

תרגיל 6 במבנים אלגבריים

89-214 סמסטר א' תשע"ח

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול.

שאלה 1. חשבו בעזרת משפט אוילר:

א. את הספרה האחרונה של המספר 63^{63} .

ב. שתי הספרות האחרונות של 543^{3838} .

ג. $89^{214} \pmod{91}$.

פתרון:

$$\text{א. } 63^{63} = (6 \cdot 10 + 3)^{63} = 3^{63} \pmod{10}$$

$$\text{נשים לב כי } 3^4 \pmod{10} = 1 \text{ ולכן } 3^{63} \pmod{10} = 3^3 \pmod{10} = 27 \pmod{10} = 7$$

ב.

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 $x = 7$ (חשבו!), ולכן

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

וקיבלנו ששתי הספרות האחרונות הן 49.

ג.

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 (חשבוי!) נמצא את ההופכי הכפלי של 89 בחבורה U_{91} , שהוא 45. לכן

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

שאלה 2. יהיה p ראשוני. כמה איברים הפיכים יש במונואיד הכפלי \mathbb{Z}_p ? כמה איברים הפיכים יש במונואיד הכפלי \mathbb{Z}_{p^2} ?

עבור \mathbb{Z}_p : מתוך האיברים $0, 1, \dots, p-1$, כולם חוץ מ-0 זרים לק כי הוא ראשוני. ולכן יש $p-1$ איברים הפיכים.

עבור \mathbb{Z}_{p^2} : מכיוון שק ראשוני, מספר יהיה זר ל p^2 אם ורק אם אין לו גורם ראשוני p , כלומר אם ורק אם הוא זר ל p .

מתוך המספרים $0, 1, \dots, p^2$ נחשוב כמה מהם לא זרים לק: אלו המספרים שיש גורם p , זאת אומרת $\{0, p, 2p, \dots, (p-1)p\}$. כלומר יש p מספרים כאלו.

ולכן מספר האיברים שהפיכים (שכן זרים) הוא $p^2 - p$.

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

א. $2790^{2753} \in \mathbb{Z}_{3233}$ בתרגול ראייתם שהתוצאה הסופית היא ההודעה שבו רצה לשלוח לאליס.

ב. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{12} \in GL_2(\mathbb{Z}_{10000})$

פתרון:
א.

נחשב ש- $101011000001_2 = 2753$. לכן נשתמש באותו תהליך שראינו בכיתה,

כשכל המשוואות הן מודולו 3233:

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

ב. נסמן $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. נחשב ש- $1100_2 = 12$, ולכן עלינו לחשב למעשה את

$$A^{12} = \left((A^2)^2 \cdot \left((A^2)^2 \right)^2 \right)^2$$

ובחישוב מלא, כשכל המשוואות הן מודולו 10000:

$$\begin{aligned} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^1 &= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^2 &= \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^4 &= \begin{pmatrix} 199 & 290 \\ 435 & 634 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^8 &= \begin{pmatrix} 5751 & 1570 \\ 2355 & 8106 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{12} &= \begin{pmatrix} 7339 & 3170 \\ 4755 & 2154 \end{pmatrix} \end{aligned}$$

שאלה 4. בוב מעוניין לשלוח לאליס הודעה באופן מוצפן. ולכן, אליס בוחרת שני מספרים ראשוניים, $p=13$ $q=23$. בנוסף, אליס בוחרת את המספר $e=35$.

א. הראה ש- e הנייל אכן בחירה תקינה.

ב. חשב את d המקיים $de \equiv 1 \pmod{\varphi(n)}$ כאשר $n = p * q$

ג. אליס שולחת לבוב את m ואת e וכעת הוא יכול להצפין. בוב מעוניין להצפין את ההודעה $m=15$. נשים לב כי ההודעה m אכן עומדת בקרטיונים. חשבו את ההודעה אותה בוב יעביר לאליס.
ד. הראו כי אליס אכן יכולה לפענח את ההודעה.

4.א. נראה ש $\gcd(\varphi(n), e) = 1$ $n=p*q$.

$\varphi(n) = (p-1)*(q-1)=264$ ולכן q, p ראשוניים

נראה בעזרת אלגוריתם אוקלידס:

$$\gcd(264,35)=[264=7*35+19]$$

$$\gcd(35,19)=[35=19*1+16]$$

$$\gcd(19,16)=[19=1*16+3]$$

$$\gcd(16,3)=[16=5*3+1]$$

$$\gcd(3,1)=1$$

$$\Rightarrow \gcd(264,35)=1$$

ב. נרצה למצוא את ההופכי של e מודולו $\varphi(n)$. ניעזר בפירוק שך סעיף א':

$$1=16-5*3$$

$$1=16-5(19-16*1)=6*16-5*19$$

$$1=6*(35-19*1)-5*19=6*35-11*19$$

$$1=6*35-11(264-7*35)=83*35-11*264$$

ולכן $d=83$

ג. בוב ירצה לשלוח את $c=m^e \pmod{n}$

$$C=15^{35} \pmod{299}$$

נעלה כאן בחזקה.

$$.c=189 \pmod{299}$$

ד. נרצה לפענח את ההודעה. נחשב:

$$c=189$$

$$d=83$$

$$n=299$$

$$m=c^d \pmod{n} = 189^{83} \pmod{299}$$

נעלה את החזקות ונקבל $15 \pmod{299}$ ולכן אליס הצליחה לפענח את ההודעה.