תולדות המתמטיקה

יובל קפלן

סיכום הרצאות פרופ׳ בנימין וייס בקורס ״תולדות המתמטיקה״ (80402)
באוניברסיטה העברית, 8–2007.

תוכן מחברת זו הוקלד ונערך על־ידי יובל קפלן. אין המרצה אחראי לכל טעות שנפלה בו. סודר באמצעות $\LaTeX\,2_\varepsilon$ ב־1 בספטמבר 2008.

עדכונים ותיקונים יופיעו ב־http://www.limsoup.net/. לתגובות, לתיקונים ובכל עניין אחר, אנא כתבו ל־yuvak@gmx.net.

סיכומים נוספים בסדרה:

2006–7	חשבון אינפיניטסימלי 1	אלגברה לינארית 1
	חשבון אינפיניטסימלי 2	אלגברה לינארית 2
	תורת הקבוצות	
2007–8	מבנים אלגבריים 1	תורת ההסתברות 1
	חשבון אינפי' מתקדם 1	
בקרוב	חשבון אינפי' מתקדם 2	מבוא לטופולוגיה
	תורת המספרים וקריפטו'	מבנים אלגבריים 2
	תולדות המתמטיקה	

תוכן עניינים

15.5.2008 העיסוק בתולדות המתמטיקה[1] החל כבר בימי הביניים. מקור השם "מתמטיקה" הוא במילה היוונית $\mu\acute{\alpha}\theta\eta\mu\alpha$ "לימוד" שנגזרת בפועל היווני $\mu\alpha\nu\theta\acute{\alpha}\nu\varepsilon\iota\nu$ "לחקור/ללמוד", כפי שמתאר זאת הרון האלכסנדרוני בצטטו את אנטוליוס:

"no one can acquire knowledge of the subject called 'mathematics' unless he has first gone through a course of instruction in it ..."

1 המתמטיקה היוונית

1.1 המספרים האי־רציונלים

גילוי המספרים האי־רציונלים על־ידי היוונים במאה ה־5 לפנה"ס מסמן, למעשה, את תחילתה של מהפכה בהתייחסות למתמטיקה; זו הפעם הראשונה בה הוכיחו שאי־אפשר לעשות דבר מסויים.

לרוב הדעות, גילוי זה התבסס על משפט פיתגוראס, שאומר ש־$A+B=C$ עבור [ציור] המקרה הפשוט ביותר של המשפט הוא עבור משולש שווה־שוקיים: [ציור נוסף] גילוי האי־רציונליים, לפי זאת, הוא הגילוי שלא ניתן למצוא מדד משותף[2] לצלע וליתר של משולש ישר־זוית ושווה־שוקיים.

הוכחה לעובדה זו מופיעה בכתביו של אריסטו)המאה השלישית לפנה"ס(:

"כל אלה שמסיקים בדרך השלילה מסיקים מסקנה שקרית ומוכיחים את הטענה המקורית היפותטית כשמשהו בלתי־אפשרי נובע מהנחת שלילתה; למשל, הקוטר של ריבוע איננו בר־השוואה עם הצלע בגלל שמספרים אי־זוגיים שווים למספרים זוגיים אם מניחים שיש מדד משותף, ואז מסיקים מכלל ההיסק שמספרים אי־זוגיים הם זוגיים, והוכח כי האלכסון איננו בר־השוואה עם הצלע, כי מגיעים למסקנה שקרית." (Analytica Priora I.23)

עם זאת, קשה להאמין שכך אכן התגלתה עובדה זו.

סברה אחרת, אותה העלה Kurt von Fritz[3], היא שהאי־רציונלים התגלו כאשר נחקרו יחסי ארכים במחומש המשוכלל. כל האלכסונים בו שווים, וכאשר מעבירים אותם, מתקבל מחומש משוכלל חדש:[4] [ציור] המטרה היא למצוא מדד משותף לצלע (הקטע AB) ולאלכסון (AC). לשם כך, משתמשים באלגוריתם האוקלידי.

נחפש נקודה B' על AC כך ש־$|AB|=|AB'|$: [שרטוט] כעת, מדד משותף ל־AB ול־$B'C$ ימדוד את AC.[5] נמשיך בתהליך: [ציור] כלומר, מחפשים C' על AB' כך ש־$|B'C|=|AC'|$. הבעיה כעת היא למצוא מדד משותף עבור AC' ו־$B'C'$, אולם מתקיים $|C'D|=|AC'|$, ולכן התהליך לעולם לא יסתיים: חזרנו לאותה בעיה.

הבסיס ההיסטורי לסברה זו איננו מוצק.

[1] המערבית; לא נדון במתמטיקה מאיזורים אחרים בעולם, כמו סין, הודו ודרום אמריקה.

[2] דהיינו, סרגל שימדוד כל אחת מהצלעות במספר חלקים שלם.

[3] ב־Annals of Mathematics 46 (1945) עמ׳ 242–46, The Discovery of Incommensurability by Hippasus of Metapontum.

[4] כל זאת מטעמי סימטרייה – סיבוב ב־72°.

[5] נעיר כי אם מגדירים את B' להיות נקודת חיתוך האלכסונים, מתקבל $|AB|=|AB'|$ – הוכח!

ההצגה הטבעית לכל $0 < t < 1$ היא כשבר משולב, המוגדר על־ידי $t = \frac{1}{a_1+r_1}$ כאשר $a_1 = [\frac{1}{t}]$ ו־$r_1 = \frac{1}{t} - [\frac{1}{t}]$ ($0 < r < 1$) וחוזרים על התהליך עבור r_1. מקבלים לבסוף ביטוי מהצורה $t = \frac{1}{a_1+\frac{1}{a_2+\ddots}}$ ($a_i \geq 1$). הפיתוח סופי אם ורק אם t רציונלי.[6]

היחס של הצלע לאלכסון במחומש המשוכלל הוא, אם כן, המספר האי־רציונלי "הכי פשוט": השבר המשולב הפשוט ביותר הוא זה שעבורו $1 = a_1 = a_2 = \ldots$, והוא מתקבל כאן, שכן $1 < \frac{|AB|}{|AC|} = \frac{1}{2}$ והיות שהתהליך שביצענו זהה לתהליך פיתוח השבר המשולב וחזרנו בו לנקודת ההתחלה, מקרה זה מתקבל. כלומר, $t = \frac{1}{1+\frac{1}{1+\ddots}}$ ולמעשה $t = \frac{1}{1+t}$, כלומר $t^2 + t - 1 = 0$ ו־$t = \frac{-1+\sqrt{5}}{2}$.[7]

Wilbur Knorr[8] מייחס את גילוי המספרים האי־רציונלים לתיאון מסמירנה, שמתאר סדרה של זוגות מספרים להם הוא קורא "מספרי צלע" ו"מספרי אלכסון". מספרים אלה מיוצרים מהזוג $(1,1)$ על־ידי הנוסחאות $s_{n+1} = s_n + d_n$ ו־$d_{n+1} = d_n + 2s_n$: $\binom{1}{1}, \binom{2}{3}, \binom{5}{7}, \binom{12}{17}$. בסדרה זו, מתקיים

$$\begin{aligned} d_{n+1}^2 - 2s_{n+1}^2 &= (d_n + 2s_n)^2 - 2(s_n + d_n)^2 \\ &= d_n^2 + 4d_n s_n + 4s_n^2 - 2s_n^2 - 4s_n d_n - 2d_n^2 \\ &= 2s_n^2 - d_n^2 \\ &= (-1)(d_n^2 - 2s_n^2) \end{aligned}$$

היחסים בין הזוגות הללו נותנים קירובים ל־$\frac{\sqrt{2}}{2}$.

פרוקלוס (אמצע המאה החמישית לספירה), בפירושו על כתבי אפלטון, מסביר את המספרים הללו כך: הפיתגוראים הציעו את המשפט האלגנטי הבא על אלכסונים וצלעות, והוא, כאשר מוסיפים לאלכסון את הצלע ומוסיפים לצלע את פעמיים האלכסון, מקבלים צלע חדשה ואלכסון חדש.

הוא מפנה לספר השני של "היסודות" לאוקלידס, טענה 10:

$$(2a + b)^2 + b^2 = 2a^2 + 2(a + b)^2$$

(זו, למעשה, הזהות מקודם: $(2a + b)^2 - (a + b)^2 = 2a^2 - b^2$). לצידה מופיעה גם טענה 9:

$$(2a - b)^2 + b^2 = 2a^2 + 2(a - b)^2$$

(וגם כאן, אם מעבירים אגפים שוב מקבלים רקורסיה ששומרת על התחלפות הסימן, אך מקטינה את המספרים). מה היתה מטרת אוקלידס בניסוח טענות אלו?

כדי לבחון טענה זו, נתבונן בשרטוטים שבאמצעותם הוכיח אוקלידס את המשפטים האלו.[9]

[ציור 01.2]

[6] כמו־כן, על־ידי קטימת הצגה זו ניתן לקבל את הקירובים הרציונליים הטובים ביותר.

[7] על־ידי קטימת השבר המשולב הזה, מתקבלת סדרת פיבונאצ'י: $1, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}, \ldots$.

[8] ב־Rational Diameters and the DIscovery of Incommensurability, שפורסם ב־American Mathematical Monthly 1998 pp421–9.

[9] יש לציין שכל כתבי היד שידועים לנו מכילים את השרטוטים. Reviel Netz כתב ספר שדן בחשיבות השרטוטים בכתבים המתמטיים היווניים.

כאן, $AD = 2a + b$ ו־$DF = b$, ולפי משפט פיתגוראס, אגף שמאל שווה ל־$|AF|^2$, עבורו מתקיים $|AF|^2 = |AE|^2 + |EF|^2$. אך $|AE|^2 = 2a^2$ ו־$|EF|^2 = 2(a+b)^2$, ומכאן מתקבל הדרוש.

[ציור 9.2]

כאן, $|AF|^2 = |HF|^2 + |AH|^2 = (2a-b)^2 + b^2 = |AE|^2 + |EF|^2$, אך נשים לב ש־$|AE|^2 = 2(a-b)^2$ ו־$|EF|^2 = 2a^2$, ומתקבל הדרוש.

מצד שני, כפי שמראה קנור, ניתן לפתור את הבעיות בשרטוטים פשוטים בהרבה:]ציור[

אם כן, מדוע נותן אוקלידס הוכחה מסובכת? לשם כך יש לבחון את ההקשר בו מופיעות ההוכחות. בספר השני ישנם עוד משפטים דומים על ריבועים, ולמעשה זוהי גירסה גיאומטרית לבעיות ריבועיות מהסוג בו יש למצוא מספרים x ו־y כאשר נתונה מכפלתם xy וסכומם $x+y$. בכתב יתדות, למשל, מוצאים הרבה בעיות כנ״ל עם פתרונות.

22.5.2008 אם כן, אצל השומרים והבבלים היו שיטות לפתור בעיות מסדר שני מהצורה ״נתון סכום של שני מספרים ומכפלתם; מצא את שני המספרים״. ניתן לעקוב אחר שיטות אלה לפי (מאות) הלוחות שנמצאו.[10]

הטענות II.9,10 מתאימות לפתרון בעיות מהסוג ״נתון $x^2 + y^2$ ו־$x - y$; מצא את x ו־y״. מכאן, טוען קנור, הבנייה הלא־כל־כך טבעית. קנור טוען גם שאת הנוסחה למספרי אלכסון וצלע גילו על־ידי התבוננות בציור זה: אם מציבים $s = b$ ו־$d = a$, מקבלים מספרים שמתאימים למשולש הקטן יותר. לפי כך שיש רקורסיה, לא ניתן למדוד את ארכי הצלעות; קנור טוען שכאן גילו היוונים את האי־רציונליים.

1.2 חתכים חרוטיים

היוונים פיתחו גם את תיאוריית החתכים החרוטיים. כבר בזמנו של אוקלידס, במאה השלישית לפנה״ס, הכירו את תכונותיהם של האליפסה, ההיפרבולה, הפרבולה והמעגל. אפולוניוס כתב ספר שלם על כך, עם הרבה תוצאות (כנראה שלו).

ארכימדס, במאה השלישית לפנה״ס, הצליח לחשב שטחים ונפחים של כל מיני גופים. למשל, בהינתן פרבולה ומיתר בה, הוא ידע לחשב את השטח הכלוא בין הפרבולה ובין המיתר:

חוצים את המיתר ($AC = CB$). מעבירים ישר CM המקביל לציר הפרבולה[11] דרך C. מסמנים את נקודת החיתוך שלו עם הפרבולה ב־D.

משפט 1: השטח בין המיתר לפרבולה שווה ל־$\frac{4}{3}$ שטח המשולש ADB.

יש לציין שהיוונים לא הכירו כלל את המתמטיקה השומרית. אוקלידס היה בין הראשונים שספריו תורגמו להרבה לשונות. ספריו של ארכימדס היו מוכרים היטב ברנסנס, בזכות אוקלידס, בין היתר. EMXIF

[10] זו ככל הנראה מסורת עתיקת יומין להוגיע תלמידי בית־ספר בפתרון בעיות שלא ברור הצורך בפתרונן.

