

מדור חדשות מתמטיות

פרופ' (אמריטוס) נצה מובטוביץ-הדר



חברת סגל בטכניון משנת 1975. כיהנה כדיקנית הפקולטה לחינוך במדע וטכנולוגיה, ניהלה את המוזאון הלאומי למדע, טכנולוגיה וחלל בחיפה, הייתה מורה למתמטיקה במשרה מלאה 12 שנה ובתוך כך נשלחה מטעם הפיקוח לאוניברסיטת קולומביה בניו יורק כדי להביא לישראל את "תוכנית קולומביה". הנהיגה צוותי כתיבה של תוכניות לימודים חדשניות במתמטיקה, בהן סדרת המשדרים "חשבון פשוט" ועליהן קיבלה הטלוויזיה החינוכית פרסים בין-לאומיים. פרופ' מובטוביץ-הדר פרסמה מאמרים רבים ושני ספרים, והעמידה דור של מורים למתמטיקה ותלמידי מחקר. הקימה בשנת 1987 את "קשר חם" - מרכז מו"פ לקידום שיפור וריענון החינוך המתמטי בישראל ועומדת בראשו מאז. מאז צאתה לגמלאות היא מתמסרת לפיתוח הבזקי חדשות ושילובם בהוראת המתמטיקה בחטיבה העליונה ולהמשך פיתוח אתר "רמזור למורה".

לאחרונה פיתחה עבור "קמפוס 10" קורס מוק בשם "מתמטיקה - המלכה והמשרתת של ההווה האנושית" עם צוות מט"ח.

מדור חדשות מתמטיות

נצה מובשוויץ-הדר

אי אפשר למצוא את הפתרון לחידת סודוקו מבלי לנסות תחילה אפשרויות רבות. האם יכול להיות שהסיבוכיות הנראית לעין של בעיות מסוימות ב- NP היא רק אשליה ולכל בעיה ב- NP יש אלגוריתם כלשהו שיכול למצוא לה פתרון (ואז $P=NP$) או שמא יש בעיות שלכאורה הן פתירות ואפשר לבדוק כל ניחוש, אבל למעשה הן יישארו לנצח מחוץ לתחום ההישג של השכל האנושי? מסגרת המחקר היא תורה חדשה יחסית שנקראת **תורת הסיבוכיות** (complexity theory). למרות עשרות שנים של מאמצים של חוקרים בתחום תורת הסיבוכיות החישובית (computational complexity) – התחום העוסק בחקר שאלות על הקושי הפנימי הטמון בבעיות לסוגיהן – פתרון לשאלת P לעומת NP עדיין לא נראה בר השגה. אף כי הנטייה הגורפת היא להאמין ש- $P \neq NP$ אינן קבוצות שוות, כלומר שיש בעיות ב- NP שאינן ב- P , אפילו לא ברור איך יכולה להתחיל הוכחה לכך. נראה שהניסיון להוכיח שבעיות חישוביות מסוימות אינן "קלות" לפתרון הוא משימה קשה. אבל למה זה קשה כל כך? וכמה זה קשה? שאלות אלו מניעות את התחום קדימה באמצעות הפניית העדשות של תאוריית הסיבוכיות חזרה אל תוך עצמה. זוהי בעצם סיבוכיות-על.

במאמר **מומלץ ביותר** שכותרתו "המסע בן 50 שנה של תורת הסיבוכיות אל גבולות הידע" והתפרסם באוגוסט 2023 בעיתון האינטרנטי Quanta Magazine, הציג בן ברובייקר (Ben Brubaker) בקצרה ובחן רב את סיפורה של הדרך הארוכה והמפותלת בת 50 שנה בערך שהחלה מהמחקר על בעיית P לעומת NP והתקדמה עד אל המחקר העכשווי על סיבוכיות-על. זה לא היה מסע קל. הדרך הייתה זרועה במכשולים ובחסימות, וחזרה על עצמה שוב ושוב. עם זה בעבור חוקרי סיבוכיות-על, המסע עצמו אל חבל ארץ פראי ובלתי נודע הוא מקור לסיפוק רב.

