

החשבון המודולרי בשירות האינדוקציה

עופר ליבה

אוניברסיטת בן-גוריון בנגב, באר-שבע

מבוא

מספר עקרונות בסיסיים של החשבון המודולרי יכולים לאפשר לנו להוכיח בפשטות ובמהירות תכונות התחלקות של ביטויים, אף מורכבים למדי, ובעיקר לבנות ביטויים כאלה ולהכליל לקטגוריות שלמות, וכך "לגלות את הסוד" העומד מאחורי טענות המוכחות באינדוקציה (ולעתים על-ידי "אינדוקציה בתוך אינדוקציה")

הערה: למען פשטות הכתיבה והקריאה, אנו לא נכמת "לכלי", "יש", "עבור איזשהו", "לכל n טבעי", וכיו"ב את הטענות המופיעות בגוף המאמר הכימות יהיה מובן מתוך ההקשר

1. הגדרת היחס המודולרי

$a \equiv b [m]$ (קרי a שקול ל-b מודולו m את המונח "שקול" נצדיק בהמשך) אם ורק אם m מחלק את $a - b$, כלומר $a - b = mt$.

הגדרה חלופית $a \equiv b [m]$ אם a ו- b משאירים אותה שארית כשמחלקים אותם ב- m למען הפשטות, m יהיה חיובי, כי הרי ברור ש- $a \equiv b [m]$ ורק אם $a \equiv b [-m]$ דוגמאות $12 \equiv 9 [3]$, $7 \equiv -5 [4]$, $-1 \equiv -15 [7]$, $0 \equiv 12 [3]$

2. תכונות מרכזיות של היחס המודולרי

- א $a \equiv a$ (רפלקסיביות)
 - ב $a \equiv b \Rightarrow b \equiv a$ (סימטריות)
 - ג $(a \equiv b \wedge b \equiv c) \Rightarrow a \equiv c$ (טרנזיטיביות)
 - ד $(a \equiv b \wedge a' \equiv b') \Rightarrow a + a' \equiv b + b'$ ("חיבוריות")
 - ה $(a \equiv b \wedge a' \equiv b') \Rightarrow a \cdot a' \equiv b \cdot b'$ ("כפליות")
- (כל השקילויות מודולו m)

הוכחות

א ברור

ב ברור

ג נתון $a - b = mt$, $b - c = mk$

על-ידי חיבור אגף-אגף, מקבלים $a - c = m(t - k)$

ד נתון $a - b = mt$, $a' - b' = mt'$

על-ידי חיבור אגף-אגף, מקבלים

$$(a + a') - (b + b') = m(t + t')$$

ה נתון $a - b = mt$, $a' - b' = mt'$

$$aa' - bb' = aa' - ab' + ab' - bb' =$$

$$= a(a' - b') + b'(a - b) = amt' + b'mt = m(at' + b't)$$

שלוש התכונות הראשונות מאפשרות לנו להעניק את "התואר" שקילות ליחס המודולרי שתי התכונות האחרונות יאפשרו לנו להוכיח מספר רב של טענות פרטיות וכלליות

3. שקילות בין שתי תבניות מעריכיות

דוגמה

$$7^n - 4^n \equiv 3 \pmod{3} \text{ או } 7^n \equiv 4^n \pmod{3}$$

הוכחה (באינדוקציה)

$$[3] 7^1 \equiv 4^1 \pmod{3}$$

$$7^k \equiv 4^k \pmod{3} \text{ ונוכיח } 7^{k+1} \equiv 4^{k+1} \pmod{3}$$

לפי התכונה ה מכפילים אגף-אגף את $7^k \equiv 4^k \pmod{3}$ ואת $7^1 \equiv 4^1 \pmod{3}$ ומקבלים את התוצאה

נכליל את הדוגמה במשפט הבא

משפט 1: $a^n - b^n$ מתחלק ב- m לכל n , אם $a - b$ מתחלק ב- m .

הוכחה זהה לזו שבדוגמה

כך מקבלים קטגוריה שלמה של טענות התחלקות, כולל עבור זוגיים או אי-זוגיים לדוגמה

$$[3] 7 \equiv -5 \pmod{3}, \text{ לכן } [3] (-5)^n \equiv 7^n \pmod{3}, \text{ כלומר } 7^n - (-5)^n \equiv 0 \pmod{3}$$

לכל n טבעי

מכאן שתי מסקנות מידיות

$$7^n - 5^n \equiv 0 \pmod{3} \text{ לכל } n \text{ זוגי, } 7^n + 5^n \equiv 0 \pmod{3} \text{ לכל } n \text{ איזוגי}$$

דוגמה של שילוב

$$2^n - 3^n + 9^n - 10^n \equiv 7 \pmod{7}$$

הוכחה

$$[7] 10^n \equiv 3^n \pmod{7}, \text{ לפי משפט 1}$$

$$[7] 9^n \equiv 2^n \pmod{7}, \text{ לפי משפט 1}$$

נחבר אגף-אגף (לפי תכונה ד, החיבוריות), ונקבל

$$10^n + 9^n \equiv 3^n + 2^n \pmod{7}$$

כדאי להזכיר, שההוכחה באינדוקציה של טענה מהסוג הזה היא בדרך כלל ארוכה, ואף דורשת "אינדוקציה בתוך אינדוקציה"

