

פתרון תרגיל בית 8 במבנים אלגבריים 89-214 סמסטר א' תשפ"ג

שאלה 1 (חימום). נניח ואליס הגרילה ראשוני מאוד גדול p . האם יש בעיה שהיא תבחר את $n = p^2$ כחלק מהמפתח הציבורי שלה באלגוריתם RSA?

פתרון. אפשר לחשב שורש כמספר ממשי יחסית מהר בשיטות של אנליזה נומרית. אם ידוע מראש שמדובר במספר ריבועי, אז זה אפילו יותר קל. קראו עוד על **שיטות כאלו** בויקיפדיה.

שאלה 2. קודדו ב-ASCII את האות הראשונה של שמכם באנגלית למספר, שאותו נסמן A . קודדו גם את האות הקטנה המתאימה ל- A למספר ואותו נסמן λ . חשבו בשיטה של **חישוב חזקה בעזרת ריבועים** את $A^\lambda \pmod{1001}$. לדוגמה אם שמכם הוא זְרוּבָבֶל הקידוד של Z הוא 90 והקידוד של z הוא 122. אתם מתבקשים לחשב את $90^{122} \pmod{1001}$. מותר להשתמש במחשבון (כולל בפונקציית המודולו) לחישובי הביניים, שאותם צריך לפרט.

פתרון. למי שרוצה, יש לנו את התשובות הסופיות. אפשר גם לכתוב פונקציה שמדפיסה את השלבים השונים (שבהם לכל היותר $2 \log_2 \lambda$ חישובי ביניים) ולוודא שחישבתם נכון.

שאלה 3. ידוע כי $p = 257$ הוא ראשוני ושהחבורה U_{257} היא ציקלית. בעזרת הנתונים

$$89 \equiv 214^{186} \pmod{257} \quad 99 \equiv 214^{90} \pmod{257} \quad U_{257} = \langle 214 \rangle$$

מצאו $0 \leq x < 257$ כך ש- $99 \equiv 89^x \pmod{257}$.

אל תשברו את בעיית הלוגריתם הבדיד הזו בכוח, אלא במוח. רמז: מתישהו תצטרכו את אלגוריתם אוקלידס המורחב בחבורה אחרת, ולא הרבה מעבר לזה. דרך הפתרון צריכה לעבוד גם עבור p -י גדולים.

פתרון. בכל מקרה אתם צריכים לכתוב עם משפטים מלאים מה אתם עושים. רצף של משוואות נטול נימוקים הוא כמעט תמיד לא כתיבה מתמטית טובה, כי לא קל להבין רצף שכזה. לפי הצבת הנתונים במשוואה האחרונה נקבל

$$214^{90} \equiv 89^x \equiv 214^{186x} \pmod{257}$$

נשים לב כי $214 \in U_{257}$, שהרי 257 ראשוני, אז הוא בוודאי זר ל-214. לכן נוכל לכפול את המשוואה האחרונה ב- 214^{-90} ולקבל

$$214^{186x-90} \equiv 1 \pmod{257}$$

כבר ראינו את הטענה שבכל חבורה G מתקיים $g^n = e_G$ אם ורק אם $o(g) | n$. אצלנו $G = U_{257}$ ואיבר היחידה הוא 1. לכן $o(214) | (186x - 90)$. נתון כי 214 יוצרת את U_{257} שהיא מסדר

$$\varphi(257) = 257 - 1 = 256$$

ולכן $186x - 90 \equiv 0 \pmod{256}$. לא במקרה זה דומה להוכחת הנכונות של הפענוח באלגוריתם RSA. כעת הגענו לבעיה יותר מוכרת

$$186x \equiv 90 \pmod{256}$$

שבה נרצה "להפוך" את 186. הבעיה היא ש- $186 \notin U_{\varphi(257)} = U_{256}$. עדיין אפשר להציל את המצב כי שני האגפים הם כפולה של 2:

$$2 \cdot 93x \equiv 2 \cdot 45 \pmod{256}$$

וכעת $93 \in U_{256}$ ואפשר למצוא לו הופכי. אם נכפיל ב- 93^{-1} ונמצא פתרון x למשוואה, אז סיימנו. נעזר באלגוריתם אוקלידס המורחב:

$$\begin{aligned} (256, 93) &= [256 = 2 \cdot 93 + 70] \\ (93, 70) &= [93 = 1 \cdot 70 + 23] \\ (70, 23) &= [70 = 3 \cdot 23 + 1] \\ (23, 1) &= [23 = 23 \cdot 1 + 0] = 1 \end{aligned}$$

