Exercices Série 8

1. Trouvez le PGCD ainsi que les coefficients de Bézout pour a = 2869 et b = 235. Trouvez l'inverse de 2869 modulo 235 ou prouvez qu'il n'en existe pas.

2. Montrez que $a \times (b + c) \equiv_N (a \; mod \; N) * (b \; mod \; N) + (a \; mod \; N) * (c \; mod \; N)$.

3. Appliquez l'algorithme d'exponentiation rapide pour calculer $14^{603} \; mod \; 11$.

Corrigé :

1. PGCD(2869, 235) = $\mathbf{1} \; = \; 2869 \times \; \mathbf{24} \; + \; \; 235 \; \times \; (-\mathbf{293})$.
   Le résultat ci-dessus nous dit que $1 \; = \; 2869 \times \; 24 \; + \; \; 235 \; \times \; (-293)$. Prenons le modulo 235 des deux côtés, cela nous donne que
   $1 \; mod \; \; 235 \; = (2869 \times \; 24) mod \; 235 \; + \; \; \big(235 \; \times \; (-293)\big) mod \; 235.$

   Or, par définition du modulo, $\big(235 \; \times \; (-293)\big) mod \; 235 = 0$ (c'est un multiple de 235 !), et $1 \; mod \; \; 235 \; = 1$ (car $1 \in [0, 234]$) donc

   $$1 = (2869 \times \; 24) mod \; 235$$

   Autrement dit, 24 est l'inverse modulaire de 2869 ou, si a et b sont premiers entre eux, alors $PGCD(a, b) = \; 1 = a \times x + b \times y$. Le coefficient de Bézout x est l'inverse de a modulo b, et de même, y est l'inverse de b modulo a !

2. Par définition du modulo, notons que
   $a = K_a N + r_a$, $b = K_b N + r_b$ et $c = K_c N + r_c$. Ainsi on a que

   $a \times (b + c) = ab + ac = (K_a N + r_a) \times (K_b N + r_b) + (K_a N + r_a) \times (K_c N + r_c)$
   $= (K_a K_b N + K_a r_b + K_b r_a) \times N + r_a \times r_b \; + \; \; (K_a K_c N + K_a r_c + K_c r_a) \times N + r_a \times r_c$
   $= \Delta_{ab} N + r_a r_b + \; \Delta_{ac} N + r_a r_c = (\Delta_{ab} + \Delta_{ac}) N + r_a r_b + r_a r_c$

   Prenons le modulo des deux côtés => les multiples de N tombent !
   $[a \times (b + c)] mod \; N = [r_a r_b + r_a r_c] mod \; N$
   Où $r_a = a \; mod \; N, r_b = b \; mod \; N$ et $r_c = c \; mod \; N$ par définition.
   Ayant le $mod \; N$ des deux côtés de l'équation, nous pouvons remplacer celle-ci par une congruence modulo N, ainsi

   $a \times (b + c) \equiv_N r_a r_b + r_a r_c = \; (a \; mod \; N) * (b \; mod \; N) + (a \; mod \; N) * (c \; mod \; N)$.

   CQFD.

3. $14^{603} \; mod \; 11 = 5$.