שאלה מס' 1 (30%)

<u>הרצת FFT</u>. (בשאלה זו סעיף א' כן להגשה, **וסעיף ב' לא להגשה**). נביט בפולינום $p(x) = x^3 + 2x^2 - 3x - 1$ שדרגתו קטנה מ-4. רישמו את כל החישובים מעל שדה המרוכבים (לרבות הקריאות הרקורסיביות) עבור:

(א) הרצת FFT מסדר 4 (הרצת $FFT(\cdot, \omega_4)$) על מקדמי הפולינום.

<u>א) P(x):</u>

$$P(x) = x^3 + 2x^2 - 3x - 1 \to \underbrace{-1}_{a_0} \underbrace{-3}_{a_1}x + \underbrace{2}_{a_2}x^2 + \underbrace{1}_{a_3}\cdot x^3$$

$w = i$

נקבל:

$FFT((-1,-3,2,1), w)$

$FFT((-1,2), w^2)$

$FFT((-1,), w^4)$

$return\ (-1,)$

$FFT((2,), w^4)$

$return\ (-2,)$

$return\ (-1-2\cdot w^2, -1+2\cdot w^2) = (1,-3)$

$FFT((-3,1), w^2)$

$FFT((-3,), w^4)$

$return\ (-3,)$

$FFT((1,), w^4)$

$return\ (1,)$

$return\ (-3-1\cdot w^2, -3+1\cdot w^2) = (-2,4)$

$f(1) = 1+(-2) = -1$

$f(i) = -3+i\cdot(-4) = -3-4i$

$f(-1) = 1+(-1)\cdot(-2) = 3$

$f(-i) = -3+(-i)\cdot(-4) = -3+4i$

return $(-1, -3-4i, 3, -3+4i)$

שאלה מס' 2 (35%)

<u>כפל שלמים בגישת FFT</u>: כפל מספרים שלמים הינה בעיה אלגוריתמית בעלת חשיבות מעשית עליונה. לשם פשטות להלן נניח ששני המספרים המוכפלים שווי אורך (לשניהם ייצוג בינארי של n ביטים), וששניהם חיוביים. בתרגיל זה יוצגו עיקר הרכיבים באחד האלגוריתמים היעילים ביותר המוכרים כיום לכפל שלמים: <u>זמן הריצה</u> שלו הוא $\Theta(n\log^2 n)$ בלבד.

זכור, אלגוריתם הכפל של **Karatsuba** מבוסס על פיצול הספרות של כל קלט לשני בלוקים שווי גודל, ורץ בזמן $\Theta(n^{\log_2 3})$. הציגו אלגוריתם משופר, שמחלק כל קלט ל- (n/k) בלוקים בגודל k. היעזרו באלגוריתם ה-FFT לפתרון תתי-הבעיות המתקבלות. הניחו לשם פשטות (וללא הצדקה), כי ההכפלות שמתבצעות במהלך הקריאות הרקורסיביות אינן מגדילות את אורכם של המספרים, ולכן ניתן לממש הכפלות אלו בצורה תמימה תוך ביצוע $\Theta(k^2)$ פעולות על ביטים. בחרו לבסוף את גודלם של הבלוקים להיות $k=\log n$.

<u>הסבר:</u>

יהי x,y מספרים בייצוג בינארי באורך n.

נפרק אותם ל- $\frac{n}{k}$ חלקים:

$$x=\sum_{i=1}^{\frac{n}{k}} x_i$$

$$y=\sum_{i=1}^{\frac{n}{k}} y_i$$

נריץ אלגוריתם FFT על $(x_i)_i^{\frac{n}{k}}$ ועל $(y_i)_i^{\frac{n}{k}}$ (כמו $(a_i)_i^n$ באלגוריתם "רגיל")

קיבלנו 2 פולינומים עם $\frac{n}{k}$ נקודות המייצגות כל אחד מהפולינומים כנ"ל.

ניקח

$$z = x(w_i)\cdot y(w_i)$$

נריץ IFFT על z ונקבל מקדמים של $(z_i)_i^{\frac{n}{k}}$

עבור כל מקדם k נספים את z. ונחזיר את המספר מיוצר בחזרה לבסיס עשרוני.

נכונות:

נובע ישירות מ- FFT ומ- IFFT, ומהמרה של מספר לבסיס 10 כרגיל.

