הצירים במקום כלשהו עליו. המשואות (4) תהיינה במקרה זה

(13) $$\xi^2+\eta^2+\zeta^2-2\xi x_\nu-2\eta y_\nu+Q_\nu = 0$$

(13') באשר $$Q_\nu = x_\nu^2+y_\nu^2-r_\nu^2$$

Q_v יהיה הפעם תלוי ב v. יהי שוב הכדור (5) משיק לארבעת הכדורים S_v, אזי צריך להתקיים, בדומה ל ("6) לעיל

$$x^2+y^2+z^2+s^2-2xx_v-2yy_v-2s\varepsilon_v s_v+Q_v=0 \tag{14}$$

או, בעזרת (7),

$$P-2x_vx-2y_vy-2\varepsilon_v s_v s=-Q_v. \tag{14'}$$

יש לנו ארבע משואות ליניאריות לארבעת הנעלמים x,y,s,P ורואים גם באופן הסתכלותי שהגדלים האלה מופיעים באופן חד-ערכי, מכיון שהפתרונות סימטריים כלפי המישור $z=0$. נסתכל כעת במטריצה

$$|Q_v,1,-2x_v,-2y_v,-2\varepsilon_v s_v| \tag{15}$$

ונסמן שוב את הדטרמיננטות* המתקבלות ממנה ע"י מחיקת עמודות משמאל לימין ע"י a,b,c,d,e. נקבל את פתרונות (14') בצורה

$$P=b/a\ ,\ x=-c/a\ ,\ y=d/a\ ,\ s=-e/a \tag{16}$$

ומכאן לפי (7):

$$z=\pm\sqrt{ab-c^2-d^2-e^2}/a \tag{17}$$

לא אפרט כאן את החישובים למקרה שיש אין-סוף נקודות בעלות חזקה שוה כלפי כל ארבעת הכדורים (למשל אם שנים מן הכדורים מתלכדים). אפשר אז לבחור מערכת ε_v כאלה, שהשורות של המטריצה (9) או (15) תהיינה תלויות. אחרי בחירה כזו ישנם גם אין-סוף כדורים המשיקים לארבעת הכדורים שלנו, והכדורים הללו עוטפים משטח הנקרא בשם ציקלידה של דיפן (Dupin).

קשר בין סכומי חזקות מסדר 3

דב ירדן

ידוע, כי בסדרה $v_0=2,\ v_1=1,\ \dots,\ v_n=v_{n-1}+v_{n-2},\dots$ קים $v_n^2-v_{2n}=(-1)^n2$. v_n הוא סכום החזקות ה n-יות של שרשי המשואה $x^2-x-1=0$. אפשר להוכיח בנקל כי קים ביתר כלליות: $S_n^2-S_{2n}=2(a_2/a_0)^n$, באשר S_n הוא סכום החזקות ה n-יות של שרשי המשואה $a_0x^2+a_1x+a_2=0,\ (a_0a_2\neq0)$. ברשימה הנוכחית יש ברצוני להביא נוסחה אנלוגית לסכומי חזקות מסדר 3.

<u>משפט.</u> לכל n שלם קים

$$S_n^2-S_{2n}=2\bar{S}_n,$$

באשר S_n הוא סכום החזקות ה n-יות של שרשי המשואה ממעלה 3

$$a_0x^3+a_1x^2+a_2x+a_3=0,\qquad (a_0a_3\neq0) \tag{1}$$

ו $\bar{S}_n$ הוא סכום החזקות ה n-יות של שרשי המשואה ממעלה 3

$$a_0^2X^3-a_0a_2X^2+a_1a_3X-a_3^2=0 \tag{2}$$

בפרט, אם $a_0=-ra_3$, יהיה תמיד $\bar{S}_n=r^{-n}S_{-n}$. אם $a_0=-a_3$, יהיה תמיד $\bar{S}_n=S_{-n}$.

<u>הוכחה.</u> אם x_1,x_2,x_3 הם שרשי המשואה (1), יהיה:

$$S_n^2-S_{2n}=(x_1^n+x_2^n+x_3^n)^2-(x_1^{2n}+x_2^{2n}+x_3^{2n})=2((x_1x_2)^n+(x_1x_3)^n+(x_2x_3)^n)=2\bar{S}_n,$$

באשר $(\bar{S}_n)$ היא סדרת סכומי חזקות מסדר 3 ששרשי משואתה הם:

$$X_1=x_1x_2,\ X_2=x_1x_3,\ X_3=x_2x_3$$

למשואה ישנה אפוא הצורה

$$A_0X^3+A_1X^2+A_2X+A_3=0,\qquad (A_0A_3\neq0),$$

באשר

$$-A_1/A_0=X_1+X_2+X_3=x_1x_2+x_1x_3+x_2x_3=a_2/a_0,$$
$$A_2/A_0=X_1X_2+X_1X_3+X_2X_3=(x_1+x_2+x_3)x_1x_2x_3=a_1a_3/a_0^2,$$
$$-A_3/A_0=X_1X_2X_3=(x_1x_2x_3)^2=a_3^2/a_0^2.$$

המשואה היא אפוא (2).

אם $a_0=-ra_3$, נקבל מ (2):

$$a_3(rX)^3+a_2(rX)^2+a_1(rX)+a_0=0 \tag{2'}$$

מן המשואה (2') מתקבלת (1) על-ידי הטרנספורמציה $X=1/rx$. לכן

$$\bar{S}_n=X_1^n+X_2^n+X_3^n=(1/rx_1)^n+(1/rx_2)^n+(1/rx_3)^n=r^{-n}S_{-n}.$$

בשימנו $r=1$, נקבל: $\bar{S}_n=S_{-n}$.

השקה בין קו גיאודטי וקו אסימפטוטי

גדעון יקותיאלי

ברשימה זו תוכח בדרך אחידה מציאותן של ארבע שמורות של קוים משיקים על משטח עקום, והן נוסחאות Meusnier, Bonnet, Laguerre ועוד נוסחה אחת, שעד כמה שידוע לי לא הובאה עדין בספרות. שמוש בשתי הנוסחאות האחרונות במקרה פרטי של קו גיאודטי וקו אסימפטוטי יתן שתי נוסחאות קשר בין העקום, העקול ונגזרותיהם של הקוים הנ"ל.

