

שאלות פתורות וסתומות בתורת המספרים האלמנטרית.

בשמחה רבה נענית לבקשה החביבה להרצות על אחד הנושאים משדות החקירה שלי והנני בוחר בפרק המתמטיקה אשר קושיותיו מובנות בנקל למו שאינו מבקעל המקצע. קושיות אלו עולות מאליהן בבואנו לחשב במספרים הרגילים הטבעיים 1,2,3, ... אין פוגשים בשברים ומה גם במספרים אירציונליים בשאלות הללו; השאלות מובנות איפוא אפילו למו שאינו בעל מקצע ואשר שכח כבר את המתמטיקה של בית הספר. אך ממחר אני להוסיף שפתרון של שאלות רבות, העולות כאילו מאליהן והנראות לקלות מאד, לא הושג אפילו בעזרת כל אמצעי-העזר של המתמטיקה המודרנית ולמרות התאמצותם של גדולי המתמטיקונים של כל עמי התבל. למטרת הרצאתי זו יאה, כמובן, שלא להביא את ההוכחות אפילו לשאלות הפתורות. רוצה אני להביא לפניכם שאלות אחרות במספרים שלמים, שאלות פתורות וסתומות אשר נקל להבונן.

המושג מספר ראשוני ידוע זה אלפי שנים. זה הוא מספר a הגדול מ-1 ואשר לו רק אפן אחד של פרוק לשני גורמים שלמים וחיוכיים ($a.1$ או $1.a$). מספר כזה אינו מתחלק איפוא לשום מספר טבעי חוץ מ-1 והמספר a עצמו. למשל 2, 3, 5, 7, אבל לא $2=4$, $2=6$, 3. היונים הקדמונים ידעו כבר שאפשר להרכיב כל מספר הגדול מ-1 באפן יחיד וקבוע ממספרים ראשוניים, כך למשל $2.2.3=12$. והנה כאן עומדת כבר

שאלה א. האם רבים המספרים הראשוניים עד אינסוף? כי בדרך ההגיון אפשר לחשב שלמשל 1000 מספרים ראשוניים יספיקו לבנון כל המספרים, היות ומותר להשתמש בכל אבן-בנון כמה פעמים שנרצה. הן מן המספר הראשוני 2 בלבד יש להרכיב אם לא את כל המספרים הרי בכל זאת מספרים רבים עד אינסוף. הלא הן החזקות של 2: 2, 4, 8, ... שאלה זו פתר לפני אלפים שנה או קצת דם בהוכיחו שיש מספר אינסופי של מספרים ראשוניים.

שאלה ב. האם ישנם מספרים ראשוניים רבים עד אינסוף הנגמרים ב-5 או ב-24? תשובה: לא. במקרה הראשון רק 5 הוא מספר ראשוני היות וכל מספר הנגמר ב-5 מתחלק ל-5. במקרה השני אין אף מספר אחד כזה, כי כל מספר הנגמר ב-24 מתחלק ל-4.

שאלה ג. האם ישנם מספרים ראשוניים רבים עד אינסוף הנגמרים ב-21? התשובה החיובית לשאלה זו היא אחת הפעולות הגדולות ביותר של אחד המתמטיקונים אשר קדמו לי בגוטינגן, דיריכלט (*Dirichlet*). הוא הוכיח באפן כללי את המשפט:

בכל מערכה אריתמטית אשר לאברה הראשון ולהבדלה אין גורמים משותפים, ישנם מספרים ראשוניים רבים עד אין סוף. ז. א. נצא ממספר קבוע l (כאן 21) ונוסיף תמיד מספר קבוע אחר k (כאן 100) אשר אין לו גורם משותף עם l ; בשורת המספרים המתקבלת באופן זה ישנם מספרים ראשוניים רבים עד אין-סוף. אילו היה ל- k ול- l גורם משותף, כי אז היתה התשובה שלילית כמו במשל $l=24; k=100$ של השאלה ב'. דבר זה לא קשה היה לשער, כי בזרקנו מספר אין-סופי של עצמים (את המספרים הראשוניים) ל-100 תבות בהתאמה למאה המספרים הנכתבים בשתי ספרות, מדוע לא יפלו באחת התבות האלו עצמים רבים עד אין-סוף? אולם אין זאת הוכחה למושפט דיריכלט; לו היתה זאת הוכחה, כי אז הן היו גם מספרים ראשוניים רבים עד אין-סוף הנגמרים ב-24 מה שאין כן לפי המבואר לעיל. הוכחה זו היתה, כמו שאמרתי כבר, פעולה גדולה אשר המתמטיקה הגרמנית יכולה להתגאות בה. ההוכחה של דיריכלט הצליחה רק הודות לשימוש באמצעי-עזר עמוקים בטורים אין-סופיים, וגם היום עוד אי-אפשר להוכיח את המושפט הזה בדרך קצרה מאד.

