משפט השאריות הסיני

תזכורת: למדנו שאם קיים פתרון שקול לינארי מסוג $ax \equiv b \pmod{m}$ למדנו שיש פתרון אם $d=(a,m) \mid b$ אז יש d פתרונות שונים מודולו m.

מטרת משפט השאריות הסיני: לפתור מערכת משוואות כגון:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

3,5,7 ראשוניים

וכם למצוא פתרון... (שקל!) פתרון אפשרי: 52 (נבדוק!)

הפתרון הזה לא יחיד מודולו $3\cdot5\cdot7=105$, כלומר כל הפתרונות האפשריים הם $52, 52+105, 52+2\cdot105, \ldots, 52-105, \ldots$ ואין עוד פתרונות.

(זה פתרון שלם נופל ל-52 כפולה של 105 עבור כל פתרון. אבל לא ברור לי אם אין עוד).

משפט השאריות הסיני: יהיו $n_1,\ldots,n_r$ מספרים ראשוניים בינם לבין עצמם. אז למערכת השקילות הלינארית

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

יש פתרון יחיד מודולו $M = n_1 \cdot \ldots \cdot n_r = lcm(n_1,\ldots,n_r)$

lcm - הגדרה המקבילה ל-gcd שאותו ל סדרה

n מספרים ראשוניים בינם לבין עצמם שווה למכפלתם

$$\boxed{\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}}$$

דוגמה

$n_1 \quad n_2 \quad n_3$

$3, 5, 7$

$M = 3\cdot5\cdot7 = 105$

$M_1 = \frac{105}{3} = 5\cdot7 = 35 \Rightarrow (M_1, n_1) = 1$ ($M_1 = 5\cdot7$, $n_1 = 3$)

$M_2 = \frac{105}{5} = 3\cdot7 = 21 \Rightarrow (M_2, n_2) = 1$ ($M_2 = 3\cdot7$, $n_2 = 5$)

$M_3 = \frac{105}{7} = 3\cdot5 = 15 \Rightarrow (M_3, n_3) = 1$ ($M_3 = 3\cdot5$, $n_3 = 7$)

למה הנה - לחישוב המשפט

יהיו $n_1,\ldots,n_r$ מספרים ראשוניים בינם לבין עצמם.

יהי $M = \prod_{i=1}^{r} n_i$

ויהי $M_k = \frac{M}{n_k}$ לכל $1 \le k \le r$

אז $(M_k, n_k) = 1$ לכל $1 \le k \le r$

הוכחה: מכיוון ש- $n_1,\ldots,n_r$ ראשוניים בינם לבין עצמם אין ל- M_k שום גורם ראשוני משותף עם n_k ∎

הוכחת משפט השאריות הסיני

לכל $1 \le k \le r$ נסמן $M_k = \frac{M}{n_k}$

נתבונן בשקילות מהצורה $M_k \cdot y_k \equiv 1 \ (n_k)$

לפי למת ההכנה $(M_k, n_k) = 1$ ולכן לפי התפרטת מתמטית הנ"ל יש לכל שקילות כזו פתרון מינימלי y_k מודולו n_k.

יהי $x = a_1 M_1 y_1 + \dots + a_r M_r y_r$

נטען כי x פתרון למערכת המשוואות.

דוגמה

$M_1 = 5 \cdot 7 = 35$

$M_2 = 3 \cdot 7 = 21$

$M_3 = 3 \cdot 5 = 15$

$$\left.\begin{aligned} \overset{M_1}{35} y_1 &\equiv 1 \ (\overset{n_1}{\text{mod } 3}) \\ 21 y_2 &\equiv 1 \ (\text{mod } 5) \\ 15 y_3 &\equiv 1 \ (\text{mod } 7) \end{aligned}\right\} \text{הופכים מודולו משוואות הדרגה}$$

