

פתרון תרגיל בית 7 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. בדקו האם a הוא עד לראשוניות של N , לפי אלגוריתם מילר-רבין. הציגו את החישוב לכל a , גם אם אתם כבר יודעים שהמספר אינו ראשוני. **הציגו כל שלב בחישוב באמצעות חזקה מודולרית!**

רשמו בכל סעיף האם N אכן ראשוני.

1. $N = 233$. בדקו עבור $a = 10, a = 53, a = 191$.

2. $N = 437$. בדקו עבור $a = 101, a = 102, a = 103$.

פתרון. ב. ראשית, נציג את $N - 1$ כנדרש:

$$N - 1 = 232 = 2^3 \cdot 29$$

כעת, אנו צריכים לחשב את $a^{2^9}, a^{2 \cdot 2^9}$ ועל זו הדרך. עבור $a = 53$, נקבל:

$$\begin{aligned} 53^2 &\equiv 13 \pmod{233} \\ 53^4 &\equiv (13)^2 \pmod{233} \equiv 169 \pmod{233} \\ 53^8 &\equiv (169)^2 \pmod{233} \equiv 135 \pmod{233} \\ 53^{16} &\equiv (135)^2 \pmod{233} \equiv 51 \pmod{233} \\ 53^{29} &\equiv 53^{16} \cdot 53^8 \cdot 53^4 \cdot 53 \equiv 136 \pmod{233} \end{aligned}$$

נמשיך ונחשב את החזקות:

$$53^{2 \cdot 2^9} \equiv (136)^2 \pmod{233} \equiv 89 \pmod{233}$$

מכאן אי-אפשר לקבוע מה ומי. נמשיך:

$$53^{2^2 \cdot 2^9} \equiv (89)^2 \pmod{233} \equiv 232 \pmod{233}$$

$232 \equiv -1 \pmod{233}$, ולכן אפשר לעצור; $a = 53$ הוא עד חזק לראשוניות של 233.

עבור $a = 10$, נקבל:

$$\begin{aligned} 10^2 &\equiv 100 \pmod{233} \\ 10^4 &\equiv 214 \pmod{233} \\ 10^8 &\equiv (214)^2 \pmod{233} \equiv 128 \pmod{233} \\ 10^{16} &\equiv (128)^2 \pmod{233} \equiv 74 \pmod{233} \\ 10^{29} &\equiv 10^{16} \cdot 10^8 \cdot 10^4 \cdot 10 \equiv 12 \pmod{233} \end{aligned}$$

נמשיך ונחשב את החזקות:

$$10^{2 \cdot 29} \equiv (12)^2 \pmod{233} \equiv 144 \pmod{233}$$

מכאן אי-אפשר לקבוע מה ומי. נמשיך:

$$10^{2^2 \cdot 29} \equiv (144)^2 \pmod{233} \equiv 232 \pmod{233}$$

$232 \equiv -1 \pmod{233}$, ולכן אפשר לעצור; $a = 53$ הוא עד חזק לראשוניות של 233.

עבור $a = 191$, נקבל:

$$\begin{aligned} 191^2 &\equiv 133 \pmod{233} \\ 191^4 &\equiv (133)^2 \pmod{233} \equiv 214 \pmod{233} \\ 191^8 &\equiv (214)^2 \pmod{233} \equiv 128 \pmod{233} \\ 191^{16} &\equiv (128)^2 \pmod{233} \equiv 74 \pmod{233} \\ 191^{29} &\equiv 191^{16} \cdot 191^8 \cdot 191^4 \cdot 191 \equiv 136 \pmod{233} \end{aligned}$$

בדומה ל- $a = 53$, נקבל שגם $a = 191$ הוא עד לראשוניות של 233. 233 הוא אכן מספר ראשוני.

ב. ראשית, נציג את $N - 1$ כדרוש:

$$N - 1 = 436 = 2^2 \cdot 109$$

עבור $a = 101$, נקבל:

$$\begin{aligned} 101^2 &\equiv 150 \pmod{437} \\ 101^4 &\equiv (150)^2 \pmod{437} \equiv 213 \pmod{437} \\ 101^8 &\equiv (213)^2 \pmod{437} \equiv 358 \pmod{437} \\ 101^{16} &\equiv (358)^2 \pmod{437} \equiv 123 \pmod{437} \\ 101^{32} &\equiv (123)^2 \pmod{437} \equiv 171 \pmod{437} \\ 101^{64} &\equiv (171)^2 \pmod{437} \equiv 399 \pmod{437} \\ 101^{109} &\equiv 101^{64} \cdot 101^{32} \cdot 101^8 \cdot 101^4 \cdot 101 \equiv 247 \pmod{437} \end{aligned}$$

