סיפורן של ספרות היחידה

מאת: שמואל אביטל ומוריס לובר
המחלקה להכשרת מורים, הטכניון, חיפה

ההשקפה הפסיכולוגית המודרנית מדגישה את חשיבות ההפעלה ההדדית בין היחיד, בגיל הילדות, לבין סביבתו. לפי השקפה זו, כל ההתפתחות ההכרתית של היחיד, בשלב הנקרא "שלב ההתפתחות האופרטיבית", מקורה בהפעלה הדדית כזו. המסקנה המתקבלת מהשקפה זו היא, שיש חשיבות מיוחדת להמחשה בגיל זה. כדי שהמחשה זו תהיה יעילה, חיוני שלא תהיה המחשה שבראווה בלבד, אלא המחשה שבהפעלה, כאשר היחיד מתנסה ממש בפעילות של התהוות המושא וביטולו.

הלמידה מתבצעת בתוך תוכו של הלומד, המתאבק בתודעתו בתופעות שהוא שותף, הן ליצירתן, והן לנסיונות המוצלחים והבלתי מוצלחים המביאים לחיסולן או לשינוי צורתן. מאבק זה שבין היחיד לבין סביבתו הוא המקור העיקרי ללמידה, בגיל אשר בו הלומד נמצא בשלב ההתפתחות שהזכרנו. ומה אחר-כך? מה הם המקורות לחיזוק הלמידה כאשר היחיד הגיע למה שמכונה ה"שלב הפורמלי"? האומנם נעשה בלמידתו בלתי תלוי לחלוטין בסביבה, וכל חומר שיוגש לו ייקלט?
מסתבר שאין הדבר כך. אלא שכאן המושג "סביבה" מתרחב ומקיף לא רק את הסביבה הפיסית והחברתית של הלומד, אלא גם את הסביבה האינטלקטואלית שלו עצמו, ומערכת הייחוס שהוא בנה, שהיא סך הכל של כל אותן ההתנסויות שהתנסה בהן בהיסטוריה שלו, ושהוא הצליח להפנים את מסקנותיהן. מערכת זו מורכבת הן מתכנים של חומר לימוד והן ממודלים וסכימות המשמשים כפיגומים לצרכי אירגון של חומר. מערכת זאת מושפעת עתה יותר ויותר מן העושר האינטלקטואלי החרות בתודעתו.

את מקומה של ההתנסות האופרטיבית, כגורם מכריע בלמידה, תופסת עתה המוכרות המוקדמת. בכל שלב של למידה פורמלית, כאשר היחיד נחשף לחומר חדש, הרי מידת הקליטה, מידת היכולת לארגן את החומר החדש בצורת מיבנה, תלויה במידת הקשר של חומר זה לנושאים ולהתנסויות קודמות. רק במידה שהלומד מצליח לקשור בין הנושאים החדשים לבין תחומים שנתקל בהם לפני כן, ושהשאירו את רישומם, ייקלטו נושאים אלה וייהפכו לחלק ממערכת הייחוס של הלומד, הלמידה תהיה בעלת משמעות.
מכאן החשיבות הרבה שיש למודלים בלמידה הפורמלית, כלומר למציאת מערכת נתונים שהיא ידועה ומוכרת ללומד ואשר אליה יכול הוא לקשור את הנושאים החדשים כדי להבינם ולהופכם למיבנים.

כדי שמערכת כזו תמלא את ייעודה, הכרחי שיתמלאו שני תנאי יסוד: א) שהיא תהיה מוכרת היטב ללומד ו ב) שהוא יוכל להטיל עליה חלק משמעותי מן המבנה של החומר החדש. חשיבות מיוחדת יש למערכות היכולות לכסות חלק רציני של נושא שלם, כלומר שהיחיד יכול לקשור אליהן לא רק משפטים בודדים, אלא מערכות של משפטים, בתורה שהוא מנסה ללמדה.

ננסה לתאר כאן מערכת כזו, אשר לחקירתה נוכל לקשור מערכת מקיפה של בעיות ומשפטים בתורת המספרים האלמנטרית. מדובר במערכת של בעיות הדנות בספרת היחידות של מספרים טבעיים, הכתובים לפי בסיסים שונים. נביא כאן דוגמא לשאלות שונות העולות בחקירה זאת, המתקשרות למשפטים יסודיים בתורת המספרים. את המשפטים הקשורים בחקירה נצטט, אבל לא נוכיח אותם. הקורא יכול למצוא את ההוכחה באחד הספרים המצוטטים בסוף המאמר.

