נושא חדש

הפעם אין לי בדיחה טובה

בעיה רגילה

- בהינתן מספר n הדפיסו את סכום המספרים $S_n = \sum_{i=1}^{n} i$.
  $n \leq 10^{18}$

- שאלה קלה לא?

- כולנו יודעים שמתקיים $S_n = \frac{n(n+1)}{2}$ אבל מה קורה אם התוצאה ממש גדולה?

אבל מה הבעיה

- Longlong מסוגל להכיל עד כ- 10^{18}, אבל מבחינת הדפסה התוצאה עשויה לעשות overflow ($10^{18} \cdot 10^{18}$)
- הדרך של אתרים לפתור את זה היא להשתמש במודולו, אבל בהכרח אחד ראשוני וגדול.

- הרעיון הוא שכדי שמספר יהיה זהה למספר אחר mod מספר ראשוני גדול p. הסיבה לבחירה הזו היא שמודולו גדול יותר מקטין את הסיכויים ששני מספרים שווים תחת המודולו "בטעות", והסיבה לראשוני תהיה ברורה יותר בהמשך (בכלליות ראשוניים משחקים יפה עם תורת המספרים).

- אם כך אז מה הבעיה פשוט נדפיס מודולו?

מה אנחנו כן יודעים?

- חיבור: $(mod\ c)$ $\quad a + b \equiv a \bmod c + b \bmod c$
- כפל: $(mod\ c)$ $\quad a \cdot b \equiv a \bmod c \cdot b \bmod c$
- חיסור: $(mod\ c)$ $\quad a - b \equiv a \bmod c - b \bmod c + c$ (כלומר בקוד: `(a - b + md) % md;`)

- מה לגבי חלוקה?

כרגע הבעיה – לחלק ב-2

- שימו לב שאם נניח שמכפלת שני מספרים ומודולו ניתנים להחלפה:
- (כלומר $a \cdot b \bmod c = (a \bmod c) \cdot (b \bmod c)$)
- עדיין נותרנו עם חלוקה ב-2 וזה לא מתחלף עם מודולו (נסו עם $p = 7, n = 3$).

- נשים לב שעבור 7 ניתן להכפיל כל מספר ב-4 ואז להפעיל מודולו 7 ולקבל בדיוק את התוצאה הנכונה.

מאיפה מגיע ה-4 המסתורי?

- אז ב1640 היה בחור כזה צרפתי שאהב מתמטיקה, פייר דו פרמה, והוא החליט שיש לו

  משפט מאוד מטורף שהוא יודע את ההוכחה אבל הוא לא רוצה לגלות לנו אותה.

  קוראים לו המשפט האחרון של פרמה, עשו עליו סרט.

ובנוסף הוא גם הודיע על הלמה הקטנה שלו, והיא האחת שאנחנו מדברים עליה היום. לכל ראשוני p ומספר שלם a שאינו מתחלק בp, ניתן להגיד:

$$a^{p-1} \equiv 1 \ (mod \ p)$$

שימו לב שאם a היה מתחלק בp אז בוודאי החזקה הייתה 0.

לאחר מכן

- לאחר מכן השתמשו בלמה הקטנה של פרמה כדי לכפול את שני הצדדים בהופכי תחת מודולו של a , וגילו כי

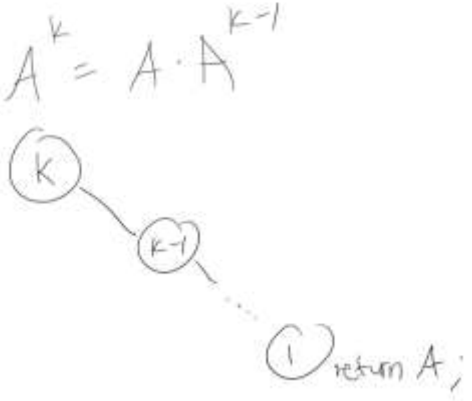
$$a^{p-2} \equiv a^{-1} \pmod p$$

וככה נוכל לחלק במספרים – פשוט נעלה אותם תחת מודולו בחזקה $p-2$ וקיבלנו את ההופכי!

