Tema 3

Cătălin Răpeanu

1) 8. Folosiți algoritmul Miller-Rabin pentru a determina primalitatea nr. 77773 (cel mult 3 martori

$n = 77773$

$n-1 = 77772 : 2 = 38886$, $38886 : 2 = 19443$

$$\begin{array}{l|l} 77772 & 2 \\ \underline{6} & 38886 \\ 17 & \\ \underline{16} & \\ =17 & \\ \underline{16} & \\ =17 & \\ \underline{16} & \\ =12 & \\ \underline{12} & \\ == & \end{array} \qquad \begin{array}{l|l} 38886 & 2 \\ \underline{2} & 19443 \\ 18 & \\ \underline{18} & \\ ==8 & \\ \underline{8} & \\ =8 & \\ \underline{8} & \\ =6 & \\ \underline{6} & \\ = & \end{array}$$

$$2^{19443} \equiv 2 \cdot (2^2)^{9721} \equiv 2 \cdot 4 \cdot (4^2)^{4860} \equiv 8 \cdot (16^2)^{2430} \equiv$$

$$\equiv 8 \cdot (256^2)^{1215} \equiv 8 \cdot 65536 \cdot 65536^{1214} \equiv$$

$$\equiv 57650 \cdot (-12237)^{1214} \equiv 57650 \cdot (12237^2)^{607} \equiv$$

$$\equiv 57650 \cdot 31144 \cdot (31144^2)^{303} \equiv 61895 \cdot 41653 \cdot (41653^2)^{15}$$

$$\equiv 15258 \cdot 12325 \cdot (12325^2)^{75} \equiv 77509 \cdot 14956 \cdot (14956^2)^{\equiv}$$

$$\equiv 18039 \cdot 6788 \cdot (6788^2)^{18} \equiv 34030 \cdot (35328^2)^{9} \equiv$$

$$\equiv 34030 \cdot 44253 \cdot (44203^2)^{4} \equiv 10991 \cdot (3869^2)^{2} \equiv$$

$$\equiv 10991 \cdot 36745^2 \equiv 10991 \cdot 55745 \equiv 75374 \pmod{77773}$$

$(2^{19443})^2 \equiv 75374^2 \equiv 77772 \equiv -1 \pmod{77773}$

$(2^{19443})^4 \equiv -1^2 \equiv 1 \pmod{77773}$

$\Rightarrow 77773$ este prim