Matrice de Pascal, comptage de points sur les courbes elliptiques et fonctions sphéroïdales prolates

W. Riley Casper

Résumé : Les vecteurs propres de la matrice de Pascal symétrique T_N de taille $(N+1)\times(N+1)$, sont analogues aux fonctions d'onde sphéroïdales prolates dans le cadre discret.

Les fonctions génératrices des vecteurs propres de T_N sont des fonctions sphéroïdales prolates, au sens où elles sont simultanément fonctions propres d'un opérateur différentiel du troisième ordre et d'un opérateur intégral sur la droite critique $\{z\in\mathbb{C} : \mathrm{Re}(z)=1/2\}$.

Pour les entiers pairs positifs N, on obtient une formule explicite pour la fonction génératrice du vecteur propre de la matrice de Pascal symétrique associé à la valeur propre 1. Lorsque $N=p-1$ pour un nombre premier impair p, nous montrons que la fonction génératrice est équivalente modulo p à $(\#E_z(\mathbb{F}_p)-1)^2$, où $\#E_z(\mathbb{F}_p)$ est le nombre de points de la courbe elliptique de Legendre $y^2=x(x-1)(x-z)$ sur le corps fini $\mathbb{F}_p$.

De plus, lorsque $N=p^n-1$, notre fonction génératrice est le carré d'une période de E_z modulo p^n dans le disque unité p-adique ouvert.

1 Introduction

Les opérateurs intégraux possédant la propriété de sphéroïdalité prolate, qui consiste à commuter avec un opérateur différentiel, apparaissent en théorie des matrices aléatoires et en traitement du signal [19, 20, 22, 23].

L'exemple le plus connu est l'opérateur différentiel de Slepian :

$$\partial_x(x^2-\tau^2)\partial_x-\omega^2x^2$$

Issu du traitement du signal, il commute avec l'opérateur de limitation en temps et en bande :

$$(T_{\omega,\tau}f)(x)=\int_{-\tau}^{\tau}\frac{\sin(x-y)}{x-y}f(y)dy.$$

Les fonctions propres conjointes de ces opérateurs sont appelées **fonctions d'onde sphéroïdales prolates** et ont trouvé d'importantes applications en analyse numérique, en théorie spectrale et en géophysique.

Il est important de noter que le noyau $K_\omega(x,y)$ de l'opérateur de limitation en temps et en bande $T_{\omega,\tau}$ est donné (à un facteur scalaire près) par

$$K_\omega(x,y)=\int_{-\omega}^{\omega}\psi_{\exp}(x,z)\overline{\psi_{\exp}(y,z)}dz,$$

Département de Mathématiques, Université de l'État de Californie Fullerton, Fullerton, CA 92831, U.S.A.
Traduction : Denise Vella-Chemla, décembre 2025.

où $\psi_{\exp}$ désigne la fonction bispectrale exponentielle.

$$\psi_{\exp}(x,z) = e^{2\pi i x z}.$$

Ici, une fonction est bispectrale si $\psi(x,z)$ est une famille de fonctions propres d'un opérateur en x, et simultanément une famille de fonctions propres d'un opérateur en z [7].

En remplaçant la fonction bispectrale exponentielle par les fonctions bispectrales d'Airy ou de Bessel, on obtient les opérateurs intégraux possédant la propriété de sphéroïdalité prolate, découverte par Tracy et Widom dans la théorie des matrices aléatoires [22, 23]. En fait, il est possible de démontrer que cette recette générique engendre des opérateurs intégraux possédant la propriété de sphéroïdalité prolate pour de nombreuses fonctions bispectrales [1, 4].

La construction a été étendue dans de nombreuses directions, notamment aux fonctions bispectrales discrètes-continues et matricielles (par exemple, les polynômes orthogonaux ou les polynômes matriciels orthogonaux satisfaisant des équations différentielles) [3].

Les fonctions propres de l'opérateur différentiel commutatif généralisent naturellement les fonctions sphéroïdales prolates dans divers contextes.

Récemment, Connes et Moscovici ont mis en évidence des similarités intéressantes entre les valeurs propres de l'opérateur prolate de Slepian et les zéros de la fonction zêta de Riemann [6].

L'un des objectifs de cet article est de rechercher des liens similaires en théorie des nombres pour les opérateurs prolates dans l'un de ces contextes étendus.

La matrice (symétrique) de Pascal de taille $(N+1)\times(N+1)$

$$T_N = \begin{bmatrix} \binom{0+0}{0} & \binom{0+1}{0} & \cdots & \binom{0+N}{0} \\ \binom{1+0}{1} & \binom{1+1}{1} & \cdots & \binom{1+N}{1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{N+0}{N} & \binom{N+1}{N} & \cdots & \binom{N+N}{N} \end{bmatrix} \tag{1}$$

est un analogue discret de la construction d'un opérateur intégral présentée ci-dessus.

