אלגברה מודרנית - הרצאה 1

כותב: איתי ויסמן, מרצה: רון אהרוני

26 באפריל 2019

נתעסק בחבורות ובמספרים טבעיים שמסומנים: $\mathbb{N} = \{...0,1,2,3\}$
ובמספרים השלמים שמסומנים: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
יש חומרים בmoodle, ומומלץ הספר Herstein.

1 חלוקה עם שארית

למשל: $35 : 8 = 7(3)$

משפט. לכל שני מספרים טבעיים a, b יש מספרים $0 \le r \le b$ כך שמתקיים: $a = kb + r$

הוכחה. יהא k המספר הגדול ביותר כך ש-$kb \le a$. טענה: מתקיים $a - kb < b$. הוכחה: אם לא, אזי $a - kb \ge b$ ואז $a \ge kb + b = (k+1)b$ בסתירה לכך ש k הוא מקסימלי כך ש- $a \ge kb$. ■

טענה. $b|(a_1 - a_2) \iff a_1 \equiv a_2 mod(b)$ כלומר $a_1 - a_2$ מחלק את b.

הוכחה. כיוון אחד, כיוון שני קל להוכיח בבית. אם $a_1 \equiv a_2 mod(b)$ אזי מתקיים: $a_1 - a_2 = (k_1 - k_2)b = kb$. ■

2 סגירות לחיבור וחיסור

הגדרה. נאמר כי תת קבוצה $S \subseteq \mathbb{Z}$ סגורה לחיבור אם לכל $s, t \in S$ מתקיים $s + t \in S$.

לדוגמה הקבוצה $\mathbb{N}, -\mathbb{N}$, קבוצת הזוגיים ב$\mathbb{Z}$, כל המספרים ב$\mathbb{Z}$ הגדולים ממס' מסויים x.

הערה. $S \subseteq \mathbb{Z}$ תקרא סגורה לחיסור אם לכל $s, t \in S$ מתקיים $s - t \in S$.

מסתבר שסגירות לחיסור זה רק עבור קבוצות מסוג $k \cdot \mathbb{Z}$.
דוגמאות לקבוצות המקיימות סגירות לחיבור וגם סגירות לחיסור: $k \cdot Z$ הכפולות של מס' מסויים k.

משפט. אם $S \subseteq \mathbb{Z}$ סגורה גם לחיבור וגם לחיסור אזי קיים $k \in \mathbb{Z}$ כך ש $S = k \cdot \mathbb{Z}$, אפשר גם לקחת $k \in \mathbb{N}$.

טענה. לקבוצה שסגורה לחיבור ולחיסור נלמד בהמשך שנקראת חבורה.

הוכחה. תהי קבוצה $S \subseteq Z$ סגורה לחיבור ולחיסור. צריך להוכיח כי קיים $k \in \mathbb{N}$ כך ש-$S = k \cdot \mathbb{N}$.
נשים לב שאם נמצא k כזה אז הוא יהיה איבר ב-S. זאת משום שמתקיים: $S = \{k \cdot a | a \in \mathbb{Z}\}$ ולכן עבור $a = 1$ יתקיים $k \in S$.
מניחוש של תלמיד, k הזה יהיה המספר הטבעי הכי קטן ב-S. ∎

טענה. יהא k המס' הטבעי הכי קטן ב-S. $S = k \cdot Z$.

הוכחה. פר נראה כי $S \subseteq k \cdot \mathbb{Z}$ ולאחר מכן נראה $S \supseteq k \cdot \mathbb{Z}$, כלומר נראה הכלה דו כיוונית.
כיוון אחד: מתקיים מסגירות לחיבור $2k = k + k \in S$ וכן $3k = k + k + k \in S$ ולכן גם עבור $m \cdot k = k + k + k + \cdots + k \in S$. זה עבור המספרים החיובים. עבור המספרים השליליים ניתן להראות אותו דבר מסגירות לחיסור כי לכל $m < 0$, מכיוון ש $0 \in S$ אזי $-k = 0 - k \in S$ ולכן לכל $m < 0$ כזה $m \cdot -k \in S$. זה מראה את הכיוון הראשון.
כיוון שני: עבור S, יהא $s \in S$ נניח כי $s > 0$ נרצה להראות כי עבור m מסויים מתקיים $s = mk$.
עבור $s = 0$ קיים $m = 0$ כך ש $s = mk = 0$.
עבור $s > 0$ נשתמש במשפט החלוקה ולכן קיימים $0 \leq r \leq k$ כך ש $s = mk + r$ ולכן $r = s - mk$ ומסגירות לחיסור $r \in S$ ומכיוון ש$r \leq k$ אם $r \neq 0$ נקבל כי הוא קטן יותר מk ובתוך S וזאת בסתירה למינימליות k. לכן בהכרח $r = 0$ ומתקיים כי $s = mk$.
עבור $s < 0$ אזי מתקיים: $-s = 0 - s \in \mathbb{Z}$. נשתמש בשיטת ה"קומקום", כלומר נשתמש במה שכבר הוכחנו, עבור המספרים החיוביים. לכן קיים m כך ש-$-s = mk$ ולכן $s = (-m)k$ ולכן $s \in k\mathbb{Z}$.
ולכן לכל $s \in S$ הטענה מתקיימית ולכן $s \subseteq k\mathbb{Z}$ ∎

הערה: צריך להוכיח את נכונות המשפט גם עבור המקרה המיוחד בו $S = \{0\}$.

