

שיעור 2

8 בנובמבר 2016

0.0.1 אובייקטים מתמטיים:

חבורות	(פעולה יחידה, $+$ או $\cdot$)
חוגים	($+$ וגם $\cdot$)
שדות	($+$ וגם $\cdot$, בנוסף לתכונות נוספות)

1 מתמטיקה מודולרית

המספרים בהם נעסוק יהיו שלמים. סימון: $a \equiv b \pmod m$ פירושו m מחלק את $a - b$. $a \pmod m$ יסמן את שארית החלוקה של a ב- m (השארית בין 0 ל- $m-1$). עבור $\mathbb{Z}_m, m \geq 1$ יסמן את קבוצת המספרים $\{0, \dots, m-1\}$. ונגדיר את הפעולות $+_m, \cdot_m$, פעולות הכפל והגריליות בשלמים כשהתוצאה נלקחת $\pmod m$. $\{ \mathbb{Z}_m, +_m, \cdot_m \}$ המבנה המתמטי הזה נקרא חוג (ring), ספציפית זהו חוג השלמים מודולו m .

- בחוג זה החיבור והכפל הם קומוטטיבים ($a +_m b = b +_m a, a \cdot_m b = b \cdot_m a$)
- יש איבר נייטרלי ביחס לחיבור - 0 ($a +_m 0 = 0 +_m a = a$)
- וכן יש איבר נייטרלי ביחס לכפל - 1 ($a \cdot_m 1 = 1 \cdot_m a = a$)
- הכפל הוא דיסטריבוטיבי מעל החיבור ($a \cdot_m (b +_m c) = a \cdot_m b + a \cdot_m c$)
- לכל $a \in \mathbb{Z}_m$ יש הופכי חיבורי יחיד $a +_m b = b +_m a = 0$
- בהינתן $a \in \mathbb{Z}_m$, נאמר כי b הוא הופכי כיפלי שלו אם $a \cdot b = b \cdot a = 1$

שאלה: האם לכל איבר (שאינו 0) ב- $\mathbb{Z}_m$ יש הפכי כפלי? זה תלוי...בשאלה האם m ראשוני או לא, התשובה כן אם ורק אם m ראשוני

דוגמא: $m = 6, a = 5$ אזי $b = 5$ הוא הופכי כיפלי מאחר ו- $5 \cdot 5 = 25 \equiv 1 \pmod 6$
דוגמא: נראה כי עבור $a = 4$ אין הופכי $\pmod 6$

$$\begin{aligned}4 \cdot 1 &\neq 1 \\4 \cdot 2 &\neq 1 \\4 \cdot 3 &\neq 1 \\4 \cdot 4 &\neq 1 \\4 \cdot 5 &\neq 1\end{aligned}$$

שיטה זאת עובדת אך מאוד לא יעילה, מומלצת רק עבור m -ים קטנים
הוכחה "כשרה":

לכל b , מעל השלמים $4 \cdot b$ זוגי ולכן השארית בחלוקה ב-6 (זוגי בעצמו) אף היא זוגית ובפרט אינה 1.
לכן ל-4 אין הופכי כפלי ב- $\mathbb{Z}_6$.

משפט 1.1 (ללא הוכחה), למשוואה $a \cdot x = b \pmod m$, יש פתרון יחיד $x \in \mathbb{Z}_m$ אם $\gcd(a, m) = 1$ (זאת אומרת a, m זרים)

למשל עבור $m = 6$ והמשוואה $3 \cdot x = 0$ יש 3 פתרונות - $x = 0, 2, 4$
מאידך ל- $5 \cdot x = 1$ יש פתרון יחיד $x = 5$
נחזור לשאלה - לאיזה a יש הופכי כיפלי ב- $\mathbb{Z}_m$? (המשוואה $a \cdot x = 1$)
מהמשפט נובע כי אם a זר ל- m , אז יש פתרון x והוא הופכי כיפלי
לבדוק: האם זה גם תנאי הכרחי - אם $\gcd(a, m) > 1$ אז ל- a אין הופכי כפלי $\pmod m$? (תשובה: כן)
לכן ב- $\mathbb{Z}_7, \mathbb{Z}_{11}, \mathbb{Z}_{13}$ ובאופן כללי $\mathbb{Z}_p$ כאשר p הוא ראשוני לכל $1 \leq a \leq p-1$ יש הופכי כפלי (כי a זר ל- p היות ש- p ראשוני)

המשך במצגת (בנקודות)

- gcd
- שימוש באלגוריתם אוקלידס למציאת gcd
- זהות בזו (אם מתקיים $gcd(r_0, r_1) = g$ אזי קיימים A, B כך ש $A \cdot r_0 + B \cdot r_1 = g$ וניתן למצוא אותם בעזרת אלגוריתם אוקלידס)
- SageMathCloud
- חזרה על שיעור 1 (במצגת)
- דוגמא ל perfect cipher – one time pad (הצפנה $p \oplus k = c$, פענוח $c \oplus k = p$)
- קשר בין סיבוכיות לקריפטוגרפיה
- pseudo random distribution A_n תיקרא פסאודו אקראית אם היא התפלגות שלא ניתן להבדיל בזמן פולינומי בינה ובין התפלגות האחידה)
- G כיפלי של G אם מתקיים $G = \{g, g^2, \dots, g^{p-1}\}$ כאשר $|G|=p-1$
- pseudo random generator פונקציה שניתן לחשב בזמן פולינומי שאי אפשר להבדיל בין הפלט שלה לפלט אקראי בזמן פולינומי
- one way function פונקציה שאי אפשר להפוך את הפלט שלה (לקבל מהפלט שלה את הקלט) בזמן פולינומי
- synchronous stream cipher מחכה one time pad, לוקח גרעין קטן seed מרחיב אותו בעזרת pseudo random generator ומצפין אות ההודעה בסגנון one time pad עם ההרחבה שייצרנו.
- LFSR-linear feedback shift registers דוגמא ל pseudo random generator