**Recasages possibles** : 101, 123, 152, 190
**Référence** : Carnet de voyages en algébrie, Caldero, Peronnier (p. 9, 70-73).

**Développement**

**Lemme 1** En notant $g_n = \#\mathrm{GL}_n(\mathbb{F}_q)$, on a $g_n = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

**Théorème 2**

(i) On a $\#\mathcal{D}_n(\mathbb{F}_q) = \displaystyle\sum_{\substack{(n_1,\dots,n_q)\in\mathbb{N}^q \\ n_1+\cdots+n_q=n}} \frac{g_n}{\displaystyle\prod_{i=1}^{q} g_{n_i}}$

(ii) La probabilité de choisir une matrice diagonalisable lors d'un tirage aléatoire uniforme dans $\mathcal{M}_n(\mathbb{F}_q)$ tend vers $\frac{1}{n!}$ lorsque $q$ tend vers $+\infty$.

- *Preuve du Lemme 1* : Une matrice $M$ est élément de $\mathrm{GL}_n(\mathbb{F}_q)$ si et seulement si ses colonnes forment une famille libre (donc une base) de $\mathbb{F}_q^n$. Ainsi, on se ramène à dénombrer les familles libres $(e_1,\dots,e_n)$ de vecteurs de $\mathbb{F}_q^n$. Le premier vecteur $e_1$ d'une telle famille est nécessairement non nul (toute famille contenant le vecteur nul est liée), mais par le théorème de la base incomplète, tout vecteur non nul convient : il y a $q^n-1$ choix. Pour que la famille reste libre, il est nécessaire que $e_2 \notin \mathrm{Vect}(e_1)$. Or, $\#\mathrm{Vect}(e_1) = q$ car $\mathbb{F}_q \simeq \mathrm{Vect}(e_1)$ (en tant que $\mathbb{F}_q$-espaces vectoriels, donc en tant qu'ensembles). De plus, à nouveau par la base incomplète, tout vecteur de $\mathbb{F}_q^n \setminus \mathrm{Vect}(e_1)$ convient : il y a $q^n-q$ choix. De la même manière, il faut et il suffit que $e_3 \notin \mathrm{Vect}(e_1,e_2)$ : il y a $q^n-q^2$ choix. On réitère le raisonnement jusqu'à $e_n \notin \mathrm{Vect}(e_1,e_2,\dots,e_{n-1})$ pour lequel on obtient $q^n-q^{n-1}$ choix. Tous ces choix étant indépendants les uns des autres, on voit que le nombre de familles libres de $n$ vecteurs de $\mathbb{F}_q^n$ est $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$. Par le raisonnement du début, on obtient bien $g_n = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

- *Preuve du Théorème 2, (i)* : Considérons l'action de $\mathrm{GL}_n(\mathbb{F}_q)$ sur $\mathcal{D}_n(\mathbb{F}_q)$ par conjugaison, *i.e* l'application

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{F}_q)\times\mathcal{D}_n(\mathbb{F}_q) & \longrightarrow & \mathcal{D}_n(\mathbb{F}_q) \\ (P,A) & \longmapsto & PAP^{-1} \end{array}$$

Cette action est bien définie car si $P \in \mathrm{GL}_n(\mathbb{F}_q)$ et $A \in \mathcal{D}_n(\mathbb{F}_q)$, il existe $P' \in \mathrm{GL}_n(\mathbb{F}_q)$ et $D \in \mathcal{M}_n(\mathbb{F}_q)$ diagonale telle que $A = P'DP'^{-1}$. Mais alors,

$$PAP^{-1} = PP'DP'^{-1}P^{-1} = PP'D(PP')^{-1}.$$

Comme $PP' \in \mathrm{GL}_n(\mathbb{F}_q)$, on a bien que $PAP^{-1} \in \mathcal{D}_n(\mathbb{F}_q)$. On veut alors appliquer l'équation aux classes pour cette action de groupe, ce qui donnera le résultat souhaité. Pour cela, introduisons quelques notations : on note $\zeta_1,\dots,\zeta_q$ les éléments deux à deux distincts de $\mathbb{F}_q$ ; pour $\nu = (n_1,\dots,n_q) \in \mathbb{N}^q$ tel que $n_1+\cdots+n_q = n$, on note $D_\nu$ la matrice suivante :

$$D_\nu = \begin{pmatrix} \zeta_1 I_{n_1} & 0 & \dots & 0 \\ 0 & \zeta_2 I_{n_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \zeta_q I_{n_q} \end{pmatrix}$$

