פתרון תרגיל בית 7 במבנים אלגבריים
89-214 סמסטר א' תשפ"ג

שאלה 1. נסמן ב-abc את שלוש הספרות הראשונות של מספר הת"ז שלכם וב-yz את שתי הספרות האחרונות.

מצאו בעזרת אלגוריתם אוקלידס המורחב את $\gcd(abc, yz+12)$ ואת מקדמי הצירוף הלינארי שלהם ששווה לו.

פתרון. פנו אלינו אם אתם רוצים לוודא את התשובה שלכם (השתמשנו במחשב לחישוב כל האפשרויות). אפילו יותר טוב זה לנסות לבדוק את הפתרון של חברים בקורס, והם בתמורה יבדקו את שלכם.

שאלה 2. רמז: אלגוריתם אוקלידס עובד גם עם פרמטרים.

א. הוכיחו שלכל n שלם מתקיים $(4n+3, 7n+5) = 1$.

ב. מצאו $s, t \in \mathbb{Z}$ (ואולי תלויים ב-n) כך ש-$(4n+3)s + (7n+5)t = 1$.

פתרון.

א. נשתמש כמה פעמים בכך שאם $n = qm + r$, אז $(n, m) = (m, r)$.

$$\begin{aligned}(7n+5, 4n+3) &= [7n+5 = 2\cdot(4n+3) + (-n-1)]\\ (4n+3, -n-1) &= [4n+3 = -4\cdot(-n-1) - 1]\\ (-n-1, -1) &= 1\end{aligned}$$

אפשר לעשות את החישוב בכמה דרכים, למשל כאשר נמנעים ממקדמים שליליים ל-n:

$$\begin{aligned}(7n+5, 4n+3) &= [7n+5 = 1\cdot(4n+3) + (3n+2)]\\ (4n+3, 3n+2) &= [4n+3 = 1\cdot(3n+2) + (n+1)]\\ (3n+2, n+1) &= [3n+2 = 3\cdot(n+1) - 1]\\ (n+1, -1) &= 1\end{aligned}$$

ב. משתמשים בשלבים של אלגוריתם אוקלידס המורחב, לפי הסעיף הקודם:

$$\begin{aligned}-n-1 &= 1\cdot(7n+5) - 2\cdot(4n+3) \quad \Rightarrow\\ -1 &= 1\cdot(4n+3) + 4\cdot(-n-1)\\ &= 4\cdot(7n+5) - 7\cdot(4n+3)\end{aligned}$$

ולכן נקבל $s = 7, t = -4$, שאינם תלויים ב-n!

שאלה 3. חשבו בעזרת חבורת אוילר ומשפט אוילר את הסעיפים הבאים:

א. שתי הספרות האחרונות של המספר $89^{3602} + 5783^{4121}$.

ב. $118^{287} \pmod{95}$.

פתרון.

א. לפי הנוסחה של פונקציית אוילר מתקיים

$$\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

לפי משפט אוילר, לכל x זר ל-100 מתקיים $x^{40} \equiv 1 \pmod{100}$. יתר על כן, המספרים 89 ו-5783 זרים ל-100 ומתקיים

$$\begin{aligned} 3602 &\equiv 2 \pmod{40} \\ 4121 &\equiv 1 \pmod{40} \end{aligned}$$

לכן

$$\begin{aligned} 89^{3602} + 5783^{4121} &\equiv 89^2 + 83^1 \equiv (-11)^2 + 83 = 121 + 83 \\ &= 204 \equiv 4 \pmod{100} \end{aligned}$$

וקיבלנו שהתשובה היא 04.

ב. לפי הנוסחה של פונקציית אוילר מתקיים

$$\varphi(95) = 95\left(1-\frac{1}{5}\right)\left(1-\frac{1}{19}\right) = 95 \cdot \frac{4}{5} \cdot \frac{18}{19} = 72$$

בנוסף $118 \equiv 23 \pmod{95}$. לכן לפי משפט אוילר,

$$118^{287} \equiv 23^{287} = 23^{4\cdot 72-1} \equiv 23^{-1} \pmod{95}$$

לכן נותר למצוא את ההופכי של 23 ב-U_{95} (23 אכן זר ל-95). נפעיל את אלגוריתם אוקלידס ונקבל

$$\begin{aligned} 95 &= 4 \cdot 23 + 3 \\ 23 &= 7 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

לכן $\gcd(23, 95) = 1$. כעת נחשב לאחור ונקבל

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (23 - 7 \cdot 3) \\ &= 8 \cdot 3 - 1 \cdot 23 \\ &= 8 \cdot (95 - 4 \cdot 23) - 1 \cdot 23 \\ &= 8 \cdot 95 - 33 \cdot 23 \end{aligned}$$

מכאן ההופכי של 23 ב-U_{95} הוא -33. על מנת לבחור נציג חיובי, נוסיף 95 ונקבל שהתשובה היא 62.