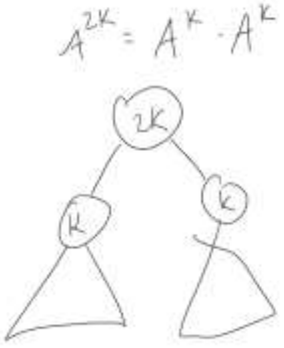
רגע איך מעלים בזמן טוב את המספר – לינארי בחזקה זה לא טוב כי אמרנו שהמספר גדול בדרך כלל.

העלאה בחזקה (מהר הפעם)

- נשים לב לעץ הרקורסיבי של חזקה:

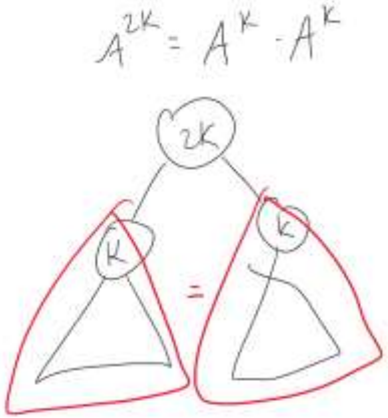


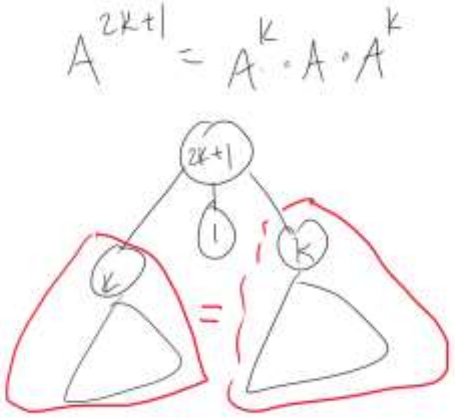
- בגלל שזה עץ, מה אם נשתדל לאזן אותו?
- במילים אחרות: שימו לב כי $A^{2k} = A^k \cdot A^k$



אני רואה בעיני הקטנה ....   דיפי (בערך)

- נשים לב כי אין שום סיבה להכנס לעץ השמאלי אם נכנסנו לימני, פשוט נשתמש בתוצאה שחושבה !
- במילים אחרות, הפונקציה הבאה:





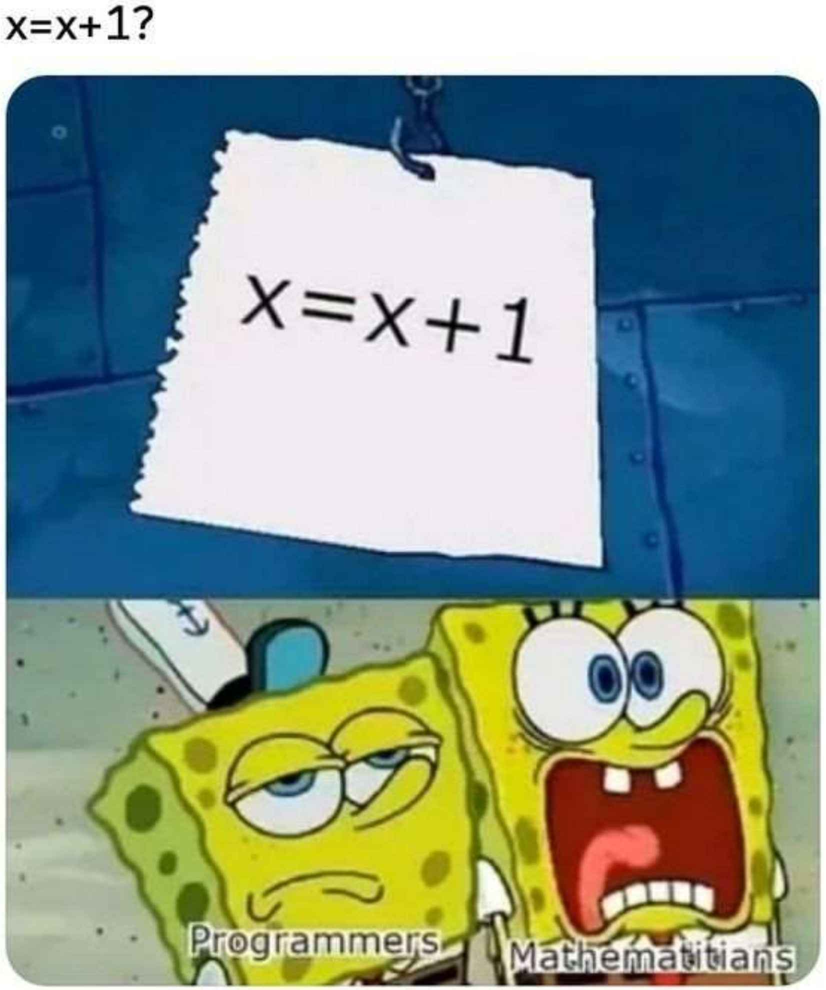

```
const int md = 1e9+7;
int pw(int a, int b){
    a %= md;
    if(b < 2) return b ? a : 1;
    int a_sqr = pw(a, b/2);
    return (((b&1) ? a : 1) * a_sqr % md) * a_sqr % md;
}
```