En particulier, on peut considérer T_N comme l'opérateur intégral discret :

$$(T_N\vec{v})_k = \sum_{j=0}^{N} K_N(j,k)v_j,$$

associé à la fonction bispectrale discrète-discrète $\psi(x,y) = \begin{pmatrix} x \\ y \end{pmatrix}$, dont le noyau est défini par :

$$K_N(j,k) = \sum_{\ell=0}^{N} \psi(j,\ell)\psi(k,\ell) = \begin{pmatrix} j+k \\ j \end{pmatrix}.$$

Compte tenu de la propriété de sphéroïdalité prolate évoquée dans le cadre continu, il n'est pas surprenant que T_N commute avec un analogue discret d'un opérateur différentiel.

Plus précisément, les matrices tridiagonales peuvent être vues comme des versions discrètes d'opérateurs différentiels du second ordre.

Dans [5], les auteurs démontrent que T_N commute avec la matrice tridiagonale $(N+1)\times(N+1)$.

$$J_N = \begin{bmatrix} b(0) & a(1) & 0 & \dots \\ a(1) & b(1) & a(2) & \dots \\ 0 & a(2) & b(2) & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}, \tag{2}$$

avec les entrées suivantes :

$$a(n) = (N+1)^2 n - n^3, \quad \text{et} \quad b(n) = 2n^3 + 3n^2 + 2n - (N+1)^2 n.$$

Par analogie, les vecteurs propres de J_N (équivalent de T_N) devraient être un analogue discret des fonctions d'onde sphéroïdales prolates.

Par conséquent, nous prévoyons que les vecteurs propres de T_N auront de nombreuses applications.

Par exemple, on peut les utiliser pour engendrer des bases orthogonales des sous-espaces propres de la transformation binomiale [5].

En particulier, cela rend la recherche d'expressions explicites pour les vecteurs propres particulièrement intéressante.

Lorsque N est pair, la matrice de Pascal T_N possède $\lambda = 1$ comme valeur propre simple.

Notre premier théorème principal fournit une formule explicite pour la fonction génératrice associée à un vecteur propre.

Théorème A. *Soit N pair. Alors la matrice de Pascal T_N de taille $(N+1)\times(N+1)$ possède un unique vecteur propre $\vec{v} = (v_k)_{k=0}^N$ de valeur propre $\lambda = 1$ (normalisée par $v_N = 1$) donné par la formule de la fonction génératrice :*

$$\sum_{k=0}^N v_k z^{N-k} = {}_2F_1\left[\begin{matrix} -N/2 \;\; N/2+1 \\ -N \end{matrix}; z\right] \cdot {}_2F_1\left[\begin{matrix} -N/2 \;\; N/2+1 \\ -N \end{matrix}; \frac{z}{z-1}\right](1-z)^{N/2}. \tag{3}$$

Pour tout vecteur $\vec{v} \in \mathbb{C}^{N+1}$, on appelle l'expression

$$f(\vec{v}; z) = \sum_{k=0}^N v_k z^{N-k}$$

la fonction génératrice du vecteur $\vec{v}$.

Il s'avère que si $\vec{v}$ est un vecteur propre de J_N, alors c'est un vecteur propre de T_N et la fonction génératrice $f(\vec{v};z)$ est une fonction sphéroïdale prolate classique, au sens où elle est simultanément une fonction propre d'un opérateur intégral et d'un opérateur différentiel.

Théorème B. *Soit $\vec{v} \in \mathbb{C}^{N+1}$ un vecteur propre de la matrice J_N de l'équation* (2) *de valeur propre μ.*

Alors $\vec{v}$ est un vecteur propre de T_N pour une certaine valeur propre λ de T_N et la fonction génératrice $f(\vec{v};z)$ satisfait l'équation intégrale

$$\frac{1}{2\pi i}\int_{\mathrm{Re}(w)=\frac{1}{2}} \frac{1}{w^{N+1}(1-w)^{N+1}(1-z+zw)} f\left(\vec{v};w\right) dw = \lambda f(\vec{v};z) \tag{4}$$

et l'équation différentielle de troisième ordre

$$\begin{aligned}\mu y = {} & z^2(1-z)^2 y''' + 3z(1-z)((N-1)z-N)y'' \\ & + N((2N-5)z^2 + (2-5N)z + 2N+1)y' \\ & + N((2N+1)z + N^2 + N + 1)y\end{aligned} \tag{5}$$

avec $y = f(\vec{v};z)$.

Enfin, nous abordons le problème de l'interprétation des coefficients de $\vec{v}$.

Motivés par le récent résultat de Connes et Moscovici [6], on pourrait espérer que nos fonctions prolate puissent être reliées à une version de la fonction zêta dans un contexte fini bien choisi.

Sur un corps fini $\mathbb{F}_p$, la fonction zêta de Hasse-Weil d'une courbe algébrique est liée au nombre de points de cette courbe sur les extensions algébriques de $\mathbb{F}_p$.

De même, notre troisième théorème principal relie l'expression de notre fonction génératrice au nombre de points d'une courbe elliptique sur le corps fini $\mathbb{F}_p$.