שאלה 4. הוכיחו כי אם m, n שלמים חיוביים אז $(m^2, m+n) = (n^2, m+n)$.

פתרון. ניעזר באלגוריתם אוקלידס ונקבל

$$\begin{aligned}(m^2, m+n) &= \big(m^2 - (m-n)(m+n), m+n\big)\\ &= \big(m^2 - (m^2-n^2), m+n\big)\\ &= \big(n^2, m+n\big)\end{aligned}$$

שאלה 5. רמז: המספר $\varphi(n)$ הוא סדר של חבורה מוכרת.

א. הוכיחו כי לכל $n \geq 3$ טבעי המספר $\varphi(n)$ זוגי.

ב. הוכיחו שלכל $m, s > 1$ טבעיים מתקיים כי $m|\varphi(s^m - 1)$.

פתרון. הנה שתי הוכחות לסעיף הראשון:

א. <u>הוכחה ראשונה:</u> נעזר ברמז ונתבונן בחבורה U_n. לפי טענה מההרצאה,

$$(n, n-1) = (n, n-(n-1)) = (n, 1) = 1$$

לכן $n-1 \in U_n$. מכיוון ש-$n \geq 3$ מתקיים ש-$n-1 \not\equiv 1 \pmod{n}$. יתר על כן

$$(n-1)^2 \equiv (-1)^2 = 1 \pmod{n}$$

לכן הסדר של $n-1$ הוא $o(n-1) = 2$. לפי ממשפט לגראנז' נסיק

$$2 \mid |U_n| = \varphi(n)$$

<u>הוכחה שנייה:</u> נסתכל על U_n כתת-קבוצה של $(\mathbb{Z}_n, +)$ כאשר מתעלמים מפעולת הכפל. לכל a שלם $(a, n) = (-a, n)$. לכן לכל $a \in \mathbb{Z}_n$ מתקיים ש-$a \in U_n$ אם ורק אם $-a \in U_n$. מכאן אפשר לחלק את U_n לזוגות: איבר והנגדי לו, ביחס לפעולת החיבור ב-$\mathbb{Z}_n$. בכך סיימנו אלא אם יש איבר הנגדי לעצמו. נניח שיש איבר כזה a כאשר בוחרים נציג שעבורו $0 \leq a < n$. במקרה כזה

$$\begin{aligned}a &\equiv -a \pmod{n}\\ 2a &\equiv 0 \pmod{n}\end{aligned}$$

ולכן $n|2a$. מכיוון ש-$0 \leq a < n$ נובע כי $0 \leq 2a < 2n$. לכן $2a = 0$ או $2a = n$. אם $2a = 0$, אז $a = 0$, ואז $a \notin U_n$, שזו סתירה. לכן נניח $2a = n$. במקרה זה n זוגי, ואז $a = \frac{n}{2}$. מתקיים כי

$$\gcd\left(\frac{n}{2}, n\right) = \frac{n}{2} > 1$$

כאשר השתמשנו בנתון $n \geq 3$. לכן $a \notin U_n$, וזו שוב סתירה.

ב. לפי הרמז נשים לב כי $\varphi(s^m - 1) = |U_{s^m-1}|$. אם נמצא איבר $x \in U_{s^m-1}$ מסדר m, אז נסיים לפי המסקנה ממשפט לגראנז' שבה מראים כי סדר של איבר מחלק את סדר החבורה.
נבחר את $x = s$. קל לבדוק כי $s^{m-1} \cdot s - 1 \cdot (s^m - 1) = 1$ ולכן $(s, s^m - 1) = 1$. כלומר $s \in U_{s^m-1}$. נותר להראות שהסדר של s בחבורה הוא m. תחילה להיתכנות, מחשבים

$$s^m \equiv 1 \pmod{s^m - 1}$$

שהרי $s^m - 1 \equiv 0 \pmod{s^m - 1}$, ולכן $o(s)|m$. למינימליות של הסדר, נשים לב כי $s^i < s^m - 1$ לכל $i < m$ כמספרים טבעיים. לכן גם בהכרח s^i אינו שקול ל-1 מודולו $s^m - 1$. בסך הכל $o(s) = m|\varphi(s^m - 1)$.

