

פתרון תרגיל בית 6 במבנים אלגבריים 89-214 סמסטר א' תשפ"ג

שאלה 1 (חימום). תארו את כל המחלקות השמאליות ב- $\mathbb{Z}_{60}/\langle 3 \rangle$. פתרו. האיבר 3 הוא מסדר 20, ולכן $|\langle 3 \rangle| = 20$. לפי משפט לגראנז' נקבל

$$|\mathbb{Z}_{60}/\langle 3 \rangle| = \frac{|\mathbb{Z}_{60}|}{|\langle 3 \rangle|} = \frac{60}{20} = 3$$

והמחלקות, עד כדי בחירת נציגים, הן $\{\langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$.

שאלה 2. תהי G חבורה מסדר n ויהי $\Phi: G \rightarrow S_n$ שיכון קיילי. הוכיחו שאיבר $g \in G$ הוא מסדר m אם ורק אם $\Phi(g)$ הוא מכפלה של $\frac{n}{m}$ מחזורים זרים מאורך m . פתרו. נניח כי g הוא מסדר m . לכן $g^m = e_G$ וגם $g^i \neq e_G$ לכל $0 < i < m$. שיכון קיילי מוגדר לפי $\Phi(g) = l_g$ כאשר l_g הוא הפונקציה של כפל משמאל ב- g . כדי להבין את מבנה המחזורים של $l_g \in S_n$ צריך להבין לאן l_g שולחת כל איבר של G . נראה הרכבה חוזרת שלו על איבר $x \in G$ מסוים:

$$x \xrightarrow{l_g} gx \xrightarrow{l_g} g^2x \xrightarrow{l_g} g^3x \xrightarrow{l_g} \dots \xrightarrow{l_g} g^{m-1}x \xrightarrow{l_g} g^m x = x$$

לכן $x \in G$ שייך למחזור מאורך m בדיוק. הרי אם $g^i x = g^j x$, אז $g^{i-j} = e$ ולכן $m | i - j$. כך אפשר להמשיך באינדוקציה על איבר מ- G שאינו במחזור לעיל (כלומר לא אף $g^i x$ עבור האיבר x שבחרנו). לבסוף נקבל שישנם בדיוק $\frac{n}{m}$ מחזורים, וכל אחד מהם מאורך m . אפשר לבדוק כי האיברים בכל מחזור הם המחלקות הימניות של תת-החבורה $\langle g \rangle$. בכיוון השני, זה בסך הכל לחשב סדר של תמורה. הסדר של $\Phi(g)$ הוא כמ"מ אורכי המחזורים בהצגה של התמורה כמכפלת מחזורים זרים, ואצלנו זה $\text{lcm}(m, \dots, m) = m$, לפי הנתון. מפני ש- Φ הוא שיכון, אז גם הסדר של g הוא m .

שאלה 3. מצאו את האינדקסים הבאים.

א. $[5\mathbb{Z} : 20\mathbb{Z}]$

ב. $[\mathbb{Z}_{60} \times \mathbb{Z}_{60} : \langle (3, 3) \rangle]$ רמז: משפט לגראנז' הוא שימושי.

ג. $[\mathbb{Z} \times \mathbb{Z} : \langle (3, 3) \rangle]$ רמז: קודם תארו את המחלקות השמאליות.

ד. $[S_4 \times S_3 \times \mathbb{Z}_{12} : \langle (1432) \rangle \times A_3 \times \langle 9 \rangle]$ רמז: משפט לגראנז' הוא שימושי.

פתרו.

א. נמצא את המחלקות השמאליות באופן מפורש:

$$5\mathbb{Z}/20\mathbb{Z} = \{20\mathbb{Z}, 5 + 20\mathbb{Z}, 10 + 20\mathbb{Z}, 15 + 20\mathbb{Z}\}$$

לכן האינדקס המבוקש הוא 4.