שאלה ד'. האם יש למצא שני מספרים ראשוניים הנאים זה אחר זה וההבדל ביניהם גדול כרצוננו? למשל בין המספרים הראשוניים 863 ו-877 אין שום מספר ראשוני אחר. ההבדל בין שני מספרים ראשוניים שכנים אלה הוא איפוא 14. האם יכול מרחק זה להיות לפעמים < 100 או < 1000 זכו. תשובה: כן; ולא קשה לכאור ענין זה. בתור יוצא מן הכלל רוצה אני להביא כאן את ההוכחה. יהי $n < 1$. נעיון במספרים $n!+2; n!+3; \dots; n!+n$ אלה הם מספרים רבים כרצוננו והנאים בזה אחר זה. מספרים אלה מרכיבים הם (ז. א. אינם מספרים ראשוניים), כי מתחלקים הם בהתאמה ל- $2, 3, \dots, n$ והנם שונים מגורמים אלה.

שאלה ה'. האם חוזר ההבדל 1 פעמים רבות עד אין-סוף?
תשובה: לא. כי החל ממספר 1 כל מספר ראשוני הוא אי-זוגי.

שאלה ו'. האם חוזר ההבדל 2 פעמים רבות עד אין-סוף?
(ידוע שהבדל זה חוזר פעמים אחדות. למשל 17, 19; 101, 103). זאת ידע השטן. רצוני לאמר, חוץ מרכונו של עולם אין מי שידע זאת, אפילו לא ידידי הרדי (Hardy) באוקספורד אשר בין כל העובדים אתי הנהו החוקר המעמיק ביותר בשדה-חקירה זה.

שאלה ז'. $2+2=4, 3+3=6, 3+5=8$ אולי גם יתר המספרים הזוגיים הם סכום של שני מספרים ראשוניים? זאת לא אדע; ישנם מחקרים חדשים בכון זה, אולם רחוקים הם עדיין מהמטרה אשר שמו לעצמם להשיב תשובה על שאלה זו.

שאלה ח. האם יש מספרים ראשוניים רבים עד אינסוף בתבנית x^2-1 , ז. א. העומדים מיד לפני מספר רבועי? (למשל בין המספרים 3, 8, 15, 35).
תשובה: לא; כי $(x+1)(x-1)=x^2-1$. זהו מספר מרכב החל מ $x > 2$.

שאלה ט. האם יש מספרים ראשוניים רבים עד אין סוף בתבנית $2x^2+1$ אינו יודע זאת, ואני יודע שאיני יודע זאת ושאיני יודעים את זאת.

שאלה י. אותה השאלה כשכיל התבנית $2x^2+11y^2$ כן, זאת הוכיח דירי כלט ג'כ בעזרת המתודה שלו.

שאלה י"א. כאן נשאלת כבר שאלה עמוקה יותר אבל עוד יכול כל איש להבינה. אחרי אשר דירי כלט הוכיח שיש מספר אינסופי של מספרים ראשוניים הנגמרים ב-3 או ב-7, נשאל בלשון שאינה מדויקת, אם כמויות המספרים האלה שוות בערך, ז. א. בלשון מדויקת, אם המנה של הכמויות האלו עד מקום ידוע הולכת וקרבה ליחידה כל כמה שנרצה. תשובה: כן. זאת הוכיחו לפני 30 שנה בערך המתמטיקון היהודי יעקב הדמר (*J. Hadamard*) בפרוזה המלומד הבלגי המצוין *de la Vallée Poussin*. אני עשיתי זאת אח"כ באופן פשוט הרבה יותר והוכחתי בפעם הראשונה את המשפט המתאים לזה בתורת גופי המספרים האלגבראיים, תורה אשר תורת המספרים הרגילה היא המקרה הכי פשוט בין המקרים הפרטיים שלה הרבים עד אינסוף. אולם בהרצאתי זו הן רציתי לדבר רק על המספרים השלמים הרגילים.

