שקילות מודולו n (קונגרואנציה)   הרצאה 6

דוגמה: המספרים $1, 5, 13, 21$ שקולים כולם מודולו 4 (משאירים אותה שארית בחלוקה ב-4). מסמנים: $5\equiv 13 \pmod 4$ "5 שקול ל-13 מודולו 4"

חופף

קונגרואנטי

שימו לב: ההפרש בין שניים תמיד כפולה של 4.

הגדרה: יהיו $a,b\in\mathbb{Z}$, $m\in\mathbb{N}$. נאמר כי a שקול ל-b מודולו m ונסמן $a\equiv b \pmod m$ אם $m \mid a-b$. (שני מס' שקולים מוד m אם הפרשם הוא כפולה של m)

טענה (הגדרה אלטרנטיבית 1): עבור m,b,a כנ"ל
$a\equiv b \pmod m \iff a=b+km$ עבור $k\in\mathbb{Z}$ (שני מס' שקולים מוד m אם הם נבדלים בכפולות)

הוכחה: ($\Leftarrow$) $a\equiv b \pmod m \Leftarrow m\mid a-b \Leftarrow$ ק' $k\in\mathbb{Z}$ כ"ש $mk=a-b \Leftarrow a=b+mk$

($\Rightarrow$) אם $a=b+km \Leftarrow a-b=km \Leftarrow m\mid a-b$. ∎

טענה (הגדרה אלטרנטיבית 2): עבור a,b,m כנ"ל
$a\equiv b \pmod m \iff$ בפירוק המובטח ע"י משפט החלוקה $a=mk+r$ $0\le r<m$ (עם a,m)
$b=m\cdot k'+r'$ $0\le r'<m$ (עם b,m)
מתקיים $r=r'$ (שני מס' שקולים מוד m אם משאירים אותה שארית בחלוקה ב-m)

הוכחה:

($\Leftarrow$) אם $a\equiv b \pmod m$ $\overset{\text{הטענה קודמת}}{\Leftarrow}$ $a=b+qm$ עבור $q\in\mathbb{Z}$ $\overset{\text{הצבה מהנתון}}{\Leftarrow}$ $a=\underbrace{mk'+r'}_{b}+qm$

$\Leftarrow a=m(k'+q)+r'$, $0\le r'<m$ ומהיחידות של משפט החלוקה נקבל $r'=r$.

($\Rightarrow$) כעת נניח $\begin{cases} a=mk+r \\ b=mk'+r \end{cases}$ אותו r $\Leftarrow a-b=mk-mk' \Leftarrow a-b=m(k-k')$

$\Leftarrow m\mid a-b$. ∎

אבחנה: שקילות מודולו m $(m\in\mathbb{Z})$ הינה יחס שקילות
- רפלקסיבי (א' שקול לא')
- סימטרי (אם א' שקול לב' אז ב' שקול לא')
- טרנזיטיבי (אם א' שקול לב' וב' שקול לג' אז א' שקול לג')

רע': - [illegible]

הוכחה:

① רפלקסיבי: לכל $a\in\mathbb{Z}$ $a\equiv a \pmod m$ כי $m\mid a-a$.

② סימטרי: לכל $a,b\in\mathbb{Z}$: $a\equiv b \pmod m$ אמ"מ $b\equiv a \pmod m$ כי:

$a\equiv b \pmod m \iff m\mid a-b \iff m\mid b-a \iff b\equiv a \pmod m$.

③ טרנזיטיביות: לכל $a,b,c\in\mathbb{Z}$ אם $a\equiv b \pmod m$ ו-$b\equiv c \pmod m$ אז $a\equiv c \pmod m$

כי: (נתון: $a\equiv b \pmod m$ $\overset{\text{הגד'}}{\Leftarrow}$ $a=b+km$ עבור $k\in\mathbb{Z}$

$b\equiv c \pmod m$ $\Leftarrow$ $b=c+k'm$ עבור $k'\in\mathbb{Z}$

$\Leftarrow$ $a=b+km=c+k'm+km=c+(k'+k)m$ $\overset{\text{הגד'}}{\Leftarrow}$ $a\equiv c \pmod m$

יחס השקילות מחלק את השלמים למחלקות שקילות.