המשטח העקום במרחב של שלושה ממדים יגדר כאגודה בת שני פרמטרים (u^1,u^2) במרחב ישר שלש ממדי $(x^1x^2x^3)$ ע"י הוקטור $x^i(u^\alpha)$ $i=1,2,3;$ $\alpha=1,2;$ המטריקה של האגודה נתונה ע"י תבנית המדה $g_{\alpha\beta}=\frac{\partial x^i}{\partial u^\alpha}\cdot\frac{\partial x^i}{\partial u^\beta}$ תבנית העקום של האגודה מגדר ע"י $h_{\alpha\beta}=\bar{n}^i\frac{\partial^2 x^i}{\partial u^\alpha \partial u^\beta}$ ו-$\bar{n}^i$ הוא וקטור יחידה מאונך לאגודה באותה נקודה. כל וקטור A^i במרחב השלש-ממדי אפשר להפרידו לסכום של וקטור פנימי באגודה A^α ומרכיב חיצוני מאונך $\bar{A}$ לפי הנוסחה:

$$A^i=\frac{\partial x^i}{\partial u^\alpha}A^\alpha+\bar{n}^i\bar{A}$$

הפרוק של המשיק t^i, הנורמל n^i והבינורמל b^i לקו עקום באגודה, אם הנורמל של הקו הנ"ל n^i יוצר זוית θ עם הנורמל לאגודה $\bar{n}^i$, יהיה בהתאמה:

$$t^i=\frac{\partial x^i}{\partial u^\alpha}\cdot t^\alpha \qquad t^\alpha=\frac{du^\alpha}{ds}$$ s פרמטר הארך

$$n^i=\frac{\partial x^i}{\partial u^\alpha}\mu^\alpha\sin\theta+\bar{n}^i\cos\theta \qquad t^\alpha g_{\alpha\beta}t^\beta=1;\ \mu^\alpha g_{\alpha\beta}\mu^\beta=1 \tag{1}$$

$$b^i=-\frac{\partial x^i}{\partial u^\alpha}\mu^\alpha\cos\theta+\bar{n}^i\sin\theta \qquad \mu^\alpha g_{\alpha\beta}t^\beta=0$$

הצבת פרוק זה במשואות Frenet,

$$\frac{dt^i}{ds}=-kn^i\ ;\ \frac{dn^i}{ds}=-kt^i+\tau b^i\ ;\ \frac{db^i}{ds}=-\tau n^i \tag{2}$$

(k ו-τ העקום והעקול) ושמוש בנוסחאות העזר

$$\frac{\partial^2 x^i}{\partial u^\alpha \partial u^\beta}=\left\{{\gamma \atop \alpha\beta}\right\}\frac{\partial x^i}{\partial u^\gamma}+h_{\alpha\beta}\bar{n}^i$$ $\left\{{\gamma \atop \alpha\beta}\right\}$ סמן כריסטופל מהמין ה II

$$\frac{\partial \bar{n}^i}{\partial u^\beta}=-h_{\beta\varepsilon}g^{\varepsilon\gamma}\frac{\partial x^i}{\partial u^\gamma} \qquad g_{\alpha\beta}g^{\beta\gamma}=\delta_{\alpha\gamma} \tag{3}$$

יתנו את ארבע הנוסחאות הבאות:

$$k\cos\theta=h_{\alpha\beta}t^\alpha t^\beta=k_g \qquad \text{Meusnier נוסחת} \tag{4}$$

$$\tau+\frac{d\theta}{ds}=h_{\alpha\beta}t^\alpha\mu^\beta=\tau_g \qquad \text{Bonnet נוסחת} \tag{5}$$

בשני המקרים האגף הימני הוא שמורה לכל הקוים באגודה שיש להם משיק משותף באותה נקודה. הציון g משיך את העקום והעקול לקו הגיאודטי המשיק באותו כוון.

שתי הנוסחאות האחרות הן:

$$\frac{dt^\alpha}{ds}+\left\{{\alpha \atop \beta\gamma}\right\}t^\beta t^\gamma=k\sin\theta\,\mu^\alpha \tag{6}$$

$$\frac{d\mu}{ds}+\left\{{\alpha \atop \beta\gamma}\right\}t^\beta\mu^\gamma=-k\sin\theta\,t^\alpha \tag{7}$$

$k\sin\theta$ הוא העקום הפנימי של הקו ואלה הן משואות Frenet באגודה.

גזירת שני אגפי (4) לפי פרמטר הארך s ושמוש ב (6,5,4) נותנת את נוסחת Laguerre.

$$\frac{dk}{ds}\cos\theta - k\sin\theta\,\left(3\frac{d\theta}{ds} + 2\tau\right) = \left(\frac{\partial h_{\alpha\beta}}{\partial u^\gamma} - 2h_{\varepsilon\beta}\left\{{\varepsilon \atop \alpha\gamma}\right\}\right)t^\alpha t^\beta t^\gamma = h_{\alpha\beta,\gamma}t^\alpha t^\beta t^\gamma \tag{8}$$

$h_{\alpha\beta,\gamma}$ היא הנגזרת הקווריינטית של $h_{\alpha\beta}$. האגף הימני היא שמורה של כל הקוים באגודה שיש להם משיק משותף בנקודה נתונה.

גזירת שני אגפי (5) לפי הפרמטר s ושמוש ב (7,6,4) יתנו:

$$\frac{d^2\theta}{ds^2} + \frac{d\tau}{ds} + k\sin\theta(h_{\alpha\beta}t^\alpha t^\beta - h_{\alpha\beta}\mu^\alpha\mu^\beta) = \left(\frac{\partial h_{\alpha\beta}}{\partial u^\gamma} - \left\{{\varepsilon \atop \alpha\gamma}\right\}h_{\varepsilon\beta} - h_{\varepsilon\alpha}\left\{{\varepsilon \atop \beta\gamma}\right\}\right)t^\alpha\mu^\beta t^\gamma$$

האגף הימני הוא שמורה של כל הקוים שיש להם משיק משותף בנקודה נתונה. $k_g = h_{\alpha\beta}t^\alpha t^\beta$ הוא העקום הגיאודטי של קו משיק באותו כוון; $k_{\bar{g}} = h_{\alpha\beta}\mu^\alpha\mu^\beta$ העקום של הקו הגיאודטי המאונך לכוון זה. ולכן תכתב הנוסחה הנ"ל:

$$\frac{d^2\theta}{ds^2} + \frac{d\tau}{ds} + k\sin\theta\,(k_g - k_{\bar{g}}) = h_{\alpha\beta,\gamma}t^\alpha\mu^\beta t^\gamma \tag{9}$$

שמוש בנוסחאות (8) ו (9) למקרים של קו גיאודטי $\theta=0$ וקו אסימפטוטי $\theta = \frac{\pi}{2}$ נותן:

$$\left(\frac{dk}{ds}\right)_g + 2(k\tau)_a = 0 \tag{10}$$

$$\left(\frac{d\tau}{ds}\right)_g = k_a(k_g - k_{\bar{g}}) + \left(\frac{d\tau}{ds}\right)_a \tag{11}$$

הציון a משיך את הגדל לקו אסימפטוטי ו g לקו גיאודטי.

בדרך כלל כאשר קו אסימפטוטי משיק לגיאודטי קים בנקודת ההשקה $\tau_a = \tau_g$ (5) נוסחה (11) מראה כי התנאי לקיום $\left(\frac{d\tau}{ds}\right)_a = \left(\frac{d\tau}{ds}\right)_g$ דרוש תנאי נוסף $k_a = 0$ ז.א. העקום האסמפטוטי מתאפס או $k_g = k_{\bar{g}}$: העקום הגיאודטי בכוון המשיק לאסמפטוטי שוה לעקום הגיאודטי בכוון המאונך, ולהיפך.