ב. הסדר של החבורה $\mathbb{Z}_{60} \times \mathbb{Z}_{60}$ הוא $60 \cdot 60 = 3600$, והסדר של תת-החבורה $\langle (3, 3) \rangle$ הוא כסדר של האיבר $(3, 3)$, שהוא 20. נחשב בעזרת משפט לגראנז' ונקבל

$$[\mathbb{Z}_{60} \times \mathbb{Z}_{60} : \langle (3, 3) \rangle] = |\mathbb{Z}_{60} \times \mathbb{Z}_{60}| / |\langle (3, 3) \rangle| = 3600/20 = 180$$

ג. נוכיח כי $[\mathbb{Z} \times \mathbb{Z} : \langle (3, 3) \rangle] = \infty$ לפי זה שנראה ש- $\{(0, n) + \langle (3, 3) \rangle\}$ היא קבוצה אינסופית של מחלקות שמאליות שונות (אלו לא כל המחלקות). אם $(0, n) + \langle (3, 3) \rangle = (0, m) + \langle (3, 3) \rangle$ אז אומר

$$-(0, m) + (0, n) \in \langle (3, 3) \rangle$$

כלומר ש- $(0, n - m) = (3k, 3k)$ לכן $0 = 3k$ גורר כי $0 = n - m$, ולכן $n = m$. כלומר יש אינסוף מחלקות שמאליות שונות.

ד. נחשב את הסדר של החבורה ושל תת-החבורה. נזכר כי

$$|S_4| = 4! = 24 \quad |S_3| = 3! = 6 \quad |\mathbb{Z}_{12}| = 12$$

ראינו כי הסדר של חבורה ציקלית הוא סדר היוצר, ולכן $|\langle (1432) \rangle| = 4$ בחבורה S_4 , וגם $|\langle 9 \rangle| = 4$ בחבורה \mathbb{Z}_{12} . בנוסף $|A_3| = 3!/2 = 3$. לכן

$$|S_4 \times S_3 \times \mathbb{Z}_{12}| = 24 \cdot 6 \cdot 12 \\ |\langle (1432) \rangle \times A_3 \times \langle 9 \rangle| = 4 \cdot 3 \cdot 4$$

והאינדקס לפי משפט לגראנז' שווה למנת הסדרים $(24 \cdot 6 \cdot 12)/(4 \cdot 3 \cdot 3) = 36$.

שאלה 4. נסמן שני איברים של החבורה $GL_2(\mathbb{Q})$:

$$M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

ונסמן ב- H את תת-החבורה הקטנה ביותר של $GL_2(\mathbb{Q})$ שמכילה את M, N .

א. ידוע כי הסדר של H הוא 8. מצאו את כל איברי H .

ב. מצאו שיכון מפורש של H ל- S_8 . כלומר חשבו והוכיחו לאן עובר כל איבר בשיכון שמצאתם. (הערה: יש שיכון של H אפילו לתוך S_4 , אבל לא חייבים למצוא אותו).

פתרון.

א. נחשב את כל האיברים המתקבלים מ- M, N על ידי מכפלות שלהם (כולל חזקות) בכל סדר, ונקבל:

$$H = \{M, M^2 = -I, M^3 = -M, M^4 = N^2 = I, \\ N, MN = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -NM, M^2N = -N, M^3N = -MN\}$$

לפי הנתון על הסדר של H אלה כל איבריה (מוזמנים לבדוק שזו אכן תת-חבורה ואין עוד. ברור כי יש ארבע חזקות של M , אז הסדר H מתחלק ב-4. בתוספת N יש לפחות חמישה איברים ב- H , ולכן הסדר של H הוא לפחות 8).

ב. נסמן:

$$\begin{array}{cccc} I \leftrightarrow 1 & -I \leftrightarrow 2 & M \leftrightarrow 3 & -M \leftrightarrow 4 \\ N \leftrightarrow 5 & -N \leftrightarrow 6 & MN \leftrightarrow 7 & -MN \leftrightarrow 8 \end{array}$$

בעזרת השוויונות שלעיל נוכל לחשב בקלות (בלי לבצע אף כפל מטריצות נוסף) לאן נשלח כל איבר תחת שיכון קיילי (כזכור הוא נשלח לתמורה המתאימה לכפל משמאל באותו איבר):

$$\begin{aligned} \varphi(1) &= \text{id} \\ \varphi(2) &= (12)(34)(56)(78) \\ \varphi(3) &= (1324)(5768) \\ \varphi(4) &= (1423)(5867) \\ \varphi(5) &= (15)(26)(38)(47) \\ \varphi(6) &= (16)(25)(37)(48) \\ \varphi(7) &= (17)(28)(35)(46) \\ \varphi(8) &= (18)(27)(36)(45) \end{aligned}$$

דרך נוספת לחסוך הכפלות מטריצות היא להיעזר בכך ששיכון קיילי הוא הומומורפיזם ולכן תמונה של מכפלה נשלחת על ידו למכפלת התמונות, כלומר להרכבת התמורות המתאימות.