דוגמה - ל-3 מחלקות שקילות מודולו 3

"מחלקת השקילות של 0 מודולו 3"

$[0]_3=\{\dots,-6,-3,0,3,6,9,\dots\}$

$[1]_3=\{\dots,-5,-2,1,4,7,\dots\}$ → שימו לב כי $-5\equiv 1\ (3)$ כאן לפי כל ההגדרות. למרות ש-$5\equiv 2\ (3)$

$\underbrace{[2]_3}_{\text{נציגים מסומנים}}=\{\dots,-4,-1,2,5,8,\dots\}$

$\bar0_3,\bar1_3,\bar2_3$

$\{0,1,2\}$ זו "מערכת שארית שלמה מודולו 3"

$\{3,4,8\}$ " " " " (נציג מכל מחלקה!)

הגדרה: מערכת שארית שלמה מודולו m זה אוסף של מספרים ב-$\overset{+}{\mathbb{Z}}$, ש
שכל שלם שקול לבדיוק אחד מהמספרים באוסף מודולו m.

לפי משפט החלוקה עם $m\in\mathbb{N}$ $0,1,\dots,m-1$ זו מערכת שארית שלמה מודולו m. (קנונית)

סימון: $[x]_m$ (או: $\bar{x}_m$) מסמן את מחלקת השקילות של x מודולו m.

טענה: יהי $m\in\mathbb{N}$. כל m שלמים בלתי שקולים בזוגות יוצרים מערכת
כל זוג הוא בלתי שקול
שארית שלמה מודולו m. (ההפך ראינו למעלה)

הוכחה: תהי S קב' של m שלמים בלתי שקולים בזוגות.

לכל $s\in S$ יש לפי משפט החלוקה $s=k_s m+r_s$ k_s,r_s שלמים $0\le r_s<m$

תהי $R=\{r_s \mid s\in S\}$ אוסף השארית.

אם נניח בשלילה כי S אינה מערכת שארית שלמה מודולו m, נקבל כי $|R|\le m-1$
(לא כל השאריות מופיעות ב-R)

ולכן מעקרון שובך היונים (יש m יונים שהשובכים הם השאריות) יש $s\neq s'$ ב-S ש
$r_s=r_{s'}$ בסתירה לכך שאמרנו S בלתי שקולים בזוגות. ☑

חשבון מודולרי

דוגמה: מצאו את $3122\cdot 35 \pmod 3$ תוך 10 שניות.

אם נחשב את המכפלה ואז נקח שארית בחלוקה ב-3 זה יקח הרבה זמן.

במקום זה נקח כל גורם מוד 3 ונקבל $2\cdot 2=4\equiv 1 \pmod 3$ ולכן $3122\cdot 35\equiv 1 \pmod 3$.

אותו דבר אם היה לנו חיבור או חיסור..

משפט - חשבון מודולרי

יהיו $a,b,c,d\in\mathbb{Z}$, $m\in\mathbb{N}$ כך ש- $a\equiv b \pmod m$, $c\equiv d \pmod m$

אז ① (חיבור) $a+c\equiv b+d \pmod m$

(הוכחה למקרה החיבור: צ"ל $m\,|\,\underbrace{(a+c)-(b+d)}_{\underset{m|\quad m|}{(a-b)+(c-d)}}$)

② (חיסור) $a-c\equiv b-d \pmod m$

③ (כפל) $ac\equiv bd \pmod m$

נוכיח את ③ (היתר קלים יותר, תרגיל)

צ"ל: $m\,|\,ac-bd$. הוכחה:

$$ac-bd=ac-bc+bc-bd=c(a-b)+b(c-d)$$

מהנתון $\left.\begin{matrix} m\,|\,a-b \\ m\,|\,c-d\end{matrix}\right\}$

ולכן m מחלק את אגף ימין (יש לנו בדף האלמנטרי להראות שאם m מחלק 2 מס' הוא מחלק כל צ"ל שלהם)

ולכן $m\,|\,ac-bd$

מה לגבי חילוק? (מה הכוונה?) שכל $\frac{a}{c}\equiv\frac{b}{d}$? זה לא מש רלוונטי כי אולי יוצא לא שלם).