הערה לבעית המספרים המשוכללים אי-הזוגיים

דב ירדן

מספר משוכלל הוא, כידוע, מספר טבעי, כמו $6=1+2+3$, $28=1+2+4+7+14$, וכדומה, השוה לסכום מחלקיו הקטנים ממנו. בעוד שידועות 12 דוגמות של מספרים משוכללים <u>זוגיים</u>, אין ידועה אף דוגמה אחת של מספר משוכלל אי-זוגי ואין ידוע, האם מספרים כאלה קימים או לא. בכל אפן הוכח, שאם קים מספר משוכלל אי-זוגי n, צורתו היא $n=(4a+1)^{4b+1}q^2$, כאשר $p=4a+1$ הוא מספר ראשוני ו q הוא מספר טבעי זר ל p. כן הוכח שלכל מספר משוכלל אי-זוגי יש לפחות 6 גורמים ראשוניים שונים, ושאם m הוא מספר הגורמים הראשוניים השונים של n, הגורם הראשוני המינימלי של n איננו עולה על m. כדאי אולי עוד להביע במפורש את העובדה הפשוטה דלקמן:

<u>משפט.</u> אם $n=(4a+1)^{4b+1}q^2$ הוא מספר משוכלל אי-זוגי, כאשר $p=4a+1$ הוא מספר ראשוני ו q הוא מספר טבעי זר ל p, $2a+1$ מחלק ל q^2.

<u>הוכחה.</u> אם נסמן כרגיל ב $\sigma(n)$ את סכום המחלקים של n (n בכלל), נקבל מצד אחד, לפי הנוסחה הידועה,

$$\sigma(n) = \frac{p^{4b+2}-1}{p-1}\,\sigma(q^2)$$

מצד שני, בגלל זה ש n הוא מספר משוכלל,

$$\sigma(n)=2n,$$

ועל-ידי השואה

$$2n = \frac{p^{4b+2}-1}{p-1}\,\sigma(q^2)$$

מכאן

$$n=\frac{p+1}{2}\cdot\frac{p^{2b+1}-1}{p-1}\cdot\frac{p^{2b+1}+1}{p+1}\sigma(q^2)=(2a+1)(p^{2b}+\ldots+1)(p^{2b}-\ldots+1)\sigma(q^2).$$

מכאן, $2a+1$ מחלק ל n. אך $2a+1$ זר ל $4a+1=2a+(2a+1)$. לכן $2a+1$ מחלק ל q^2.

תאור חבורה על ידי סכימה מעוקבת

דב ירדן

תאור החבורה על ידי סכימה רבועית לפי Cayley לקוי בזה, שאינו מגלה בנקל את חק הקבוציות השורר בחבורה (השוה A. Speiser, Gruppentheorie מהדורה ראשונה, 1923, עמוד 3 ומהדורה שניה, 1927, עמוד 14). לקוי זה מסתלק עם תאור החבורה על ידי סכימה מעוקבת, שנקרא לה קובית-כפל של החבורה. היא מתקבלת מסכימה רבועית של Cayley מסדר g, אם בונים עליה כעל בסיס קוביה בעלת g^3 תאים ושמים בשורתה ה k, עמודה l, קומה m את האבר $(A_kA_l)A_m$. סכימה מעוקבת כזאת נתנת כמובן להבנות גם על כל מערכת G של g אברים הערוכים ברבוע של g^2 משבצות כך שבכל שורה ועמודה עומדים בדיוק אותם g האברים, בתנאי שנבין גם כאן בסמל A_kA_l את האבר העומד בשורה k, עמודה l. כאבר-יחידה A_1 ישמש האבר העומד בשורה ראשונה ועמודה ראשונה, וכאבר הפוך לאבר נתון בשורה הראשונה - אבר העמודה הראשונה העומד בקצה המלבן, אשר ב 3 קצותיו האחרים עומדים האבר הנתון ו 2 אברי-יחידה. קל לראות, שבקובית-הכפל של מערכת G יעמדו בכל שורה, עמודה וקומה אותם g אברי המערכת. חק הקבוציות מתגלה אז לפי המשפט הבא:

<u>משפט.</u> מערכת G של g אברים $A_1,...,A_g$ הערוכים ברבוע של g^2 משבצות כך שבכל שורה ועמודה עומדים בדיוק אותם g האברים מתארת חבורה אז ורק אז, אם g העמודות של כל אחד מ $g-1$ הרבועים המקבילים לרבוע היסודי בקובית-הכפל של המערכת G מהוות תמורה (מסדר g, שאבריה הן העמודות) של עמודות הרבוע היסודי.

<u>הוכחה.</u> תהי ראשית G חבורה מסדר g בעלת האברים $A_1,...,A_g$. אז יהיה, לפי החק הקבוצי, $(A_kA_l)A_m=A_k(A_lA_m)$, לכל k,l,m. וזאת אומרת: האבר, העומד בשורה k, עמודה l, קומה m בקובית-הכפל של החבורה, שוה לאבר הרבוע היסודי, העומד בשורה k ועמודה, המתחילה באבר $A_n=A_lA_m$. עם כל l,m קבועים, גם A_l,A_m, ולפיכך גם $A_n=A_lA_m$, קבועים. ולפי שבשורה הראשונה של הרבוע היסודי מופיע כל אבר החבורה רק פעם אחת, יוצא שעמודה l, קומה m מתלכדת בעמודת הרבוע היסודי, המתחילה באבר $A_n=A_lA_m$. נקבע עכשו את m וניתן ל l לעבר על כל הערכים $l=1,...,g$. אז יעבר $A_n=A_lA_m$ על כל אברי החבורה וכל עמודה l בקומה m תתלכד באחת ורק אחת העמודות ברבוע היסודי.

תהי שנית G מערכת המקימת את תנאי המשפט. כדי להוכיח שהמערכת G מהוה חבורה די להוכיח שקים בה החק הקבוצי, ובכן שקים בה $(A_kA_l)A_m=A_k(A_lA_m)$ לכל k,l,m. לשם זה די להוכיח שהאבר העומד בשורה k, עמודה l, קומה m מתלכד באבר הרבוע היסודי, העומד בשורה k והעמודה, המתחילה באבר $A_n=A_lA_m$. מכיון שעמודות קומה m הן, לפי ההנחה, תמורה של עמודות הרבוע היסודי ואברי השורות הראשונות בכל קומה שונים ביניהם, לפיכך די להוכיח, שהאבר העומד בשורה <u>ראשונה</u>, עמודה l, קומה m מתלכד באבר הרבוע היסודי, העומד בשורה ראשונה <u>ובעמודה</u>, המתחילה באבר $A_n=A_lA_m$. זה נכון, מפני שקים בעליל: $(A_1A_l)A_m=A_lA_m=A_1(A_lA_m)=A_1A_n$. הוכחנו אפוא את משפטנו.

דוגמה. חמשת הרבועים הבאים מתארים את קובית-הכפל של החבורה הצקלית מסדר 5. הקומות מצוינות לפי סדרן בספרות רומיות, שמהן הספרה I מצינת את הרבוע היסודי. רואים בנקל, שעמודות כל קומה הן תמורה של עמודות הרבוע היסודי.

I	II	III	IV	V
1 2 3 4 5	2 4 1 5 3	3 1 5 2 4	4 5 2 3 1	5 3 4 1 2
2 4 1 5 3	4 5 2 3 1	1 2 5 4 5	5 3 4 1 2	3 1 5 2 4
3 1 5 2 4	1 2 3 4 5	5 3 4 1 2	2 4 1 5 3	4 5 2 3 1
4 5 2 3 1	5 3 4 1 2	2 4 1 5 3	3 1 5 2 4	1 2 3 4 5
5 3 4 1 2	3 1 5 2 4	4 5 2 3 1	1 2 3 4 5	2 4 1 5 3

לעומת זה אין הסכימה המעוקבת דלקמן I'-V' מתארת חבורה, לפי שכבר עמודות קומתה השניה II' אינן תמורה של עמודות הקומה I'.