ובהצבה לאחור נקבל

$$\begin{aligned} 1 &= 1 \cdot 70 - 3 \cdot 23 \\ &= 1 \cdot 70 - 3 \cdot (1 \cdot 93 - 1 \cdot 70) = -3 \cdot 93 + 4 \cdot 70 \\ &= -3 \cdot 93 + 4 \cdot (1 \cdot 256 - 2 \cdot 93) = 4 \cdot 256 - 11 \cdot 93 \end{aligned}$$

כלומר $93^{-1} \equiv -11 \equiv 245 \pmod{256}$. לכן

$$\begin{aligned} 93^{-1} \cdot 93x &\equiv 93^{-1} \cdot 45 \pmod{256} \\ x &\equiv 245 \cdot 45 \equiv 17 \pmod{256} \end{aligned}$$

ואכן $186 \cdot 17 \equiv 90 \pmod{256}$. לכן $x = 17$. כדאי לבדוק שאכן $99 \equiv 89^{17} \pmod{257}$ כדי שתראו שקיבלתם את התוצאה הרצויה.

שאלה 4. אליס ובוב רצו לשלוח זה לזה הודעות מוצפנות עם RSA. שניהם השתמשו במעריך ההצפנה $e = 7$. אליס הגרילה את הראשוניים p, q ובוב הגריל את הראשוניים p', q' ויצרו את המפתחות הציבוריים שלהם

$$n = pq = 38009, \quad n' = p'q' = 34427$$

בשאלה הזו אפשר להשתמש במחשבון פשוט לחישובי הביניים, אבל צריך לפרט אותם.

א. בוב רצה לשלוח לאליס את מספר הקורס 214 באופן מוצפן. הראו איך בוב יצפין את ההודעה. (כדאי לוודא אחר כך שאליס מצליחה לפענח את ההודעה נכון, אבל זה לא חלק מהשאלה.)

ב. בחרו מילה בת שלוש אותיות באנגלית וקודדו אותה ל-ASCII. עזרו לאליס למצוא דרך לקודד את המילה ולשלוח אותה לבוב באופן מוצפן עם שליחת שתי הודעות בלבד. הראו את ההודעות המוצפנות שאליס שלחה. שימו לב שמותר לאליס ובוב לתאם מראש את דרך הקידוד (כלומר אתם בונים פרוטוקול תקשורת שבו מסבירים איך נראית הודעה).

ג. המחשבים של אליס ובוב לא טובים בהגרלת ראשוניים, ומבלי לדעת חלק מהראשוניים p, q, p', q' שהגרילו לא שונים זה מזה. מצאו את המפתח הפרטי d של אליס ואת המפתח הפרטי d' של בוב בעזרת חישוב $\gcd(n, n')$.

פתרון.

א. ההודעה המוצפנת היא

$$\begin{aligned} c &\equiv m^e \equiv 214^7 \pmod{38009} \\ &\equiv 214 \cdot (214 \cdot (214)^2)^2 \pmod{38009} \\ &\equiv 214 \cdot (214 \cdot 7787)^2 \pmod{38009} \\ &\equiv 214 \cdot (32031)^2 \pmod{38009} \\ &\equiv 214 \cdot 8024 \pmod{38009} \\ &\equiv 6731 \pmod{38009} \end{aligned}$$

כאשר שלבי הביניים הם חישוב חזקה עם ריבועים. הפיענוח גם הוא קל, אם יודעים מהו המפתח הפרטי של אליס מהסעיף האחרון, ולכן נחשב $m \equiv c^d \equiv 214 \pmod{38009}$ ואת זה מוודאים שוב עם העלאה בחזקה עם ריבועים.

