תרגול 8

נושאי התרגול

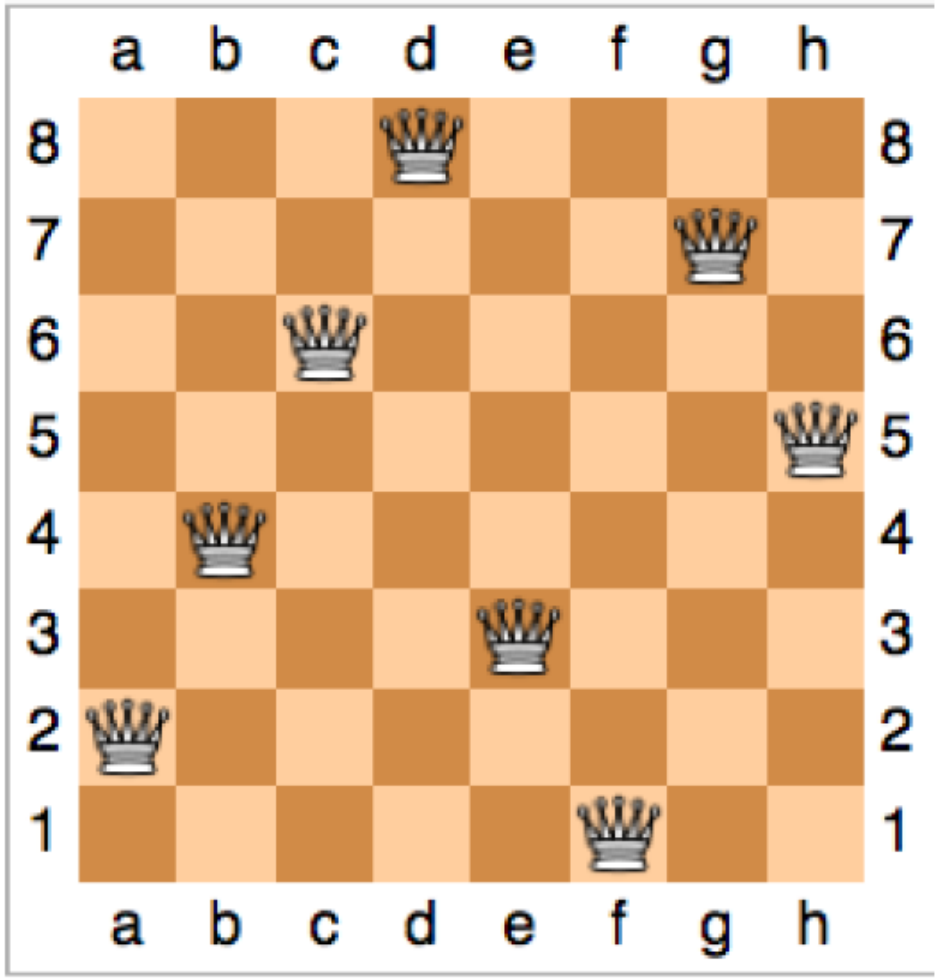
- רקורסיה (המשך)
- קריפטוגרפיה-
  - מספרים ראשוניים.
  - Diffie Hellman

בעיית N המלכות

- תיאור הבעיה:

בכמה דרכים ניתן לסדר N מלכות בלוח שחמט בגודל $N \times N$?

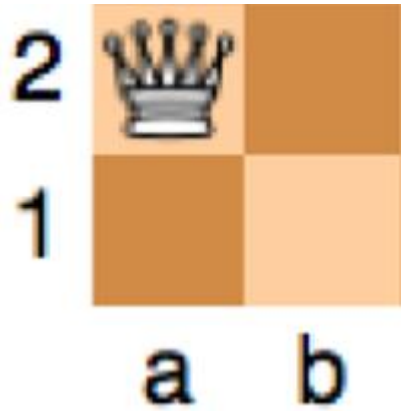
האתגר: אף מלכה לא מאיימת על מלכה אחרת.



N=8

דוגמא

- האם ניתן לסדר 2 מלכות על לוח בגודל 2×2?
- מה לגבי 3 מלכות על לוח בגודל 3×3?