חוקרים התעניינו בשאלה של גבולות החשיבה המתמטית הפורמלית זמן רב לפני שהבעיה P לעומת NP הועלתה לראשונה. בשנת 1921, זמן רב לפני תחילת התקופה של מדעי המחשב המודרניים, הציע המתמטיקאי דייוויד הילברט (David Hilbert) שהתמודד עם אותה שאלה, תוכנית מחקר לביסוס המתמטיקה בוודאות מוחלטת על יסודות איתנים. הוא קיווה להתחיל מהנחות פשוטות אחדות,

הידעתם? בשנים האחרונות, בכל שנה מתווספים למעלה מ-125,000 פריטים המתפרסמים ב-650 כתבי עת מתמטיים למאגר המידע הבין-לאומי המנוהל בידי החברה המתמטית האמריקאית MathSciNet: AMS database of reviews, abstracts and bibliographic info. רוב הפריטים מכילים תוצאות חדשות ב-97 ענפי המתמטיקה לסוגיהם.

מדור החדשות בגיליון זה שהוא גיליון העשור ומוקדש לחשיבה מתמטית, מתמקד הפעם בשלוש שאלות הקשורות לכך: מדוע קשה להוכיח שבעיות מתמטיות הן קשות להוכחה? האם הוכחת השערת פרמה בידי אנדרו וויילס לפני 30 שנה הייתה סוף הדרך? איך חשיבה מחוץ לקופסה הביאה לאחרונה לתגלית מתמטית בתחום הריצופים?

מדוע קשה להוכיח שבעיה מתמטית היא קשה להוכחה? על תורת הסיבוכיות וסיבוכיות-על

הבעיה "האם P שווה ל- NP ?" היא אחת משבע הבעיות שנודעו בשם **בעיות המילניום** והיא מעסיקה כבר עשרות שנים את הקהילייה העוסקת במחקר מתמטי. בבעיה זו P ו- NP הם סמלים של שתי קבוצות של בעיות מתמטיות חישוביות, אולי השתיים המפורסמות ביותר, באוסף הולך וגדל של מאות קבוצות של בעיות מתמטיות שהחוקרים ממיינים לכל מיני מחלקות מבחינת הקושי לפתור אותן. בלשון פשוטה, הקבוצה P היא אוסף של כל הבעיות שאפשר לפתור אותן בעזרת אלגוריתם (הליך) ידוע, למשל, לעשות רשימה ארוכה של שמות לפי סדר אלף-בית של האות הראשונה או למצוא שורש של מספר ממשי בקירוב רצוי. הבעיות האלה נחשבות ל"קלות". הקבוצה NP היא אוסף של כל הבעיות שאם יש הצעה לפתרון, אפשר לבדוק אותו בקלות ולדעת אם הוא נכון או שגוי, כמו למשל פתרון לחידת סודוקו, אבל לא ידוע אלגוריתם שמאפשר למצוא להן פתרון. מכיוון שקל לבדוק גם את פתרון של כל הבעיות הנחשבות קלות לפתרון, כל בעיה ב- P היא גם ב- NP . השאלה היא האם כל בעיה ב- NP היא גם ב- P (ואז שתי הקבוצות שקולות) או שיש בעיות מסוימות ב- NP שאינן ב- P , כלומר אין אלגוריתם שמאפשר למצוא להן פתרון. למשל ככל הנראה



כלומר אקסיומות, ולפתח תורה מתמטית מאוחדת שעומדת בשלושה תנאים מרכזיים: עקביות, שלמות וכריעות.

התנאי הראשון של הילברט, **עקביות**, היה הדרישה החיונית שמתמטיקה תהיה נקייה מסתירות. שהרי אם אפשר להוכיח שתי טענות הצהרתיות שסותרות זו את זו על בסיס אותן אקסיומות, התורה כולה תלך לאבדון. אבל תורה יכולה להיות נקייה מסתירות ועדיין מוגבלת בטווח שלה. זה היה המניע לתנאי השני של הילברט, **שלמות**: זוהי הדרישה שאפשר להוכיח כל טענה מתמטית הצהרתית נכונה מתוך מערכת האקסיומות. התנאי השלישי, **כריעות**, דרש קיום של אלגוריתם שיאפשר להכריע, כלומר לקבוע קביעה חד־משמעית אם טענה מתמטית כלשהי היא אמת או שקר. בנאום בוועידה ב-1930, הכריז הילברט: "הסיסמה שלנו תהיה: 'אנחנו חייבים לדעת, אנחנו נדע'". ('We must know, we will know').

