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 : $a \equiv b \ mod \ m$ פירושו m מחלק את $a-b$. $a \mod m$ 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 $\{0,\ldots,m-1\}$. ונגדיר את הפעולות $+_m, \cdot_m$, פעוולות הכפל הרגילות בשלמים כשהתוצאה נלקחת $\mod m$ $\{Z_m, +_m, \cdot_m\}$.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 דיסטריביוטיבי מעל החיבור ($a \cdot_m (b +_m c) = a \cdot_m b + a \cdot_m c$)
- לכל $a \in \mathbb{Z}_\mathrm{m}$ יש הופכי חיבורי יחיד $\forall a \exists b. a +_m b = b +_m a = 0$
- בהינתן $a \in \mathbb{Z}_m$, נאמר כי bהוא 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$5 \cdot 5 = 25 \mod 6 \equiv 1$

דוגמא: נראה כי עבור $a = 4$ אין הופכי $\mod 6$

$$4 \cdot 1 \neq 1$$
$$4 \cdot 2 \neq 1$$
$$4 \cdot 3 \neq 1$$
$$4 \cdot 4 \neq 1$$
$$4 \cdot 5 \neq 1$$

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$\mathbb{Z}_b$.

משפט 1.1 (ללא הוכחה), למשוואה בנעלם x, ($a \cdot x = b \mod m$) יש פתרון יחיד $x \in \mathbb{Z}_m$ אמ"ם $gcd(a,m) = 1$ (זאת אומרת m,a 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 $ax = 1$)

מהמשפט נובע כי אם a זר לm, אז יש פתרון x והוא הופכי כיפלי

לבדוק: האם זה גם תנאי הכרחי ־ אם $gcs(a,m) > 1$ אז ל־a אין הופכי כפלי $\mod m$? (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)

ההמשך 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 one time pad $-$ perfect cipher (הצפנה $p \oplus k = c$, פענוח $c \oplus k = (p \oplus k) \oplus k = p \oplus (k \oplus k) = p$)
- קשר בין סיבוכיות לקריפטוגרפיה
- pseudo random distribution(A_n תיקרא פסאודו אקראית אם היא התפלגות שלא ניתן להבדיל בזמן פולינומי בינה ובין התפלגות האחידה)
- gיוצר כיפלי של G אם מתקיים $G = \{g, g^2, \ldots, g^{p-1}\}$ כאשר p-1=$|G|$
- 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 לpseudo random generator