I'	II'	III'	IV'	V'
1 2 3 4 5	2 4 1 5 3	3 5 4 1 2	4 3 5 2 1	5 1 2 3 4
2 4 1 5 3	4 5 2 3 1	5 1 3 2 4	3 2 4 1 5	1 3 5 4 2
3 5 4 1 2	1 3 5 2 4	4 2 1 3 5	5 1 2 4 3	2 4 3 5 1
4 3 5 2 1	5 1 3 4 2	1 4 2 5 3	2 5 1 3 4	3 2 4 1 5
5 1 2 3 4	3 2 4 1 5	2 3 5 4 1	1 4 3 5 2	4 5 1 2 3

שמושים לתורת המשואות הדיפרנציאליות הליניאריות

שמשון עמיצור

(המשך מעמוד 49)

חלק ב. שמושים.

סעיף 3: השדה הקומוטטיבי עם אבר a.

יהי F שדה לא קומוטטיבי שמרכזו M. נסמן ב D את הגזירה הפנימית הנוצרת ע"י אבר a (משפט עזר 4). ב F_a תסומן קבוצת כל אברי F הקומוטטי-ביים עם a.

משפט 3 *): כאשר a הוא אלגברי מעל המרכז M וממעלה n - F הוא מודול ימני ושמאלי מעל F_a מסדר n.

הוכחה: יהי $g(x)$ הפולינום המינימלי (המתוקן) של a מעל M, מעלתו היא n. כיון ש $F_R=F$ (משפט עזר 2) נקבל שבחוג $E(F)$ $g(a_R)=0$; $a_R=D-a_L$ (משפט עזר 4) לכן $g(D-a_L)=0$, מקדמי הפולינום $g(x)$ שיכים למרכז M, a_L ו D קומוטטיביים וכמו כן הם מתחלפים עם כל המקדמים, לכן:

$g(a_L-D)=(-1)^nD^n+b_{L,1}D^{n-1}+\dots+b_{L,n}=0$ המקדמים $b_{L,i}$ שיכים לשדה F_L כפולינומים של a_L עם מקדמים מהמרכז M.

מכאן שלכל c מתוך השדה F:

$$0=c^o=c^{g(a_L-D)}=(-1)^nc^{(n)}+b_1c^{(n-1)}+\dots+b_nc^{(o)}=0 \qquad [5]$$

כאשר b_i הם האברים בשדה F המתאימים ל $b_{L,i}$ בשדה F_L. אברי F הם אפוא פתרונות של המשואה הדיפרנציאלית הימנית [5], F_a הוא שדה הקונסטנטות לגבי גזירה זו, לכן לפי משפט 1 F הוא מודול ימני מסדר לכל היותר n מעל F_a.

אם $F:F_a$ הוא מסדר k יקימו אברי F משואה דיפרנציאלית ימנית ממעלה k (משפט 2):

$$z^{(k)}+c_1z^{(k-1)}+\dots+c_kz^{(o)}=0$$

יהיו אברי F_L $c_{L,i}$ המתאימים לאברים c_i ב F, אזי האופרטור $h(D)=D^k+c_{L,1}D^{k-1}+\dots+c_{L,k}\equiv0$. לכן:

$$h(D)=h(a_L-a_R)=(-1)^ka_R^k+d_{L,1}a_R^{k-1}+\dots+d_{L,k}=f_L(a_R)=0$$

הפתוח אפשרי כי a_R מתחלף עם כל אברי F_L, וכן $d_{L,i}$ שיכים ל F_L כפולינומים ב a_L עם מקדמים השיכים ל F_L. לכן לכל c השיך ל F:

$$0=c^o=c^{f_L(a_R)}=(-1)^kc.a^k+d_1ca^{k-1}+d_2ca^{k-2}+\dots+d_kc.a^o=0 \qquad [6]$$

d_i הם אברי F המתאימים לאברים $d_{L,i}$ ב F_L. כאשר $c\neq0$ נכפיל את [6] מימין ב c^{-1} ונקבל ש cac^{-1} הוא שרש ימני של הפולינום $f(x)=(-1)^kx^k+d_1x^{k-1}+\dots+d_k$.
מכאן שהפולינום $f(x)$ מאפס מימין את כל הצמודים של a. פולינום בעל תכונה זו הוא כפולה שמאלית של הפולינום המינימלי של a מעל המרכז M **) שמעלתו לפי ההנחה היא n, לכן $n\leq k$, בחלק הראשון של הוכחה זו הוכח ש $k\leq n$ לכן $k=n$. הגזירה הפנימית D שהשתמשנו בה היא גם גזירה שמאלית, לכן באותה דרך הוכחה נקבל גם ש F הוא מודול שמאלי מעל F_a מסדר n.

סעיף 4: שדות צקליים.

יהי F שדה (לאו דוקא קומוטטיבי) בעל אוטומורפיזם T מסדר n. C יהי השדה הנשאר אינורינטי אבר אבר ע"י האוטומורפיזם T.

משפט 4: F הוא מודול ימני ושמאלי מעל C מסדר לכל היותר n.

כי $T^n=E$ (E אוטומורפיזם היחידה ואבר היחידה של $E(F)$). נסתכל

---

*) Artin, Whaples: The Theory of Simple Rings, Amer. J. Math. 65 (1943), 87-107.

**) Dickson: Algebras and their Arithmetics.

בגזירה $D=T-E$ (משפט עזר 5). גזירה זו תקיים:

$$0=T^n-E=(D+E)^n-E=D^n+\binom{n}{1}D^{n-1}+\dots+\binom{n}{n-1}D=h(D)$$

ולכן כל אברי השדה F יהיו פתרונות של המשואה הדיפרנציאלית הימנית (והשמאלית):

$$0=z^0=z^{h(D)}=z^{(n)}+\binom{n}{1}z^{(n-1)}+\dots+\binom{n}{n-1}z'=0$$

ולפי משפט 1 אברי F הם מודול ימני (ושמאלי) מעל השדה C מסדר לכל היותר n.

כאשר שום חזקה של T הקטנה מ n איננה אוטומורפיזם פנימי, F:C הוא מודול מסדר n בדיוק *). נראה כי המשפטים הידועים על הרחבות צקליות של שדות קומוטטיביים יתקימו גם במקרה הכללי בתנאי ש F מעל C הוא מודול מסדר n, לכן נגדיר הרחבה צקלית במקרה הכללי באופן הבא:

הגדרה: השדה F יקרא הרחבה צקלית מסדר n מעל השדה C כאשר F הוא מודול ימני ושמאלי מסדר n מעל C, ויש לו חבורה צקלית של אוטומורפיזמים שסדרה n, באשר C הוא שדה כל האברים הנשארים אינורינטים ע"י אוטומורפיזמים אלו.

נעסק בהרחבות צקליות בשני מקרים: א) הכרכטריסטיקה של השדה F היא אפס או $p\neq 0$ באשר $(p,n)=1$. ב) הכרכטריסטיקה של F היא $p\neq 0$, ו $n=p^e$.