שנה בלבד לאחר מכן הנחית הלוגיקן קורט גדל (Kurt Gödel) את המכה הראשונה על חלומו של הילברט. הוא הוכיח שמתוך כל מערכת של אקסיומות אפשר להסיק טענה שסותרת את עצמה. נתייחס למשל אל הטענה האומרת: "את הטענה הזאת אי אפשר להוכיח". אם אכן אי אפשר להוכיח טענה זאת, אז היא מעידה על כך שהתורה אינה שלמה, ואילו אם אפשר להוכיח אותה, אז ההוכחה מראה על נכונות הטענה שאי אפשר להוכיח את הטענה, ומתוך כך נסתם הגולל על העקביות של התורה – תוצאה גרועה עוד יותר. באותו מאמר הוכיח גדל גם ששום תורה מתמטית לא תוכל להוכיח את העקביות של עצמה. עדיין חוקרים קיוו למצוא תורה מתמטית כריעה, גם אם לא שלמה. הם קיוו שיוכלו לפתח שיטות וכלים לזיהוי כל הטענות שכן אפשר להוכיחן מתוך התרחקות מהצעות בעייתיות כמו זו שהציע גדל. הצרה הייתה שאיש לא ידע איך לפתח כלים כאלה בשיטתיות.

ואז בשנת 1936 סטודנט לתואר שני בן 23 ששמו אלן טיורינג (Alan Turing) ניסח מחדש את תנאי הכריעות של הילברט בשפת החישוביות שהייתה חדשנית אז והנחית עליו מכה אנושה. טיורינג הציע מודל מתמטי – הידוע כיום בשם מכונת טיורינג – שיכול לייצג כל אלגוריתם שיש. הוא הראה שאילו ההליך שחיפש הילברט היה קיים, היה אפשר לייצג אותו בעזרת מכונת טיורינג, ואז השתמש בשיטות דומות לאלו של גדל (הפניה עצמית) כדי להוכיח את קיומן של טענות שאי אפשר להכריען או בלשון שקולה, קיומן של בעיות שאי אפשר לחשב אותן בשום חישוב וששום אלגוריתם לא יכול לפתור.

התוכנית של הילברט הייתה לעיי חורבות: לנצח יהיו

מגבלות יסוד על מה שאפשר להוכיח ועל מה שאפשר לחשב. אבל עם זה, במהלך ההתפתחות של המחשבים מרעיונות תאורטיים מופשטים למכונות של ממש, הבינו החוקרים שההבחנה שיצר טיורינג בין בעיות פתירות לבעיות בלתי פתירות, הניחה למעשה שאלות רבות ללא מענה. לכן עד שנות השישים של המאה העשרים, פיתחו מדעני המחשב אלגוריתמים מהירים למדי לצורך פתרון של בעיות מסוימות, בעוד עבור בעיות רבות אחרות האלגוריתמים היחידים שהיו ידועים היו איטיים עד מאוד. השאלה שהציקה לא הייתה רק **האם** אפשר לפתור את הבעיה, אלא **עד כמה קשה** לפתור אותה. לעיתים הבדלים קטנים בין שתי בעיות משפיעים השפעה רבה על רמת הקושי לפתור אותן.

כדי להמחיש זאת, ברובייקר בוחן במאמר הנזכר לעיל צמד בעיות דומות שעוסקות בגרפים. כאן גרפים הם רשתות של נקודות המחוברות בקווים. כל נקודה נקראת צומת וכל קו נקרא צלע או קשת. מדעני מחשב משתמשים בגרפים כדי לבנות מודלים לכל דבר כמעט, החל בחישוב קוונטי ועד לזרימת התעבורה (המתעניינים מוזמנים לקרוא על פרדוקס התעבורה באתר "**רמזור למורה**").