אזהרה/שקר:

④ אם $ac\equiv bc \pmod m$ אז $a\equiv b$.

שקר! $\underbrace{7\cdot 2}_{14}\equiv\underbrace{4\cdot 2}_{8} \pmod 6$ אבל $7\not\equiv 4 \pmod 6$.

כלל הצמצום: יהיו $a,b,c\in\mathbb{Z}$, $m\in\mathbb{N}$ ויהי $d=(c,m)$. אזי:

$$ac\equiv bc \pmod m \iff a\equiv b \left(\bmod \frac{m}{d}\right)$$

(מתי ראינו זה? לכם זה "כלל הצמצום")

דוגמה: $7\cdot 2\equiv 4\cdot 2 \pmod 6$

$\Downarrow$

$7\equiv 4\left(\bmod \left(\frac{6}{(2,6)}\right)\right)$

$7\equiv 4 \pmod 3$

$\not\Downarrow$ $7\equiv 4 \pmod 6$

$50\equiv 20 \pmod{15}$

$5\cdot 10\equiv 2\cdot 10 \pmod{15}$

$\Downarrow$

$5\equiv 2 \bmod\left(\frac{15}{(\text{[illegible]},15)}\right)$

$5\equiv 2 \pmod 3$

$\not\Downarrow$ $5\equiv 2 \pmod{15}$

בס״ד

הוכחה (קל לכתוב ולהבין לא לפחד)

(⇐) נתון $ac\equiv bc\ (\mathrm{mod}\ m) \Leftarrow m\mid ac-bc \Leftarrow \boxed{ac-bc=km}$ עבור $k\in\mathbb{Z}$ כלשהו.

כמו כן $d=(c,m) \Leftarrow \begin{cases} c=d\cdot r \\ m=d\cdot s \end{cases}$ כאשר $(r,s)=1$

(d מכיל את הגורמים המשותפים של m,c,
ולכן r,s מכילים גורמים ראשוניים שונים)

נציב ב-□ ונקבל:

$$(a-b)\cdot d\cdot r=k\cdot ds$$
$$\Downarrow$$
$$(a-b)r=k\cdot s$$
$$\Downarrow$$
$$s\mid(a-b)\cdot r$$

אבל $(s,r)=1$ ולכן (מהלמה של אוקלידס) $a\equiv b\ (\mathrm{mod}\ \underset{\frac{m}{d}}{\underset{\shortparallel}{s}}) \Leftarrow s\mid a-b$

(⇒) (זה בעצם לעשות את הכיוון הקודם מהסוף להתחלה)

נתון כמו קודם $\begin{cases} c=d\cdot r \\ m=d\cdot s \end{cases}$ כאשר $(r,s)=1$

$s\mid(a-b)\cdot r \Leftarrow s\mid a-b \Leftarrow a\equiv b\ (\mathrm{mod}\ s) \Leftarrow a\equiv b(\mathrm{mod}\ \frac{m}{d})$ נתון

$\Leftarrow (a-b)\cdot dr=k\cdot ds \Leftarrow (a-b)\cdot r=k\cdot s$ כך ש- $k\in\mathbb{Z}$ יש $\Leftarrow$

▨ $ac\equiv bc\ (\mathrm{mod}\ m) \Leftarrow m\mid ac-bc \Leftarrow ac-bc=km \Leftarrow (a-b)c=km$.