N=2

בעיית N המלכות: כיוון כללי

- נבנה פתרון בצורה הדרגתית.
- בכל קריאה רקורסיבית נקבל כקלט פתרון חלקי בו מוקמו k מלכות.
- ננסה להרחיב את הפתרון ולמקם את המלכה ה $(k+1)$
- שאלה חדשה: בכמה דרכים ניתן **<u>להשלים</u>** לוח שיש בו k מלכות שכבר מיקמנו

בעיית N המלכות: תנאי העצירה

מתי נסיים?

1. סידרנו N מלכות ← סידור חוקי. נחזיר 1. (יש רק השלמה אחת – לא לשנות כלום בלוח).
2. ואם סידרנו $k < N$ ואין לנו איך להמשיך?

מקרה (2) יפתר מעצמו.

נסיון ראשון

- בהינתן לוח עם k מלכות, נבדוק את כל $N^2 - k$ האפשרויות למקם את המלכה הבאה.
  - כמה בנים יש לכל צומת ברמה ה-k?
  - האם יש חישובים מיותרים?
  - **האם בהכרח כל פתרון חוקי נספר פעם אחת בלבד?**

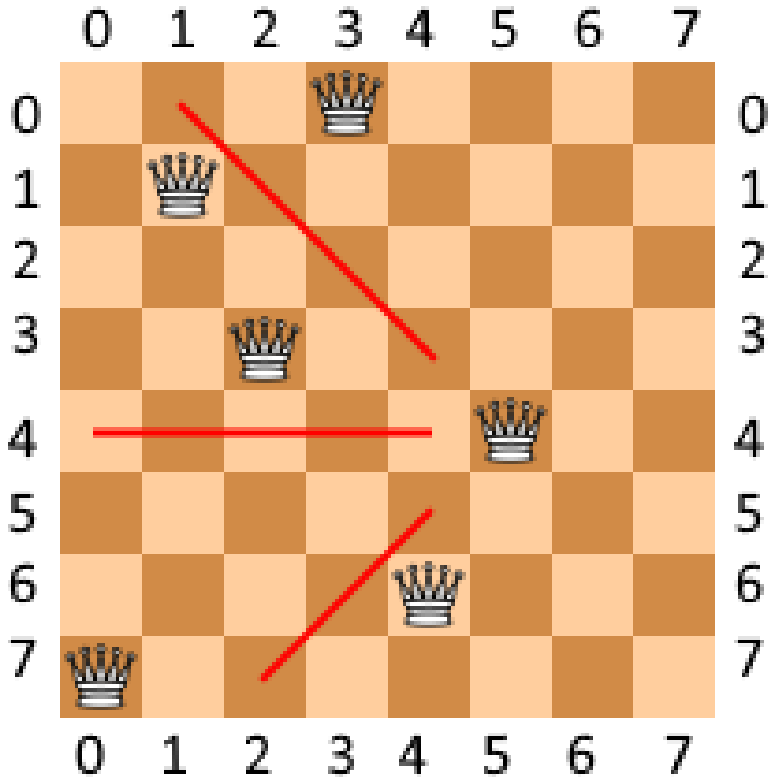
- נחפש פתרון מוצלח יותר

נסיון שני לפתרון

- מה המספר המקסימלי של מלכות בעמודה אחת?
- ומה המינימלי?
- הקלט: מיקום ב-k העמודות הראשונות (בהתחלה $k = 0$)
- איך מייצגים את הקלט? הרשימה $partial$
- צעד הרקורסיה: לכל מיקום חוקי j בעמודה ה-$k + 1$ נקרא רקורסיבית עם $partial + [j]$
- נסכום פתרונות
- איך בודקים אם מיקום הוא חוקי???