ב. העניין הוא שאות ב-ASCII תופסת לכל היותר 8 סיביות (יותר נכון לומר 7 סיביות, אבל זה לא חשוב). נשים לב כי $2^{15} = 32768 > n'$ ולכן כדי לשלוח $3 \cdot 8 = 24$ סיביות המרכיבות מילה בת שלוש אותיות, רק צריך להסכים ששולחים את האות האמצעית חצויה. לכן נשלח שתי הודעות שכל אחת מהן היא עם 12 סיביות (כלומר לכל היותר $2^{12} = 4096$) שאפשר לשלוח במגבלת הגודל של n' . יש אפילו מקום לסמן בהודעה האם היא כוללת אות אחת, או אות וחצי, למשל על ידי זה שנבחר שהסיבית הראשונה דולקת במקרה כזה. ההודעות בפרוטוקול הזה יהיו באורך 13 סיביות, ומסכימים שאם נשלחת הודעה עם אות וחצי, אז ההודעה אחריה מכילה קודם חצי אות ואז אות שלמה. לדוגמה אם המילה היא Win, אז קודם נקודד אותה ל-ASCII:

$$\begin{array}{lll} W \leftrightarrow 87_{10} & i \leftrightarrow 105_{10} & n \leftrightarrow 110_{10} \\ = 01010111_2 & = 01101001_2 & = 01101110_2 \end{array}$$

ובמקום לשלוח את הרצף **010101110110100101101110** נשלח שתי הודעות:

$$\begin{aligned} 1010101110110_2 &= 5494_{10} \\ 1100101101110_2 &= 6510_{10} \end{aligned}$$

כאשר הסיביות הגבוהות (השמאליות ביותר) מציינות שאנחנו שולחים אות וחצי. אז אליס תשלח את ההודעות המוצפנות בעזרת המפתח הציבורי של בוב:

$$\begin{aligned} 5494^7 &\equiv 20758 \pmod{34427} \\ 6510^7 &\equiv 10859 \pmod{34427} \end{aligned}$$

שחישבנו כמו בסעיף הקודם עם העלאה בחזקה בעזרת ריבועים. ודאו שאתם מבינים איך בוב יפענח את ההודעות המוצפנות ואיך הוא ירכיב חזרה את המילה שנשלחה.

ג. נניח בלי הגבלת הכלליות כי $p = p'$, כי לפחות אחד מ- p או q שווה ל- p' או q' . לכן $\gcd(n, n') \geq p$. נחשב לפי אלגוריתם אוקלידס כי

$$\begin{aligned} (38009, 34427) &= [38009 = 1 \cdot 34427 + 3582] \\ (34427, 3582) &= [34427 = 9 \cdot 3582 + 2189] \\ (3582, 2189) &= [3582 = 1 \cdot 2189 + 1393] \\ (2189, 1393) &= [2189 = 1 \cdot 1393 + 796] \\ (1393, 796) &= [1393 = 1 \cdot 796 + 597] \\ (796, 597) &= [796 = 1 \cdot 597 + 199] \\ (597, 199) &= [597 = 3 \cdot 199 + 0] \\ (199, 0) &= 199 \end{aligned}$$

לכן $p = p' = 199$ ונחשב $q = n/p = 191$ ו- $q' = n'/p' = 173$. כלומר $n = 199 \cdot 191$ וגם $n' = 199 \cdot 173$.

