בעיקבות המספרים הראשוניים

מאת: ישראל קליינר
אוניברסיטת יורק, טורונטו, קנדה.

נושא המאמר הוא במסגרת הענף המתמטי שנקרא תורת המספרים ועניינו בתכונותיהם של המספרים הטבעיים. הבעיות בתורת המספרים הן קלות לניסוח ולהבהרה, אך הפתרונות הם לעיתים עמוקים וקשים למדי. מאז ומתמיד נמצא בנושא זה קסם הן לחובבים והן למתמטיקאים מעולים וגם כיום רבים מתעניינים בו.

פיזור המספרים הראשוניים

יחודם וחשיבותם של המספרים הראשוניים בקרב המספרים הוא היותם "אבני הבנין" עבור כל הטבעיים. ואמנם, אם ניצור את כל המכפלות האפשריות של המספרים הראשוניים נקבל בדרך זו את כל המספרים הטבעיים ללא חזרות. הסבר: מכפלות שונות של מספרים ראשוניים נותנות מספרים שונים. (ניסוח זה שקול למה שמקובל לקרוא "המשפט היסודי של תורת המספרים" האומר: כל מספר טבעי ניתן להצגה יחידה כמכפלה של מספרים ראשוניים). על מנת להראות כי תוצאה זו אינה ברורה מעצמה נביא דוגמא למערכת שבה משפט זה אינו מתקיים. נתבונן בקבוצת המספרים הזוגיים בלבד. במערכת זו מספר הוא ראשוני אם אי אפשר לכתוב אותו כמכפלה של שני זוגיים. למשל, 2, 6, 10, 30 הם מספרים ראשוניים. אם נרשום $2\cdot 30 = 60$ ו- $6\cdot 10 = 60$ נראה כי במערכת זו הפירוק לגורמים ראשוניים אינו יחיד.

תרגיל 1

השתמש במשפט היסודי של תורת המספרים על מנת להראות כי $\sqrt{n}$ הוא מספר אירציונלי עבור כל n שאינו ריבוע שלם. (תוכל למצוא רמז במאמר "סיפור $\sqrt{2}$" שהתפרסם בשבבים, תיק מס' 12).

נרשום לפנינו את 50 המספרים הראשוניים הראשונים:

2 , 3 , 5 , 7 , 11 , 13 , 17 , 19 , 23 , 29 , 31 , 37 , 41 , 43
47 ,53 ,59 , 61 , 67 , 71 , 73 , 79 , 83 , 89 , 97 ,101 ,103
107 ,109 ,113 ,127 ,131 ,137 ,139 ,149 ,151 ,157 ,163 ,167
173 ,179 ,181 ,191 ,193 ,197 ,199 ,211 ,223 ,227 ,229

מה נוכל לומר על פיזור המספרים הראשוניים בקרב כל המספרים הטבעיים?

תחילה עולה השאלה: האם מספרם של הראשוניים הוא סופי או אינסופי?
ובכן, ידועה לנו עובדת היות המספר אינסופי אבל זוהי תוצאה לא ברורה מאליה (באמת, מדוע יהיו אינסוף מספרים ראשוניים? - חשוב על כך').

המחבר מודה לנורית זהבי על תרגום המאמר מאנגלית ועל הערותיה המועילות.

עובדה זו היתה ידועה כבר ליוונים לפני 2000 שנה וגם הוכחה על ידם (אוקלידס). מעניין לציין כי הוכחה קלסית זו מופיעה עד היום בכל ספר בסיסי בנושא זה. (אם לא פגשת בהוכחה זו עד כה, מומלץ כי תעיין בה - היא קצרה ויפה (1)).

האם ניתן להבחין בחוקיות כלשהי בפיזור המספרים הראשוניים? נתבונן ברשימה שלעיל ונראה כי יש הרבה זוגות של ראשוניים הנבדלים זה מזה ב- 2. למשל,

$$3,5 \;;\; 11,13 \;;\; 17,19 \;;\; 29,31; \;\ldots\; ; 107,109; \;\ldots$$

קוראים לזוגות כאלה: "ראשוניים תאומים". האם יש מספר סופי או אינסופי של זוגות תאומים? התשובה לשאלה זו אינה ידועה, אך ההשערה היא כי מספרם אינסופי (הזוג הגדול ביותר שהיה ידוע ב-1976 הוא: $76\cdot 3^{139}-1 \;,\; 76\cdot 3^{139}+1$). אולם, מספר הזוגות של ראשוניים תאומים אינו "כל כך גדול" במובן הבא: סכום המספרים ההפכיים של המספרים הראשוניים

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{23}+\frac{1}{29}+\cdots$$

הוא מתבדר (2). ואילו סכום המספרים ההפכיים של כל הראשוניים התאומים מתכנס. תכונת ההתכנסות של סכום זה היא קשה להוכחה. המתמטיקאי ברון הוכיח אותה בשנות השלושים של המאה הנוכחית (3).