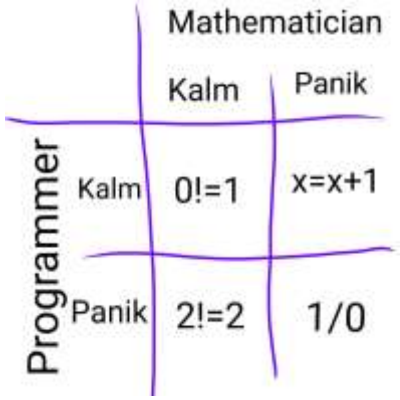
אפשר בלי רקורסיה?

- כן!
- נבצע כמו מקודם רק בכיוון ההפוך – נביט על הייצוג הבינארי של k , ונעבור עליו לפי סדר עולה, ונתחזק a בחזקה של חזקת 2 המתאימה לביט הנוכחי (זה פשוט יותר ממה שזה נשמע). אם הביט הנוכחי דולק ב-k , תכפיל את התוצאה בחזקה הנוכחית.

```
const int md = 1e9+7;
int pw(int a, int b){
    int res = 1;
    while(b > 0){
        if(b & 1) res = res * a % md;
        b /= 2;
        a = a * a % md;
    } return res;
}
```

מתמטיקה חישובית





math

חזרה על מה יש לנו כרגע

- חיבור
- חיסור
- כפל
- חילוק
- חזקה ($O(\log k)$)

- מה עוד אפשר לעשות?

מה לגבי עצרת?

- לינארי זה בערך הכי טוב שאפשר. בדרך כלל עושים $preprocessing$ ומחשבים לפני שקולטים בכלל קלט את כל העצרות למיניהן במערך, ע"י האיבר הקודם כפול האינדקס מודולו md .

- למה בערך?
- כי יש אלגוריתם שעושה משהו מעניין עבור מודולו p בזמן לינארי בו, אבל זה לא מספיק טוב לצרכינו (ולרמת הקורס).

- ככל שאנחנו מודאגים – נכנס לינארי בגודל המקסימלי שנדרשים לחשב עצרת.

מה לגבי בינום?

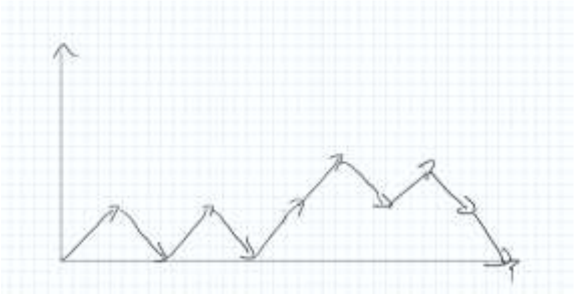
- אם ניתן לעשות עצרת וניתן לחלק ולהכפיל – קל לראות שגם בינום אפשר לעשות.
- $\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$