4. שקילות בין תבנית מעריכית למספר (קבוע)

$$\text{משפט 2: } a^n - 1 \text{ מתחלק ב- } m \text{ לכל } n, \text{ אם } a - 1 \text{ מתחלק ב- } m.$$

הוכחה מציבים $b = 1$ במשפט 1

דוגמאות

א $8^n - 1$ מתחלק ב-7 לכל n טבעי

ב $1 - (-5)^n$ מתחלק ב-3 לכל n טבעי, ומכאן

1 $5^n - 1$ מתחלק ב-3 לכל n זוגי, $5^n + 1$ מתחלק ב-3 לכל n אי-זוגי

תבנית מעריכית אינה חייבת להיות שקולה "רק" למספר 1

נראה זאת בדוגמה הבאה

$$8^n \equiv 15 \pmod{7}$$

הוכחה

$$8^n \equiv 1 \pmod{7} \text{ (ראינו)}$$

$$1 \equiv 15 \pmod{7} \text{ כמו-כך}$$

בהתאם לתכונה ג (טרנוטיביות), מקבלים $8^n \equiv 15 \pmod{7}$ (כלומר

$$15 - 8^n \text{ מתחלק ב-} 7)$$

נוכל להחליף את 15 בכל מספר אחר השקול לו, למשל -6,

$$\text{ולקבל } 8^n \equiv -6 \pmod{7},$$

נכליל במשפט הבא

$$\text{משפט 3: אם } a \equiv 1 \pmod{m} \text{ ואם } b \equiv 1 \pmod{m}, \text{ אז } a^n \equiv b^n \pmod{m}.$$

הוכחה כמו בדוגמה

דוגמה של שילוב

$$10^n + 8^n - 3^n + 6 \text{ מתחלק ב-} 7$$

הוכחה

$$10^n \equiv 3^n \pmod{7}, \text{ לפי משפט 1}$$

$$8^n \equiv -6 \pmod{7}, \text{ לפי משפט 3}$$

מחברים אגף-אגף ומקבלים את התוצאה

5. שקילויות מורכבות בין תבניות מעריכיות

דוגמה 1

$$4^n - 7^n - 4 \text{ מתחלק ב-} 3$$

הוכחה

$$4 \equiv 7 \pmod{3}, \text{ מכאן}$$

$$[3] 4^n \equiv 7^n, \text{ לפי משפט 2,}$$

$$[3] 4 \equiv 7 \text{ (תכונה ב, או ישירות)}$$

באמצעות תכונה ה (כפליות), מקבלים $[3] 7^n \equiv 4^n$

ובאופן כללי

$$\text{משפט 4: אם } a - b \text{ מתחלק ב- } m, \text{ אז } a^n \cdot b - b \cdot a^n \text{ מתחלק ב- } m.$$

(באותו אופן, $a^n \cdot b^2 - b^2 \cdot a^n$ מתחלק ב- m , או $a^3 \cdot b^n - b^3 \cdot a^n$)

מתחלק ב- m , וכן הלאה)

