CIORNEI MIREL-ALIN
GRUPA M531

TEMA 3

6) Alg. Solovay-Strassen $n = 66601$

- $b = 2 \Rightarrow$

$$2^{33300} \equiv 16 \cdot (2^{16})^{2081} \equiv 16 \cdot (-1065)^{2081} \equiv -16 \cdot 65^{2081} (-2^{16}) \equiv 1 \pmod{66601}$$

$$\left(\frac{2}{66601}\right) \equiv (-1)^{\frac{66601^2-1}{8}} = (-1)^{\frac{66600 \cdot 66602}{8}} = (-1)^{33301} = -1 \pmod{66601}$$

Deci $2^{33300} \equiv \left(\frac{2}{66601}\right) \pmod{66601}$

- $b = 7$

$$7^{33300} \equiv (7^6)^{5550} \equiv (-15553)^{5550} \equiv (977)^{2775} \equiv -1 \pmod{66601}$$

$$\left(\frac{7}{66601}\right) = (-1)^{\frac{6 \cdot 66600}{4}} \left(\frac{66601}{7}\right) \equiv \left(\frac{3}{7}\right) = (-1)^{\frac{3-1}{4}} \left(\frac{7}{3}\right) = (-1) \cdot \left(\frac{1}{3}\right) = -1 \pmod{66601}$$

Deci $7^{33300} \equiv \left(\frac{7}{66601}\right) \pmod{66601}$

$a = 11$

$11^{33300} \equiv -1 \pmod{66601}$

$\left(\frac{11}{66601}\right) = (-1)^{\frac{10 \cdot 66600}{4}} \left(\frac{66601}{11}\right) = \left(\frac{1}{11}\right) = (-1)^{\frac{6 \cdot 10}{4}} \left(\frac{11}{7}\right) = -1 \left(\frac{4}{7}\right) =$

$\Rightarrow 11^{33300} \equiv \left(\frac{11}{66601}\right) \pmod{66601}$

PA motivii 2, 7, 11 am obț. egalitate, deci putem afirma că 66601 este prim cu o probabilitate de $1 - \frac{1}{8} = \frac{7}{8} \Rightarrow 87,5$

(Nr. 66601 fiind chiar prim după testarea cu un algoritm determinist)

Teorema 1) $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, $a^{p_i} \equiv a \pmod{p_i}$, $\forall p_i \Rightarrow a^n \equiv a \pmod{n}$

RR PA, $a^n \equiv a \pmod{n} \Rightarrow a^n = X + nK$, $X \in \{1, 2, \ldots, n-1\}$

$\Rightarrow a^n \equiv X + a p_1^{\alpha_1} \cdots p_k^{\alpha_k} K \Rightarrow a^n \equiv X \pmod{p_i}$

Știm că $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, $a^{p_i} \equiv a \pmod{p_i}$ $\forall i \in \{1, \ldots, k-1\}$, $a \equiv X \pmod{p_i}$

$\Rightarrow a^n \equiv a^{\prod_{i=1}^{k} p_i^{\alpha_i}} \equiv \left(a^{p_1 \cdots p_{k-1}}\right)^{p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k}} \equiv a^{p_1 \cdots p_k} \equiv \ldots \equiv a^{p_k}$

$a^n \equiv a \pmod{n} \Rightarrow$

$a^{p_1} \equiv a \pmod{p_1} \Rightarrow a^{p_1} \equiv a \pmod{p_1}$

3) Pp. n compus $\Rightarrow \exists p, q$ a.î. $n = pq$, $p, q > 1$

$2^{pq} - 1 = (2^p - 1)(1 + 2^p + 2^{2p} + \ldots + 2^{(q-1)p})$ $\Rightarrow$ $\begin{cases} 2^p - 1 > 1 \\ 1 + 2^p + \ldots + 2^{(q-1)p} > 1 \end{cases}$

$p > 1$, $q > 1$

$\Rightarrow 2^{pq} - 1$ - compus $\Rightarrow 2^n - 1$ - prim $\Rightarrow n$ - prim