# Exercices Série 7

1) Appliquez l'algorithme d'exponentiation rapide pour calculer $12^{27}\ mod\ 15$.

2) Montrez que $(a+b)\ mod\ N \equiv_N (a\ mod\ N) + (b\ mod\ N)$

# Réponses

1) $12^{27}\ mod\ 15 = (12^{16} \times 12^{8} \times 12^{2} \times 12^{1})\ mod\ 15 = (12^{16} mod\ 15 \times 12^{8} mod\ 15 \times 12^{2} mod\ 15 \times 12^{1} mod\ 15) mod\ 15 = (6 \times 6 \times 9 \times 12) mod\ 15 = 3$.

2) Si $(a+b)\ mod\ N = X$ alors il existe $K \in \mathbb{N}$ tel que $(a+b) = K \times N + X$.

   De plus, notons $a\ mod\ N = Y$ et $b\ mod\ N = Z$, ce qui signifie qu'il existe $L, M \in \mathbb{N}$ tels que $a = L \times N + Y$ et $b = M \times N + Z$.
   Remplaçons $a$ et $b$ avec $X, Y$ et $Z$, nous aurons
   $$(a+b) = K \times N + X = (L \times N + Y) + (M \times N + Z)$$

   En regroupant les termes, on aura
   $$K \times N + X = (L+M) \times N + (Y+Z)$$

   Prenons le modulo $N$ des deux côtés, cela nous donnera
   $$(a+b)\ mod\ N = X = [(L+M) \times N + (Y+Z)] mod\ N$$
   Rappelons que nous avons noté $(a+b) mod\ N = X$. De plus, par définition du modulo $mod\ N$, tout multiple de $N$ est égal à zéro, donc
   $(L+M) \times N + (Y+Z) \equiv_N (Y+Z)$, $(L+M) \times N$ étant un multiple de $N$ !

   Par conséquent, nous avons prouvé que $(a+b)\ mod\ N = X \equiv_N Y + Z$ or, en remplaçant les définitions de $Y$ et $Z$, cela donne que
   $$(a+b)\ mod\ N \equiv_N (a\ mod\ N) + (b\ mod\ N). \qquad \square$$