(12) Folosind algoritmul Miller-Rabin, determinați dacă numărul 40289 este prim sau compus

$n = 40289 \Rightarrow n-1 = 40288 = 2^5 \cdot 1259$

40288	2
20144	2
10072	2
5036	2
2518	2
1259	1259
1	

Obținem: $2^{1259} \pmod{40289} \equiv$

$= 2 \cdot 2^{1258} \pmod{40289} =$

$= 2 \cdot (2^2)^{629} \pmod{40289} =$

$= 2 \cdot 4 \cdot 4^{628}$ (-//->) =

$= 8 \cdot (4^2)^{314}$ (-//-) $= 8 \cdot ((16)^2)^{157}$ (-//) =

$= 8 \cdot 16^2 \cdot (16^2)^{156}$ (-//-) $= 2048 \cdot (256^2)^{78}$ (-//-) =

$= 2048 \cdot (65536)^{78} \pmod{40289} \equiv$

$\equiv 2048 \cdot (25247)^{78} \pmod{40289} =$

$65536 : 40289 = 1$
40289
25247

$637411009 : 40289 =$
$= 15820 \text{ r } 39029$

$1587600 : 40289 =$
$= 39 \text{ r } 16329$

$= 2048 \cdot (25247^2)^{36} \pmod{40289} =$

$= 2048 \cdot (637411009)^{36} \pmod{40289} =$

$\equiv 2048 \cdot 39029^{36} \pmod{40289} =$

$\equiv 2048 \cdot (-1260)^{36} \pmod{40289} =$

$= 2048 \cdot (1260^2)^{18}$ (-//-) =

$= 2048 \cdot (1587600)^{18}$ (-//-)

$\equiv 2048 \cdot 16329^{18} \pmod{40289} =$

$= 2048 \cdot (16329^2)^9 \pmod{40289} =$

$\equiv 2048 \cdot (266636241)^9 \pmod{40289} \equiv$

$\equiv 2048 \cdot (3639)^9 \pmod{4029} = 2048 \cdot 3639 \cdot (3639^2)^4$ (-//-)

$= 7452672 \cdot (13242321)^4$ (-//-) $\equiv$

$\equiv 39496 \, (27529)^4 \pmod{40289} =$

$\quad\ (-793) \qquad (-12760)$

$= (-793) \cdot (12760^2)^2 \pmod{40289}$

$= (-793) \cdot 162817600^2 \ (-\|-) \equiv$

$\equiv (-793) \cdot 9751^2 \pmod{40289} \equiv$

$\equiv (-793) \cdot 95082001 \ (-\|-) \equiv$

$\equiv (-793) \cdot 40250 \pmod{40289} \equiv$

$\equiv (-793) \cdot (-39) \ (-\|-) = 30927 \ (-\|-) \Rightarrow$

$\Rightarrow 2^{1259} \equiv 30927 \pmod{40289} \equiv -9362 \pmod{40289}$

$2^{2 \cdot 1259} \equiv (-9362)^2 = 87647044 \equiv 18469 \pmod{40289}$

$2^{2^2 \cdot 1259} \equiv 18469^2 \equiv 17287 \pmod{40289}$

$2^{2^3 \cdot 1259} \equiv 17287^2 \equiv 16856 \pmod{40289}$

$2^{2^5 \cdot 1259} \equiv 2^{2^3 \cdot 1259} \cdot 2^{2^2} \equiv 16856 \cdot 2^4 = 16856 \cdot 256 \equiv$

$\equiv 4315136 \equiv 4213 \neq -1 \Rightarrow$ не е [illegible]