Exercices Série 9

1. Appliquez l'algorithme d'exponentiation rapide pour calculer $12^{117}\ mod\ 23$.

2. Montrez que $a \in \mathbb{N}^*$ a un inverse modulaire modulo N ***si et seulement si*** $PGCD(a, N) = 1$.

3. Vérifiez que le Petit Théorème de Fermat s'applique pour $a = 10$ et $p = 7$. Vérifiez également si cela fonctionne pour 3 paires a et p de votre choix (essayez au moins une paire dont le PGCD n'est PAS 1) !

4. Calculez l'indice d'Euler pour $n = 10, 12\ et\ 23$.

5. Montrez que si n est un nombre premiers, alors $\varphi(n) = n - 1$.

Corrigé :

1. $12^{117}\ mod\ 23 = 16$
2. Les preuves de « si et seulement si » doivent se faire dans les deux sens entre les deux propositions. Ici
   A : $a \in \mathbb{N}^*$ a un inverse modulaire modulo N
   B : $PGCD(a, N) = 1$.

   <u>A => B</u>

   Comme a un inverse modulo N, on peut dire qu'il existe $x \in \mathbb{Z}^*$ tel que $ax \equiv_N 1$. Par définition du modulo, cela signifie qu'il existe un entier $k \in \mathbb{N}$ tel que $ax = 1 + Nk$. Si on réarrange, on obtient que $ax - Nk = 1$. Or, en posant $y = -k$, cela nous donne l'équation de Bachez-Bézout : $ax + Ny = 1$. Donc $PGCD(a, N) = 1$ par le Théorème de Bachez-Bézout. Cela prouve que A => B.

   <u>B => A</u>
   Si $PGCD(a, N) = 1$ par le théorème de Bachet-Bézout, il existe deux entiers $x, y \in \mathbb{Z}$ tels que $PGCD(a, N) = 1 = ax + Ny$.
   Prenons le modulo N des deux côtés de l'égalité, cela donne que

   $$1\ mod\ N \equiv_n (ax + Ny)\ mod\ N \equiv_n (ax)\ mod\ N + (Ny) mod\ N$$

   Or Ny étant un multiple de N, $(Ny) mod\ N = 0$ et donc
   $1 \equiv_n ax$. Ce qui prouve que a a bien un inverse modulaire, modulo N. Cela prouve que B => A.

   CQFD.

3. Vous pouvez utiliser l'algorithme d'exponentiation rapide ou via la calculatrice vérifier que $1'428'571 \times 7 = 9'999'997$ et $10^7 = 1'428'571 \times 7 + 3 \equiv_7 3 = 10\ mod\ 7$.
   De même, on vérifie que $10^6 = 142'857 \times 7 + 1 \equiv_7 1$.

4. $\varphi(10) = 4$ (1,3,7,9)
   $\varphi(12) = 4$ (1,5,7,11)
   $\varphi(23) = 22$ (1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,1,19,20,21,22,23).

5. Si n est premier, alors par définition, ses seuls diviseurs sont 1 et n lui-même. Par conséquent, 2, 3, …, $n-1$ sont premiers avec n. De plus, $PGCD(1,n) = 1$ donc 1 compte aussi dans l'indice d'Euler – en fait, seul n n'est pas premier avec n ! Donc, il y a $n-1$ nombres qui sont premiers avec n entre 1 et n, donc $\varphi(n) = n - 1$.

   CQFD.