Remarquons que dans chaque orbite de l'action, il y a une unique matrice de la forme $D_\nu$ pour un $\nu \in \mathbb{N}^q$ de somme $n$. En effet, si $A \in \mathcal{D}_n(\mathbb{F}_q)$, $A$ est dans la même orbite qu'une matrice diagonale à coefficients dans $\mathbb{F}_q$, donc quitte à conjuguer par une matrice de permutation (qui est bien dans $\mathrm{GL}_n(\mathbb{F}_q)$), on obtient dans l'orbite de $A$ une matrice de la forme $D_\nu$. Pour l'unicité, on voit que si $\nu = (n_1,\dots,n_q), \nu' = (n'_1,\dots,n'_q)$ sont tels que $D_\nu$ soit semblable à $D_{\nu'}$, alors leurs polynômes caractéristiques sont égaux, donc

$$\prod_{i=1}^{q}(X-\zeta_i)^{n_i} = \prod_{i=1}^{q}(X-\zeta_i)^{n'_i}$$

Par unicité de la décomposition en irréductibles dans $\mathbb{F}_q[X]$, on obtient $n_i = n'_i$ pour tout $i \in [\![1,q]\!]$, donc $\nu = \nu'$. Par conséquent, les orbites de l'action étudiée sont paramétrées par les $(n_1,\dots,n_q) \in \mathbb{N}^q$ tels que $n_1+\cdots+n_q = n$. Fixons un tel $q$-uplet $\nu$ et étudions le stabilisateur de $D_\nu$. Plus précisément, montrons que $\mathrm{Stab}(D_\nu)$ est l'ensemble des matrices diagonales par blocs de la forme

$$\begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_q \end{pmatrix} \quad \text{avec } \forall i \in [\![1,q]\!],\ A_i \in \mathrm{GL}_{n_i}(\mathbb{F}_q)$$

Soit $A$ une telle matrice. Le calcul par blocs de son déterminant assure que $A \in \mathrm{GL}_n(\mathbb{F}_q)$. De plus, on a

$$AD_\nu = \begin{pmatrix} \zeta_1 A_1 & 0 & \dots & 0 \\ 0 & \zeta_2 A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \zeta_q A_q \end{pmatrix} = D_\nu A.$$

Ainsi, on a $AD_\nu A^{-1} = D_\nu$ donc $A \in \mathrm{Stab}(D_\nu)$. Réciproquement, soit $M \in \mathrm{GL}_n(\mathbb{F}_q)$ telle que $MD_\nu M^{-1} = D_\nu$. Écrivons $M$ par blocs de la même manière que $D_\nu$ :

$$M = \begin{pmatrix} M_{1,1} & M_{1,2} & \dots & M_{1,q} \\ M_{2,1} & M_{2,2} & \dots & M_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ M_{q,1} & M_{q,2} & \dots & M_{q,q} \end{pmatrix} \quad \text{avec } \forall i,j \in [\![1,q]\!],\ M_{i,j} \in \mathcal{M}_{n_i,n_j}(\mathbb{F}_q)$$

On a alors

$$MD_\nu = \begin{pmatrix} \zeta_1 M_{1,1} & \zeta_2 M_{1,2} & \dots & \zeta_q M_{1,q} \\ \zeta_1 M_{2,1} & \zeta_2 M_{2,2} & \dots & \zeta_q M_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_1 M_{q,1} & \zeta_2 M_{q,2} & \dots & \zeta_q M_{q,q} \end{pmatrix}$$

et

$$D_\nu M = \begin{pmatrix} \zeta_1 M_{1,1} & \zeta_1 M_{1,2} & \dots & \zeta_1 M_{1,q} \\ \zeta_2 M_{2,1} & \zeta_2 M_{2,2} & \dots & \zeta_2 M_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_q M_{q,1} & \zeta_q M_{q,2} & \dots & \zeta_q M_{q,q} \end{pmatrix}$$

Ainsi, si $i \neq j$, comme $\zeta_i \neq \zeta_j$, on obtient de $\zeta_i M_{i,j} = \zeta_j M_{i,j}$ que $M_{i,j} = 0$. Par conséquent, $M$ est diagonale par blocs, et comme $M$ est inversible, ses blocs diagonaux $M_{i,i}$ le sont aussi, d'où $M_{i,i} \in \mathrm{GL}_{n_i}(\mathbb{F}_q)$. On a bien identifié $\mathrm{Stab}(D_\nu)$ et en particulier, son cardinal vaut $\#\mathrm{Stab}(D_\nu) = \prod_{i=1}^{q} g_{n_i}$, car on a $g_{n_1}$ choix pour $M_{1,1}$, puis $g_{n_2}$ choix pour $M_{2,2}$, *etc.* Finalement, l'équation aux classes de cette action donne

$$\#\mathcal{D}_n(\mathbb{F}_q) = \sum_{\substack{\nu=(n_1,\dots,n_q)\in\mathbb{N}^q \\ n_1+\dots+n_q=n}} \frac{\#\mathrm{GL}_n(\mathbb{F}_q)}{\mathrm{Stab}(D_\nu)} = \sum_{\substack{(n_1,\dots,n_q)\in\mathbb{N}^q \\ n_1+\dots+n_q=n}} \frac{g_n}{\prod_{i=1}^{q} g_{n_i}}$$