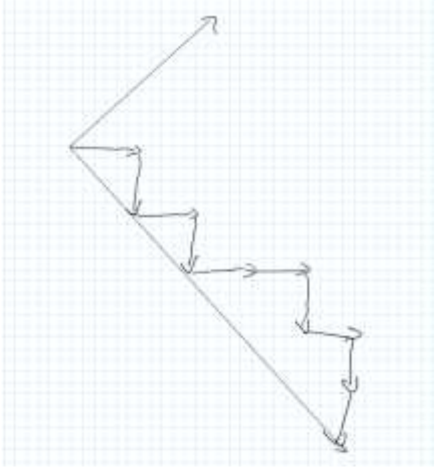
שאלה בקומבינטוריקה

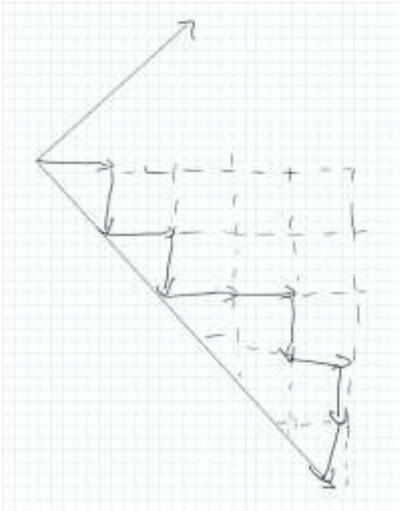
- יהי המישור הקרטזי. כמה דרכים תקינות יש להשתמש ב - n ווקטורים מבין $\searrow$, $\nearrow$ כך שהם לא ירדו מתחת לציר x ?

- חסמים:
- $1 \leq n \leq 10^6$

בואו נפתור שאלה בסיפי



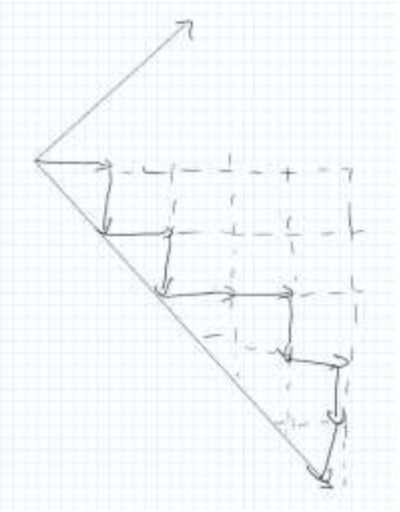




- הרבה יותר נוח לחשוב על בעיות של טבלאות מאשר המישור הקרטזי.
- בואו נסובב את הלוח ב-45 מעלות:
- הרבה יותר טוב. כעת הבעיה הופכת להיות:
- "כמה דרכים יש בטבלה $n \times n$ כאשר מותר לזוז ימינה ולמטה,

  ואסור לחצות את האלכסון הראשי?"

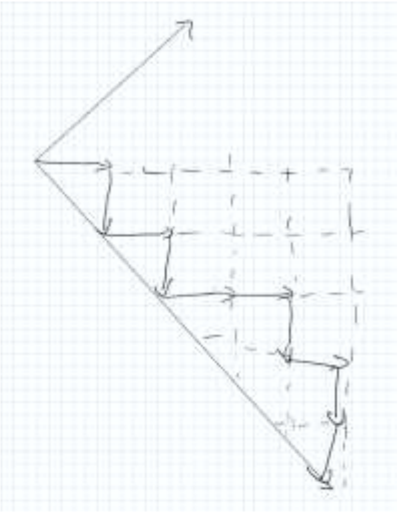
בואו נפתור שאלה בסיפי



- "כמה דרכים יש בטבלה $n \times n$ כאשר מותר לזוז ימינה ולמטה,

  ואסור לחצות את האלכסון הראשי?"
- שאלה קלה יותר – כמה דרכים שבהן זזים ימינה ולמטה יש בטבלה כזו?