החשיבות החינוכית של המערכת שנביא היא בכך, שגם תלמידים בכיתות היסוד, או בחטיבת הביניים, יוכלו לחקור אותה בעצמם, באופן אינדוקטיבי, ולהעלות השערות. ההוכחות עצמן דורשות בגרות מתימטית מסויימת.

ספרות היחידה לפי בסיס עשר הן 0,1,2,3,4,5,6,7,8,9. נעלה ספרות אלה בריבוע ובתוצאות נתבונן שוב רק בספרות היחידה. נקבל, לפי הסדר, 0,1,4,9,6,5,6,0,4,1. לא קבלנו בחזרה את כל עשר הספרות, אלא רק 0,1,4,5,6,9. מובן שנקבל אותה תוצאה אם נתבונן בספרות היחידה של הריבועים של מספרים טבעיים כלשהם. במלים אחרות, אם נחלק ב 10 ריבוע של מספר טבעי כלשהו ונתבונן בשאריות, לא נקבל את כל עשר הספרות, אלא רק את שש הנ"ל. מסיבות אלה נוהגים לכנות מספרים אלה בשם שאריות ריבועיות לפי חילוק ב 10. ומה יקרה אם נעלה את הספרות מ 0 עד 10 בחזקות השלישית, הרביעית וכו'? במלים אחרות: אלו שאריות יתקבלו, בחילוק ב 10, של חזקות שלישיות, רביעיות וכו' של מספרים טבעיים? לשם התבוננות נערוך את התוצאות בטבלה:

טבלה 1: שאריות בחילוק ב 10 של חזקות שונות של מספרים טבעיים הכתובים לפי בסיס עשר

שאריות מסדר ראשון	9	8	7	6	5	4	3	2	1	0
שאריות ריבועיות	1	4	9	6	5	6	9	4	1	0
שאריות החזקות השלישיות	9	2	3	6	5	4	7	8	1	0
שאריות החזקות הרביעיות	1	6	1	6	5	6	1	6	1	0
שאריות החזקות החמישיות	9	8	7	6	5	4	3	2	1	0

מהטבלה ברור שאין טעם להמשיך אחרי החזקה החמישית, כי מחזקה זאת והלאה סדר השאריות יהיה מחזורי (מדוע?).

עיון בטבלה זאת מעלה מספר בעיות:

1. מה תהיה החזקה הבאה עבורה יופיעו שוב כל השאריות לפי הסדר?

2. אם נתעלם מהשארית 0 אנו רואים שבחזקה הראשונה, השלישית והחמישית ערוכות השאריות כך שסכום השאריות, המרוחקות במידה שווה מהקצוות, הוא תמיד 10. (למשל, בחזקה השלישית $1 + 9 = 2 + 8 = 7 + 3 = 4 + 6 = 5 + 5 = 10$). לעומת זאת בחזקה השניה והרביעית שוות זו לזו השאריות המרוחקות במידה שווה מהקצוות.

   האם זה מקרה, או נוכל לגלות סיבה מתימטית לכך?

3. הטבלה מראה שאמנם בחזקה השלישית אנו מקבלים בחזרה את כל ספרות היחידה, אבל <u>לא</u> לפי הסדר. רק בחזקה החמישית קיבלנו שוב את כל ספרות היחידה לפי הסדר המקורי. ושוב האם זה מקרה? מדוע דווקא בחזקה החמישית? האם הסיבה לכך נעוצה בתכונות יסוד של המספרים הטבעיים?

4. שאלה יסודית המתבקשת מאליה היא, מה הם פני הדברים כאשר כותבים את המספרים לפי בסיס שונה מ 10? אם התופעות שגילינו מקורן בתכונות היסוד של המספרים, הרי שהן יחזרו, בצורה מתאימה, גם כאשר נכתוב את המספרים הטבעיים לפי בסיס כלשהו b.

א.