מסקנה שימושית במיוחד: מתי $ac\equiv bc(m) \Leftarrow a\equiv b(m)$? כאשר $d=(c,m)=1$
״אפשר לצמצם כאשר האיבר בו מצמצמים זר למודולו״

לדוגמא: $7\cdot2\equiv12\cdot2\ (\mathrm{mod}\ 5)$
$$\Downarrow$$
$7\equiv12\ (\mathrm{mod}\ 5)$ $\qquad (2,5)=1$

״דבר ראשוני למסקנה״: אם p ראשוני, $a,b,c\in\mathbb{Z}$ וכן $\overset{\overset{\text{חשוב}}{\downarrow}}{\boxed{p\nmid c}}$
אז אם $ac\equiv bc\ (\mathrm{mod}\ p)$ נקבל $a\equiv b(\mathrm{mod}\ p)$ (כי אז האיבר בו מצמצמים זר למודולו)

לפני המסקנה הבאה נשאל שאלה: אמת/שקר:

אמת או שקר: אם $ab\equiv0\ (\mathrm{mod}\ m)$ אז $a\equiv0(m)$ או $b\equiv0(m)$

שקר: $2\not\equiv0\ (6)$, $3\not\equiv0(6)$ אבל $2\cdot3\equiv0(\mathrm{mod}\ 6)$

תיקון: יהיו $a,b\in\mathbb{Z}$, $m\in\mathbb{N}$, אם $a\cdot b\equiv0(m)$ וגם $\overset{\overset{\text{עיקרי}}{\downarrow}}{\boxed{(a,m)=1}}$ אז $b\equiv0(m)$.

הוכחה: $b\equiv0(m) \underset{\downarrow}{\Leftarrow} ab\equiv a\cdot0\ (m) \Leftarrow a\cdot b\equiv0\ (m)$.
כי $(a,m)=1$ אפשר לצמצם באיבר זר למודולו

בס״ד

״יסוד החשבוני״ למון יהי $a,b\in\mathbb{Z}$, p ראשוני. אם $ab\equiv 0(p)$ אז $a\equiv 0(p)$ או $b\equiv 0(p)$.

הוכחה: אם $a\equiv 0(p)$ סיימנו. אחרת $(a,p)=1$ ומהלמון נקבל $b\equiv 0(p)$.

אמת/שקר: עבור $k,m\in\mathbb{N}$ $a,b\in\mathbb{Z}$ אם $a\equiv b(\mathrm{mod}\, m)$ אז $a^k\equiv b^k(m)$

אמת, מוכיחים באינדוקציה לפי חוק הכפל של החשבון המודולרי. (לא נעשה זאת כאן)

אמת/שקר: אם $a^2\equiv b^2(m)$ $\Leftarrow$ $a\equiv b(m)$

שקר, לדוגמא $2^2\equiv 4^2(3)$ אבל $2\not\equiv 4(3)$

שקילות לינארית

שקילות לינארית היא משוואה מהצורה $ax\equiv b(\mathrm{mod}\, m)$ (דוג׳ $2x\equiv 1(\mathrm{mod}\, 3)$)

לשים ♥ לב שאם 2 פתרון אז כל מי׳צג אחר ממחלקת השקילות שלו הוא פתרון.

משפט (מתי יש פתרון לשקילות לינארית)

נתונה השקילות הלינארית $ax\equiv b(\mathrm{mod}\, m)$ ($m\in\mathbb{N}$, $a,b\in\mathbb{Z}$)

ויהי $d=(a,m)$.

1. אם $d\nmid b$ אין פתרון למשוואה.
2. אם $d|b$ יש d פתרונות שאינם שקולים זה לזה מודולו m.

מסקנה: אם $(a,m)=1$ אז יש לשקילות הנ״ל פתרון יחיד מודולו m.

הוכחת המשפט

1. למשוואה $ax\equiv b(m)$ יש פתרון אמ״מ $ax=b+ym$ עבור $y\in\mathbb{Z}$

וזה קורה אמ״מ למשוואה הדיאופנטית $\underset{\text{נעלם}}{x}$ $a\underset{}{x}-m\underset{}{y}=b$ יש פתרון

נעלם נעלם

וזה קורה אמ״מ $(a,-m)|b$

$$(a,-m) = (a,m) = d$$

הערה: במסגרת ״כדי לפתור שקילות לינארית צריך לפתור משוואה דיאופנטית״

$$ax\equiv b(m)$$
$$\downarrow$$
$$ax-my=b$$

כל x מפתרון המשוואה הדיאופנטית פותר את השקילות הלינארית

(עד כה הראנו שאם $d\nmid b$ אין פתרון ואם $d|b$ יש פתרון. אבל רוצים להראות שאם $d|b$ יש d פתרונות.)

