QCM

Nom et prénom :

. . . . . .

. . . . . .

Durée/Duration : 15 minutes.
Aucun document n'est autorisé.
No document allowed.
L'usage de la calculatrice est interdit.
Using a calculator is forbidden.
Les questions faisant apparaître le symbole ♣ peuvent présenter une ou plusieurs bonnes réponses.
Questions with ♣ symbole may have one or several correct answers.
Les autres ont une unique bonne réponse.
The other ones have a unique correct answer.

— Si aucune réponse n'est cochée pour une question, alors aucun point n'y est attribué ni retranché.
If no answer is marked, then no point is earned nor removed.
— Sinon, si seules toutes les bonnes réponses sont cochées, alors un point y est attribué.
Otherwwise, if only all the correct answers are marked, then one point is earned.
— Sinon un point y est retranché.
Otherwise a point is removed.

Question [`eval1`] ♣ On sait évaluer un polynôme de degré $n-1$ en un point en
We know how to evaluate a polynomial of degree $n-1$ in a point in

- ■ $O(n)$ opérations/operations.
- ■ $O(n^2)$ opérations/operations.
- ■ $O(\mathsf{M}(n)\log n)$ opérations/operations.
- □ *Aucune de ces réponses n'est correcte.*

Question [`evaln`] ♣ On sait évaluer un polynôme de degré $n-1$ en n points en
We know how to evaluate a polynomial of degree $n-1$ in n points in

- ■ $O(\mathsf{M}(n)\log n)$ opérations/operations.
- □ $O(n)$ opérations/operations.
- ■ $O(n^2)$ opérations/operations.
- □ *Aucune de ces réponses n'est correcte.*

Question [`asympteval`] Asymptotiquement, il est plus facile d'évaluer un polynôme de degré $n-1$ en n points que de l'interpoler en ces n points.
Asymptotically, it is easier to evaluate a polynomial of degree $n-1$ in n points than to interpolate it in these n points.

- □ Vrai/True.
- ■ Faux/False.

Question [`asymptinterpol`] Asymptotiquement, il est aussi difficile d'interpoler un polynôme de degré $n-1$ en n points que de l'évaluer en ces n points.
Asymptotically, it is as difficult to interpolate a polynomial of degree $n-1$ in n points than to evaluate it in these n points.

- ■ Vrai/True.
- □ Faux/False.

Question [`Aprime0`] Si pour $i \neq j$, $x_i \neq x_j$ et $A = \prod_{i=0}^{n-1}(x - x_i)$, alors on peut avoir $A' \bmod (x - x_i) = 0$.
If for $i \neq j$, $x_i \neq x_j$ and $A = \prod_{i=0}^{n-1}(x - x_i)$, then we can have $A' \bmod (x - x_i) = 0$.

- □ Vrai/True.
- ■ Faux/False.

Question [`diveucl`] ♣ On sait effectuer la division euclidienne d'un polynôme de degré $2n$ par un polynôme de degré n en
We can perform the Euclidian division of a polynomial of degree $2n$ by one of degree n in

- □ $O(n)$ opérations/operations.
- ■ $O(\mathsf{M}(n)\log n)$ opérations/operations.
- ■ $O(\mathsf{M}(n))$ opérations/operations.
- ■ $O(n^2)$ opérations/operations.

Question [`Aprime0`] Pour $x_0, \dots, x_{n-1}$ des points disctints deux à deux et $L_i = \prod_{\substack{0 \leqslant j \leqslant n-1 \\ j \neq i}} (x - x_j)$, on sait calculer $L_0(x_0), \dots, L_{n-1}(x_{n-1})$ en $O(\mathsf{M}(n))$ opérations.
For pairwise distinct points $x_0, \dots, x_{n-1}$ and $L_i = \prod_{\substack{0 \leqslant j \leqslant n-1 \\ j \neq i}} (x - x_j)$, we know how to compute $L_0(x_0), \dots, L_{n-1}(x_{n-1})$ in $O(\mathsf{M}(n))$ operations.

☐ Vrai/True. ■ Faux/False.

Question [`Shamir1`] Le partage de clef de Shamir de régime $(1; n)$ ne nécessite qu'un seul participant pour retrouver le secret.
Shamir's secret sharing of parameters $(1; n)$ only requires one participant to recover the secret.

■ Vrai/True. ☐ Faux/False.