שתי הבעיות עוסקות במציאת מסלול שעובר **בכל צימת** או **בכל צלע** של הגרף פעם אחת ויחידה. להלן הבעיה הראשונה: נניח שנותנים לך גרף קטן ופשוט ומבקשים אותך למצוא משהו שנקרא מסלול המילטון – מסלול שעובר בכל צומת פעם אחת ורק אחת. די ברור שאפשר לפתור את הבעיה הזאת כי יש רק מספר סופי של מסלולים אפשריים, כך שבמקרה הכי גרוע אפשר פשוט לבדוק כל אחד מהם. אך מה אם יש הרבה צמתים? עבור גרפים גדולים יותר, האפשרויות הרבות הופכות את האלגוריתם הפשוט שלנו (בדיקת כל האפשרויות) לחסר תועלת. אומנם יש אלגוריתמים מתוחכמים ויעילים יותר למציאת מסלול המילטון, אבל גם הזמן הדרוש בשבילם למציאת פתרון גדל גדילה מעריכית (אקספוננציאלית) עם גודל הגרף. במילים אחרות, מיטב האלגוריתמים הידועים לא יצליחו למצוא מסלול בפרק זמן 'סביר' (כשהכוונה ב'סביר' היא ל"לפני שהיקום יבוא אל קיצו..."). לבעיית מסלול המילטון יש תכונה מעניינת נוספת. אם מישוהו טוען שמצא מסלול המילטון על גרף מסוים, הוא יכול לבדוק במהירות אם הפתרון אכן נכון, גם אם הגרף גדול מאוד. כל מה שצריך לעשות הוא לעקוב אחר המסלול, לסמן את הצמתים בזה אחר זה, ולוודא שאף צומת לא מסומן פעמיים. אם בסוף הבדיקה לא חסרים צמתים, המסלול הוא אכן מסלול המילטון. הזמן הדרוש לביצוע אלגוריתם לבדיקת פתרונות הוא פרופורציונלי לגודל



מסוימת שיש לה תכונה מוזרה, היא "אוניברסלית". זוהי בעיה שאם ימצא אלגוריתם פולינומיאלי שיכול לפתור אותה, הוא יכול לפתור גם כל (!) בעיה אחרת במחלקה NP . במילים אחרות די לפצח את הבעיה הזאת וכל שאר הבעיות ב- NP יפתרו איתה. הבעיה האוניברסלית של קוק כנראה הפרידה את הבעיות הקשות לכאורה מהבעיות הקלות. אבל קוק הבין שלמצוא אלגוריתם פולינומיאלי כזה שיפתור את הבעיה האוניברסלית שזיהה, זה אתגר גדול ורחוק מאוד מלהיות עניין של מה בכך.

בערך באותו זמן זיהה לאוניד לוי (Leonid Levin), סטודנט לתואר ראשון בברית המועצות, כמה וכמה בעיות אוניברסליות וגילה תוצאה דומה לתוצאה של קוק. שנה לאחר מכן גילה החוקר ריצ'רד קארפ (Richard Karp) כי תכונה זו שנקראה לימים NP -completeness, מאפיינת כמעט כל בעיית NP שעבורה טרם נמצא אלגוריתם פולינומיאלי.

משמעות הדבר היא שכל הבעיות שהן NP -complete – בעיית מסלול המילטון, סודוקו ואלפי אחרות – הן שקולות במובן הכי מדויק. מתברר כמעשה כשפים שכל הבעיות המגוונות האלו הן בעצם וריאציה על אותה בעיה, אבל עדיין אנחנו לא יודעים אם הבעיה האחת הזאת היא פתירה או לא, האם יש בעבורה אלגוריתם פולינומי או לא. כעת כל מה שנשאר לעשות בתורת הסיבוכיות הוא לפתור בעיה אחת: האם $P = NP$ או לא?

