Tema 3

2. Folosind algoritmul Miller-Rabin, verificați dacă 229 este prim sau compus (cel mult trei martori).

$n = 229$

$n-1 = 228 = 2^2 \cdot 57$

$b = 2$

$2^{57} \pmod{229} \equiv 2 \cdot 2^{56} \equiv 2 \cdot (2^2)^{28} \equiv$

$\equiv 2 \cdot 4^{28} \equiv 2 \cdot (4^2)^{14} \equiv 2 \cdot 16^{14} \equiv$

$\equiv 2 \cdot (16^2)^7 \equiv 2 \cdot (256)^7 \equiv 2 \cdot (27)^7$

$\equiv 2 \cdot 27 \cdot (27)^6 \equiv 54 \cdot (27^2)^3 \equiv 54 \cdot (729)^3$

$\equiv 54 (42)^3 \equiv 54 \cdot 42 \cdot (42)^2$

$\equiv 2268 \cdot 1764 \equiv 207 \cdot 161 \equiv 122 \pmod{229}$

$(2^{57})^2 \pmod{229} \equiv (2^2)^{57} \equiv 4 \cdot 4^{56}$

$\equiv 4 \cdot (4^2)^{28} \equiv 4 \cdot (16)^{28} \equiv 4 \cdot (16^2)^{14}$

$\equiv 4 \cdot (256)^{14} \equiv 4 \cdot (27)^{14} \equiv 4 \cdot (27^2)^7$

$\equiv 4 \cdot (42)^7 \equiv 4 \cdot 42 \cdot (42)^6 \equiv 168 \cdot (42^2)^3$

$\equiv 168 \cdot (-68)^3 \equiv 168 \cdot (-68) \cdot (-68)^2$

$\equiv (-61) \cdot (-68) \cdot 4624 \equiv 4148 \cdot 44$

$\equiv 26 \cdot 44 \equiv 1144 \equiv 228 \equiv -1 \pmod{229}$

$\Rightarrow$ 229 prim

$b = 3$

$3^{57} \pmod{229} \equiv 3 \cdot 3^{56} \equiv 3 \cdot (3^2)^{28} \equiv 3 \cdot 9^{28}$

$\equiv 3 \cdot (9^2)^{14} \equiv 3 \cdot (81)^{14} \equiv 3 \cdot (81^2)^7$

$\equiv 3 \cdot (149)^7 \equiv 3 \cdot (-80)^7 \equiv 3 \cdot (-80) \cdot (-80)^6$

$\equiv (-249) \cdot ((-80)^2)^3 \equiv (-11) \cdot (6400)^3 \equiv$

$\equiv (-11) \cdot (217)^3 \equiv (-11) \cdot (-12)^3 \equiv (-11) \cdot (-12) \cdot (-12)^2$

$\equiv 132 \cdot 144 \equiv 1 \pmod{229}$

$(3^{57})^2 \pmod{229} \equiv (3^2)^{57} \equiv 9^{57} \equiv 9 \cdot 9^{56}$

$\equiv 9 \cdot (9^2)^{28} \equiv 9 \cdot (81)^{28} \equiv 9 \cdot (81^2)^{14}$

$\equiv 9 \cdot (-80)^{14} \equiv 9 \cdot ((-80)^2)^7 \equiv 9 \cdot (-12)^7$

$\equiv 9 \cdot (-12) \cdot (-12)^6 \equiv (-108) \cdot ((-12)^2)^3$

$\equiv (-108) \cdot (144)^3 \equiv (-108) \cdot (85)^3 \equiv (-108) \cdot 85$

$\cdot 85^2 \equiv (-9180) \cdot 7225 \equiv 209 \cdot 126 \equiv 228$

$\equiv -1 \pmod{229}$

$\Rightarrow$ 229 prim

$b=5$

$5^{57} \pmod{229} \equiv 5 \cdot 5^{56} \equiv 5 \cdot (5^2)^{28}$

$\equiv 5 \cdot 25^{28} \equiv 5 \cdot (25^2)^{14} \equiv 5 \cdot (625)^{14}$

$\equiv 5 \cdot (167)^{14} \equiv 5 \cdot (167^2)^7 \equiv 5 \cdot (180)^7$

$\equiv 5 \cdot 180 \cdot (180^2)^3 \equiv 213 \cdot ((-49)^2)^3$

$\equiv (-16) \cdot (111)^3 \equiv (-16) \cdot 111 \cdot 111^2$

$\equiv (-1776) \cdot 128 \equiv 56 \cdot 101 \equiv 160 \pmod{229}$

$(5^{57})^2 \pmod{229} \equiv (5^2)^{57} \equiv 25^{57} \equiv$

$\equiv 25 \cdot 25^{56} \equiv 25 \cdot (25^2)^{28} \equiv 25 \cdot (167)^{28}$

$\equiv 25 \cdot (167^2)^{14} \equiv 25 \cdot (180)^{14} \equiv 25 \cdot (180^2)^7$

$\equiv 25 \cdot (111)^7 \equiv 25 \cdot 111 \cdot (111^2)^3 \equiv 27 \cdot 101^3$

$\equiv 27 \cdot 101 \cdot 101^2 \equiv 208 \cdot 125 \equiv 123 \pmod{229}$