Question [`Shamir2`] ♣ Dans un partage de clef de Shamir de régime $(2; 3)$, si les clefs des participants sont $(1, 1)$ et $(2, 1)$ dans $\mathbb{F}_3$, alors la clef secrète est
In Sharmir's secret sharing of parameters $(2; 3)$, if the shared are $(1, 1)$ and $(2, 1)$ in $\mathbb{F}_3$, then the secret is

■ 1. ☐ 2.
☐ 0. ☐ *Aucune de ces réponses n'est correcte.*

Question [`Hankelcreuse2`] Une famille $(M_n)_{n \in \mathbb{N}}$ de matrices de Hankel dans $\mathbb{K}^{n \times n}$ est une famille de matrices creuses.
A family $(M_n)_{n \in \mathbb{N}}$ of Hankel matrices in $\mathbb{K}^{n \times n}$ is a family of sparse matrices.

☐ Vrai/True. ■ Faux/False.

Question [`diagcreuse`] Une famille $(M_n)_{n \in \mathbb{N}}$ de matrices diagonales dans $\mathbb{K}^{n \times n}$ est une famille de matrices creuses.
A family $(M_n)_{n \in \mathbb{N}}$ of diagonal matrices in $\mathbb{K}^{n \times n}$ is a family of sparse matrices.

■ Vrai/True. ☐ Faux/False.

Question [`mulcreuse`] ♣ Deux matrices creuses de tailles n et ayant $m \geqslant n$ coefficients non nuls peuvent être multipliées en
Two sparse matrices of size n with $m \geq n$ nonzero entries can be multiplied in

■ $O(mn)$ opérations/operations. ■ $O(m^2)$ opérations/operations.
■ $O(n^3)$ opérations/operations. ☐ $O(m)$ opérations/operations.

Question [`LUcreuse`] ♣ La décomposition LU d'une matrice creuse
The LU decomposition of a sparse matrix

■ peut être dense/can be dense. ☐ est toujours dense/is always dense.
■ peut être creuse/can be sparse. ☐ est toujours creuse/is always sparse.

Question [`Wiedemann1`] Si une matrice $M \in \mathbb{K}^{n \times n}$ vérifie $M^d + p_{d-1}M^{d-1} + \cdots + p_0 \mathrm{Id} = 0$, alors pour tout $x, y \in \mathbb{K}^n$ et $i \in \mathbb{N}$, $u_{i+d} + p_{d-1}u_{i+d-1} + \cdots + p_0 u_i = 0$ avec $u_i = y^{\mathrm{T}} M^i x$.
If a matrix $M \in \mathbb{K}^{n \times n}$ satisfies $M^d + p_{d-1}M^{d-1} + \cdots + p_0 \mathrm{Id} = 0$, then for all $x, y \in \mathbb{K}^n$ and $i \in \mathbb{N}$, $u_{i+d} + p_{d-1}u_{i+d-1} + \cdots + p_0 u_i = 0$ with $u_i = y^{\mathrm{T}} M^i x$.

■ Vrai/True. ☐ Faux/False.

Question [`Wiedemann2`] Si une matrice $M \in \mathbb{K}^{n \times n}$ et un vecteur $x \in \mathbb{K}^n$ vérifient pour tout $i \in \mathbb{N}$, $s_{i+d} + p_{d-1}s_{i+d-1} + \cdots + p_0 s_i = 0$ avec $s_i = M^i x$, alors M vérifie $M^d + p_{d-1}M^{d-1} + \cdots + p_0 \mathrm{Id} = 0$.
If a matrix $M \in \mathbb{K}^{n \times n}$ and a vector $x \in \mathbb{K}^n$ satisfy for all $i \in \mathbb{N}$, $s_{i+d} + p_{d-1}s_{i+d-1} + \cdots + p_0 s_i = 0$ with $s_i = M^i x$, then M satisfies $M^d + p_{d-1}M^{d-1} + \cdots + p_0 \mathrm{Id} = 0$.

☐ Vrai/True. ■ Faux/False.