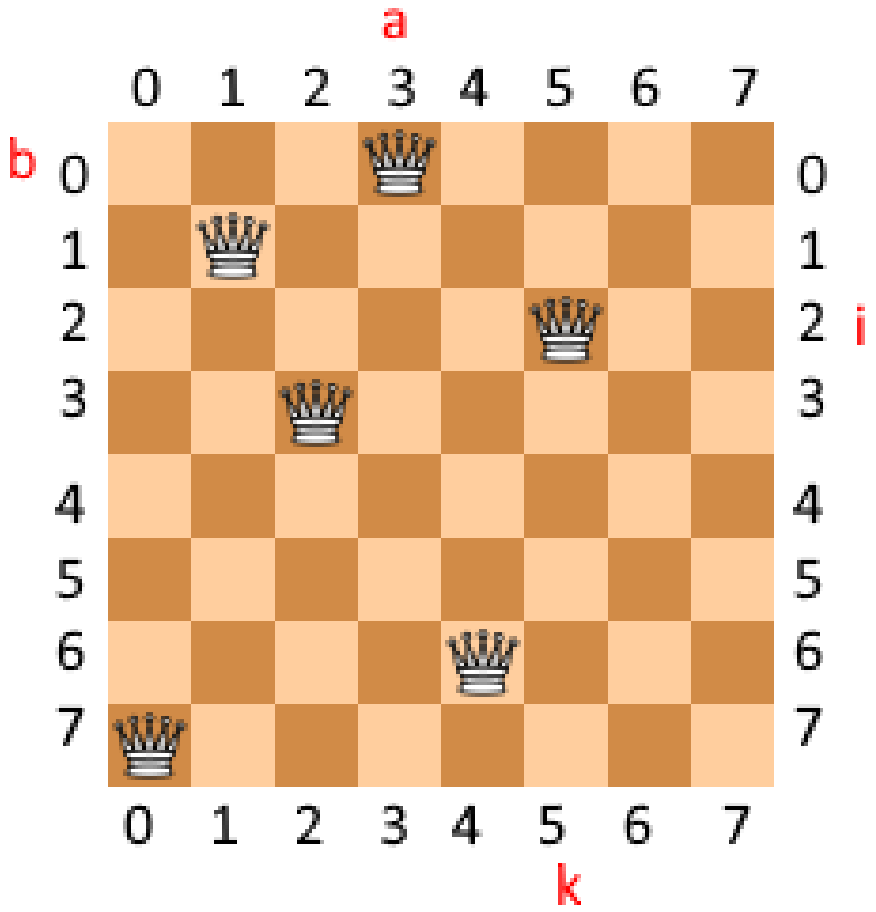
נסיון שני לפתרון

- בלוח בתמונה אפשר למקם מלכה בעמודה 5 ושורה 4
- איך יודעים אם אפשר למקם?
- קל יותר לבדוק אם **<u>אי אפשר</u>** למקם



נסיון שני לפתרון

- בלוח בתמונה אי-אפשר למקם מלכה בעמודה 5 ושורה 2
- איך פוסלים מיקום?
  - שורה לא חוקית
  - או אלכסון עולה שמאלה לא חוקי
  - או אלכסון יורד שמאלה לא חוקי
  - למה לא צריך לבדוק אלכסונים ימינה?
- פה: $2 = 0 + (5 - 3)$
- בנוסף: $2 = 7 - (5 - 0)$



בעיית N המלכות: סיבוכיות זמן

נראה במקביל חסם עליון ותחתון על גודל העץ, לפי מספר הבנים המינימלי/מקסימלי שיש לכל צומת בעץ על פי הרמה שלו.

זמן הריצה לינארי ב-N (ונראה שזניח מבחינתנו)

רמה	מספר בנים מקסימלי	מספר בנים מינימלי
0	N	N
1	N	N - 3
2	N	N - 6
…	…	…
k	N	N - 3k

בעיית N המלכות: סיבוכיות זמן

כעת נחסום את גודל העץ T_N מלמעלה ומלמטה:

חסם **<u>עליון</u>**:

- בדרגה ה-k של העץ לכל צומת יש <u>לכל היותר</u> $N-k$ בנים
- לכן מספר הצמתים בעץ הוא <u>לכל היותר</u>

$$1+N+N\cdot(N-1)+\cdots+N!=\sum_{i=0}^{N}\frac{N!}{i!}\le N!\cdot\sum_{i=0}^{\infty}\frac{1}{i!}=N!\cdot e=O(N!)$$

- מתרגיל בית 3 $e\cdot N!=2^{\theta(NlogN)}$

חסם **<u>תחתון</u>**:

