TEMA 3

ex. 5. Alg. Miller-Rabin pt. nr. 81991 (cel mult 3 martori)

$n = 81991$

$n-1 = 81990 = 2 \cdot 3^2 \cdot 5 \cdot 911$

$= 2 \cdot 45 \cdot 911$

$40\,995$

81990	10 = 2·5
8199	3
2733	3
911	

81990

Aleg $b = 2$: $2^{40\,995} \pmod{81991} =$

$= 2 \cdot 2^{40\,994} = 2 \cdot 4^{20\,497} = 8 \cdot 4^{20\,496} =$

$= 8 \cdot 16^{10\,248} = 8 \cdot 256^{5124} = 8 \cdot 65536^{2562} =$

$= 524\,288 \cdot 65536^{2561} = 32\,342 \cdot 65536 \cdot 65536^{2560}$

$=$

Aleg. $b=5$: $\cdot 5^{45\cdot 911} \pmod{81991}$

$= 5 \cdot 5^{44\cdot 911} = 5 \cdot 25^{22\cdot 911} =$

$= 5 \cdot 625^{11\cdot 911} = 5 \cdot 625 \cdot 625^{10\cdot 911} = 3125 \cdot 625 \cdot 625$

$1.953.125$

$= 67.332 \cdot 625^{10\cdot 910} =$

Aleg. ~~$b=11$~~ $\cdot 11^{45\cdot 911} \pmod{81991}$

$= 11$

Aleg $b=287$: $\cdot 287^{45\cdot 911} = 287 \cdot (287^2)^{22\cdot 911}$

$= 287 \cdot 82369 \cdot 287^{22\cdot 911}$

$\equiv 26.495 \cdot 287^2 \cdot 287^{11\cdot 9}$

~~mod (81991)~~ 378

$\equiv 26.496 \cdot 378 \cdot 287 \cdot 287^{10\cdot 911} = 26.496 \cdot 26.496$

$\equiv 4578 \cdot \frac{287^2}{378} \cdot 287^{5\cdot 911} = 8673 \cdot 287 \cdot 287^{4\cdot 911}$

$\equiv 29.421 \cdot \frac{378 \cdot 378}{60.893} \cdot 287^{911}$

$\Rightarrow 81991$ nu este prim

402.011.520

3562

730.484

2.489.151

142.884

ex. 3. $2^n - 1$ prim $\Rightarrow$ n prim ?

Pp. R.A. ~~$2^n - 1$ prim~~ $n \neq$ prim

$n \neq$ prim $\Rightarrow \exists$ un divizor d al lui n

$d \neq 1 \neq n$.

Adică $n = d \cdot k$

$2^n - 1 = 2^{d \cdot k} - 1$

$2^n - 1 = (2-1)(2^{n-1} + 2^{n-2} + 2^{n-3} + \dots + 1)$

$= 2^n + 2^{n-1} + 2^{n-2} + \dots + 2 - 2^{n-1} - 2^{n-2} - \dots - 1$

$= 2^n - 1$

$(2^d)^k - 1 = (2^d - 1)(2^{(d(k-1))} + 2^{(d(k-2))} + \dots + 1) = 2^n - 1$

$\hookrightarrow 2^d - 1 \mid 2^n - 1 \Rightarrow 2^n - 1$ are cel puțin un divizor propriu $\rightarrow 2^n - 1 \neq$ prim (contradicție) $\Rightarrow$ Pp. făcută este falsă.

$\Rightarrow n$ este prim