[11] פרבולה נוצרת על־ידי חיתוך מישור עם חרוט, שלו יש ציר סימטרייה EMXIF

שיטת ההוכחה של ארכימדס – שיטת המיצוי: קירוב השטח על־ידי מצולעים חוסמים וחסומים.[12]

אקסיומת ארכימדס: אם גודל a שונה מ־0, אז לכל גודל אחר b קיים n כך ש־$na > b$.

"על השיטה": ספר של ארכימדס שלא היה ידוע עד לפני כמאה שנים – מצאו אותו על קלף שנמחק וכתבו עליו מחדש בכנסיית הקבר בירושלים. זיהויו הוודאי של הספר נעשה על־ידי Heiberg. לאחר שהוא הוציא את הספר בתרגום לגרמנית (ואז תורגם לאנגלית), נעלם כתב היד שוב למשך כ־90 שנה, ואז מצאו אותו, מכרוהו במכירה פומבית ותרמוהו לאוסף כלשהו במרילנד.

הספר נכתב עבור ארתוסטנס, מגדולי המלומדים באלכסנדריה, שהיה אחראי על הספרייה בה. ארכימדס כתב: "מזמן שלחתי לך את המשפטים שמצאתי ... עכשיו אני רוצה לשלוח לך דברים נוספים ...".

לפי ארכימדס, אאודוקסוס הוכיח את .הוא טוען שכבר דמוקריטוס ידע על שיטת המיצוי.

ההוכחה של ארכימדס למשפט בדבר שטח הפרבולה מתבססת על מכניקה: אם יש מוט עם משקלות, שיווי משקל יתקבל אם מתקיים $aw = bv$.

ארכימדס "שוקל" את הפרבולה מצד אחד, ומצד שני את 4־פעמים שטח המשולש.

המשיק בנקודה D מקביל למיתר AB.

המשיק ב־B חותך את הישר CD בנקודה E כך ש־$DE = CD$. באופן כללי יותר, T נקודה שרירותית[13]; מעלים את הישר שמקביל לציר ומסמנים את נקודות החיתוך ב־S ו־R. היחס TS ל־TR שווה ליחס AT ל־AB.

ניקח קטע באורך ST ונשים אותו בצורה מקבילה כך שמרכזו ב־G. המרכז של RT נמצא בנקודה Q על הישר RT. מתכונות הפרבולה, $S'T'$ ו־RT בשיווי משקל ביחס למוט GB שנשען על הנקודה F, כי FA ו־TQ מקבילים. מכאן, הקטע של הפרבולה שרצינו לשקול נמצא בשיווי משקל עם המשולש ABH. ידוע שמרכז הכובד של משולש הוא במפגש התיכונים; המשולש כולו שוקל פי שלושה מהקטע של הפרבולה. מכאן, הקטע של הפרבולה שוקל כנגד $\frac{4}{3}$ המשולש ADB.

ניתן לראות בהוכחה זו את ניצני האינטגרציה.

יש לציין שארכימדס טען שזו לא הוכחה, אלא רק "דרך לגלות משפטים".

בגובה h יש עיגול ברדיוס r ששטחו πr^2. מצד שני, מהחרוט, πh^2. אז $\pi(r^2 + h^2) = \pi R^2$ בכל גובה. מכאן, נפח הכדור שווה ל־$\frac{2}{3}$ נפח הגליל החוסם אותו.

זה מזכיר את עיקרון Cavalieri (שנוסח לפני חשבון אינפיניטסימלי): אם אורך כל חתך שווה בין הגופים, שטחיהם שווים. מה שארכימדס באמת עושה כאן הוא להעביר את הכדור לחרוט כאשר הבסיס הוא מעגל ששטחו כשטח הכדור.

מי הכיר את זה?

מסתבר שהקהילה של המתמטיקאים בתקופת היוונים היתה מאוד קטנה; היו כמה בתי ספר ביוון ובאסיה הקטנה ומרכז בספרייה באלכסנדרייה, אבל לא בכל מקום בו לימדו שירה ורטוריקה לימדו גם מתמטיקה. עם זאת, בסופו של דבר המתמטיקה עברה לביזנטים ומשם לערבים ולמערב.

[12] מוכיחים, בין היתר, את הקשר בין שטח מעגל והיקפו (כלומר, השטח הוא רדיוס פעמים חצי ההיקף) בשיטה זו.

[13] לאו דווקא בין A ל־C, כמו ששורטט.

1.3 תורת המספרים

29.5.2008 מקורה של תורת המספרים בעולם ההלניסטי. עניינה הוא תכונות של מספרים שלמים.

כמה מספריו של אוקלידס מיוחדים לתורה זו. בפרט, הטענות הבאות:

VII.30: אם שני מספרים, כאשר כופלים אותם, נותנים מספר – ומספר ראשוני מחלק ("מודד") את המכפלה – אזי המספר הראשוני מחלק את אחד המספרים המקוריים.

VII.31: מספר שאיננו ראשוני מתחלק על־ידי מספר ראשוני.

משתי טענות אלו ניתן להוכיח את המשפט היסודי של תורת המספרים: כל מספר טבעי הוא מכפלה יחידה, עד כדי סדר, של מספרים ראשוניים.

אוקלידס איננו מוכיח ואף אינו מציין את המשפט היסודי. נראה שהכיר אותו, אך זה לא ודאי.

הנקודה העיקרית בהוכחת המשפט היא כזו: n שאיננו ראשוני מתחלק ב־n_1. אם גם הוא איננו ראשוני, אזי הוא מתחלק בראשוני. היחידות מוכחת תוך שימוש בטענה הראשונה.

בנייה נוספת שמוצאים אצל אוקלידס: IX.36: אם נציג את החזקות של 2 ונסכם אותן החל מ־1 עד שהסכום יתן מספר ראשוני ונכפול את הסכום בחזקה האחרונה, נקבל מספר מושלם. כלומר, אם $p = 2^k + \ldots + 2^1 + 1$ ראשוני, $n = p2^{k-1}$ מושלם – כלומר, $\sum d_i = n$ ל־n | $d_i \neq n$.

למשל, $6 = 1 + 2 + 3$ ו־$28 = 1 + 2 + 4 + 7 + 14$ מספרים מושלמים.

אוקלידס רק מראה שכל מספר מהצורה הנ"ל מושלם; אוילר, במאה ה־18, הוכיח שאם מספר זוגי הוא מושלם אזי הוא מהצורה $(2^k - 1)2^{k-1}$ כאשר $2^k - 1$ ראשוני.

הבדיקה האם יש מספר מושלם אי־זוגי מושארת כתרגיל לקורא.

1.4 קומבינטוריקה

עד לפני קצת יותר מעשר שנים, חשבו שרמת הקומבינטוריקה בתקופה ההלניסטית היתה מאוד בסיסית, על־סמך כך שלא שרדו ידיעות בנושא. אולם היו כמה שורות מסתוריות בכתביו של פלוטארכוס, שכתב בתיאור של ארוחת ערב כך: "כריסיפוס אומר שמספר הטענות המורכבות מ־10 טענות פשוטות הוא יותר ממיליון. היפארכוס אכן סתר את הטענה הזו על־ידי שהראה שבצד החיובי ישנן 103,049 טענות מורכבות, ובצד השלילי 310,952."

עד 1997, לא היה ידוע מה פשרם של מספרים אלו.

תלמיד אוניברסיטה בשם D. Hough בוושינגטון שם לב שהמספר הראשון הוא מספר שרדר העשירי – דבר מעניין, שכן כתוב שמדובר בעשר טענות. הוא מצא את הציטטה בספרו של Stanley וכתב אליו בנושא. המספר השני נותר תמוה.

לאחר כשנה, שמו לב כמה אנשים ש־$\frac{S(11)-S(10)}{2} = 310954$, כאשר $S(n)$ הוא מספר שרדר ה־n. יכול להיות שהיתה טעות בהעתקת כתביו של פלוטארכוס וזה אכן המספר שמופיע במקור. אולי זה קשור לכך ש־4 נכתב על־ידי Δ, ואילו המילה במקור היתה $\Delta v o$.

כך או כך, מאוחרי התגלית ישנה משמעות עמוקה יותר: לא קל להגיע למספר כזה על־ידי ספירת כל האפשרויות. כנראה היתה שיטת חישוב כלשהי. ודאי ששיטת חישוב זו לא היתה יעילה

כמו שהיטות המודרניות, אך עצם העובדה שהיוונים הגיעו למספרים הללו מעידה שידיעותיהם בקומבינטוריקה היו יחסית גבוהות.[14]

מהם מספרי שרדר?

שרדר היה מתמטיקאי מהמאה ה־19. המספרים הקרויים על שמו מייצגים את מספר הדרכים להקיף בסוגריים n סימנים שונים, כאשר מקיפים לפחות שניים (ומגדירים $S(1) = 1$). למשל, $S(2) = 1$ (כי $((x)(x)) = (xx)$), $S(3) = 3$ (האפשרויות הן (xxx), $(xx)x$, $x(xx)$).

הנוסחה הרקורסיבית לחישוב: $S(n) = \sum_{i_1+\ldots+i_k=n,k\geq 2} S(i_1)S(i_2)\ldots S(i_k)$.

יותר קל לחשב את $S(n)$ על־ידי פונקציות יוצרות. אחת הדרכים היא להגדיר $f(x) = S(1)x + S(2)x^2 + S(3)x^3 + \ldots + S(n)x^n$ (טור חזקות שמתכנס כש־x מספיק קטן ו־n לא גדול מדי: לבטח אין יותר סוגריים מאשר ביטויים, לכן ניתן לחסום את $S(n)$ למשל על־ידי $S(n) \leq 100^n$. חסם כזה אומר שיש רדיוס התכנסות לפונקציה).

כעת, ננסה לבטא את הנוסחה הרקורסיבית: $f(x)^2 = S(1)S(1)x^2 + (S(1)S(2) + S(2)S(1))x^3 + \ldots$ ו־$f(x)^3 = S(1)^3x^3 + (3S(1)^2S(2))x^4 + \ldots$ וכו׳. לא קשה לראות כי $f(x) = x + f(x)^2 + f(x)^3 + \ldots$.

נכתוב $z = f(x)$. אז $z = x + z + z^2 + \ldots = x + \frac{z^2}{1-z}$. מכאן, $z - z^2 = x - xz + z^2$, או $2z^2 - (1+x)z + x = 0$. מקבלים שצריך לפתח את $z = \frac{(1+x)-\sqrt{(1+x)^2-8x}}{4}$.

ניעזר בפיתוח $(1-t)^{\frac{1}{2}} = \sum_0^\infty \binom{\frac{1}{2}}{n}(-t)^n = 1 - \frac{1}{2}t - \frac{1}{8}t^2 - \ldots - (1-t)^k = \sum_0^k \binom{k}{j}(-t)^j$.[15]

מכאן, $f(x) = x + \sum_2^\infty S(n)x^n = \frac{1}{4}[1 + x - (\sum_0^\infty \binom{\frac{1}{2}}{n}(-6x+x^2)^n)]$ (כי $(1+x)^2 - 8x = 1 - (6x - x^2)$).

מספרי שרדר מתארים גם את מספר האפשרויות לעצים מישוריים כשכל קדקוד מתפצל לפחות פעמיים.

הטענות המורכבות מ־10 טענות פשוטות הן הדרכים לצירוף באמצעות סוגריים של 10 טענות, ועבור $\frac{S(10)+S(11)}{2}$ – מוסיפים למחרוזת של עשר הטענות שלילה בהתחלה – כשהשלילה מתייחסת לטענה המורכבת הראשונה; אם יש רק טענה אחת, שתי הדרכים מתלכדות. אז כל הדרכים להקיף את עשר הטענות הראשונות עם הטענה הראשונה שנשללה נותן את המספר הנ״ל.

1.5 האסכולה השימושית: הרון

5.6.2008 בניגוד לתיאורטיות (התבססות על אקסיומות והוכחות) של אוקלידס וארכימדס, **הרון** – במאה ה־I לספירה – ייצג את המתמטיקה השימושית יותר. דוגמה מוכרת: נוסחת הרון לשטח משולש, שאף שהוא כנראה לא גילה אותה, הופיעה בספרו ״מטריקה״ – עם הוכחה: בהינתן משולש שארכי צלעותיו a, b, c, נסמן $S = \frac{a+b+c}{2}$ ושטח המשולש הוא $\sqrt{S(S-a)(S-b)(S-c)}$.

[14] צריך להיזהר מלהסיק שדבר מסוים לא קיים אם לא מצאנו אותו: חוסר הידיעה שלנו לגבי ידיעותיהם לא אומר שהם לא ידעו.

[15] המקדם הבינומי השברי מוגדר על־ידי $\binom{k}{j} = \frac{k(k-1)\cdots(k-j+1)}{j!}$.

נוסחת **ברמגופטה** (מהמאה ה־8, הודו) מכלילה את נוסחת הרון: אם מרובע שצלעותיו a, b, c, d חסום במעגל, נסמן $S = \frac{a+b+c+d}{2}$ ושטח המרובע הוא $\sqrt{S(S-a)(S-b)(S-c)(S-d)}$.

1.6 המתמטיקה העברית

החיבור המתמטי הידוע הקדום ביותר בעברית הוא **משנת המידות**. זהו חיבור בן מספר עמודים שמשתמש במינוח ייחודי, שיש לו דמיון מסוים בחלק מהמונחים למונחים הערביים. בשנות ה־30, ש. גנץ הוציא לאור מהדורה של החיבור. הוא תיארך אותו למאה השנייה או השלישית לספירה וטען שהחיבור השפיע על הערבים. ב־1960, גד בן־עמי צרפתי טען, בהתבסס על ניתוח לשוני בין היתר, שהחיבור מהמאה השביעית או השמינית, ושכיוון ההשפעה הפוך.