כדי להוכיח שמתקיים השוויון $P = NP$, יצטרכו החוקרים למצוא אלגוריתם מהיר (פולינומיאלי) לפתרון בעיה כלשהי באוסף NP -complete. לא ידוע אם יש פתרון כזה ואין ערובה לכך שזה יקרה בזמן הקרוב. עד כה התגלו אלגוריתמים גאוניים לפתרון בעיות שנראו לכאורה קשות (אם כי לא ב- NP -complete) וזה דרש עשרות שנים של עבודה.

כדי להוכיח שמתקיים $P \neq NP$, חוקרים של תורת הסיבוכיות יצטרכו לקבוע שאין ולא יכול להיות אלגוריתם מהיר (פולינומיאלי) לפתרון בעיה כלשהי באוסף NP -complete ולמעשה לסכל את המאמצים של כל מי שמנסה להוכיח ש- $P = NP$.

עדיין השאלה נשארה בלי מענה. יש המשווים חשיבה על השאלה 'מה אפשר לחשב?' לניסיון למיפוי גאוגרפי של שטח עצום שאין יכולת לראות את כולו. אנחנו נמצאים בתחתית ההר ולא יכולים לתצפת מפסגתו על הנוף, אלא במקרה הטוב לקפוץ למעלה ולמטה כדי לקבל תצפית טובה קצת יותר. אי-הידעה מאיפה להתחיל היא חלק מהבעיה. אבל זה לא שחוקרים לא ניסו. במהלך עשרות

הגרף ולכן הוא ישים בזמן סביר גם כשמדובר בגרפים גדולים. זוהי דוגמה לאלגוריתם פולינומיאלי, כלומר כזה שזמני ההרצה שלו גדל כפונקציה פולינומיאלית של גודל הגרף. צמיחה פולינומיאלית היא מרוסנת בהשוואה לצמיחה מעריכית, ולכן אלגוריתמים פולינומיאליים הם בני ביצוע בזמן סביר גם כשמדובר בגרפים גדולים. הם יעילים במידה ניכרת יותר מאלגוריתמים שזמן ההרצה שלהם גדלים כפונקציה מעריכית של גודל הגרף.

ובכן, בבעיית מסלול המילטון יש הבדל גדול בין אימות של פתרון לעומת איתור של פתרון. אפשר לאמת פתרון באמצעות אלגוריתם פולינומיאלי מהיר, אבל כדי למצוא פתרון נחוץ אלגוריתם מעריכי איטי. הדבר לא אמור להפתיע. הרי יותר קל לזהות יצירת מופת ואמנותית מאשר ליצור יצירה כזאת, יותר קל לבדוק הוכחה מתמטית להשערה נתונה מאשר למצוא לה הוכחה. ובכל זאת, לא לכל הבעיות החישוביות יש תכונה כזאת. למעשה בעיה דומה מאוד למציאת מסלול המילטון מתנהגת אחרת לגמרי.

זוהי הבעיה השנייה: נניח ששוב נותנים לך גרף, אבל עכשיו עליך למצוא בין נקודותיו "מסלול אוילר", מסלול שעובר על כל צלע פעם אחת ורק אחת. שוב, יש אלגוריתם פולינומיאלי לבדיקת פתרונות אפשריים, אבל בניגוד לבעיית מסלול המילטון, כאן יש גם אלגוריתם פולינומיאלי לאיתור פתרון לבעיה בגרף בכל גודל, בתנאי שמדובר בגרף קשיר (כלומר יש מסלול בין כל שני צמתים בגרף) ושכל צומת יוצא מספר זוגי של צלעות – אחרת המסלול עלול להיתקע בצומת שממנו יוצא מספר אי-זוגי של צלעות. מותר שיהיו בדיוק שני צמתים עם מספר אי-זוגי של צלעות, ואלו יהיו נקודת ההתחלה והסיום של המסלול. תורת הסיבוכיות מראה שמסלולים מסוימים נראים קלים לאיתור יותר מאחרים.

