

Left-Right Binary Exp.

$$P(2) = ? \quad a^{p(2)}$$

$$I = 3 \quad 2 \quad 1 \quad 0$$
$$B = 1 \quad 1 \quad 0 \quad 1$$

$$p(1) = a^1$$

$$i = I - 1$$

$$i = 2 \rightarrow p = 2p + b_i \quad b_i = 1$$

$$I = 3$$
$$p = 2 \cdot 1 + 1$$
$$= 3$$

Right to Left

$a^n \rightarrow$ hasplenek ten

$$Q^n = \sigma^{b_I 2^I + \dots + b_i 2^i + \dots + b_0} \quad i = I-1$$

$$= \sigma^{b_I 2^I} \dots \sigma^{b_i 2^i} \dots \sigma^{b_0 2^0} \rightarrow \text{baslangic: } a^{2^i} = 1 = a \text{ olun}$$

$$a^{2^i} = \left(a^{\frac{2^i}{2}}\right) = \left(a^{2^{i-1}}\right)^2$$

$$Q^{b_i 2^i} = ? \rightarrow \begin{cases} a^{2^{i-1}} \\ 1 \end{cases} \quad \begin{matrix} b_i = 1 \\ b_i = 0 \end{matrix}$$

$$\text{if } \begin{matrix} b_0 = 1 & \text{ise} & p = a \\ b_0 = 0 & \text{ise} & p = 1 \end{matrix}$$

~~8~~ $\rightarrow ? \rightarrow$

1	0	0	0	$\rightarrow ?$
I = 3	2	1	0	$\rightarrow w_0 = 0$ obs: for $p = 1$

(Arrows indicate the sequence of operations: 1 to 3, 3 to 2, 2 to 1, 1 to 0)

$i = 1$ iter $\rightarrow t = a \cdot a \rightarrow a^2$

$i = 2$ iter $\rightarrow t = t \cdot t \rightarrow a^2 \cdot a^2 = a^4$

$i = 3$ iter $\rightarrow t = t \cdot t \rightarrow a^4 \cdot a^4 = a^8$

~~13~~ $\rightarrow ? \rightarrow$

1	1	0	1
3	2	1	0

$\rightarrow w_0 = 1$ for $p = a$

Binary Exponentiation

$$\begin{array}{c}
 013 \\
 \swarrow
 \end{array}$$

$$13 \rightarrow \begin{array}{cccc} 1 & 1 & 0 & 1 \\ \swarrow & \downarrow & \downarrow & \downarrow \\ b_3 & b_2 & b_1 & b_0 \end{array} \rightarrow n = b_0, b_1, b_2 \text{ or } b_3 \text{ does not}$$

$$\begin{aligned}
 13 &\rightarrow 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^0 \\
 &\quad 1 \cdot 8 + 1 \cdot 4 + 1 \cdot 1 \\
 &\quad = 8 + 4 + 1
 \end{aligned}$$

$$013 = 0 \underbrace{\frac{1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0}{0}}_{03}$$

Left to Right

$a \rightarrow$ start say

$b(n) \rightarrow$ izi gösterim dişi

$a^i = ?$

a^13

$n=13=1101_2$

$product(p) = a$

$i = 1-1$ 'den 0'a kadar

$p = p * p$

if ($b_i == 1$)

$p = p * a$

return p

\rightarrow ilk olarak 1101 olarak atılır.

i önce 0'a kadar hareket edecek

başlangıç olarak $p = p * p$ dedik ve $p = a^2$ oldu.

Sonra $i == 2$ ise $p = p * a$ dedik. Eğer 0, 1'e

çatırsa p 'yi sadece a ile çarpacağız ve i 2 olarak

çğer 0'a çatırsa hiçbir şey yapmadan i 'yi 2'ye

çatır.

1-) 1101

$p = p * p$ $i \neq 1 \checkmark \rightarrow p = p * a$
 $\rightarrow p = a * a * a$
 $= a^3$

2-) 1101

$p = p * p$ $i \neq 1 \times \rightarrow p = a^3 * a^3 = a^6$

3-) 1101

$p = p * p$ $i \neq 1 \checkmark \rightarrow a^6 * a^6 * a = a^{13}$

Maliyet $(I-1)$ 'den O'ya kadar hesaplanma

$$|I| = \log_2 n \xrightarrow{\substack{1101 \\ 8421}} (\log_2 n) \text{ defa hesaplanma}$$

$$|3| = \log_2 8$$

$$(\log_2 n) - 1 \text{ defa sayma}$$

$$(\log_2 n) - 1 \text{ defa hesaplanma}$$

$$= \log_2 n - 1 \text{ ile } 2 \log_2 n - 1 \text{ arasında değişir.}$$

Right to Left

a = bit sayı

b = bit dizisi (n sayının binary)

$$a^{13} \quad n=13=1101_2$$

b_0

ilk eleman 0 ise $p=1$

1 ise $p=a$ olarak seçilerek başlanır

diğer elemanlar sırasıyla döner $b_1 \dots \rightarrow n$

$$t = t + t$$

$$bx, 1 \text{ ise } p = p \cdot t$$

return p

başlangıç

↓

0

$$t = t + t \\ (a^2) \\ 2. adım$$

$$\rightarrow p = a \quad \begin{matrix} t = a \\ \text{başlangıç} \end{matrix}$$

$$\begin{matrix} t = t + t \\ \downarrow \\ a^8 \\ b_1 = 1 \\ p = t \cdot p = a^5 \\ \downarrow \\ a^8 \\ \text{son adım } p = a^{13} \end{matrix}$$

$$\begin{matrix} t = t + t \\ \downarrow \\ a^4 \\ b_1 = 1 \\ p = t \cdot p \\ p = a^5 \end{matrix}$$

Måliyet $2 \cdot (\log n - 1)$ er for lå

R \rightarrow L

~~1~~ 16 8 4 2 \rightarrow (30)
1 1 1 1 0

$$\begin{array}{c} 1 \\ a^{16} \\ a^{16} \cdot a^{16} = a^{32} \end{array}$$

$$\begin{array}{c} 1 \\ a^8 \\ a^8 \cdot a^8 = a^{16} \end{array}$$

$$\begin{array}{c} 1 \\ a^4 \\ a^4 \cdot a^4 = a^8 \end{array}$$

$$\begin{array}{c} 1 \\ a^2 \\ a^2 \end{array}$$

$$\begin{array}{cc} 0 & (b^p) \\ a & + \\ 1 & p \end{array}$$

L \rightarrow R

~~1~~ 1 1 1 0 0

$$\begin{array}{c} 1 \\ a \\ a^2 \cdot a = a^3 \\ (a^3)^2 \cdot a = a^7 \\ (a^7)^2 \cdot a = a^{15} \end{array}$$

$$\begin{array}{cc} 0 & 0 \\ a^{15} \cdot a^{15} & a^3 \cdot a^{30} \\ a^{30} & a^{60} \\ \hline \hline \end{array}$$

