TP-test

1. Écrire une procédure **evalue** qui à un polynôme P et une matrice carrée A associe $P(A)$. Tester cette procédure sur

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & 6 \\ 0 & 0 & 2 \end{pmatrix}, \qquad P(x) = x^3 - 2x^2 - x + 2.$$

2. Les permutations sont données sous forme de liste. Par exemple,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix} \text{ est donnée sous la forme } \mathbf{tau}\text{: } [\mathbf{3}, \mathbf{4}, \mathbf{2}, \mathbf{5}, \mathbf{1}].$$

   Écrire une procédure **valeurinverse** qui a une permutation σ est un entier i associe l'entier $\sigma^{-1}(i)$. L'utiliser pour écrire une procédure donnant l'inverse d'une permutation σ. Tester cette procédure sur la permutation τ ci-dessus. *Remarque* : on ne demandera pas à ces procédures de vérifier que σ est bien une permutation.

3. Écrire une procédure donnant la matrice de transvection $T_{i,j}(\lambda)$ de taille n.

4. On dit que $n \in \mathbb{N}$ satisfait au test de Fermat pour le témoin $a \in \{1, ..., n-1\}$ si a et n ne sont pas premiers entre eux ou bien si n est un diviseur de $a^{n-1} - 1$. Écrire une procédure **testFermat**(n,a) qui retourne **true** si n passe le test de Fermat de témoin a et retourne **false** sinon. Par exemple la procédure retournera **true** pour $n = 561$ et $a = 3$ et $a = 7$ mais **false** pour $n = 400$ et $a = 3$

5. On dit que $n \in \mathbb{N}$ est pseudo-premier s'il passe le test de Fermat pour tous les témoins $a \in \{1, ..., n-1\}$. Écrire une procédure **estPseudoPremier**(n) qui teste si n est un pseudo-premier. Vérifier que 561 est pseudo-premier.

6. Un nombre pseudo-premier qui n'est pas premier est appelé nombre de Carmichael. Écrire une procédure **Carmichael** retournant les nombres de Carmichael inférieur ou égaux à 3000.

Aide-mémoire

— **hipow** permet de calculer le degré d'un polynôme.
— **coeff** permet d'extraire les coefficients d'un polynôme.
— **A^^k** calcule la puissance k-ième de A, lorsque A est une matrice carrée.
— **ident** permet de créer une matrice identité.
— **ematrix** permet de créer une matrice élémentaire.
— **length** permet d'obtenir la longueur d'une liste.
— **append** permet de concaténer des listes.
— **gcd** permet de calculer le pgcd de deux nombres.
— **mod** permet de tester si un nombre est divisible par un autre.
— **primep** permet de tester si un nombre est premier.