שאלה י"ב. האם אפשר להעריך את כמות המספרים הראשוניים עד x בעזרת אחד הכטויים האלמנטריים הרגילים התלויים ב- x , באופן ששגיאת ההערכה תהיה לאחרונה אינסוף קטנה לגבי הערך האמתי? גדול המתמטיקונים הגרמניים נאום שער, אולם רק הדמר ודדל היו ליפוסן הוכיחו שהכטוי הפשוט $\frac{x}{\log x}$ ממלא דרישה זו. הערכת השגיאה עמדה במשך 25 שנים בלי כל שנוי ורק לפני חרשים מעטים עלה בידי יודי לט לווד (*Littlewood*) בקמברידג' (*Trinity College*) למצא הערכה הרופה הרבה יותר. אחרי י"ב שאלות אלו עוזב אני את המספרים הראשוניים. אמנם הודיתי לכם עפ"י על אריידיעתי, אולם רוצה אני להוסיף שהנני המחבר של ספר-הלמוד היחידי על נושא זה והיה ביכלתי בכ"ז לכתב 961 עמודים על שאלות פתורות בפרק זה, גם הכילו עמודים אלה אחדות מחקרתי הפרטיות.

שאלה י"ג. נעיון כשורת המספרים הרבועיים $0=0.0 ; 1=1.1 ; 4=2.2 ; 9=3.3 ; 16=4.4$; וכו'. שורה זו אינה מכילה את כל המספרים השלמים. אנו שואלים: אולי מתפרק בצורת חבור כל מספר לשני רבועים? לא, כפי שמלמדנו מסל המספר 3. אולי אפשר לתאר כל מספר בתור סכום של 3 רבועים?

לא, המספר 7 למשל אינו נתן לתאור כזה.
 אולי בתור סכום של 1000 או של מספר קבוע אחר של רבועים?
 כן; כי לג'רנ'ג' (Lagrange) הוכיח זה לפני 150 שנה שכל מספר מתפרק
 לארבעה רבועים; למשל $0+1+16+81=98$.

שאלה י"ד. האם יש מספר קבוע כזה גם בשביל קוביות חיוביות (גם
 0 בכלל), בשביל חזקות רבועיות, וכו'. בשביל חזקות k -יות? מספר קבוע זה
 מותר כמובן שיהיה תלוי ב- k . תשובה: כן; זו היא "השערת ורינג' (Waring)
 המפורסמת משנת 1770 ורק אחרי 139 שנים בשנת 1909 הוכיח אותה חברו
 דוד הילברט (D. Hilbert) בגזטינגן.

שאלה ט"ו. נשאר במקרה הכי פשוט של הקוביות. מה היא כמות
 המחברים הכי קטנה המספיקה לחבורו של כל מספר? המספר 23 דורש כפי
 הנראה 9 קוביות היות ואין פרוק יותר קצר מ-8 ועוד 8 ועוד 7 יחידות. המספר
 הטוב ביותר אינו יכול אפוא להיות קטן מתשע. ובאמת מספיקות 9 קוביות
 המיד כפי שיש להבין ממאמר אחד של ויפרייך (Wieferich). החל במקום
 ידוע מספיקות אפילו 8 קוביות כפי שהוכחתי אני.

שאלה ט"ז. אני ממשיך בקוביות. מה היא הכמות הכי קטנה של קוביות
 המספיקה לכל מספר גדול? לפי הנאמר 1 או 2 או... או 8. מוכיחים בלי קשי
 שאין המספר המבוקש יכול להיות קטן מ-4; אם הוא 8 או קטן מ-8, זאת אין יודעים
 עד היום.

