עם כל הכבוד לאלגוריתם הדטרמיניסטי בזמן פולינומיאלי, הצופן לא יישבר

מאת תמיר טסה

הכתבה "המספרים הראשונים יזוהו, הצופן יישבר" ("הארץ", 19.8) דיווחה על מציאתו של אלגוריתם המשמש לבדיקת ראשוניותם של מספרים. אולם המסקנות שגזר הכתב מעצם הגילוי היו סנסציוניות ובלתי מבוססות.

בדיקת ראשוניותם של מספרים היא אכן בעיה קלאסית, בעלת חשיבות תיאורטית ומעשית כאחד. דרך בדיקה פשוטה היא לנסות לחלק את המספר בכל המספרים עד לשורש שלו. אם כל ניסיונות החלוקה נכשלו - לפנינו מספר ראשוני. אך "זמן הריצה" של אלגוריתם כזה הוא בלתי סביר כאשר מדובר במספרים גדולים. בלשון התיאוריה של מדעי המחשב, זמן הריצה של אלגוריתם כזה הוא "מעריכי באורך הקלט". כלומר, אם נרצה לבדוק את ראשוניותו של מספר בעל d ספרות עשרוניות (d מציין במקרה זה את "אורך הקלט"), מספר פעולות החלוקה שנצטרך לבצע יהיה, בקירוב, עשר בחזקת d/2 . למשל, לצורך בדיקת הראשוניות של המספר 728639 (שעבורו d=6), מספר הפעולות שנצטרך לבצע יהיה בקירוב עשר בחזקת 3 (d/2), כלומר כאלף פעולות. המשמעות מבחינה מעשית היא שהאלגוריתם נהפך לבלתי מעשי אפילו כשמדובר במספרים צנועים בגודלם. מכיוון שבמימושים של אבטחת מידע אנו נדרשים למספרים

ראשוניים ענקיים (למשל, בני 1024 ביטים, השקולים לכ-309 ספרות עשרוניות), נחוצות דרכים אחרות.

מפאת קוצר היריעה נדלג על היסטוריה בת 300 שנה, שהחלה עם פרמה במאה ה-17 וננחת בשנת 1980, אז פרסם המתמטיקאי מיכאל רבין, חתן פרס ישראל ופרס טיורינג, את גרסתו למבחן של ג.ל. מילר משנת 1976 לבדיקת ראשוניות. מדובר באלגוריתם רנדומלי מהסוג הידוע בכינוי "מונטה קרלו". אלגוריתם כזה עורך סדרת ניסויים על המספר הנתון. אם אחד הניסויים נכשל, האלגוריתם עוצר ומכריז על המספר כפריק (לא ראשוני) בלוויית סימן קריאה בוטח. לעומת זאת, אם כל הניסויים הצליחו, האלגוריתם מצביע על המספר כראשוני בלוויית הערת השוליים "בהסתברות גבוהה מאוד". למשל, אם ההסתברות של מספר פריק לעבור בהצלחה ניסוי בודד היא רבע (25%), ההסתברות שהוא יצלח סדרה של עשרים ניסויים יורדת לרבע בחזקת 20 - מספר זעום ביותר. ככל שנגדיל את מספר הניסויים, כך נקטין את ההסתברות לזהות בטעות מספר פריק כראשוני.

מבחינה מעשית, האלגוריתם פשוט וקל למימוש: הוא עובד במהירות וביעילות, גם על מספרי ענק כמקובל בעסקי ההצפנות, וניתן לממש אותו גם במחשב ביתי. את מספר הניסויים ניתן לכוון כך שנקבל הסתברויות שגיאה זניחות לחלוטין, הנמוכות אלפי מונים מן ההסתברות שמטאור ענק יתרסק על כדור הארץ בטרם יסיים הקורא לקרוא משפט זה.