תרגיל 2

הראה כי הסכום של כל זוג מספרים ראשוניים תאומים (פרט לזוג הראשון 5, 3) הוא כפולה של 12.

תרגיל 3

המספרים הראשוניים 3, 5, 7 נקראים "שלישית הראשוניים". הראה כי לא קיימת שלישית ראשוניים נוספת. (כלומר, יש להראות כי לא קיימים שלושה מספרים ראשונים אחרים p, q, r כך ש: $q-p=r-q=2$).

אם נחפש מספרים ראשוניים בקרב הטבעיים ההולכים וגדלים נמצא כי הם פחות צפופים ונדירים יותר. לדוגמא, אחרי המספר הראשוני 370261 מופיעים 111 מספרים עוקבים פריקים. יתרה מזאת, נראה כי קיימת סדרה של 999999 מספרים עוקבים פריקים:

$$10^6!+2 \;,\; 10^6!+3 \;,\; 10^6!+4 \;,\ldots, 10^6!+10^6 \;.$$

זוהי סדרה בת 999999 איברים, וברור כי האיבר הראשון בסדרה מתחלק ב-2, השני ב-3, השלישי ב-4 וכך הלאה והאיבר האחרון מתחלק ב- 10^6 .

תרגיל 4

תן דוגמא לסדרה בת 434256378 מספרים פריקים עוקבים. התוכל להכליל את הדוגמא לכל מספר n כרצונך?

ראינו לעיל דוגמאות לרווחים גדולים כרצוננו בין מספרים ראשוניים, אך בכל זאת אין הם "כל כך" רחוקים זה מזה במובן הבא: עבור כל n טבעי יש לפחות מספר ראשוני אחד בין n ו- 2n . טענה זו ידועה בתור משפט ברטרנד והוכחה במאה ה-19 (4).

תרגיל 5

א. הראה כי קיימים לפחות שלושה מספרים ראשוניים שכל אחד מהם בעל 26 ספרות.

ב. כנ"ל עבור 185 ספרות.

ג. התוכל להכליל לכל מספר ספרות?

תרגיל 6

עבור $n \geq 3$ הראה כי יש לפחות מספר ראשוני אחד בין $\sqrt{n}$ ו n .

נסכם את מה שראינו עד כה: בדיקות מראות (אך אין הוכחה לכך) כי יש מספר אינסופי של מספרים ראשוניים קרובים זה אל זה ככל האפשר - הראשוניים התאומים. מאידך גיסא קיימות סדרות גדולות כרצוננו של מספרים עוקבים אשר ביניהן אין אף מספר ראשוני. ואולם, תמיד נוכל למצוא "לא יותר מדי רחוק" מספר ראשוני אחרי סדרה כזו (משפט ברטרנד). העדר חוקיות כזאת הנראית לעין בפיזורם של המספרים הראשוניים הניע את המתמטיקאי המפורסם אוילר (במאה ה-18) לקבוע: "עד היום ניסו המתמטיקאים לשווא לגלות חוקיות של הופעת המספרים הראשוניים, ויש לנו סיבות להאמין כי מוח האדם לא יוכל לעולם לחדור למיסתורין זה."

התברר כי אוילר לא צדק. אמנם אין רואים חוקיות אם מסתכלים על המספרים הראשוניים כיחידים-אין לנו נוסחה למציאת המספר הראשוני הבא אחרי ראשוני מסוים, אבל אם נסתכל עליהם כעל אוסף של מספרים נראה כי גאוס (במאה ה-19) מצא חוקיות לגבי הפיזור של כלל המספרים הראשוניים. זוהי דוגמא לכך שבמתמטיקה צריך לדעת איזה שאלות לשאול. גאוס ניסה למנות את המספרים הראשוניים ברווח מסוים, ולא לקבל נוסחה למספר ראשוני הבא אחרי מספר ראשוני מסוים. אם נסמן ב- $\pi(x)$ את מספר הראשוניים שאינם עולים על x, הרי שגאוס ניסה למצוא נוסחת קירוב המתארת את התנהגות הפונקציה $\pi(x)$ (לנוסחה מדויקת לא נוכל לצפות).