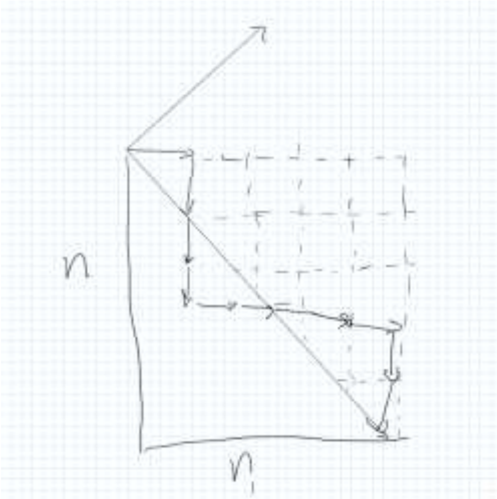
בואו נפתור שאלה בסיפי



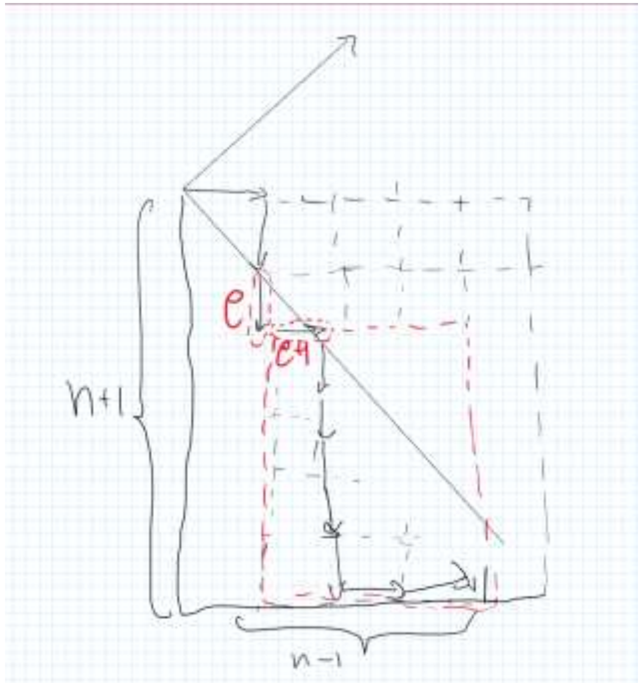
- "כמה דרכים יש בטבלה $n \times n$ כאשר מותר לזוז ימינה ולמטה,

  ואסור לחצות את האלכסון הראשי?"
- שאלה קלה יותר – כמה דרכים שבהן זזים ימינה ולמטה יש בטבלה כזו?
- תשובה: $\binom{2n}{n}$ וזאת כי יש בדיוק $2n$ צעדים, ובדיוק n מהם חייבים להיות למטה והשאר ימינה.
- כעת כמה כאלה יש שבוודאות עוברים בהן באלכסון הראשי?

בואו נפתור שאלה בסיפי

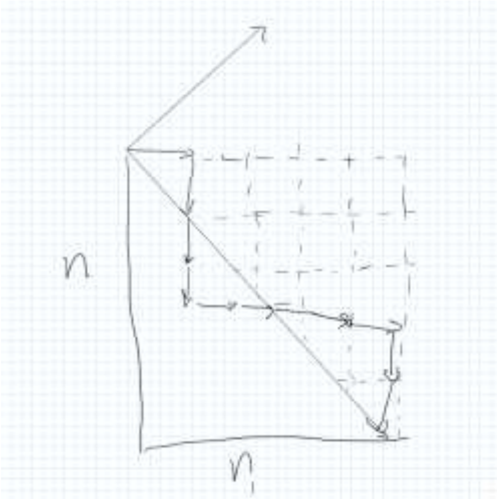


- כעת כמה כאלה יש שבוודאות עוברים בהן באלכסון הראשי?
- יהיה P מסלול שעובר מתחת לאלכסון, ויהי e האינדקס של הקשת הראשונה שהוא עובר בה, אשר חוצה מתחת לאלכסון. נביט על $e+1$:

