

קונגרואנציות

הבצרה - 'י' מ טבעי, $\mathbb{Z}, a, b \in \mathbb{Z}$ נקראים קונגרואנטיים מודולו m אם $a \equiv b \pmod{m}$
 כל פירמלי - $a \equiv b \pmod{m}$ משמרים את אותה שארית בחלוקה ב- m
 סימון - $a \equiv b \pmod{m}$ (אומרים גם שקולים מודולו m)

* היחס הוא יחס שקילות!
 את מחלקת השקילות מסמנים \mathbb{Z}_m
 בקבוצה זו קיימים הפעמים מודולו m
 נבחר את הנציגים $0, 1, \dots, m-1$
 מצד אחד נציגים

בהינתן $a \in \mathbb{Z}$, עפי הטענה זה חלוקה עם שארית, יש q, r כך ש- $a = qm + r$
 $0 \leq r < m$ → $r = a - qm$
 בעל היחידות הטענה ניתן לראות שכל מספר בטווח זה מייצג מחלקה שונה.

נראה שניתן לבצע פעולות טבעיות 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 - $m | a - a'$ → יש r כך ש- $rm = a - a'$
 $m | b - b'$ → יש q כך ש- $qm = b - b'$

נחבר - $a + b - (a' + b') = a - a' + b - b' = rm + qm = (r+q)m$

יקבלו: $a + b \equiv a' + b' \pmod{m}$ (כי $m | a + b - (a' + b')$)
 חיבור ופסל מוכחים באותו אופן.

סקנה - ב- \mathbb{Z}_m אפשר לבצע פעולות חיבור חיבור ופסל וזו ביצור אותו פעולות על נציגים של מחלקת שקילות כל הפעמים המוגדרים טקיימים ב- \mathbb{Z} המקיימים גם ב- \mathbb{Z}_m

סקנה - אם $a = a_0 + a_1x + \dots + a_nx^n$ ו- f פולינום בערכים שלמים, אז f מצד פונקציה יא שלמים מודולו m , שוב יזי חישוב עם נציגים.

תכונות - שדה הטו קבוצה עם פעולות חיבור ופסל המקיימות 9 אקסיומות: חיבור- אסוציאטיבי, קומוטטיבי, איברי נייטרלי (0), אצרי הפכי (-), כפל - אסוציאטיבי, קומוטטיבי, איברי נייטרלי (1), אצרי הפכי (x), חוק הפילוף

* הערה - קבוצה המקיימת את האקסיומות למעט חוק הפיר חוד. אז הוכחנו ש- \mathbb{Z}_m חוד.

הבצרה - איבר $a \in \mathbb{Z}_m$ נקרא הפכי אם יש $b \in \mathbb{Z}_m$ כך ש- $ab \equiv 1 \pmod{m}$
 סימון - $(\mathbb{Z}_m)^*$

מי הם הפוכים האצרי? $a \in (\mathbb{Z}_m)^* \leftrightarrow \exists b \in \mathbb{Z}_m$ כך ש- $ab \equiv 1 \pmod{m}$
 $\leftrightarrow \exists b \in \mathbb{Z}$ כך ש- $ab - 1 = km$ $\leftrightarrow \exists b, k \in \mathbb{Z}$ כך ש- $ab - km = 1$
 $\leftrightarrow \exists b, k \in \mathbb{Z}$ כך ש- $ab - km = 1$ $\leftrightarrow \gcd(a, m) = 1$
 הוכחנו טענה: $a \in (\mathbb{Z}_m)^* \leftrightarrow \gcd(a, m) = 1$

טענה - נניח $a, b \in \mathbb{Z}_m$, $K \in \mathbb{Z}$, $\gcd(K, m) = 1$ אזי: $a \equiv b \pmod{m} \iff Ka \equiv Kb \pmod{m}$

הוכחה: \rightarrow ברור
 \leftarrow K הפך. עטן טכס להכפיל ב- K^{-1} :
 $K^{-1}Ka = K^{-1}Kb \pmod{m} \rightarrow a = b \pmod{m}$

מסקנה - \mathbb{Z}_m שדה אחר m ראשוני.

הוכחה: \rightarrow אם m ראשוני, לכל $1 \leq x \leq m-1$, $\gcd(x, m) = 1$, $x-1$ הפך.
 אז כל האיברים ב- \mathbb{Z}_m הפיכים. אז \mathbb{Z}_m שדה.

\leftarrow נניח ש- m לא ראשוני, נטח u - \mathbb{Z}_m אינו שדה.
 אז קיימים $a, b \in \mathbb{Z}_m$ כן u - $ab = m$
 פשוט $ab \equiv 0 \pmod{m}$ אך $a, b \not\equiv 0 \pmod{m}$. אז \mathbb{Z}_m לא שדה.