Théorème C. *Soit $N = p-1$ pour un nombre premier impair p. Alors, le vecteur propre $\vec{v}$ de la matrice de Pascal T_N de taille $p \times p$ du théorème A satisfait :*

$$f(\vec{v};z) = \sum_{k=0}^{N} v_k z^{N-k} \equiv (\#E_z(\mathbb{F}_p) - 1)^2 \mod p, \tag{6}$$

où $\#E_z(\mathbb{F}_p)$ est le nombre de points $\mathbb{F}_p$ sur la courbe elliptique E_z de la famille des courbes de Legendre

$$E_z : y^2 = x(x-1)(x-z).$$

Ce théorème découle d'une transformation pfaffienne et de l'égalité

$${}_2F_1\left[\begin{matrix}-N/2 \;\; N/2+1 \\ -N\end{matrix}; z\right] \equiv {}_2\mathbb{P}_1\left[\begin{matrix}\phi \;\; \phi \\ -\end{matrix}; z; p\right] \mod p$$

où ${}_2\mathbb{P}_1\left[\begin{matrix}\phi\ \phi\\ \_\end{matrix};z;p\right]$ est la fonction de période

$$ {}_2\mathbb{P}_1\left[\begin{matrix}\phi\ \ \phi\\ -\end{matrix};z;p\right]=\sum_{x\in\mathbb{F}_p}\phi(x(x-1)(x-z)) $$

pour $\phi(\cdot)=\left(\frac{\cdot}{p}\right)$ le symbole de Legendre [11].

1.1 Une représentation plus approfondie des nombres p-adiques

Le lien entre les fonctions sphéroïdales prolates en traitement du signal et en théorie des nombres, présenté par le théorème C, est surprenant au premier abord.

On peut trouver une explication plus approfondie en considérant l'évaluation de notre fonction génératrice sur les nombres p-adiques pour un nombre premier impair p.

Considérons la série :

$$ F(z)={}_2F_1\left[\begin{matrix}1/2\ \ 1/2\\ 1\end{matrix};z\right]=\sum_{k=0}^{\infty}\binom{2k}{k}^2\frac{z^k}{8^k}. \tag{7} $$

Pour z appartenant au disque unité complexe, cette série est égale à une période de la courbe elliptique de Legendre E_z.

De plus, la série converge p-adiquement pour $z\in\mathbb{Q}_p$ avec $|z|_p<1$ et est une solution p-adique de l'équation différentielle hypergéométrique associée [8, 12].

$$ z(1-z)f''(z)+(1-2z)f'(z)-\frac{1}{4}f(z)=0. \tag{8} $$

Soit $N_n=p^n-1$.

En comparant les coefficients de la série, il apparaît clairement que la fonction génératrice du vecteur propre de la matrice de Pascal symétrique T_{N_n} de taille $(N_n+1)\times(N_n+1)$ trouvée dans le théorème A, c'est-à-dire :

$$ U_n(z)={}_2F_1\left[\begin{matrix}-N_n/2\ \ N_n/2+1\\ -N_n\end{matrix};z\right]\cdot{}_2F_1\left[\begin{matrix}-N_n/2\ \ N_n/2+1\\ -N_n\end{matrix};\frac{z}{z-1}\right](1-z)^{N_n/2} $$

satisfait

$$ U_n(z)\equiv F(z)^2 \mod p^n \quad \text{pour tout } z\in\mathbb{Q}_p \text{ avec } |z|_p<1. $$

Par conséquent, nous avons une convergence p-adique :

$$ U_n(z)\to F(z)^2 \quad \text{pour tout } z\in\mathbb{Q}_p \text{ avec } |z|_p<1. $$

Cette convergence s'explique par une raison conceptuelle plus profonde.

La fonction génératrice $U_n(z)$ est solution de l'équation différentielle du troisième ordre du théorème B, avec $\mu = (N^2 + 2N)/2$ et $N = N_n$.

À la limite, lorsque $n \to \infty$, cette équation différentielle est le carré symétrique de l'équation 8 (voir la définition 3.1) :

$$z^2(1-z)^2 f'''(z) + 3z(1-z)(1-2z)f''(z) + (1 - 7z(1-z))f'(z) - (1/2 - z)f(z) = 0, \qquad (9)$$

dont l'espace des solutions est engendré par les produits des solutions de l'équation 8.

Par ailleurs, l'opérateur intégral du théorème B converge vers la transformation de Kummer $T : f(z) \mapsto \frac{1}{1-z} f\left(\frac{1}{1-z}\right)$.

La transformation T agit sur les solutions de l'équation 9 et est Frobenius-équivariante ; elle préserve donc la filtration de l'espace des solutions par les pentes de Frobenius.

En particulier, la pente 0 (c'est-à-dire la droite de la racine unitaire) est constituée des vecteurs propres de T.

Or, puisque $U_n(z)$ est prolate, elle converge nécessairement vers une solution de l'équation 9 qui est une fonction propre de T, c'est-à-dire une fonction appartenant à la droite de la racine unitaire. Puisque la droite de racine unitaire de l'équation 9 est engendrée par $F(z)^2$ et que $U_n(0) = F(0)^2 = 1$, on en déduit que $U_n(z)$ converge vers $F(z)^2$.

Remarque 1.1 : Le fait que $F(z)^2$ plutôt que $F(z)$ apparaisse ici est naturel, car cela évite notamment d'avoir recours à une racine carrée dans la transformation de Kummer, permettant ainsi à T d'avoir une représentation en série locale T_n au voisinage de $z = 0$.

1.2 Brève histoire de Pascal

Il convient de noter que la matrice symétrique de Pascal T_N possède une longue histoire mathématique.

