פרופסור יחזקאל-אדמונד לנדאו

שאלות פתורות וסתומות בתורת המספרים האלמנטרית.

בשמחה רבה נעניתי לבקשה החביבה להרצות על אחד הנושאים משדות החקירה שלי והנני בוחר בפרק המתמטיקה אשר קושיותיו מובנות בנקל למי שאינו מבעלי המקצע. קושיות אלו עולות מאליהן בבואנו לחשב במספרים הרגילים הטבעיים 1,2,3, ... אין פוגשים בשברים ומה גם במספרים אי־רציונליים בשאלות הללו; השאלות מובנות איפוא אפילו למי שאינו בעל מקצע ואשר שכח כבר את המתמטיקה של בית הספר. אך ממהר אני להוסיף שפתרונן 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 אחדות במספרים שלמים, שאלות פתורות וסתומות אשר נקל להבינן.

המושג מספר ראשוני ידוע זה אלפי שנים. זה הוא מספר a הגדול מ־1 ואשר לו רק אפן אחד של פרוק לשני גורמים שלמים וחיוביים ($a.1$ או $1.a$). מספר כזה אינו מתחלק איפוא לשום מספר טבעי חוץ מ־1 והמספר a עצמו. למשל 2, 3, 5, 7, אבל לא $4=2.2$, $6=2.3$. היונים הקדמונים ידעו כבר שאפשר להרכיב כל מספר הגדול מ־1 באפן יחיד וקבוע ממספרים ראשוניים, כך למשל $12=3.2.2$. והנה כאן עומדת כבר

שאלה א׳. האם רבים המספרים הראשוניים עד אין־סוף? כי בדרך ההגיון אפשר לחשב שלמשל 1000 מספרים ראשוניים יספיקו לבנין כל המספרים, היות ומותר להשתמש בכל אבן־בנין כמה פעמים שנרצה. הן מן המספר הראשוני 2 בלבד יש להרכיב אם לא את כל המספרים הרי בכל זאת מספרים רבים עד אין־סוף. הלא הן החזקות של 2: 2, 4, 8,... שאלה זו פתר לפני אלפים שנה אוקלידס בהוכיחו שיש מספר אין־סופי של מספרים ראשוניים.

שאלה ב׳. האם ישנם מספרים ראשוניים רבים עד אין־סוף 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 אין־סוף 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 באפן 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 לשערו, 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 למשפט 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 לשמוש באמצעי־עזר עמוקים בטורים אין־סופיים, וגם היום עוד אי־אפשר להוכיח את המשפט הזה בדרך קצרה מאד.

שאלה ד׳. האם יש למצא שני מספרים ראשוניים הבאים 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 וכו׳. תשובה: כן; ולא קשה לבאר ענין זה. בתור יוצא מן הכלל רוצה אני להביא כאן את ההוכחה. יהי $n>1$. נעיין במספרים $n!+2$; $n!+3$; ...; $n!+n$. אלה הם מספרים רבים כרצוננו והבאים בזה אחר זה. מספרים אלה מרכבים הם (ז. א. אינם מספרים ראשוניים), כי מתחלקים הם בהתאמה ל־$2, 3, ..., n$ 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 מרבונו 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 בכוון זה, אולם רחוקים הם עדיין מהמטרה אשר שמו לעצמם להשיב תשובה על שאלה זו.

שאלה ח׳. האם יש מספרים ראשונים רבים עד אין־סוף בתבנית x^2-1, ז. א. העומדים מיד לפני מספר רבועי? (למשל בין המספרים 3, 8, 15, 35).
תשובה: לא; כי $x^2-1=(x+1)\cdot(x-1)$ וזהו מספר מרכב החל מ $2<x$.

שאלה ט׳. האם יש מספרים ראשונים רבים עד אין סוף בתבנית x^2+1?
איני יודע זאת, ואני יודע שאיני יודע זאת ושאין יודעים את זאת.

שאלה י׳. אותה השאלה בשביל התבנית x^2+111y^2?
כן, זאת הוכיח דיריכלט ג״כ בעזרת המתודה שלו.

שאלה י״א. כאן נשאלת כבר שאלה עמוקה יותר אבל עוד יכול כל איש להבינה. אחרי אשר דיריכלט הוכיח שיש מספר אין־סופי של מספרים ראשונים 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*) בפריז והמלומד הבלגי המצוין *de la Vallée Poussin*. אני עשיתי זאת אח״כ באפן 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 אין־סוף. אולם בהרצאתי זו הן רציתי לדבר רק על המספרים השלמים הרגילים.

שאלה י״ב. האם אפשר להעריך את כמות המספרים הראשונים עד x בעזרת אחד הבטויים האלמנטריים הרגילים התלויים ב־x, באפן ששגיאת ההערכה תהיה לאחרונה אין־סוף קטנה לגבי הערך האמתי? גדול המתמטיקונים הגרמניים גאוס שער, אולם רק הדמר ודה־לה־ולי־פוסן הוכיחו שהבטוי הפשוט $\frac{x}{\log x}$ ממלא דרישה זו. הערכת השגיאה עמדה במשך 25 שנים בלי כל שנוי ורק לפני חדשים מעטים עלה בידי ידידי לטלווד (*Littlewood*) בקמברידג׳ (*Trinity College*) למצא הערכה חריפה הרבה יותר.

אחרי י״ב שאלות אלו עוזב אני את המספרים הראשונים. אמנם הודיתי לכם עפ״ר על אי־ידיעתי, 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 מחקירותי הפרטיות.