שאלה י"ז. גם אם נדרש את הפרוק ל-5 קוביות של כל המספרים חוץ
 מכמות אשר ערכה הפרוצנטואלי קטן כרצוננו, יהיה ה-5 הקטן ביותר לפחות 4 כפי
 שנקל להוכיח ולכל היותר 8 לפי האמור לעיל. כאן הוכיחו הרדי וילסון
 לפני זמן מה, שהמספר הנכון הוא לכל היותר 5. ובכן מספר זה הוא 4 או 5. בקצור:
 כמעט כל המספרים מתפרקים ל-5 קוביות. דרכי הוכחתם הן יפות ונהדרות מכל
 מה שראיתי ולמדתי בחיי. הם יכלו גם לקבע בדיוק את המספר המתאים לדור
 רבועים (= חזקות רבועיות). מספר זה 15 הנהו. מעולם לא שערתו שעוד בימינו
 יעלה בידו מי שהוא לפתר שאלה מתמטית זו הנראית ליודעי-דבר כחסרת נקודת-
 אחוזה. הרצאת הוכחתם לדור-רבועים ולכל $k < 4$ ארכה בשעורי 2 חדשים 4 שעות
 לשבוע.

שאלה י"ח. אמנם אין זה אלא משל אשר בו נוכל לשאל את השאלה רק
 אחרי אשר נשוב את התשובה. נערך לפי גדלם את כל השברים המקוצרים בין 0
 ל-1 אשר מכנם לכל היותר n ; כך למשל בשביל $n = 7$

$$\frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7};$$

או רואים שבשני שברים שכנום $\frac{a}{b}$ ו $\frac{c}{d}$ המספר $bc-ad$ (אשר הנהו חיובי כמובן מפני $\frac{bc-ad}{bd} = \frac{c}{d} - \frac{a}{b} > 0$) תמיד שזה ל"ו וגם קל להוכיח דבר זה.

שאלה י"ט. משפט קלסי בתורת המספרים (מאת פרמט *Fermat* במאה ה-XVII) אומר: יהי p איזה מספר ראשוני שהוא או מתחלק $2^p - 2$ ל- p . למשל $30 = 2^5 - 2$ מתחלק ל-5. ובכלל $ap - a$ ל- p . והנני שואל: האם יקרה לפעמים שיתחלק $2^p - 2$ ל- p^2 , והאם יקרה זה לעתים קרובות עד ∞ . התשובה לשאלה זו חשיבות יתרה לה לשמוש ידוע. מספרים p אחרים כאלה ידועים. אולם אין יודעים אם רבים הם עד ∞ או אולי לא ותאים לכך שום p החל מ- p ידוע. הזמן הקצר לא ירשה לי לצקרו לחשב לפניכם ש- $2^{1093} - 2$ מתחלק ל- 1093^2 .

שאלה כ'. השאלה הבאה שיוכת לגאומטריה אולם נאום הביא את השאלה הזאת בעזרת האלגברה לידו שאלה בתורת המספרים. בביה"ס לומדים שאפשר לרשם בתוך מעגל נתון בעזרת סרגל ומחוגה את המצולע המשוכלל בעל 3, 4, 5, 6, 8, 10, 12, 15, 16, 20 צלעות ועוד אחרים רבים עד ∞ (הלא הם, בעלי $2^{a+2}, 2^a \cdot 3, 2^a \cdot 5, 2^a \cdot 3 \cdot 5$ צלעות; a מספר שלם איזה שהוא $0 \leq a$). נציין ב- n את מספר צלעות המצולע. ואז נשאלת שאלה: האם אפשרות הבניה הנ"ל בשביל כל n שהוא? או מה הוא n אשר בשבילו אין הבניה אפשרית. נאום הוכיח: אין הבניה אפשרית במקרה $n=7$; הוכחה זו לא היתה קשה ביותר; הבניה הנ"ל אפשרית היא בשביל $n=17$; זו היתה אחת המצאותיו הגדולות ביותר והציור המתאים חרות על מצבת הזכרון שלו בעיר בראונשוויג. בדרך כלל אפשרות הבניה רק במקרה ש- n מכיל כל גורם ראשוני אי-זוגי רק פעם אחת וכל גורם ראשוני אשר כזה יהיה בעל התבנית $2^{2^m} + 1$ והמספר m חיובי או שזה ל-0. אם $m=0$ נקבל $n=3$; אם $m=1$ נקבל $n=5$; אם $m=2$ נקבל $n=17$; אם $m=3$ נקבל $n=257$; אם $m=4$ נקבל $n=65537$. וכעת מתעוררת השאלה אם המספרים הראשוניים האלה של נאום רבים הם עד ∞ . התשובה: אינו יודע. ואפילו אין יודעים להוכיח אם יש מספר אחד אשר כזה אחרי 65537. אולי אין אף אחד, ואולי אחרים ואולי רבים עד אין-סוף.