הוכחה כמו בדוגמה

דוגמה 2

$$[12] 3^n + 4^n \equiv 7^n$$

הוכחה

מצד אחד $[3] 3^n + 4^n \equiv 7^n$, כי $3^n \equiv 0 \pmod{3}$

מצד שני $[4] 3^n + 4^n \equiv 7^n$, כי $3^n \equiv 7^n \pmod{4}$

כלומר $3^n + 4^n - 7^n$ מתחלק הן ב-3 והן ב-4, ולכן הוא מתחלק

ב-12

אם נחליף את 7 ב-5 (כי הרי $[12] 7 \equiv -5$), נקבל

$$(-5)^n - (3^n + 4^n) \text{ מתחלק ב-} 12 \text{ לכל } n \text{ טבעי,}$$

$$5^n - 3^n - 4^n \text{ מתחלק ב-} 12 \text{ לכל } n \text{ זוגי,}$$

$$3^n + 4^n + 5^n \text{ מתחלק ב-} 12 \text{ לכל } n \text{ אי-זוגי}$$

נכליל במשפט הבא

$$\text{משפט 5: } (a + b)^n \equiv a^n + b^n \pmod{ab}.$$

הוכחה לכאורה, ההוכחה אמורה להיות זהה לזו שבדוגמה, אך

עליו להיות זהירים, כיוון שמספר יכול להתחלק בשני מספרים

אך לא במכפלתם לדוגמה 12 מתחלק הן ב-4 והן ב-6, אך

אינו מתחלק ב-24 ייתכן שיש צורך להתנות ש- a ו- b יהיו

זרים או נאמץ את ההוכחה הבאה שתראה לנו, כי אין צורך

בתנאי זה

הוכחה

$$(a + b)^n = a^n + na^{n-1}b + \dots + nab^{n-1} + b^n$$

כיוון ש-

$$[ab] na^{n-1}b + \dots + nab^{n-1} \equiv 0 \pmod{ab}$$

$$[ab] (a + b)^n \equiv a^n + b^n \pmod{ab}$$

6. שקילות בין תבנית מעריכית לבין תבנית

ממעלה ראשונה ושנייה

דוגמה

$$[9] 4^n \equiv 3n + 1 \text{ (} 4^n - 3n - 1 \text{ מתחלק ב-} 9)$$

הוכחה (באינדוקציה) $[9] 1 + 1 \equiv 3 \pmod{9}$ ברור

$$[9] 4^k \equiv 3k + 1, \text{ ונוכיח כי } [9] 4^{k+1} \equiv 3(k+1) + 1$$

$$(a + 1)^n \equiv 1 + n \cdot a + \frac{1}{2} \cdot n \cdot (n-1) \cdot a^2 [a^3]$$

לדוגמה, אם נציב $a = 4$, נקבל

$$5^n = (1 + 4)^n \equiv 1 + n \cdot 4 + \frac{1}{2} \cdot n \cdot (n-1) \cdot 4^2 [64]$$

פשוט

$$5^n \equiv 8n^2 - 4n + 1 [64]$$

(נסו להוכיח באינדוקציה)

7. לקינוח...

בסעיף זה ננסה להכליל את משפט 6, ונשאל את עצמנו מה יקרה אם נחליף את 1 במספר כלשהו b

ניעזר שוב בפיתוח הבינום, ונקבל

$$(a + b)^n = b^n + n \cdot b^{n-1} \cdot a + \dots + b^{n-2} \cdot a^2$$

ולכן

$$(a + b)^n \equiv b^n + n \cdot b^{n-1} \cdot a [a^2]$$

כדי לקבל תוצאה "יפה יותר", נחליף את n ב- $n + 1$, ונקבל

$$(a + b)^{n+1} \equiv b^{n+1} + (n + 1) \cdot b^n \cdot a [a^2]$$

נוציא את b^n כגורם משותף, ונקבל

$$(a + b)^{n+1} \equiv b^n \cdot (a + b + na) [a^2] \text{ משפט 7}$$

לדוגמה, נציב $a = 3, b = 2$, ונקבל

$$5^{n+1} \equiv 2^n (5 + 3n) [9]$$

$$4^{k+1} \equiv 4 \cdot (3k + 1) = 12k + 4 = 9k + 3k + 4 \equiv 0 + 3k + 4$$

$$(4^{n+1} \equiv 3n + 4 [9]) \text{ קיבלנו עוד טענה}$$

נכליל במשפט הבא

$$(a + 1)^n \equiv a \cdot n + 1 [a^2] \text{ משפט 6}$$

הוכחה א (באינדוקציה)

$$(a + 1)^1 \equiv a + 1 + 1 [a^2]$$

$$\text{נניח } (a + 1)^k \equiv a \cdot k + 1 [a^2]$$

$$\text{ונוכיח } (a + 1)^{k+1} \equiv a \cdot (k + 1) + 1 [a^2]$$

$$(a + 1)^{k+1} = (a + 1)^k (a + 1) \equiv$$

$$(a \cdot k + 1)(a + 1) = a^2 k + ak + a + 1 \equiv a \cdot (k + 1) + 1$$

הוכחה ב

$$(a + 1)^n = (1 + a)^n = 1 + n \cdot a + \dots + a^2 + \dots + a^3$$

$$\text{לכן } (a + 1)^n \equiv 1 + n \cdot a [a^2]$$

אל נשכח ש- a יכול להיות שלילי לדוגמה, על-ידי חצבת $a = -5$ מקבלים

$$[25] \quad (-4)^n \equiv 1 - 5n$$

וניתן כרגיל לקבל את הטענות הנלוות עבור n זוגי ועבור n אי-זוגי

ההוכחה השנייה של משפט 6 מראה לנו שניתן לקבל, באותו דרך, שקילות בין תבנית מעריכית לבין תבנית ממעלה שנייה כדלקמן

מחקר: ירידה ברמת בחינות הבגרות של שלוש יחידות במתמטיקה

מאת רינת קליין

מחקר חדש, שנערך בבית הספר לחינוך באוניברסיטת תל אביב, עולה כי הלה ירדה ברמה הנדרשת בבחינות הבגרות של שלוש יחידות במתמטיקה. את המחקר ערכה נעמה שילה, במסגרת עבודה לתואר שני, והוא פורסם בעיתון שיעור חופשי של המתורגמות המורים במהלך המחקר.

נבדקו כל השאלונים של בחינות הבגרות במתמטיקה, במסגרת הקיץ, משנת 1957 ועד סוף 1995. מניתוח השאלונים עולה כי עד שנת 1972 ניכרה מגמה של עלייה ברמת הדרג שנדרש לבחינה זו ואף לו מ-1975 ואילך הלה ירדה. ניתוח רמות הישג של המבחן נים נעשה באמצעות מולם של ד"ר גות החשיבה, שגובש במהלך המבחן קב בעזרתו של פרופ' עמנואל ארליך.

(מחקר "ידיעות אחרונות")