גאוס שיער כי קיים הקשר הבא:

$$\pi(x) \sim \frac{x}{\ln x}$$

לקירוב יש משמעות מתמטית לפי מושג הגבול:

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

לא היה ביכולתו של גאוס להוכיח זאת והדבר נעשה רק כעבור חמישים שנה (ב-1896) באמצעות כלים מתמטיים בעלי עוצמה רבה (2). בשל החשיבות הרבה שיש לתוצאה זו היא נקראת "משפט המספרים הראשוניים". כאמור, המשפט נותן אינפורמציה לא על הופעת מספרים ראשוניים, כי אם על שכיחות הופעתם בקרב הטבעיים. אם נרשום את הנוסחה באופן הבא:

$$\frac{\pi(x)}{x} \sim \frac{1}{\ln x}$$

נוכל לומר כי המשמעות היא שההסתברות למציאת מספר ראשוני בין x השלמים הראשונים היא בקירוב $\frac{1}{\ln x}$.

נוסחאות ה"מייצרות" מספרים ראשוניים

נעיין עתה בפונקציות אחדות ה"מייצרות" מספרים ראשוניים.

בשלבי החיפוש אחר פונקציות כאלה נצמצם בהדרגה את הדרישות משלב לשלב.

בשלב ראשון מחפשים פונקציה "יפה" $f(n)$ המייצרת את כל המספרים הראשוניים ורק אותם.

בשלב שני מסתפקים בפונקציה הנותנת רק מספרים ראשוניים (אבל מספרם יהיה אינסופי).

בשלב שלישי דורשים רק כי הפונקציה תיתן מספר אינסופי של מספרים ראשוניים.

בשלב רביעי מחפשים פונקציה המספקת מספר סופי בלבד של מספרים ראשוניים.

נתייחס עתה לארבעה השלבים בזה אחר זה ונראה מה היו ההישגים בתקופות השונות.

(i) לגבי השלב הראשון, כפי שראינו בדיון הקודם, אין לצפות שתמצא נוסחה "יפה" כזו.

ניתן כמובן לרשום נוסחה טריויאלית כמו:

$$f(n) = \begin{cases} 2 & \text{עבור } n \text{ לא ראשוני} \\ n & \text{עבור } n \text{ ראשוני} \end{cases}$$

נוסחה מעניינת יותר היא:

$$f(x\ ,y) = \frac{y-1}{2}\left[\left|B^2 - 1\right| - (B^2 - 1)\right] + 2$$

כאשר:

$$B = x(y + 1) - (y! + 1)$$

לא קשה להוכיח (5) כי פונקציה זו, אשר התחום שלה הוא כל הזוגות של מספרים טבעיים נותנת את כל הראשוניים, רק אותם וכל ראשוני איזוגי בדיוק פעם אחת.

אם נתבונן היטב בפונקציה הרשומה לעיל, נראה כי גם היא אינה באמת "יפה" ובוודאי לא שימושית. ואמנם ניתן לרשום אותה גם באופן הבא:

$$f(x\ ,y) = \begin{cases} 2 & \text{עבור } B^2 \geq 1 \\ y + 1 & \text{עבור } B^2 = 0 \end{cases}$$

נשים לב כי $B = 0$ כאשר $x = \frac{y! + 1}{y + 1}$ והשוויון $f(x\ ,y) = y + 1$ מתקבל אם ורק אם $y + 1$ הוא מספר ראשוני.

תוצאה זו מתקבלת בקלות ממשפט בסיסי בתורת המספרים הנקרא משפט וילסון הטוען כי מספר n הוא ראשוני אם ורק אם n מחלק את $(n-1)!+1$. אנו רואים אם כן, כי הנוסחה לעיל היא בעצם ניסוח של משפט וילסון.

הישג מרשים אך מורכב התקבל כתוצאה מעבודה רבה ומעמיקה בלוגיקה על ידי המתמטיקאי בן ימינו Matijasevich ב-1970. הוא בנה פולינום אשר ערכיו החיוביים הם כל ורק המספרים הראשוניים. מאחר והמדובר בפולינום מהמעלה ה-25 בעל 26 משתנים לא נביא אותו כאן. (ראה (6))

