# Atividade INDIVIDUAL sobre a teoria dos números

(Esta atividade vale uma questão de 1 ponto da prova 1)

**Prazo: 07/11/2018 às 23:55h**

**Regras gerais:**

- Os programas devem ser elaborados para testes automatizados. Portanto as entradas e saídas devem ser precisamente implementadas.
- ATENÇÃO: Cada teste terá um **único caso de teste**.
- Os **múltiplos valores** de entrada ou saída serão separados por um único **espaço**, **finalizando com caractere de final-de-linha**.

1. Implementar o algoritmo de Euclides Estendido para o cálculo do GCD e inverso (se existir). Os detalhes do algoritmo foram apresentados em sala de aula e podem ser encontrados facilmente na literatura.

Entrada: Dois números inteiros $X$ e $N$, com $2 \leq X$ , $N < 2^{31}$.

Saída: Dois números inteiros $G$ (gcd) e $I$ (inverso), tal que $I = X^{-1} \bmod N$. Se não existir o inverso deve ser escrito a letra "N".

Exemplos

| Entrada | Saída |
|---|---|
| 5 13 | 1 8 |

| Entrada | Saída |
|---|---|
| 15 102 | 3 N |

2. Implementar o algoritmo do Quadrado-e-Multiplicação para calcular a exponenciação modular de inteiros, $Y = X^k \bmod N$. Os detalhes do algoritmo foram apresentados em sala de aula e podem ser encontrados facilmente na literatura.

Entrada: Três números inteiros X, k, N, com $2 \leq X$ , $k$, $N < 2^{32}$.

Saída: Um número inteiro Y, resultado da exponenciação.

Exemplos

| Entrada | Saída |
|---|---|
| 6 11 13 | 11 |

| Entrada | Saída |
|---|---|
| 2215 5545 16381 | 11105 |

Qualquer dúvida pode ser retirada por e-mail.