כעת נמצא את המפתחות הפרטיים עם אלגוריתם אוקלידס המורחב. תחילה צריך לוודא כי $(\varphi(n), e) = 1$ וגם $(\varphi(n'), e) = 1$. נחשב

$$\varphi(n) = (p-1)(q-1) = 37620 \quad \varphi(n') = (p'-1)(q'-1) = 34056$$

ולכן

$$(37620, 7) = [37620 = 5374 \cdot 7 + 2]$$

$$(7, 2) = [7 = 3 \cdot 2 + 1]$$

$$(2, 1) = 1$$

ומהצבה לאחור נקבל

$$1 = 1 \cdot 7 - 3 \cdot 2 = 1 \cdot 7 - 3 \cdot (1 \cdot 37620 - 5374 \cdot 7) = -3 \cdot 37620 + 16123 \cdot 7$$

וכך קיבלנו כי

$$d \equiv 7^{-1} \equiv 16123 \pmod{37620}$$

הוא המפתח הפרטי של אליס. כעת נחשב

$$(34056, 7) = [34056 = 4865 \cdot 7 + 1]$$

$$(7, 1) = 1$$

ומהצבה לאחור נקבל $1 = 1 \cdot 34056 - 4865 \cdot 7$. כך קיבלנו כי

$$d' \equiv 7^{-1} \equiv -4865 \equiv 29191 \pmod{34056}$$

הוא המפתח הפרטי של בוב.

שאלה 5 (תכנות). ממשו בעצמכם פונקציה בשם $\text{superpower}(x, k, n)$ 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

$$x^i = y \pmod{n}$$

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

$$89^1 = 89 \pmod{101}$$

$$89^2 = 43 \pmod{101}$$

$$89^4 = 31 \pmod{101}$$

$$89^5 = 32 \pmod{101}$$

$$89^{10} = 14 \pmod{101}$$

$$89^{11} = 34 \pmod{101}$$

נסו להריץ את $\text{superpower}(x, k, 89214)$ עבור מספרים "גדולים" יחסית x, k שעבורם אתם עדיין יכולים לוודא את הפתרון.

שאלה 6 (רשות). בעזרת שיטת צעדי גמד וצעדי ענק שראינו בכיתה מצאו את הפתרון למשוואה

$$71 \equiv 7^x \pmod{101} \text{ ופתרון למשוואה } 72 \equiv 7^y \pmod{101}$$

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 $0 \leq x, y, z < 101$.

פתרון. נזכר בדוגמה מהכיתה לפיה 101 ראשוני, החבורה $G = U_{101}$ היא ציקלית והאיבר $g = 7$ הוא יוצר שלה. לכן קל לחשב $\varphi(101) = |G| = o(7) = n$. נסמן $m = \lceil \sqrt{100} \rceil = 10$ חישבנו כי

$$g^{-m} \equiv 7^{-10} \equiv 14 \pmod{101}$$

ויצרנו טבלה עם כל החזקות g^j עבור $0 \leq j < m$:

j	0	1	2	3	4	5	6	7	8	9
7^j	1	7	49	40	78	41	85	90	24	67

נריץ את ההתקפה עבור 71. נאתחל $\alpha \leftarrow 71$. עבור $i = 0$, נשים לב כי α לא נמצא בשורה השנייה בטבלה. נחשב $14\alpha = 85$ ונמשיך עם $i = 1$. נשים לב כי עבור $j = 6$ מצאנו כי α מופיע בטבלה. לכן $x = 10 \cdot 1 + 6 = 16$ ותוכלו לוודא עם הפונקציה מהשאלה הבאה כי $71 \equiv 7^{16} \pmod{101}$.

קעת נריץ את ההתקפה עבור 72. נאתחל $\alpha \leftarrow 72$. עבור $i = 0$, נשים לב כי α לא נמצא בשורה השנייה בטבלה. נמשיך בהרצה

$\alpha \leftarrow 14\alpha = 99$	$i = 1$
$\alpha \leftarrow 14\alpha = 73$	$i = 2$
$\alpha \leftarrow 14\alpha = 12$	$i = 3$
$\alpha \leftarrow 14\alpha = 67$	$i = 4$

נשים לב שאם $i = 4$, אז α מופיע בטבלה עם $j = 9$. לכן $y = 10 \cdot 4 + 9 = 49$ ותוכלו לוודא עם הפונקציה מהשאלה הבאה כי $72 \equiv 7^{49} \pmod{101}$.