נמשיך ונחשב את החזקות:

$$101^{2 \cdot 109} \equiv (247)^2 \pmod{437} \equiv 266 \pmod{437}$$

$266 \not\equiv \pm 1 \pmod{437}$, ולכן $a = 101$ מעיד ש-437 אינו ראשוני. עבור $a = 102$, נקבל:

$$\begin{aligned} 102^2 &\equiv 353 \pmod{437} \\ 102^4 &\equiv (353)^2 \pmod{437} \equiv 64 \pmod{437} \\ 102^8 &\equiv (64)^2 \pmod{437} \equiv 163 \pmod{437} \\ 102^{16} &\equiv (163)^2 \pmod{437} \equiv 349 \pmod{437} \\ 102^{32} &\equiv (349)^2 \pmod{437} \equiv 315 \pmod{437} \\ 102^{64} &\equiv (315)^2 \pmod{437} \equiv 26 \pmod{437} \\ 102^{109} &\equiv 102^{64} \cdot 102^{32} \cdot 102^8 \cdot 102^4 \cdot 102 \equiv 7 \pmod{437} \end{aligned}$$

נמשיך ונחשב את החזקות:

$$101^{2 \cdot 109} \equiv (7)^2 \pmod{437} \equiv 49 \pmod{437}$$

$a = 102$ ולכן $a \equiv \pm 1 \pmod{437}$, ולכן $a \not\equiv \pm 1 \pmod{437}$.
עבור $a = 103$, נקבל:

$$\begin{aligned} 103^2 &\equiv 121 \pmod{437} \\ 103^4 &\equiv (121)^2 \pmod{437} \equiv 220 \pmod{437} \\ 103^8 &\equiv (220)^2 \pmod{437} \equiv 330 \pmod{437} \\ 103^{16} &\equiv (330)^2 \pmod{437} \equiv 87 \pmod{437} \\ 103^{32} &\equiv (87)^2 \pmod{437} \equiv 140 \pmod{437} \\ 103^{64} &\equiv (140)^2 \pmod{437} \equiv 372 \pmod{437} \\ 103^{109} &\equiv 103^{64} \cdot 103^{32} \cdot 103^8 \cdot 103^4 \cdot 103 \equiv 274 \pmod{437} \end{aligned}$$

נמשיך ונחשב את החזקות:

$$101^{2 \cdot 109} \equiv (274)^2 \pmod{437} \equiv 349 \pmod{437}$$

$a = 103$ ולכן $a \equiv \pm 1 \pmod{437}$, ולכן $a \not\equiv \pm 1 \pmod{437}$.

שאלה 2. אליס ובוב רוצים לתאם ביניהם מפתח סודי בפרוטוקול דיפי-הלמן, בחבורה U_{37} , $g = 17$. לאליס ידוע המספר $a = 8$, לבוב ידוע המספר $b = 10$. כתבו מה המפתח אותו הם מקבלים. מצאו את המפתח גם עבור אליס וגם עבור בוב. **הציגו כל שלב בחישוב באמצעות חזקה מודולרית!**

פתרון. א. אם כן, אליס מחשבת:

$$\begin{aligned} 17^2 \pmod{37} &\equiv 30 \pmod{37} \\ 17^4 &\equiv (30)^2 \pmod{37} \equiv 12 \pmod{37} \\ 17^8 &\equiv 12^2 \pmod{37} \equiv 33 \pmod{37} \end{aligned}$$

ובוב יחשב:

$$\begin{aligned} 17^2 \pmod{37} &\equiv 30 \pmod{37} \\ 17^4 &\equiv (30)^2 \pmod{37} \equiv 12 \pmod{37} \\ 17^8 &\equiv 12^2 \pmod{37} \equiv 33 \pmod{37} \end{aligned}$$

ובנוסף:

$$17^{10} \equiv 17^8 \cdot 17^2 \equiv 30 \cdot 33 \pmod{37} \equiv 28 \pmod{37}$$

כעת, אליס תשלח לבוב את 33, ובוב ישלח לאליס את 28.
בשלב השני, אליס תחשב:

$$\begin{aligned} 28^2 \pmod{37} &\equiv 7 \pmod{37} \\ 28^4 &\equiv (7)^2 \pmod{37} \equiv 12 \pmod{37} \\ 28^8 &\equiv 12^2 \pmod{37} \equiv 33 \pmod{37} \end{aligned}$$

ובאופן דומה בוב יקבל את המפתח, 33.

שאלות רשות

השאלות לא נבדקות, ולא יינתן עליהן ציון.

שאלה 3. חשבו האם ניתן לממש את אלגוריתם RSA באמצעות חבורה לא אבלית (כמו S_n , למשל)? מה משתבש?

שאלה 4. 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 $n = 23360947609$.