<u>שקילויות</u>

הגדרה: יהי $m \in \mathbb{Z}^+$ ויהיו $a, b \in \mathbb{Z}$. נאמר כי a שקול ל-b מודולו m ונרשום $a \equiv b \ (mod\ m)$ אם $m | a - b$.

משפט 1: יהי $m \in \mathbb{Z}^+$ ויהיו $a, b \in \mathbb{Z}$. אזי $a \equiv b \ (mod\ m)$ אם ורק אם $a = b + km$ עבור $k \in \mathbb{Z}$ כלשהו.

הוכחה:

<u>כיוון ראשון</u>: אם $a \equiv b \ (mod\ m)$ אזי $m | a - b$ כלומר $km = a - b$.

<u>כיוון שני</u>: אם $a = b + km$ עבור $k \in \mathbb{Z}$ כלשהו אזי $a - b = km$ ולכן $m | a - b$. $\blacksquare$

<u>**דוגמה**</u>: $13 \equiv 8 \ (mod\ 5)$ שכן $13 = 8 + 5 \cdot 1$.

הגדרה: בהינתן $m \in \mathbb{Z}^+$ נגדיר את היחס

$$R_m \coloneqq \{(a, b) \in \mathbb{Z}^2 : a \equiv b \ (mod\ m)\}.$$

משפט 2: יהי $m \in \mathbb{Z}^+$. היחס R_m מגדיר מחלקות שקילות "מודולו m". כלומר, הוא מקיים את התכונות הבאות:

1. <u>רפלקסיביות</u>: $a \equiv a \ (mod\ m)$ לכל $a \in \mathbb{Z}$.
2. <u>סימטריות</u>: אם $a, b \in \mathbb{Z}$ אזי $a \equiv b \ (mod\ m)$ אם ורק אם $b \equiv a \ (mod\ m)$.
3. <u>טרנזיטיביות</u>: אם $a, b, c \in \mathbb{Z}$ כך ש $a \equiv b \ (mod\ m)$ וגם $b \equiv c \ (mod\ m)$ אזי $a \equiv c \ (mod\ m)$.

הוכחה:

<u>רפלקסיביות</u> נובעת ישירות מכך ש $m | a - a$ לכל a.
<u>סימטריות</u> נובעת מהאבחנה ש $m | a - b$ אם ורק אם $m | b - a$.
<u>טרנזיטיביות</u> נובעת מכך שאם $m | a - b$ וגם $m | b - c$
אזי

$$a = b + k_1 m, \quad b = c + k_2 m$$

ולכן נציב ונקבל

$$a = c + (a - b) + (b - c) = c + k_1 m + k_2 m$$
$$= c + (k_1 + k_2) m$$

כלומר $m | a - c$. $\blacksquare$

הגדרה: *מערכת שאריות שלמה מודולו* m היא קבוצת שלמים כך שכל $a \in \mathbb{Z}$ שקול לאיבר יחיד של אותה קבוצה מודולו m.

דוגמה: תהי הקבוצה $S = \{16,11,12,19,14,27\}$ ויהי $m = 6$. על כל איבר בקבוצה S נפעיל פעולת $mod\ 6$ ונרשום את התוצאה: $S' = \{4,5,0,1,2,3\}$. כל איבר בקבוצה S שקול לאיבר מהקבוצה S', והקבוצה S' מכילה את כל השאריות של חלוקה ב 6. לכן, S הינה מערכת שאריות שלמה מודולו 6. כמו-כן, הקבוצה S' הינה *מערכת שאריות קנונית מודולו* 6.

משפט 3 (עיקרון שובך היונים): אם n יונים מתחלקים בין לכל היותר $n-1$ שבכים, אזי לאחר החלוקה קיים שובך המכיל לפחות שני יונים.

משפט 4: יהי $m \in \mathbb{Z}^+$. כל קבוצה של m מספרים לא שקולים מודולו m מהווה מערכת שאריות שלמה מודולו m.

הוכחה: תהי קבוצה S בגודל m. לכל איבר $s \in S$ נפעיל את משפט החלוקה ונקבל $s = k_s m + r_s$. תהי $R \coloneqq \{r_s : s \in S\}$ קבוצת השאריות. נניח בשלילה כי S מכילה m מספרים לא שקולים מודולו m אך עדיין אינה מייצגת מערכת שאריות שלמה מודולו m. לכן, $|R| \leq m-1$, כלומר, יש m מספרים ולכל היותר $m-1$ שאריות, ולכן קיימים $s, s' \in S$ כך שמתקיים $s \neq s'$ ועדיין $r_s = r_{s'}$ לפי עיקרון שובך היונים (משפט 3). לכן, s, s' שקולים מודולו m. סתירה. ■

משפט 5: (אריתמטיקה מודולרית)

יהיו $a, b, c, d \in \mathbb{Z}$ ויהי $m \in \mathbb{Z}^+$ כך ש $a \equiv b \ (mod\ m), c \equiv d \ (mod\ m)$. אזי:

1. <u>חיבור</u>: $a + c \equiv b + d \ (mod\ m)$.
2. <u>חיסור</u>: $a - c \equiv b - d \ (mod\ m)$.
3. <u>הכפלה</u>: $ac \equiv bd \ (mod\ m)$.

הוכחה: לפי ההנחה מתקיים $a - b = km, \quad c - d = lm$. (1)

<u>חיבור</u>: נשים לב כי

$$(a + c) - (b + d) = (a - b) + (c - d).$$

נציב את (1) וסיימנו.

<u>חיסור</u>: נשים לב כי

$$(a - c) - (b - d) = (a - b) - (c - d).$$

נציב את (1) וסיימנו.

<u>הכפלה</u>: נשים לב כי מתקיים

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= c(a - b) + b(c - d) \\ &= kmc + lmb \\ &= m(kc + lb) \end{aligned}$$

ולכן $m | ac - bd = m(kc + lb)$. ■

<u>**דוגמה**</u>: $13 \equiv 8 \ (mod\ 5)$, $24 \equiv 4 \ (mod\ 5)$. לכן מתקיים

$$24 + 13 = 37 \equiv 4 + 8 \equiv 12 \ (mod\ 5)$$

$$24-13=11\equiv 4-8\equiv -4\ (mod\ 5)$$

$$24\cdot 13=312\equiv 4\cdot 8\equiv 32\ (mod\ 5)$$

משפט 6: יהיו $a,b,c\in\mathbb{Z}$ ויהי $m\in\mathbb{Z}^+$ כך ש $d=(c,m)$. אזי $ac\equiv bc\ (mod\ m)$ אם ורק אם $a\equiv b\ (mod\ {}^{m}/_{d})$.

הוכחה:

<u>כיוון ראשון</u>: נניח כי $ac\equiv bc\ (mod\ m)$. כלומר $m|c(a-b)$ ובמילים אחרות

$$mk=c(a-b)$$

עבור $k\in\mathbb{Z}$ כלשהו. לפי הגדרת gcd ניתן לרשום $m=ds, c=dr$ כאשר $(s,r)=1$. נציב ונקבל

$$ks=r(a-b),$$

כלומר, $s|r(a-b)$. היות ומתקיים $(s,r)=1$ אזי בהכרח $s|(a-b)$. היות והגדרנו $s={}^{m}/_{d}$, סיימנו.

<u>כיוון שני</u>: כיוון זה זהה לכיוון הראשון, רק שעובדים "מלמטה למעלה". ■

<u>דוגמה</u>: $2\cdot 10=20\equiv 2\cdot 7\equiv 14\ (mod\ 2\cdot 3)$ אם ורק אם $10\equiv 7\ (mod\ 3)$.