התשובה לשאלה מס' 1 היא מיידית. החזקה הבאה תהיה התשיעית ולאחריה ה- 13 וכו'. כדי לענות לשאלות האחרות ניגש תחילה לחקירה אינדוקטיבית של סדר הופעת השאריות, כאשר המספרים רשומים לפי בסיס b, שונה מ 10. נעשה זאת עבור בסיס שלוש עד חמש עשרה. ברור שברישום לפי בסיס 2 נקבל לסרוגין 0 ו 1. לפיכך נפסח על בסיס זה. כמו כן נפסח על השאריות של החזקות 0 ו 1, כי ברור שאלו שוות תמיד ל 0 ול 1 בהתאמה.

טבלה 2: שאריות בחילוק ב b של חזקות שונות של מספרים טבעיים כאשר <u>המספרים עצמם רשומים לפי בסיס b עבור b בין 3 ו 15.</u>

	בסיס 3	בסיס 4	בסיס 5	בסיס 6	בסיס 7	בסיס 8	בסיס 9	בסיס 11
ספרות יסוד *	1,2	1,2,3	1,2,3,4	1,2,3,4,5	1,2,3,4,5,6	1,2,3,4,5,6,7	1,2,3,4,5,6,7,8	1,2,3,4,5,6,7,8,9, α
שאריות ריבועיות	1,1	1,0,1	1,4,4,1	1,4,3,4,1	1,4,2,2,4,1	1,4,1,0,1,4,1	1,4,0,7,7,0,4,1	1,4,9,5,3,3,5,9,4,1
חזקה שלישית	1,2	1,0,3	1,3,2,4	1,2,3,4,5	1,1,6,1,6,6	1,0,3,0,5,0,7	1,8,0,1,8,0,1,8	1,8,5,9,4,7,2,6,3,α
חזקה רביעית		1,0,1	1,1,1,1		1,2,4,4,2,1	1,0,1,0,1,0,1	1,7,0,4,4,0,7,1	1,5,4,3,9,9,3,4,5,1
חזקה חמישית			1,2,3,4		1,4,5,2,3,6	1,0,3,0,5,0,7	1,5,0,7,2,0,4,8	1,α,1,1,1,α,α,α,1,α
חזקה שישית					1,1,1,1,1,1		1,1,0,1,1,0,1,1	1,9,3,4,5,5,4,3,9,1
חזקה שביעית					1,2,3,4,5,6		1,2,0,4,5,0,7,8	1,7,9,5,3,8,6,2,4,α
חזקה שמינית								1,3,5,9,4,4,9,5,3,1
חזקה תשיעית								1,6,4,3,9,2,8,7,5,α
חזקה עשירית								1,1,1,1,1,1,1,1,1,1
חזקה אחת-עשרה								1,2,3,4,5,6,7,8,9,α

	בסיס 12	בסיס 13	בסיס 14	בסיס 15
ספרות יסוד *	1,2,3,4,5,6,7,8,9,α,β	1,2,3,4,5,6,7,8,9,α,β,γ	1,2,3,4,5,6,7,8,9,α,β,γ,δ	1,2,3,4,5,6,7,8,9,α,β,γ,δ,ε
שאריות ריבועיות	1,4,9,4,1,0,1,4,9,4,1	1,4,9,3,γ,α,α,γ,3,9,4,1	1,4,9,2,β,8,7,8,β,2,9,4,1	1,4,9,1,α,6,4,4,6,α,1,9,4,1
חזקה שלישית	1,8,3,4,5,0,7,8,9,4,β	1,8,1,γ,8,8,5,5,1,γ,5,γ	1,8,δ,8,δ,6,7,8,1,6,1,6,δ	1,8,γ,4,5,6,δ,2,9,α,β,3,7,ε
חזקה רביעית	1,4,9,4,1,0,1,4,9,4,1	1,3,3,9,1,9,9,1,9,3,3,1	1,2,β,4,9,8,7,8,9,4,β,2,1	1,1,6,1,α,6,1,1,6,α,1,6,1,1
חזקה חמישית		1,6,9,α,5,2,β,8,3,4,7,γ	1,4,5,2,3,6,7,8,β,γ,9,α,δ	1,2,3,4,5,6,7,8,9,α,β,γ,δ,ε
חזקה שישית		1,γ,1,1,γ,γ,γ,γ,1,1,γ,1	1,8,1,8,1,8,7,8,1,8,1,8,1	
חזקה שביעית		1,β,3,4,8,7,6,5,9,α,2,γ	1,2,3,4,5,6,7,8,9,α,β,γ,δ	
חזקה שמינית		1,9,9,3,1,3,3,1,3,9,9,1		
חזקה תשיעית		1,5,1,γ,5,5,8,8,1,γ,8,γ		
חזקה עשירית		1,α,3,9,γ,4,4,γ,9,3,α,1		
חזקה אחת-עשרה		1,7,9,α,8,β,2,5,3,4,6,γ		
חזקה שתים-עשרה		1,1,1,1,1,1,1,1,1,1,1,1		
חזקה שלוש-עשרה		1,2,3,4,5,6,7,8,9,α,β,γ		