היו מי שהוכיחו שגם 72 הוא יוצר של U_{101} (זה משהו שצריך להוכיח, למשל כי 49 זר ל-100), ומצאו את z בעזרת שיטת צעדי גמד וצעדי ענק. כמובן שזה ייתן את התשובה הנכונה, אבל זו יותר מדי עבודה, ולא בטוח יעבוד אילולא 72 היה יוצר (כלומר צריך לעבור לתת-החבורה $\langle 72 \rangle$ שתיאורטית יכולה להיות מסדר קטן יותר). נראה שיטה יותר מהירה, שמסתמכת על מציאת x, y עם סיבוכיות מקום $O(1)$.

לפי הפתרונות הקודמים המשוואה $71 \equiv 7^{2z} \pmod{101}$ היא למעשה

$$7^{16} \equiv 7^{49z} \pmod{101}$$

מפני שכאמור $7 \in U_{101}$, אפשר לחלק ב- 7^{16} ולקבל $7^{49z-16} \equiv 7^0 = 1 \pmod{101}$. כפי שראינו בכיתה $\varphi(101) = o(7) = 100$. בכיתה הוכחנו כי בחבורה G מתקיים לכל איבר $a \in G$ כי $a^n = e$ אם ורק אם $n \mid o(a)$. מפני ש-1 הוא איבר היחידה, נסיק מהתרגיל בכיתה כי $100 \mid (49z - 16)$. כלומר $49z \equiv 16 \pmod{100}$. מפני ש- $49 \in U_{100} = U_{100-1}$, אז יש לו הופכי. נמצא אותו עם אלגוריתם אוקלידס המורחב:

$$\begin{aligned} (100, 49) &= [100 = 2 \cdot 49 + 2] \\ (49, 2) &= [49 = 24 \cdot 2 + 1] \\ (2, 1) &= 1 \end{aligned}$$

ולכן בהצבה לאחור נקבל

$$1 = 1 \cdot 49 - 24 \cdot 2 = 1 \cdot 49 - 24 \cdot (1 \cdot 100 - 2 \cdot 49) = -24 \cdot 100 + 49 \cdot 49$$

ויוצא במקרה $49^{-1} \equiv 49 \pmod{100}$ לכן $z \equiv 16 \cdot 49 \equiv 84 \pmod{100}$. לא במקרה זה דומה להוכחת הנכונות של אלגוריתם RSA.

שאלה 7 (אתגר). 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 $-k s_1 m_1 + a_1 = k s_2 m_2 + a_2$ ומה אפשר לעשות עם זה.

כהערת אגב, זאת גרסה (מעט משוכללת) של משפט השאריות הסיני, והפתרון שמוצאים הוא יחיד עד כדי שקילות מודולו $\text{lcm}(m_1, m_2)$.

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

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 (באופן יעיל ולא נאיבי) את x עבור התמורה

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

פתרון.

(א) נעזר בהדרכה. מהנתון $a_1 \equiv a_2 \pmod{\gcd(m_1, m_2)}$, ולפי הגדרת שקילות מודולו, נסיק שקיים $k \in \mathbb{Z}$ עבורו $a_1 = a_2 + k \cdot \gcd(m_1, m_2)$. לכן $a_1 - a_2 = k \cdot \gcd(m_1, m_2)$. בנוסף קיימים $s_1, s_2 \in \mathbb{Z}$ המקיימים

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

נציב את אגף שמאל במשוואה הראשונה ונקבל

$$a_1 - a_2 = k \cdot \gcd(m_1, m_2) = k(s_1 m_1 + s_2 m_2) = k s_1 m_1 + k s_2 m_2$$