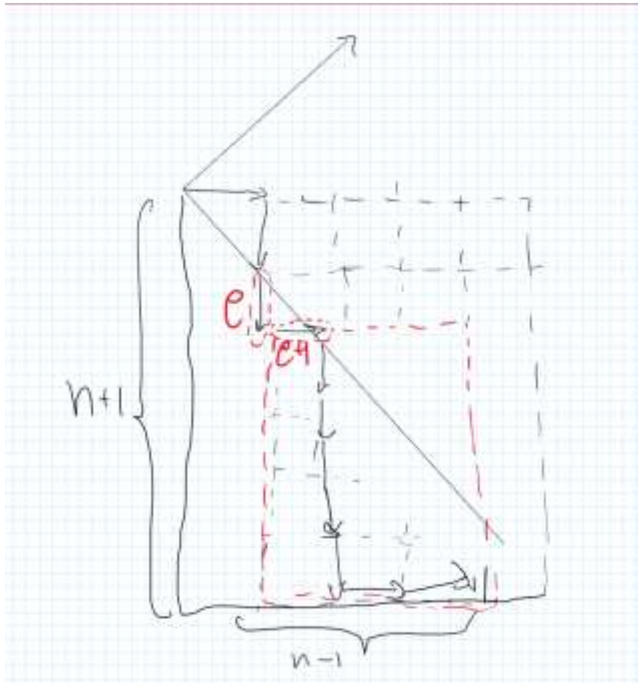


- אם ניקח את המשך המסלול החל מ $e+1$ (ולא e), ונעשה לו היפוך מראה על הציר של האלכסון, תמיד נקבל מסלול חדש שפונה ימינה ולמטה ונמצא בטבלה $(n-1)\times(n+1)$, וברור שכל מסלול בטבלה הזו יחצה את האלכסון – ומכאן יש התאמה חחע ועל והקבוצות האלה שוות בגודלן.

בואו נפתור שאלה בסיפי



- כעת כמה כאלה יש שבוודאות עוברים בהן באלכסון הראשי?
- במילים אחרות: התשובה שרצינו היא כמו כמות המסלולים שהולכים ימינה או למטה, אבל בטבלה $(n-1) \times (n+1)$ ומכאן התשובה היא $\binom{2n}{n-1}$.



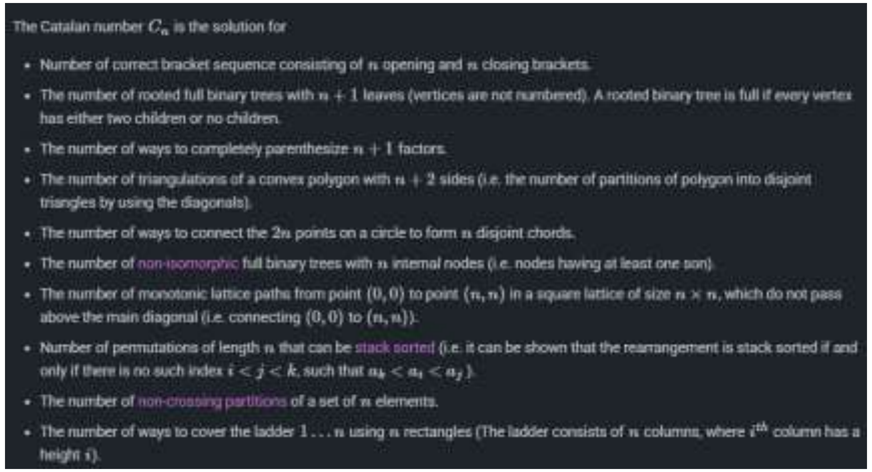
וכעת השגנו תשובה לשאלה ההתחלתית - כמה דרכים תקינות יש להשתמש ב - n ווקטורים מבין ↘ , ↗ כך שהם לא ירדו מתחת לציר x ?

תשובה: $\binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}$

מספרי קטאלאן

- המספר שחישבנו עכשיו נקרא מספר קאטלאן מסדר n : $C_n = \frac{1}{n+1}\binom{2n}{n}$

- הם פשוט מופיעים הרבה בשאלות של קומבינטוריקה אז חשוב שנכיר אותם ☺.
- הרבה:



The Catalan number C_n is the solution for

- Number of correct bracket sequence consisting of n opening and n closing brackets.
- The number of rooted full binary trees with $n+1$ leaves (vertices are not numbered). A rooted binary tree is full if every vertex has either two children or no children.
- The number of ways to completely parenthesize $n+1$ factors.
- The number of triangulations of a convex polygon with $n+2$ sides (i.e. the number of partitions of polygon into disjoint triangles by using the diagonals).
- The number of ways to connect the $2n$ points on a circle to form n disjoint chords.
- The number of non-isomorphic full binary trees with n internal nodes (i.e. nodes having at least one son).
- The number of monotonic lattice paths from point $(0,0)$ to point (n,n) in a square lattice of size $n \times n$, which do not pass above the main diagonal (i.e. connecting $(0,0)$ to (n,n)).
- Number of permutations of length n that can be stack sorted (i.e. it can be shown that the rearrangement is stack sorted if and only if there is no such index $i < j < k$, such that $a_k < a_i < a_j$).
- The number of non-crossing partitions of a set of n elements.
- The number of ways to cover the ladder $1 \dots n$ using n rectangles (The ladder consists of n columns, where i^{th} column has a height i).

זהו להיום

עד הפעם הבאה