גם בעיית מסלול המילטון וגם בעיית מסלול אוילר נמצאות במחלקה NP הכוללת את כל הבעיות שאפשר לבדוק את פתרונותיהן באמצעות אלגוריתמים פולינומיאליים. בעיית מסלול אוילר שייכת גם למחלקה P מכיוון שידוע אלגוריתם פולינומיאלי לפתרונה, אבל ככל הנראה זה לא המצב בבעיית מסלול המילטון. מדוע שתי הבעיות הדומות האלה שונות כל כך זו מזו? – זו המהות של בעיית P לעומת NP .

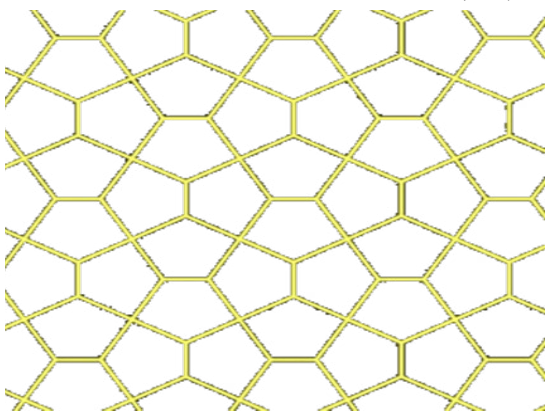
בדומה למה שעשינו בשתי הדוגמאות לעיל, המיון של בעיות חישוב לפי שייכותן ל- NP או ל- P נראה שימושי ומבטיח. בשנת 1971 פרסם החוקר סטיבן קוק (Stephen Cook) תוצאה יוצאת דופן. הוא זיהה בעיית NP



כלשהם. עם השנים נמצא שיש לעקומים אליפטיים קשר לאובייקטים מתמטיים בעלי סוגים רבים מאוד של סימטרייה – תבניות מודולריות (modular forms). בשנות השישים גרמו תבניות אלו למתמטיקאי הקנדי רוברט לנגלנדס (Robert Langlands) לשער השערות מרחיקות לכת, המתוות רשת של קשרים מפתיעים ביותר בין תחומי מתמטיקה למיניהם כגון אריתמטיקה ואנליזה. רשת זאת נקראת כיום "תוכנית לנגלנדס" (Langlands Program)⁴. בקרב מתמטיקאים רבים וגדולים, בהם אנדרו ויילס, היא נחשבת לפרויקט הגדול ביותר של המתמטיקה בת־זמננו ואפילו בתור העתיד של המתמטיקה.

פריצת דרך בנושא הריצופים - פתרון בעיית הריצוף הלא רגולרי

במדור החדשות של גיליון 4 (כאן, עמ' 4–11)⁵ כתבתי על בעיית הריצוף במחומשים שהמחקר עליה היה מסקרן. הריצופים באריחים שמתחברים צלע־אל־צלע וקודקוד־אל־קודקוד המוכרים לנו, רובם ככולם הם מחזוריים, כלומר יש להם סימטרייה של הזזה, יש וקטור הזזה שגורם לריצוף (האינסופי) להתלכד עם עצמו. במילים אחרות, יש אריח יסודי או יחידה כלשהי של אריחים צמודים שחוזרת על עצמה. לדוגמה, לריצוף המחומש האינסופי שחלקו מופיע באיור 1 יש שלושה וקטורי הזזה שיכולים לגרום לו להתלכד עם עצמו (מה כיווניהם?). באופן טבעי עולה השאלה: האם יש ריצופים לא מחזוריים? כלומר ריצופים שאין להם וקטור הזזה כזה? התשובה היא כן – יש אינסוף ריצופים כאלו.



איור 1

4. מומלץ בחום ולצפות בווידאו שבו המתמטיקאי אלכס קנטרוביץ, פרופסור באוניברסיטת ראטגרס, השוקד על הנגשת המתמטיקה בת זמננו לציבור, מנחה את הצופים בדרך ידידותית וציורית לצורך היכרות עם התוכנית (כאן). כמו כן מומלץ לקרוא על modular forms כפעולה הבסיסית החמישית של המתמטיקה (נוסף על ארבע פעולות החשבון) במאמר שהופיע בספטמבר 2023: <https://www.quantamagazine.org/ behold-modular-forms-the-fifth-fundamental-operation-of-math-20230921>

5. כאן אציין ואומר שבגיליון הקודם נפלה טעות במילה ממשיים והכוונה לשלמים.

