

נבחן את כמות הפעולות שמבצעת האלגוריתם הכפול  
 של שני מספרים  $A, B$  בק, ש  $n_A, n_B$  מספרי הביטים  
 של  $A, B$  בהתאמה. מבצעים בקיור  $n_A \cdot n_B$  פעולות  
 עבור כל הביטים ולערוך  $n_A \cdot n_B$  פעולות עבור חיבור  
 הביטים (נראה בהמשך) שפחות הפעולות המקוריות אין  
 השפעה על סיבוכיות החזקה שנחשב. למכפלה  $n_A + n_B$  ביטים  
 יהיו  $a, b$  מספרים בק, ש  $n$  מספר הביטים ב  $a$   
 ו  $m$  מספר הביטים ב  $b$ .

נשים לב שמספר פעולות הכפל תלוי ב  $2^{\text{power}}$   
 (ומכאן באופן ישיר גם הכפל של המספרים הארוכים ביותר)  
 מתקבל אם בכל איטרציה בעילאה ה  $\text{while}$  נקבל  
 ש  $b$  אי-זוגי. אכן קורה עבור מספרים מהצורה  $1 - 2^k = b$   
 יהי  $\lfloor \log_2 b \rfloor \leq i \leq 0$  מספר האיטרציות בעילאה ה  $\text{while}$   
 (מתחילים עם  $i = 0$ ). עבור  $i = 0$  מספר הביטים של  $a$  בתחילת  
 בעילאה הוא  $n$ , ובסופה  $2n$  ( $a \cdot a = a + n \leftarrow 2n$ )  
 ומספר הביטים של  $\text{result}$  בתחילת בעילאה הוא  $n$  ובסופה  $n$   
 ( $\text{result} = 1 \cdot a$ ). מאינדקסים פשוטים, באיטרציה ה-  $i$  מספר  
 הביטים של  $a$  בתחילת בעילאה הוא  $n \cdot 2^i$  ושל  $\text{result}$  הוא  
 $n \cdot (2^i - 1)$ , שתיים אלו הן כאלו  $n \cdot 2^i$  מחוסר השפעה על

הסיבוכיות הסופית: אף שהקורצור  $a = a \cdot a$ ,  $\text{result} = \text{result} \cdot a$   
 מוריד  $2 \cdot (n \cdot 2^i)^2$  פעולות כל אחת, אף סק, כל הפעולות:

$$\sum_{i=0}^{\lfloor \log_2 b \rfloor} 2 \cdot \sum_{(*)} (n \cdot 2^i)^2 = \sum_{i=0}^m 4 \cdot (2^2)^i \cdot n^2 = 4n^2 \cdot \sum_{i=0}^m 4^i$$

סכום סדרה  
 הנדסית

$$4 \cdot n^2 \cdot \frac{1 \cdot 4^{m+1} - 1}{3} = \frac{4}{3} \cdot n^2 (4^{m+1} - 1) \leq \frac{4}{3} \cdot n^2 \cdot 4^{m+1}$$

ומכאן הסיבוכיות של  $2^{\text{power}}$  היא  $O(4^{m+1} \cdot n^2)$