2. אם $d|b$ אז ראינו שיש ∞ פתרונות למשוואה הדיאופנטית $\underbrace{}_{ax-my=b}$ והם כולם מהצורה

$y=y_0-\left(\frac{a}{d}\right)t$ $\quad$ $x=x_0+\left(\frac{-m}{d}\right)t$ לכל $t\in\mathbb{Z}$ (כאשר $\langle x_0,y_0\rangle$ פתרון)

פתרון משוואה דיאופנטית:
$x_1=x_0+\left(\frac{b}{d}\right)t$
$y=y_0-\left(\frac{a}{d}\right)t$

כמו כן אם $<x,y>$ הוא פתרון למשוואה הדיאופנטית אז x פותר את השקילות הלינארית $ax\equiv b \pmod m$.

אנחנו רוצים להבין כמה x-ים שונים יש מודולו m. אם נניח $d=3$ $m=6$

$$x=x_0+\overset{-2t}{\left(\frac{-6}{3}\right)t} \rightarrow x\equiv x_0\,(6) \text{ עם } t=3,6,9,\dots \text{ עבור}$$

$x\equiv x_0-2\,(6)$ עם $t=1,4,7,10,$ עבור.

$x\equiv x_0-4\,(6)$ עם $t=2,5,8,\dots$ עבור

נשים לב שאם x_1,x_2 פתרונות שונים עבור x, אז שקולים $x_1\equiv x_2\,(m)$ אמ"מ $t_1\equiv t_2(d)$ ולכן יש d מחלקות שקילות של פתרונות ל-x מודולו m (המתקבלים למשל ע"י הצבת $t=0,1,\dots,d-1$)

$\downarrow$

<u>הסבר:</u>

נסמן $x_1=x_0-\frac{m}{d}t_1$

$x_2=x_0-\frac{m}{d}t_2$

$$\frac{m}{d}t_1\equiv\frac{m}{d}t_2(m)\overset{\text{צמצום חיבור}}{\iff}x_0-\frac{m}{d}t_1\equiv x_0-\frac{m}{d}t_2(m)\overset{\text{הצבה}}{\iff}x_1\equiv x_2(m)$$

$$t_1\equiv t_2(d)\iff t_1\equiv t_2\left(\frac{m}{\left(\frac{m}{d}\right)}\right)\underset{\text{כי } \frac{m}{d}|m}{\iff}t_1\equiv t_2\left(\frac{m}{(m,\frac{m}{d})}\right)\underset{\text{חוק הצמצום}}{\iff}$$

<u>הפכי מודולרי</u>

<u>הגדרה:</u> יהי $a\in\mathbb{Z}$, $m\in\mathbb{N}$ כך ש-$(a,m)=1$. הפתרון (היחידי!) לשקילות $ax\equiv 1 \pmod m$ נקרא ההפכי של a מודולו m.

לפי המשפט שהוכחנו קודם לכן

<u>דוגמה:</u> $7,\boxed{?}$ הפכיים מודולו 31.

$$\overset{a}{7}\cdot\boxed{x}\equiv\overset{b}{1}\pmod{31}$$

דרך א' $\downarrow$

אפשר לנחש פתרון

7 כפולה

$31+1=32$

$31\times2+1=63$

$\Downarrow$

$x=9$

דרך ב' $\leftarrow$ לפי המסקנה מעמ' 37

כאן צריך לפתור משוואה דיאופנטית מהצורה

$7x-31y=1$

$(ax-my=b)$

(בשיטת 3 השלבים שלמדנו וזה קל)

$$\begin{cases}x=9\\y=2\end{cases}$$

∎ שיטה כללית יותר.

לכן 7,9 הפכיים מודולו 31. בעצם 9 אשר גם לוקח כל נציג אחר של מחלקת השקילות שלו מוד 31, למשל 40.