Left-Right Binary Exp.

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

$I = 3\ 2\ 1\ 0$

$B = 1\ 1\ 0\ 1$ $\quad P(1) = a^1$ $\quad i = I - 1$

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

$I = 3$ $\quad P = 2 \cdot 1 + 1$

$= 3$

Right to Left

a^n → hesaplamak için

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

$= a^{b_I 2^I} \cdots a^{b_i 2^i} \cdots \boxed{a^{b_0 2^0}}$ → başlangıç değeri $= 1 = a^0$ olsun

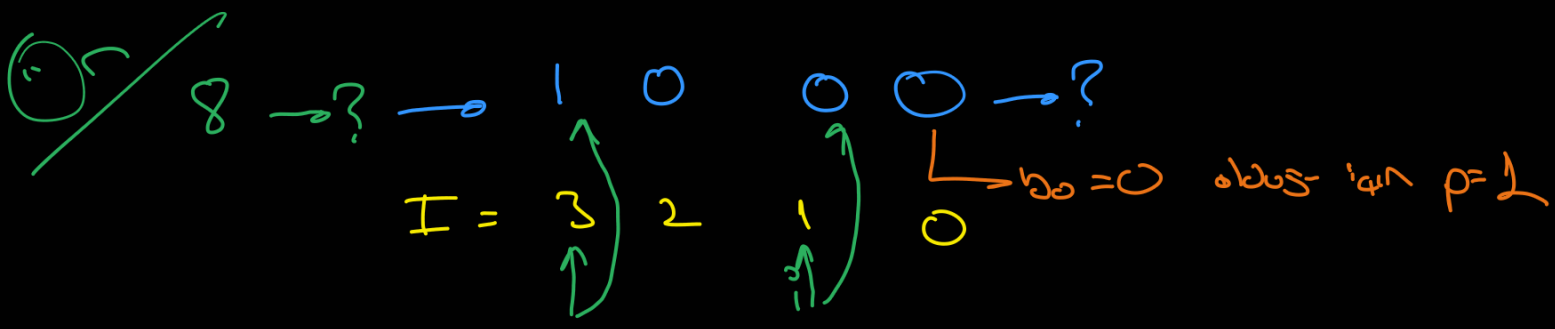
$$a^{2^i} = \left(a^{\frac{2^i}{2}}\right) = \left(a^{2^{i-1}}\right)^2$$

$a^{b_i 2^i} = ?$

$= \begin{cases} a^{2^i} & b_i = 1 \\ 1 & b_i = 0 \end{cases}$

if $b_0 = 1$ ise $p = a$

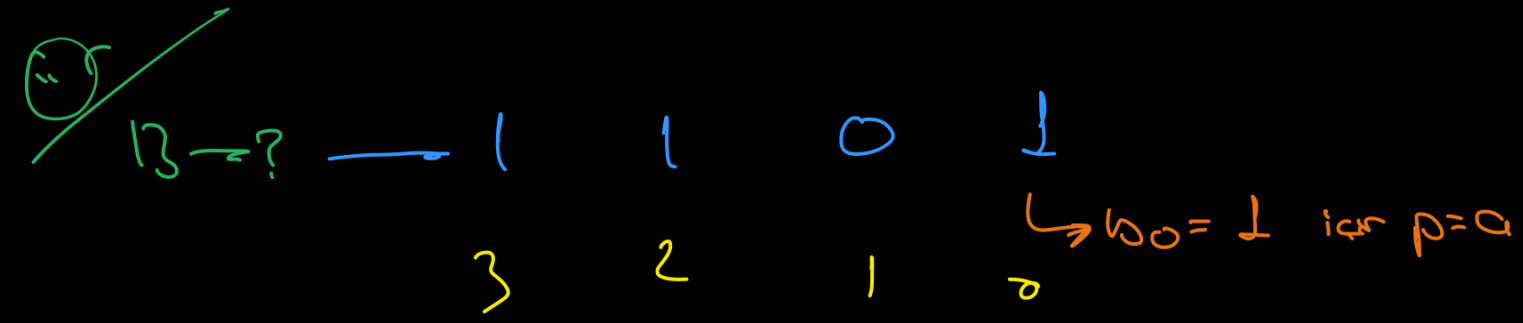
$b_0 = 0$ ise $p = 1$



i = 1 için → t = a.a → a^2

i = 2 için → t = t.t → $a^2 . a^2 = a^4$

i = 3 için → t = t.t → $a^4 . a^4 = a^8$



Binary Exponation

a^{13}

$13 \rightarrow 1101$

$b_3\ b_2\ b_1\ b_0$ $\longrightarrow n = b_0, b_1, b_2$ ve b_3 dahil

$13 \rightarrow 1.2^3 + 1.2^2 + 0.2^1 + 1.2^0 = 1.2^3 + 1.2^2 + 1.2^0$

$1.8 + 1.4 + 1.1$

$= 8 + 4 + 1$

$a^{13} = a^{1.2^3 + 1.2^2 + 0.2^1 + 1.2^0}$

$a^8 \quad a^4 \quad a^0 \quad a^1$

Left to Right

a → sabit sayı

b(n) → ikili gösterim dizisi

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

product(p) = a

i = 1-1 'den 0'a kadar

```
p = p*p
if( b_i == 1 )
    p = p*a
return p
```

→ ilk olarak atanır.

i sıfırdan 0'a kadar küçük eşitse

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

Sonra $q == 1$ ise $p = p \cdot a$ dedik. Eğer q, 1'e eşitse p'yi sadece a ile çarpacağız ve i 1 azalacak eğer 0'a eşitse hiçbir şey yapmadan i'yi 1 azaltacağız.

