S T Q Q S S D

__/__/__

11Q → a) Temos que $x^e \equiv a \pmod N$ satisfaz:

$$0 \leq x^e < N$$

E, como dito em aula, podemos assumir que $e > 0$.

Como sabemos, a aritmética modular é caracterizada pela congruência com relação a um determinado valor, isto é, o módulo.

Sendo $0 \leq x^e < N$, onde N é o valor do módulo, podemos dizer que não haverá a existência de múltiplos ciclos, isto é, a lógica responsável para descobrir o valor de

$$x^e \equiv a \pmod N$$

irá se assemelhar a aritmética comum.

Logo, para descobrirmos o valor de $x^e \equiv a \pmod N$, satisfazendo as condições citadas anteriormente, basta realizarmos o mesmo processo que em aritmética comum.