2 המתמטיקה בימי הביניים

2.1 תנועת גרמי שמיים

2.1.1 סיבובים של המעגל

נתבונן ב־$R_\alpha : S^1 \to S^1$ (כש־S^1 מעגל היחידה) המוגדרת על־ידי $R_\alpha(e^{it}) = e^{i(\alpha+t)} = e^{i\alpha}e^{it}$. זהו סיבוב ב־$\alpha$.

אם α כפולה רציונלית של 2π, אזי ההעתקה מחזורית: $\alpha = \frac{p}{q}2\pi$ אזי $(R_\alpha)^q = R_{\alpha q} = id$.
אם α איננה כפולה רציונלית של 2π, אזי כל הנקודות $(R_\alpha)^n z_0$ שונות.

משפט 2 (קרונקר): אם α איננה כפולה רציונלית של 2π, אזי לכל z_0, הסדרה $(R_\alpha)^n z_0$ צפופה במעגל, כלומר בכל קטע z_1z_2 נמצא נקודות מצורה זו.

ב־1887, ניתנה גירסה $d \geq 1$־מימדית של המשפט; עבור $d = 1$, המשפט הופיע כבר במאמר של דיריכלה מ־EMXIF1842 עם הכללה, כאשר הוא מעיר שהמשפט הפשוט ידוע מזמן (לא ברור למה התכוון בזה).

משפט 3 (הכללה): נתונים מספרים ממשיים $\theta_1, \ldots, \theta_n$ כך שאם $u_0, \ldots, u_m$ שלמים מקיימים $u_0 + u_1\theta_1 + \ldots + u_m\theta_m = 0$ אזי לכל $0 \leq i \leq m$, $u_i = 0$.[16] אז לכל שלם s, קיימים שלמים $|u_i| \leq 2s$ כך ש־$0 < |u_0 + u_1\theta_1 + \ldots + u_m\theta_m| < \frac{1}{s^m}$.

דוגמה. כאשר $m = 1$, זה אומר שכפולות של θ_1 מתקרבות ל־0.

הוכחה. נסתכל על הביטויים $a_0 + a_1\theta_1 + \ldots + a_m\theta_m$ כאשר ה־a_i־ים, ל־$1 \leq i \leq m$, עוברים על המספרים $(-s, -s+1, \ldots, -1, 1, \ldots, +s)$. ישנם $(2s)^m$ ביטויים שונים כאלה; עבור כל בחירה כזו, ניקח a_0 כך שהסכום $0 < a_0 + a_1\theta_1 + \ldots + a_m\theta_m < 1$. אלו ה"יונים". כעת, נחלק את הקטע $(0, 1)$ לקטעים באורך $\frac{1}{(2s)^m}$. אלו ה"תאים". מספר היונים שווה למספר התאים.

אם יש שתי יונים בתא אחד,

[16] כלומר, אם מסתכלים על $\mathbb{R}$ כמרחב וקטורי מעל $\mathbb{Q}$, אזי $1, \theta_1, \ldots, \theta_m$ בלתי־תלויים.

$$0 < |(a_0 + a_1\theta_1 + \ldots + a_m\theta_m) - (a'_0 + a'_1\theta_1 + \ldots + a'_m\theta_m)| < \frac{1}{(2s)^m}$$

. אחרת, יש סכום בין 0 ל־$\frac{1}{(2s)^m}$.

2.1.2 ניקול אורזמי

ניקול אורזמי ניתח תנועת גרמי שמיים. הוא התעניין בנקודות המפגש בין שניים, ואחר־כך שלושה, גופים שמסתובבים בתנועה מעגלית קבועה – חישוב בעל השלכות אסטרולוגיות.

בספר הראשון, הוא מברר שאם שני גופים נעים במהירויות שונות עם מדד משותף ביניהן (כלומר, יחס רציונלי), אזי תהיה נקודת פגישה. (ההנחה בכל ספר I היא שיחס המהירויות רציונלי.)

טענה 4 (I.4): אם שני גופים נפגשים כעת, אזי הם בהכרח ייפגשו באותו מקום בזמנים אחרים.

הוכחה (בסימונים מודרניים). יהיו V_a, V_b המהירויות ויהי $\frac{V_a}{V_b} = \frac{p}{q}$ יחס המהירויות. אזי כאשר a יעבור q סיבובים שלמים, b יעבור p סיבובים שלמים, והם יחזרו לאותה נקודת מפגש.

בספר השני, הוא דן במקרה בו יחס המהירויות איננו רציונלי:

נסמן ב־d את נקודת המפגש הראשונה וב־e את נקודת המפגש השנייה. ההנחה שיחס המהירויות אי־רציונלי שקולה לכך שהזווית של הקשת ed איננה כפולה רציונלית של π: "לאחר מספר חזרות של הקשת de, המעגל הוקף בשלמותו, ונקודת המפגש נופלת בקשת de בנקודה g. הקשת בין נקודת המפגש השנייה והשלישית תיחתך באותה צורה, וכך הלאה, עד שלא תישאר קשת בין נקודות מפגש שארכה גדול מ־dg.[17]

"התהליך הזה ייִמשך ad infinitum ויחתוך את המעגל לקשתות יותר ויותר קטנות. לא תהיה קשת כל־כך קטנה במעגל כך שהיא לא תכיל נקודות מפגש עתידיות."

יש כאן ניסוח בהיר של משפט קרונקר שהוזכר קודם. השאלה היא האם זוהי הוכחה; לשם כך, דרוש מנגנון שיראה שארכי הקשתות שואפים ל־0. זה לא כל־כך מופיע כאן.

פון פלאטו ניסה למלא את החסר בהוכחה כך: ראשית, הוא טיפל במקרה ש־dg קטן מ־ge – אם חוזרים על התהליך, מגיעים בסופו של דבר למצב בו האורך המקסימלי של קשת בין נקודות הוא באמת dg. כך הקטנו את האורך הקשת המקסימלית ביותר מחצי. דבר דומה קורה גם כאשר dg גדול מ־ge, ומוביל למסקנה שאחרי מספר סופי של סיבובים, הקשת המקסימלית היא באורך קטן מ־$\frac{1}{2}de$.

בצורה כזו ניתן למלא את החסר. ספק רב אם אורזמה באמת חשב על כל זה באותה מידת דיוק: אין כאן, כמו אצל ארכימדס, הוכחה שהסדרה מתכנסת ל־0 (על־ידי כך שהוא מראה שהגודל קטן פי 2). עם זאת, הוא בהחלט הקדים את זמנו.

2.2 פתרון משוואות

בתיכון לומדים לפתור משוואות ממעלה ראשונה ושנייה. כבר לפני אלפי שנים, השומרים והבבלים ידעו לפתור בעיות ממעלה שנייה על־ידי הוצאת שורש. בעולם העתיק לא ידעו איך לגשת לבעיה

[17] יש כאן אי־דיוק, שכן לא בהכרח g מעבר לחצי הקשת de, ואז ge גדולה יותר; אורזמה כנראה מתעלם מכך.

כללית ממעלה שלישית.

במאה ה־16, היו פריצות דרך על־ידי מתמטיקאים כמו Cardano (מאבות תורת ההסתברות), Tartaglia, Ferroro ועוד, שמצאו דרך לפתרון משוואות ממעלה שלישית ורביעית.

באוניברסיטאות הראשונות, באיטליה, התעסקו בפתרון בעיות מתמטיות. כשהחלו לעסוק במשוואות ממעלה חמישית, ההתקדמות נעצרה – עד אשר התברר שבלתי־אפשרי למצוא פתרון באותה דרך.

12.6.2008 נתבונן ב־$x^2+ax+b=0$ ונחפש הזזה $x=y-s$ כך ש־$(y-s)^2+a(y-s)+b=0$, כלומר $y^2-(2s-a)y+s^2-as+b=0$. אם ניקח s כך ש־$2s-a=0$, אזי $y^2=as-b-s^2$ ואין ברירה אלא להוציא שורש ריבועי.

עבור משוואה ממעלה a 3 $= x^3$, אפשר באותו אופן להגיע ל־$x^3+px=q$. לראשונה התפרסם לכך פתרון כללי בספר של קרדנו Ars Magna (1545). באותן שנים לא היתה קביעות באוניברסיטאות האיטלקיות, לכן היו תחרויות בין מלומדים. מספר שנים לפני פרסום הספר, קרדנו שמע ש־Tantaglia מצא דרך כללית לפתרון בעיות ממעלה 3; הוא הפעיל לחץ כבד עליו כדי שיגלה לו את הדרך. הוא אכן גילה לו, אבל קרדנו נאלץ להבטיח שלא יפרסם את השיטה. באותם ימים תכנן לפרסם את הספר הנ״ל ורצה לכלול בו את הפתרון למשוואה ממעלה 3. הוא גילה שבין הכתבים של Scipio del Fero, שכבר מת, נמצא הכלל. אם כן, לטרטליה לא היתה בעלות על השיטה, וקרדנו פרסם את הנוסחה, שקרויה על שמו.

האסטרטגיה לפתרון המשוואות היא הכנסת משתנים נוספים, כדי להגיע למשוואה שבה יהיו רק חזקות 3. נתבונן במשוואה $x^3+px=q$ (מאפסים את החלק הריבועי על־ידי הזזת המשתנה). ננסה להציב $x=u-v$. נקבל

$$\begin{aligned}(u-v)^3+p(u-v) &= q\\ u^3-3u^2v+3uv^2-v^3+p(u-v) &= q\\ u^3-v^3-3uv(u-v)+p(u-v) &= q\\ u^3-v^3+(u-v)[p-3uv] &= q\end{aligned}$$

כדי לפשט את הביטוי נבחר u ו־v כך ש־$p=3uv$. אז $u^3-v^3=q$, ולכאורה אנו תקועים, אך נשים לב שמתוך הבחירה של u ו־v מתקיים $u^3v^3=\frac{p^3}{27}$, וכאן נכנס פתרון שכבר הבבלים ידעו – מכפלה והפרש של שני מספרים.

נסמן $s-t=q$, $st=\frac{p^3}{27}$. אם כן, $s^2-2st+t^2=q^2$ ואז $(s+t)^2=s^2+4st+t^2=q^2+\frac{4p^3}{27}$. אם כן, $s+t=\pm\sqrt{q^2+\frac{4p^3}{27}}$.

נקבל $x=u-v=\sqrt[3]{\frac{q}{2}+\frac{1}{2}\sqrt{q^2+\frac{4p^3}{27}}}-\sqrt[3]{\frac{q}{2}-\frac{1}{2}\sqrt{q^2+\frac{4p^3}{27}}}$.

בעיה! כאשר $q^2+\frac{4p^3}{27}$ שלילי, לא נוכל להוציא שורש; במקרה כזה, נקבל מספר מדומה, אבל עדיין פתרון ממשי למשוואה.

קרדנו מדבר על פתרון תרגילים כמו למצוא שני מספרים שסכומם 10 ומכפלתם 40. אם כן, $u+v=10$, $uv=40$. הוא כותב $(5+x)(5-x)=25-x^2=40$. אם כן, $x^2=-15$, כלומר $x=\pm\sqrt{-15}$. המספרים הם $5-\sqrt{-15}$ ו־$5+\sqrt{-15}$. קרדנו טוען שאין מספר שאם

נעלה אותו בריבוע נקבל -15, אבל משאיר את הכתיבה כך.[18] למעשה, עבור התרגיל הזה הפתרון הממשי קיים: $(\sqrt{65}+5)(\sqrt{65}-5) = 40$.

באותו ספר, קרדנו מצטט את הפתרון למשוואה ממעלה רביעית, אותו הוא לוקח מפרארי.

Colla שאל איך ניתן לחלק את 10 לשלושה מספרים ביחס מתמשך (כלומר, איך למצוא $a < b < c$ כך ש־$a+b+c=10$ ו־$\frac{b}{a}=\frac{c}{b}$). פרארי פתר את הבעיה הזו: נסמן את המספר האמצעי ב־x, ואז הראשון הוא $\frac{6}{x}$ והאחרון הוא $\frac{x^3}{6}$. מכך מקבלים $\frac{x^3}{x}+x+\frac{x^3}{6}=10$ ומכאן $x^4+6x^2+36x=60x$. נוסיף $6x^2$ לשני האגפים: נקבל $x^4+12x^2+36x=6x^2+60x$. נשלים לריבוע: $(x^2+6)^2=6x^2+6x$.

אילו באגף הימני היה ריבוע, היינו מוציאים שורש ומקבלים משוואה ריבועית. באופן כללי, גם כאן, כמו בבעיה הקודמת, הוסיפו פרמטר y:

$(x^2+6+y)^2=(x^2+6)^2+y^2+2y(x^2+6)=(6x^2+60x)+y^2+2y(x^2+6)$. נרצה שגם הביטוי באגף ימין יהיה ריבוע מושלם, לכן נתוב $(6+2y)x^2+60x+(y^2+12y)=$. התנאי לכך שביטוי זה יהיה ריבוע מושלם הוא שיתקיים $3600=4(y^2+12y)(6+2y)$.[19] פותרים את המשוואה ומוצאים y כך שאגף ימין הוא ריבוע מושלם; מוציאים שורש ומקבלים משוואה ריבועית עבור x.

