

הצגה - י' מ טבעי, $\mathbb{Z}_m$ קראים קונגרואנציות מודולו m אם $a \equiv b \pmod{m}$

כל פרמלי - מודולו, מטאורים את אותה שארית בחלקה ב- m

סימון - $a \equiv b \pmod{m}$ (אומרים גם שקולים מודולו m)

* היחס הוא יחס שקילות!
את מחלקת השקילות מסמנים $\mathbb{Z}_m$
שקבוצה זו קראים המסלולים מודולו m .
נבחר את הנציגים $0, 1, \dots, m-1$
מקוצצו ונציגים

בהינתן $a \in \mathbb{Z}$, לפי הטענה של חלקה עם שארית, יש q, r כך ש- $a = mq + r$, $0 \leq r < m$
כלומר $a \equiv r \pmod{m}$ $\leftarrow$ r הוא שארית של a בחלקה עם m
הכלל היחידות הטענה ניתן לראות שכל מספר בטווח $0 \leq r < m$ מתחלק שונה.

נראה שניתן לבצע פעולות חשבוןיות על $\mathbb{Z}_m$:

סגור - 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 - $a \equiv a' \pmod{m} \leftarrow$ יש r כך ש- $rm = a - a'$
 $b \equiv b' \pmod{m} \leftarrow$ יש q כך ש- $qm = b - b'$

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

יקבלו: $a+b \equiv a'+b' \pmod{m} \leftarrow m \mid a+b - (a'+b')$

וכפס
חיסור מוכחים באותו אופן.

מסקנה - ב- $\mathbb{Z}_m$ אפשר לבצע פעולות חיבור חיסור וכפס וז' ביצא אותו
פעולות על נציגים של מחלקת שקילות כל הפעולות המוגדרים שקיימים
ב- $\mathbb{Z}$ מתקיימים גם ב- $\mathbb{Z}_m$

מסקנה - אם $a = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ פולינום בערכים שלמים, אז f מצייר
פונקציה על שלמים מודולו m , שוב וז' חשבו עם נציגים.

תצטרפת - שדה הטו קבוצה עם פעולות חיבור וכפס, המקיימות
9 אקסיומות: חיבור - אסוציאטיבי, קומוטטיבי, אידי (נייטרלי) (0), אלמנט הפכי (ז-)
כפס - אסוציאטיבי, קומוטטיבי, אידי (נייטרלי) (1), אלמנט הפכי (ז-)
חוק הפיפול

* הערה - קבוצה המקיימת את האקסיומות למעט חוק נקרא חוג.
אז הוכחנו ש- $\mathbb{Z}_m$ חוג.

הצגה - איבר $a \in \mathbb{Z}_m$ נקרא הפי אם יש $b \in \mathbb{Z}_m$ כך ש- $ab \equiv 1 \pmod{m}$

סימון - $(\mathbb{Z}_m)^*$

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

לענה - 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. δ ן טכס להכפיל ב- k^{-1} :
 $k^{-1}ka = k^{-1}kb \pmod{m} \rightarrow a \equiv b \pmod{m}$

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

הוכחה: $\rightarrow$ אם m ראשוני, לכל $1 \leq x \leq m-1$, $\gcd(x, m) = 1$, ו- x 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 $a, b \in \mathbb{Z}_m$ כך ש- $ab = m$
 כלומר $ab \equiv 0 \pmod{m}$ אך $a, b \not\equiv 0 \pmod{m}$. אז $\mathbb{Z}_m$ לא שדה.

לענה - נניח ש- r מחלק משותף של k, m . אזי:
 $ka \equiv kb \pmod{m} \iff \left(\frac{k}{r}\right)a \equiv \left(\frac{k}{r}\right)b \pmod{\frac{m}{r}}$

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

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

נשתמש באלגוריתם אוקלידס כדי למצוא צירוף $18k + 25m = 1$, ו- k יהיה ההפכי.
 $18x \equiv 11 \iff 18kx = 11k \iff x = 11k$

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

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

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

* להשלים הוכחה

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

מסקנה - $\emptyset$ כפולית

לענה - לכל n טבעי, $\sum_{d|n} \phi(d) = n$

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

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

ובעקבות כפולית 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 משל הפיתונות של $(*)$ ב- $\mathbb{Z}_m$ היא:

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

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

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

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

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

דבר $d \mid b$.

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- $\bar{x} \in \mathbb{Z}$ נציב של מחלקת השקולים של x . נניח $x \equiv \bar{x} \pmod{m}$. אז נציב של $\bar{x}$ הוא x ונקבל ש- x פיתרון של $(*)$ וכל פיתרון של $(*)$ שקול ל- x (שקול לפיתרון במשוואה ב- $\mathbb{Z}_m$ מראה $(\beta = b, \alpha = a, \lambda = d)$).

דוגמה - פתור את $35x = 56 \pmod{77}$

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

יש פיתרון יחיד כאן: 6.

אז שם הפיתרון היחיד הוא $x \equiv 6 \pmod{11}$. הפיתונות הם כל המספרים ב- $\mathbb{Z}_{77}$ השקולים ל-6 ב- $\mathbb{Z}_{11}$.

משפט הסיני הסיני

נניח $a_1, \dots, a_k, m_1, \dots, m_k$ זרים בזוגות. יש $x \in \mathbb{Z}$ כן ש- $x \equiv a_i \pmod{m_i}$ $(*)$ אזי $x \equiv y \pmod{M}$ כאשר $M = \prod_{i=1}^k m_i$.

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

הוכחה - נסמן

$$\gcd(n_j, m_j) = 1 \text{ כי } m_j \text{ זרים בזוגות. } \text{לכן יש פיתרון } x_j$$

$$n_j x_j \equiv a_j \pmod{m_j}$$

נבחר $x_j \in \mathbb{Z}$ כן ש- $n_j x_j \equiv a_j \pmod{m_j}$ (וגזיר)

$$x = n_1 x_1 + \dots + n_k x_k$$

x פיתרון של $(*)$ כי לכל i : $x \equiv n_i x_i + \dots + n_k x_k \pmod{m_i} \equiv n_i x_i \pmod{m_i} \equiv a_i \pmod{m_i}$

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

* נמצאה הוכחה נוספת, צריך להשלים.

משפט פרמה הקטן

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

הוכחה - אם $p=2$ - בוצ'ק יזנית וזה נכון.
נניח $p \geq 3$ איז:

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

(סמן)

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

g מכפלת הפיכים וענן הפין, ענן:

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

$$x^{p-1} \equiv 1 \pmod{p}$$

מכפול בהופכי של g ונקבל

הכללה: משפט אוילר
יהי $m \in \mathbb{N}$, $m \geq 2$, אז $x^{\phi(m)} \equiv 1 \pmod{m}$, $x \in \mathbb{Z}_m^*$

הוכחה - זהה לקודמת.

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 $p=2$ - בוצ'ק יזנית וזה נכון.
נניח $p \geq 3$. $\mathbb{Z}_p^*$ שזרה וענן סגור.
נראה ש $a \equiv a^{-1} \pmod{p}$?

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

ענן $a \equiv 1$ או $a \equiv -1$ כדומה $\{a \in \mathbb{Z} \pm 1\}$.
נסתכל על $(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1)$.
 a ו a^{-1} ברשימה, והם שונים. ענן הם מוצגים $\pmod{p}$.
וענן

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