טענה - נניח ש- r מחלק מנותק של K, m . אז: $Ka \equiv Kb \pmod{m} \iff \left(\frac{K}{r}\right)a \equiv \left(\frac{K}{r}\right)b \pmod{\frac{m}{r}}$

מסקנה - $a \equiv b \pmod{\frac{m}{\gcd(K, m)}} \iff Ka = Kb \pmod{m}$

דוגמה לפרטים: מצא הפכי 18 ב- \mathbb{Z}_{25} , ובטור $18x = 11 \pmod{25}$

נשתמש באלגוריתם אוקלידס כדי למצוא צירוף $18K + 25M = 1$, $1 - K$ יהיה ההופכי.
 $18x = 11 \iff 18Kx = 11K \iff x = 11K$

הצורה - עבור \mathbb{Z}_m טבעי, נסמן $\phi(m) = |\mathbb{Z}_m^*|$

טענה - אם $n = p_1^{r_1} \dots p_k^{r_k}$ אזי:

$$\phi(n) = \prod_{i=1}^k p_i^{r_i-1} (p_i - 1) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

* ערשטים הוכחה

הצורה - $\Psi: \mathbb{Z} \rightarrow \mathbb{C}$ נקראת כפלית אם $\gcd(m, n) = 1$, $n, m \in \mathbb{Z}$
 $\Psi(mn) = \Psi(m)\Psi(n)$ מתקיים:

מסקנה - \emptyset כפלית

טענה - עם n טבעי, $\sum_{d|n} \phi(d) = n$

הוכחה: בתרגיל הוכחנו שאם $f: \mathbb{N} \rightarrow \mathbb{C}$ כפלית, אז גם $F(n) = \sum_{d|n} f(d)$ כפלית.

$$\sum_{d|p^k} \phi(d) = 1 + \sum_{i=1}^k \phi(p^i) = \sum_{i=1}^k (p^i - p^{i-1}) + 1 = p^k$$

ובתוצרה כפלית מוגדרת ע"י ערכיה על חזקות ראשוניים:

$$\sum_{d|p_1^{r_1} \dots p_k^{r_k}} \phi(d) = \prod_{i=1}^k \sum_{d|p_i^{r_i}} \phi(d) = \prod_{i=1}^k p_i^{r_i} = n$$

פיתרון קונגרואנציה ממעלה ראשונה: $(*) = ax = b \pmod{m}$

משפט - נסמן $d = \gcd(a, m)$. אז אם הפיתרון 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 עם הפיתויות ב- $\mathbb{Z}_{m/d}$ הוא 1.

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

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

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

לכן $d \mid b$.

נניח $d \mid b$. נסמן $a = da, b = db, m = dm$. אז משוואה $(*)$ היא $ax = b \pmod{m}$. יש פיתרון יחיד ב- \mathbb{Z}_m כי $\gcd(a, m) = 1$.

נסמן ב- \mathbb{Z} $\bar{x} \in \mathbb{Z}$ נציב של מחלקת השקולים של x . נניח $(*)$ היא $x \equiv \bar{x} \pmod{m}$. אז נפרט את הטענה מההוכחה הקודמת ונקבל ש- x פיתרון של $(*)$, וכל פיתרון של $(*)$ שקול לפיתרון במשוואה ב- \mathbb{Z}_m (שהיא $a = da, b = db, m = dm$).

דוגמה - פתור את $35x = 56 \pmod{77}$

$d = \gcd(35, 77) = 7$. נחלק ב- d ונקבל $5x = 8 \pmod{11}$.

יש פיתרון יחיד כאן: 6. אז עם משפט הפיתויות הם כל האינסופיים ב- \mathbb{Z}_{77} השקולים ל-6 ב- \mathbb{Z}_{11} .

משפט הסיני הסיני

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

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

הוכחה - נסמן

$\gcd(n_j, m_j) = 1$ כי ה- m_i זרים בזוגות. לכן יש פיתרון של $n_j x = c_j \pmod{m_j}$.

נבחר $x_j \in \mathbb{Z}$ כן ש- $n_j x_j = c_j \pmod{m_j}$ (וגדיר $x = n_1 x_1 + \dots + n_k x_k$).

x פיתרון של $(*)$ כי לכל i : $x = n_1 x_1 + \dots + n_k x_k \equiv n_i x_i \equiv c_i \pmod{m_i}$.

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

* נמצאה הוכחה נוספת, צריך להשלים.

משפט פרמה הקטן

אם p ראשוני, אז $x^{p-1} \equiv 1 \pmod{p}$ עבור $x \not\equiv 0 \pmod{p}$.

הוכחה - אם $p=2$ - בוצק'ים יזנית וזה נכון.
 נניח $p \geq 3$. אז:

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

(מסו)

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

g מכפלת הפיכים ועם הפיך. עכ"ל:

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

\downarrow
 $xa=b$

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

הכללה: משפט אוילר

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

הוכחה - נהיה סקוצמתי.

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

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

ב) הראה כי $2^{98} + 3^{98} \pmod{13}$ 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, אז $(p-1)! \equiv -1 \pmod{p}$.

הוכחה - אם $p=2$ - בוצק'ים יזנית וזה נכון.
 נניח $p \geq 3$. אז \mathbb{Z}_p^* שזרה ועם סכום $a \equiv a^{-1} \pmod{p}$?
 נטאף מתי

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

עכ"ל $a \equiv 1$ או $a \equiv -1$ כדומה $\{a \in \mathbb{Z} \pm 1\}$.
 נסתכל על $(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1)$.
 אם a זוגי ו- a^{-1} ברשימה, והם שונים. עכ"ל הם מוצמנים \pmod{p} .
 ועכ"ל $(p-1)! \equiv 1 \cdot -1 \equiv -1 \pmod{p}$