1) 

$p = p \cdot p$ $\quad i?1$ √ → $p = p \cdot a$ → $p = a^3 \cdot a = a^4$

2) 

$p = p \cdot p$ $\quad i?1$ x → $p = a^3 \cdot a^3 = a^6$

3) 

$p = p \cdot p$ $\quad i?=1$ √ → $a^6 \cdot a^6 \cdot a = a^{13}$

Maliyet $(I-1)$'den 0'a kadar karşılaştırma

$|I| = \log_2 n$ → $(\log_2 n)$ defa karşılaştırma

1101
8421

$|3| = \log_2 8$

$(\log_2 n) - 1$ defa toplama

$(\log_2 n) - 1$ defa karşılaştırma

$= \log n - 1$ ile $2 \log n - 1$ arasında değişir.

Right to Left

a = sabit sayı

b = bit dizisi (n sayının binary)

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

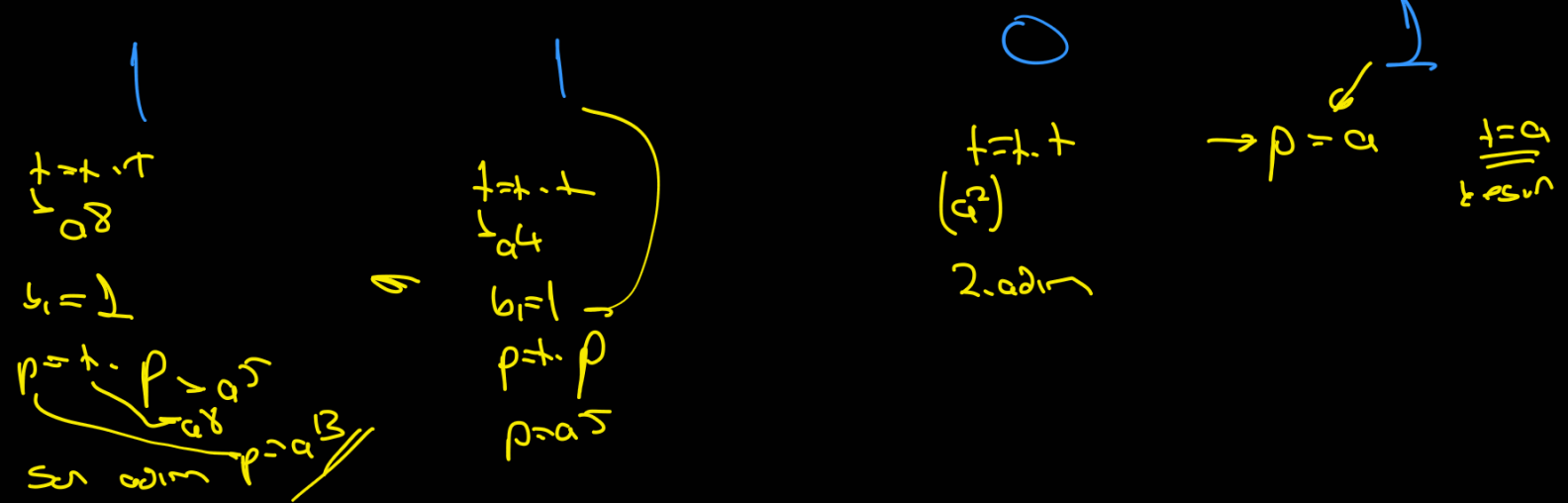
bo
ilk elemanı 0 ise $p=1$
1 ise $p=a$ olacak şekilde başla

diğer elemanlar için ise döner $b_i \dashrightarrow n$

$t = t \cdot t$
$b_x, 1$ ise $p = p \cdot t$

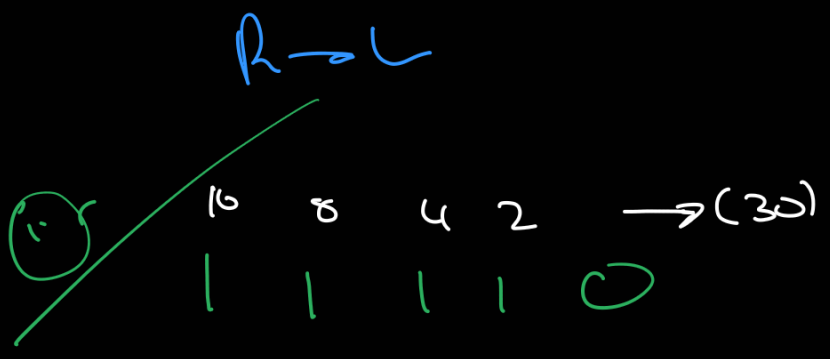
return p

başlangıç



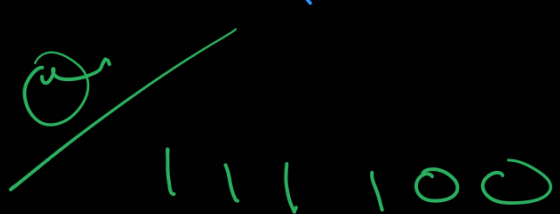
Maliyet $2 \cdot (\log n - 1)$ en fazla

R → L



1	1	1	1	0	(b^0)
a^{16}	a^8	a^4	a^2	a	a^1
$a^{16} \cdot a^{16} = a^{30}$	$a^8 \cdot a^8 = a^{16}$	$a^4 \cdot a^4 = a^8$	$a^2 \cdot a^2 = a^4$	1	p

L → R



1	1	1	1	0	0
a	$a^2 \cdot a = a^3$	$(a^3)^2 \cdot a$	$(a^3)^2 \cdot a$	$a^{15} \cdot a^{15}$	$a^{30} \cdot a^{30}$
		a^7	a^{15}	a^{30}	a^{60}