- *Preuve du Théorème 3, (ii)* : Essayons d'abord de rassembler dans cette somme les termes qui se ressemblent. Pour un $q$-uplet $(n_1,\dots,n_q) \in \mathbb{N}^q$ de masse totale $n$, si on note $m \in [\![1,n]\!]$ le nombre de $n_i$ non nuls, on peut associer à notre $q$-uplet le $m$-uplet $(n_{i_1},\dots,n_{i_m})$ de ces $n_i$ non nuls (où les indices sont ordonnés : $1 \leqslant i_1 < \dots < i_m \leqslant q$). On a encore alors $\sum_{j=1}^{m} n_{i_j} = n$ puisque l'on n'a enlevé que des termes nuls. Inversement si on se donne un $m$-uplet $(\nu_1,\dots,\nu_m) \in \mathbb{N}^{*q}$ tel que $\sum_{j=1}^{m} \nu_j = n$, le nombre de $q$-uplets auxquels il est associé de cette manière est $\binom{q}{m}$ : il faut choisir $1 \leqslant i_1 < \dots < i_m \leqslant q$ et poser $n_{i_j} = \nu_j$ pour tout $j$ (les autres $n_i$ sont automatiquement tous nuls). De plus, tous les $q$-uplets auxquels $\nu$ est associé aboutissent au même terme dans la somme de $\#\mathcal{D}_n(\mathbb{F}_q)$. En effet, on a alors $\prod_{i=1}^{q} g_{n_i} = \prod_{j=1}^{m} g_{\nu_j}$. Par conséquent, en regroupant ces termes similaires, on obtient

$$\#\mathcal{D}_n(\mathbb{F}_q) = \sum_{m=1}^{n} \binom{q}{m} \sum_{\substack{(\nu_1,\dots,\nu_m)\in\mathbb{N}^{*m} \\ \nu_1+\dots+\nu_m=n}} \frac{g_n}{\prod_{j=1}^{m} g_{\nu_j}}$$

Cette expression permet de voir que $\#\mathcal{D}_n(\mathbb{F}_q)$ est une fraction rationnelle en $q$, ce qui permet de ne regarder que le terme de plus haut degré pour obtenir le comportement de $\#\mathcal{D}_n(\mathbb{F}_q)$ quand $q$ est grand. D'après le **Lemme 1**, $g_k$ est un polynôme de degré $k^2$ en $q$ pour tout $k \in \mathbb{N}^*$. Le coefficient binomial

$$\binom{q}{m} = \frac{q!}{m!(q-m)!} = \frac{q(q-1)\cdots(q-m+1)}{m!}$$

est quant à lui un polynôme de degré $m$ en $q$. Ainsi, chaque terme $\binom{q}{m} \frac{g_n}{\prod_{j=1}^{m} g_{\nu_j}}$ est un polynôme en $q$ de degré $m + n^2 - \sum_{j=1}^{m} \nu_j^2$. Or, pour tout $j \in [\![1,m]\!]$, $\nu_j \geqslant 1$, donc $\nu_j^2 \geqslant \nu_j$ et ainsi, le degré de chaque terme de la somme est majoré par $m + n^2 - \sum_{j=1}^{m} \nu_j \leqslant m + n^2 - m = n^2$. On a égalité dans cette majoration si et seulement si $\sum_{j=1}^{m} \nu_j = m$ et $\sum_{j=1}^{m} \nu_j^2 = \sum_{j=1}^{m} \nu_j$ *i.e* si et seulement si $\nu_j = 1$ pour tout $j \in [\![1,m]\!]$. Le terme correspondant dans $\#\mathcal{D}_n(\mathbb{F}_q)$ est

$$\frac{q(q-1)\cdots(q-n+1)}{n!} \times \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{(q-1)^n}$$

dont le monôme dominant est $\frac{q^{n^2}}{n!}$. Ainsi, $\#\mathcal{D}_n(\mathbb{F}_q) \underset{q\to+\infty}{\sim} \frac{q^{n^2}}{n!}$. Mais puisque $\#\mathcal{M}_n(\mathbb{F}_q) = q^{n^2}$, la probabilité de tomber sur une matrice diagonalisable lors d'un tirage uniforme sur $\mathcal{M}_n(\mathbb{F}_q)$ tend vers $\frac{\frac{q^{n^2}}{n!}}{q^{n^2}} = \frac{1}{n!}$.