לסיכום, השלבים הם – השלמה לריבוע באגף שמאל, הוספת פרמטר, השלמה לריבוע בעזרתו באגף ימין, פתרון משוואה ריבועית.

דרכי פתרון אלה הוכחו בסביבות 1540, אולם מאז לא פותחה האלגברה בכיוון זה. האנליזה התקדמה, היה פיתוח של סימנים וכיוצ״ב, אבל השאלה כיצד לפתור משוואות ממעלה 5 ומעלה נותרה פתוחה.

מי שתרם רבות למחקר בנושא היה לגראנז׳, שניתח את השיטות וגילה שמה שעומד מאחורי האפשרות לפתרון הוא מציאת פונקציות של השרשים שמקיימות משוואות ממעלה נמוכה יותר. הוא מתייחס למשוואה $x^3+ax^2+bx+c=0$; המקדמים מבטאים פונקציות סימטריות של השרשים r_1,r_2,r_3: $a=-(r_1+r_2+r_3)$, $b=r_1r_2+r_2r_3+r_3r_1$, $c=-r_1r_2r_3$.

ניוטון ואחרים ניתחו עוד קודם נוסחאות עבור סכום החזקות של השרשים: $r_1^2+r_2^2+r_3^2=a^2-2b$ (ניתן לחישוב ללא ידיעת השרשים עצמם).

גישת הפונקציות הסימטריות הובילה עד אשר אבל הוכיח בתחילת המאה ה־19 שלא ניתן למצוא פתרון של משוואה כללית מסדר חמישי על־ידי הוצאת שרשים. ההבנה של חיפוש פונקציות לשרשים איפשרה לגאוס בהמשך לחלק את המעגל ל־17.

19.6.2008 דיברנו על קרדנו ופררי ופתרונות של משוואות ממעלה שלישית ורביעית במאה ה־16 (בסביבות 1545). במרוצת השנים, הסימונים האלגבריים המוכרים לנו הוכנסו: ax^n+bx^{n-1} וכו׳.

דקרט מטפל באלגברה של ארכי קווים: היוונים התייחסו למכפלת ארכים כאל שטח, אך דקרט שם לב לבנייה שמאפשרת להגיע למכפלה: אם הישרים מקבילים, מקבלים $\frac{a}{e}=\frac{c}{b}$, כלומר $ab=$

[18] במובן הרחב; למעשה, הסימון שלו הוא $15 : m$ ל־-15, ושורש מסומן כ־℞. אז הכתיבה שלו היא $15 : m$ ℞ $: 5\varnothing$, $15 : m$ ℞ $: 5m$.

[19] כלומר, ל־$ax^2+bx+c=0$, מתקיים $b^2-4ac=0$.

ec, ואם נקבע e כיחידה, אזי המכפלה ab היא c.

בראשית המאה ה־17, הראשון (כנראה) שטן שתמיד לפולינום יש שורש היה Girard.

הזכרנו פונקציות סימטריות לשרשי פולינום ואת נוסחאות ניוטון:

נניח ש־$r_1, r_2, \ldots, r_d$ שרשים של פולינום

$$x^d - \sigma_1 x^{d-1} + \sigma_2 x^{d-2} - \ldots + (-1)^d \sigma_n = \prod_{i=1}^{d}(x - r_i)$$

(כאשר $\sigma_1 = \sum_1^d r_i$, $\sigma_2 = \sum_{1 \le i < j \le d} r_i r_j$ עד $\sigma_d = r_1 r_2 \ldots r_d$).

משפט: כל פולינום סימטרי במשתנים $r_1, \ldots, r_d$ הוא פולינום בביטויים $\sigma_1, \sigma_2, \ldots, \sigma_d$, ואם לפולינום המקורי מקדמים שלמים, גם לפולינום החדש מקדמים שלמים.

דוגמה. $s_k = \sum_{i=1}^d r_i^k$

$\prod_{i=1}^d (x - r_i) = \sum_{j=0}^d (-1)^j \sigma_j x^{d-j} = p(x)$, כאשר מגדירים $\sigma_0 = 1$. נתבונן ב־$\frac{p'(x)}{p(x)} = \sum_1^d \frac{1}{x - r_i} = \frac{\sum (-1)^j (d-j) x^{d-j-1}}{\sum (-1)^j \sigma_j x^{d-j}}$. עכשיו נחליף משתנה ל־$t = \frac{1}{x}$ ונקבל $\sum \frac{1}{1 - r_i t} = \frac{\sum_0^d (-1)^j (d-j) \sigma_j t}{\sum_0^d (-1)^j \sigma_j t^j} = \frac{A(t)}{B(t)}$. נפתח את אגף שמאל: נשים לב ש־

$$\sum_{i=1}^{d} \frac{1}{1 - r_i t} = \sum_{i=1}^{d} \sum_{k=0}^{\infty} (r_i t)^k = \sum_{k=0}^{d} (\sum_{i=1}^{d} r_i^k) t^k = \sum_{k=0}^{\infty} s_k t^k$$

אז $A(t) = B(t) \sum_0^\infty s_k t^k$. קיבלנו

$$(1 - \sigma_1 t + \sigma_2 t^2 + \ldots)(d + s_1 t + s_2 t + \ldots)^2 = d - (d-1)\sigma_1 t + (d-2)\sigma_2 t^2 + \ldots$$

באגף שמאל נקבל $d + (-d\sigma_1 + s_1)t + (d\sigma_2 - \sigma_1 s + s_2)t^2 + \ldots$, ומכאן $d = d$, $d\sigma_1 - s_1 = (d-1)\sigma$ (כלומר $s_1 = \sigma_1$); $d\sigma_2 - \sigma_1 s_1 + s_2 = (d-2)\sigma_2$ (כלומר $s_2 = \sigma_1^2 - 2\sigma_2$). קל לכתוב נוסחה כללית.

2.2.1 Lagrange, 1770/1

בזמנו היתה כבר הבנה טובה של שרשי יחידה;[20] ניתח בצורה עמוקה את פתרונותיהם של קרדנו ופררי.

קרדנו שם לב שאם a, b, c שרשים של $x^3 + px + q = 0$ ... . לגראנז׳ שם לב בנוסף שאם מתבוננים ב־$R = (a + \omega b + \omega^2 c)^3$ כאשר $\omega^3 = 1$, $\omega \neq 1$, הפונקציה הזו של a, b, c מקבלת רק שני ערכים שונים כאשר מבצעים תמורות של השרשים:

$$R = (\omega(a + \omega b + \omega^2 c))^3 = (\omega a + \omega^2 b + c)^3 = (\omega^2 a + b + \omega c)^3$$

(כי $\omega^3 = 1$) ו־

$$S = (a + \omega^2 b + \omega c)^3$$

(ועוד שתי תמורות), אבל $R + S$ ו־RS הן פונקציות סימטריות של השרשים, כי כל תמורה לא תשנה אותם. אלו ביטויים במקדמים p ו־q. חוזרים לנוסחאות קרדנו: $R + S = \pm(-27)q$, $RS = \pm(-3)p^3$. פותרים עבור R, S, מוציאים שורש שלישי וכו׳.

כעת נתבונן בפולינום ממעלה רביעית עם השרשים a, b, c, d. נסתכל על $u = ab + cd$. האפשרויות האחרות לביטויים מהצורה הזו הן $v = ac + bd$, $w = ad + bc$. ניתן לחשב אותם כשרשי פולינום

[20] פעל אחרי אוילר ודה־מואבר.

ממעלה 3: $(x-u)(x-v)(x-w)=x^3-(u+v+w)x^2+(uv+uw+vw)x-uvw$. המספרים u,v,w סימטריים, לכן ניתן לחשבם בהינתן השרשים a,b,c,d על־ידי כתיבה $(x-a)(x-b)(x-c)(x-d)=x^4+px^2+qx+r$ והתבוננות ב־p,q,r. אם יודעים מה ערכם של u,v,w, ניתן לבודד את מכפלות השרשים וקל לפתור את המשוואה המקורית: מידיעת $ab+cd$ ו־$r=abcd$ ניתן להגיע ל־ab ול־cd על־ידי פתרון משוואה ריבועית; כעת, אנו יודעים מהו $(a+b)+(c+d)=0$ (זה המקדם השלישי, שמתאפס) ו־$ab(c+d)+cd(a+b)=ab(-(a+b))+cd(a+b)=-q$. אנו כבר יודעים מהם ab ו־cd, לכן נוכל לקבל $\frac{-q}{ab-cd}=a+b$ (אם $ab\neq cd$).[21]

לגראנז׳ הראה שהמפתח לפתרון משוואות הוא על־ידי מציאת פונקציות של השרשים שמקבלות מספר ערכים קטן כשעוברים על כל התמורות של השרשים. תובנות אלו איפשרו לאבל ולגלואה להראות שבאופן כללי, אי־אפשר לפתור משוואות בעזרת הוצאת שרשים.

2.2.2 Gauss

ב־1801, פירסם ספר בשם Disquitiones Arithmeticae, בו בין היתר ניתח פתרון משוואות מהצורה $x^n-1=0$ בעזרת הוצאת שרשים ריבועיים. העניין בהוצאת שורש ריבועי חוזר לגיאו־מטרייה היוונית, שעסקה בבניות בעזרת סרגל ומחוגה. שלוש הבעיות הקלאסיות: ריבוע המעגל (כלומר, למצוא ריבוע ששווה בשטחו לשטח מעגל נתון); להכפיל את הקובייה (זוהי בעצם בניית $\sqrt[3]{2}$); לחלק זווית נתונה לשלוש זוויות שוות. הגירסה הדו־מימדית של שתי הבעיות האחרונות היו ידועות (הכפלת הריבוע - על־ידי בניית ריבוע חדש על אלכסון הריבוע המקורי; חציית זווית). דקארט שם לב שאפשר להוציא שורש על־ידי סרגל ומחוגה, מה שגם היוונים ידעו לעשות - אך קישר את זה עם אורך קטע .

היוונים ידעו, למשל, לבנות מחומש: זו בעצם הבעיה $x^5-1=x^4+x^3+x^2+x+1=0$; מחלקים ב־x^2 ומקבלים $\frac{1}{x^2}+\frac{1}{x}+1+x+x^2=0$. נסמן $y=x+\frac{1}{x}$, ואז $y^2=x^2+2+\frac{1}{x^2}$ ומקבלים $y^2+y-1=0$. שאלות הבנייה מצטמצמות לשאלה עבור אלו ראשוניים p ניתן לחלק את המעגל ל־p חלקים שווים על־ידי סרגל ומחוגה, שהרי על־ידי משולש וריבוע, למשל, ניתן לבנות מצולע בן 12 צלעות. גאוס גילה שעבור ראשוניים מהצורה $2^{2^a}+1$ ניתן לבצע את החלוקה.[22]

משפט Gauss: אם $p=2^{2^p}+1$, ניתן לפתור את $x^p-1=0$ על־ידי סדרת הוצאת שרשים ריבועיים.

דוגמה. $p=2^4+1=17$

[21] לגראנז׳ הסתכל על ביטויים עם שרשי יחידה גם כאן, אבל זה יותר מורכב.

[22] פרמה הראה שמספר מהצורה 2^m+1 ראשוני רק אם ל־m אין גורם אי־זוגי: למשל, $2^{5m}+1=(2^m)^5+1=(2^m+1)(\ldots)$ (כי $x^5+1=(x+1)(x^4-x^3+x^2-x+1)$). פרמה חשב ש־$2^{32}+1$ ראשוני, אך אבוי! וילר גילה ש־$4294967297=641\cdot 6700417$. לא ידועים ראשוניי פרמה נוספים מלבד $2^1+1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1$.

מעט רקע נחוץ מתורת המספרים

נסמן על־ידי ρ שורש של x^17-1, $\rho \neq 1$. כל השרשים הם $\rho, \rho^2, \ldots, \rho^{16}$. הפולינום שאנו בעצם מנסים לפתור הוא $x^{16}+x^{15}+\ldots+1$ – פולינום ציקלוטומי.

פולינומים ציקלוטומיים נקראים כך על־שום שהם מחלקים את המעגל: עבור n, זהו $\Phi_n(x) = \prod_{\{r_j \text{ : primitive n−th root of unity}\}}(x-r_j)$. r שורש פרימיטיבי מסדר n אם $r^n=1$ אך $r^k \neq 1$ לכל $1 \leq k < n$. למשל, עבור x^4-1, השרשים הם $-i, +1, -1, 1$; השרשים הפרימיטיביים הם $-i, +i$ ולכן $\Phi_r(x) = x^2+1$. עוד דוגמאות: $\Phi_2(x) = x+1$, $\Phi_1(x) = x-1$. ניתן להוכיח כי $\Phi_p(x) = x^{p-1}+x^{p-2}+\ldots+1$ עבור p ראשוני.

מקדמי Φ_i שלמים: $(x^n-1) = \prod_1^n(x-r_i)$ כאשר r_i הם כל שרשים, כי כל שורש פרימיטיבי.[23]

לדוגמה, $x^n-1 = \Phi_n(x)\prod_{\{d|n,d<n\}}\Phi_d(x)$: $x^6-1 = (x^3+1)(x^3-1) = (x+1)(x^2-x+1)(x-1)(x^2+x+1) = \Phi_2\Phi_6\Phi_1\Phi_3$.

