Tema 3

9. Aplicați algoritmul Solovay - Strassen pentru a verifica dacă numărul 86113 este prim sau compus (cel mult 3 martori)

$n = 86113 \to$ impar $\Rightarrow b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) (\bmod n), \forall b \in \{1, 2, \dots, n-1\}$

$b = 23 \Rightarrow 23^{43056} \equiv 70467 (\bmod 86113)$

$\frac{b}{n} = \frac{23}{86113} = \underbrace{(-1)^{\frac{22\cdot 86112}{4}}}_{=1}\cdot\left(\frac{86113}{23}\right) = \frac{1}{23} = (-1)^{\frac{23^2-1}{1}} = 1$

$23^{43056} \equiv (23^2)^{21528} \equiv (529^2)^{10764} \equiv (21502^2)^{5382} = (81420^2)^{2691} =$

$= 81420\cdot(81420^2)^{2690} = 81420\cdot(65434^2)^{1345} = 81420\cdot 65434\cdot(65434^2)^{1344} =$

$= 83309\cdot(69996^2)^{672} = 83309\cdot(40881^2)^{336} = 83309\cdot(61170^2)^{168} =$

$= 83309\cdot(72937^2)^{84} = 83309\cdot(3168^2)^{42} = 83309\cdot(47116^2)^{21} =$

$= 83309\cdot 47116\cdot(47116^2)^{20} = 70191\cdot(10429^2)^{10} = 70191(3322^2)^5 =$

$= 70191\cdot 3322\cdot(3322^2)^4 = 66611\cdot(13220^2)^2 = 66611\cdot 45123^2 =$

$= 66611\cdot 29357 = 70467 (\bmod 86113)$

$b = 1000 \Rightarrow 1000^{43056} \equiv$

$\frac{b}{n} = \frac{1000}{86113} = \underbrace{(-1)^{\frac{999\cdot 86112}{4}}}_{par \Rightarrow (-1)^{par} = 1}\cdot\left(\frac{86113}{1000}\right) = \left(\frac{113}{1000}\right) = \cancel{(-1)^{\frac{1000^2-1}{113}}} = (-1)^{\underbrace{\frac{999\cdot 112}{4}}_{par}}\cdot\left(\frac{1000}{113}\right) =$

$= \left(\frac{1000}{113}\right) = \left(\frac{96}{113}\right) = (-1)^{\underbrace{\frac{112\cdot 95}{4}}_{par}}\cdot\left(\frac{113}{96}\right) = \left(\frac{113}{96}\right) = \left(\frac{17}{96}\right) = (-1)^{\underbrace{\frac{95\cdot 16}{4}}_{par}}\cdot\left(\frac{96}{17}\right) = \left(\frac{96}{17}\right) = \left(\frac{11}{17}\right) =$

$= (-1)^{\underbrace{\frac{16\cdot 10}{4}}_{par}}\left(\frac{17}{11}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\cdot\left(\frac{3}{11}\right) = (-1)^{\underbrace{\frac{2\cdot 10}{4}}_{impar}}\left(\frac{11}{3}\right) =$

$= (-1)\left(\frac{11}{3}\right) = (-1)\left(\frac{2}{3}\right) = (-1)\cdot(-1)^{\frac{3^2-1}{8}} = (-1)\cdot(-1) = 1$

$1000^{43056} = (1000^2)^{21528} = (52757^2)^{10764} = (42776^2)^{5382} = (57152^2)^{2691} =$

$= 57152\cdot(57152^2)^{2690} = 57152\cdot(85014^2)^{1345} = 57152\cdot 85014\cdot(85014^2)^{1344} =$

$= 52442\cdot(2219^2)^{672} = 52442\cdot(15520^2)^{336} = 52442\cdot(12339^2)^{168} =$

$= 52442\cdot(3137^2)^{84} = 52442\cdot(23887^2)^{42} = 52442\cdot(4031^2)^{21} = 52442\cdot 4031\cdot$

$\cdot(4031^2)^{20} = 72400\cdot(59717^2)^{10} = 72400\cdot(8533^2)^5 = 72400\cdot 8533\cdot(8533^2)^4 =$

$= 14538\cdot(46604^2)^2 = 14538\cdot 76843^2 = 14538\cdot 78239 = 58078 (\bmod 86113)$