Q1

סעיף א':

בסעיף זה אסמן כדלקמן: $a=k*b+r$, $a \bmod b=r$, k שלם כלשהו.

ובנוסף $b=m*b+R$, $c \bmod b=R$, m שלם כלשהו.

אשתמש בכל תתי-הסעיפים בסימון זה.

i. הוכחה:

$(a+c) \bmod b= ((kb+r)+(mb+R)) \bmod b= (b(k+m)+r+R) \bmod b= (r+R) \bmod b$

כאשר המעבר האחרון נובע מכך ש: $\mathbf{b(k+m) \bmod b= 0}$

כעת נציב את הזהות של r,R ונקבל את המבוקש:

$(r+R) \bmod b= ((a \bmod b)+ (c \bmod b)) \bmod b$

ii . הוכחה:

$(a*c) \bmod b= ((kb+r)(mb+R)) \bmod b= (kmb^2+b(kR+rm)+r*R) \bmod b=(r*R) \bmod b$

כאשר המעבר האחרון נובע משתי הבחנות חשובות:

$(kmb^2) \bmod b=0$ וגם מתקיים $b(kR+rm) \bmod b= 0$

לכן נקבל בהתאם לסימונים: $(r*R) \bmod b= ((a \bmod b)(c \bmod b)) \bmod b$

כנדרש.

iii. הוכחה:

בסיס האינדוקציה: עבור $c=1$ טריוויאלי:

$(a \bmod b) \bmod b= (r) \bmod b= r= a \bmod b$

הנחת האינדוקציה: נניח שהטענה נכונה עבור $c-1$:

$(a \bmod b)^{c-1} \bmod b= a^{c-1} \bmod b$

אם כן, עבור c זה יראה כך:

$(a \bmod b)^c=((a \bmod b)^{c-1}(a \bmod b)) \bmod b$ $\leftarrow$

לפי השוויון בהנחת האינדוקציה נקבל: $((a^{c-1} \bmod b)(a \bmod b)) \bmod b$ $\leftarrow$

מ- ii נקבל ש: $(a^{c-1}a) \bmod b= a^c \bmod b$

כדרוש.

סעיף ב':

כדי להוכיח את הטענה תחילה נראה ש-a' ו-a הם שני פרמטרים זהים במונחים של פרוטוקול דיפי הלמן, כלומר הם משמשים לאותו החישוב. במילים אחרות, החלפה בין שני הפרמטרים לא משנה את המפתח של אליס ושל בוב (אליס ובוב מנסים להעביר ביניהם מידע מוצפן).

המפתח של אליס יהיה: $y^a \bmod p=(g^b \bmod p)^a \bmod p= g^{ba} \bmod p=(g^a \bmod p)^b \bmod p$

כאשר המעברים התבססו על ההוכחה בסעיף א iii. מכך ש: $g^{a'} \bmod p = g^a \bmod p$

נקבל: $\underline{\mathbf{g^{a'b} \bmod p}}$ $=(g^{a'} \bmod p)^b \bmod p$.

המפתח של בוב יהיה: $x^a \bmod p=(g^a \bmod p)^b=(g^{a'} \bmod p)^b=\underline{\mathbf{g^{a'b} \bmod p}}$

כאשר במעברים הסתמכנו כמובן על סעיף א' iii וגם על הנתון $g^{a'} \bmod p = g^a \bmod p$

קיבלנו אם כן שלבוב ולאליס אותו המפתח, שלפי דיפי הלמן היה זהה למפתח

$\underline{\mathbf{g^{ab} \bmod p}}$ **.** אם ידוע לנו שבעצם המפתחות זהים, מספיק לנו למצוא אחד מהם.

נמצא את המפתח $\underline{\mathbf{g^{a'b} \bmod p}}$ בסיבוכיות של $O(n^3)$:

$g^{a'b} \bmod p=(g^b \bmod p)^{a'} \bmod p$ כעת נשים לב ש: $g^b \bmod p$ ידוע לנו. גם a' ידוע.

ולכן נוכל לחשב ביעילות modular_exponantiation שראינו בהרצאה, ולו סיבוכיות פולינומיאלית של $O(n^3)$.

