קונגרואנציות

הסיפור שלנו מתחיל עם בחור גרמני יוצא דופן בשם קארל פרדריך גאוס. גאוס נולד ב 1,777 ואת הכישרון המתמטי שלו הפגין כבר כשתיקן טעות בחישוב של אביו, בגיל שלוש.

כשהגיע גאוס לאחד משיעורי המתמטיקה שלו בבית הספר היסודי, כתור משימה או עונש דרשה המורה מהתלמידים לחבר את כל המספרים מ 1 עד 100. משימה שהייתה אמורה להימשך זמן רב לקחה לגאוס מספר שניות. גאוס יותר מאוחר הודה כי הוא שם לב לכך שישנם 50 זוגות מספרים שסכום כל אחד מהם הוא 101. 100 ו-1 הם זוג כזה, 99 ו-2 הם זוג נוסף, 50 ו 51 הם הזוג האחרון אם אנחנו מתחילים מהקצוות ומתקרבים לאמצע. גאוס פשוט הכפיל את מספר הזוגות (50) בסכום כל זוג (101) והגיע לתוצאה 5,050.

בשנת 1,801, כאשר גאוס הגיע לגיל 24, הוא פרסם את חיבורו Disquisitiones Arithmeticae, חיבור שהניח את היסודות לתורת המספרים המודרנית. בפרק הראשון בחיבור היסטורי זה גאוס מציג את מושג הקונגרואנציה, ועליו ארחיב בסעיף זה.

גאוס אמר כי אם מספר n מודד הפרש בין שני מספרים, אז המספרים הללו שקולים ביחס ל n, אם ההפרש לא יכול להימדד על ידי n אז המספרים אינם שקולים ביחס ל n. נסתכל לדוגמא על n=5, המספרים 13 ו 28 שקולים ביחס ל n כי ההפרש ביניהם (15) מתחלק ב 5 (או בלשונו של גאוס, נמדד על ידי 5). כדוגמא נוספת ניקח את 23 ו 13, מספרים אלו שקולים ביחס ל 10, הם שקולים גם ביחס ל 5 וגם ביחס ל-2.

גאוס השתמש בסימון ≡ בכדי לתאר שקילות של שני מספרים ביחס למספר מסוים. הוא בחר בסימון הזה, המזכיר מאוד את סימן השוויון האלגברי, כי כפי שנראה מיד, הדמיון בין הפעולות הללו הוא מרתק. הבה נגדיר במדויק את מושג הקונגרואנציה:

הגדרת הקונגרואנציה

יהי n מספר טבעי. נאמר שמספרים שלמים a ו- b הם שקולים מודולו n ונסמן

$$a \equiv b (\mathrm{mod}\, n)$$

אם n מחלק את ההפרש $a-b$, כלומר אם קיים k טבעי כך ש $a-b=kn$.

בכדי לעקל את ההגדרה הבט בדוגמאות הבאות:

$$14 \equiv 8 (\mathrm{mod}\, 6)$$

$$-5 \equiv 1 (\mathrm{mod}\, 3)$$

$$-11 \equiv -3 (\mathrm{mod}\, 4)$$

נשים לב שכל שני מספרים שלמים שקולים זה לזה מודולו 1, וששני מספרים שקולים זה לזה מודולו 2 אם ורק אם שניהם זוגיים או שניהם אי זוגיים.
בהינתן מספר שלם a, נסמן ב q וב-r את המנה והשארית המתקבלות מחילוק a ב-n. כלומר,

$$a = qn + r$$
$$(0 \le r < n)$$

מהגדרת השקילות מודולו n מקבלים ש $a \equiv r$. יש n ערכים אפשריים ל r ולכן כל מספר מודולו n שקול לאחד מהמספרים $0,1,2,...,n-1$.