Selon Muir, F. Calderara a été le premier à considérer T_N et à démontrer que $\det(T_N) = 1$ en 1871. Rutishauser a ensuite démontré que T_N admet une décomposition de Cholesky à l'aide de la transformée binomiale [15], fournissant ainsi une démonstration plus simple du théorème de Calderara.

Le comportement des *valeurs propres* de T_N pour $N = p^n - 1$ modulo p a été étudié par Strauss et Waterhouse en 1986 et 1987 [21, 24], mais aucun vecteur propre n'a été trouvé.

Dans des travaux plus récents, les propriétés de la matrice de Pascal ont été étudiées par Edelman et Strang [9] et Brawer et Pirovino [2], entre autres.

À notre connaissance, notre article est le premier à obtenir une expression explicite pour tout vecteur propre de T_N.

En effet, [2] a été le premier à montrer que T_N possède un vecteur propre rationnel de valeur propre 1, c'est-à-dire que le système diophantien

$$\sum_{k=0}^{N} \binom{j+k}{k} v_k = v_j$$

admet une solution non triviale dans $\mathbb{Q}$ (et donc dans $\mathbb{Z}$) lorsque N est pair. Cependant, les solutions de ce système n'avaient été données numériquement que pour $N = 2, 4, 5, 8$ et 10, et jusqu'à présent, aucune formule explicite pour une solution n'était connue. Le théorème A ci-dessus fournit la solution explicite :

$$v_\ell = \sum_{\substack{j+k=\ell \\ 0 \le j,k \le N/2}} \frac{(-N/2)_j(-N/2)_k(N/2+1)_j(-3N/2-1)_k}{j!k!(-N)_j(-N)_k}, \quad 0 \le \ell \le N,$$

où $(q)_k = q(q+1)\dots(q+k-1)$ est le symbole de Pochhammer (ascendant).

2 Fonctions génératrices des vecteurs propres

2.1 Propriétés fondamentales

Nous commençons par démontrer quelques propriétés fondamentales de l'action de T_N et de J_N sur les fonctions engendrant des vecteurs.

Définition 2.1 : Soit $\vec{v} = (v_k)_{k=0}^N \in \mathbb{C}^{N+1}$.

On définit la fonction génératrice de $\vec{v}$ comme le polynôme suivant :

$$f(\vec{v}; z) = \sum_{k=0}^{N} v_k z^{N-k}.$$

La propriété d'un vecteur $\vec{v}$ d'être un vecteur propre de T_N se traduit directement par une certaine équation fonctionnelle sur la fonction génératrice de $\vec{v}$ grâce au lemme suivant.

Lemme 2.2 : Soit $\vec{v} = (v_k)_{k=0}^N \in \mathbb{C}^{N+1}$. La fonction génératrice de $\vec{v}$ satisfait :

$$f(T_N\vec{v}; z) = \left(\frac{z}{z-1}\right)^{N+1} z^N f\left(\vec{v}; 1-\frac{1}{z}\right) + \frac{1}{z}\sum_{j=0}^{N} v_j \binom{N+1+j}{j} {}_2F_1\left[\begin{matrix}1 \;\; j+N+2 \\ N+2\end{matrix}; \frac{1}{z}\right].$$

Preuve : D'après la série binomiale

$$\begin{aligned}
f(T_N\vec{v};z) &= \sum_{k=0}^{N}\sum_{j=0}^{N}\binom{j+k}{j}v_j z^{N-k} \\
&= \sum_{j=0}^{N} v_j\left(\sum_{k=0}^{\infty}\binom{j+k}{j}z^{N-k} - \sum_{k=N+1}^{\infty}\binom{j+k}{j}z^{N-k}\right) \\
&= \sum_{j=0}^{N} v_j\left[z^N\left(1-\frac{1}{z}\right)^{-j-1} - z^{-1}\binom{j+N+1}{j}{}_2F_1\left[\begin{matrix}1, j+N+2\\ N+2\end{matrix}; z^{-1}\right]\right] \\
&= \frac{z^{2N+1}}{(z-1)^{N+1}}f(\vec{v};1-1/z) - z^{-1}\sum_{j=0}^{N}v_j\binom{j+N+1}{j}{}_2F_1\left[\begin{matrix}1, j+N+2\\ N+2\end{matrix}; z^{-1}\right].
\end{aligned}$$

□

En conséquence immédiate, nous pouvons reformuler la recherche des vecteurs propres de T_N en termes d'un certain problème de valeurs propres d'intégrale résiduelle.