* הסימנים α,β,γ,δ,ε באים לסמל ספרות המציינות את המספרים 10,11,12,13,14 בהתאמה.

ב. הופעת 0 בחזקות מסויימות

עיון בטבלה מספר 2 מגלה שלפעמים מקבלים שארית ריבועית 0, אף כי העלינו בחזקה שארית שונה מאפס. זה קורה בבסיסים ארבע, שמונה, תשע ובבסיס התריסר. מתברר שדבר זה יקרה בשביל כל בסיס b אשר בפרוק לגורמים שלו מופיע לפחות גורם ראשוני אחד בחזקה גבוהה מ 1 (למשל הפירוק לגורמים של בסיס התריסר הוא $12 = 2^2 \cdot 3$).

הוכחה

הפירוק של הבסיס b יהיה

$$b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i} \ldots p_k^{\alpha_k}$$

כאשר p_j ראשוניים לכל j ו $\alpha_i > 1$

נוכל איפוא לכתוב את b כך:

$$b = p_i \overbrace{(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i - 1} \ldots p_k^{\alpha_k})}^{r}$$

ואז p_i ו r הן שאריות מסדר ראשון של הבסיס b ושתיהן שונות מאפס.

אם נעלה את r בריבוע נקבל כפולה שלמה של b :

$$r^2 = (p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i - 2} \ldots p_k^{\alpha_k})\, b$$

ולכן השארית הריבועית של r שווה לאפס.

נראה למשל לגבי הבסיס 12.

$$12 = 2^2 \cdot 3 = 2(2 \cdot 3)$$

במקרה זה $r = 6$. כלומר 6 היא שארית מסדר ראשון השונה מ 0.

$$r^2 = 6^2 = 3 \cdot 12$$

אם נכתוב זאת בבסיס התריסר נקבל $r^2 = 30_{\text{תריסר}}$ כלומר השארית אחרי חילוק ב $10_{\text{תריסר}}$ תהיה אפס.

ברור כי בבסיסים אלה לא נקבל חזרה בתור שארית את כל הספרות, בשום חזקה שהיא (מדוע?)

לפיכך לשאלה 2 שמנינו לעיל יש משמעות רק ביחס לבסיסים "חופשיים מריבוע" כלומר בסיסים שבהם אף גורם ראשוני איננו מופיע בחזקה גבוהה מ- 1.

ג. סדר הופעת השאריות

אם מסתכלים בטבלה מס' 2, מתברר כי ההבדל בסדר הופעת השאריות, אותו מצאנו בחזקות של שאריות לפי בסיס 10, נשמר בכל הבסיסים (כולל אלה שאינם חופשיים מריבוע). ואמנם בכל הבסיסים, בחזקות עם מעריך זוגי סדר השאריות הוא סימטרי, כלומר שאריות המרוחקות מרחק שווה מהקצוות, שהן שאריות במקומות k ו b-k שוות זו לזו, ובחזקות עם מעריך אי-זוגי סכום שאריות כאלה הוא תמיד מספר המתחלק בבסיס ללא שארית (כלומר או 0 או b).

ההוכחה לעובדה זו היא תוצאה מהפיתוח הבינומי של $(b - k)^n$. עבור n זוגי מקבלים תמיד בפיתוח זה ביטוי הניתן לרישום בצורה $bf(b) + k^n$ כלומר סכום של k^n ומספר המתחלק ב b. מכאן שהשארית, בחילוק ב b של $(b - k)^n$ שווה לזו של k^n.

מאידך, עבור n אי-זוגי מקבלים תמיד בפיתוח זה ביטוי מהצורה $bf(b) - k^n$ כלומר, השארית בחילוק ב d של $(b - k)^n$ היא במקרה זה שווה לשארית המתקבלת מחילוק $-k^n$ ב b.

