בספר

לא דוגמה $[1,5]$ הפכים מודולו 10

1 $\underbrace{(5,10)}_{b}$ ולכן אין פתרון לשוויון $\overset{ax}{5x} \equiv \overset{b}{1} \pmod{\overset{m}{10}}$

$\gcd(a,m)$ לפי המשפט מעל ל-3

מסקנה: p ראשוני $\Leftarrow$ לכל $1 \le a \le p-1$ יש הפכי מודולו p. (כי אז $(a,m)=1$). ויש פתרון יחיד למשוואה $ax \equiv 1 \ (p)$

שאלה לדיון: האם יתכן מספר שהפכי עצמו מודולו p?

דוגמה: $4 \cdot 4 \equiv 1 \ (5)$, $1 \cdot 1 \equiv 1 \ (5)$ ומתברר שאין עוד.

טענה: יהי $a \in \mathbb{Z}$, p ראשוני. אז a הפכי של עצמו מודולו p אם ורק אם $a \equiv 1 \ (p)$ או $a \equiv (-1) \ (p)$

שני אלו הם הפתרונות הפשוטים ביותר של מצב שקילות הפכי (ולמען אל כמה הרבה הם.

הוכחה: ($\Longrightarrow$) פירוק.

($\Longleftarrow$) נניח $a^2 \equiv 1 \ (p) \Leftarrow p \mid a^2-1 \Leftarrow p \mid (a-1)(a+1) \Longrightarrow$ אמר ראשוני מחלק מכפלה הוא מחלק מ-אחד הגורמים

$p \mid a-1$ או $p \mid a+1 \Leftarrow a-1 \equiv 0 \ (p)$ או $a+1 \equiv 0 \ (p) \Leftarrow a \equiv 1 \ (p)$ או $a \equiv -1 \ (p)$

הכללה של הטענה הנ"ל: יהי $p \ge 3$ ראשוני, $k \in \mathbb{N}$, $a \in \mathbb{Z}$

a הפכי של עצמו מודולו p^k $\Longleftrightarrow$ $a \equiv \pm 1 \ (p^k)$ (לא נכון עבור $p=2$! לדוגמה $3^2 \equiv 1 \ (8)$ אבל $3 \not\equiv \pm 1 \ (8)$)

הוכחה: נבדוק הטענה בפשטות רבה שונה מההוכחה הקודמת.

עלינו למצוא את פתרונות המשוואה $x^2 \equiv 1 \ (p^k)$ ולהראות שהם רק ± 1.

$x^2 \equiv 1 \ (p^k) \Longleftrightarrow p^k \mid x^2-1 \Longleftrightarrow p^k \mid (x+1)(x-1)$

מכיוון ש $(x-1)$ $(x+1)$ נבדלים ב-2 ו-p גדול מ-2 כי p מחלק בדיוק אחד

מכיוון $(x-1)$ $(x+1)$ $\cdot$ אם $p^k \mid x-1$ אז $x-1 \equiv 0 \ (p^k)$ כלומר $x \equiv 1 \ (p^k)$ (עם p^k מחלק בדיוק אחד מבין $x-1$ ו-$x+1$).

ואם $p^k \mid x+1$ אז $x+1 \equiv 0 \ (p^k)$ כלומר $x \equiv -1 \ (p^k)$.

דיון: לשים לב איך ההוכחה נפלה עבור $p=2$: $2^3 \mid (x+1)(x-1)$ ואפילו $(3+1)(3-1)$ אבל 2^3 מחלק את $x-1$ לא מחלק את $x+1$.

דוגמא למציאת הפכי מודולו 5

מחלקת שקילות מוד 5	0	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
הפכי מוד 5	אין	$[1]_5$	$[3]_5$	$[2]_5$	$[4]_5$

הפכי עצמו — זוגות — הפכי עצמו

דוגמאות לפתרון שקילות לינארית

הדוגמאות הללו יהוו תזכורת עבורך את כל האלגוריתם החישובים שעשינו עד עתה בקורס (שקילות לינארית, הפכי מודולו, דיופנטי, אלגוריתם האוקלידי...)

פיבונאצ'י

מצאו את כל הפתרונות לשקילות

$9x \equiv 12 \ (15)$

המשפטים הרלוונטיים

$(9,15) = 3 \mid 12$

לכן יש 3 פתרונות לא שקולים מוד 15

לשקילות $ax \equiv b \ (m)$ יש $d = (a,m)$ פתרונות לא שקולים מוד m אם $d \mid b$.

