

Tema 9

3. Afișati că dacă $2^m \mid n$, atunci n este pînă:

$$\begin{aligned} & \text{P} \wedge \text{R} \wedge \text{S} \wedge \text{T} \wedge \text{U} \wedge \text{V} \wedge \text{W} \wedge \text{X} \wedge \text{Y} \wedge \text{Z} \wedge \text{A} \\ & \text{d} = 2^m - 1 = (2^m - 1) (2^{m-1} + \dots + 2^1 + 1) \end{aligned}$$

$$\begin{aligned} & 2^m - 1 = 2^m - 2^0 = 2^m - 2^0 \cdot 1 = 2^m - 2^0 \cdot (2^0 - 1) = \{ \dots \\ & \text{deocamdată } \Rightarrow 2^m - 1 \leq 2^m - 1 \cdot 2^0 = 2^m - 1 \text{ este număr} \} \\ & \alpha < m \end{aligned}$$

dificultate de 1 și 2

crescător

\Rightarrow

$2^m - 1$ este pînă
cu pînă / contradicție cu
împărțirea

✓

% Făcând algoritmul Miller-Rabin, determinați numărul 52469 este număr
compus.

$$n = 52469 \quad n-1 = 2^2 \cdot 1317$$

$$m-1 = 52468 \quad \text{mărimea } b_0 = 2$$

$$\begin{aligned} & 52468 \mid 2 \\ & \begin{array}{r} 26234 \\ 13117 \end{array} \quad \begin{array}{r} 2 \\ 1 \\ 1 \end{array} \\ & \begin{array}{r} 26234 \\ 13117 \\ 13117 \end{array} \quad \begin{array}{r} 2 \\ 1 \\ 1 \end{array} \\ & 1 \end{aligned}$$

$$\begin{aligned} & (2 \cdot 3117)^2 = 2 \cdot 2 \cdot 3117^2 = 2 \cdot (2^2) \cdot 3117^2 \\ & = 2 \cdot 4 \cdot 3117^2 = 2 \cdot (4^k) \cdot 3117^2 \\ & 3117 \mid 6 = 2 \cdot 8 \\ & 2 \quad 16 \cdot (2^k) \cdot 3117 = 16 \cdot 6 \cdot 16^38 \\ & 16 \cdot 2 \cdot (64^k) \cdot 3117 = 32 \cdot 4096 \cdot 2^3 \\ & = 32 \cdot 11056 \cdot 4096 \\ & = 32 \cdot 11056 \cdot (10936^2) \quad 4096 \\ & \cong 26534 \cdot 26720 \cdot 11056 \\ & \cong 26534 \cdot 26720 \cdot 26720 \cdot 11056 \\ & \cong 18 \end{aligned}$$

$$\begin{aligned} & 13116 : 2 = 6558 \quad : 2 = 3279 \\ & \frac{12}{11} \quad \frac{6}{5} \\ & = 11 \\ & = 10 \\ & \frac{4}{10} \\ & = 10 \\ & \frac{15}{15} \\ & = 15 \\ & \frac{4}{14} \\ & = 14 \\ & \frac{15}{15} \\ & = 15 \\ & \frac{8}{8} \\ & = 8 \\ & \frac{15}{15} \\ & = 15 \\ & \frac{8}{8} \\ & = 8 \end{aligned}$$

$$\begin{aligned} & 13117 \quad 2 = 1 \quad \text{mod} \quad 52468 \rightarrow \text{nu este prim} \end{aligned}$$

compozit

$$d = 3$$

$$\begin{aligned} 3^{13117} &= 3 \cdot (3^2)^{13116} = 3 \cdot (9^2)^{6558} = 3 \cdot 81^{6558} \\ &= 3 \cdot 81 \cdot 6558 = 3 \cdot 81 \cdot (81^2) = 3 \cdot 81 \cdot 32749 = 3 \cdot \cancel{81} \cdot 6491 = 3 \cdot 6491 \cdot 6491 \\ &= 19673 \cdot (6491^2) = 19673 \cdot 18809 \\ &= 19673 \cdot 6451 \cdot 6451 \end{aligned}$$

$\frac{2}{2} \quad \frac{2}{81} \quad \underline{\frac{6451}{6451}}$