סכום שאריות המרוחקות מרחק שווה מהקצוות יהיה איפוא עבור n אי זוגי:

$$(b - k)^n + k^n = bf(b) - k^n + k^n$$

כלומר מספר המתחלק תמיד ב b.
על סמך מספרים אלה ברור כי אם חישבנו ע"י כפל וחילוק את כל השאריות עד $\frac{b+1}{2}$ או עד $\frac{b}{2}$ בשביל זוגי, נוכל לקבוע את יתר השאריות בדרך פשוטה ביותר

ד. שחזור כל השאריות לפי הסדר

טבלה מספר 2 מגלה תופעה שלא ראינו אותה בחזקות של השאריות לפי בסיס 10 והיא: בבסיסים מסויימים מופיעות חזקות, בהן כל השאריות הן 1. זה קרה בבסיס שלוש - בחזקות הריבועיות, בבסיס חמש - בחזקה החמישית, בבסיס שבע - בחזקה הששית ובבסיס אחת עשרה - בחזקה העשירית.
המשותף לכל הבסיסים האלה הוא שהם מספרים ראשוניים.

נוכל לנסח השערה: בכל בסיס b כאשר b ראשוני החזקה ה $b - 1$ של כל אחת מהשאריות מסדר ראשון נותנת בחילוק ב b שארית 1.

ואמנם השערה זאת היא תוצאה ישירה של משפט הנקרא על שם המתימטיקאי הצרפתי פרמה (Pierre de Fermat 1601-1665) שגילה כי לכל ראשוני ולכל מספר שלם a שאיננו מתחלק ב P, קיים כי a^{P-1} נותן שארית 1 בחילוק ב P, במילים אחרות $a^{P-1} \equiv 1 \pmod{P}$.

טבלה 2 מגלה אמנם כי ישנן שאריות השוות ל 1 כבר בחזקות קטנות מ $P - 1$, למשל הריבוע של 4, לפי בסיס 5 או החזקה השלישית של 2 ו 4 לפי בסיס 7. קל מאוד להוכיח כי הריבוע של $(P - 1)$ נותן שארית 1 בחילוק ב P. אבל, לפי הטבלה נוכל לשער ש $P - 1$ הוא המעריך הקטן ביותר שעבורו כל השאריות בחילוק ב P שוות ל 1.
השערה זו גם היא נכונה והיא תוצאה ישירה ממשפט של המתמטיקאי הגרמני גאוס (Carl Friedrich Gauss 1777-1855), שהוכיח כי לכל P ראשוני ישנן שאריות a כאלו המקיימות כי החזקה ה $P - 1$ שלהן נותנת שארית 1 בחילוק ב P, ו $P - 1$ הוא המעריך הקטן ביותר המקיים זאת.

לשאריות כאלה אשר בחזקה $P - 1$ הן נותנות שארית 1, בחילוק ב P, אבל לא בחזקה בת מעריך קטן מ $P - 1$ קרא גאוס בשם שורשים פרימיטיביים. גאוס הוכיח גם שמספרם של השורשים הפרימיטיביים המתקבלים בחילוק במספר ראשוני P הוא כמספר המספרים הקטנים מ $(P - 1)$ וזרים לו. ואמנם בטבלה 2 רואים כי לבסיסים 5, 7 ישנן שתי שאריות כאלה, ולבסיס 11, ישנן 4 שאריות כאלה (ובאמת ל $1 - 5 = 4$ ישנם שני מספרים הקטנים ממנו וזרים לו (שהם 1 ו 3). גם ל $1 - 7 = 6$ ישנם שני מספרים (1 ו 5) הקטנים ממנו וזרים לו, בשעה של $1 - 11 = 10$ ישנם ארבעה מספרים (1, 3, 7 ו 9) הקטנים ממנו וזרים לו.

מאידך אם שארית כלשהיא a לפי בסיס ראשוני P מקיימת ש a^t נותנת גם היא בחילוק ב P שארית השווה ל a, כלומר, $a^t = qp + a$ כאשר q מספר שלם, קיים גם $a(a^{t-1} - 1) = qp$. כיוון ש a אינו מתחלק ב P חייב $a^{t-1} - 1$ להתחלק ב P. על סמך משפט גאוס, זה יקרה לכל השאריות רק כאשר $t - 1 = P - 1$.