שאלה 6. בחבורה A_9, מצאו איברים מהסדרים $4, 6, 7, 8, 10, 12, 14$ או שהוכיחו שלא קיים איבר כזה.

פתרון. ניזכר כי עבור $\sigma \in S_n$ מתקיים $\sigma \in A_n$ אם ורק אם $\operatorname{sign}(\sigma) = 1$. נבדוק כל אפשרות:

א. נוכיח שקיים איבר מסדר 4. נבחר $\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$. אכן מתקיים

$$\operatorname{sign}(\sigma) = (-1)^{4-1}(-1)^{4-1} = 1$$
$$o(\sigma) = \operatorname{lcm}(4,4) = 4$$

ב. נוכיח שקיים איבר מסדר 6. נבחר $\sigma = (1\ 2)(3\ 4)(5\ 6\ 7)$. אכן מתקיים

$$\operatorname{sign}(\sigma) = (-1)(-1)(-1)^2 = 1$$
$$o(\sigma) = \operatorname{lcm}(2,2,3) = 6$$

ג. נוכיח שקיים איבר מסדר 7. נבחר $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$. σ מעגל באורך 7 ולכן $o(\sigma) = 7$. 7 אי זוגי ולכן σ תמורה זוגית.

ד. נוכיח שלא קיים איבר מסדר 8. נניח בשלילה שקיים איבר σ לעיל. נפרק למכפלת מחזורים זרים לא טריוויאליים $\sigma = \prod_{i=1}^{n} \tau_i$ ונסמן $o(\tau_i) = a_i$. אזי $\operatorname{lcm}(a_1, \ldots, a_n) = 8$. נקבל שלכל i מתקיים $a_i \mid 8$ ולכן a_i חזקת 2. הכפולה המשותפת המינימלית של חזקות 2 היא החזקה המקסימלית בקבוצה ולכן קיים i כך ש-τ_i מחזור באורך 8. בלי הגבלת הכלליות $i = 1$ וגם $\tau_1 = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$. כעת 9 בהכרח נשלח לעצמו וקיבלנו כי $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$. אך σ מחזור באורך זוגי ולכן תמורה אי זוגית, סתירה.

ה. נוכיח שקיים איבר מסדר 10. נבחר $\sigma = (1\ 2\ 3\ 4\ 5)(6\ 7)(8\ 9)$. אכן מתקיים

$$\operatorname{sign}(\sigma) = (-1)^{5-1}(-1)(-1) = 1$$
$$o(\sigma) = \operatorname{lcm}(5,2,2) = 10$$

ו. נוכיח שקיים איבר מסדר 12. נבחר $\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)$. אכן מתקיים

$$\operatorname{sign}(\sigma) = (-1)^{4-1}(-1)^{3-1}(-1)^{2-1} = 1^{3+2+1} = 1$$
$$o(\sigma) = \operatorname{lcm}(4,3,2) = 12$$

ז. נוכיח שלא קיים איבר מסדר 14. נניח בשלילה שקיים איבר σ לעיל. נפרק למכפלת מחזורים זרים לא טריוויאליים $\sigma = \prod_{i=1}^{n} \tau_i$ ונסמן $o(\tau_i) = a_i$. אזי $\operatorname{lcm}(a_1, \ldots, a_n) = 14$. מכיוון ש-7 ראשוני ומחלק את 14 נובע שקיים i כך ש-$a_i \mid 7$. בלי הגבלת הכלליות $a_1 \mid 7$. מתקיים כי $a_1 \leq 9$ ולכן $a_1 = 7$. מכאן ניתן להניח בלי הגבלת הכלליות כי $\tau_1 = (1\ 2\ 3\ 4\ 5\ 6\ 7)$. כעת יש רק שתי אפשרויות ל-σ: $(7\ 6\ 5\ 4\ 3\ 2\ 1)$ או $(7\ 6\ 5\ 4\ 3\ 2\ 1)(8\ 9)$. אם $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ אז $o(\sigma) = 7$ ולכן σ לא מקיים את הדרישות. אם $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)(8\ 9)$ אז $\operatorname{sign}(\sigma) = (-1)^{7-1}(-1) = -1$ ולכן $\sigma \notin A_9$, סתירה.