באינדוקציה, לפולינום Φ_d מקדמים שלמים־מתוקנים.

המעלה של Φ_n היא $\varphi(n)$ – מספר ה־a־ים כך ש־$(a,n)=1$. $n = \sum_{d|n}\varphi(d)$.

כתרגיל, לכל p ראשוני יש שורש פרימיטיבי g במובן ש־$(g,p)=1$ ו־$g, g^2, \ldots, g^{p-1}$ עוברים על כל המספרים $1, 2, \ldots, p-1$ מודולו p. (הפתרון דומה לפירוד של x^n-1.)

קונגרואנציות מודולו n: $a \equiv b \pmod n$ אם $a-b$ מתחלק ב־n. 26.6.2008

משפט 5 (פרמה): אם p ראשוני ו־$a \not\equiv 0 \pmod p$, אזי $a^{p-1} \equiv 1 \pmod p$.

מכתב שנכתב על־ידי פרמה ל־Frénicle, 1640: פרניקל שאל את פרמה האם יש מספר מושלם בעל עשרים ספרות או יותר, $2^{p-1}(2^p-1)$ כאשר 2^p-1 ראשוני. היה צריך לברר את הראשוניות של $2^{37}-1$. כלומר, $2^{37} \equiv 1 \pmod q$ וצריך לברר האם q ראשוני. אבל $2^{q-1} \equiv 1 \pmod q$, ואם כך קל לראות ש־37 חייב לחלק את $q-1$. אז $74k = q-1$, כלומר q צריך להיות מהצורה $74k+1$.

Dickinson — History of the Theory of Numbersאבן עזרא, מאה 12: 6 "מספר השווה בחלקיו". טען שבכל מערכת מספר יש מספר מושלם אחד (אך טעה בזאת). (נמצא בפירוש שלו לספר שמות, פרק ג': "אהיה אשר אהיה".)

פרמה כתב שהוכיח את המשפט, אך טעה. ההוכחה של אוילר למשפט פרמה התבוססה על העובדה שכל המקדמים הבינומיים $\binom{p}{k}$ ל־$1 \leq k \leq p-1$ מתחלקים ב־p: $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. מכאן, לכל a, $(a+1)^p - a^p - 1 \equiv 0 \pmod p$ ולכן $(a+1)^p-(a+1) \equiv a^p - a \pmod p$. כאשר $a=1$, אגף ימין מתאפס, ולכן באינדוקציה, לכל a, $a^p - a = (a^{p-1}-1) \equiv 0 \pmod p$ ואם $a \not\equiv 0 \pmod p$ אפשר לחלק ב־a.

[23] כדי ששורש לא יהיה פרימיטיבי, צריך שהחזקה הראשונה שתאפס אותו תחלק את n, וזה לא קורה עבור $k<n$ אם n ראשוני.

מכאן מגדירים: a שייך למעריך d אם $a^d \equiv 1 \pmod p$, אבל לכל $1 \le d' < d$, $a^{d'} \not\equiv 1 \pmod p$. מוכיחים ש־$d$ מחלק את $p-1$, כי אם לאו, $(p-1,d) = e < d$ ואפשר לכתוב $e = u(p-1)+vd$ ל־u ו־v שלמים, ואז $a^e = a^{u(p-1)+vd} = (a^{p-1})^u(a^d)^v \equiv 1 \pmod p$.

משפט 6: לכל p, אפשר למצוא מספרים ששייכים למעריך $p-1$. (מספרים אלה נקראים **שרשים פרימיטיביים**.)

הוכחה. נניח ש־a שייך למעריך d. מבין d המספרים $a^0, a^1, \dots, a^{d-1}$ מודולו p, נשאל כמה שייכים למעריך d. מבין החזרות האלו, רק חזקות כך ש־a^f כך ש־f זר ל־d יהיו שייכים למעריך d, כי אם $(f,d) = e > 1$, על־ידי כפולה f הקטנה מ־d נקבל כפולה של d, $(a^f)^{d'} = (a^d)^{e'} \equiv 1 \pmod p$, $d' < d$. לכן אם נזכור את הסימון של אוילר $\varphi(d)$ מספר ה־$1 \le e < d$ כך ש־$(e,d) = 1$, קיבלנו שבין החזקות $a^1, a^2, \dots, a^{d-1}$ לכל היותר $\varphi(d)$ מספרים פותרים את $a^{d-1} \equiv 1 \pmod p$.

נסמן על־ידי $\psi(d)$ את מספר ה־a־ים הקטנים מ־p ושייכים למעריך d. קיבלנו $\psi(d) = 0$ או $\psi(d) = \varphi(d)$, כי כל הפתרונות למשוואה $x^{d-1} \equiv 1 \pmod p$ נמצאים ברשימה $a, a^2, \dots, a^{d-1}$ כי כולם שונים ומספרם $d-1$, ולמשוואה $x^d \equiv 1 \pmod p$ יש לכל היותר d פתרונות, כי ל־$a_kx^k + a_{k-1}x^{k-1} + \ldots + a_0 \equiv 0 \pmod p$ לכל היותר k פתרונות שונים ב־$0, 1, \dots, p-1$.

אנו מעוניינים לקבל $a^{d-1} \equiv 1 \pmod p$. $\sum_{d|p-1}\varphi(d) = p-1$ ו־$\psi(d) \le \varphi(d)$ לכל $d \mid p-1$, ו־$\sum_{d|p-1}\psi(d) = p-1$. מכאן נובע הדרוש.

דוגמה. $\frac{1}{12}, \frac{2}{12} = \frac{1}{6}, \frac{3}{12} = \frac{1}{4}, \frac{4}{12} = \frac{1}{3}, \frac{5}{12}, \frac{6}{12} = \frac{1}{2}, \frac{7}{12}, \frac{8}{12} = \frac{2}{3}, \frac{9}{12} = \frac{3}{4}, \frac{10}{12} = \frac{5}{6}, \frac{11}{12}, \frac{12}{12} = 1$

$$12 = \varphi(12) + \varphi(6) + \varphi(4) + \varphi(3) + \varphi(2) + \varphi(1)$$

כעת נניח ש־p מהצורה $2^{2^k}+1$, למשל $17 = 2^{2^2}+1$. מתעניינים במשוואה $x^{17}-1=0$ במספרים מרוכבים. $x^{17}-1 = (x-1)(x^{16}+x^{15}+\ldots+x+1)$. נסמן על־ידי z שורש פרימיטיבי של היחידה, כלומר z שפותר את $x^{17}-1$ אך לא $x^a-1=0$ עבור $a<17$. גאוס בוחר בשורש הפרימיטיבי 10 מודולו 17. הוא כותב $1, 10, 15, 14, 4, 6, 9, \ldots$.

נרשום שני מחזורים: $\eta_1 = z^1+z^{15}+z^4+z^9+z^{16}+z^2+z^{13}+z^8$, $\eta_2 = z^{10}+z^{14}+z^6+z^5+z^7+z^3+z^{11}+z^12$. אז $\eta_1+\eta_2=-1$. $\eta_1\eta_2 = 4\eta_1+4\eta_2=-4$. $\eta_1\eta_2a.......$. אז $\eta_1, \eta_2 = \frac{1}{2}(-1\pm\sqrt{17})$, $\eta_1' = z+z^4+z^{16}+z^{13}$, $\eta_2' = z^{15}+z^9+z^2+z^8$, $\eta_3' = z^{10}+z^6+z^7+z^11$, $\eta_4' = z^{14}+z^5+z^3+z^{12}$, $\eta_1'+\eta_2'=\eta_1$, $\eta_3'+\eta_4'=\eta_2$, $\eta_1'\eta_2' = \eta_1'+\eta_2'+\eta_3'+\eta_4' = -1$

גאוס לא הראה כי כאשר p איננו מהצורה $p = 2^{2^k}+1$ לא ניתן לפתור את המשוואה $z^p-1 = 0$ על־ידי סדרה של הוצאת שרשים ריבועיים (הוא הראה את הכיוון ההפוך). Wantzel הראה זאת ב־1837.

2.2.3 לנדאו

בין הכתבים של לנדאו, 28.6.1897, נמצאה הוכחה קצרה לכך שאי־אפשר לחלק זוית כללית לשלושה חלקים שווים על־ידי סרגל ומחוגה: בספר של L. Bieberbach, Theorie der Geometrischen Kenstracktionen. תוצאה זו סותמת את הגולל על שתי הבעיות הקלאסיות של היוונים.

הבעיה השלישית של היוונים – ריבוע המעגל: קשורה לחישוב של π. Lambert הראה בסביבות 1770 ש־π איננו רציונלי, אך לא ענה על השאלה האם ניתן לקבלו על־ידי בנייה בעזרת סרגל ומחוגה. בשנות השמונים של המאה ה־19, Hermite ו־Lindensam הראו ש־$e = \sum_0^\infty \frac{1}{n!}$ ו־π אינם מספרים אלגבריים, כלומר אינם פותרים שום משוואה אלגברית מעל הרציונלים.

ליוביל, בסביבות 1840, הוכיח ש־$\sum_1^\infty \frac{1}{10^{n!}}$ אינו אלגברי.

יש הרבה שאלות פתוחות בדבר רציונליות ואלגבריות מספרים: האם πe רציונלי? האם קבוע אוילר $\gamma = \lim(\ln n - \sum_1^n \frac{1}{k})$ אלגברי?

3.7.2008 רופיני, אבל וגאוס פיתחו את התורה שאיפשרה להוכיח שלמשוואות ממעלה 5 או גבוהה יותר אין פתרון כללי.

גאוס כותב, ללא הוכחה, שפרט לחלוקות הנובעות מחלוקת המעגל ל־p חלקים ($p = 2^{2^k} + 1$ ראשוני) וחציית זווית, אי אפשר לחלק את המעגל ל־m חלקים שונים. הראשון שהוכיח זאת היה Wantzel, 1837.

E. Landau נתן ב־28/6/1897 הוכחה ("חדשה") לכך שאי־אפשר לחלק זווית לשלושה חלקים שווים בעזרת סרגל ומחוגה.

בבסיס, כל בנייה בעזרת סרגל ומחוגה בונה ארכים של ישרים שניתן לקבל מאורך נתון (1) על־ידי ארבע פעולות החשבון ($+, -, \times, \div$) והוצאת שורש ריבועי (דקארט הראה זאת כבר במאה ה־17). העובדה שרק ביטויים כאלו מתקבלים נובעת מהעובדה שחיתוך מעגל וישר או חיתוך שני מעגלים הוא פתרון משוואות ריבועיות.

לחלק זווית לשלושה חלקים, בהינתן $a = \sin\varphi$, זו בעיית מציאת $x = \sin\frac{\varphi}{3}$, והנוסחאות הטריגונומטריות מובילות ל־$4x^3 - 3x + a = 0$. בנייה תוביל אונו לסדרת גדלים $y_1, y_2, \dots, y_s$ כאשר $y_{i+1}^2 = P_i(y_1, \dots, y_s, a)$, כאשר P_i פונקציה רציונלית ב־$y_1, \dots, y_s, a$. אך y_{i+1} איננו בשדה מעל $\mathbb{Q}$ הנוצר על־ידי $y_1, \dots, y_s, a$.

בסופו של דבר, פתרון מתקבל בצורה $x = \alpha + \beta y_s$ כאשר α ו־β ב־$P(a, y_1, \dots, y_{s-1})$ (בסימוניו, השדה מעל $\mathbb{Q}$ שנוצר על־ידי $a, y_1, \dots, y_{s-1}$). אז בהכרח גם $\alpha - \beta y_s$ פותר את המשוואה: ל־$f(x) = 4x^3 - 3x + a$, $0 = f(\alpha + \beta y_s) = A + By_s$ כאשר A ו־B ב־$P(a, y_1, \dots, y_{s-1})$. אם $B \neq 0$, אזי $y_s = -\frac{A}{B}$, ואז y_s היה נמצא ב־$P(a, y_1, \dots, y_{s-1})$, בניגוד להנחה. אז גם $A - By_s = 0$ ולכן $f(\alpha - \beta y_s) = 0$ ולכן $\beta \neq 0$ ולכן $\alpha + \beta y_s \neq \alpha - \beta y_s$. סכום שלושת השרשים של $f(x) = 0$ הוא 0, ולכן -2α הוא שורש של המשוואה. $\alpha \in P(y_1, \dots, y_{s-1}, a)$. אילו α היה מהצורה $\alpha' + \beta' y_{i+1}$ כאשר $\alpha', \beta' \in P(y_1, \dots, y_i, a)$, אז באותה צורה היינו מקבלים שגם $\alpha' - \beta' y_{i+1}$ הוא שורש, והיינו מקבלים ארבעה שרשים של $f(x) = 0$. זה בלתי אפשרי, ולכן -2α ביטוי רציונלי ב־a. אבל קל לראות של־$f(x)$ אין שורש

שהוא פונקציה רציונלית של a.