יש לציין שקיים גם אלגוריתם דטרמיניסטי לבדיקת ראשוניות, כזה המסוגל להכריע את השאלה לכאן או לכאן בוודאות גמורה. זמן הריצה שלו טוב בהרבה מזמן ריצה מעריכי, אך הוא עדיין איננו פולינומיאלי (הכוונה היא לזמן ריצה שבו מופיע אורך הקלט, d, רק בבסיס החזקה, למשל d^2 או d^{10}, להבדיל מ-2^d או 10^d המעריכיים). מכיוון שאלגוריתם מילר-רבין מהיר וקל יותר מהאלגוריתם הדטרמיניסטי, הוא זה המשמש ברוב היישומים.

שלושת המתמטיקאים מהמכון הטכנולוגי של קנפור פיתחו אלגוריתם דטרמיניסטי המכריע באופן ודאי את שאלת הראשוניות/פריקות של מספר נתון, ועושה זאת בזמן ריצה פולינומיאלי. עובדה זו היא המקנה לאלגוריתם זה את חשיבותו, שכן לפני כן לא היה ברור אם בעיית הראשוניות ניתנת להכרעה בזמן פולינומיאלי. אך חשיבות זו היא, לפחות בשלב זה, תיאורטית בלבד. ראוי לציין בהקשר זה שהשאלה העמוקה ביותר בתיאוריה של מדעי המחשב קשורה לאפיון משפחת הבעיות שאותן ניתן לפתור בזמן פולינומיאלי. שאלה זו, כנראה, רחוקה עדיין מפתרון.

וכעת לעניין הצפנים: בדיקת ראשוניותם של מספרים חיונית בעת הקמת מערכות לאבטחת מידע. קביעה זו תקפה, למשל, ביחס למערכת ההצפנה הידועה RSA, שיטת Diffie-Hellman המשמשת להחלפת מפתחות, או פרוטוקול החתימה הדיגיטלית DSA. אך לבעיית בדיקת הראשוניות אין ולא יכולה להיות שום השלכה על שבירת מערכות כאלה. אם היכולת לבדוק

ראשוניות היתה בעלת השלכה כה הרסנית, הרי שכתבה מודאגת בנושא היתה מתפרסמת כבר ב-1980 ואפילו קודם לכן.

כל שיטת הצפנה השייכת למשפחת השיטות של "מפתח פומבי", שאת טבען תיארה הכתבה, משליכה את יהבה על בעיה מתמטית קשה מאוד לפתרון. למשל, שיטת RSA מבוססת על ההנחה שקשה מאוד לפרק מספר נתון לגורמיו הראשוניים אם גורמים אלה הם מספרים מאוד גדולים. בשיטה זו, המפתח הפומבי כולל מספר המהווה מכפלה של שני מספרים ראשוניים ענקיים (אחד הגדלים המקובלים למספרים אלו הוא 512 ביטים, שהם כ-155 ספרות עשרוניות). בעת בנייה של מערכת כזאת, משתמשים באלגוריתם מילר-רבין על מנת למצוא שני מספרים ראשוניים כאלה.

הבעיה העומדת בפני תוקף המעוניין לשבור כזה צופן, כלומר לחשב את המפתח הפרטי מתוך הפומבי על מנת להיות מסוגל לפענח את ההודעות המוצפנות, היא בעיית פירוק מספר לגורמיו הראשוניים. זוהי בעיה שונה בתכלית מבעיית בדיקת הראשוניות, ונכון לעכשיו היא עדיין נחשבת לקשה ביותר. קיימים אלגוריתמים לפתרונה, אך אין הם יעילים כלל ועיקר מול המספרים הגדולים המשמשים בפועל.

האלגוריתם החדש, כמו האלגוריתמים שקדמו לו, מאפשר לזהות בהצלחה מספרים ראשוניים. אלא שמי שמבקש לפרוץ את שיטת RSA איננו נדרש לסתם מספרים ראשוניים, אלא לשני מספרים ראשוניים מאוד מסוימים. כלומר, מי שמבקש לפרק מספר לגורמיו איננו מחפש מספר ראשוני; הוא מחפש מחלק של מספר נתון. וזוהי אופרה אחרת לגמרי.

ד"ר טסה הוא איש סגל בחוג למתמטיקה שימושית באוניברסיטת תל אביב