Μήκος λέξης: 64 bit

n με κ-ψηφία (b-αδικό)

$$n = \underbrace{(b-1)(b-1)\cdots}_{\kappa\text{-ψηφία}}(b-1) = b^{\kappa} - 1$$

$$\lceil \log_b n \rceil + 1 \geq \kappa$$

$$\| \quad O(\log n)$$

$$\rightsquigarrow \quad \log_b n = \frac{\log_\alpha n}{\log_\alpha b}$$

• Πρόσθεση: ←

$$\begin{array}{r} 53 \\ +\,35 \\ \hline 88 \end{array} \qquad \begin{array}{r} 5\cdot 10^1 + 3\cdot 10^0 \\ +\quad 3\cdot 10^1 + 5\cdot 10^0 \\ \hline 8\cdot 10^1 + 8\cdot 10^0 \end{array}$$

Πρόταση: Πρόσθεση 3 ψηφίων σε b-αδικό σύστημα

⇒ 2 ψήφιο αριθμό.

Απόδ.

$$\begin{array}{r} b-1 \\ b-1 \\ +\,b-1 \\ \hline 3b-3 \leq b^2 - 1 \quad \ldots \end{array}$$

$$\begin{array}{r} {\scriptstyle 1\ \ 1\ \ 1} \quad \\ 110101 \\ +\ 100011 \\ \hline 1011000 \end{array} \rightsquigarrow \begin{array}{r} +1\cdot 2^2 + 1\cdot 2^1 \quad \\ 1\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 \\ 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 \\ \hline \ldots\ldots \qquad 0\cdot 2^1 + 0\cdot 2^0 \end{array}$$

miro

Χρόνος : ~~$\Theta(\log n)$ αν η είσοδος πλησιάζει το μέγιστο n.~~

: $\Theta(n)$ αν η είσοδος έχει μέγεθος n (n ψηφία)

- Πολλαπλασιασμός

$$1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0$$

$$\begin{array}{r} 13 \\ \times\ 10 \\ \hline 130 \end{array} \qquad \begin{array}{r} 1101 \\ \times\ 10 \\ \hline 11010 \end{array}$$

$$\begin{array}{r|l} 135 & 10 \\ \cline{2-2} 5 & 13 \end{array} \qquad \begin{array}{r|l} 1101 & 10 \\ \cline{2-2} 1 & 110 \end{array}$$

$$\begin{array}{r} 13 \\ \times\ 11 \\ \hline 13 \\ +\ 13 \\ \hline 143 \end{array} \qquad \begin{array}{r} 13 \\ \times\ 1\cdot 10^1 + 1\cdot 10^0 \\ \hline 13 \\ +\ 130 \\ \hline 143 \end{array}$$

$$\begin{array}{r} 1101 \\ \times\ 1011 \\ \hline 1101 \\ 1101 \\ 0000 \\ 1101 \\ \hline 10001111 \end{array}$$

Αν πολ/με αριθμούς μεγέθους n

$$\underbrace{O(n) + \cdots + O(n)}_{n\text{-φορές}} = O(n^2)$$

$$\downarrow$$

$$O(n^{1,59})$$

Πολ/σμος Ρώσων Αγροτών:

$1 \cdot 2^0$	11	13	$2^0 \cdot 13$
$1 \cdot 2^1$	5	26	$2^1 \cdot 13$
$0 \cdot 2^2$	~~2~~	~~52~~	$2^2 \cdot 13$
$1 \cdot 2^3$	1	104	$2^3 \cdot 13$
		143	

$$x \cdot y = \begin{cases} 2 \cdot (x \cdot \lfloor y/2 \rfloor), & \text{αν } y \text{ είναι άρτιος} \\ x + 2(x \cdot \lfloor y/2 \rfloor), & \text{αν } y \text{ περιττός} \end{cases}$$

multiply(x,y):

```
Είσοδος:  Ακέραιοι $x, y \geq 0$ ($n$ bit)
Έξοδος:   Ο $x \cdot y$
if $y = 0$, return 0
  $z$ = multiply($x$, $\lfloor y/2 \rfloor$)
if $y$ είναι άρτιος
      return $2 \cdot z$   (μετατόπιση αριστερά)
else
      return $x + 2 \cdot z$   (μετατοπ. + πρόσθεση)
```

Χρόνος:

$O(n)$ - αναδρομικές κλήσεις

$O(n)$ (σε κάθε αναδρ. κλήση)

" $O(n^2)$

$O(n)$

• Διαίρεση:

$$\begin{array}{c|c} 13 & 5 \\ \cline{2-2} 2 & 3 \end{array}$$

$$\begin{array}{c|c} \begin{array}{c} 6 \\ \| \\ \lfloor 13/2 \rfloor \end{array} & 5 \\ \cline{2-2} 1 & 1 \\ \cdot & \cdot \\ 2 & 2 \\ & + \\ & 1 \\ \| & \| \\ 2 & 3 \end{array}$$