במקרה א נוכיח את המשפטים הבאים:

משפט 5: כאשר השדה C מכיל את שרשי היחידה מסדר n $w_1=1,w_2,\dots,w_n$ מכיל השדה F מערכת אברי בסיס ימניים מעל C: $b_1=1, b_2,\dots,b_n$ אשר [7] $b_i^T=w_ib_i$; ומערכת אברי בסיס שמאליים מעל C: $d_1=1, d_2,\dots,d_n$ אשר [8] $d_i^T=d_iw_i$, וכן כל קבוצת אברים (b_i) המקימת את [7] היא מערכת בסיס ימנית (של המודול הימני F מעל C), וקבוצה (d_i) המקימת את [8] היא מערכת בסיס שמאלית (של המודול השמאלי F מעל C).

הוכחה: נסמן ב K את כל אברי המרכז של השדה F הנשארים אינורינטים ע"י האוטומורפיזם T, $\bar{K}$ יהי ההרחבה של השדה K ע"י הוספת שרשי היחידה. $\bar{K}$ הוא אפוא שדה קומוטטיבי ונשאר אינורינטי ע"י T. בחוג E(F): השדה F אנטיאיזומורפי ל F_L, ובהתאמה זו לשדה $\bar{K}$ יתאים השדה $\bar{K}_L$. אברי השדה $\bar{K}_L$ קומוטטיביים (בחוג E(F)) עם הגזירה $T-E=D$, כי לכל k_L השיך ל $\bar{K}_L$ ולכל a השיך ל F:

$$a^{k_LT}=(a^{k_L})^T=(ka)^T=ka^T=a^{Tk_L}$$

כיון ש $k^T=k$ לכל k השיך ל $\bar{K}$, ולכן $k_LT=Tk_L$. אברי $\bar{K}_L$ מתחלפים עם T ולכן גם עם $D=T-E$.

הפולינום h(D) מתפרק ב E(F): $0=h(D)=(D+E)^n-E=h_i(D)(D+E-w_{L,i})$

באשר $w_{L,i}$ בשדה F_L המתאים ל w_i בשדה F. קים אבר x אחד לפחות אשר $x^{h_i(D)}\neq 0$, אחרת היה $x^{h_i(D)}=x^{(n-1)}+h_{i,1}x^{(n-2)}+\dots+h_{i,n-1}x^{(o)}=0$

ואברי השדה F הם פתרונות של משואה דיפרנציאלית ממעלה n-1, לכן F:C הוא מודול ימני ממעלה לכל היותר n-1, בנגוד להנחה שהסדר של F מעל C הוא n.

ויהי b_i האבר $b_i=x_i^{h_i(D)}\neq 0$ $i=1,2,\dots,n$. אזי יתקים:

$$0=x_i^0=x_i^{h(D)}=x_i^{h_i(D)(D+E-w_{L,i})}=b_i^{D+E-w_{L,i}}=b_i^{T-w_{L,i}}=b_i^T-w_ib_i=0$$

לכן [7] $b_i^T=w_ib_i$ $i=1,2,\dots,n$, מערכת אברים המקימת [7] היא בלתי תלויה מימין מעל C, כי אם $\sum_{i=1}^{n} b_ic_i=0$ ע"י התמונה ה T^k $k=0,1,\dots,n-1$ נקבל $\sum_{i=1}^{n} b_i^{T^k}c_i=\sum_{i=1}^{n} w_i^k(b_ic_i)=0$. מערכת שויונות אלו פרושה שעמודי המטריצה W תלויים מימין ב F.

- -

*) Jacobson: Galois Theory for Quasi-Fields, Ann. of Math. 41 (1940), 1-7.

אך המטריצה W דרגתה n בשדה $\bar{K}$ (כי $|W|^2$ בשדה הקומוטטיבי $\bar{K}$ היא הדיסקרימיננטה של הפולינום x^n-1, וזו $\neq 0$ כאשר $(n,p)=1$ או $p=0$). ולכן דרגת המטריצה W היא n בכל שדה F המכיל את $\bar{K}$. מכאן שתלות זו תתכן אך ורק כאשר $b_ic_i=0$ כיון ש $b_i\neq 0$. לכן $c_i=0$, $i=1,\dots,n$. מספרם של b_i הוא n והם בלתי תלויים סימין מעל C לכן הם מהוים אברי בסיס של המודול הימני F (מסדר n) מעל C.

$$W=\begin{pmatrix} 1 & 1 & \dots & 1 \\ w_1 & w_2 & \dots & w_n \\ \dots & \dots & \dots & \dots \\ w_1^{n-1} & \dots & \dots & w_n^{n-1} \end{pmatrix}$$

ההוכחה לגבי הבסיס השמאלי (d_i) דומה, מתוך העובדהש D היא גם גזירה שמאלית.

<u>משפט 6:</u> תהי F הרחבה צקלית מסדר n מעל C, ויהיו שרשי היחידה מסדר n שיכים למרכז של C ונשארים אינורינטים ע״י האוטומורפיזם T. אז קים אבר a בשדה F, אשר $a^n=c$, c שיך לשדה C, והאברים: $1,a,a^2,\dots,a^{n-1}$ הם אברי בסיס של המודול הימני והשמאלי F מעל C.

הוכחה: יהי w שרש פרימיטיבי מסדר n, קים לפי משפט 5 אבר a אשר $a^T=wa$ ולכן $(a^i)^T=w^i.a=aw^i$ $i=0,1,\dots,n-1$. לכן $1,a,\dots,a^{n-1}$ הם אברי בסיס ימניים ושמאליים (משפט 5) $(a^n)^T=w^na=a$ לכן $a^n=c$ אשר c שיך לשדה C.

כשהמרכז של השדה C מכיל את שרשי היחידה מסדר n, נוכל לבנות את כל ההרחבות הצקליות מסדר n מעל F (אם הן קימות בכלל), בדרך הבאה:

<u>משפט 7:</u> בתנאים הנ״ל, תהי F הרחבה צקלית מסדר n מעל השדה C. קים אז אוטומורפיזם S בשדה C אשר S^n הוא אוטומורפיזם פנימי ב C הנוצר ע״י אבר c.

את השדה F אפשר לציין באופן הבא: ב $C[t]$ נסמן את חוג הפולינומים ב t אם מקדמים מהשדה C אשר $dt=t.d^S$ לכל d השיך ל C. האידיאל הימני ב $C[t]$ הנוצר ע״י הפולינום t^n-c הוא דו-צדדי ראשוני שנסמנו ב A ו F איזומורפי לשדה המנה $C[t]-A$.

הוכחה: לכל אבר d בשדה C האבר $a^{-1}da$ שיך גם כן לשדה C. כי $(a^{-1}da)^T=(a^{-1})^Td^Ta^T=w^{-1}a^{-1}daw=a^{-1}da$ כי $d^T=d$ ו w קומוטטיבי עם כל אברי F. לכן ההתאמה $d\longrightarrow a^{-1}da$ היא אוטומורפיזם S של השדה C. $d^{S^n}=a^{-n}.da^n=c^{-1}dc$, S^n הוא אוטומורפיזם פנימי ב C, כי c שיך לשדה C. כיון ש $d^S=a^{-1}da$ נקבל $ad^S=da$.

קל להוכח ש F איזומורפי ל $C[t]-A$ ע״י ההתאמה: ל a נתאים את המשתנה t, ולאברי C יתאימו אותם האברים של C.