דוגמה. עבור $a = \frac{1}{2}$, $4x^3 - 3x + \frac{1}{2} = 0 \iff 8x^3 - 6x + 1 = 0$; נחליף משתנה ל־$u$ $2x =$ ונקבל $u^3 - 3u + 1 = 0$. זו משוואה אי־פריקה מעל הרציונלים (אם היה לה פתרון ברציונלים, היה לה כבר פתרון בשלמים, לפי הלמה של גאוס, וזה אינו קורה).

בסביבות 1770, Lambert הוכיח ש־π איננו רציונלי. ההוכחה מתבססת על הפיתוח של $\tan^{-1} x$ כשבר משולב כללי. מאות שנים לפני כן, היו טענות דומות, אך לא ידעו להוכיח זאת. Liouville גילה שיש מספרים שאינם פותרים אף משוואה אלגברית עם קדמים שלמים. הוא הוכיח זאת בכמה דרכים; אחת מהן:

משפט 7 (1851): אם x (אי־רציונלי) פותר משוואה אי פריקה מעל השלמים ממעלה $n \geq 2$, אזי קיים $A > 0$ ולכל $\frac{p}{q}$ ($(p,q) = 1$) מתקיים $|\frac{p}{q} - x| > \frac{1}{Aq^n}$.

דוגמה. מספר כמו $\theta = \frac{1}{10} + \frac{1}{10^2} + \ldots + 110^{n!} + \ldots$ איננו אלגברי, כי $\theta - \sum_1^n \frac{1}{10^{k!}} = \frac{1}{10^{(n+1)!}}(1 + \frac{1}{10} + \ldots)$, כלומר $|\theta - \sum_1^n \frac{1}{10^{k!}}| \leq \frac{2}{10^{(n+1)!}}$, וקל לראות שזה סותר את המשפט.

הוכחה. נניח ש־$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$. אז אם x_0 הוא שורש של f, $f(\frac{p}{1}) = f(x_0) + f'(\xi)(\frac{p}{q} - x_0) = 0$ ולכן $\frac{p}{q} - x_0 = \frac{f(\frac{p}{q})}{f'(\xi)}$. בגלל ש־$x_0$ איננו שורש כפול (מאי־פריקות f), $f'(x_0) \neq 0$ ומקבלים חסם תחתון A ל־$|f'(\xi)|$.

כעת, $a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \ldots + a_0 = \frac{z}{q^n}$ ל־z שלם; אז $|\frac{p-q}{-}x_0| \geq \frac{1}{A} \cdot \frac{\text{int}}{q^n} \geq \frac{1}{Aq^n}$.

Liouville: θ אלגברי ממעלה n, אז $|\frac{p}{q} - \theta| \geq \frac{c}{q^n}$. Thue 1900 שיפר את הקבוע ($\frac{n}{2}$). Siegel 1925 הוריד ל־$\sqrt{n}$. Roth, 1955: $|\frac{p}{q} - \theta| \geq \frac{c}{q^{2+\varepsilon}}$ לכל $\varepsilon > 0$.

Hermite הראה ב־1872 ש־e איננו אלגברי. Lindemann הוכיח ב־1878 ש־π איננו אלגברי.

3 חשבון אינפיניטסימלי

ראשית החשיבה האינפיניטסימלית נמצאת בשיטה של ארכימדס לחישוב השטח מתחת פרבולה באמצעות חלוקתה לישרים.

גזירות, חישוב שטחים וכו' העסיקו את המתמטיקאים החל מראשית המאה ה־17. Barrow – קודמו של ניוטון בקיימברידג' – כבר ניסח גירסה גיאומטרית של המשפט היסודי, שניסוחו המודרני הוא $\int_a^b f'(t)dt = f(b) - f(a)$. ניוטון ולייבניץ, באופן בלתי־תלוי, התחילו את הפיתוח הפורמלי.

במאה ה־18, ברנולי, אוילר ועוד התמקדו בפיתוחים פורמליים, כאשר היסודות לא תמיד היו ברורים דים.

ל־$k \geq 2$, $\sum \frac{1}{n^k} < \infty$; אוילר מצא ש־$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \text{rational} \cdot \pi^{2k}$ (למעשה מספר ברנולי). לדוגמה, $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

בשנות ה־70, Apery הוכיח ש־$\sum_1^\infty \frac{1}{n^3}$ אי־רציונלי במאמר שכותרתו The Proof that Euler Missed (לא הסתמך על פיתוחים מאוחרים). בעשור האחרון היו התקדמויות נוספות בחקר $\sum \frac{1}{n^k}$ ל־k אי־זוגי.

3.1 ברנרד בולצאנו, 1848־1781

ב־1817, פרסם ספרון בו הוכיח בצורה מדויקת למדי את המשפט שאם פונקציה רציפה מקבלת ערכים חיוביים ושליליים אזי היא מתאפסת ביניהם (משפט ערך הביניים).

משפט: למשוואה אלגברית ממעלה אי־זוגית יש תמיד שורש ממשי.

במאה ה־18 נימקו זאת בצורה אינטואיטיבית; בולצאנו ניסה להוכיח את המשפט.

בסעיף 7, נקודה חלשה –

משפט: אם לסדרת גדלים $F_1x, F_2x, \ldots, F_nx, \ldots, F_{n+r}x$ יש התכונה שההפרש בין F_nx ו־$F_{n+r}x$ קטן מכל גודל נתון לכל r ו־n מספיק גדול, אזי יש ערך קבוע יחיד שביטויי הסדרה יתקרבו אליו בכל דרגת קרבה אם ממשיכים מספיק רחוק.

משפט זה בעצם אומר שלסדרת קושי יש גודל יחיד. ההוכחה, במילים, היא שניתן לתת קירובים טובים יותר ויותר לגודל ולכן הגבול יחיד, ולכן קיים גודל ממשי ששווה לגבול הזה. זו נקודה חלשה, כי הוא איננו מפתח את בניית הישר הממשי כמשהו שמקיים את התכונה הזו.

בולצאנו מעיר שלמרות שמתקרבים יותר ויותר, אפשר שהגבול יהיה רציונלי, ומדגים זאת עם $0.1, 0.11, \ldots$ (הגבול הוא $\frac{1}{9} = \frac{\frac{1}{10}}{1-\frac{1}{10}} = \frac{1}{10} + \frac{1}{10^2} + \ldots$).

בסעיף 12, **משפט:** אם תכונה M איננה מתקיימת עבור כל ערכים של משתנה x אבל כן מתקיימת עבור כל הערכים הקטנים מ־u מסוים, אזי קיים U שהוא הכי גדול בין אלו שניתן לומר עליהם שהתכונה מתקיימת לכל $x < U$.

משפט זה בעצם אומר שאם קבוצה $E \subset \mathbb{R}$ מקיימת $E \neq \mathbb{R}$ וקיים u כך ש־$(-\infty, u) \subset E$, אזי קיים U כך ש־$(-\infty, U) \subset E$ אך לכל $u' > U$, $(-\infty, u') \not\subset E$.

הוכחה. גלל ש־M מתקיים לכל $x < u$ אך לא לכל x, יש $D > 0$ כך ש־M איננו מתקיים לכל $x < u + D$. נשאל האם M מתקיים לכל $x < u + \frac{D}{2^m}$. זה איננו נכון עבור $m = 0$; אם לכל m זה איננו נכון, אזי $u = U$.

אחרת, יש m כך ש־M מתקיים לכל $x < u + \frac{D}{2^m}$. זה יוצר סדרה שמקיימת את המשפט מסעיף 7.

הוא מעיר שהניסוח "אם M ... אזי יש מספר גדול ביותר עבורו תכונת M מתקיימת" איננו נכון, כיוון שהסופרמום לא חייב להיות חלק מהקבוצה.

[חסר קצת] 10.7.2008

משפט 8 (סעיף 15): אם שתי פונקציות של x, fx ו־φx, משתנות ברציפות לכל x (או לכל x בין α ו־β $[\alpha, \beta]$), ואם $f\alpha$ ...

הוכחה. ... $\varphi x < fx$ – התכונה M. יש $\omega > 0$ קטן מספיק כך שלכל $\alpha = x < a + \omega$ M מתקיימת (בגלל הרציפות של f, φ). לעומת זאת, עבור β התכונה הנ״ל איננה מתקיימת, כי עבור $0 < \omega$ מספיק קטן, $f(\beta+\omega) > \varphi(\beta+\omega)$, ולכן מהמשפט יש U הכי גדול שמקיים את התכונה, וקל לראות שעבור U מתקיים $fU = \varphi U$.

משפט 9 (סעיף 17): כל פונקציה מהצורה $a + bx^m + c6n + \ldots + px^r$ שבה $m, n, \ldots, r$ הם מספרים שלמים חיוביים היא רציפה.

משפט 10 (סעיף 18): אם פונקציה מהצורה $fx = x^n + ax^{n-1} + bx^{n-2} + \ldots + px + q$ חיובית עבור $x = \alpha$ ושלילית עבור $x = \beta$, אזי למשוואה $fx = 0$ יש לפחות שורש ממשי אחד בין α ו־β.

הוכחה. מפוצלת למקרים לפי סימני α ו־β.

3.2 משפט שוויון הנגזרות החלקיות

ראשית נעיר כי לא תמיד $f_{xy} = f_{yx}$. יש כל מיני דוגמאות נגדיות: למשל, $f(x,y) = y^2 \arctan \frac{x}{y} - x^2 \arctan \frac{y}{x}$ בנקודה $(0,0)$, או $g(x,y) = xy\frac{x^2-y^2}{x^2+y^2}$ (או משהו דומה). עם זאת, אף מתמטיקאים מכובדים כברנולי וכאוילר נתנו הוכחות שהתעלמו מהדוגמאות הנגדיות, ואף במאה ה־19 המשיך הדבר, עד אשר שוורץ ניסח תנאים נכונים והוכיח את המפשט כהלכה.

בתחילת המאה ה־18, ברנולי הסתכל על משפחת עקומים והתבונן במשיקים ב־x, $x + \Delta x$, y_α, $y_{\alpha'}$,

בולצאנו מדבר על פונקציות רציפות בכלל ולא רק על טורי חזקות, אם כי דוגמאות הוא נותן רק על־ידי טורי חזקות; לגראנז׳ הוכיח ב־1772 את המשפט כאשר הניח שלפונקציה f יש פיתוח כטור חזקות $f(x,y) = \sum c_{n,m}x^ny^m$. הנחה זו הופכת את המשפט לברור, כי אז מתקיים $f_{yx}(0,0) = c_11 = f_{xy}(0,0)$ – ניתן לקבל נגזרות על־ידי גזירת הטור. אבל לא כל הפונקציות הן כאלה.

בניגוד למאה ה־18 בה הדגש היה על החישובים, במאה ה־19 הקפידו על פורמאליות. ב־Cours d'analyse של קושי (182X), הוא טוען שאם f פונקציה של כמה משתנים ורציפה בכל משתנה, אזי f רציפה גם כפונקציה של כמה משתנים: כלומר, כאשר α, β, γ אינפיניטסימלים, $f(x+\alpha, y+\beta, z+\gamma, \ldots) - f(x,y,z,\ldots)$ אינפיניטסימלי.

ההוכחה שהוא נותן היא

$$\begin{aligned} f(x+\alpha, y+\beta, z+\gamma_1, \ldots) - f(x,y,z,\ldots) &= f(x+\alpha, y, z, \ldots) - f(x,y,z,\ldots) \\ &\quad + f(x+\alpha, y+\beta, z, \ldots) - f(x+\alpha, y, z, \ldots) \\ &\quad + f(x+\alpha, y+\beta, z+\gamma, \ldots) - f(x+\alpha, y+\beta, z, \ldots) \\ &\quad + \ldots \end{aligned}$$

אבל אמנם $f(x+\alpha, y+\beta, z, \ldots) - f(x+\alpha, y, z, \ldots)$ שואף ל־0 כש־α קבוע, אך זה לא בהכרח המצב כש־α משתנה (ידיעת ההשתנות בכיוון הצירים לא בהכרח מקנה גם את ידיעת

ההשתנות בכיוונים האחרים: למשל, עבור הפונקציה

$$f(x,y) = \begin{cases} \frac{xy}{x^2+y^2} & (x,y) \neq 0 \\ 0 & x=y=0 \end{cases}$$

על הישרים $y = ax$, $\frac{ax^2}{x^2+ax^2} = \frac{a}{1+a^2}$, כלומר הנגזרת הכיוונית בכיוון הישרים האלו מתאפסת, בעוד שעל $y=0$, $x=0$ היא אינה מתאפסת).

קושי, בהוכחה זו מ־1823, מסתמך על רציפות נגזרות שונות בלי לציין במפורש. לינדלוף, ב־1867, נתן דוגמאות נגדיות. שוורץ נתן ב־1873 את ההוכחה המדויקת הראשונה תחת התנאים הבאים:

משפט 11: $f_{xy}(x,y) = f_{yx}(x,y)$ לכל (x,y) בתחום ההגדרה אם f_x, f_y, f_{xy}, f_{yx} כולם קיימים ורציפים בתחום.[24]

הוכחה. $\Delta_{h,k}f = (f(x+h,y+k)f(x+h,y)) - (f(x,y+k) - f(x,y)) = (f(x+h,y+k) - f(x,y+k)) - (f(x+h,y) - f(x,y))$. כלומר, יש שתי דרכים לראות את ההפרש. בראשונה מביניהן, נקבע את $y, y+k$ ונחשוב על הביטוי כפונקציה של x: $F(x+h) - F(x)$. לפי משפט ערך הביניים, $F(x+h) - F(x) = hF'(x+\theta h)$. אם כן, קיים $0 < \theta < 1$ (התלוי ב־$y, y+k$) כך ש־$\Delta_{h,k}f = h[f_x(x+\theta h, y+k) - f_x(x+\theta h, y)]$. נשתמש פעם נוספת במשפט ערך הביניים: $= hkf_xy(x+\theta(y,k)h, y+\theta'(x+\theta h,y)k)$, $0 < \theta' < 1$. לכן $\frac{\Delta_{h,k}}{hk} = f(x+\theta h, y+\theta' k)$.