Théorème 2.3 : *Soit $\vec{v} \in \mathbb{C}^{N+1}$. Alors, $\vec{v}$ est un vecteur propre de T_N de valeur propre λ si et seulement si*

$$\frac{1}{2\pi i}\int_{\mathrm{Re}(w)=\frac{1}{2}} \frac{1}{w^{N+1}(1-w)^{N+1}(1-z+zw)} f(\vec{v};w)\,dw = \lambda f(\vec{v};z).$$

Preuve : Puisque $f(T_N\vec{v};z)$ est un polynôme, le lemme précédent nous indique qu'il est égal à la partie polynomiale de

$$\frac{z^{2N+1}}{(z-1)^{N+1}} f\left(\vec{v};1-\frac{1}{z}\right).$$

Ainsi, par le théorème des résidus de Cauchy, on a

$$f(T_N\vec{v};z) = \frac{1}{2\pi i(z-1)^{N+1}}\oint_{|u-1|=1}\left(\frac{1}{u-z} - \sum_{k=0}^{N}\frac{(z-1)^k}{(u-1)^{k+1}}\right)u^{2N+1} f\left(\vec{v};1-\frac{1}{u}\right)du.$$

En calculant la somme géométrique et en utilisant le changement de variables $w = 1 - 1/u$, on obtient :

$$\begin{aligned}
f(T_N\vec{v};z) &= \frac{1}{2\pi i}\oint_{|u-1|=1}\left(\frac{1}{u-1}\right)^{N+1}\frac{u^{2N+1}}{u-z} f\left(\vec{v};1-\frac{1}{u}\right)du \\
&= \frac{1}{2\pi i}\int_{\mathrm{Re}(w)=\frac{1}{2}}\frac{1}{w^{N+1}(1-w)^{N+1}(1-z+zw)} f(\vec{v};w)\,dw.
\end{aligned}$$

L'énoncé du théorème en découle immédiatement.

□

De même, la propriété d'un vecteur $\vec{v}$ d'être un vecteur propre de J_N se traduit directement par une propriété de sa fonction génératrice. On obtient alors que $f(\vec{v};z)$ est une fonction propre polynomiale d'une certaine équation différentielle du troisième ordre.

Théorème 2.4. : *Un vecteur $\vec{v} \in \mathbb{C}^{N+1}$ est un vecteur propre de J de valeur propre associée μ si et seulement si $y = f(\vec{v};z)$ est une solution de*

$$\begin{aligned}\mu y &= z^2(1-z)^2 y''' + 3z(1-z)((N-1)z - N)y'' \\ &\quad + N((2N-5)z^2 + (2-5N)z + 2N + 1)y' \\ &\quad + N((2N+1)z + N^2 + N + 1)y\end{aligned}$$

Preuve : Soit $\vec{v} \in \mathbb{C}^{N+1}$ et soit

$$a(z) = (N+1)^2 z - z^3, \quad \text{et} \quad b(z) = 2z^3 + 3z^2 + 2z - (N+1)^2 z$$

les polynômes définissant la structure de la matrice de Jacobi J_N dans l'équation (2). Alors, puisque $a(N+1) = 0$ et $a(0) = 0$,

$$\begin{aligned}f(J\vec{v};z) &= \sum_{k=0}^{N} v_k (a(k+1) z^{N-k-1} + b(k) z^{N-k} + a(k) z^{N-k+1}) \\ &= \sum_{k=0}^{N} v_k (a(k+1) z^{N-k-1} + b(k) z^{N-k} + a(k) z^{N-k+1}) \\ &= \sum_{k=0}^{N} v_k (z^{-1} a(N - z\partial_z + 1) z^{N-k} + b(N - z\partial_z) z^{N-k} + z a(N - z\partial_z) z^{N-k}) \\ &= (z^{-1} a(N + 1 - z\partial_z) + b(N - z\partial_z) + z a(N - z\partial_z)) \cdot f(\vec{v};z)\end{aligned}$$

Le reste du théorème découle du calcul explicite de l'opérateur

$$z^{-1} a(N + 1 - z\partial_z) + b(N - z\partial_z) + z a(N - z\partial_z).$$

□

En combinant les deux théorèmes précédents, on obtient directement l'énoncé du théorème B.

Preuve du théorème B : Supposons que $\vec{v}$ soit un vecteur propre de J_N associé à la valeur propre μ.

Puisque J_N est une matrice jacobienne, son spectre est simple.

Comme J_N et T_N commutent, $\vec{v}$ est également un vecteur propre de T_N associé à une certaine valeur propre λ.

L'énoncé du théorème B découle alors automatiquement des théorèmes 2.3 et 2.4

2.2 Vecteurs propres et transformation binomiale

La matrice de Pascal symétrique T_N admet la décomposition de Cholesky suivante :

$$T_N = B_N B_N^*,$$

où B_N désigne la transformation binomiale $(N+1) \times (N+1)$.

$$(B_N \vec{v})_j = \sum_{k=0}^{N} (-1)^k \binom{j}{k} v_k, \quad 0 \leq j \leq N.$$

La transformation binomiale est involutive et elle relie par conjugaison T_N en T_N^{-1}. Par conséquent, λ est une valeur propre de T_N si et seulement si λ^{-1} est une valeur propre de T_N. De plus, la transformation binomiale définit un isomorphisme entre les sous-espaces propres associés [5]

$$\begin{tikzcd} E_\lambda(T_N) \arrow[r, bend left, "B"] & E_{1/\lambda}(T_N) \arrow[l, bend left, "B"] \end{tikzcd} .$$

Cette symétrie des données propres se traduit par certaines propriétés des fonctions génératrices correspondantes. Ceci est explicité dans le lemme suivant.

Lemme 2.5 : Soit $\vec{v} = (v_k)_{k=0}^N \in \mathbb{C}^{N+1}$.