אנו לא נכנס לפרטי ההוכחה אבל מתברר שמספר רב מהתכונות של אופרטור השוויון מקיים גם אופרטור השקילות, ביניהן: רפלקסיביות, סימטריות, טרנזטיביות, ועוד. הנה רשימה המסכמת את הדומה בין אופרטור השוויון לאופרטור השקילות:

א. $a \equiv a(\bmod n)$ **(רפלקסיביות)**.
ב. $a \equiv b(\bmod n) \Leftrightarrow b \equiv a(\bmod n)$ **(סימטריות)**.
ג. אם $a \equiv b(\bmod n)$ ו $b \equiv c(\bmod n)$, אז $a \equiv c(\bmod n)$ **(טרנזטיביות)**.
ד. אם $a \equiv b(\bmod n)$ ו $c \equiv d(\bmod n)$, אז $a + c \equiv b + d(\bmod n)$ ו $ac \equiv bd(\bmod n)$.
ה. אם $a \equiv b(\bmod n)$, אז $a + c \equiv b + d(\bmod n)$ ו $ac \equiv bd(\bmod n)$.
ו. אם $a \equiv b(\bmod n)$, אז $a^k \equiv b^k(\bmod n)$.

נביט על דוגמא בכדי לעקל את תכונות השקילות, ואת דרך השימוש בהן בכדי להתמודד עם תכונות התחלקות של מספרים גדולים: ננסה להראות ש 41 מחלק את $2^{20} - 1$:

נשים לב תחילה כי

$$2^5 \equiv -9(\bmod 41)$$

לכן לפי (ו)

$$(2^5)^4 \equiv (-9)^4(\bmod 41)$$

אבל

$$81 \equiv -1(\bmod 41)$$

ולכן

$$81 \cdot 81 \equiv 1(\bmod 41)$$

מכאן נגזור את המסקנה:

$$2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0(\bmod 41)$$

כלומר 41 מחלק את $2^{20} - 1$ כנדרש.

אני אציג דוגמא נוספת: הוכח כי $4444^{3333} + 3333^{4444}$ מתחלק ב 7.
נשים לב כי $4444 \equiv -1(\bmod 7)$ (כי 4445 מתחלק ב 7).

נשים לב עוד כי $3333 \equiv 1 (\mod 7)$ (כי 3332 מתחלק ב 7).
לפי (ו) נאמר כי

$$4444^{3333} \equiv (-1)^{3333} \equiv -1 (\mod 7)$$

ו

$$3333^{4444} \equiv 1^{4444} \equiv 1 (\mod 7)$$

נחבר את הקונגרואנציות ונקבל כי

$$4444^{3333} + 3333^{4444} \equiv (-1) + 1 \equiv 0 (\mod 7)$$

כפי שרצינו להוכיח.

נסתכל על דוגמא נוספת. הפעם נוכיח כי לכל מספר טבעי n החלוקה של 2^n ב-7 אף פעם לא תשאיר שארית של 3. (למען האמת נוכיח יותר מזה).

ובכן, כל מספר טבעי n יכול להשאיר שארית של 0,1 או 2 בחלוקה של 3. ובניסוח מתמטי n יכול ללבוש את אחת הצורות הבאות: $n = 3k$, $n = 3k+1$ או $n = 3k+2$ (לכל k שלם). נטפל בכל אחד מהמקרים ונראה כי באף מקרה החלוקה של 2^n ב 7 לא משאירה שארית 3.

עבור $n = 3k$ נאמר כי

$$2^n = 2^{3k} = (2^3)^k = 8^k \equiv 1^k \equiv 1 (\mod 7)$$

קיבלנו כי כאשר n מתחלק ב 3 השארית של 2^n בחלוקה של 7 היא תמיד 1. לדוגמא:

$$2^6 = 64 = 63 + 1 \equiv 0 + 1 \equiv 1 (\mod 7)$$

נבדוק את השארית עבור $n = 3k+1$:

$$2^n = 2^{3k+1} = (2^3)^k \cdot 2 = 8^k \cdot 2 \equiv 1^k \cdot 2 \equiv 2 (\mod 7).$$

ולסיום נבדוק את השארית עבור המקרה בו $n = 3k+2$:

$$2^n = 2^{3k+2} = (2^3)^k \cdot 2^2 = 8^k \cdot 4 \equiv 1^k \cdot 4 \equiv 4.$$

בעצם הוכחנו כי השארית לא רק שלא תהיה 3 אלא גם לא 5, 6 או 0.