נכתוב את המשוואה הדיאופנטית:

$\underbrace{9}_{a}x - \underbrace{15}_{m}y = \underbrace{12}_{b}$

כדי לפתור שקילות לינארית $ax \equiv b \ (m)$ אנו לפתור משוואה דיאופנטית $ax - my = b$ כל x מפתרון הדיאופנטית פותר את השקילות הלינארית

(בתנאי הדיאופנטי שונה בקצרה)

מתוך לפתרון משוואה דיאופנטית $ax - my = b$ כאשר $(a,m) \mid b$:

① יש אלגוריתם אקלידס המורחב מצאו את $d = (a,m)$ ומצאו x_1, y_1 עבור $ax_1 - my_1 = d$

(בתנאי הדיאופנטי שונה בקצרה)

$(9,15)$

$(15,9)$ $\quad 15 = 1 \cdot 9 + 6$ $\quad 3 = 1 \cdot 9 + (-1)[15 - 1 \cdot 9] = 2 \cdot 9 + (-1) \cdot 15$

$(9,6)$ $\quad 9 = 1 \cdot 6 + 3$ $\xrightarrow{\text{מצמצם}}$ $3 = 1 \cdot 9 + (-1) \cdot 6$

$(6,3)$ $\quad 6 = 2 \cdot 3$ $\quad 3 = 0 \cdot 6 + 1 \cdot 3$

$(3,0)$

$\Downarrow$

$(15,9) = 3$

$\underbrace{9}_{a} \cdot \underbrace{2}_{x_1} - \underbrace{15}_{m} \cdot \underbrace{1}_{y_1} = \underbrace{3}_{d}$

② מוכפלים t עבור $d \cdot t = b$

③ הפתרון המקורי הוא $\underbrace{tx_1}_{x_0}, \underbrace{ty_1}_{y_0}$

$t = 4$

$4 \cdot 9 \cdot 2 - 4 \cdot 15 \cdot 1 = 12$

$9 \cdot \underbrace{4 \cdot 2}_{tx_1} - 15 \cdot \underbrace{4 \cdot 1}_{ty_1} = 12$

④ אופן הפתרונות של הדיאופנטית הם

$x = x_0 + \frac{-m}{d} t$ $\quad$ ו $y = y_0 - \frac{a}{d} t$

פתרון הדיאופנטית: (כאן ה-x מעניין)

$x = 8 + \frac{-15}{3} t = 8 - 5t$

יש 3 פתרונות לא שקולים מוד 15 (שאנו עדיים לא שקולים של t מודולו 3)

נשתמש ב הבאים $t = 0,1,2$

פתרון I: $x \equiv 8 \ (15)$ $\quad$ עבור $t=0$

פתרון II: $x \equiv 3 \ (15)$ $\quad$ עבור $t=1$

פתרון III: $x \equiv 13 \ (15) \equiv -2$ $\quad$ עבור $t=2$

סוף

עשיר ראשון פיטמה נוסף שתיתן לנו רעיון איך לפתרון שאלה לינארית במספרים מסוימים.

דוגמא: מצאו את כל הפתרונות לשאלה $16x \equiv 9 \ (35)$

כלום המשפטים הרלוונטיים

לשאלה $ax \equiv b \ (m)$ ו $d=(a,m)$ פתרונות אי שקולים מוד m אם $d|b$

$(16,35)=1$

שכיון יחיד מודולו 35 בטוח לכל אותו משוואה הקונגרוונטית ורלה לקבל אותן הפתרון שני הנבדים בהפכי של 16 מודולו 35.

אם $(a,m)=1$ אז יש ל-a הפכי יחיד מודולו m.

מצא את ההפכי של 16 מודולו 35:

$16 \cdot \square \equiv 1 \ (35)$ אם כמה פותרים השאלה הקודמת זו משוואה דיופנטית, לכן גם לא מעניין אותנו מצאנו סתם אם יודעים מספר אין לנו הפכי (נניח מערך קודם ולא שרטוטים בנ"ל)

נניח שלו: $16 \cdot 11 \equiv 1 \ (35)$.

אז: נתבונן בשאלה המקורית

$16x \equiv 9 \ (35) \quad \backslash \cdot 11$

$\underbrace{16 \cdot 11}_{\equiv 1 \ (35)} \cdot x \equiv 9 \cdot 11 \ (35)$

$x \equiv 99 \equiv 29 \ (35)$

עשיר ראשון פיטמה נוסף שתיתן לנו רעיון איך לפתרון שאלה לינארית במספרים מסוימים.

דוגמא: מצאו את כל הפתרונות לשאלה $16x \equiv 9 \ (35)$

כלום המשפטים הרלוונטיים

לשאלה $ax \equiv b \ (m)$ ו $d=(a,m)$ פתרונות אי שקולים מוד m אם $d|b$

$(16,35)=1$

שכיון יחיד מודולו 35 בטוח לכל אותו משוואה הקונגרוונטית ורלה לקבל אותן הפתרון שני הנבדים בהפכי של 16 מודולו 35.

אם $(a,m)=1$ אז יש ל-a הפכי יחיד מודולו m.

מצא את ההפכי של 16 מודולו 35:

$16 \cdot \square \equiv 1 \ (35)$ אם כמה פותרים השאלה הקודמת זו משוואה דיופנטית, לכן גם לא מעניין אותנו מצאנו סתם אם יודעים מספר אין לנו הפכי (נניח מערך קודם ולא שרטוטים בנ"ל)

נניח שלו: $16 \cdot 11 \equiv 1 \ (35)$.

אז: נתבונן בשאלה המקורית

$16x \equiv 9 \ (35) \quad \backslash \cdot 11$

$\underbrace{16 \cdot 11}_{\equiv 1 \ (35)} \cdot x \equiv 9 \cdot 11 \ (35)$

$x \equiv 99 \equiv 29 \ (35)$