La fonction génératrice de $\vec{v}$ satisfait :

$$f(B_N^* \vec{v}; z) = (z-1)^N f\left(\vec{v}; \frac{z}{z-1}\right)$$

$$f(B_N \vec{v}; z) = \left(\frac{z}{z-1}\right)^{N+1} f(\vec{v}; 1-z) - z^{-1} \sum_{j=0}^{N} v_j (-1)^j \binom{N+1}{j} {}_2F_1\left[\begin{matrix} 1 \;\; N+2 \\ N+2-j \end{matrix}; \frac{1}{z}\right].$$

Preuve : Du théorème du binôme,

$$\begin{aligned} f(B_N^* \vec{v}; z) &= \textstyle\sum_{k=0}^N \sum_{j=0}^N (-1)^k \binom{j}{k} v_j z^{N-k} \\ &= \textstyle\sum_{j=0}^N v_j z^{N-j} \sum_{k=0}^N \binom{j}{k} (-1)^k z^{j-k} \\ &= \textstyle\sum_{j=0}^N v_j z^{N-j} (z-1)^j = (z-1)^N f\left(\vec{v}; \frac{z}{z-1}\right). \end{aligned}$$

Également à partir de la série binomiale,

$$\begin{aligned}
f(B_N\vec{v};z) &= \sum_{k=0}^{N}\sum_{j=0}^{N}(-1)^j\binom{k}{j}v_j z^{N-k} \\
&= \sum_{j=0}^{N} v_j(-1)^j\left(\sum_{k=0}^{\infty}\binom{k}{j}z^{N-k} - (-1)^j\sum_{k=N+1}^{\infty}\binom{k}{j}z^{N-k}\right) \\
&= \sum_{j=0}^{N} v_j(-1)^j\left(z^{N+1}\frac{1}{z-1}(z-1)^{-j} - \sum_{k=N+1}^{\infty}\binom{k}{j}z^{N-k}\right) \\
&= \left(\frac{z}{z-1}\right)^{N+1} f(\vec{v},1-z) - z^{-1}\sum_{j=0}^{N} v_j(-1)^j\binom{N+1}{j}{}_2F_1\left[\begin{matrix}1, N+2\\ N+2-j\end{matrix}; z^{-1}\right].
\end{aligned}$$

□

En utilisant le lemme précédent, on peut relier la fonction génératrice d'un vecteur proprre $\vec{v}$ à la fonction génératrice de $B_N\vec{v}$.

Théorème 2.6 : *Soit $\vec{v} \in \mathbb{C}^{N+1}$ un vecteur propre de T_N associé à la valeur propre λ. Alors*

$$\lambda f(\vec{v};z) = (z-1)^N f\left(B_N\vec{v};\frac{z}{z-1}\right).$$

Preuve : En utilisant le lemme précédent avec $B_N\vec{v}$ à la place de $\vec{v}$, on trouve

$$\lambda f(\vec{v};z) = f(T_N\vec{v};z) = f(B_N^* B_N\vec{v};z) = (z-1)^N f\left(B_N\vec{v};\frac{z}{z-1}\right).$$

□

La transformation binomiale permute également les vecteurs propres de J_N [5], et plus précisément, elle intervertit les sous-espaces propres de valeur propre λ et ceux de valeur propre $N^2+2N-\lambda$

$$\begin{tikzcd} E_\lambda(J_N) \arrow[r, bend left, "B"] & E_{N^2+2N-\lambda}(T_N) \arrow[l, bend left, "B"] \end{tikzcd}.$$

Par conséquent, lorsque N est pair, J_N possède un vecteur propre de valeur propre $\frac{N^2+2N}{2}$. Ce vecteur propre est nécessairement un vecteur propre de T_N de valeur propre 1.

Théorème 2.7 : *Soit N pair. Alors $(N^2+2N)/2$ est une valeur propre de J_N et*

$$E_{(N^2+2N)/2}(J_N) \subseteq E_1(T_N).$$

Preuve : Remarquons que $N+1$ est impair et que J_N a un spectre simple ; par conséquent, J_N possède nécessairement un nombre impair de sous-espaces propres non triviaux. La transformation binomiale agit comme une involution sur l'ensemble des sous-espaces propres, donc au moins un sous-espace propre de J_N est préservé par B_N. Puisque B_N transforme le sous-espace propre de λ en celui de $N^2+2N-\lambda$, la seule valeur propre fixe est $\lambda = (N^2+2N)/2$.

Comme J_N a un spectre simple, le sous-espace propre correspondant est engendré par un seul vecteur :

$$E_{(N^2+2N)/2}(J_N) = \mathrm{span}\{\vec{v}\}.$$

De plus, puisque B_N transforme ce sous-espace propre en lui-même, $\vec{v}$ est un vecteur propre de B_N.

Enfin, puisque J_N et T_N commutent, $\vec{v}$ est également un vecteur propre de T_N.