מסקנה: עבור בסיס P ראשוני החזקה ה P היא הראשונה שעבורה כל השאריות משוחזרות לפי הסדר המקורי.

ומה בדבר בסיסים b לא ראשוניים?
כפי שראינו כבר, אם הבסיס איננו חופשי מריבועים מוכרחה להופיע שארית 0 בחזקה מסויימת ולא נקבל שחזור של כל השאריות. נשאר לכן לדון בבסיסים שהם חופשיים מריבועים.
נשאלת השאלה:
האם ייתכן בסיס b, לא ראשוני אבל חופשי מריבועים, שעבורו קיים מעריך α כזה כך שכל השאריות בחזקת α יתנו שאריות השוות ל 1?

מתברר שהדבר בלתי אפשרי.
כי אם b לא ראשוני הרי ש $b = st$ כאשר s ו t שלמים וגדולים מ 1. המספרים s ו t הן איפוא שאריות לפי הבסיס b. מכאן, ל s^k יהיה מחלק משותף עם b לכל מעריך k טבעי. מאידך השוויון $s^\alpha = 1 + qb$ אומר שהמחלק המשותף הגדול ביותר של s^α ו b הוא 1. נתקבלה סתירה. כלומר עבור b לא ראשוני לא ייתכן שתהיה חזקה כזאת אשר עבורה כל השאריות בחילוק ב b שוות ל 1.

עם זאת נראה כי בשביל b חופשי מריבועים יש תמיד חזקה אשר עבורה כל השאריות מתקבלות מחדש לפי הסדר המקורי. ואמנם טבלה 2 מראה:
בבסיס $3 \times 2 = 6$ כל השאריות חוזרות בחזקה השלישית.
בבסיס $7 \times 2 = 14$ כל השאריות חוזרות בחזקה השביעית.
ובסיס $5 \times 3 = 15$ כל השאריות חוזרות בחזקה החמישית.

על סמך משפט פרמה, שהבאנו לעיל, אפשר להוכיח בקלות כי המעריך n אמנם מחזיר לנו את כל השאריות לפי הסדר המקורי. נשאר להראות שזה המעריך הקטן ביותר. דבר זה ניתן להוכחה באמצעות משפט גאוס, שציטטנו לעיל, ומשפט הידוע בשם "משפט השאריות הסיני" (עיין ברשימת הספרים בסוף המאמר). את ההוכחה נשאיר לקורא!

ה. ספרות החוזרות כל הזמן

בכל אחד מהבסיסים שחקרנו יש מספר שאריות המופיעות בכל אחת מהחזקות בטבלה באותו מקום (באותה עמודה). (ברור מראש כי מספיק לחפש שאריות כאלה בחזקה השניה בלבד. כי אם שארית חוזרת על עצמה בחזקה זאת היא תחזור על עצמה בכל חזקה שהיא.) למשל, לפי בסיס 10 אלה הן השאריות 0,1,5,6, לפי הבסיסים 4,3 ו 5 אלה הן השאריות 0,1 בלבד. אבל לפי בסיס 6 אלה הן השאריות 0,1,3,4. הנוכל גם כאן לגלות חוקיות ברורה? מתברר שכן. ובמקרה זה המסקנה שלנו תיהיה נכונה לכל בסיס b ולא רק לבסיסים חופשיים מריבוע.

מטבלה 2 הננו למדים כי ביחס לבסיסים 13,11,7,5,3 רק השאריות 0,1 מופיעות בכל חזקה באותו מקום. עובדה זו נכונה עבור כל בסיס ראשוני, כיוון שאנו מחפשים כאן את הפתרון (במספרים שלמים) של המשוואה $t^2 = t + qb$ כאשר $0 < t < b$ היא השארית המבוקשת. קיים איפוא: $t(t - 1) = qb$. אם b ראשוני הוא מוכרח לחלק את t או את $t - 1$ וזה ייתכן אם ורק אם $t = 0$ או $t = 1$.

תוצאה זו נכונה לא רק כאשר b הוא ראשוני אלא גם כאשר b הוא חזקה של מספר ראשוני, דהיינו $b = p^n$. דבר זה נובע מהעובדה ש $t < b$.