$$\left.\begin{aligned} 35 y_1 &\equiv 1 \ (\text{mod } 3) \\ \underbrace{33 y_1}_{\equiv 0} + 2 y_1 &\equiv 1 \ (\text{mod } 3) \\ &\boxed{y_1 \equiv 2 \ (\text{mod } 3)} \\ 21 y_2 &\equiv 1 \ (\text{mod } 5) \\ \underbrace{20 y_2}_{\equiv 0} + y_2 &\equiv 1 \ (\text{mod } 5) \\ &\boxed{y_2 \equiv 1 \ (\text{mod } 5)} \\ 15 y_3 &\equiv 1 \ (\text{mod } 7) \\ 14 y_3 + y_3 &\equiv 1 \ (\text{mod } 7) \\ &\boxed{y_3 \equiv 1 \ (\text{mod } 7)} \end{aligned}\right\} \text{אפשר לפי שלב הפרי מודולו. כאן ב' אינם לקחו בכל}$$

$$x = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1$$

$$= 157 \equiv 52 \ (\text{mod } 105)$$

כאן כל החלק התאום של פתרון תבאל את משפט השאריות הסיני.

מצא $x \equiv \overset{1}{a_1} \ (3)$

נסתכל על x מ"ד 3

$$x = \overset{a_1}{1} \cdot \underbrace{\overset{m_1}{35} \cdot \overset{y_1}{2}}_{\equiv 1} + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1$$

$m_1 y_1$ שמוגדר מ"ד 3

בשביל הוסיף 3 ולכן גם הכל סמוך 3

מצא $x \equiv \overset{2}{a_2} \ (5)$

$$x = 1 \cdot \cancel{35} \cdot 2 + \overset{a_2}{2} \cdot \underbrace{21 \cdot 1}_{\equiv 1 \ (5)} + 3 \cdot \cancel{15} \cdot 1$$

מצא $x \equiv \overset{3}{a_3} \ (7)$

$$x = 1 \cdot \cancel{35} \cdot 2 + 2 \cdot \cancel{21} \cdot 1 + \overset{a_3}{3} \cdot \underbrace{15 \cdot 1}_{\equiv 1 \ (7)}$$

אם, עבור $1 \le k \le r$ נראה כי $x \equiv a_k (n_k)$.

אז לכל $j \ne k$, $1 \le j \le r$, מתקיים $n_k | M_j$

ולכן כל המחוברים מהצורה $a_j M_j y_j$ שקולים ל-0

מודולו n_k. לכן

$$x \equiv a_k M_k y_k \pmod{n_k}$$

אבל $M_k y_k \equiv 1 (n_k)$ ולכן $x \equiv a_k (n_k)$

<u>הוכחת יחידות:</u> נניח כי x_0, x_1 שני פתרונות מודולו M למערכת. כלומר לכל $1 \le k \le r$

$$\begin{cases} x_0 \equiv a_k \pmod{n_k} \\ x_1 \equiv a_k \pmod{n_k} \end{cases}$$

אם

$\Leftarrow$ לכל $1 \le k \le r$ $n_k | x_0 - x_1$ $\Leftarrow$ $M = n_1 \cdots n_r | x_0 - x$ $\Leftarrow$ $x_0 \equiv x_1 (M)$.

<u>הסבר אלגוריתם לחישוב עצמאי:</u>
כי n_k $(1 \le k \le n)$ ראשוניים בינם לבין
ולכן אם נכפיל את המכפלה
$n_1 \cdots n_r$
לפירוק לראשוניים, $n_1 \cdots n_r = p_1^{a_1} \cdots p_s^{a_s}$
לא יהיה מחלק יותר מפעם אחת
אחת ולכן יוסיף זה ב-$(x_0 - x_1)$.

<u>טענה חלוקה של lcm:</u>
אז $t | n_1, \dots, n_r$
אם $t | [n_1, \dots, n_r] = \underset{\text{אפשרי}}{lcm}(n_1, \dots, n_r) = n_1 \cdots n_r$
ניתן להוכיח באמצעות הטענה שמעלה תוך 3.

lcm = מכפלת כל הגורמים הראשוניים בחזקה הגדולה יותר.