על ידי העברת אגפים נקבל $a_1 - k s_1 m_1 = a_2 + k s_2 m_2$ ונוכיח שהערך הזה הוא פתרון משותף, שנסמן x . אכן

$$x \equiv a_1 - k s_1 m_1 \equiv a_1 \pmod{m_1}$$

כי $-k s_1 m_1$ מתחלק ב- m_1 . באופן דומה

$$x \equiv a_2 + k s_2 m_2 \equiv a_2 \pmod{m_2}$$

נשים לב להערה בהדרכה לגבי שאר הפתרונות. ברור שאם x הוא פתרון, אז לכל $k' \in \mathbb{Z}$ המספר $x + k' \text{lcm}(m_1, m_2)$ גם הוא פתרון, כי $\text{lcm}(m_1, m_2)$ מתחלק ב- m_1 וב- m_2 . מצד שני, אם גם y הוא פתרון, אז

$$x - y \equiv a_1 - a_1 \equiv 0 \pmod{m_1}$$

$$x - y \equiv a_2 - a_2 \equiv 0 \pmod{m_2}$$

ולכן $(x - y \equiv 0 \pmod{\text{lcm}(m_1, m_2)})$ כלומר הם שקולים מודולו $\text{lcm}(m_1, m_2)$. בנוסף, אם קיים פתרון למערכת המשוואות, אז נפעיל מודולו $\text{gcd}(m_1, m_2)$ ונקבל שיש פתרון למערכת המשוואות

$$\begin{cases} x \equiv a_1 \pmod{\text{gcd}(m_1, m_2)} \\ x \equiv a_2 \pmod{\text{gcd}(m_1, m_2)} \end{cases}$$

ולכן $a_1 \equiv a_2 \pmod{\text{gcd}(m_1, m_2)}$

(ב) נחשב את ההצגה של σ כמכפלת מחזורים זרים, נניח $\sigma = \mu_1 \mu_2 \dots \mu_r$ כאשר μ_i הוא מחזור מאורך m_i . הסדר של σ הוא $\text{lcm}(m_1, m_2, \dots, m_r)$. ידוע לנו כי

$$\tau = \sigma^x = (\mu_1 \mu_2 \dots \mu_r)^x = \mu_1^x \mu_2^x \dots \mu_r^x = \mu_1^x \pmod{m_1} \mu_2^x \pmod{m_2} \dots \mu_r^x \pmod{m_r}$$

כאשר בשיויון השלישי השתמשנו בכך שהמחזורים μ_i הם זרים, ולכן מתחלפים. בשיויון האחרון השתמשנו בכך שהסדר של μ_i הוא m_i , ולכן מעניינת אותנו רק השארית מודולו m_i . נניח שהמספרים במחזור הם $\mu_i = (c_{i,0}, c_{i,1}, \dots, c_{i,m_i-1})$. אילו σ הייתה מחזור אחד μ_1 , אז x נקבע לחלוטין לפי $\mu_1(c_{1,0}) = c_{1,a}$. לכן אם יודעים את המיקום של הערך $\mu_i(c_{i,0})$ במחזור μ_i , מצאנו את a_i שהוא x מודולו m_i (בדיקת שפיות תהיה $\mu_i^0 = \text{id}$ ואכן $\mu_i(c_{i,0}) = c_{i,0} = \text{id}(c_{i,0})$). בהנתן $\tau \in \langle \sigma \rangle$, כל מה שאנחנו יודעים זה שהוא חזקה של σ . יש לו הצגה כמכפלת מחזורים זרים, שאנחנו יודעים לגלות שהם מגיעים מחזקות של המחזורים μ_i (שימו לב כי μ_i^x יכול להיות מכפלה של כמה מחזורים):

$$\tau = \mu_1^{a_1} \mu_2^{a_2} \dots \mu_r^{a_r}$$

כלומר קיים פתרון משותף x למערכת המשוואות

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

שאותו צריך למצוא. נשים לב שאם $m_i = m_j$, אז אפשר להתעלם מהמשוואה עם m_j , כי היא תהיה זהה למשוואה עם m_i . למעשה אם $m_j | m_i$, גם אז ניתן להתעלם מהמשוואה עם m_j , כי הפתרון עבור המשוואה עם m_i יהווה פתרון גם עבור המשוואה עם m_j .