חשבון דומה בהסתמך על הדרך השנייה לכתיבת $\Delta_{h,k}f$ מביא אותנו לנוסחה $\frac{D_{hk}}{hk} = f_{yx}(x+\varphi h, y+\varphi' k)$, $0 < \varphi, \varphi' < 1$.

מרציפות נובע $f_{xy}(x,y) = f_{yx}(x,y)$.

אם $f(x,y) = u(x) + v(y)$, $\Delta_{h,k}f \equiv 0$. לכן $0 = \frac{\Delta_{h,k}f}{hk}$ $\lim_{(h,k)\to(0,0)}$. הנגזרת הראשונה $\frac{f(x+h)-f(x)}{h}$, $f''(x) = \lim_{h\to 0}\frac{h(x+h)-2f(x)+f(x-h)}{h^2}$

3.3 טורים טריגונומטריים

17.7.2008 $\frac{\partial^2 y}{\partial x^2}\alpha^2 = \frac{\partial^2 y}{\partial t^2} L$=זמן

d'Alembert (1752): $f(x+\alpha) + \varphi(x-\alpha t)$ עבור φ ו־f פונקציות כלליות של משתנה אחד.

כבר D. Bernoulli מצא צורה אחרת: $y = \sum a_n \sin(\frac{n\pi x}{l})\cos(\frac{n\pi\alpha(t-\beta_n)}{l})$.

$y = u(x)v(t)$. $\frac{\partial^2 y}{\partial x^2} = u''(x)v(t)$ $\frac{\partial^2 y}{dt^2} = u(x)v''(t)$ $\alpha^2 u''v = uv'' = \frac{u(x)}{(u''(x)}$

$-K^2 = \alpha^2\frac{v(t)}{v''(t)}$ אז $u + K^2u'' = 0$. אחד הפתרונות: $u(x) = \sin Kx$.

כאשר $t = 0$, $y(x,0) = \sum a_n \sin(\frac{n\pi}{l}x)$ – תנאי התחלה.

פורייה חקר את התפשטות החום והגיע למשוואת החום $\frac{\partial y}{\partial t} = C\frac{\partial y}{\partial x^2}$.

האם ניתן לרשום פונקציה שרירותית כסכום טור טריגונומטרי? למשל, פונקציה אי־זוגית $f(x)$: האם $f(x) = \sum_1^\infty a_n \sin nx$, ואם כן, מהם a_n?

[24] הוא מוכיח גם שמספיק להניח קיום ורציפות של f_{xy} בלבד.

ניתן לכתוב, עבור b_k ידועים,

$$\sum_0^\infty b_k x^{2k+1} = \sum_1^\infty a_n(\sum_{k=0}^\infty (-1)^k \frac{(nx)^{2k+1}}{(2k+1)!}) = \sum_{k=0}^\infty(\sum_{n=1}^\infty a_n n^{2k+1})(-1)^k \frac{x^{2k+1}}{(2k+1)!}$$

אם כן, $b_k = \frac{(-1)^k}{(2k+1)!}\sum_{n=1}^\infty a_n n^{2k+1}$ ל־$k=0,1,2,\dots$. זו מערכת אינסופית של משוואות לינאריות עבור המקדמים הלא־ידועים a_n. פורייה מציע לקטום ב־N ולהסתכל רק על N המשוואות הראשונות $b_k = \frac{(-1)^k}{(2k+1)!}\sum_{n=1}^N a_n n^{2k+1}$, $k=0,1,\dots,N-1$. הוא משנה את אגף שמאל עבור N ומקבל ביטוי למקדמים $a_n(N)$ ומזהה את הגבול כאינטגרל $a_n = \frac{1}{\pi}\int_{-\pi}^{\pi}\sin nx f(x)dx$.

פורייה לא נתן הצדקות בספרו. בספרו Divergent Series, הארדי נותן פירוט של התנאים בהם ניתן להצדיק את הצעדים.

אם כן, עבור פונקציה רציפה אי־זוגית על π, $-\pi$ ניתן להגדיר את a_n כך. האם מתקיים $f(x) = \sum_1^\infty a_n \sin nx$, ובפרט, האם הסכום מתכנס?

הראשון שהוכיח שבתנאים מסוימים אכן התשובה חיובית היה דיריכלה, 1829, שהראה זאת ל־f גזירה.

ההגדרה של רימן לאינטגרל של פונקציה "כללית" ניתנה בעבודה הזאת,[25] וגם דוגמאות לפונקציות אינטגרביליות שאינן רציפות בכל נקודה רציונלית בקטע $[0,1]$.

$a_1\sin x + a_2\sin 2x + a_3 \sin 3x + \dots$ $\qquad$ $\frac{1}{2}b_0 + b_1\cos x + b_2\cos 2x + b_3\cos 3x + \dots$

נגדיר $A_0 = \frac{1}{2}b_0$, $A_n = a_n \sin nx + b_n \cos nx$. נסמן את הטור $\Omega = A_0 + A_1 + \dots$ ואת הערך $f(x)$, שמוגדר רק היכן שהטור מתכנס.

כדי שהטור יתכנס, צריך להתקיים $A_n \to 0$. בהמשך הוא מניח שגם a_n ו־b_n שואפים לאפס, וזה מבטיח שלכל x, $A_n \to 0$; כנראה לא הכיר את המשפט הבא, שממילא מבטיח זאת:

משפט 12 (Cantor, 1870): אם $A_n(x)$ שואף ל־0 לכל x, אזי גם a_n וגם b_n שואפים ל־0.

$F(x) = C + C'x + A_0\frac{x^2}{2} - A_1 - \frac{A_2}{4} - \frac{A_3}{9} - \dots - \frac{A_n}{n^2}$ (האינטגרל השני של $f(x)$).

$F(x)$ פונקציה רציפה.

ל־$\alpha > 0$, $\frac{F(x-2\alpha)-2F(x)+F(x+2\alpha)}{4\alpha^2} = A_0 + A_1(\frac{\sin\alpha}{\alpha})^2 + A_2(\frac{\sin 2\alpha}{2\alpha})^2 + \dots = *$

נחשב: $\sin n(x+2\alpha) = \sin nx\cos 2\alpha + \sin n(x-2\alpha) = \sin nx \cos 2\alpha - \cos nx \sin 2\alpha$

$-2\sin nx = -2\sin x\cos nx \sin 2\alpha$

$2\cos 2\alpha - 2 = 2w\cos 2\alpha = 2\cos^2\alpha - 2\sin^2\alpha = 2 - 2\sin^2\alpha\, 2(\sin nx)(\cos 2\alpha - 1)$

$-4\sin^2\alpha$

כאשר $\alpha \to 0$, $(\frac{\sin n\alpha}{n\alpha})^2 \to -1$. רימן מראה שאם הטור מתכנס, כלומר אם $A_0 + A_1 + \dots + A_n \to f(x)$, אזי $*$ שואף ל־$f(x)$ כאשר $\alpha \to 0$.

[25] עד אז השתמשו בהגדרה של קושי - $\int_0^1 f(x)dx = \lim_{n\to\infty}\frac{1}{n}\sum_{k=0}^{n-1} f(\frac{k}{n})$. הגדרה זו טובה לפונקציות רציפות.

תרגיל: אם $\lim_{n\to\infty} u_n \to \overline{u}$ אזי גם (סכימת צ׳זארו) $\lim_{n\to\infty} \frac{1}{n}\sum_1^n u_i = \overline{u}$ וגם (סכימת אבל) $\lim_{r\nearrow 1}(1-r)\sum_0^\infty r^n u_n = \overline{u}$.

מכאן רימן קיבל תנאים המבטיחים את התכנסות הטור.

שאלת קנטור: אם לכל x $A_0 + A_1 + \ldots + A_n \to 0$, האם זה גורר שכל המקדמים a_n ו־b_n מתאפסים? (זו בעצם שאלת היחידות.)

התשובה חיובית. כחלק מההוכחה, הוא הראה שהם לפחות שואפים ל־0 (צוטט קודם כמשפט קנטור). ההוכחה לכך: לכל $x \in (-\pi,\pi)$, $\lim_{n\to\infty} a_n \sin nx + b_n \cos nx = 0$. האסטרטגיה: להראות שבהינתן סדרה $n_k \to \infty$, יש תת־סדרה כך ש־$a_{n'_k} \to 0$, $b_{n'_k} \to 0$. נכתוב $\sqrt{a_n^2+b_n^2}(\frac{a_n}{\sqrt{a_n^2+b_n^2}} \sin nx + \frac{b_n}{\sqrt{a_n^2+b_n^2}} \cos nx) = \sqrt{a_n^2+b_n^2}(\cos\theta_n + \sin\theta_n) = \sqrt{a_n^2+b_n^2}\sin(nx+\theta_n)$ (ניתן למצוא θ כזו כי סכום הריבועים הוא 1).

בהינתן $n_k \nearrow \infty$, נמצא תת־סדרה n'_k ו־x_0 כך ש־$|\sin(n'_k x_0 + \theta_{n'k})| \geq \frac{1}{10}$. עבור N גדול, הקבוצה $\{x \in (-\pi,\pi) \ : \ |\sin(Nx+\theta_N)| \geq \frac{1}{10}\}$ נראית כך:

אם $\{x \in (-\pi,\pi) \ : \ |\sin(10Nx+\theta_{10N})| \geq \frac{1}{10}\}$, רק צריך לדאוך לכך שבתת־סדרה $n'_{k+1} \geq 10n'_k$ ואז ניתן למצוא סדרה יורדת של קטעים בתוך $(-\pi,\pi)$ כך שעל הקטע ה־n'_k כל הביטויים $|\sin n'_i + \theta_{n'_i}| \geq \frac{1}{k}$ לכל הקודמים. הנקודה x_0 היא חיתוך הקטעים האלו.

בזה קנטור הוכיח את המשפט שאם לכל x $a_n \sin nx + b_n \cos nx \to 0$, אזי $a_n^2 + b_n^2 \to 0$.

כעת, כדי להוכיח את משפט היחידות, הוא היה צריך לדעת כיצד להוכיח

24.7.2008 כעת קנטור מצטט את המשפט שרימן הוכיח: בהנחה ש־$a_n^2+b_n^2 \to 0$, רימן הגדיר $F(x) c_1 x + c_0 - \sum_1^\infty \frac{a_n}{n^2}\sin nx + \frac{b_n}{n^2}\cos nx$ (ה־a_i־ים חסומים). הטור הזה מתכנס במידה שווה ומגדיר פונקציה רציפה F. התכנסות הטור המקורי גוררת כי $\lim_{\alpha\to 0}\frac{F(x-\alpha)-2F(x)+F(x+\alpha)}{\alpha^2} = 0$ לכל x.

כעת, כדי להוכיח את היחידות, הוא היה צריך לדעת כיצד להוכיח

טענה: אם עבור פונקציה רציפה $F(x)$ מתקיים שלכל x, $\lim_{h\to 0}\frac{F(x+h)-2F(x)+F(x-h)}{h^2} = 0$, אזי בהכרח קיימים קבועים כך ש־$F(x) = c + c'x$.

הוא נתקע בהוכחה, ופנה לשוורץ לבקש את עזרתו. הוא נתן לקנטור הוכחה של הטענה, שבעצם מוכיחה טענה חזקה יותר:

טענה 13: אם F רציפה ולכל x, $\lim_{\alpha\to 0}\frac{F(x-\alpha)-2F(x)+F(x+\alpha)}{\alpha^2} \geq 0$, אזי F קמורה. כאשר הגבול מתאפס, היא גם קעורה, ולכן היא חייבת להיות לינארית.

הוכחה. פירושה של קמירות הוא $F(\frac{u+\theta}{2}) \leq \frac{F(u)+F(\theta)}{2}$.

נניח בשלילה שישנם $u_0 < \theta_0$ כך ש־$F(\frac{u_0+\theta_0}{2}) > \frac{F(u_0)+F(\theta_0)}{2}$. נוסיף ל־$F$ פולינום מהצורה $\varepsilon x^2 + bx + c$ כך ש־$G(x) = F(x) + \varepsilon x^2 + bx + c$ מתאפס ב־u_0 וב־θ_0 וכן $G(\frac{u_0+\theta_0}{2}) > 0$.

הוספנו ל־F פונקציה כך ש־F מתאפסת ב־u_0, θ_0. G מקבלת מקסימום בקטע הפתוח (u_0,θ_0) כי היא חיובית באמצע ומתאפסת בקצוות. יהי w מקסימום. בנקודה זו מתקיים $\lim_{\alpha\to 0}\frac{G(w-\alpha)-2G(w)+G(w+\alpha)}{\alpha^2} \geq 2\varepsilon$. עבור α מספיק קטן, מקבלים סתירה (כי $G(w-\alpha)-G(w) \leq 0$ ו־$G(w+\alpha)-G(w) \leq 0$, מכך ש־w מקסימום).