שאלה 5. רמז: הביטו במחלקות.

א. תהי G חבורה מסדר 600, ותהי $H \leq G$ תת-חבורה מסדר 300. הוכיחו כי לכל $a \in G$ מתקיים כי $a^2 \in H$.

ב. נתבונן בחבורה $G = S_3 \times \mathbb{Z}_{100}$ שהיא מסדר 600. מצאו תת-חבורה $H \leq G$ מסדר 200 ואיבר $a \in G$ עבורו לא מתקיים $a^3 \in H$.

פתרון.

א. לפי משפט לגראנז' נקבל כי $[G : H] = \frac{600}{300} = 2$. כלומר יש שתי מחלקות שמאליות של H -ב- G . אחת מהן היא H , והשנייה חייבת לכלול את כל האיברים שאינם ב- H . לכן עבור $a \in G$ יש שתי אפשרויות. האפשרות הראשונה היא $a \in H$, ואז לפי סגירות הפעולה ב- H (שהיא חבורה בפני עצמה) נקבל $a^2 \in H$.

האפשרות השנייה היא $a \notin H$. כלומר $aH \neq H$. נניח בשלילה כי $a^2 \notin H$, ולכן $a^2H \neq H$. מפני שיש רק שתי מחלקות של H -ב- G , בהכרח נקבל כי $a^2H = aH$. אבל לפי תכונה של יחס השקילות שמגדיר את המחלקות השמאליות של H נקבל כי $a^{-1} \cdot a^2 \in H$. כלומר $a \in H$, וזו סתירה לנתון. לכן $a^2 \in H$. (תזכורת: מתקיים $xH = yH$ אם ורק אם $y^{-1}x \in H$ לכל $x, y \in G$. אנחנו הצבנו $y = a$ ו- $x = a^2$.)

ב. בהמשך הקורס נראה שחייבים לבחור תת-חבורה לא נורמלית מסדר 200 (יש שלוש אפשרויות לחבורה הנתונה). אפשר לבחור לדוגמה את

$$H = \langle (12) \rangle \times \mathbb{Z}_{100}$$

שהיא מסדר 200 כי $|\langle (12) \rangle| = 2$. נבחר את האיבר $a = ((23), 89)$. אז

$$a^3 = ((23)^3, 3 \cdot 89) = ((23), 67) \notin H$$

שהרי $\langle (12) \rangle = \{\text{id}, (12)\}$.

שאלה 6. הוכיחו כי לכל $a, n, m \in \mathbb{Z}$, $0 \neq a$, מתקיים $(an, am) = |a|(n, m)$.
פתרון. נסמן $d = (n, m)$, בשורה אחת, שאינה הוכחה מלאה,

$$(an, am) = |a| \cdot d \Leftrightarrow \left(\frac{an}{d}, \frac{am}{d}\right) = |a| \Leftrightarrow |a| \left(\frac{n}{d}, \frac{m}{d}\right) = |a| \Leftrightarrow \left(\frac{n}{d}, \frac{m}{d}\right) = 1 \Leftrightarrow (n, m) = d$$

דרך אחרת, דו־כיוונית (ומפורטת יותר): מצד אחד, ישנם מספרים u, v כך שמתקיים $(an, am) = uan + vam$. ידוע כי d מחלק כל צירוף לינארי של n ו- m , ובפרט את $uan + vam$. לכן $|a| \cdot d$ מחלק את $uan + vam$, ולכן $(|a| \cdot d) | (an, am)$. מצד שני, ישנם מספרים s, t כך שמתקיים $d = sn + tm$. נכפיל ב- $|a|$ ונקבל $|a|d = |a|sn + |a|tm$. ידוע כי (an, am) מחלק כל צירוף לינארי של an ו- am , ובפרט את $|a|sn + |a|tm$. לכן $(an, am) | |a|d$. לסיכום קיבלנו $(an, am) = |a|d$, כדרוש. ניתן להוכיח את הטענה גם בעזרת שימוש בהצגה של ממ"מ כמכפלת חזקות ראשוניים. במקרה זה מוכיחים כי $\min(n + a, m + a) = \min(n, m) + a$, שהיא אנלוגית להוכחה $(an, am) = |a|(n, m)$.