תורת הקונגרואנציות לא מסתיימת כאן, ניתן להרחיב את הדיון למערכת של מספר שקילויות על מספר נעלמים. אנו לא נלך לשם, אלא נמשיך ונלמד על שיטת פרמה לפירוק לגורמים.

אני רק tעיר לסיום כי אם המודולו ידוע, נהוג להשמיט אותו. לדוגמא אם אנו יודעים שהמודולו הוא 15 בדוגמא הבאה ניתן לכתוב:

$-30 \equiv 0$

במקום

$-30 \equiv 0 (\mathrm{mod} 15)$

אני מציע שתשחק קצת עם מושג הקונגרואנציות בכדי להבין יותר את הכוח הטמון בו. הסימון ביחד עם הקונספט שגאוס הוריש לנו מהווים כלי מעולה כנגד תהיות התחלקות של מספרים גדולים. אם תרצה נסה למצוא את השארית המתקבלת מחלוקה של הסכום $1^5+2^5+3^5+...+99^5+100^5$ ב 4.

שיטת פרמה לפירוק לגורמים

פרמה (Pierre de Fermat), גאון מתמטי ידוע בעיקר בעקבות המשפט הידוע בכינוי "המשפט האחרון של פרמה", נולד ב 1601, כ 17 עשורים לפני הולדת גאוס. פרמה לא היה מתמטיקאי במקצועו והתייחס למתמטיקה כאל תחביב. העובדה הפשוטה היא שפרמה היה פנומנה מתמטית. הוא הניח את היסודות הטכניים לחשבון האינפיניטסימאלי, ויחד עם גאון מתמטי אחר, בלייז פסקל, פיתח את יסודות תורת ההסתברות.

אבל לתורת המספרים פרמה שמר מקום מיוחד בליבו, ובמוחו. ואליו ניתן לייחס את תחיית העניין בצידה המופשט של תורת המספרים. פרמה העדיף שלא לפרסם את מאמריו ולצערנו גם את הוכחותיו, אבל תודות לתחלופת המכתבים שלו עם גאונים מתמטיים בני זמנו אנו יכולים ללמוד לא מעט על עבודתו וגאונותו.

באחד המכתבים ששלח פרמה לכומר מרסן ב 1643, הציע פרמה שיטה משלו לפירוק מספרים גדולים לגורמים. זו הייתה ההתקדמות הראשונה לפירוק מספרים מאז השיטה הקלאסית, אותה שיטה בה יש לבדוק אם המספר מתחלק עבור כל המספריים האי זוגיים עד לשורש המספר הנתון.
פרמה הבחין כי אם מספר נתון n הוא הפרש של שני מספרים ריבועיים אזי הוא פריק, כי:

$$n = x^2 - y^2 = (x+y)(x-y)$$

ולכן גורמיו הם $x+y$ ו $x-y$.

נסדר קצת את השוויון:

$$x^2 - n = y^2$$

מכיוון ש y^2 הוא תמיד חיובי אנו נסתכל על ה-k המינימאלי המקיים $k^2 \geq n$. לאחר שנחסר את n מ- k^2 נבדוק אם התוצאה היא ריבוע שלם. אם כן אז בעצם $k^2 - n = y^2$ מתקיים ולכן
$n = k^2 - y^2 = (k+y)(k-y)$. מצאנו אם כן זוג גורמים של n.

אם ה $k^2 - n$ אינו ריבוע שלם נעבור לבדוק אם $(k+1)^2 - n$ הוא ריבוע שלם. אם כן מצאנו זוג גורמים של n. אחרת נבדוק את k+2 וכו'...

התהליך אינו יכול להמשיך בלי סוף, שהרי בסופו של דבר נקבל את הפירוק הטריוויאלי $n = n \cdot 1$, או בכתיב הפרש הריבועים:

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

אם הגענו לידי כך נסיק כי n ראשוני.