שאלה כ"א. בעזרת אמצעים מתורת המספרים פתרו גם את השאלה הגאומטרית של הקנדרטורה של הקגול. לפני 40 שנה הוכיח מורי לינדמן (*Lindemann*) במינכן שאי-אפשר להפך עגול לרבוע בעזרת מחוגה וסרגל. הדבר החשוב בהוכחתו הוא שהוכיח, שהמספר הידוע π אינו שרש של משוואה בעלת מקדמים שלמים; שמספר זה הנהו, כפי שנוהגים לאמר, טרנסצנדנטי.

שאלה כ"ב. בלשון נאומטרית: הקו העקום $x^2 - Dy^2 = 1$ (מספר חיובי שלם) הוא היפרבולה. האם מונחת על קו זה נקודות פריג במספר איךסופי?

(נקודות פריג הן נקודות אשר להן קואורדינטות בנות מדה במספרים שלמים).

בלשון אריתמטית: האם יש למשוואה זו ב־ x ו־ y מספר ∞ של פתרונות במספרים שלמים. אם D הוא רבוע, $E^2 = D$, אז התשובה שלילית היא; כי במקרה זה $1 = (x+Ey)(x-Ey)$ ו־ $1 = x - Ey = x + Ey$ ומכאן רק שני הפתרונות $O = y; \pm 1 = x$. לכל D שאינו רבוע ושהוא $0 <$ הוכיח לגרנג'י שיש ∞ פתרונות.

שאלה כ"ג. בשאלה המתאימה לקודמת אשר בצדה השמאלי נמצא בטור ב־ x ו־ y בעל סדר < 2 ושאינו מתפרק ומוימן במקום 1 יכול להמצא איזה מספר שלם שהוא, הוכיח המתמטיקן הנורבגי תואה (Thue) את העובדה הבלתי צפויה שישנו תמיד רק מספר סופי של פתרונות.

במספר זה של כ"ג שאלות רוצה אנכי להפסיק; כי כ"ג הוא מספר ראשוני ו־ A . מספר הנאה לנו מאד. בטוח אני שאין עלי לפחד פן תשאלוני לשם מה עוסקים בתורת המספרים ולמה תוכל לשמש; כי עוסקים אנו במדע לשנו ובהתעסקות בו היתה לנו לנתמה בימי המלחמה הפנימית והחיצונית אשר בתור יהודים וגרמנים נלחמנו ונלחמנו עוד כיום.

נאום הפרופסור
יחזקאל (ארמונד) לנדאו

Professor E. LANDAU.

אני מודה לכם בעד הכבוד אשר
חלקתם לי בהזמנתכם אותי בתור באיכח
המדע המתמטי לאמר טלום אתרות בתג
ירית אבן הפנה של המכון למתמטיקה
ולפיסיקה.

המתמטיקה והפיסיקה אחיות הן. באוניברסיטאות האירופיות הגדולות
לא יוכל אמנם בנין אחד להכיל את שתיהן מפני גדל ההיקף של כל אחת
מהן. אולם כאן בירושלם הרי באים אנו רק כיום ליסוד את האוניברסיטה
ויכולים אנחנו להניח אכרפנה משותפת לבנין אשר בו יטפלו בשני המדעים
בעלי נקודות מגע כה רבות.

ובנוגע למתמטיקה עצמה, הן ידוע מה גדול היה חלקם של יהודי ארצות
אירופה בהתפתחות המדע הזה; ואני רוצה לקוות שמבין כתלי הכנין שאנו
בונים כיום, תתן עוד היהדות לאנושיות תשורות רבות ונאות בצורת תגליות
והמצאות חשובות להלכה, ובעלות ערך למעשה.

יהי רצון ותצא מבורת זה תועלת רבה למדע הטהור, אשר אינו יודע
גבולות בין עם לעם; ומי יתן ותצא הכרה זאת מציון ותחדור גם ללכם
של אלה הרחוקים עדיין מדעת זו.