Puisque $B_N\vec{v} \in \mathrm{span}(\vec{v})$, on sait que $\vec{v}$ appartient à un sous-espace propre de T_N préservé par B_N. Le seul candidat possible est le sous-espace propre associé à la valeur propre 1. Le théorème en découle immédiatement. □

3 Formule explicite de la fonction génératrice et comptage des points

3.1 Vecteur propre associé à la valeur propre $\lambda = 1$

La fonction génératrice d'un vecteur propre associé à la valeur propre 1 peut être calculée explicitement. La clé de ce calcul réside dans le fait que la fonction génératrice présente, dans ce cas, une symétrie supplémentaire. En termes d'opérateur différentiel, cette symétrie peut être décrite par le fait que l'opérateur différentiel est le carré symétrique d'un opérateur différentiel du second ordre. Ceci nous permet de résoudre explicitement l'équation différentielle en termes de solutions d'une équation différentielle du second ordre.

Définition 3.1 : Soient $\{f_1(z), \ldots, f_m(z)\}$ et $\{g_1(z), \ldots, g_n(z)\}$ les bases des noyaux de deux opérateurs différentiels unitaires L et $\widetilde{L}$, d'ordre m et n respectivement. Le produit symétrique de deux opérateurs différentiels unitaires $L \circledS \widetilde{L}$ est l'unique opérateur différentiel unitaire dont le noyau est engendré par $\{f_j(z)g_k(z) : 1 \leq jm,\ 1 \leq k \leq n\}$. Si $L = \widetilde{L}$, alors $L \circledS \widetilde{L}$ est appelé le **carré symétrique** de L, et on le note $L^{\circledS 2}$.

Nous rappelons d'abord un critère simple permettant de vérifier si un opérateur différentiel du troisième ordre est un carré symétrique.

Lemme 3.2 : (Singer [17]) *Un opérateur différentiel du troisième ordre*

$$S = \partial_z^3 + u_2(z)\partial_z^2 + u_1(z)\partial_z + u_0(z)$$

est le carré symétrique de l'opérateur différentiel du second ordre

$$L = \partial_z^2 + v_1(z)\partial_z + v_0(z)$$

si et seulement si

$$\begin{aligned}
u_2(z) &= 3v_1(z), \\
u_1(z) &= 4v_0(z) + v_1'(z) + 2v_1(z)^2, \\
u_0(z) &= 2v_0'(z) + 4v_0(z)v_1(z).
\end{aligned}$$

En utilisant ce critère, nous pouvons démontrer que pour la valeur propre 1 de T_N (ou, de manière équivalente, pour la valeur propre $(N^2+2N)/2$ de J_N), notre opérateur différentiel est un carré symétrique.

Lemme 3.3 : L'équation différentielle du troisième ordre

$$S = \partial_z^3 - 3\frac{2z-1}{z(1-z)}\partial_z^2 + \left(\frac{N^2+2N-6}{z(1-z)} - \frac{N^2+2N}{z^2(1-z)^2}\right)\partial_z + \frac{N^2+2N}{z^2(1-z)} - \frac{\mu}{z^2(1-z)^2}$$

est le carré symétrique d'un opérateur différentiel du second ordre si et seulement si $\mu = (N^2 + 2N)/2$.

Dans ce cas, $S = L^{\circledS 2}$ pour

$$L = \partial_z^2 + \frac{1-2z}{z(1-z)}\partial_z - \frac{(N^2+2N)(z^2-z+1)+1}{4z^2(1-z)^2}.$$

Preuve : il nous faut déterminer quand le système surdéterminé d'équations différentielles du lemme 3.2 admet une solution.

En résolvant les deux premières équations du lemme, on obtient :

$$v_1(z) = \frac{1-2z}{z(1-z)} \quad \text{et} \quad v_0(z) = -\frac{(N^2+2N)(z^2-z+1)+1}{4z^2(1-z)^2}.$$

En remplaçant ces expressions dans la troisième équation du lemme, on trouve : $\mu = (N^2+2N)/2$. L'énoncé du lemme en découle immédiatement.

Le lemme précédent nous permet de construire un ensemble fondamental de solutions pour notre équation différentielle.

Lemme 3.4 : La solution générale de l'équation différentielle du troisième ordre

$$y''' - 3\frac{2z-1}{z(1-z)}y'' + \left(\frac{N^2+2N-6}{z(1-z)} - \frac{N^2+2N}{z^2(1-z)^2}\right)y' + \frac{(N^2+2N)(1/2-z)}{z^2(1-z)^2}y = 0$$

a la base de solutions

$$\begin{aligned}
y_1 &= \left(\frac{z}{1-z}\right)^{N+1} {}_2F_1\left[\begin{matrix}-N/2, N/2+1 \\ -N\end{matrix}; 1-z\right]^2 \\
y_2 &= {}_2F_1\left[\begin{matrix}-N/2, N/2+1 \\ -N\end{matrix}; 1-z\right] {}_2F_1\left[\begin{matrix}-N/2, N/2+1 \\ -N\end{matrix}; z\right] \\
y_3 &= \left(\frac{1-z}{z}\right)^{N+1} {}_2F_1\left[\begin{matrix}-N/2, N/2+1 \\ -N\end{matrix}; z\right]^2
\end{aligned}$$

