פתרון קונגרואנציות

הגדרה - יהי m טבעי, $a,b\in\mathbb{Z}$ נקראים **קונגרואנטים** מודולו m אם $m\mid b-a$

כאן מרמלו - a,b משאירים את אותה שארית בחלוקה ב-m

סימון - $a\equiv b\pmod m$ (אומרים בכך שהם מודולו m)

* היחס הינו יחס שקילות!
את מחלקות השקילות מסמנים $\mathbb{Z}_m$.
לפקבודה על קונגרואנטים **נפעלים מודולו m**.
נבחר את הנציגים $0,1,\dots,m-1$
מדוע אכן נציגים?
מהגדרת $\mathbb{Z}$, לכל a ההצגה עם חלוקה עם שארית, יש לו"ק $a=qm+r$
$m\mid r-a \iff \exists q\in\mathbb{Z}\ r=qm+a$ $0\le r<m$
במקרה של יחידות ההצגה, ניתן לראות שכל מספר בהכרח נמצא במחלקה שונה.

נרצה שניתן לבצע פעולות חשבוניות על $\mathbb{Z}_m$:

טענה - אם $a\equiv a'\pmod m$, $b\equiv b'\pmod m$ אז $a+b\equiv a'+b'\pmod m$
$a-b\equiv a'-b'\pmod m$
$ab\equiv a'b'\pmod m$

הוכחה - $m\mid a-a'$ ← יש r כך ש- $a-a'=mr$
$m\mid b-b'$ ← יש q כך ש- $b-b'=mq$

נחבר - $a+b-(a'+b')=a-a'+b-b'=$
$=mr+mq=m(r+q)$

יקבלנו:
$m\mid a+b-(a'+b') \longleftarrow a+b\equiv a'+b'\pmod m$

ובכפל מוכיחים באותו אופן.

מסקנה - ב-$\mathbb{Z}_m$ אפשר לבצע פעולות חיבור וכפל כי מיד את הפעולות עם נציגים שכל מחלקות שקולות כך הכללים המוגדרים שיימים ב-$\mathbb{Z}$ מתקיימים גם ב-$\mathbb{Z}_m$

מסקנה - אם $a_nx^n+\dots+a_1x+a_0=f(x)$ פולינום במקדמים שלמים, אז f מגדיר פונקציה גם שלמים מודולו m, שגם אי' תמיד עם נציגים.

תכונות - שהיו הכוונה עם פעולות חיבור וכפל, המקיימות
$\mathbb{Q}$ אקסיומות: חבורה- אסוציאטיבי, קומוטטיבי, איבר נ"ט (0), איבר הפכי ($-x$)
כפל - " - " - " - (1), " - " - ($\frac{1}{x}$)
חוק הפילוג

* הערה - קבוצה המקיימת את האקסיומות שמעל נקראת **שדה**.

אל הוכחתנו ש- $\mathbb{Z}_m$ שדה.

הגדרה - איבר $a\in\mathbb{Z}_m$ נקרא **הפיך** אם $b\in\mathbb{Z}_m$ כך ש- $ab\equiv 1\pmod m$

סימון - $\mathbb{Z}_m^*$

מי הם ההפיכים האלה? $a\in\mathbb{Z}_m^*$ ↔ יש $b\in\mathbb{Z}$ כך ש- $ab\equiv 1\pmod m$
↔ יש $b\in\mathbb{Z}$ כך ש- $m\mid ab-1$ ↔ יש $k,b\in\mathbb{Z}$ כך ש- $mk=ab-1$
↔ יש $k,b\in\mathbb{Z}$ כך ש- $ab-mk=1$ ↔ $\gcd(a,m)=1$

הוכחנו טענה: $a\in\mathbb{Z}_m^*$ ⟷ $\gcd(a,m)=1$

Scanned by CamScanner

טענה - יהי $a,b \in \mathbb{Z}_m$, $k \in \mathbb{Z}$ כך ש: $gcd(k,m)=1$. אזי:
$$a \equiv b \pmod m \longleftrightarrow ka \equiv kb \pmod m$$

הוכחה: $\rightarrow$ ברור
$\leftarrow$ הפוך. לכן נכפול ב- k^{-1}:
$$k^{-1}ka = k^{-1}kb \pmod m \longrightarrow a = b \pmod m$$

מסקנה - $\mathbb{Z}_m$ שדה אמ"מ m ראשוני.

הוכחה: $\rightarrow$ אם m ראשוני, אז לכל $1 \le x \le m-1$, $gcd(x,m)=1$, x הפוך.
אנו יודעים ש- $\mathbb{Z}_m$ הפיכים. אזי $\mathbb{Z}_m$ שדה.