שאלה 7. נתונים שלמים חיוביים a, b, c כך ש-$a \mid c$, $b \mid c$ וגם $(a, b) = 1$. הוכיחו כי $ab \mid c$.

פתרון. לפי הנתון קיים שלם חיובי k כך ש-$c = ak$. לכן $b \mid ak$. קיבלנו כי $(a, b) = 1$ וגם $b \mid ak$. מכאן לפי טענה מהתרגול, $b \mid k$. לבסוף $ab \mid ak = c$.

שאלה 8 (תכנות)**.** פתרו את בעיה 5 מפרוייקט אוילר: המספר 2520 הוא המספר הקטן ביותר שהחלוקה שלו בכל אחד מן המספרים מ-1 עד ל-10 היא ללא שארית.
מה הוא המספר החיובי הקטן ביותר שמתחלק ללא שארית בכל המספרים מ-1 עד ל-20?
הסבירו אם השיטה שלכם תעבוד בזמן סביר (פחות מדקה) גם למספרים מ-1 עד ל-100.

פתרון. למעשה מבקשים לחשב את הכמ"מ של $\{1,\ldots,20\}$. ניתן לכתוב פונקציה המחשבת כמ"מ של קבוצת מספרים, ולקבל את התשובה $\operatorname{lcm}(1,\ldots,20)=232792560$.
אגב, זהו גם המעריך של S_{20}. כלומר לכל $\sigma\in S_{20}$ מתקיים כי $\sigma^{232792560}=\mathrm{id}$, וזהו המספר הקטן ביותר עם התכונה הזאת. כמובן שמספר זה הרבה יותר קטן מאשר $20!$.
חישוב כמ"מ של שני מספרים יכול להעשות ביעילות בעזרת אלגוריתם אוקלידס לחישוב הממ"מ ושימוש בנוסחה $\gcd(a,b)\operatorname{lcm}(a,b)=|ab|$. לחישוב כמ"מ של קבוצת מספרים נעזרים באינדוקציה

$$\operatorname{lcm}(a_1,\ldots,a_n)=\operatorname{lcm}(\operatorname{lcm}(a_1,\ldots,a_{n-1}),a_n)$$

דרך אחרת היא לפרק כל מספר לראשוניים, ואז למצוא את החזקה המרבית של כל ראשוני שמופיע בפירוקים השונים. מפני שהמספרים עד 100 הם די קטנים ויש רק 25 ראשוניים עד 100, זה יכול להיות להעשות מהר.
גישה נאיבית שמנסה לרוץ על המספרים הטבעיים ולבדוק עבור כל n האם הוא מחלק את המספרים מ-1 עד 100 ואם הוא לא להמשיך עם $n+1$ לא תצליח לסיים לרוץ על המחשב שלכם עד הרבה אחרי סוף הסמסטר.

שאלה 9 (רשות, חבורת התמורות בטלוויזיה)**.** צפו בפרק 10 בעונה 6 של הסדרה פיוצ'רמה.

א. רשמו את עשרים החילופים המתבצעים בפרק, ובדקו שמכפלתם היא אכן מכפלת הזהות. הדרכה: היו עקביים, ורשמו בכל מקרה את הגופים המחליפים זהויות או את הזהויות המחליפות גופים.

ב. נאמר שסדרת חילופים היא נאותה אם אף חילוף אינו מופיע בה יותר מפעם אחת. בפרק, פרופסור פארנסוורת' מצהיר שכל סדרה נאותה של חילופים על n עצמים אפשר להמשיך לסדרה נאותה על n העצמים ועוד שניים, כך שמכפלת כל החילופים היא הזהות. תנו דוגמה נגדית למשפט זה, אם מסתפקים ב-n העצמים ועוד אחד.

ג. נסו להוכיח את המשפט.
רמזים וספויילרים בסרטון הזה מאת Mathologer וברשומה הזאת בבלוג המומלץ "לא מדויק" של גדי אלכסנדרוביץ'.

בהצלחה!