אתה ודאי תוהה איך העזתי להניח ש n זוגי, שהרי אם n לא היה זוגי המשוואה האחרונה שכתבתי תערב בתוכה שברים. ובכן, ההנחה של פרמה הייתה שקל מאוד לזהות מספר זוגי (הספרה האחרונה שלו היא ספרה זוגית) ולכן בהינתן מספר יש לחלק אותו ב-2 עד שמגיעים למספר אי זוגי ורק אז יש להפעיל את האלגוריתם, מבלי לשכוח כמובן את מספר הפעמים שחילקנו את המספר ב-2.

פרמה השתמש בתהליך זה כדי להגיע לפירוק $2027651281 = 44021 \cdot 46061$ ב 11 צעדים בלבד לעומת 4580 צעדים בשיטה הקלאסית. כמובן שזו הייתה דוגמה טובה במיוחד, שנועדה לקדם את השיטה. אבל בגדול השיטה של פרמה חסכונית הרבה יותר מהשיטה הקלאסית.

אני מציע שנפרק את המספר 19,847 לגורמים בכדי להתרגל לשיטת פרמה. ראשית נמצא מספר x כך שהוא המינימאלי אשר ריבועו גדול מ 19,847. כל שיש לעשות הוא לבדוק את השורש של 19,847 ולעגל למספר השלם הבא. כך נמצא כי $141^2 > 19847 > 140^2$.

נבדוק כעת מתי החיסור של 19847 מריבועי המספרים 141,142,143 וכו' יהיה ריבוע שלם.

$141^2 - 19847 = 34$

$142^2 - 19847 = 317$

$143^2 - 19847 = 602$

$144^2 - 19847 = 889$

$\vdots$

$156^2 - 19847 = 4489 = 67^2$

ואכן, אחרי 16 בדיקות מצאנו כי

$$19847 = 156^2 - 67^2 = (156+67)(156-67) = 223 \cdot 89$$

כעת יש לבדוק אם 223 ו 89 הם מספרים ראשוניים. אנו נדלג על הבדיקה, שאותה ניתן לעשות בשיטת פרמה או בשיטה הקלאסית, שנוחה לשימוש עבור מספרים קטנים. 223 ו 89 הם אכן מספרים ראשוניים. מצאנו את הפירוק המבוקש.

הבה ננסה לפרק מספר נוסף בעזרת שיטת פרמה, המספר 150463. לאחר הוצאת שורש נראה כי $387^2 < 150463 < 388^2$. נתחיל בבדיקה:

$$388^2 - 150463 = 81 = 9^2$$

התמזל מזלנו וכבר בניסיון הראשון מצאנו שני ריבועיים שהפרשם שווה ל 150463. נחשב את הגורמים:

$$150463 = 388^2 - 9^2 = (388+9)(388-9) = 397 \cdot 379$$

379 ו 397 הם מספרים ראשוניים ולכן סיימנו את הבדיקה. ניתן לראות ששיטת פרמה פועלת מהר יותר ככל שההפרש בין הגורמים קטן יותר. זאת כי הבדיקה מסתיימת כאשר ההפרש הוא ריבוע שלם, וככל שריבוע ההפרש קטן יותר כך ההפרש קטן יותר.

אני מציע שתנסה להתמודד עם פירוק המספרים הבאים לגורמים בשיטת פרמה:

1. 1711
2. 11189
3. 117079
4. 19144379

ההכללה של משפט פרמה והשיפור של קראיצ'יק

את משפט פרמה אפשר לקחת צעד אחד קדימה. במקום לדרוש ש n יהיה הפרש של שני מספרים ריבועיים נדרוש שההפרש ביניהם יהיה כפולה של n, או בלשון השקילות נדרוש כי שני מספרים ריבועיים יהיו שקולים מודולו n. בכתיב מתמטי זה נראה כך:

$$x^2 \equiv y^2 \pmod{n}$$

זוהי הכללה של הדרישה הקודמת שלנו שהרי:

$$x^2 \equiv y^2 (\mathrm{mod}\, n) \Leftrightarrow x^2 - y^2 = kn$$

ועבור $k = 1$ נקבל את שיטת פרמה לפירוק לגורמים.