אנחנו יודעים שקיים פתרון x , ולכן לפי ההערה בסוף הסעיף הקודם, נסיק שהתנאים של הסעיף הקודם מתקיימים לכל זוג משוואות. כלומר אם נסמן $d_i = \text{gcd}(m_i, m_r)$ לכל $1 \leq i, j \leq r$, אז $a_i \equiv a_j \pmod{d_{ij}}$. נמצא באינדוקציה פתרון למערכת המשוואות, כאשר הסעיף הקודם הוא בסיס האינדוקציה. זה דורש חישוב $r-1$ פעמים של אלגוריתם אוקלידס המורחב (שהוא יעיל), כאשר $r \leq n$ שהוא מספר קטן לעומת $n!$.

אם $r = 1$, אז כאמור קל למצוא את x . אם $r = 2$, נעזר בסעיף הקודם. כעת נניח כי y הוא פתרון משותף למערכת המשוואות

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_{r-1} \pmod{m_{r-1}} \end{cases}$$

ונרצה למצוא פתרון משותף x לכל המשוואות האלו וגם למשוואה $x \equiv a_r \pmod{m_r}$. הפתרון y הוא יחיד עד כדי מודולו $\text{lcm}(m_1, \dots, m_{r-1})$. כעת התנאי בסעיף הקודם דורש להוכיח כי

$$y \equiv a_r \pmod{\text{gcd}(\text{lcm}(m_1, \dots, m_{r-1}), m_r)}$$

ואנחנו כבר יודעים כי $a_r \equiv a_i \pmod{d_{ir}}$ לכל $1 \leq i < r$. קיימים s_i כך שמתקיים $a_r \equiv y + s_i m_i \pmod{d_{ir}}$. זה גורר כי $a_i = y + s_i m_i$. כלומר $a_r \equiv y \pmod{d_{ir}}$. לכל $1 \leq i < r$ לכן

$$\begin{aligned} y &\equiv a_r \pmod{\text{lcm}(d_{1r}, d_{2r}, \dots, d_{r-1,r})} \\ &\equiv a_r \pmod{\text{lcm}(\text{gcd}(m_1, m_r), \text{gcd}(m_2, m_r), \dots, \text{gcd}(m_{r-1}, m_r))} \\ &\equiv a_r \pmod{\text{gcd}(\text{lcm}(m_1, \dots, m_{r-1}), m_r)} \end{aligned}$$

כדרוש. לכן למערכת

$$\begin{cases} x \equiv y \pmod{\text{lcm}(m_1, \dots, m_{r-1})} \\ x \equiv a_r \pmod{m_r} \end{cases}$$

קיים פתרון יחיד עד כדי מודולו $\text{lcm}(\text{lcm}(m_1, \dots, m_{r-1}), m_r) = \text{lcm}(m_1, \dots, m_r)$ אינדוקציה אחרת, תראה כי קיים פתרון y כמו מקודם של $r-1$ משוואות, ופתרון z עבור המערכת

$$\begin{cases} z \equiv a_{r-1} \pmod{m_{r-1}} \\ z \equiv a_r \pmod{m_r} \end{cases}$$

לפי הנחת האינדוקציה. הוא יחיד עד כדי $\text{lcm}(m_{r-1}, m_r)$. לכן נוכל למצוא פתרון עבור מערכת $r-1$ המשוואות

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_{r-2} \pmod{m_{r-2}} \\ x \equiv z \pmod{\text{lcm}(m_{r-1}, m_r)} \end{cases}$$

ורק נותר להוכיח כי $z \equiv a_i \pmod{\text{gcd}(\text{lcm}(m_{r-1}, m_r), m_i)}$ לכל $1 \leq i < r-1$. שזה לא יותר מדי קשה.

באף שלב אין צורך למצוא את τ כמכפלה של מחזורים זרים, אלא רק את a_1, \dots, a_r . נניח כי σ היא מחזור מאורך 100, ונסמן $\sigma = (c_0, c_1, \dots, c_{99})$. לפי הסעיף הקודם, אם $\tau = \sigma^x$, אז $\sigma^x(c_0) = c_x$ עבור $0 \leq x < 100$. אז יהיה הפתרון לבעיית הלוגריתם הבדיד. שימו לב שזה עדיין דורש מציאת המיקום של c_x בתוך המחזור, ולכן זה לא זמן ריצה של $O(1)$.