שאלה י״ג. נעיין בשורת המספרים הרבועיים $0=0\cdot 0$; $1=1\cdot 1$; $4=2\cdot 2$; $9=3\cdot 3$; $16=4\cdot 4$; וכו׳. שורה זו אינה מכילה את כל המספרים השלמים.
אנו שואלים: אולי מתפרק בצורת חבור כל מספר לשני רבועים?
לא, כפי שמלמדנו משל המספר 3.
אולי אפשר לתאר כל מספר בתוך 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 ל ג ר נ 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 רביעיות, וכו'. בשביל חזקות k-יות? מספר קבוע זה מותר כמובן שיהיה תלוי ב-k. תשובה: כן; זו היא „השערת ו ר י נ ג" (*Waring*) המפורסמה משנת 1770 ורק אחרי 139 שנים בשנת 1909 הוכיח אותה חברי ד ו ד ה ל ב ר ט (*D. Hilbert*) בגוטינגן.

שאלה ט"ו. נשאר במקרה הכי פשוט של הקוביות. מה היא כמות המחוברים 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 איפוא להיות קטן מתשע. ובאמת מספיקות 9 קוביות תמיד כפי שיש להבין ממאמר אחד של ו י פ ר י ך (*Wieferich*). החל ממקום 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־s קוביות של כל המספרים חוץ מכמות אשר ערכה הפרוצנטואלי קטן כרצוננו, יהיה ה־s הקטן ביותר לפחות 4 כפי שנקל להוכיח ולכל היותר 8 לפי האמור לעיל. כאן הוכיחו ה ר ד י ו ל ט ל ו ו ד 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 לדו־רבועים (= חזקות רביעיות). מספר זה 15 הנהו. מעולם לא שערתי שעוד בימינו יעלה בידי מי שהוא לפתר שאלה מתמטית זו הנראית ליודעי־דבר כחסרת נקודת־אחיזה. הרצאת הוכחתם לדו־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 נשיב את התשובה. נערך לפי גדלם את כל השברים המקוצרים בין 0 ל־1 אשר מכנם לכל היותר n; כך למשל בשביל $n = 7$

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

אז רואים שבשני שברים שכנים $\frac{a}{b}$ ו $\frac{c}{d}$ המספר $bc-ad$ (אשר הנהו חיובי כמובן מפני $\frac{c}{d}-\frac{a}{b}=\frac{bc-ad}{bd}>0$) תמיד שוה ל־1 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, אז מתחלק 2^p-2 ל־p. למשל $2^5-2=30$ מתחלק ל־5. ובכלל a^p-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 אחדים כאלה ידועים. אולם אין יודעים אם רבים הם עד ∞ או אולי לא יתאים לכך שום p החל מ־p ידוע. הזמן הקצר לא ירשה לי לצערי לחשב לפניכם ש־$2^{1093}-2$ מתחלק ל־1093^2.

שאלה כ'. השאלה הבאה שייכת לגאומטריה אולם גאוס הביא את השאלה הזאת בעזרת האלגברה לידי שאלה בתורת המספרים. בביה"ס לומדים שאפשר לרשום 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}, $3\cdot2^a$, $5\cdot2^a$, $3\cdot5\cdot2^a$ צלעות; a מספר שלם איזה שהוא ≥0). נציין ב־n את מספר צלעות המצולע. ואז נשאלת שאלה: האם אפשרית הבניה הנ"ל בשביל כל n שהוא? או מה הוא ה־n אשר בשבילו אין הבניה אפשרית. גאוס 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 אפשרית 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 שוה 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 גאוס רבים הם עד ∞. התשובה: איני יודע. ואפילו אין יודעים להוכיח אם יש מספר אחד אשר כזה אחרי 65537. אולי אין אף אחד, ואולי אחדים ואולי רבים עד אין־סוף.

שאלה כ"א. בעזרת אמצעים מתורת המספרים פתרו גם את השאלה הגאומטרית של הקוַדרטורה של העגול. 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 משואה בעלת מקדמים שלמים; שמספר זה הנהו, כפי שנוהגים לאמר, טרנסצנדנטי.

שאלה כ"ב. בלשון גאומטרית: הקו העקום $x^2 - D\ y^2 = 1$ (D מספר חיובי שלם) הוא היפרבולה. האם מונחות על קו זה נקודות סָרִיג במספר אין־סופי?

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

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

שאלה כ"ג. בשאלה המתאימה לקודמת אשר בצדה השמאלי נמצא בטוי ב־x ו־y בעל ממד >2 ושאינו מתפרק ומימין במקום 1 יכול להמצא איזה מספר שלם שהוא, הוכיח המתמטיקון הנורבגי ת ו א ה (*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 ז. א. מספר הנאה לנו מאד. בטוח אני שאין עלי לפחד פן תשאלוני, לשם מה עוסקים בתורת המספרים ולמה תוכל לשמש; כי עוסקים אנו במדע לשמו וההתעסקות בו היתה לנו לנחמה בימי המלחמה הפנימית והחיצונית אשר בתור יהודים וגרמנים נלחמנו ונלחמים עוד כיום.

נאום הפרופסור
יחזקאל (ארמונד) לנדאו
Professor E. LANDAU.

אני מודה לכם בעד הכבוד אשר חלקתם לי בהזמינכם אותי בתור בא־כח המדע המתמטי לאמר מלים אחדות בחג 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 בירושלים הרי באים אנו רק כיום ליסד את האוניברסיטה ויכולים אנחנו להניח אבן־פנה 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 הבנין שאנו בונים כיום, תתן עוד היהדות לאנושיות תשורות רבות ונאות בצורת תגליות והמצאות חשובות להלכה, ובעלות ערך למעשה.

יהי רצון ותצא מבית זה תועלת רבה למדע הטהור, אשר איננו יודע גבולות בין עם לעם; ומי יתן ותצא הכרה זאת מציון ותחדור גם ללבם של אלה הרחוקים עדיין מדעה זו.