Temă - L3

3. Ar. că dacă $2^n - 1$ este prim, at. n este prim

PP RA n nu este prim $\Rightarrow \exists k, l \in \mathbb{Z}_{>2}$ a.î. $n = kl$

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

$2^k - 1 \in \mathbb{Z}$, $2^{kl-k} + 2^{kl-k+1} + \dots + 1 \in \mathbb{Z}$

$\Rightarrow$ PP este falsă $\Rightarrow n \in \mathbb{P} \Rightarrow 2^n - 1 \in \mathbb{P}$

3. Verificați folosind algoritmul lui Solovay - Strassen dacă numărul 49937 este prim sau compus (cel puțin 3 martori)

$$l_2^{\frac{49937-1}{2}} = l_2^{24968} \equiv \left(\frac{l}{49937}\right) \pmod{49937}$$

- $l_2 = 2 \Rightarrow \left(\frac{2}{49937}\right) = (-1)^{\frac{2493703969-1}{8}} = (-1)^{311712996} = 1$

$\Rightarrow 2^{24968} \equiv 1 \pmod{49937}$

$256^{3121} = 256^1 \cdot 256^{3120} \equiv 256^1 \cdot 65536^{1560} \equiv$

$\equiv 155995^{1560} \cdot 256 \equiv 243328810^{780} \cdot 256 \equiv 35746^{780} \cdot 256 \equiv 1$

- $l_2 = 4 \Rightarrow \left(\frac{4}{49937}\right) \left(\frac{2}{49937}\right) \cdot \left(\frac{2}{49937}\right) = 1 \cdot 1 = 1$

$\Rightarrow 4^{24968} \equiv (2^{24968})^2 \equiv 1^2 \equiv 1 \pmod{49937}$