3 כלל ההתחלקות ב-3

מספר מתחלק ב-3 אם סכום ספרותיו מתחלק ב-3.
לדוגמה: המספר 7521 משום שמתקיים $15 = 1 + 2 + 5 + 7$ וכן 15 מתחלק ב-3.
נוכיח משפט זה על ידי הוכחה של משפט כללי יותר עבור שארית כללית:

משפט. אם סכום הספרות במספר n הוא m אזי $m \equiv n(mod3)$.

למשל עבור המספר 7528 מתקיים כי $7528 \equiv 1mod(3)$.
נשאל את השאלה הבאה: מהי הספרה האחרונה במס' $2019 + 1756$. לא צריך לחשב את כל החיבור על מנת להיווכח כי הספרה הזו היא 5. לכן על מנת להבין את השאריות של המחוברים. כלומר: מתקיים $2019 = 9(mod10)$ וכן $1756 = 6(mod10)$ ולכן מתקיים $2019 + 1756 = 9 + 6(mod(10)) = 5(mod(10))$.
נשאל שאלה נוספת: מהי הספרה האחרונה במס' 2019×1756. באופן דומה קל להיווכח כי הספרה האחרונה היא 4, שכן מתקיים $6 \cdot 9 = 54$

טענה. באופן כללי אם $m = a(modk)$ וכן $n = p(modk)$ אזי $m + n = a + b(modk)$.

הוכחה. נתון $k|m-a$ וכן $k|n-b$ כלומר קיימים s,t כך ש$m-a=tk$ וכן $n-b=sk$ ולכן מתקיים $m+n-(a+b)=(s+t)k$ ולכן מתקיים $k|(m+n)-(a+b)$ ולפי המשפט לעיל יש להם אותה שארית ולכן $m+n=a+b(modk)$. ■

מה הרלוונטיות של זה לחלוקה ב-3? הסוד של כלל חלוקה ב-3 הוא שאנו עובדים בשיטה העשרונית, ומתקיים $10=1(mod3)$ ולכן עבור $10\cdot10=100$ מתקיים ממה שהוכחנו $100=1\cdot1(mod3)=1mod(3)$. כך עבור 1000 ו100001 וכ'ו. אם נחזור לדוגמה שלנו קודם: $7528=7\cdot1000+5\cdot100+2\cdot10+8\cdot1=7\cdot1+5\cdot1+2\cdot1+8\cdot1(mod3)=22mod(3)$

די התעלמנו מכך שלמשל 7 הוא בעצם שווה ל1 במודולו 3 כי נוח להסתכל בצורה זו למשפט שלנו.

מעניין להוכיח את כלל ההתחלקות ב11. לדוגמה 1331 מתחלק ב11 כי מתקיים שהמס' $1-3+3-1=0$ מתחלק ב11. זה מקיים כי $10=-1mod(11)$ ולכן $100=-1\cdot-1mod(11)=1mod(11)$.

4 מספרים ראשוניים

הגדרה. נאמר כי מס' $p\in\mathbb{N}$ ראשוני אם אין לו מחלקים ב-$\mathbb{N}$ פרט ל-1 ולעצמו. בנוסף 1 אינו ראשוני.

דוגמה. $1,2,3,5,7,...,1003$

לפני מס' שנים הייתה פריצת דרך ומצאו אלגוריתם בסיבוכיות פולינומיאלי לבדיקה האם מס' n הוא ראשוני. עבור הבדיקה הטריוויאלית של חלוקה בכל מס' ראשוני עד $\sqrt{n}$, מסתבר כי הסיבוכיות היא אקספוננציאלית בקלט, שכן הוא תלויה בגודל n, ולכן מציאת האלגוריתם בסיבוכיות פולינומיאלית היא פריצת דרך חשובה. על השאלה האם בהינתן המידע שהמס' אינו ראשוני נרצה למצוא את הפירוק שלו לגורמים עוד לא ענו, וזה מאוד חשוב לקריפטוגרפיה שכן מרבית שיטות ההצפנה כיום מתבססים על כך שקשה לפרק מספרים מאוד גדולים.

משפט. המשפט היסודי של המספרים הטבעיים.
לכל מספר n יש פירוק יחיד למספרים ראשוניים: $n=p_1\cdot p_2\cdots p_k$. למשל עבור $120=2\cdot2\cdot2\cdot3\cdot5$

משפט. משפטו של אוקלידס.
יש אינסוף מספרים ראשוניים.

הוכחה. למשפט אוקלידס. נניח בשלילה שיש רק מס' סופי של מספרים ראשוניים. נקרא להם $p_{1,}p_2,\cdots p_k$ נסתכל על $n=p_1\cdot p_2\cdots p_k+1$. n אינו מתחלק בp_1 שכן $n=1(mod(p_1))$. ולכן n אינו מתחלק בp_2 וכך לכל p_k. ולכן לפי המשפט היסודי, יש מס' ראשוני q שמחלק את n, אך q שונה מכל p_k וזאת בסתירה להנחה שיש קבוצה סופית של מס' ראשוניים. ■

הערה: השערת גאוס מביאה נוסחה לכמות המס' הראשוניים בין 0 לn כלשהו. לפי ההשערה יש בערך בין 0 ל-$\frac{n}{ln(n)}$ מספרים ראשוניים.