אם σ היא מכפלה של עשרים מחזורים מאורך 3 ועשרים מחזורים מאורך 2 (שכולם זרים זה לזה), אז הסדר שלה הוא $[3, \dots, 3, 2, \dots, 2] = 6$. מספיק לנו להסתכל על מחזור אחד מאורך 3 ומחזור אחד מאורך 2, כי אין צורך בחזרה על 50 משוואות זהות. כלומר עבור שני מחזורים מוצאים $\mu_1^{a_1} \mu_2^{a_2}$ ומחפשים פתרון למערכת המשוואות

$$\begin{cases} x \equiv a_1 \pmod{2} \\ x \equiv a_2 \pmod{3} \end{cases}$$

ואת זה עושים לפי הסעיף הראשון. למעשה מוצאים פתרון מודולו 6.

(ד) למזלנו σ כבר נתונה כמכפלת מחזורים זרים. נסמן כמו באלגוריתם שלנו

$$\mu_1 = (7, 8, 9, 10) \quad \mu_2 = (1, 3, 11, 13, 4) \quad \mu_3 = (5, 2, 6, 18, 17, 16)$$

ובפרט $m_1 = 4, m_2 = 5, m_3 = 6$. כעת נבנה את מערכת המשוואות. נחשב $\tau(7) = 9$ ולכן $a_1 \equiv 2 \pmod{4}$. נחשב $\tau(1) = a_2 = 11$ ולכן $a_2 \equiv 2 \pmod{5}$. לבסוף נחשב $\tau(5) = 17$ ולכן $a_3 \equiv 4 \pmod{6}$. כך קיבלנו כי

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{6} \end{cases}$$

לזוג המשוואות הראשונות תחילה נחשב $\gcd(5, 4) = 1 = 1 \cdot 5 - 1 \cdot 4$. במקרה הזה $2 - 2 \equiv 0 \pmod{1}$ וזה מאפשר לקחת למשל $k = 0$ ואת הפתרון $x = a_1 = a_2 = 2$ כך נפחית את מספר המשוואות

$$\begin{cases} x \equiv 2 \pmod{20} \\ x \equiv 4 \pmod{6} \end{cases}$$

כי $\text{lcm}(4, 5) = 20$. כעת נחשב $\gcd(20, 6) = 2 = 1 \cdot 20 - 3 \cdot 6$. אוקלידס המורחב. כמובן שמתקיים $2 - 4 \equiv 0 \pmod{2}$ ולכן כאן נקבל $2 = 4 - 1 \cdot 2$, כלומר $k = -1$. כך נוכל לבחור בתור פתרון את

$$x = -(-1) \cdot 1 \cdot 20 + 2 = 22 = -1 \cdot (-3) \cdot 6 + 4$$

וקיבלנו כי $\tau = \sigma^{22}$.

למי שרוצה לדעת, הפתרון שלנו מאפשר לחשב ישירות כי

$$\begin{aligned} \tau &= \sigma^{22} = (7, 8, 9, 10)^{22} (1, 3, 11, 13, 4)^{22} (5, 2, 6, 18, 17, 16)^{22} \\ &= (7, 8, 9, 10)^2 (1, 3, 11, 13, 4)^2 (5, 2, 6, 18, 17, 16)^4 \\ &= (7, 9)(8, 10)(1, 11, 4, 3, 13)(5, 17, 6)(2, 16, 18) \end{aligned}$$

על אף שזה חישוב מיותר. צריך לדעת שמאוד קל לבדוק כי $(7, 8, 9, 10)^4 = \text{id}$, ולכן זה מוזר שרבים ענו $x = 4$. ברור כי $\tau \neq \sigma^4$, שהרי למשל $\sigma^4(7) = 7$ ואילו $\tau(7) \neq 7$. זה אומר שבסעיף זה לא מקבלים נקודות, וצריך לבדוק האם הבנתם מה עושה האלגוריתם שלכם מהסעיפים הקודמים.

בהצלחה!