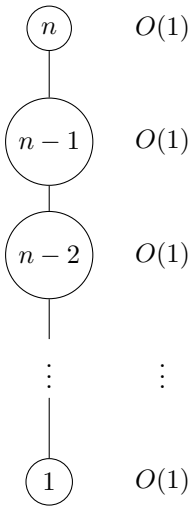
שאלה 1

א

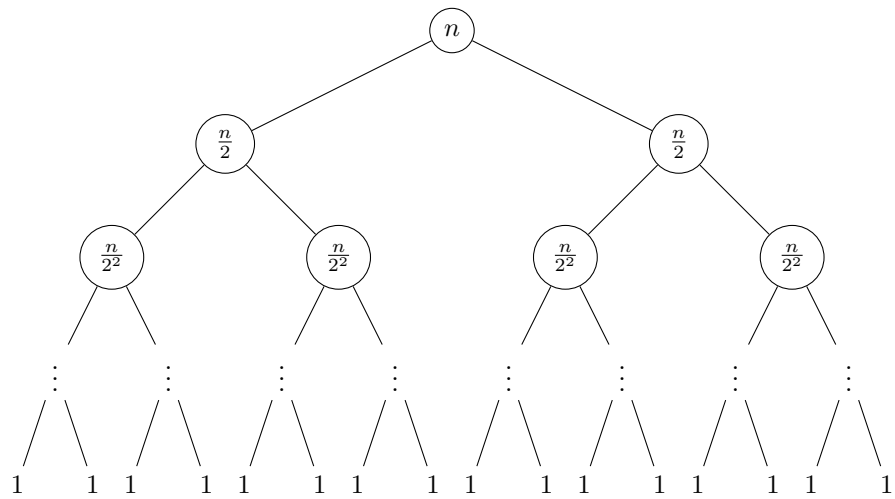
בכל צומת של הרקורסיה ישנה קריאה רקורסיבית אחת בלבד עם רשימה באורך קטן ב1 כארגומנט. לכן עץ הרקורסיה יהיה בעומק n. נשים לב כי בכל צומת של הרקורסיה הפונקציה מבצעת מספר חסום של פעולות בסיבוכיות $O(1)$, לכן סיבוכיות כל צומת היא גם כן $O(1)$. לכן הסיבוכיות של הפונקציה היא $O(n)$.



ג

בכל צומת של הרקורסיה ישנן 2 קריאות רקורסיביות עם רשימה קטנה פי 2 כארגומנט. לכן עץ הרקורסיה יהיה בעומק $\log_2 n$. נשים לב כי בכל צומת של הרקורסיה הפונקציה מבצעת מספר חסום של פעולות בסיבוכיות $O(1)$ ומכאן שסיבוכיות כל צומת היא גם $O(1)$. בכל רמה l של העץ יש 2^l צמתים ולכן הסיבוכיות של כל רמה כזו היא $O(2^l)$. מכאן שהסיבוכיות של הפונקציה עבור קלט בגודל n היא:

$$O(2^0 + 2^1 + 2^2 + \cdots + 2^{\log_2 n}) = O(2 \cdot 2^{log_2 n} - 1) = O(2n) = O(n)$$



ד

ממוצע זמני ריצה של 1000 הרצות:

Function	$n = 1000$	$n = 2000$	$n = 4000$
max1	0.01112	0.04144	0.17369
max2	0.00505	0.01017	0.01998
max_list11	0.00403	0.00807	0.01676
max_list22	0.00441	0.00872	0.01748

ה

ראשית נסתכל על זמני הריצה של max_list11 ו max_list22 . בין הרצה להרצה אנו מעלים את n פי 2 וזמני הריצה מראים עלייה של פי 2 גם. כלומר שזמני הריצה תלויים (בקירוב) ליניארית בn. הטענה מתיישבת עם זמני הריצה שחישבנו: $O(n)$.

כעת נסתכל על זמני הריצה של $max1$ בין הרצה להרצה אנו מעלים את n פי 2 וזמני הריצה מראים עלייה של פי 4. כלומר שזמני הריצה תלויים (בקירוב) ליניארית בn^2. עץ הרקורסיה של $max1$ זהה לזה של max_list11 אך סיבוכיות כל צומת בה היא $O(n)$ בגלל השימוש ב$slicing$ ומכאן נובע שסיבוכיותה הכוללת היא $O(n^2)$ בהתאמה למדידות.

זמני הריצה של $max2$ נראים ליניאריים למרות השימוש ב$slicing$. הסיבה לכך שהשימוש בו גורם לכל צומת להיות $O(\frac{n}{2^l})$, לכן סיבוכיות רמה l בעץ הרקורסיה היא $O(n)$ והסיבוכיות הכוללת היא $O(n \cdot \log_2 n)$ כאשר $\log_2 n$ בעל השפעה זניחה על זמני הריצה.

שאלה 5

א

n	100	200	300	400	500
density_primes	0.0131	0.0068	0.0053	0.0042	0.0023

לפי משפט המספרים הראשוניים $\pi(x) \approx \frac{x}{\ln x}$. לכן:

$$density(n) = \frac{\pi(2^n - 1) - \pi(2^{n-1} - 1)}{2^{n-1}} \approx \frac{2}{\ln(2^n - 1)} - \frac{1}{\ln(2^{n-1} - 1)}$$

בקירוב לתוצאות.

n	100	200	300	400	500
∼density	0.01428	0.00717	0.00479	0.00359	0.00287

ב

דני יכשל נחרצות. הסיבה לכך היא ש $witnees$ אינו בהכרח מחלק של N אלא רק עד לפריקותו. לדוגמא עבור $N = 7 \cdot 11$ קבוצת המספרים a מודולו N המקיימים $a^{N-1} \not\equiv 1 \pmod N$ (קבוצת העדים האפשריים) היא $[0, N-1] \cap \mathbb{N} \setminus \{1, 34, 43, 76\}$ ובה מספרים רבים שאינם מחלקים של N לדוגמא $2, 3, 15$.

שאלה 6

הסטודנט הזדוני יכול לחשב את הסוד המשותף של יעל ומיכל. נוכיח זאת באופן מתמטי: יהיו p, g מספרים שלמים ידועים לכל, $p > 3$ ראשוני, a, b מספרים שלמים זרים לp סודיים, ו $x \equiv g^a \pmod p$, $y \equiv g^b \pmod p$. אם ידוע a' כך ש $x \equiv g^{a'}$ אזי הסטודנט יכול לחשב:

$$y^{a'} \equiv (g^b)^{a'} \equiv g^{ba'} \equiv (g^{a'})^b \equiv x^b \equiv (g^a)^b \equiv g^{ab} \equiv key \pmod p$$