סיבוכיות:

חלוקה ל- $\frac{n}{k}$ חלקים: $\Theta(n)$

הרצת FFT: $\Theta(n\log^2(n))$

נקבל:
$$\begin{cases} T(n) = 2T\left(\frac{n}{2}\right) + \frac{n}{2k}\Theta(k^2) \\ k = \log(n) \end{cases}$$

$$T(n) = \underbrace{2}_{a}T\left(\underbrace{\frac{n}{2}}_{b}\right) + \frac{n}{2\log(n)}\Theta\left(\log^2(n)\right)$$

לפי שיטת האב

$$T(n)=\Theta\left(n\log^2(n)\right)$$

הרצת IFFT: $\Theta(n\log^2(n))$

בדומה ל- FFT, נקבל את אותה סיבוכיות.

$$\boxed{\text{וקיבלנו: } \Theta(n\log^2(n))}$$

שאלה מס' 3 (35%)

<u>כפל מטריצות ריבועיות (Strassen)</u>. ברצוננו להכפיל שתי מטריצות ריבועיות A, B מסדר $n \times n$ מעל שדה מסוים. תוצאת המכפלה הינה מטריצה $C = A \times B$ מסדר $n \times n$. נדרשות בדיוק n^3 פעולות של כפל-סקלרים (סקלר=מספר בשדה) אם מחשבים את C באופן ישיר לפי ההגדרה $C_{i,j} = \sum_{1 \le k \le n} A_{i,k} \times B_{k,j}$.

בשאלה זו נציג אלגוריתם רקורסיבי מחוכם, שמצמצם באופן ניכר את מספר הכפלות-הסקלרים (שנחשבות יקרות ביחס לפעולות של חיבור וחיסור של סקלרים). נניח לשם פשטות, כי n הינו חזקה של 2, כך שניתן "לפרק" כל מטריצה ל-4 תתי-מטריצות מסדר $(\frac{1}{2}n) \times (\frac{1}{2}n)$, כדלקמן.

$$A = \left(\begin{array}{c|c} a & b \\ \hline c & d \end{array}\right), B = \left(\begin{array}{c|c} e & g \\ \hline f & h \end{array}\right), C = \left(\begin{array}{c|c} r & s \\ \hline t & u \end{array}\right).$$

שימו לב, שמהגדרת כפל מטריצות מתקיים:

$$r = a \times e + b \times f \qquad t = c \times e + d \times f$$
$$s = a \times g + b \times h \qquad u = c \times g + d \times h$$

כעת נחשב את 7 המטריצות:

$$P_1 = a \times (g - h) \qquad P_5 = (a + d) \times (e + h) \qquad P_3 = (c + d) \times e$$
$$P_2 = (a + b) \times h \qquad P_6 = (b - d) \times (f + h) \qquad P_4 = d \times (f - e)$$
$$P_7 = (a - c) \times (e + g)$$

(א) הסבירו כיצד לחשב את 4 המטריצות הנדרשות, r, s, t, u באמצעות פעולות **<u>חיבור וחיסור</u>** בלבד על המטריצות $P_1, \ldots, P_7$ (אסורה הכפלה של מטריצות). למשל $u = -P_7 + P_5 + P_1 - P_3$.

חישוב של s: $P_1 + P_2$

חישוב של t: $P_3 + P_4 = (c + \cancel{d}) \times e + d \times (f - \cancel{e}) = c \times e + d \times f$

חישוב של r: $P_5 + P_6 + P_4 - P_2$

(ב) בדקו **<u>כמה הכפלות של סקלרים</u>** דרושות בסך הכל לאלגוריתם הרקורסיבי שתואר בשאלה זו.

1. נוכל $\Theta(n^2)$, או במדויק: $n^2 \cdot \frac{7}{4}$

2.

נכונות

$P_3 = c \times e + d \times e$

$P_4 = d \times f - d \times e$

$P_1 = ag - ah$

$P_2 = ah + bh$

$P_5 = ae + de + ah + dh$

$P_6 = bf + bh - df - dh$

$P_7 = ae + ag - ce - cg$

$S = ag + bh$

$r = ae + bf$

$P_1 + P_2 = ag - \cancel{ah} + \cancel{ah} + bh$

$= ag + bh = S$

$P_5 + P_6 = \overset{r}{\cancel{ae + bf}} + de + ah + bh - df$

$+ P_4 = ah + bh$

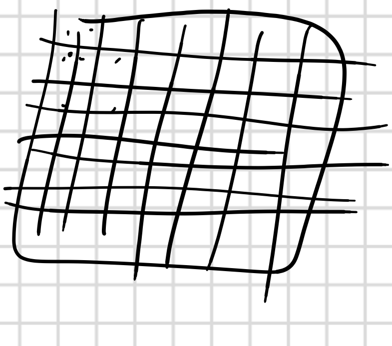
$- P_2 = 0$

בניית $T(n)$:

$$T(n) = 7T\left(\frac{n}{2}\right) + \Theta(1)$$

$\overset{2^2}{4 \times 4} = 4 \cdot 7$

$8 \times \overset{2^3}{8} = 16 \cdot 7$



$2^k \times 2^k = (2^{k-1})^2 \cdot 7$

$n = 2^k$

$$n \times n = \left(\frac{n}{2}\right)^2 \cdot 7 = \boxed{n^2 \cdot \frac{7}{4}} = \Theta(n^2)$$