אבל למה ההכלה הזו יעילה יותר משיטת פרמה? ובכן, שקילות היא מושג מאוד סלחני בכל הנוגע להחלפה של מספרים אחד בשני. שוויון מחלק את המספרים השלמים לאינסוף חלקים שאורך כל אחד מהם הוא 1. שקילות מודולו n לעומת זאת מחלקת את המספרים ל n קבוצות בדיוק, וכך ניתן להחליף מספר מאוד גדול במספר קטן הרבה יותר ששקול לו מודולו n. בגלל התכונה הזו של שקילות ניתן לפעול לפי אלגוריתם שפיתח מתמטיקאי בשם קראיצ'יק (Maurice Kraitchik) בשנות ה-20 של המאה העשרים. לפני שאציג את האלגוריתם הבה נסתכל על דוגמא למציאת גורמים לפי קראיצ'יק, וממנה יהיה קל יותר להסיק את האלגוריתם ברמה הכללית שלו.

אנו ננסה לפרק את המספר 9073.

כמו בשיטת פרמה נחפש אחר המספר שריבועו הוא הקטן ביותר הגדול מ 9073. נקבל כי

$$95^2 < 9073 < 96^2$$

עכשיו נחפש אחר מספרים שאם נעלה אותם בריבוע ונחסר **כפולה של** 9073 נקבל מספר קטן יחסית. הנה כמה דוגמאות שניסיתי עד שמצאתי את התשובה:

$$95^2 - 9073 = -48 = -2^4 \cdot 3$$
$$96^2 - 9073 = 143 = 11 \cdot 13$$
$$97^2 - 9073 = 336 = 2^4 \cdot 3 \cdot 7$$
$$136^2 - 2 \cdot 9073 = 350 = 2 \cdot 5^2 \cdot 7$$
$$\vdots$$
$$191^2 - 4 \cdot 9073 = 189 = 3^3 \cdot 7$$

שימו לב שההתייחסות היא לא להפרש אלא לגורמים של ההפרש. אנחנו מחפשים אחר השקילות $x^2 \equiv y^2 (\mathrm{mod}\, n)$ ומכיוון שבצד שמאל של השקילויות תמיד יש לנו ריבועים אנחנו מחפשים אחר שקילויות שאם נכפיל אותם אחד בשני נקבל גם בצד ימין ריבוע שלם. במקרה שלנו זה קורה עם 97 ו 191 כי:

$$(97 \cdot 191)^2 \equiv 2^4 \cdot 3 \cdot 7 \cdot 3^3 \cdot 7 \equiv (2^2 \cdot 3^2 \cdot 7)^2 (\mathrm{mod}\, 9073)$$

אבל

$$(97\cdot 191)^2 \equiv 18527^2 \equiv (381+2\cdot 9073)^2 \equiv 381^2 (\mathrm{mod}\, 9073)$$

ו

$$(2^2\cdot 3^2\cdot 7)^2 \equiv 252^2 (\mathrm{mod}\, 9073)$$

ומכאן נסיק ש

$$381^2 \equiv 252^2 (\mathrm{mod}\, 9073)$$

אם נעביר את 252^2 לצד שמאל של השקילות נקבל

$$381^2 - 252^2 \equiv (381+252)(381-252) \equiv 633\cdot 129 \equiv 0 (\mathrm{mod}\, n)$$

