Gabriel Cotizani Faria Oliveira - 20 14004

Seja n os 4 últimos dígitos do seu número de matrícula na UFOP, acrescido do dígito 1 no final. Por exemplo, um aluno com número de matrícula 20.2.1234, deverá considerar o número 12.341.

Utilize o Pequeno Teorema de Fermat para testar se este número (de 5 dígitos) é composto (não primo). Utilize o algoritmo de exponenciação modular para fazer os cálculos.

① Minha matrícula = 4004

② $a = 2$

p = número de matrícula + 1 = 40041

③ Convertendo n para binário = 1001110001101000

④ $2^{40040} \equiv 148 \bmod 40041$

$(40040)_2$	$c_0 = 1$
1	$c_1 = 1^2 \cdot 2^1 = 1 \cdot 2 = 2 \bmod 40041$
0	$c_2 = 2^2 \cdot 2^0 = 4 \cdot 1 = 4 \bmod 40041$
0	$c_3 = 4^2 \cdot 2^0 = 16 \cdot 1 = 16 \bmod 40041$
1	$c_4 = 16^2 \cdot 2^1 = 256 \cdot 2 = 512 \bmod 40041$
1	$c_5 = 512^2 \cdot 2^1 = 262144 \cdot 2 = 524288 = 3755 \bmod 40041$
1	$c_6 = 3755 \cdot 2^1 = 14100025 \cdot 2 = 28200050 = 11186 \bmod 40041$
0	$c_7 = 11186^2 \cdot 2^0 = 125126596 = 38512 \bmod 40041$
0	$c_8 = 38512^2 \cdot 2^0 = 1483174144 = 15463 \bmod 40041$
0	$c_9 = 15463^2 \cdot 2^0 = 239104369 = 19558 \bmod 40041$

1	$c_{10} \equiv 19558^2 \cdot 2^1 = 382515364 \cdot 2 = 7382 \bmod 40041$
1	$c_{11} = 7382^2 \cdot 2^1 = 54493924 \cdot 2 = 36287 \bmod 40041$
0	$c_{12} = 36287^2 \cdot 2^0 = 1316746369 = 38125 \bmod 40041$
1	$c_{13} = 38125^2 \cdot 2^1 = 1453515625 \cdot 2 = 14609 \bmod 40041$
0	$c_{14} = 14609^2 \cdot 2^0 = 213422881 = 4351 \bmod 40041$
0	$c_{15} = 4351^2 \cdot 2^0 = 18931201 = 31849 \bmod 40041$
0	$c_{16} = 31849^2 \cdot 2^0 = 1014358801 = 148 \bmod 40041$

Logo, $148 \bmod 40041$. Como 148 é o resto e é maior que 1, 40041 não é primo, mas sim composto