נניח עתה ש- $b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ כאשר ה p_i הם מספרים ראשוניים שונים. קיים משפט האומר שמספר הפתרונות של המשוואה $t^2 - t = qb$ (t השארית המבוקשת) מתברר שכל אלה הן דוגמאות למשפט כללי הטוען כי אם b חופשי מריבועים, והפרוק לגורמים ראשוניים של d הוא $b = p_1 \cdot p_2 \ldots p_k$ (כל ה p_i שונים!), הרי המעריך הקטן ביותר עבורו נקבל חזרה את כל השאריות, לפי הסדר המקורי, הוא:

$$n = [p_1 - 1 , p_2 - 1 , p_3 - 1 ,\ldots, p_k - 1] + 1$$

כאשר [...] פירושו: הכפולה המשותפת הקטנה ביותר של המספרים הכתובים בתוך הסוגריים.

הדוגמאות שהבאנו מאשרות את הטענה. ואמנם עבור בסיס עשר $10 = 5 \times 2$, $n = [4,1] + 1 = 5$ ואמנם בחזקה החמישית קיבלנו את כל השאריות לפי הסדר המקורי. כמו כן עבור בסיס שש $6 = 3 \times 2$ ו $n = [2,1] + 1 = 3$ ובחזקה השלישית קיבלנו את כל השאריות לפי הסדר המקורי.

הוא פונקציה כפלית! כלומר שמספר הפתרונות של משוואה זו הוא מכפלה של מספרי הפתרונות של המשוואות:

$$t^2 - t = q_1\, p_1^{\alpha_1}$$
$$t^2 - t = q_2\, p_2^{\alpha_2}$$
$$\vdots$$
$$t^2 - t = q_k\, p_k^{\alpha_k}$$

כפי שראינו, מספר הפתרונות השונים של כל אחת ממשוואות אלה הוא 2 (0 ו 1). מספר הפתרונות הכולל הוא איפוא 2^k כאשר k הוא מספר הגורמים הראשוניים השונים המופיעים ב b. מסתבר איפוא שלחזקה של הגורמים הראשונים אין כל השפעה על מספר הפתרונות.

לכל אחד מהמספרים 14,12,10,6 ו 15 ישנם 2 גורמים ראשוניים שונים. כמסקנה מטענתנו צריך להיות לכל אחד מהם $2^2 = 4$ שאריות שונות החוזרות על עצמן כבר בחזקה השניה ואמנם כך הדבר.

עבור 6: אלה הן השאריות 0,1,3,4 . עבור 10: 0,1,5,6 . עבור 12: 0,1,4,9 עבור 14: 0,1,7,8 ועבור 15: 0,1,6,10.

ו. שאלות נוספות

בדיון לעיל טרם מיצינו את אפס קצן של השאלות שאפשר לשאול בנושא זה. לדוגמא יכולנו לשאול:

1. בשביל בסיס b נתון, מה הוא המעריך הקטן ביותר, שעבורו מקבלים בחזרה את כל השאריות, לאו דווקא לפי הסדר המקורי? (ראינו למשל, כי לפי בסיס 10 זה קורה בחזקה השלישית).

2. מהו מספר השאריות השונות המתקבלות כאשר מעלים בריבוע את השאריות מסדר ראשון? (ראינו שלפי בסיס 10 ישנן שש כאלה, לפי בסיס 3 ישנן שתיים, לפי בסיס 4 ישנן שלוש, לפי בסיס 5 גם כן שלוש וכו').

3. שאלה כנ"ל עבור החזקות השלישית, הרביעית וכו'.

4. האם נוכל לחזות מראש אילו שאריות יתקבלו מחילוק ב b כאשר מעלים בריבוע את כל השאריות מסדר ראשון בבסיס b מסויים?

כך אפשר להמשיך ולשאול עוד ועוד. אולם נשאיר את הדברים לחקירה עצמית של הקוראים.

את הוכחת המשפטים שהתבססנו עליהם במאמר זה אפשר למצוא בספרים על תורת המספרים.
הננו ממליצים על הספרים הבאים:

Long C.T., Elementary Introductories to Number Theory, D.C. Heath & Co., 1965.

Niven J. & Zuckerman H.S., An Introduction to the Theory of Numbers, John Wiley & Sons, N.Y., 1960.

Ore O., Number Theory and Its History, McGraw-Hill, New York, 1948.

משפטים אחדים אפשר למצוא בספרו של פרופ א' פרנקל מבוא למתמטיקה, כרך א' בהוצאת מסדה.