$X = q \cdot Y + r$:

• X άρτιο: $\left\lfloor \frac{X}{2} \right\rfloor = \frac{X}{2} = q' \cdot Y + r' \xrightarrow{\cdot 2}$

$$X = \underbrace{2q'}_{q} \cdot Y + \underbrace{2r'}_{r}$$

- x περιττό: $\left\lfloor \frac{x}{2} \right\rfloor = \frac{x-1}{2} = q' \cdot y + r' \xrightarrow{\cdot 2}$

$$\xrightarrow{\cdot 2} \quad x-1 = 2q' \cdot y + 2r'$$

$$x = \underbrace{2q'}_{q} \cdot y + \underbrace{2r'+1}_{r}$$

divide (x, y):

Είσοδος: Ακέραιοι $x, y \geq 1$ (n bit)

Έξοδος: Πηλίκο q και υπόλοιπο r του x δια y

```
if $x = 0$        return $(\overset{q}{\downarrow}0, \overset{r}{\downarrow}0)$ $\rightsquigarrow O(1)$
$(q', r') = $ divide$(\lfloor x/2 \rfloor, y)$
$q = 2q'$, $r = 2r'$ $\rightsquigarrow O(n)$
if $x$ είναι περιττός $\rightsquigarrow O(1)$
    $r = r + 1$ $\rightsquigarrow O(n)$
```

```
if $r \geq y$                  ⇝ $O(n)$
    $q = q+1$ , $r = r-y$       ⇝ $O(n)$
return $(q, r)$.
```

χρόνος: $O(n)$ αλγ. [illegible]

$$O(n) \cdot O(n) = O(n^2)$$

Abziehen:

$$
\begin{array}{rcccc}
 & 1 & \overset{0}{\cancel{1}} & \overset{1}{0} & 1 \\
- & 1 & 0 & 1 & 1 \\
\hline
 & & \cancel{0}0 & 1 & 0
\end{array}
\qquad
\begin{array}{l}
\rightsquigarrow 13 \\
\rightsquigarrow 11 \\
\rightsquigarrow 2
\end{array}
$$

$$
\begin{array}{rccccccc}
 & 1 & \overset{0}{\cancel{1}} & \overset{\overset{1}{\cancel{0}}}{\cancel{1}} & \overset{1}{0} & 0 & 1 & 1 \\
- & & & 1 & 1 & 0 & 1 & 0 \\
\hline
 & 1 & 0 & 1 & 1 & 0 & 0 & 1
\end{array}
\qquad
\begin{array}{l}
\rightsquigarrow 115 \\
\rightsquigarrow 26 \\
\rightsquigarrow 89
\end{array}
$$

$O(n)$

Αλγόριθμος Ευκλείδη:

Κανόνας Ευκλείδη: x, y φυσικοί αριθμοί, $x \geq y$

τότε $\text{μκδ}(x, y) = \text{μκδ}(x \bmod y, y)$

Αποδ.

Αρκεί ν.δ.ο. $\text{μκδ}(x, y) = \text{μκδ}(x-y, y)$.

κάθε αριθμός $\left.\begin{matrix} b \mid x \\ b \mid y \end{matrix}\right\} \Rightarrow b \mid x-y$

$\ldots \Rightarrow \text{μκδ}(x, y) \leq \text{μκδ}(x-y, y)$

$$\left.\begin{array}{l} b \mid x-y \\ b \mid y \end{array}\right\} \Rightarrow b \mid x \quad \ldots \Rightarrow \text{μκδ}(x-y, y) \leq$$

$$\leq \text{μκδ}(x, y)$$

Euclid (α, b)

Είσοδος: Ακέραιοι α, b, $\alpha \geq b \geq 0$ (n bit)

Έξοδος: μκδ(α, b)

```
if  $b = 0$
    return $\alpha$
else
    return Euclid$(b, \alpha \bmod b)$.
```

Λήμμα: $\alpha \geq b \Rightarrow \alpha \bmod b < \frac{\alpha}{2}$

Απόδ.

- $b \leq \alpha/2$:

$$\alpha \bmod b < b \leq \alpha/2$$

- $b > \alpha/2$

$$\alpha \bmod b = \alpha - b < \alpha - \frac{\alpha}{2}$$

$$= \frac{\alpha}{2}$$

Έχουμε $2 \cdot n$ διαφορετικές εισόδους

||

$O(n)$

$O(n^2)$ (μία διαίρεση)

||

$O(n^3)$