פתרון תרגיל בית 8 במבנים אלגבריים
89-214 סמסטר א' תשע"ט

שאלה 1. תהי $G = GL_2(\mathbb{Z}_2)$. מצאו את תמונת כל האיברים בשיכון קיילי $\Phi: G \to S_6$.
רמז: שאלה 4 בתרגיל בית 6 ואפשר להעזר במחשב.

פתרון. לפי תרגיל הבית שברמז אנחנו יודעים מי הם האיברים ב-G. נמספר אותם כך

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad 2 \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad 3 \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad 4 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad 5 \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad 6 \leftrightarrow \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

ונמשיך לפי שיכון קיילי שראינו בכיתה,

$$\Phi \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{id} \qquad \Phi \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = (1\ 4)(2\ 3)(5\ 6)$$

$$\Phi \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (1\ 2)(3\ 5)(4\ 6) \qquad \Phi \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (1\ 5)(2\ 6)(3\ 4)$$

$$\Phi \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = (1\ 3\ 6)(2\ 4\ 5) \qquad \Phi \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = (1\ 6\ 3)(2\ 5\ 4)$$

שאלה 2. תהי G חבורה מסדר n ויהי $\Phi: G \to S_n$ שיכון קיילי. הוכיחו שאיבר $g \in G$ הוא מסדר m אם ורק אם $\Phi(g) \in S_n$ הוא מכפלה של $\frac{n}{m}$ מחזורים זרים מאורך m.

פתרון. 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:

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

לכן $x \in G$ שייך למחזור מאורך m. כך אפשר להמשיך באינדוקציה על איבר מ-G שאינו במחזור לעיל (כלומר לא $g^i x$ עבור האיבר x שבחרנו). לבסוף נקבל שישנם בדיוק $\frac{n}{m}$ מחזורים, וכל אחד מהם מאורך m.

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 $\mathrm{lcm}(m, \ldots, m) = m$, לפי הנתון. מפני ש-$\Phi$ הוא שיכון, אז גם הסדר של g הוא m.

שאלה 3. חשבו בשיטה של חישוב חזקה בעזרת ריבועים את הביטויים הבאים. מותר להשתמש במחשב (כולל בפונקציית המודולו) לחישובי הביניים, שאותם תפרטו:

א. $2790^{2753} \in \mathbb{Z}_{3233}$. רמז: בתרגול ראיתם שהתוצאה הסופית היא ההודעה שבוב רצה לשלוח לאליס.

ב. $\left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{214} \in GL_2\left(\mathbb{Z}_{1000}\right)$.

פתרון.

א. נחשב ש-$2753 = 101011000001_2$. לכן נשתמש באותו תהליך שראינו בכיתה, כשכל המשוואות הן מודולו 3233:

$$\begin{aligned}
2790^1 &= 2790\\
2790^2 &= 2269\\
2790^4 &= 1425\\
2790^5 &= 2393\\
2790^{10} &= 806\\
2790^{20} &= 3036\\
2790^{21} &= 3213\\
2790^{42} &= 400\\
2790^{43} &= 615\\
2790^{86} &= 3197\\
2790^{172} &= 1296\\
2790^{344} &= 1689\\
2790^{688} &= 1215\\
2790^{1376} &= 1977\\
2790^{2752} &= 3065\\
2790^{2753} &= 65
\end{aligned}$$

וזה פענוח ההודעה $m = 65$ שבוב שלח לאליס.

ב. נחשב ש-$214 = 11010110_2$. נסמן $A = \left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)$. כמו בסעיף הקודם, עלינו לחשב למעשה את

$$A^{214} = (A(A((A((A(A)^2)^2)^2)^2)^2)^2)^2$$

שימו לב שמכפילים ב-A אם יש סיבית דלוקה, ואז בכל מקרה מעלים בריבוע. החישוב המלא מהסוגריים הפנימיים ביותר החוצה, כשכל המשוואות הן מודולו 1000, הוא

$$\begin{aligned}
\left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^1 &= \left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right) & \left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{26} &= \left(\begin{smallmatrix}881 & 713\\ 857 & 882\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^2 &= \left(\begin{smallmatrix}73 & 81\\ 9 & 10\end{smallmatrix}\right) & \left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{52} &= \left(\begin{smallmatrix}202 & 19\\ 891 & 965\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^3 &= \left(\begin{smallmatrix}665 & 738\\ 82 & 91\end{smallmatrix}\right) & \left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{53} &= \left(\begin{smallmatrix}635 & 837\\ 93 & 984\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^6 &= \left(\begin{smallmatrix}741 & 928\\ 992 & 797\end{smallmatrix}\right) & \left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{106} &= \left(\begin{smallmatrix}66 & 103\\ 567 & 97\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{12} &= \left(\begin{smallmatrix}657 & 264\\ 696 & 785\end{smallmatrix}\right) & \left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{107} &= \left(\begin{smallmatrix}631 & 697\\ 633 & 200\end{smallmatrix}\right)\\
\left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{13} &= \left(\begin{smallmatrix}520 & 177\\ 353 & 49\end{smallmatrix}\right) & \left(\begin{smallmatrix}8 & 9\\ 1 & 1\end{smallmatrix}\right)^{214} &= \left(\begin{smallmatrix}362 & 207\\ 23 & 201\end{smallmatrix}\right)
\end{aligned}$$