בעזרת משפט זה נוכל לבנות את כל ההרחבות הצקליות מסדר n (בתנאים הנ״ל). לשם כך עלינו לצאת מאוטומורפיזם S של שדה C, אשר S^n הוא אוטומורפיזם פנימי ולבנות את האידיאל הדוצדדי A, ואת A הוא <u>ראשוני</u> אז $C[t]-A$ הוא שדה הרחבה צקלית מסדר n מעל C, האוטומורפיזם היוצר הוא $t^T=wt$ אשר w הוא שרש פרימיטיבי מסדר n. קל להוכח שאכן ההרחבה היא צקלית ומסדר n.

כאשר S הוא האוטומורפיזם האידנטי ההרחבה הצקלית נוצרת ע״י הרחבת המרכז של השדה C, ע״י הוספת שרש פולינום טהור: $x^n=m$ m שיך למרכז.

נעבר למקרה ב. כאשר הכרכטריסטיקה של F היא $p\neq 0$ ו $n=p^e$ ואף כאן נסתכל בגזירה $D=T-E$ ונוכיח את המשפטים:

<u>משפט 8:</u> א) אברי F הן פתרונות של המשואה הדיפרנציאלית $z^{(p^e)}=0$.

ב) כל הפתרונות של המשואה הדיפרנציאלית $z^{(i)}=0$ $i=1,2,\dots,p^e$ הם מודול ימני M_i מעל C מסדר i; המודול M_i נוצר ע״י כל הנגזרות של אברי המודול M_{i+1}; וכן $M_i\subset M_{i+1}$.

כמו במשפט 4, יהיה כאן: $h(D)=D^{p^e}=0$ כי $\binom{p^e}{i}\equiv 0(p)$ כאשר $1\leq i\leq p^e-1$

ולכן אברי F פתרונות של המשואה: $0=z^{h(D)}=z^{(p^e)}$.

את קיום התנאים לגבי M_i נוכיח בדרך אינדוקציה: כאשר $i=p^e$ $M_i=F$ ו $F:C$ הוא מסדר p^e לפי ההנחה. יהי המשפט נכון לגבי המודול M_{i+1}. אם a שיך ל M_{i+1} $a^{(i+1)}=a'^{(i)}=0$ לכן 'a שיך ל M_i. M_i לפי משפט 2 הוא מודול לכל היותר מסדר i. יהיו $a_1=1,a_2,\ldots,a_{i+1}$ i+1 אברי הבסיס של M_{i+1}, אזי $a_2',a_3',\ldots,a_{i+1}'$ יהיו אברים בלתי תלויים מעל C במודול M_i כי אם $\sum_{j=2}^{i+1} a_j'c_j=0$ באשר c_j שיכים לשדה C, $(\sum_{j=2}^{i+1} a_jc_j)'=0$ לכן $\sum_{j=2}^{i+1} a_jc_j=1\cdot c$ באשר c שיך לשדה C, דבר שיתכן רק כאשר $j=2,\ldots,i+1$ $c=c_j=0$ כי $1,a_2,\ldots,a_{i+1}$ בלתי תלויים מעל C.

מכאן ש M_i הוא מודול מסדר i ויש לו אברי בסיס $a_2',\ldots,a_{i+1}'$.

אם d שיך ל M_i, $d=\sum_{j=2}^{i+1} a_j'c_j$ ולכן $d=h'$ באשר $h=\sum_{j=2}^{i+1} a_jc_j$, h שיך אפוא ל M_{i+1}.

אם נסכם תוצאות אלו נקבל שהמשפט נכון לגבי M_i מתוך נכונותו לגבי M_{i+1}. ובזה הוכח המשפט. קל להוכח כי גם התנאי השני ש $M_i\subset M_{i+1}$ קים.

תוצאה: a השיך ל F הוא אינטגרבילי אז ורק אז כאשר a שיך ל M_i $i=1,2,\ldots,p^e-1$. כי אם $a=b'$ יהיה $a^{(p^e-1)}=b^{(p^e)}=0$.

<u>משפט 9:</u> ב F מעל C אפשר למצא אברי בסיס $x_1=1,x_2,\ldots,x_{p^e}$ אשר $x_i^T=x_i+x_{i-1}$, $i=2,3,\ldots,p^e$ (האברים $x_1=1,\ldots,x_i$ יהיו אברי בסיס של M_i).

נבחר את האברים x_i בדרך האינדוקציה, $x_1=1$. אם נבחרו $x_1=1,x_2,\ldots,x_i$ שהם אברי בסיס של M_i ו $i<p^e$, קים ב M_{i+1} אבר x_{i+1} אשר $x_{i+1}'=x_i$ (תוצאה של משפט 8), לכן $x_{i+1}'=x_{i+1}^{T-E}=x_{i+1}^T-x_{i+1}=x_i$
$x_1=1,x_2,\ldots,x_i,x_{i+1}$ הם אברי בסיס של M_{i+1}, כי אם a שיך ל M_{i+1}, 'a שיך אפוא ל M_i ולכן $a'=\sum_{j=1}^{i} x_jc_j=(\sum_{j=1}^{i} x_{j+1}c_j)'$ לכן $a=\sum_{j=1}^{i} x_{j+1}c_j+1\cdot c_0$
ומכאן ש $1,x_2,\ldots,x_{j+1}$ אברי בסיס של M_{i+1}.
נצטמצם למקרה $e=1$, דהיינו להרחבות צקליות מסדר p מעל C.

<u>משפט 10:</u> תהי F הרחבה צקלית מסדר p מעל C (הכרכטריסטיקה של F היא p). קימת בשדה C גזירה D אשר D^p-D היא גזירה פנימית בשדה C ונוצרת ע"י אבר a אשר $a'=0$. ב $C[t]$ נסמן את חוג הפולינומים של t מעל C אשר $ct=tc+c'$ לכל c השיך לשדה C. האידיאל הימני ב $C[t]$ הנוצר ע"י הפולינום t^p-t-a הוא ראשוני ודו-צדדי שנסמנו ב A. בתנאים אלו השדה F איזומורפי לשדה המנה $C[t]-A$.

הוכחה: קים ב F אבר y אשר $y^T=y+1$ ($y=x_2$ שבמשפט 8).

א. לכל c בשדה C $(cy-yc)^T=cy^T-y^Tc=c(y+1)-(y+1)c=cy-yc$

מכאן ש $cy-yc$ אף הוא אבר ב C, ולכן ההתאמה $c\to c^D=cy-yc$ היא גזירה ב C (כי היא גזירה פנימית ב F).

ב. $c^{D^p-D}=cy^p-y^pc-cy+yc=c(y^p-y)-(y^p-y)c=ca-ac$

כי $(y^p-y)^T=(y+1)^p-(y+1)=y^p-y=a$

a שיך לשדה C. לכן D^p-D היא גזירה פנימית ב C הנוצרת ע"י a.

a מתחלף עם y בשדה F לכן $a'=ay-ya=0$.

ג. $1,y,y^2,\ldots,y^{p-1}$ הם בלתי תלויים מימין ומשמאל מעל C, כי יהיו

$1,y,\dots,y^k$ המספר המינימלי של האברים הבלתי תלויים מעל C אז $y^{k+1}=\sum_{i=1}^{k} y^i c_i$ (תלות ימנית) בתמונה ע"י T נקבל: $(y+1)^{k+1}=\sum_{i=1}^{k}(y+1)^i c_i$

לכן $\sum_{j=0}^{k+1}\binom{k+1}{j}y^j=\sum_{i=1}^{k}\sum_{j=0}^{i}\binom{i}{j}y^j c_i$. נציג במקום y^{k+1} את ערכו נקבל:

$\sum_{j=0}^{k}\binom{k+1}{j}y^j=\sum_{i=1}^{k}\sum_{j=0}^{i-1}\binom{i}{j}y^j c_i$. המקדם של y^k בשויון זה הוא $\binom{k+1}{k}\neq 0$

כאשר $k<p-1$, אך מכאן $1,y,\dots,y^k$ תלויים מימין בנגוד להנחה (ההוכחה דומה לגבי השמאל).