הגענו לכך שהמכפלה של 633 ב 129 שקולה ל n. כעת נמצא את המחלק המשותף המקסימאלי של 129 ו 9073 בעזרת האלגוריתם של אוקלידס. אנו נגיע לכך שהמחלק המשותף המקסימאלי של שני מספרים אלו הוא 43. מכיוון ש 43 מחלק את n והוא גורם ראשוני אז מצאנו גורם ראשוני אחד של n=9073. נחלק את 9073 ב 43 ונקבל 211, שגם הוא מספר ראשוני. אם כך מצאנו את הגורמים של 9073:

$$9073 = 43\cdot 211$$

אני רק אבהיר שלא בדקתי את כל המספרים מ 95 ל 191. כאשר ההפרש בין ריבוע המספר הנבדק לכפולה הנוכחית של 9073 היה גדול מדי הגדלתי ב-1 את הכפולה הנוכחית ב 9073 ושוב חיפשתי אחר ערכים קטנים של ההפרש. לדוגמא, ב 97 כבר הגעתי לכך ש

$$97^2 - 9073 = 336$$

אם הייתי ממשיך ל 98 היינו מגיעים ל

$$98^2 - 9073 = 531$$

ו-531 די גבולי בין ההגדרה האישית שלי לגדול או קטן. לכן הכפלתי את 9073 ב 2 וחיפשתי את המספר המינימאלי שריבועו הוא הקרוב ביותר לפעמיים 9073. המספר הזה היה 135 שהרי

$$135^2 - 2\cdot 9073 = 79$$

אבל לא הייתה לי התנגדות לנסות גם את 134:

$$134^2 - 2 \cdot 9073 = -190$$

נעבור על דוגמא נוספת לפני שנמשיך הלאה. ננסה לפרק את המספר 244241:

אחרי מספר ניסיונות נבחין כי

$$966^2 \equiv 119 \equiv 7 \cdot 17 (\mathrm{mod}\, 244241)$$

וגם כי

$$1398^2 \equiv 2^2 \cdot 7 \cdot 17$$

אבל האבחנה הזו לא תוביל אותנו לשום מקום כי

$$966 \cdot 1398 \equiv 2 \cdot 7 \cdot 17 (\mathrm{mod}\, 244241)$$

הדבר דומה לשוויון 0=0 בשוויון הרגיל, ולכן נצטרך להמשיך ולחפש אחר פיתרון אחר.

הפעם מצאתי שלושה שקילויות אשר המכפלה שלהן נותנת שקילות של שני ריבועים שלמים. אלו השקילויות:

$$856^2 \equiv 13$$
$$1211^2 \equiv 5^2 \cdot 43$$
$$1563 \equiv 13 \cdot 43$$

אם נכפיל את השקילויות נקבל

$$(856 \cdot 1211 \cdot 1563)^2 \equiv (5 \cdot 13 \cdot 43)^2$$

נטפל קודם בצד שמאל

$$856 \cdot 1211 \cdot 1563 \equiv 180255$$

ובצד ימין

$$5 \cdot 13 \cdot 43 \equiv 2795$$

לכן

$180255^2 \equiv 2795^2$

אם נחשב בעזרת האלגוריתם של אוקלידס את המחלק המשותף המקסימאלי בין ההפרש של $180255 - 2795 = 177460$ יצא לנו שהמחלק המשותף המקסימאלי הוא 467. 467 הוא מספר ראשוני ולכן הוא גורם אחד של 244241. את הגורם השני נקבל מחלוקת 244241 ב 467. הגורם השני הוא 523, מספר ראשוני אף הוא. נסכם

$244241 = 467 \cdot 523$

סיכום

זה הפרק הראשון בסדרת פרקים שאני מתכוון לכתוב על תורת המספרים. אני מרגיש קצת אשם עם עצמי על זה שלא תיארתי את האלגוריתם של אוקלידס, ולא דיברתי קצת יותר על הבסיס של תורת המספרים כמו מה זה בדיוק מספר ראשוני, מהן התכונות היפות של המספרים הללו, מה זה מספר משולש, מהי השערת גולדבך וכו'. אבל כל המטרה של הפרק הזה היא שאני אסכם לעצמי את החומר. ולכן הרשתי לעצמי לדלג על החומר הקל יותר.

הפרק הבא כנראה יכלול תיאור של המשפט הקטן של פרמה ומשפט וילסון.

אשמח לשמוע את דעותיכם ולענות על שאלות במייל – webmaster@flashoo.co.il