שאלה 4. חשבו בעזרת משפט אוילר:

א. שתי הספרות האחרונות של 543^{3838}.

ב. $89^{214} \pmod{91}$.

פתרון.

א. יש לחשב את הביטוי מודולו 100. לאחר חישוב נקבל $\varphi(100) = 40$. לכן אם מספר שלם a זר ל-100, לפי משפט אוילר

$$a^{\varphi(100)} \equiv a^{40} \equiv 1 \pmod{100}$$

לכן מפני ש-$(43, 100) = 1$,

$$543 \equiv 43 \pmod{100}$$
$$543^{3838} \equiv 43^{40 \cdot 96 - 2} \equiv 1^{96} \cdot 43^{-2} \pmod{100}$$

ונותר לנו למצוא הופכי כפלי של 43 בחבורה U_{100}. כלומר רוצים למצוא מספר x שמקיים

$$43x \equiv 1 \pmod{100}$$

לפי אלגוריתם אוקלידס המורחב נקבל $x = 7$ (בדקו!) ולכן

$$543^{3838} \equiv 43^{-2} \equiv 7^2 \equiv 49 \pmod{100}$$

וקיבלנו ששתי הספרות האחרונות הן 49.

ב. באופן דומה לסעיף הקודם, נחשב

$$\varphi(91) = 91 \left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{13}\right) = 72$$

ושוב נוכל להשתמש במשפט אוילר כי $(89, 91) = 1$,

$$89^{214} \equiv 89^{3 \cdot 72 - 2} \equiv 89^{-2} \pmod{91}$$

בעזרת אלגוריתם אוקלידס המורחב (חשבו!) נמצא את ההופכי הכפלי של 89 בחבורה U_{91}, שהוא 45. לכן

$$89^{-2} \equiv 45^2 \equiv 23 \pmod{91}$$

שאלה 5. בשאלה הזו תראו שאלגוריתם מילר-רבין הוא דטרמיניסטי למספרים לא כל כך קטנים עבור קבוצת עדים נתונה.

א. חשבו ש-99 הוא עד חזק לראשוניות של 377 ואילו 110 לא. לעומת זאת, חשבו כי 110 הוא עד חזק לראשוניות של 289 ואילו 99 לא. ודאו חישובים אלו בסעיף הבא.

ב. בחרו שפת תכנות כרצונכם וכתבו פונקציה בשם $\texttt{millerrabin}(N, W)$ המממשת את אלגוריתם מילר-רבין למספר טבעי N ולקבוצת עדים נתונה W (בכיתה במקום W בחרנו באקראי כמה מספרים).
הראו שהעדים החזקים לראשוניות של 689 בקטע $[2, 687]$ הם רק $83, 242, 447, 606$.

ג. כתבו פונקציה נוספת $\texttt{first_mistake}(W)$ שמחזירה את המספר $N \geq 3$ האי זוגי הקטן ביותר שעבורו הפונקציה $\texttt{millerrabin}(N, W)$ טועה. כלומר התשובה של $\texttt{millerrabin}(N, W)$ שונה מהתשובה של $\texttt{is_prime}(N)$, המחזירה בודאות האם N ראשוני. רק עבור המימוש של $\texttt{is_prime}(N)$ אפשר להשתמש בספריות

חיצוניות[1].
דוגמה להרצה היא $\texttt{first_mistake}(\{2\}) = 2047$. כלומר לכל מספר אי זוגי $3 \leq N < 2047$ הקריאה $\texttt{millerrabin}(N, \{2\})$ מחזירה את התשובה הנכונה, אבל $\texttt{millerrabin}(2047, \{2\})$ מחזירה ש-2047 כנראה ראשוני, אבל הוא למעשה פריק: $2047 = 23 \cdot 89$. כתבו את התוצאות של הרצת:

- $\texttt{first_mistake}(\{3\})$
- $\texttt{first_mistake}(\{3, 5\})$
- $\texttt{first_mistake}(\{4, 5\})$
- $\texttt{first_mistake}(\{7, 11\})$
- $\texttt{first_mistake}(\{7, 11, 13\})$

פתרון.