החלק האחרון נובע בנקל לפי ההתאמה. ל y נתאים את המשתנה t ולאברי C יתאימו אותם אברי C. ובהתאמה זו יהיה F איזומורפי לשדה המנה $C[t]-A$.

נצטט גם את ההפוך של משפט 10 בלי הוכחה (ההוכחה מתקבלת בנקל לפי אותם הדרכים של משפט 10):

<u>משפט 11:</u> אם בשדה C קימת גזירה D, אשר D^p-D היא גזירה פנימית הנוצרת ע"י אבר a, וכן $a'=0$. כאשר הפולינום t^p-t-a ב $C[t]$ (שבמשפט 10) הוא אי פריק, אז האידיאל הימני הנוצר ע"י t^p-t-a שנסמנו ב A הוא ראשוני ודו צדדי, ושדה המנה $C[t]-A$ הוא שדה הרחבה צקלית מסדר p מעל F.

האוטומורפיזם היוצר הוא $t^T=t+1$.

תוצאות: כאשר C הוא שדה קומוטטיבי והגזירה $D=0$ משפט 10 ומשפט 11 המה משפטים ידועים על ההרחבות הצקליות מסדר p (ראה למשל בספרו של A.A. Albert: Modern Higher Algebra).

כאשר C שדה משוכלל קומוטטיבי אין בו כל גזירות מלבד האפס (משפט Baer) ולכן ההרחבות הצקליות היחידות מסדר p מעליו הם קומוטטיביות.

כי כאשר הגזירה D שבמשפט 10 היא גזירת האפס, ההרחבה הצקלית המתקבלת היא הרחבה קומוטטיבית צקלית של המרכז של השדה C.

ואמנם הגזירה $D=0$ היא למעשה גזירה פנימית הנוצרת על ידי y, לכן y קומוטטיבי עם כל אברי C וממילא הוא גם קומוטטיבי עם כל אברי השדה F, כלומר y שיך למרכז של F. ממשפט 10 מתקבל ש $y^p-y=a$; a שיך לשדה C לכן a שיך למרכז של C. וההרחבה הצקלית F מעל C מתקבלת על ידי הרחבת המרכז של C על ידי שרש של הפולינום האי פריק x^p-x-a.

אותו הדבר נכון כאשר הגזירה D שבמשפט 10 היא גזירה פנימית הנוצרת על ידי אבר d של השדה C. כי במקרה זה במקום להסתכל באבר y שבמשפט 10 נבחר את $z=y-d$ שאף הוא יקיים $z^T=z+1$, וקל להוכח כי הגזירה הפנימית ב C המגדרת על ידי z היא גזירת האפס, ולכן מצטמצם מקרה זה למקרה הקודם.

תוצאה: אם בשדה C כל גזירה היא גזירה פנימית, ההרחבות הצקליות היחידות מסדר p (באשר p הכרכטריסטיקה של C) הן ההרחבות המתקבלות ע"י הרחבה צקלית של המרכז.

תוספת: בהוכחה ב של משפט 10 השתמשנו בעובדה שאם $c^D=cy-yc$ אז $c^{D^p}=cy^p-y^pc$. ואמנם בחוג $R(F)$ $D=y_R-y_L$; y_R ו y_L קומוטטיביים לכן $D^p=(y_R-y_L)^p=y_R^p-y_L^p$. מכאן ש D^p גזירה פנימית הנוצרת על ידי y^p.

n	2^n	n	2^n
1	2	65	36893488147419103232
2	4	66	73386976294838206464
3	8	67	147573952589676412928
4	16	68	295147905179352825856
5	32	69	590295810358705651712
6	64	70	1180591620717411303424
7	128	71	2361183241434822606848
8	256	72	4722366482869645213696
9	512	73	9444732965739290427392
10	1024	74	18889465931478580854784
11	2048	75	37778931862957161709568
12	4096	76	75557863725914323419136
13	8192	77	151115727451828646838272
14	16384	78	302231454903657293676544
15	32768	79	604462909807314587353088
16	65536	80	1208925819614629174706176
17	131072	81	2417851639229258349412352
18	262144	82	4835703278458516698824704
19	524288	83	9671406556917033397649408
20	1048576	84	19342813113834066795298816
21	2097152	85	38685626227668133590597632
22	4194304	86	77371252455336267181195264
23	8388608	87	154742504910672534362390528
24	16777216	88	309485009821345068724781056
25	33554432	89	618970019642690137449562112
26	67108864	90	1237940039285380274899124224
27	134217728	91	2475880078570760549798248448
28	268435456	92	4951760157141521099596496896
29	536870912	93	9903520314283042199192993792
30	1073741824	94	19807040628566084398385987584
31	2147483648	95	39614081257132168796771975168
32	4294967296	96	79228162514264337593543950336
33	8589934592	97	158456325028528675187087900672
34	17179869184	98	316912650057057350374175801344
35	34359738368	99	633825300114114700748351602688
36	68719476736	100	1267650600228229401496703205376
37	137438953472	101	2535301200456458802993406410752
38	274877906944	102	5070602400912917605986812821504
39	549755813888	103	10141204801825835211973625643008
40	1099511627776	104	20282409603651670423947251286016
41	2199023255552	105	40564819207303340847894502572032
42	4398046511104	106	81129638414606681695789005144064
43	8796093022208	107	162259276829213363391578010288128
44	17592186044416	108	324518553658426726783156020576256
45	35184372088832	109	649037107316853453566312041152512
46	70368744177664	110	1298074214633706907132624082305024
47	140737488355328	111	2596148429267413814265248164610048
48	281474976710656	112	5192296858534827628530496329220096
49	562949953421312	113	10384593717069655257060992658440192
50	1125899906842624	114	20769187434139310514121985316880384
51	2251799813685248	115	41538374868278621028243970633760768
52	4503599627370496	116	83076749736557242056487941267521536
53	9007199254740992	117	166153499473114484112975882535043072
54	18014398509481984	118	332306998946228968225951765070086144
55	36028797018963968	119	664613997892457936451903530140172288
56	72057594037927936	120	1329227995784915872903807060280344576
57	144115188075855872	121	2658455991569831745807614120560689152
58	288230376151711744	122	5316911983139663491615228241121378304
59	576460752303423488	123	10633823966279326983230456482242756608
60	1152921504606846976	124	21267647932558653966460912964485513216
61	2305843009213693952	125	42535295865117307932921825928971026432
62	4611686018427387904	126	85070591730234615865843651857942052864
63	9223372036854775808	127	170141183460469231731687303715884105728
64	18446744073709551616	128	340282366920938463463374607431768211456