- בדרגה ה-k עבור $k<N/3$ לכל צומת יש <u>לפחות</u> $N-3k$ בנים
- נסתכל על העמודה ה-$k=N/6$. מספר הצמתים בה הוא <u>לפחות</u>:

$$N\cdot(N-3)\cdot(N-6)\cdot\ldots\cdot\left(N-\frac{N}{2}\right)\gg\left(\frac{N}{2}\right)^{\frac{N}{6}}=2^{\theta(NlogN)}$$

- בסה"כ $2^{\theta(NlogN)}\le T_N\le 2^{\theta(NlogN)}$

המשפט הקטן של פרמה

יהי p מספר ראשוני כלשהו, אזי לכל $1 \leq a < p$ מתקיים כי

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

"עדים" לפריקות של מספר

עד הוא פיסת מידע שיכולה לשמש בכדי להוכיח טענה כלשהי.

למשל: איזה עד ישכנע אותנו שהמרחק מירושלים לחיפה קטן מ-300 ק"מ?

איזו בעיה כבר ראינו בקורס שאפשר לנסח עם עדים?

הבעיה: האם m פריק?

נסתכל על שלושה סוגי עדים לבעיה זו.

סוגי "עדים" לפריקות

1. $FACT_m$ - קבוצת המחלקים של m. כל $1 < b < m$ כך ש: $m \% b = 0$
   - למשל $5 \in FACT_{10}$
2. GCD_m - קבוצת הלא-זרים של m. כל $1 < b < m$ כך ש:
   $\gcd(b,m) > 1$
   - למשל $8 \in GCD_{10}$ כי $\gcd(8,10) = 2$, אז 2 הוא מחלק של 10, ולכן 10 פריק.
3. $FERM_m$ - עדי פרמה של m. כל $1 < a < m$ כך ש:
   $a^{m-1} (mod\ m) \not\equiv 1$
   - למשל $3 \in FERM_{10}$ $(3^9\ mod\ 10 = 19683\ mod\ 10 = 3 \neq 1)$

סוגי "עדים" לפריקות

טענה: $FACT_m \subseteq GCD_m \subseteq FERM_m$.

תזכורת: חשבון מודולרי

נאמר כי $a = b \ mod \ c$ אם קיים $t \in \mathbb{Z}$ כך ש:

$$a = t \cdot c + b$$

למשל, $13 = 1 \ mod \ 12$ (צריך להיות מוכר לנו...)

באופן שקול: $a - b$ (וגם $b - a$) הוא כפולה (שלמה!) של c

תובנות בסיסיות לגבי מחלקים

אם $t > 1$ וגם t מחלק את r אז t לא מחלק את $r - 1$

אם t מחלק את r אז t מחלק כל כפולה של r

הוכחה: $FACT_m \subseteq GCD_m$

נניח ש-$1 < a < m$ מחלק את m.

מה הוא $\gcd(a,m)$?

הוכחה: $GCD_m \subseteq FERM_m$

ניקח $b \in GCD_m$ ונסמן $\gcd(b,m) = t > 1$

כיוון ש-t מחלק את b הוא מחלק את b^{m-1} אבל לא את $b^{m-1} - 1$

ננית בשלילה ש-$b \notin FERM_m$ ולכן $b^{m-1} = 1 \; mod \; m$

באופן שקול $b^{m-1} - 1$ הוא כפולה של m

אבל t מחלק את m ולכן מחלק כל כפולה של m, הגענו לסתירה!

מסקנה: $b^{m-1} \neq 1 \; mod \; m$

בדיקת ראשוניות רנדומלית

- אלגוריתם: נגריל a ונבדוק אם a הוא עד
- איזה מין עד?
- מה בעייתי בבדיקה $a \in FACT_m$ (רמז: $m = p^2$)
- מה בעייתי בבדיקה $a \in GCD_m$ (רמז: עדיין $m = p^2$)

בדיקת ראשוניות רנדומלית - ניתוח

- אם $m = p^2$ אז $GCD_m = \{p, 2p, 3p, \dots, (p-1)p\}$
- ההסתברות ליפול על $a \in GCD_m$ היא $\frac{p}{p^2} = \frac{1}{p} = 1/\sqrt{m}$
- בממוצע, נצפה להצלחה אחרי $O(\sqrt{m})$ בדיקות
- כלומר – ביצועים ממוצעים כמו ה-WC של חיפוש נאיבי

בדיקת ראשוניות רנדומלית - ניתוח

- אם $m = p^2$ אז $FACT_m = \{p\}$
- ההסתברות ליפול על $a = p$ היא $\frac{1}{p^2} = 1/m$
- בממוצע, נצפה להצלחה אחרי $O(m)$ בדיקות
- כלומר – ביצועים ממוצעים גרועים יותר מה-WC של חיפוש נאיבי!