Question [`Wiedemann3`] Si une matrice $M \in \mathbb{K}^{n\times n}$ vérifie $M^d + p_{d-1}M^{d-1} + \cdots + p_0\mathrm{Id} = 0$, alors pour tout vecteur $x \in \mathbb{K}^n$ et pour tout $i \in \mathbb{N}$, elle vérifie $s_{i+d} + p_{d-1}s_{i+d-1} + \cdots + p_0 s_i = 0$ avec $s_i = M^i x$.
If a matrix $M \in \mathbb{K}^{n\times n}$ satisfies $M^d + p_{d-1}M^{d-1} + \cdots + p_0\mathrm{Id} = 0$, then for any vector $x \in \mathbb{K}^n$ and for all $i \in \mathbb{N}$, it satifies $s_{i+d} + p_{d-1}s_{i+d-1} + \cdots + p_0 s_i = 0$ with $s_i = M^i x$.

- [x] Vrai/True.
- [ ] Faux/False.

Question [`Wiedemann4`] Si une matrice $M \in \mathbb{K}^{n\times n}$ et deux vecteurs $x, y \in \mathbb{K}^n$ vérifient pour tout $i \in \mathbb{N}$, $u_{i+d} + p_{d-1}u_{i+d-1} + \cdots + p_0 u_i = 0$ avec $u_i = y^{\mathrm{T}} M^i x$, alors M vérifie $M^d + p_{d-1}M^{d-1} + \cdots + p_0\mathrm{Id} = 0$.
If a matrix $M \in \mathbb{K}^{n\times n}$ and two vectors $x, y \in \mathbb{K}^n$ satisfies for all $i \in \mathbb{N}$, $u_{i+d}+p_{d-1}u_{i+d-1}+\cdots+p_0 u_i = 0$ with $u_i = y^{\mathrm{T}} M^i x$, then M satisfies $M^d + p_{d-1}M^{d-1} + \cdots + p_0\mathrm{Id} = 0$.

- [ ] Vrai/True.
- [x] Faux/False.

Question [`Hankelprod`] ♣ Quel produit de polynômes est représenté par le produit matrix-vecteur suivant ?
Which polynomial product is encoded by the following matrix-vector product ?

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & 0 \\ a_3 & 0 & 0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix}$$

- [x] $a_0x^3 + a_1x^2 + a_2x + a_3$ et/and $b_2x^2 + b_1x + b_0$ modulo x^4
- [ ] $a_3x^3 + a_2x^2 + a_1x + a_0$ et/and $b_2x^2 + b_1x + b_0$ modulo x^4
- [ ] $a_0x^3 + a_1x^2 + a_2x + a_3$ et/and $b_2x^2 + b_1x + b_0$ modulo x^5
- [ ] $a_3x^3 + a_2x^2 + a_1x + a_0$ et/and $b_2x^2 + b_1x + b_0$ modulo x^5

Question [`recurrence`] ♣ Pour calculer la relation de récurrence de la suite $(1, 1, 2, 0, 2, 2)$, il faut appeler l'algorithme d'Euclide étendu sur
To compute the recurrence relation of the sequence $(1, 1, 2, 0, 2, 2)$, one needs to call the extended Euclidean algorithm on

- [x] x^6.
- [x] $x^5 + x^4 + 2x^3 + 2x + 2$.
- [ ] x^5.
- [ ] $1 + x + 2x^2 + 2x^4 + 2x^5$.

Question [`recurrence2`] ♣ Pour calculer la relation de récurrence de la suite $(0, 1, 2, 3, 3, 2, 1, 0)$, il faut appeler l'algorithme d'Euclide étendu sur
To compute the recurrence relation of the sequence $(0, 1, 2, 3, 3, 2, 1, 0)$, one needs to call the extended Euclidean algorithm on

- [x] x^8.
- [x] $x^6 + 2x^5 + 3x^4 + 3x^3 + 2x^2 + x$.
- [ ] x^7.
- [ ] x^9.

Question [`bm`] ♣ Supposons que l'algorithme de Berlekamp–Massey calcule la suite de triplets $(R_i, U_i, V_i) : (x^4, 1, 0)$, $(x^3, 0, 1)$, $(0, 1, -x)$. La relation de récurrence satisfaite par la suite est alors, pour tout $i \in \mathbb{N}$,
Assume that the Berlekamp–Massey algorithm computes the triplets sequence $(R_i, U_i, V_i) : (x^4, 1, 0)$, $(x^3, 0, 1)$, $(0, 1, -x)$. The linear recurrence relation satisfied by the sequence is then, for all $i \in \mathbb{N}$,

- [x] $u_{i+1} = 0$.
- [ ] $u_i = 0$.
- [ ] $xu_i = 0$.
- [ ] *Aucune de ces réponses n'est correcte.*