11.11.2024

Seminar 6
Structuri Algebrice în Informatică

1) Aflați ultimele 2 cifre din $N = 32^{30}$, adică restul împărțirii lui N la 100 sau în $\mathbb{Z}_{100}$ cine este $\hat{N}$.

$$\widehat{32^{30}} = \hat{32}^{30} = \widehat{2^5}^{30} = \hat{2}^{5\cdot 30} = \hat{2}^{150} =$$
$$= \widehat{2^{10}}^{15} = \widehat{1024}^{15} = \hat{24}^{15} = \widehat{24^3}^{5} = \widehat{13824}^{5} =$$
$$= \hat{24}^{5} = \widehat{24^3}^{2} = \hat{24}^{2} = \hat{76}$$

sau exponențierea rapidă: scriem exponentul în baza 2.

$$n = b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + \dots + b_k \cdot 2^k \text{ cu } b_i \in \{0, 1\}$$

<u>Calculez</u>

i	0	1	----	k
a^{2^i}	a	a^2	a^4	a^{2^k}

k - ridicări la pătrat unde $k = [\log_2 n]$

$$2^k \le n \le 2^{k+1}$$
$$k \le \log_2 n < k+1$$

<u>PAS 2</u>: $a^n = a^{b_0 + 2b_1 + 2^2 b_2 + \dots + 2^k b_k}$

$$= a^{b_0} \cdot (a^2)^{b_1} \cdot (a^{2^2})^{b_2} \cdot \dots \cdot (a^{2^k})^{b_k}$$

Dacă $b_i = 0 \Rightarrow (a^{2^i})^{b_i} = 1 \rightarrow$ ignorăm

$b_i = 1 \Rightarrow (a^{2^i})^{b_i} = a^{2^i} \in$ tabloului

$\rightarrow$ facem $\leq k$ înmulțiri

$$a^n = \prod_{\substack{i=0 \\ b_i \neq 0}}^{k} a^{2^i}$$

2) Aflați restul împărțirii la 3 și la 9 pentru

$N = 38^{131}$ în $\mathbb{Z}_3$: $\hat{N} = \widehat{2^{131}} = \underbrace{\hat{2}^2 \cdot \hat{2}^2 \cdot \ldots \cdot \hat{2}^2}_{65 \text{ de ori}} \cdot \hat{2} =$

$= \hat{1} \cdot \hat{1} \cdot \hat{1} \cdot \ldots \cdot \hat{2} = \hat{2}$

$\hat{2} = -\hat{1}$ $\boxed{\widehat{38} = \hat{2} \text{ în } \mathbb{Z}_3}$

$\hat{N} = \hat{2}^{131} = -\hat{1}^{131} = -\hat{1} = \hat{2}$

în $\mathbb{Z}_9$: $\hat{N} = \widehat{38^{131}} = \widehat{2^{131}}$

$131 = 128 + 3 = 128 + 2 + 1 = 2^7 + 2^1 + 2^0$

i	0	1	2	3	4	5	6	7
2^{2^i}	$\hat{2}$	$\hat{4}$	$-\hat{2}$	$\hat{4}$	$-\hat{2}$	$\hat{4}$	$-\hat{2}$	$\hat{4}$

$\widehat{38^{131}} = \widehat{38}^{131} = \hat{2}^{2^7} \cdot \hat{2}^{2^1} \cdot \hat{2}^{2^0} =$

$= \hat{4} \cdot \hat{4} \cdot \hat{2} = \widehat{32} = \hat{5}$

3) Determinați nr. de zerouri cu care se termină $N = 25!$

$\max\{k \in \mathbb{N} \mid 10^k \mid N$ și $10^{k+1} \nmid N\} =$

$= \min\{\underbrace{v_2(25!)}_{\geq 12}, \underset{\overset{\|}{6}}{v_5(25!)}\}$

$10 = 2 \cdot 5$

$10^k \mid N \iff 2^k \mid N$ și $5^k \mid N$

p prim notăm: $v_p(n) = \max\{k \in \mathbb{N} \mid p^k \mid n\}$

$$\begin{array}{ccccc} 5 & 10 & 15, & 20 & 25 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5^1 & 5^1 & 5^1 & 5^1 & 5^2 \end{array}$$

$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$

$v_p(25!) = \underset{\overset{\|}{5}}{\left[\frac{25}{5}\right]} + \underset{\overset{\|}{1}}{\left[\frac{25}{25}\right]} + \underset{\overset{\|}{0}}{\left[\frac{25}{125}\right]} + \ldots = 5 + 1 = 6$