*) עד כה נדפסו החזקות של 2 רק עד למעריך 120 ע"י Peters ו Stein, 922
בלוחות לוגרתמיים, ועד למעריך 140 ע"י Weigel, 1933. ראה
Fletcher-Miller-Rosenhead, An Index of Math.Tables,1946,p.26.
חשובו של לוח זה נעשה בלא

n	2^n
129	680564733841876926926749214863536422912
130	1361129467683753853853498429727072845824
131	2722258935367507707706996859454145691648
132	5444517870735015415413993718908291383296
133	10889035741470030830827987437816582766592
134	21778071482940061661655974875633165533184
135	43556142965880123323311949751266331066368
136	87112285931760246646623899502532662132736
137	174224571863520493293247799005065324265472
138	348449143727040986586495598010130648530944
139	696898287454081973172991196020261297061888
140	1393796574908163946345982392040522594123776
141	2787593149816327892691964784081045188247552
142	5575186299632655785383929568162090376495104
143	11150372599265311570767859136324180752990208
144	22300745198530623141535718272648361505980416
145	44601490397061246283071436545296723011960832
146	89202980794122492566142873090593446023921664
147	178405961588244985132285746181186892047843328
148	356811923176489970264571492362373784095686656
149	713623846352979940529142984724747568191373312
150	1427247692705959881058285969449495136382746624
151	2854495385411919762116571938898990272765493248
152	5708990770823839524233143877797980545530986496
153	11417981541647679048466287755595961091061972992
154	22835963083295358096932575511191922182123945984
155	45671926166590716193865151022383844364247891968
156	91343852333181432387730302044767688728495783936
157	182687704666362864775460604089535377456991567872
158	365375409332725729550921208179070754913983135744
159	730750818665451459101842416358141509827966271488
160	1461501637330902918203684832716283019655932542976
161	2923003274661805836407369665432566039311865085952
162	5846006549323611672814739330865132078623730171904
163	11692013098647223345629478661730264157247460343808
164	23384026197294446691258957323460528314494920687616
165	46768052394588893382517914646921056628989841375232
166	93536104789177786765035829293842113257979682750464
167	187072209578355573530071658587684226515959365500928
168	374144419156711147060143317175368453031918731001856
169	748288838313422294120286634350736906063837462003712
170	1496577676626844588240573268701473812127674924007424
171	2993155353253689176481146537402947624255349848014848
172	5986310706507378352962293074805895248510699696029696
173	11972621413014756705924586149611790497021399392059392
174	23945242826029513411849172299223580994042798784118784
175	47890485652059026823698344598447161988085597568237568
176	95780971304118053647396689196894323976171195136475136
177	191561942608236107294793378393788647952342390272950272
178	383123885216472214589586756787577295904684780545900544
179	766247770432944429179173513575154591809369561091801088
180	1532495540865888858358347027150309183618739122183602176
181	3064991081731777716716694054300618367237478244367204352
182	6129982163463555433433388108601236734474956488734408704
183	12259964326927110866866776217202473468949912977468817408
184	24519928653854221733733552434404946937899825954937634816
185	49039857307708443467467104868809893875799651909875269632
186	98079714615416886934934209737619787751599303819750539264
187	196159429230833773869868419475239575503198607639501078528
188	392318858461667547739736838950479151006397215279002157056
189	784637716923335095479473677900958302012794430558004314112
190	1569275433846670190958947355801916604025588861116008628224
191	3138550867693340381917894711603833208051177722232017256448
192	6277101735386680763835789423207666416102355444464034512896

n	2^m
193	12554203470773361527671578846415332832204710888928069025792
194	25108406941546723055343157692830665664409421777856138051584
195	50216813883093446110686315385661331328818843555712276103168
196	100433627766186892221372630771322662657637687111424552206336
197	200867255532373784442745261542645325315275374222849104412672
198	401734511064747568885490523085290650630550748445698208825344
199	803469022129495137770981046170581301261101496891396417650688
200	1606938044258990275541962092341162602522202993782792835301376
201	3213876088517980551083924184682325205044405987565585670602752
202	6427752177035961102167848369364650410088811975131171341205504
203	12855504354071922204335696738729300820177623950262342682411008
204	25711008708143844408671393477458601640355247900524685364822016
205	51422017416287688817342786954917203280710495801049370729644032
206	102844034832575377634685573909834406561420991602098741459288064
207	205688069665150755269371147819668813122841983204197482918576128
208	411376139330301510538742295639337626245683966408394965837152256
209	822752278660603021077484591278675252491367932816789931674304512
210	1645504557321206042154969182557350504982735865633579863348609024
211	3291009114642412084309938365114701009965471731267159726697218048
212	6582018229284824168619876730229402019930943462534319453394436096
213	13164036458569648337239753460458804039861886925068638906788872192
214	26328072917139296674479506920917608079723773850137277813577744384
215	52656145834278593348959013841835216159447547700274555627155488768
216	105312291668557186697918027683670432318895095400549111254310977536
217	210624583337114373395836055367340864637790190801098222508621955072
218	421249166674228746791672110734681729275580381602196445017243910144
219	842498333348457493583344221469363458551160763204392890034487820288
220	1684996666696914987166688442938726917102321526408785780068975640576
221	3369993333393829974333376885877453834204643052817571560137951281152
222	6739986666787659948666753771754907668409286105635143120275902562304
223	13479973333575319897333507543509815336818572211270286240551805124608
224	26959946667150639794667015087019630673637144422540572481103610249216
225	53919893334301279589334030174039261347274288845081144962207220498432
226	107839786668602559178668060348078522694548577690162289924414440996864
227	215679573337205118357336120696157045389097155380324579848828881993728
228	431359146674410236714672241392314090778194310760649159697657763987456
229	862718293348820473429344482784628181556388621521298319395315527974912
230	1725436586697640946858688965569256363112777243042596638790631055949824
231	3450873173395281893717377931138512726225554486085193277581262111899648
232	6901746346790563787434755862277025452451108972170386555162524223799296
233	13803492693581127574869511724554050904902217944340773110325048447598592
234	27606985387162255149739023449108101809804435888681546220650096895197184
235	55213970774324510299478046898216203619608871777363092441300193790394368
236	110427941548649020598956093796432407239217743554726184882600387580788736
237	220855883097298041197912187592864814478435487109452369765200775161577472
238	441711766194596082395824375185729628956870974218904739530401550323154944
239	883423532389192164791648750371459257913741948437809479060803100646309888
240	1766847064778384329583297500742918515827483896875618958121606201292619776
241	3533694129556768659166595001485837031654967793751237916243212402585239552
242	7067388259113537318333190002971674063309935587502475832486424805170479104
243	14134776518227074636666380005943348126619871175004951664972849610340958208
244	28269553036454149273332760011886696253239742350009903329945699220681916416
245	56539106072908298546665520023773392506479484700019806659891398441363832832
246	113078212145816597093331040047546785012958969400039613319782796882727665664
247	226156424291633194186662080095093570025917938800079226639565593765455331328
248	452312848583266388373324160190187140051835877600158453279131187530910662656
249	904625697166532776746648320380374280103671755200316906558262375061821325312
250	1809251394333065553493296640760748560207343510400633813116524750123642650624
251	3618502788666131106986593281521497120414687020801267626233049500247285301248
252	7237005577332262213973186563042994240829374041602535252466099000494570602496
253	14474011154664524427946373126085988481658748083205070504932198000989141204992
254	28948022309329048855892746252171976963317496166410141009864396001978282409984
255	57896044618658097711785492504343953926634992332820282019728792003956564819968
256	115792089237316195423570985008687907853269984665640564039457584007913129639936