השנים תקפו החוקרים את הבעיה מזוויות רבות ונתקלו שוב ושוב במבוי סתום.

כשיש לפנינו תופעה כל כך עמידה, אנחנו רוצים מאוד הסבר כלשהו לכך. מומלץ ביותר לקרוא כאן את כל הסיפור שברובייקור¹ פורס לפני הקוראים של Quanta Magazine, על הדרך רבת המכשולים וההישגים שהושגו עד ימינו בניסיון להבין את גבולות הידע המתמטי.

מלאו 30 שנה להוכחת השערת פרמה. מה הלאה?

הנטייה הטבעית שלנו היא לחשוב שכאשר השערה עיקשת זוכה להוכחה, נחתם בכך פרק מתמטי שהמתין זמן ממושך להשלמת הפיתוח שלו. מה שקרה להשערת פרמה בשלושים השנה שעברו מאז הוכחתה בשנת 1993 בידי המתמטיקאי הבריטי יליד 1953, אנדרו ויילס (Andrew Wiles), מראה שההפך הוא הנכון. בעיה שנפתרה מעלה בדרך כלל אוסף של שאלות חדשות שמאתגרות את המתמטיקאים להמשיך במחקרם. זהו טבעה האמיתי, עתיר היצירה הבלתי נלאית, של התפתחות המתמטיקה בכלל ותורת המספרים בפרט.

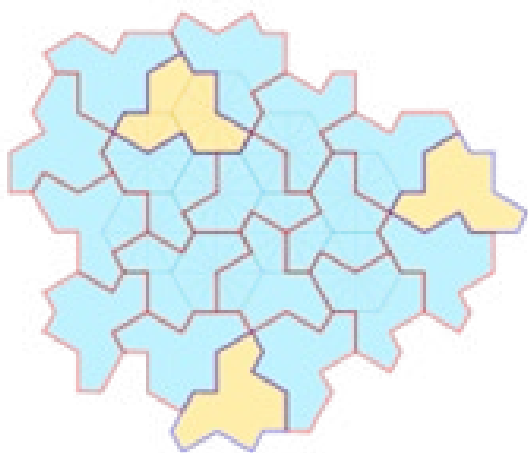
במאה השבע־עשרה, בימיו של המתמטיקאי הצרפתי פייר דה פרמה, היה ידוע שיש אינסוף שלשות של מספרים טבעיים x, y, z שמקיימים את השוויון $x + y = z$, ואינסוף שלשות פיתגוריות המקיימות את השוויון $x^2 + y^2 = z^2$, אבל לא נמצאו שלשות כאלו המקיימות את השוויון $y^n + x^n = z^n$ עבור מעריך שלם n הגדול מ־2. בשנת 1637 כתב פרמה בשולי ספר מתמטיקה שהיה ברשותו, שהוא מצא הוכחה שאין מספרים כאלה. למרבה הצער, פרמה לא מצא לנכון לרשום את ההוכחה לטענתו בשוליים הצרים של אותו ספר והיא זכתה במשך שנים רבות להכרה כ"השערת פרמה" או "המשפט האחרון של פרמה"².

בריאיון לרגל מלאת שלושים שנה לפרסום ההוכחה להשערת פרמה, אמר אנדרו ויילס כי עם פרסום ההוכחה נפתח עידן חדש במתמטיקה.³ בהוכחה נעשה שימוש בעקומים אליפטיים (elliptic curves) – אוספים של נקודות במישור שהרכיבים שלהן x, y מקיימים משוואות שצורתן הכללית היא $y^2 = x^3 + \mu x + \lambda$, עבור μ ו־ λ המסמלים קבועים

1. Brubaker, B. (2023, August 17). Complexity theory's 50 year journey to the limits of knowledge. *Quanta Magazine*. <https://www.quantamagazine.org/complexity-theorys-50-year-journey-to-the-limits-of-knowledge-20230817>
2. לקוראים שאינם מצויים בהשערת פרמה, הידועה כיום בשם "משפט פרמה־ויילס" או "המשפט האחרון של פרמה", מומלץ לעצור לכמה דקות ולקרוא כאן על הדרך בת מעל ל־350 שנה שעשתה השערת פרמה עד להשלמת הוכחתה.
3. הריאיון המלא עם אנדרו ויילס נמשך 25 דקות בערך ואפשר להאזין לו כאן.