$\leftarrow$ נניח ש- m לא ראשוני, נרצה ש- $\mathbb{Z}_m$ אינו שדה.
אזי קיימים $a,b \in \mathbb{Z}$ כך ש- $ab = m$
כלומר $ab \equiv 0 \pmod m$ אך $a,b \not\equiv 0 \pmod m$. אזי $\mathbb{Z}_m$ לא שדה.

טענה - נניח ש- r מחלק משותף של k,m. אזי:
$$ka \equiv kb \pmod m \longleftrightarrow \left(\tfrac{k}{r}\right)a = \left(\tfrac{k}{r}\right)b \pmod{\tfrac{m}{r}}$$

מסקנה -
$$ka = kb \pmod m \longleftrightarrow a \equiv b \pmod{\frac{m}{gcd(k,m)}}$$

דוגמה לתרגיל: מצא הופכי ל- 18 ב- $\mathbb{Z}_{25}$, ופתור $18x = 11 \pmod{25}$

נשתמש באלגוריתם אוקלידס כדי למצוא צירוף $1 = 25m + 18k$, k יהיה ההופכי.
ואז נעשה $x = 11k \longleftrightarrow 18x = 18k \longleftrightarrow x \equiv 11 \pmod{18}$

הגדרה - עבור $m \in \mathbb{Z}$ טבעי, נסמן $\phi(m) = |\mathbb{Z}_m^\times|$

טענה - אם $m = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$, אזי:
$$\phi(m) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

* להשלים הוכחה

הגדרה - $\psi : \mathbb{Z} \to \mathbb{C}$ נקראת כפלית אם לכל $m,n \in \mathbb{Z}$, $gcd(m,n)=1$
מתקיים: $\psi(mn) = \psi(m)\psi(n)$

מסקנה - ϕ כפלית

טענה - לכל n טבעי, $n = \sum_{d \mid n} \phi(d)$

הוכחה: בתרגיל הוכחנו שאם $f : \mathbb{N} \to \mathbb{C}$ כפלית, אזי גם $F(n) = \sum_{d \mid n} f(d)$ כפלית.
ואז:
$$\sum_{d \mid p^k} \phi(d) = 1 + \sum_{i=1}^{k} \phi(p^i) = \sum_{i=1}^{k} (p^i - p^{i-1}) + 1 = p^k$$

ופונקציה כפלית מוגדרת ע"י הערכים על חזקות הראשוניים:
$$n = \prod_{i=1}^{k} p_i^{r_i} = \prod_{i=1}^{k} \sum_{d \mid p_i^{r_i}} \phi(d) = \sum_{d \mid p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}} \phi(d)$$

Scanned by CamScanner

פיתרון קונג'רואנטיה ממעלה ראשונה: $(*) = ax \equiv b \pmod m$

משפט - נסמן ב- $d = gcd(a,m)$. אז מס' הפיתרונות של $(*)$ ב- $\mathbb{Z}_m$ הוא:

$$\begin{cases} 0 & ; d \nmid b \\ d & ; d \mid b \end{cases}$$

כמו כן, אם $d \mid b$ אז מס' הפיתרונות ב- $\mathbb{Z}_{m/d}$ הוא 1.

הוכחה - תחילה עכיח שאם יש פיתרון, אז $d \mid b$:

$$ax \equiv b \pmod m \longrightarrow \exists y \in \mathbb{Z} \,.\, ax - b = ym \longrightarrow$$

$$\longrightarrow \exists y \in \mathbb{Z} \,.\, ax - ym = b \longrightarrow (\tfrac{a}{d}x - \tfrac{m}{d}y)d = b$$

לכן $d \mid b$.

נניח $d \mid b$. נסמן $a = da_1$, $b = db_1$, $m = dm_1$.
אז למשוואה $a_1 x \equiv b_1 \pmod{m_1}$ יש פיתרון יחיד ב- $\mathbb{Z}_{m_1}$ כי $1 = gcd(a_1, m_1)$.

נסמן ב- $\bar{x} \in \mathbb{Z}$ נציג של מחלקת השקילות של x.
נגדיר $x_1 \equiv \bar{x} \pmod{m_1}$. אז נפתור את הטענה מההרצאה הקודמת, ונקבל ש- x_1 פיתרון ל- $(*)$ וכל פיתרון ל- $(*)$ שקול לפיתרון במשוואה ב- $\mathbb{Z}_{m_1}$ מלמעלה ($d = k$, $\alpha = a_1$, $\beta = b_1$)

דוגמה - פתור את $35x \equiv 56 \pmod{77}$

נחלק ב- d ונקבל $7 = gcd(35, 77) = d$. $5x \equiv 8 \pmod{11}$.
יש פיתרון יחיד כאן: 9.
אז לפי המשפט, הפיתרונות הם כל המספרים ב- $\mathbb{Z}_{77}$ השקולים 9-ל ב- $\mathbb{Z}_{11}$.