(ii) נעבור עתה לשלב השני. המתמטיקאי פרמה (במאה ה-17) היה סבור כי מצא נוסחה המספקת רק מספרים ראשוניים:

$$F(n) = 2^{2^n} + 1$$

ואומנם, $F(0) = 3$, $F(1) = 5$, $F(2) = 17$, $F(3) = 257$, $F(4) = 65537$

ארבעה מספרים אלה הם ראשוניים; אבל,

$$F(5) = 4294967297 = 641 \times 6700417$$

המתמטיקאי אוילר הוא זה שגילה במאה שנים אחרי פרמה כי $F(5)$ הוא מספר פריק. כדאי לציין כי זה לא היה סתם ניחוש מצדו של אוילר (7). פרמה עצמו הצליח למצוא הרבה תוצאות חשובות בתורת המספרים אבל בדרך כלל בלי להוכיח אותן. רוב מסקנותיו התבררו יותר מאוחר כנכונות והנוסחה ליצירת מספרים ראשוניים היא אחת היוצאות מן הכלל. עד היום לא מצאו מספרי פרמה $F(n)$ נוספים שהם ראשוניים ולעומת זאת הראו ב- 1961 באמצעות מחשב כי $F(13)$, $F(14)$ הם פריקים. לגבי $F(17)$ יודעים כי הוא בעל 39456 ספרות, אך לא ידוע אם הוא פריק או ראשוני. על מספרי פרמה אחדים אחרי $F(17)$ יודעים כי הם פריקים, הגדול בהם הוא $F(1945)$ (זהו מספר בעל יותר מ- 10^{582} ספרות!).
שאלה פתוחה היא האם בקרב מספרי פרמה יש מספר סופי או אינסופי של ראשוניים. גם בעזרת מחשב אי אפשר לטפל במספרים כל כך גדולים בגלל מיגבלות המחשב.
ראוי להצביע על קשר מעניין בין מספרי פרמה וגיאומטריה אשר נתגלה על-ידי גאוס: מצולע משוכלל בעל n צלעות ניתן לבניה בעזרת סרגל ומחוגה אם ורק אם

$$n = 2^t \cdot p_1 \cdot p_2 \cdots p_s$$

כאשר P_i הם מספרים ראשוניים שונים מהצורה $2^{2^k} + 1$.

נוסחה דומה הוצאה על-ידי מתמטיקאי אחר מהמאה ה-17, מרסן.

$$M(p) = 2^p - 1$$

נתייחס רק ל p ראשוני, שכן עבור p פריק קל לראות כי $M(p)$ אף הוא פריק.

כך נקבל, $M(2) = 3$, $M(3) = 7$, $M(5) = 31$, $M(7) = 127$

כל אלו הם מספרים ראשוניים, אבל,

$$M(11) = 2047 = 23 \cdot 89$$

גם במקרה זה לא ידוע אם יש מספר סופי או אינסופי של "מספרי מרסן" ראשוניים (2), (7)
נוסיף כאן על קשר בין "מספרי מרסן" ומספרים משוכללים. מספר n הוא "משוכלל" אם הוא שווה לסכום כל מחלקיו פרט לעצמו, אך כולל 1.

לדוגמא: 6 ו 28 הם מספרים משוכללים שכן,

$$6 = 1 + 2 + 3$$
$$28 = 1 + 2 + 4 + 7 + 14$$

קיים משפט האומר כי מספר זוגי הוא משוכלל אם ורק אם הוא מהצורה:

$$2^{p-1} \cdot (2^p - 1)$$

כאשר $2^p - 1$ הוא מספר מרסן ראשוני. כיוון אחד של משפט זה (אם מספר מקיים את התנאי אז הוא משוכלל) הוכח על ידי אוקלידס, אשר כמובן לא קרא למספרים אלו מספרי מרסן. הכיוון ההפוך הוכח כאלפיים שנה מאוחר יותר על ידי אוילר.

__תרגיל 7__ מצא עוד 4 מספרים משוכללים.

עד כאן ראינו שני נסיונות לא מוצלחים למציאת נוסחה המייצרת ראשוניים. במאה שלנו (ב-1947) מצא המתמטיקאי מילס "נוסחה" הנותנת רק מספרים ראשוניים. הוא הראה כי קיים מספר ממשי a כך שהערך השלם $[a^{3^n}]$ הוא מספר ראשוני עבור כל n טבעי (8). נוסחה זו אינה כל כך יפה-איננו יודעים את ערכו של a (רק על קיומו) וכן איננו יודעים אלו הם המספרים הראשוניים המתקבלים. אך לפחות ידוע לנו כי נוסחה כזו קיימת.