א. בפתרון מלא יש לפרט את חישובי החזקות המודולריות.
נסמן $N = 377$ ולפי הסימונים $N - 1 = 2^s M$ מהכיתה נקבל $376 = 2^3 \cdot 47$. יהי $a = 99 \in [2, 376]$. לפי אלגוריתם מילר-רבין נסמן $x = a^M$ ונחשב בלולאה את x^{2^i} עבור $0 \leq i < s$. נתחיל עם החישוב

$$x = a^{2^0 M} = 99^{47} \equiv 278 \pmod{377}$$

והרי 278 אינו ± 1 מודולו 377. לכן נמשיך

$$x^2 = a^{2^1 M} = (99^{47})^2 \equiv 376 \equiv -1 \pmod{377}$$

ולכן 99 הוא עד חזק לראשוניות של 377. עבור $a = 110$ נחשב

$$\begin{aligned} x &= a^{2^0 M} = 110^{47} \equiv 141 \pmod{377} \\ x^2 &= a^{2^1 M} = (110^{47})^2 \equiv 277 \pmod{377} \\ x^4 &= a^{2^2 M} = ((110^{47})^2)^2 \equiv 198 \pmod{377} \end{aligned}$$

אף אחד מאלו אינו שקול ל--1 מודולו 377. לכן 110 מעיד כי 377 הוא פריק. אגב, הפירוק שלו לגורמים ראשוניים הוא $377 = 13 \cdot 29$.
נסמן $N = 289$ ולכן במקרה זה בסימונים $N - 1 = 2^s M$ נקבל $288 = 2^5 \cdot 9$. יהי $a = 110 \in [2, 376]$. כמו מקודם, לפי אלגוריתם מילר-רבין נסמן $x = a^M$ ונחשב בלולאה את x^{2^i} עבור $0 \leq i < s$:

$$x = a^{2^0 M} = 110^9 \equiv 110 \pmod{289}$$

והרי 110 אינו ± 1 מודולו 289. לכן נמשיך

$$\begin{aligned} x^2 &= a^{2^1 M} = (110^9)^2 \equiv 251 \pmod{289} \\ x^4 &= a^{2^2 M} = ((110^9)^2)^2 \equiv 288 \equiv -1 \pmod{289} \end{aligned}$$

[1] כמובן שאפשר לממש בעצמכם. אפשרות טובה לשאלה הנוכחית היא ארטוסתנס של הנפה עם מטמון (Cache). לחלק הזה אפשר להשתמש במערכת תוכנה מתמטית.

ולכן 110 הוא עד חזק לראשוניות של 289. עבור $a = 99$ נחשב

$$x = a^{2^0 M} = 99^9 \equiv 207 \pmod{289}$$
$$x^2 = a^{2^1 M} = (99^9)^2 \equiv 77 \pmod{289}$$
$$x^4 = a^{2^2 M} = ((99^9)^2)^2 \equiv 149 \pmod{289}$$
$$x^8 = a^{2^3 M} = (((99^9)^2)^2)^2 \equiv 237 \pmod{289}$$
$$x^{16} = a^{2^4 M} = ((((99^9)^2)^2)^2)^2 \equiv 103 \pmod{289}$$

אף אחד מאלו אינו שקול ל--1 מודולו 289. לכן 99 מעיד כי 289 הוא פריק. אגב, הפירוק שלו לגורמים ראשוניים הוא $289 = 17^2$.

ב. נשמח לשמוע על מימושים מקוריים.

ג. שימו לב שהשגיאה היחידה שיכולה להיות באלגוריתם מילר-רבין היא שהוא יחזיר מספר פריק בתור "כנראה ראשוני". לכן התוצאות להרצות תמיד יהיו מספרים פריקים:

- $\texttt{first_mistake}(\{3\}) = 121$
- $\texttt{first_mistake}(\{3,5\}) = 112141$
- $\texttt{first_mistake}(\{4,5\}) = 5461$
- $\texttt{first_mistake}(\{7,11\}) = 88831$
- $\texttt{first_mistake}(\{7,11,13\}) = 1152271$

שאלה 6 (רשות)**.** חשבו האם ניתן לממש את אלגוריתם RSA באמצעות חבורה לא אבלית (כמו S_n)? מה משתבש?

שאלה 7 (רשות)**.** הראו שכאשר $n = pq$ והראשוניים p, q "קרובים יחסית", אפשר לתקוף די בקלות את RSA.

שימו לב שמתקיים: $n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$, ואז $\frac{p+q}{2}$ יחסית קרוב למספר $\sqrt{n}$. סמנו: $t = \frac{p+q}{2}, s = \frac{p-q}{2}$ והסבירו למה במצב כזה יחסית קל למצוא את t, s (ובאמצעותם את p, q) בהינתן n.

הדגימו זאת על $n = 23360947609$.

בהצלחה!