$\boxtimes$

<u>תרגיל:</u> מצאו שלושה מספרים שלמים שהם כפולות של <u>מספר ריבועי</u> (מהצורה $\square^2$)
<u>פתרון:</u> נחפש שלשה: $x, x+1, x+2$ עם ש

$$\begin{cases} x \equiv 0 (2^2) \\ x+1 \equiv 0 (3^2) \\ x+2 \equiv 0 (5^2) \end{cases}$$

צרים בינם לבין

$$\begin{cases} x \equiv 0 (2^2) \\ x \equiv -1 (3^2) \\ x \equiv -2 (5^2) \end{cases}$$

תוצאה

נבחר לפי משפט השאריות הסיני: $M = 2^2 \cdot 3^2 \cdot 5^2 = 900$

$M_1 = 3^2 \cdot 5^2 = 225$

$M_2 = 2^2 \cdot 5^2 = 100$

$M_3 = 2^2 \cdot 3^2 = 36$

$11y_3 \equiv 1 (25)$
$11y + 25x \equiv 1 (25)$
$(25, 11) = 1 = d$
$11 \cdot (9) + 25 \cdot 4 = 1$
$t = 1$
פתרון: $x = 4$, $y = -9$

$225 y_1 \equiv 1 (2^2)$ מודולו 22 $\Leftarrow$ $y_1 \equiv 1 (2^2)$

$100 y_2 \equiv 1 (3^2)$ $\Leftarrow$ $y_2 \equiv 1 (3^2)$

$36 y_3 \equiv 1 (5^2)$ $\Leftarrow$ $11y_3 \equiv 1 (25)$ $\Leftarrow$ $y_3 \equiv -9 \equiv 16 (25)$ (אם נה לבחור כפולה שלמה נקבל a)

המספר 900

$x = \overset{a_1 m_1 y_1}{0 \cdot 225 \cdot 1} + (-1) \cdot 100 \cdot 1 + (-2) \cdot 36 \cdot 16 = -1252 \equiv 548 (900)$ ולכן $x = 548$ מקיים את המשוואה.

משפט וילסון: (Wilson) לכל ראשוני p $(p-1)! \equiv -1 \ (p)$

דוגמא: $p=5 \Rightarrow 4! = 4\cdot 3\cdot 2\cdot 1 = 24 \equiv 4 \equiv -1 \ (5)$

הוכחה: (מן לבד... הצבר שמעיר שיאמרו שגם מעניין שהוכחתו יהיה הוכחה למשפט ווילסון.) (אז מתחלה ההוכחה)

הצבעה: p ראשוני $\Leftarrow$ לכל $1 \le a \le p-1$ יש הפכי מודולו p. בחיבור שהם הפכיים של עצמם הם 1 $(p-1)! \equiv -1$.

הוכחה לדוגמה: עבור $p=2$: $(2-1)! = 1 \equiv -1 \ (2)$.

עבור $p>2$: דוגמא: $p=7$

$6! = 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1$ ($6 = p-1$; הפכי מול 1; הפכי מול 2)

נתבונן במכפלה $1\cdot 2\cdot \ldots \cdot (p-2)(p-1) = (p-1)!$. מה קבלים כלל:

לכל $2 \le a \le p-2$ יש הפכי a' מודולו p שונה מעצמו

ולכן $aa' \equiv 1 \ (p)$. כך נתלף את הגורמים לזוגות שמכפלתם 1 מודולו p.

ולכן עכל

$(p-1)! \equiv \underbrace{1\cdot 1\cdot \ldots \cdot 1}_{\text{מתקבל לא}}\cdot \underbrace{1\cdot 1}_{\text{מתקבל לא}}\cdot (p-1) \equiv (p-1) \ (p)$

משפט הפוך לוילסון: יהי $2 \le n \in \mathbb{N}$. אם $(n-1)! \equiv -1 \ (n)$ אז n ראשוני.