בדיקת ראשוניות ע"י עדים

- אלגוריתם: נגריל a ונבדוק אם $a \in FERM_m$
- מה יקרה אם m ראשוני?
- מה יקרה אם m פריק?
- מה לגבי ביצועים?

בדיקת ראשוניות

ה-"חוזק" של פרמה: אם m פריק, $|FERM_m| \geq \frac{m}{2}$. תמיד?

כלומר, הסיכוי ש-$a \in FERM_m$ הוא לפחות $\frac{1}{2}$!

זה מספיק טוב לנו?

מה יקרה אם נחזור על התהליך 100 פעמים?

הסיכוי לטעות

- נניח שm הוא פריק שאינו "מספר קרמייקל"
- אזי עבור $a < m$ אקראי יחיד $\Pr(a \in FERM_m) \geq \frac{1}{2}$
- נחזיר תשובה שגויה אם לכל a אקראי שבחרנו מתקיים ש $a \notin FERM_m$
- הסיכוי לטעות הינו לכל היותר $\frac{1}{2^{100}}$ (הסיכוי לטעות בכל אחת מ100 ההגרלות הבלתי תלויות)

בדיקת ראשוניות

הערות:

- במחברת ניתן לראות כי הקוד טועה עבור מספרי קרמייקל (גדולים). למזלנו, מספרי קרמייקל הם מאוד נדירים ולכן לא נטעה לרוב.
- למספרי קריימקל יש עדים (למשל קבוצת כל המחלקים של המספר), אך הם מועטים. למעשה, מספרי קרמייקל הם בדיוק המספרים בהם $GCD_m = FACT_m$.

משפט המספרים הראשוניים

עבור n מספיק גדול, צפיפות המספרים הראשוניים בעלי n ביטים היא $O\left(\frac{1}{n}\right)$.

דיפי-הלמן

אליס ובוב רוצים לשלוח ביניהם הודעות מוצפנות.
יש להם:

- פונקציית הצפנה enc(msg, key)→ enc_msg
- פונקציית פענוח dec(enc_msg, key)→msg
- עליהם להחליט על מפתח סודי משותף key

דיפי-הלמן

פרוטוקול למציאת מפתח סודי משותף:

לבוב יש:

p, g

לאליס יש:

מספר ראשוני – p

g < p

דיפי-הלמן

למדנו בכיתה את הפרוטוקול הצפנה של דיפי הלמן.

תזכורת:

