Questão 4 - parte 2 V ou F

Nº	Afirmativa	Resposta	Explicação
1	O algoritmo de Euclides estendido é utilizado para calcular o inverso modular de um número.	**V**	O código mostrado é justamente uma implementação do **Algoritmo de Euclides estendido**, que calcula o inverso modular `x1` de `a` em relação a `m`.
2	Se mdc(G, Zn) ≠ 1, o programa ainda consegue encontrar o inverso de G em Zn.	**F**	O inverso modular **só existe** quando `mdc(G, Zn) = 1`. Caso contrário, o cálculo não é válido.
3	A operação `(H * inverso) % Zn` representa a divisão modular de H por G.	**V**	Dividir em aritmética modular é o mesmo que multiplicar pelo inverso: `H / G mod Zn = (H * G⁻¹) mod Zn`.
4	Se n1 for primo, o código aplica o Pequeno Teorema de Fermat para simplificar o cálculo de a^x mod n1.	**V**	Quando `n1` é primo, vale `a^(n1-1) ≡ 1 (mod n1)` (se `a` e `n1` são coprimos); o código reduz o expoente com base nisso.
5	A função powMod implementa o cálculo de potência modular utilizando multiplicações diretas sem otimização.	**F**	A função usa **exponenciação binária** (`exp & 1`, `exp >>= 1`), que é o método **otimizado**, não multiplicações diretas.
6	Quando o resultado do inverso é negativo, o código ajusta o valor somando o módulo m0.	**V**	O trecho `if (x1 < 0) x1 += m0;` faz exatamente esse ajuste.
7	O cálculo de φ(n1) (função totiente de Euler) é utilizado apenas quando n1 não é primo.	**V**	Se `n1` for primo aplica-se Fermat (`n1-1`), e se não for primo aplica-se Euler (usa φ(n1)).