קצת אחרי שהוכיח את המשפט הזה, הוא פרסם אותו ב־Mathematische Annalen ב־1872: "על הרחבה של משפט מטורים טריגונומטריים".

בסעיף הראשון, הוא נתן הגדרה של הממשיים כגבולות של סדרות של רציונליים (זו הבנייה המפורסמת שגירסתה המודרנית היא במשפט שלכל מרחב מטרי (X,d) יש מרחב מטרי שלם $(\hat{X},\hat{d})$ יחיד כך שניתן לשכן את X ב־$\hat{X}$).

בסעיף השני, הראה שניתן להחליש את ההנחה על הטור $\frac{1}{2}b_0+\sum A_n(x)$ לכך שהטור מתכנס ל־0 לכל x, למעט מספר נקודות סופי: אם יש כמה נקודות יוצאות מן הכלל, אז בקטעים הפתוחים ביניהן, נובע שיש פונקציות לינאריות שונות. כדי להראות שזה "מתיישר" לפונקציה לינארית אחת, הוא השתמש בטענה שאם $a_n^2+b_n^2\to 0$ אזי $\lim_{\alpha\to 0}\frac{F(x-\alpha)-2F(x)+F(x+\alpha)}{\alpha}=0$ לכל x.[26] לפיכך, הנגזרת ב־x מימין ומשמאל משתוות (שהרי ניתן לפרק את הסכום ולקבל $\frac{F(x+\alpha)-F(x)}{\alpha}-\frac{F(x-\alpha)-F(x)}{-\alpha}\to 0$).

טיעון זה תקף עבור מספר סופי של נקודות. אם יש קבוצת נקודות אינסופית שמתכנסת לגבול, אפשר לוותר גם עליה. אך על כמה נקודות אפשר לוותר? קנטור חיפש משפט כללי מהצורה "אם הטור $\lim\sum_1^N A_n(x)=0$ לכל x שאיננו בקבוצה E, אזי כל המקדמים מתאפסים". (הקבוצה E נקראת **קבוצת יחידות**.)

ההכללה הובילה את קנטור למושג הסודרים.

קנטור התחיל עם המספרים הרציונליים (zahlen). אחר־כך הוא רצה להרחיב זאת לגדלים מספריים (כלומר, סדרות מתכנסות של רציונליים). כשהוא רוצה לדבר על נקודה על הישר, הוא ממקם על הישר את הרציונליים ומתבונן בגבולות של סדרות ברציונליים (תוך שימוש בכך שלכל גודל מספרי – כלומר, לכל סדרה מתכנסת – קיימת נקודה יחידה על הישר). לנקודות על הישר הוא קורא punkte.

כעת, קנטור מגדיר נקודת גבול: תהא P קבוצת נקודות, כלומר קבוצה על הישר. **נקודת גבול** (grenzpunkt) של P היא נקודה x שבכל סביבה שלה $(x-h,x+h)$ יש אינסוף נקודות מ־P.

כל נקודות גבול של P מהוות קבוצה שנקראת P'. הקבוצה P'' נגזרת מ־P'. אם $P^{(\nu)}$ מתקבלת אחרי ν צעדים, נקרא ל־P "קבוצה מטיפוס ν". הקבוצה P' היא מטיפוס $\nu-1$ וכו'.

במאמר הוא מוכיח את המשפט הבא:

משפט 14: אם הטור מתכנס ל־0 לכל נקודה x שאיננה בקבוצה P מטיפוס ν, אזי כל המקדמים $a_n,b_n=0$.

ההוכחה בשלבים, כאשר הבסיס הוא $0=\lim\frac{F(x-\alpha)-2F(x)+F(x+\alpha)}{\alpha}\quad\forall x$.

קנטור שם לב לעובדה כי קבוצת נקודות הגבול של הקבוצה המקורית P מכילה את נקודות הגבול של הסדרה $\dots\supset P''\supset P'$. נגדיר $P^\infty=\bigcap P^{(\nu)}$. אחרי ה־$\infty$, אפשר גם להגדיר $P^{\infty+1}=(P^\infty)'$. כאן קנטור הגיע לרעיון שניתן לספור אחרי ה־∞ הראשון.

[26] כאן במכנה יש α, לא α^2.

לא קשה להוכיח שלכל סודר α בן־מניה יש קבוצה P ב־$(0,1)$ כך ש־P^{α} סופי אך P^{β} אינסופי לכל $\beta < \alpha$.

31.7.2008 אם כן, ההכללה הביאה את קנטור להגדיר סודרים מעבר ל־ω שהוא הסודר המתאים $\{1, 2, 3, \dots, \}$. $P^{(\omega)}$ חיתוך של כל ה־$P^{(v)}$, $P'^{(\omega)} = P^{(\omega+1)}$.

ב־1873 הוכיח שלמספרים הממשיים אין מניה – כלומר, אי־אפשר לרשום אותם כסדרה $u_1, u_2, \dots$ שתכלול את כל הממשיים בקטע (α, β) כלשהו. באותו מאמר הוא הראה שלמספרים האלגבריים יש מנייה, ולכן יש מספרים "לא אלגבריים" – את המספרים האלגבריים אפשר למנות (משפט של ליוביל).

ההוכחה שקנטור נתן: נניח כי $u_1, u_2, \dots$ הם כל המספרים בקטע (α, β). נגדיר $\alpha' = u_1$, $\beta' = u_{i_1}$. ניקח כ־α'' את ה־u_i הראשון אחרי u_1 כך ש־α'' נמצא בקטע (α', β'), ו־$\beta'' = u_{i_2}$ המספר הראשון שגדול מ־α'' ונמצא בקטע (α', β'). נמשיך כך ונקבל סדרת קטעים $\alpha' < \alpha'' < \dots < \beta'' < \beta'$

יהי $a = \lim \alpha^{(\nu)}$, $b = \lim \beta^{(\nu)}$. הטענה היא שכל נקודה בקטע $[a, b]$ איננה ברשימה (ואם $a = b$, אז זו נקודה שלא בקטע): אם היא היתה ברשימה, היינו בוחרים בה.

הוכחה זו חיזקה אצל קנטור את השאיפה לחקור את האינסוף. שאלה טבעית: האם כל קבוצה אינסופית E או ניתנת לרשימה כסדרה או נמצאת בהתאמה חח"ע עם הקטע כולו? קנטור שיער שזה המצב (**השערת הרצף**) והוכיח זאת עבור קבוצות סגורות. עד היום זו בעיה פתוחה.

3.4 משפט Cantor-Bendixon

הגדרה: קבוצה E של ממשיים תיקרא מושלמת אם כל נקודה ב־E היא נקודת הצטברות של E, ולהיפך. כלומר, $E' = E$.

כל קבוצה סגורה E ב־$\mathbb{R}^d$ היא איחוד קבוצה מושלמת וקבוצה בת מניה.

פורסם ב־Acta Mathematica vII, 1883, שנערך בתחילה על־ידי Mittag-Leffler, שעל־שמו קרוי מכון מתקדם למתמטיקה בשטוקהולם.

בנדיקסון העמיד את קנטור על טעות בניסוח המשפט; הוא נתן דוגמה נגדית, ניסוח נכון והוכחה, שמבוססת על השיטות של קנטור.

משפט קנטור המקורי: אם ל־P' עצמה מהסוג השני (כלומר, P' איננה בת־מניה), אזי את P' ניתן להציג בצורה יחידה כאיחוד $P^{(1)} \equiv R + S$ (כלומר, $R \cup S$) ול־S, R התכונות הבאות: R, לאחר תהליך חוזר של גזירה מגיעים ל־$R^{(\gamma)} \equiv 0$ (כלומר, אין בה נקודות), כאשר γ סודר בן־מניה (סודר מטיפוס ראשון – סופי – או שני – בן־מניה); R כזאת היא "פריקה" (reductibel). S, לעומת זאת, מקימת $S^{(1)} = S$ והיא נקראת מושלמת (perfecte).

הדוגמה הנגדית:

לוקחים E_1 סדרת נקודות באמצע הקטעים שמשמיטים בבנייה של קבוצת קנטור. לכל נקודה כזאת מצרפים סדרה מתכנסת, E_2. אם $P = E_2$, $P' = E_1 \cup C$, כאשר C היא קבוצת קנטור

– קבוצת כל המספרים מהצורה $C = \{\sum_1^\infty \frac{e_n}{3^n}\}$ ($e_n \in \{0,2\}$). C קבוצה מושלמת. $E_1' = C$ גם־כן.

קנטור בסוף מאמרו תיקן את הניסוח המקורי לטענה $P^{(1)} = R+S$ וקיים γ כך ש־$\mathcal{D}(R, R^{(\gamma)}) = 0$ (חיתוך שתי הקבוצות; איחוד = $\mathcal{M}(A,B)$, איחוד זר = $A+B$).

לכל הקטעים אותה עצמה – ל־$\mathbb{R}^n$ ול־$\mathbb{R}^d$ אותה עצמה.

קנטור שאל, ולמעשה שיער, שכל קבוצה חלקית ל־$\mathbb{R}$, אם איננה בת מניה, היא מעצמת $\mathbb{R}$. (זו **השערת הרצף**.)

משפט Cantor-Bendixon מוכיח את השערת הרצף עבור קבוצות סגורות ב־$\mathbb{R}$.

בעקבות השערת הרצף, פותחה תורת הקבוצות התיאורית, 1916 ואילך: סוסלין הוכיח את השערת הרצף עבור קבוצות בורל (σ־אלגברה של קבוצות ב־$\mathbb{R}$ הנוצרת על־ידי הקבוצות הפתוחות) על־ידי המצאת מערכות סוסנין, קבנוצות אנליטיות.

Gōdel הוכיח ב־1938-40 שאם מוסיפים את השערת הרצף ואת אקסיומת הבחירה לאקסיומות של תורת הקבוצות של צרמלו־פרנקל (ZF), אזי אם לא הגענו לסתירה לפני ההוספה, לא נגיע לסתירה לאחר ההוספה.

ב־What is the Continuum Hypothesis, הוא טען שחייבת להיות תשובה להשערת הרצף.

1963, P. Cohen: גם אם נשלול את השערת הרצף ואת אקסיומת הבחירה לא נגיע לסתירה חדשה.

כלומר, השערת הרצף ואקסיומת הבחירה בלתי־תלויים באקסיומות צרמלו־פרנקל של תורת הקבוצות.

4 כמה מילים על השערת רימן

Gauss ספר כמה ראשוניים ישנם עד n. אם נכנה את מספרם ב־$\pi(n)$, $\pi(8) = 4$, $\pi(20) = 8$.

גאוס חישב את זה ל־n־ים גדולים יחסית וקיבל קירוב: $\pi(n) \approx \frac{n}{\log}$.

ברטרנג, בסביבות 1840, שיער שלכל n, בין n ל־$2n$ נמצא מספר ראשוני.

צ׳בישף (סביבות 1860) הוכיח שישנם קבועים C_1, C_2 כך שלכל n, $C_1 \frac{n}{\log n} \leq \pi(n) \leq C_2 \frac{n}{\log n}$, והראה שאם למנה $\frac{\pi(n)}{\frac{n}{\log n}}$ יש גבול, אזי הגבול שווה ל־1.

אוקלידס כבר הוכיח שיש אינסוף ראשוניים. אוילר נתן הוכחה אנליטית לכך, שהיתה מבוססת על הטור $\zeta(z) = \sum_1^\infty \frac{1}{n^z} = \prod_p \frac{1}{1-\frac{1}{p^z}}$.[27] – מתבסס על כך שלכל n יש פירוק יחיד למספרים ראשוניים. הטור מתכנס כאשר $\mathbb{R}z > 1$. כאשר $z \searrow 1$, הטור $\sum \frac{1}{n} = +\infty$ ולכן גם המכפלה $\prod_p \frac{1}{1-\frac{1}{p}}$ מתבדרת, מה שאינו אפשרי אם יש מספר סופי של ראשוניים.

רימן פיתח נוסחה פונקציונלית עבור הקשר בין $\zeta(z)$ ו־$\zeta(1-z)$, $\Gamma(z)$ וכו׳, והראה מהנוסחה שאפשר להגדיר את $\zeta(z)$ כפונקציה (מרומורפית) אנליטית בכל $\mathbb{C}$, והראה שאם נדע שכל האפסים

[27] אוילר גם מצא ש־$\zeta(2n) = B_{2k}\pi^{2k}$ ל־$B_{2k} \in \mathbb{Q}$.

של $\zeta(z)$ נמצאים על הישר $\mathbb{R}(z)=\frac{1}{2}$ (ציר הסימטרייה בנוסחה הפונקציונלית), נדע את ההתנהגות של $\pi(n)$ בצורה מאוד מדויקת.

Hadamard, Poussin בסביבות 1895 הוכיחו שאכן $\lim_{n\to\infty}\pi(n)/\frac{n}{\log n}=1$ על־ידי כך שהראו שאין ל־$\zeta(z)$ אפסים על הישר $\mathbb{R}(z)=1$.

$\pi(n)=\frac{n}{\log n}+O(n^{\frac{1}{2}+\varepsilon})$ לכל $\varepsilon>0$ $\iff$ השערת רימן.