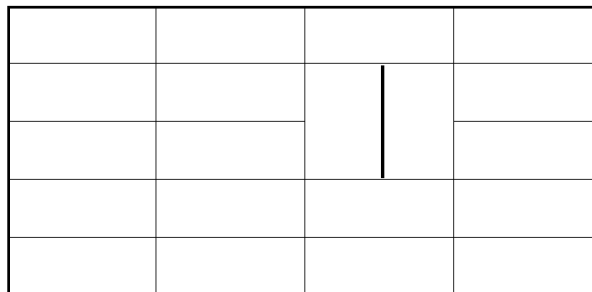
דעת שונים, נמצא לה פתרון שנקרא "אריח הכובע" (ראו איור 4) – אריח שמרצף את המישור עם תמונת הראי שלו. מהר מאוד מצאו אותם החוקרים שיש לא רק אריח אחד כזה, אלא משפחה אינסופית⁷ של אריחים כאלה, וגם אריח שמרצף את המישור ריצוף לא מחזורי ואינו דורש את השותפות של תמונת הראי שלו.



איור 4

6. תוכלו לקרוא עוד על 'בעיית איינשטיין' ופתרונותיה [כאן](#) (באנגלית) וגם [כאן](#) (בעברית). מומלץ לקרוא על עוד הרחבות מעניינות על ריצוף של המישור [כאן](#).

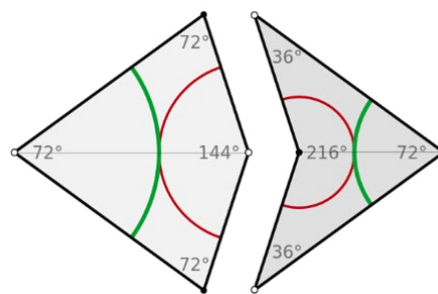
באיור 2 להלן מופיעה דוגמה פשוטה לריצוף באריחים מלבניים חופפים שאין הזזה שיכולה לגרום להתלכדותו עם עצמו – כי מלבד שני המלבנים האנכיים, כל המלבנים האחרים במישור מונחים באופן אופקי.



איור 2

קל ליצור באריחים מלבניים ריצוף מחזורי, כלומר ריצוף שכן חוזר על עצמו בהזזה. די לסובב ב-90 מעלות את שני האריחים המונחים בניצב לכל האחרים. נשאלת השאלה, האם יש אריח או קבוצת אריחים שמרצפים את המישור בריצוף לא מחזורי, אבל **אי אפשר** ליצור באמצעותם ריצוף מחזורי?

גם לשאלה זאת נמצאה תשובה חיובית, ויותר מאחת, עוד בשנות השבעים של המאה העשרים. נמצאו הרבה קבוצות של אריחים כאלה.⁶ הקבוצות הראשונות שנמצאו כללו אריחים רבים מאוד (למשל, [אריחי וואנג](#) היפהיים), ובזמן המרוץ שהתחיל אחר הקבוצה המינימלית של אריחים כאלה נמצא זוג [אריחי פנרוז](#), שנודעו בשם העפיפון והחץ (ראו איור 3).



איור 3

שאלה אחת נשארה בלא מענה – האם יש ריצוף לא מחזורי בעזרת אריח יחיד?

השאלה הזאת זכתה לכינוי "בעיית איינשטיין" (לא, זה לא על שמו של המדען הנודע. מקור השם בגרמנית: אבן אחת, Ein Stein). היא נשארה פתוחה עד שבראשית שנת 2023, לאחר שיתוף פעולה בין ארבעה חוקרים מתחומי

6. תוכלו למצוא [כאן](#) רשימה עם איורים של ריצופים לא מחזוריים