שאלה 7. מצאו בעזרת אלגוריתם אוקלידס את ה- \gcd של המספרים הבאים:

א. $(890, 214)$

ב. $(5340, -1284)$, רמז: העזרו בשאלה הקודמת.

פתרון.

א. נשתמש באלגוריתם אוקלידס:

$$(890, 214) = [890 = 4 \cdot 214 + 34]$$

$$(214, 34) = [214 = 6 \cdot 34 + 10]$$

$$(34, 10) = [34 = 3 \cdot 10 + 4]$$

$$(10, 4) = [10 = 2 \cdot 4 + 2]$$

$$(4, 2) = [4 = 2 \cdot 2 + 0]$$

$$(2, 0) = 2$$

ולכן $(890, 214) = 2$.

ב. נשים לב כי $-1284 = -6 \cdot 214$ וכן $5340 = 6 \cdot 890$. לכן לפי השאלה הקודמת

$$(5340, -1284) = |6| \cdot (890, 214) = 6 \cdot 2 = 12$$

שאלה 8. תהי G חבורה ציקלית מסדר n ויהי $g \in G$. מצאו נוסחה עבור $o(g)$. מה התנאי לכך ש- g יוצר את כל G ?

פתרון. יהי $a \in G$ יוצר של G . קיים i כך ש- $a^i = g$. נשתמש בנוסחה לחישוב סדר של חזקה של איבר:

$$o(g) = o(a^i) = \frac{o(a)}{(o(a), i)} = \frac{n}{(n, i)}$$

האיבר g יוצר את כל G אם ורק אם n ו- i זרים, כלומר: $(n, i) = 1$ (אז ורק אז $o(g) = n = |G|$ ולכן הוא יוצר).

שאלה 9. בחרו שפת תכנות כרצונכם וכתבו פונקציה בשם xgcd המממשת את אלגוריתם אוקלידס המורחב. כלומר כתבו פונקציה המקבלת כקלט שני מספרים שלמים a, b ומחזירה שלשה של מספרים (d, s, t) כך שמתקיים $d = (a, b) = sa + tb$.

הוסיפו את התוצאות של הרצת

`xgcd(5782, 2022)` `xgcd(654321, 123456)` `xgcd(314159, -161803)`

הערה: בעוד ש- d הוא יחודי, המקדמים s, t הם לא בהכרח יחודיים. לדוגמה `xgcd(24, 44)` תוכל להחזיר את השלשה $(4, 2, -1)$ כי $4 = 2 \cdot 24 - 1 \cdot 44$ אבל גם $(4, 13, -7)$ זו תוצאה מותרת, ולכן יתכנו מימושים נכונים שונים. דוגמאות נוספות

`xgcd(-5, 0) → (5, -1, 0)` `xgcd(100, 11) → (1, 1, -9)`

פתרון. נזכר כי באלגוריתם אוקלידס הרגיל מתחילים עם זוג מספרים (a, b) כשמניחים כי $0 \leq b < a$. אם $b = 0$, אזי $(a, b) = a$. אחרת נכתוב $a = qb + r$ כאשר $0 \leq r < |b|$ ונמשיך בשלב הבא עם חישוב (b, r) . בכל שלב באלגוריתם קיבלנו כי ניתן להציג את השארית r כצירוף לינארי $r = a - qb$.