הוכחה: נניח בשלילה כי n פריק, $n=ab$, $2 \le a,b < n$

אז $\boxed{a \mid (n-1)!}$

מצד שני, מכיוון ש-$(n-1)! \equiv -1 \ (n)$ נובע

$\underbrace{1+(n-1)!}_{\text{כי } (n)} \mid n$ ולכן גם $\boxed{1+(n-1)! \mid a}$ (כי $a \mid n$)

הערה (לא מהספר) - מסיון הוכחה שני:

אם $n=ab$ אז $(n-1)! = (n-1)\cdot \ldots \cdot a \cdot \ldots \cdot b \equiv 0 \ (n)$ אז מתקיים כי אם $a=b$

נובע (משני ה-□) כי $\underbrace{(n-1)! - (1+(n-1)!)}_{=1} \mid a$ בסתירה לכך ש- $a \ge 2$. ∎

אלגוריתם (לא יעיל) לבדיקת ראשוניות: נניח לבדוק אם n ראשוני נבדוק האם $(n-1)! \equiv -1 \ (n)$. לפיכך, האם 6 ראשוני? נבדוק האם $(6-1)! \equiv -1$

$5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120 \equiv 0 \not\equiv -1 \ (6)$

דוגמה נוספת: מצאו את השארית של $15!$ בחלוקה ב-17.

פתרון: מהמשפט (17 לפי מודולו) $15!$. לפי וילסון $16! \equiv -1 \ (17)$

ולכן $-1 \equiv 16! \equiv 16\cdot 15! \equiv 15!\cdot(-1) \ (17) \Rightarrow 15! \equiv 1 \ (17)$

ולכן $n>1$ הראשוני אמ"מ $(n-2)! \equiv 1 \ (n)$

הוכחה: לפי וילסון: n ראשוני אמ"מ $(n-1)! \equiv (n-1) \pmod{n}$

(נעבור לבמלא את שני האגפים ב-$(n-1)$ - מותר לבמלא כאשר הגורם הוא מלבמלא עם מודולו n)

$$\boxed{\text{תכונות כלל הבמלאה}\quad ac \equiv bc \ (m) \iff a \equiv b \left(\frac{m}{(c,m)}\right)}$$

ולפי כלל הבמלאה נקבל כי

$$(n-2)! \equiv 1 \mod \underbrace{\left(\frac{n}{(n-1,n)}\right)}_{=1}$$

כלומר אמ"מ $(n-2)! \equiv 1 \ (n)$ $\boxed{///}$

המשפט הקטן של פרמה

(המשפט הקטן של פרמה אומר שמספר ראשוני p מקיים $p \mid a^p - a$ לכל a.)

יהי p ראשוני, ויהי $a \in \mathbb{N}$ כך ש- $p \nmid a$. אז $a^{p-1} \equiv 1 \pmod{p}$

דיון: למה לבקש את התנאי $p \nmid a$? כי אחרת $a^{p-1} \equiv 0 \ (p)$.

הוכחה:

שני שלבים

שלב ראשון:

$$a \cdot (2a) \cdot (3a) \cdot \ldots \cdot ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p} \quad (*)$$

נגדיר $S = \{a, 2a, 3a, \ldots, (p-1)a\}$

מספרים שונים כי:

אם אמרנו S כולו שקולים בשאר מודולו p, אז אחד מאברי S אינו שקול ל-0 מודולו p.

נראה אם a: נניח בשלילה כי $ja \equiv 0 \ (p)$

עבור $1 \le j \le p-1$, אז $p \mid ja \Rightarrow p \mid j$, סתירה.

"ולפי הנחה שני מאחר מספר הוא מחלק את אחד האגפים"

$p \nmid a$ -!

נראה אם אי: נניח כי $ja \equiv ka \ (p)$ עבור $1 \le j < k \le p-1$

$\Leftarrow j \equiv k \ (p)$, סתירה לכך ש- $1 \le j < k \le p-1$

(כלל הבמלאה כי $(a,p)=1$)

(נגדיר מדיון $(*)$ נקבל הנדרש.

[נגדיר "לבמלאה" את $(*)$ ב- $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$]

לפי כלל הבמלאה, נקבל מ-$(*)$

$$a^{p-1} \equiv 1 \left(\mod \frac{p}{(p, 1 \cdot 2 \cdot \ldots \cdot (p-1))}\right)$$

אמ"מ

אבל $(p,(p-1)!)=1$ ולכן נקבל

$a^{p-1} \equiv 1 \ (\mod p)$ כנדרש.

$$\boxed{\text{תכונות כלל הבמלאה}\quad ac \equiv bc \ (m) \iff a \equiv b \left(\frac{m}{(c,m)}\right)}$$