משפט השאריות הסיני

נניח $m_1, \ldots, m_k$ זרים בפעולות. יש $x \in \mathbb{Z}$ כך ש- $x \equiv c_i \pmod{m_i}$ $(*)$
אז אם $y \in \mathbb{Z}$ פיתרון ל- $(*)$ אזי $x \equiv y \pmod M$
כאשר $M = \prod_{i=1}^{k} m_i$

הוכחה - נסמן $n_j = \prod_{i \neq j} m_i = \frac{M}{m_j}$

כי m_i זרים בפעולות. לכן יש פיתרון ל- $gcd(n_j, m_j) = 1$:
$n_j x \equiv c_j \pmod{m_j}$
נבחר $x_j \in \mathbb{Z}$ כך ש- $n_j x_j \equiv c_j \pmod{m_j}$, ונגדיר
$x = n_1 x_1 + \ldots + n_k x_k$
x פיתרון ל- $(*)$ כי לכל i:

$$x = n_1 x_1 + \ldots + n_k x_k \pmod{m_i} \equiv n_i x_i \equiv c_i \pmod{m_i}$$

$$n_j \equiv 0 \pmod{m_i}, \quad i \neq j$$

* נשאלה הוכחה נוספת בדרך להשלים.

Scanned by CamScanner

משפט פרמה הקטן

יהי p ראשוני, $x \not\equiv 0 \pmod p$, אזי $x^{p-1} \equiv 1 \pmod p$

הוכחה - אם $p=2$ - מוודאים ידנית ונה נכון.
נניח $p \geq 3$. אזי:

$$|\mathbb{Z}_p^*| = \phi(p) = p-1$$

נסמן

$$g = \prod_{a \in \mathbb{Z}_p^*} a = 1 \cdot 2 \cdot \ldots \cdot (p-1)$$

g מכפלת הפרטים ולכן הפיך. לכן:

$$x^{p-1} g \equiv x^{p-1} \prod_{a \in \mathbb{Z}_p^*} a \equiv \prod_{a \in \mathbb{Z}_p^*} (xa) \equiv \prod_{\substack{\downarrow \\ xa=b}} b \equiv g \pmod p$$

נכפול בהופכי של g ונקבל $x^{p-1} \equiv 1 \pmod p$

הכללה: משפט אוילר

יהי: $m \in \mathbb{N}$, $m \geq 2$. אזי לכל $x \in \mathbb{Z}_m^*$, $x^{\phi(m)} \equiv 1 \pmod m$

הוכחה - נהה לקונדמנט.

דוגמאות: או) חשב את $2^{20} \pmod{17}$.

$$2^{20} = 2^{16} \cdot 2^4 = 2^4 = 16 = -1 \pmod{17}$$

גם הראה כי $2^{98} + 3^{98}$ מתחלק ב-13.

$$98 = 96 + 2 = 8 \cdot 12 + 2$$

$$2^{98} + 3^{98} = 2^{96} \cdot 4 + 3^{96} \cdot 9 \equiv 4 + 9 \equiv 0 \pmod{13}$$

משפט וילסון

יהי p ראשוני. אזי $(p-1)! = -1 \pmod p$

הוכחה - אם $p=2$ - מוודאים ידנית ונה נכון.
נניח $p \geq 3$. $\mathbb{Z}_p$ שדה, ולכן לכל $a \in \mathbb{Z}_p / \{0\}$, a הפיך.
נשאול את עצמנו מתי $a \equiv a^{-1} \pmod p$?

$$a \equiv a^{-1} \pmod p \longrightarrow a^2 \equiv 1 \pmod p \longrightarrow (a+1)(a-1) \equiv a^2 - 1 \equiv 0 \pmod p$$

לכן $a \equiv 1$ או $a \equiv -1$, כלומר $a \neq \pm 1$.
נסתכל על $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$. לכל $2 \leq a \leq p-2$, $a \neq a^{-1}$ ו a^{-1} ברשימה, והם שונים. לכן הם מצטמצמים $\pmod p$.
ולכן

$$(p-1)! \equiv 1 \cdot -1 \equiv -1 \pmod p$$

Scanned by CamScanner