לבוב יש: p,g

$b < p$

לאליס יש: p,g

$a < p$

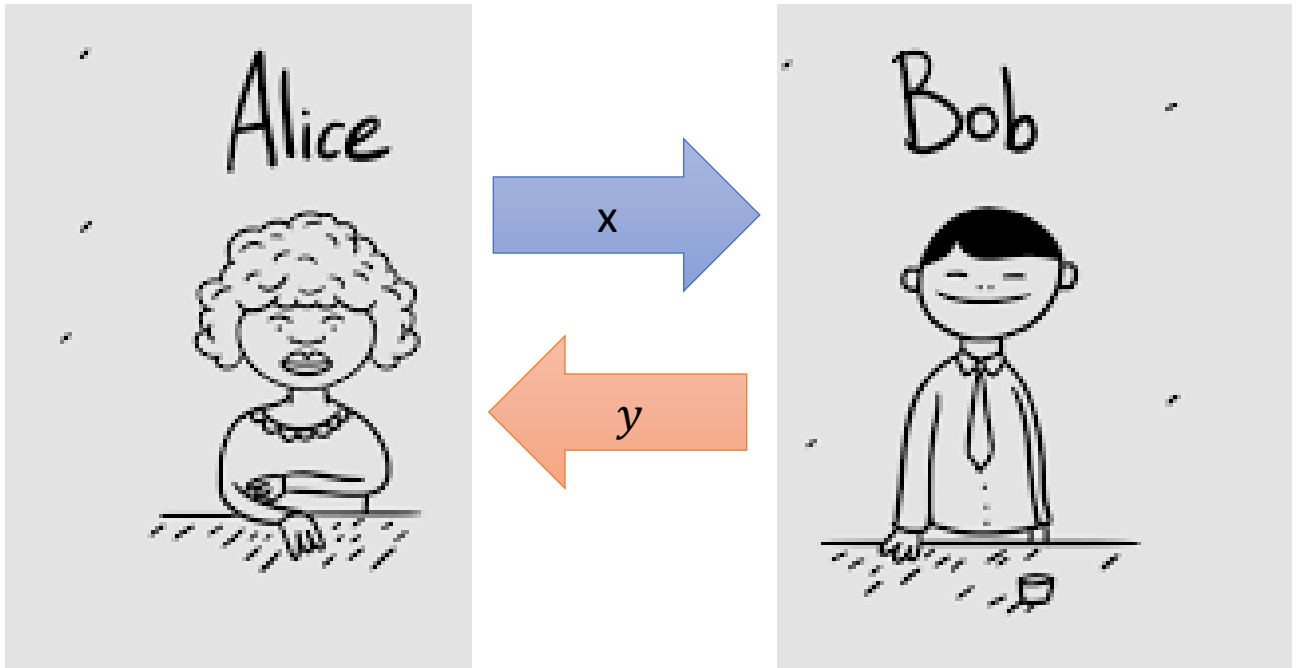
דיפי-הלמן

למדנו בכיתה את הפרוטוקול הצפנה של דיפי הלמן.

תזכורת:

לאליס יש: p,g,a

$x \equiv g^a (mod\ p)$



לבוב יש: p,g,b

$y \equiv g^b (mod\ p)$

דיפי-הלמן

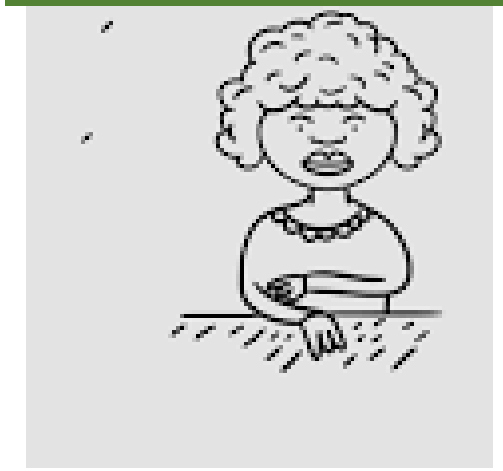
למדנו בכיתה את הפרוטוקול הצפנה של דיפי הלמן.

תזכורת:

לאליס יש:
p,g,a,x,y

ה-"קסם":
$(g^a \ mod \ p)^b \ mod \ p = (g^b \ mod \ p)^a \ mod \ p$

לבוב יש:
p,g,b,x,y



key
$\equiv y^a (mod \ p)$
$\equiv g^{ab} (mod \ p)$

key
$\equiv x^b (mod \ p)$
$\equiv g^{ab} (mod \ p)$

דיפי-הלמן

ראשית, נמצא ראשוני:

```
def find_prime(n):
    """ find random n-bit long prime """
    while(True):
        candidate = random.randrange(2**(n-1), 2**n)
        if is_prime(candidate):
            return candidate
```

כמה זמן זה ייקח?

דיפי-הלמן

```
def DH_exchange(p):
    """ generates a shared DH key """
    g = random.randint(1, p - 1)
    a = random.randint(1, p - 1)# Alice's  secret
    b = random.randint(1, p - 1)# Bob's  secret
    x = pow(g, a, p)
    y = pow(g, b, p)
    key_A = pow(y, a, p)
    key_B = pow(x, b, p)
    #the next line is different from lecture
    return g, a, b, x, y, key_A #key_A=key_B
```

סימולציה (דו-צדדית):

זמן ריצה (בדקו!): $O(n^3)$