__תרגיל 8__

הראה כי שום פולינום $f(x) = a_o + a_1x + a_2x^2 + \dots + a_nx^n$ בעל מקדמים שלמים, אשר מציבים בו מספרים טבעיים אינו יכול ל"תת" מספרים ראשוניים בלבד.

__רמז:__ ההוכחה בדרך השלילה. נניח כי, $f(m) = p$ כאשר m ו p הם שלמים קבועים ו p ראשוני. התייחס ל $f(m + kp)$, כאשר k מקבל ערכים חיוביים שלמים והראה כי לא יתכן שמספר זה יהיה ראשוני עבור כל ערך של k.

(iii) נעבור לשלב השלישי שבו מסתפקים בפונקציות אשר בטווח שלהן יש מספר אינסופי של ראשוניים. יש כמובן דוגמאות טריויאליות כמו $f(n) = n$ ו $f(n) = 2n + 1$.

__תרגיל 9__

הראה כי בטווח של הפונקציה $f(n) = 4n + 3$ (התחום: המספרים הטבעיים יש אינסוף מספרים ראשוניים. (רמז: תוכל להוכיח זאת באופן דומה להוכחה בדבר קיום מספר אינסופי של מספרים ראשוניים).

המתמטיקאי דיריכלה (במאה ה-19) הוכיח כי עבור מספרים שלמים וזרים כלשהים a ו b, פונקציות מהצורה $f(n) = an + b$ (התחום: המספרים הטבעיים) "מייצרות" מספר אינסופי של מספרים ראשוניים.
זהו משפט חשוב מאוד וקשה להוכחה (2), (3).

תרגיל 10

א. הראה (בעזרת המשפט האחרון) כי קיים מספר אינסופי של מספרים ראשוניים שבהם מופיעה הספרה 0 לפחות 89 פעמים רצופות.

ב. התוכל להכליל את הטענה?

ב-1963 הוכיח Bredihin כי הפונקציה: $f(x,y) = x^2 + y^2 + 1$ (התחום: הזוגות של מספרים טבעיים) מייצרת אינסוף מספרים ראשוניים.

(iv) בשלב הרביעי ניתן כמה דוגמאות לפונקציות המספקות מספר סופי של מספרים ראשוני

$f(n) = n^2 - n + 41$ עבור כל $n \leq 40$

$f(n) = n^2 - 79n + 1601$ עבור כל $n \leq 79$

$f(n) = 2n^2 + 29$ עבור כל $n \leq 28$

הערה: אלו הן דוגמאות טובות להמחיש כי "אינדוקציה" על סמך בדיקת שורה של מקרים אינה נכונה מבחינה מתמטית.

לסיום נציג כמה "שאלות פתוחות" בנושא:

1. האם הפונקציה $f(n) = n^2 + 1$ "מייצרת" אינסוף מספרים ראשוניים? (ההשערה היא כי התשובה חיובית).

2. האם קיימים אינסוף מספרים ראשוניים הנכתבים רק בעזרת הספרה 1? למשל 11 או 11111111111111111111111 מקיימים את התנאים.

3. האם קיימים אינסוף מספרים ראשוניים, אשר נשארים ראשוניים גם אחרי כל השינויים האפשריים של סדר ספרותיהם?
למשל 13 ו 113 הם כאלה שכן 13 ו-31 הם ראשוניים וגם 113, 131 ו- 311.

4. האם כל מספר זוגי (גדול מ 2) הוא סכום של שני מספרים ראשוניים?
(לפני כמאתיים שנה שיער גולדבך כי התשובה חיובית).

5. האם עבור כל n קיים מספר ראשוני בין n^2 ו $(n + 1)^2$?

מקורות:

1. אברהם הלוי פרנקל, מבוא למתמטיקה, כרך ראשון, הוצאת "מסדה", תשכ"ו.

2. T.M. Apostol, *Introduction to Analytic Number Theory;* Springen Verlag, 1976.

3. H. Rademacher, *Lectures on Elementary Number Theory;* Blaisdell Publ., 1964.

4. W.J. Le Veque, *Topics in Number Theory;* Addison-Wesley, 1956.

5. R. Honsberger, *Mathematical Gems II;* Mathematical Association of America, 1975.

6. J.P. Jones, D. Sato, H. Hada and D. Wiens, *Diophantine Representation of the Set of Prime Numbers;* American Mathematical Monthly 83 (1976), 449-464.

7. I.N. Herstein and I. Kaplansky, *Matters Mathematical;* Harper & Row, 1974.

8. U. Dudley, *History of a Formula for Primes;* American Mathematical Monthly 76 (1969), 23-28.