Q2

סעיף א':

i. נבדוק את זמני הריצה שנובעים מלולאות הבדיקה של הפונקציות is_sorted . is_prime self.factor מסיבוכיות O(1) כמובן.
מבחינת is_sorted האלגוריתם פועל פולינומיאלית, ולכן מרשימה של k איברים סיבוכיות תהיה O(k) . מבחינת is_prime אז הוא משתמש ב-modpow שראינו שהוא מסיבוכיות O(n**3) כאשר n מייצג את מספר הביטים. אם כן אורך הפלט הסופי הוא n ביטים ולכן כל המספרים בקבוצה P קטנים או שווים לאורך הפלט. (שוויון אם קיים מספר אחד בקבוצה וזה אומר שהפלט הוא מספר ראשוני בעצמו). הדבר נובע כמובן מפעולת האלגוריתם שנועד לחשב את number - אנחנו רק מגדילים את הקלט ע"י הכפלות של מספרים גדולים מ-1. n יהווה חסם הדוק מספיק טוב כי כאשר מכפילים שני מספרים נניח אחד באורך L ביטים והשני באורך M ביטים אז מספר הביטים

של התוצאה יהיה O(M+L) , וכאמור האורך הסופי במקרה שלנו הוא n ביטים.
מכיוון שברשימה יש k איברים נקבל שסיבוכיות הזמן מהלולאה השניה היא $O(k*n^3)$.
ובסה"כ מכל פעולת האתחול הסיבוכיות תהיה $O(k*n^3)$.

ii. אם המספר בעצמו ראשוני אז אורך הרשימה הוא 1.
אם המספר פריק אז אורך הרשימה המקסימלי יווצר כאשר הוא כפולה של מספר יחיד. וליתר דיוק כפולה של המספר הראשוני 2. כי אם צריך להגיע לפלט באורך n ביטים בסופו של דבר, הרי שמספר האיברים ב-P יגדל כמה שיותר אם נכפיל בראשוני הקטן ביותר. ולכן מספר האיברים הגדול ביותר יהיה n-1 -על כל ביט יהיה את המספר 2 ב- P . (החיסור של 1 היא כי מתחילים לספור מ-0 את החזקות של 2 בייצוג בינארי. זה בערך כמו להגיד שאת 1 ניתן להוסיף לכל קבוצה P כי כפולה של כל מספר ב-1 נותנת את המספר עצמו).
לכן הטווח יהיה: $1 \le k \le n-1$.

Q4

סעיף ב' (ii):

סיבוכיות הזמן היא כמובן לינארית בכמות הצמתים בעץ, קרי O(n) , כאשר n הוא מס' הצמתים בעץ כולו. הסיבה לכך היא שעבור כל אב אנו בודקים תנאי על שני בניו O(1) וכאמור אנו מוכרחים לרדת עד לעלים כדי לוודא שאכן מדובר בערימת מינימום. לפי הקוד נקרא רקורסיבית לבן השמאלי ולבן הימני של צומת האב ונוודא שהם מקיימים את התנאי. אם באיזשהו צומת בדרך התנאי לא מתקיים נחזיר False . ואם אין הפרה של התנאי והגענו עד לעלים וגם הם מקיימים את התנאי אז הרי שנחזיר True .

Q5

מתחילים עם a שהוא באורך n ביטים. נשאל מה יהיה אורך (גודל) הפלט לאחר הכפלת התוצאה ב- a ונתחשב בכמה הוא גדל כתלות במספר האיטרציות. נתייחס למקרה הגרוע ביותר שהוא a= a*a . במצב זה גודל הפלט שיתקבל בסוף כל איטרציה הוא הגדול ביותר. להיות כל פעם במצב זה פירושו b mod 2=0 . מספר האיטרציות שהוא

מספר ההכפלות יהיה O(m) , לפי שיקולים שהוצגו בהרצאה. (מחיקת ביט אחד בכל פעם).

בהכפלה הראשונה: **n*n** - ראשית, יתקבל פלט באורך O(2n) . שנית, תתבצענה 2^0*n^2 הכפלות.

בהכפלה השנייה: **2n*2n** – ראשית יתקבל פלט באורך O(4n). שנית תתבצענה 2^2*n^2 הכפלות.

בהכפלה השלישית: **4n*4n** - ראשית יתקבל פלט באורך O(8n) . שנית תתבצענה 4^2*n^2 הכפלות.

וכן הלאה.

סה"כ נקבל סכום סדרה הנדסית: $0+2^0*n^2+2^2*n^2+...+(2^{m-1})^2*n^2$

כלומר : $\sum_{k=0}^{m}(n^2)\,(2^{k-1})^2$. ניתן לסדר ולהגיע לביטוי מפורש יותר:

$$(1/4) * n^2 \sum_{k=0}^{m} 2^{2k}$$

←

$$(1/4)n^2 \sum_{k=0}^{m} 4^k$$

נשתמש במה שיודעים על סכום סדרה הנדסית ונקבל שהסכום שבסיגמה הוא

$(4^m - 1)/3$

לאחר הורדת הקבועים נקבל בסה"כ את הסיבוכיות המבוקשת: ***$O(n^2 * 4^m)$*** . כאמור אקספוננציאלי ב- *m* וזה מספיק לנו כדי להבין שפעולת העלאה בחזקה היא "יקרה".