באלגוריתם אוקלידס המורחב אנו שומרים בשלב מספר i את המקדמים s_i, t_i והשארית r_i כך שמתקיים $r_i = s_i a + t_i b$, שבעזרתם נביע לבסוף את d כצירוף לינארי. נניח ובשלב קודם באלגוריתם קיבלנו כי

$$r_{\text{prev}} = s_{\text{prev}}a + t_{\text{prev}}b$$

ובשלב הנוכחי $r = sa + tb$. נרצה לדעת מי יהיו המקדמים $s_{\text{new}}, t_{\text{new}}$ לשלב הבא. נבצע חלוקה אוקלידית של השאריות מהשלב הקודם והשלב הנוכחי $r_{\text{prev}} = qr + r_{\text{new}}$. כעת נשתמש במשוואות לעיל ונקבל

$$r_{\text{new}} = r_{\text{prev}} - qr = (s_{\text{prev}}a + t_{\text{prev}}b) - q(sa + tb) = (s_{\text{prev}} - qs)a + (t_{\text{prev}} - qt)b$$

לכן

$$s_{\text{new}} = s_{\text{prev}} - qs \qquad t_{\text{new}} = t_{\text{prev}} - qt$$

האלגוריתם מתחיל בשלב שבו $r_0 = a, r_1 = b$, כלומר

$$r_0 = a = s_0a + t_0b \qquad r_1 = b = s_1a + t_1b$$

ולכן $s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$.

נציג פתרון איטרטיבי בפית'ון, ולאחריו נוסיף הערות על המימוש.

```

1 def xgcd(a, b):
2     """
3     Extended Euclidean algorithm
4
5     Returns (d, s, t) where `d` is the greatest common
6     divisor of the integers `a` and `b`, where the
7     numbers `s` and `t` are such that `d = sa+tb`.
8     """
9     prev_r, r = a, b
10    prev_s, s = 1, 0
11    prev_t, t = 0, 1
12    while r:
13        q = prev_r // r
14        prev_s, s = s, prev_s - q*s
15        prev_t, t = t, prev_t - q*t
16        prev_r, r = r, prev_r - q*r
17
```

```

18     if prev_r < 0:
19         return (-prev_r, -prev_s, -prev_t)
20     else:
21         return (prev_r, prev_s, prev_t)

```

שורות 2–8 נועדו לתיעוד הפונקציה. בשורה 9, וגם בהמשך הקוד, מופיע שימוש בהשמה מקבילית (בפיית'ון המינוח הוא tuple packing and sequence unpacking) ובו בו־זמנית מציבים ערכים בשני משתנים. הערכים באגף ימין בהשמה מקבילית מחושבים לפני ההשמה באגף שמאל.

בשורה 13 מופיע שימוש ב"חלוקת רצפה", המחזירה את המנה השלמה של שני מספרים. בשפות תכנות רבות זו החלוקה הרגילה.

הלולאה שמתחילה בשורה 12 מבטיחה רק כי $0 \leq |r|$, ולא בהכרח $0 \leq r$. האלגוריתם עדין יעצר שכן $|r_i|$ קטן. במקרה וקיבלנו $a < b$, האיטרציה הראשונה בלולאה תהפוך את הסדר שלהם (עד כדי שינוי בסימן, שאינו משפיע על הממ"מ).

הבדיקה בשורה 18 מוודאת כי הממ"מ המתקבל הוא לא שלילי. פתרון רקורסיבי לבעיה בפיית'ון:

```

1 def rxgcd(a,b):
2     "Recursive version of xgcd."
3     if b == 0:
4         if a < 0:
5             return (-a, -1, 0)
6         else:
7             return (a, 1, 0)
8     else:
9         q, r = divmod(a, b)
10        d, s, t = rxgcd(b, r)
11        return (d, t, s - q*t)

```

הפונקציה divmod בשורה 9 היא פונקציה סטנדרטית המחזירה שני מספרים q, r שהם המנה והשארית בחלוקה a/b כך שמתקיים $a = qb + r$. בשורה 10 נקבל $d = sb + tr$, ולכן בשורה 11 מחזירים לאחר הצבה

$$d = sb + tr = sb + t(a - qb) = ta + (s - qt)b$$

תוצאות אפשריות לחישובים שנתבקשו בשאלה הן

$$\begin{aligned} \text{xgcd}(5782, 2022) &= (2, -178, 509) \\ \text{xgcd}(654321, 123456) &= (3, 8819, -46741) \\ \text{xgcd}(314159, -161803) &= (1, 53352, 103589) \end{aligned}$$

בהצלחה!