תרגיל בית 8 במבנים אלגבריים
89-214 סמסטר א' תש"ף

שאלה 1 (חימום). נניח והגרלנו ראשוני מאוד גדול p. מה הבעיה בבחירה $n = p^2$ למפתח הציבורי באלגוריתם RSA?

שאלה 2. בעזרת שיטת צעדי גמד וצעדי ענק שראינו בכיתה מצאו את הפתרון למשוואה $71 \equiv 7^x \pmod{101}$ ופתרון למשוואה $72 \equiv 7^y \pmod{101}$.
קצת יותר קשה: משני הפתרונות האלו מצאו פתרון למשוואה $71 \equiv 72^z \pmod{101}$, וכנראה בדרך תצטרכו את החבורה $U_{\varphi(101)}$. הפתרונות צריכים לקיים $0 \le x, y, z < 101$.

שאלה 3. ממשו בעצמכם פונקציה בשם $\texttt{superpower}(x, k, n)$ המקבלת מספרים טבעיים x, k, n ומחשבת את $x^k \pmod{n}$ לפי שיטת העלאה בחזקה בעזרת ריבועים, ובכל פעם שאתם מכפילים או מעלים בריבוע הדפיסו

```
x^i = y (mod n)
```

כאשר במקום x, i, y, n מופיעים המספרים המתאימים. למשל x ו-n הם הפרמטרים לפונקציה וזהים בכל השורות, ואילו רק בשורה האחרונה i הוא k. מספר השורות לא אמור לעלות על $2\log_2 k$. דוגמה להרצה של $\texttt{superpower}(89, 11, 101)$:

```
89^1 = 89 (mod 101)
89^2 = 43 (mod 101)
89^4 = 31 (mod 101)
89^5 = 32 (mod 101)
89^10 = 14 (mod 101)
89^11 = 34 (mod 101)
```

הוסיפו את הרצת $\texttt{superpower}(a + b + 9, 3000 + 10 \cdot a + b, 89214)$ כקובץ טקסט, כאשר a, b הן שתי הספרות האחרונות בת"ז שלכם. זכרו לצרף את קובץ קוד המקור שלכם.

שאלה 4. המחשבים של אליס ובוב לא טובים בהגרלת ראשוניים, והם עדיין רצו לשלוח הודעות מוצפנות עם RSA. אליס הגרילה את $n = pq$ ובוב הגריל את $n' = p'q'$ כאשר

$$n = 78719, \qquad n' = 73813$$

מבלי לדעת שחלק מהראשוניים p, q, p', q' שהגרילו הם לא שונים. שניהם השתמשו במעריך ההצפנה $e = 91$, וחישבו את המפתחות הפרטיים שלהם.

א. מצאו את המפתח הפרטי d של אליס ואת המפתח הפרטי d' של בוב בעזרת חישוב $\gcd(n, n')$ ומחשבון פשוט בלבד.

ב. בוב רצה לשלוח לאליס את מספר הקורס $m = 214$. הראו איך בוב יצפין את ההודעה, ואיך אליס תפענח אותה, כשמותר להעזר ב-superpower.

ג. אליס שלחה לבוב את הציון המוצפן שלה $c' = 38845$. מצאו את הציון שלה, כשמותר להעזר ב-`superpower`.

שאלה 5. בעיית הלוגריתם הבדיד ל-S_n אומרת שבהנתן תמורה $\sigma \in S_n$ ותמורה $\tau \in \langle\sigma\rangle$, יש למצוא מספר שלם x כך ש-$\tau = \sigma^x$.

א. יהיו a_1, a_2, m_1, m_2 שלמים המקיימים $a_1 \equiv a_2 \pmod{\gcd(m_1, m_2)}$. הוכיחו שלמשוואות

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

יש פתרון משותף. הדרכה אפשרית: הוכיחו כי $a_1 - a_2 = k \cdot \gcd(m_1, m_2)$ עבור k שלם כלשהו. לפי איפיון הממ"מ כצירוף לינארי, קיימים מקדמים s_1, s_2 המקיימים

$$s_1 m_1 + s_2 m_2 = \gcd(m_1, m_2)$$

שמוצאים אותם בעזרת אלגוריתם אוקלידס המורחב. הסבירו למה $ks_1 m_1 + a_1 = -ks_2 m_2 + a_2$ ומה אפשר לעשות עם זה.
כהערת אגב, זאת גרסה (מעט משוכללת) של משפט השאריות הסיני, והפתרון שמוצאים הוא יחיד עד כדי שקילות $\operatorname{lcm}(m_1, m_2)$.

ב. הציעו אלגוריתם לפתרון בעיית הלוגריתם הבדיד ל-S_n, שיהיה יעיל גם לחבורה גדולה כמו S_{300} (יש בה איברים מסדר שגדול מ-10^{17}). רמז: אינדוקציה.

ג. הסבירו איך האלגוריתם שלכם יפעל במקרה שבו σ היא מחזור מאורך 100 ובמקרה שבו σ היא מכפלה של 50 מחזורים זרים שחצי מהם מאורך 3 וחצי מהם מאורך 2.

ד. נבחר את התמורה

$$\sigma = (7, 8, 9, 10)(1, 3, 11, 13, 4)(5, 2, 6, 18, 17, 16) \in S_{18}$$

הראו איך האלגוריתם שלכם מהסעיף השני מוצא את x עבור התמורה

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 11 & 16 & 13 & 3 & 17 & 5 & 9 & 10 & 7 & 8 & 4 & 12 & 1 & 14 & 15 & 18 & 6 & 2 \end{pmatrix} \in \langle\sigma\rangle$$

בהצלחה!