Preuve : Si l'on effectue le changement de variables $t = 2z - 1$, alors l'équation différentielle

$$y'' + \frac{1-2z}{z(1-z)}y' - \frac{(N^2+2N)(z^2-z+1)+1}{4z^2(1-z)^2}y = 0$$

devient

$$4y'' - \frac{8t}{(1-t^2)}y' - \frac{(N^2+2N)(t^2+3)+4}{(1-t^2)^2}y = 0,$$

et se simplifie en l'équation différentielle de Legendre

$$(1-t^2)y'' - 2ty' + \left(\frac{N(N+2)}{4} - \frac{(N+1)^2}{1-t^2}\right)y = 0.$$

Deux solutions linéairement indépendantes de cette équation sont données par la fonction de Ferrers

$$\left(\frac{1+t}{1-t}\right)^{N+1} {}_2F_1\left[\begin{matrix}-N/2 \;\; N/2+1\\ -N\end{matrix}; \frac{1}{2} - \frac{1}{2}t\right]$$

et sa rotation de 180 degrés

$$\left(\frac{1-t}{1+t}\right)^{N+1} {}_2F_1\left[\begin{matrix}-N/2 \;\; N/2+1\\ -N\end{matrix}; \frac{1}{2} + \frac{1}{2}t\right].$$

L'énoncé de notre lemme découle alors de ces résultats en effectuant la substitution $t = 2z-1$ et en utilisant le lemme 3.3. $\square$

Avant de démontrer le théorème A, on a besoin d'une identité supplémentaire concernant les fonctions hypergéométriques.

Lemme 3.5 : Pour tout entier non négatif N,

$$\begin{aligned}{}_2F_1\left[\begin{smallmatrix}-N/2 \;\; N/2+1\\ -N\end{smallmatrix}; \tfrac{z}{z-1}\right](1-z)^{N/2} &= {}_2F_1\left[\begin{smallmatrix}-N/2 \;\; N/2+1\\ -N\end{smallmatrix}; z\right](1-z)^{N+1}\\ &\quad + (-1)^{N/2}{}_2F_1\left[\begin{smallmatrix}-N/2 \;\; N/2+1\\ -N\end{smallmatrix}; 1-z\right]z^{N+1}\end{aligned}$$

Preuve : notons d'abord que $(1-z)^{N+1}{}_2F_1\left[\begin{smallmatrix}-N/2 \;\; N/2+1\\ -N\end{smallmatrix}; z\right]^2$ et que ${}_2F_1\left[\begin{smallmatrix}-N/2 \;\; N/2+1\\ -N\end{smallmatrix}; 1-z\right]z^{N+1}$ sont des solutions linéairement indépendantes de l'équation différentielle hypergéométrique

$$z(1-z)y'' + (-N+2Nz)y' - N(3N+1)y = 0$$

à proximité de $z = 1$. Par la transformation de Pfaff

$${}_2F_1\left[\begin{matrix}-N/2 \;\; N/2+1\\ -N\end{matrix}; \frac{z}{z-1}\right](1-z)^{N/2} = {}_2F_1\left[\begin{matrix}-N/2 \;\; -3N/2-1\\ -N\end{matrix}; z\right],$$

de telle façon que $F(z)$ est une solution de la même équation différentielle hypergéométrique. Par conséquent

$$\begin{aligned} {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; \frac{z}{z-1}\right](1-z)^{N/2} &= A \cdot {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; z\right](1-z)^{N+1} \\ &\quad + B \cdot {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; 1-z\right] z^{N+1} \end{aligned}$$

pour certaines constantes A et B. En évaluant en $z = 0$, on voit immédiatement que

$$A = {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; 0\right] = 1.$$

Pour obtenir B, on souhaite prendre la limite lorsque $z \to 1$. Puisque ${}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; z\right]$ est un polynôme palindrome, on a

$${}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; \frac{z}{z-1}\right](1-z)^{N/2} = (-1)^{N/2} {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; \frac{z-1}{z}\right] z^{N/2}.$$

et donc en prenant la limite, on trouve

$$B = (-1)^{N/2} {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; 0\right] = (-1)^{N/2}.$$

Ceci termine la preuve.

$\square$

En combinant tous les lemmes précédents, on peut maintenant démontrer un théorème qui est essentiellement le même que le théorème A.

Théorème 3.6 : *Pour $N > 0$ un entier pair et $\mu = (N^2 + 2N)/2$, l'équation différentielle*

$$\begin{aligned} \mu\widetilde{y} &= z^2(1-z)^2\widetilde{y}''' + 3z(1-z)((N-1)z - N)\widetilde{y}'' \\ &\quad + N((2N-5)z^2 + (2-5N)z + 2N+1)\widetilde{y}' \\ &\quad + N((2N+1)z + N^2 + N + 1)\widetilde{y} \end{aligned}$$

a la solution polynomiale

$$\widetilde{y} = {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; z\right] {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; \frac{z}{z-1}\right](1-z)^{N/2}.$$

Preuve : si on fait la substitution $\widetilde{y} = z^{N+1}y$, alors l'équation différentielle se simplifie en l'équation du troisième ordre dans le lemme 3.3. Donc le lemme 3.4 nous apprend que

$$\widetilde{y} = (1-z)^{N+1} {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; z\right]^2 + (-1)^{N/2} z^{N+1} {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; 1-z\right] {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix}; z\right]$$

est une solution. Maintenant, si on applique le résultat du lemme 3.1, le théorème en découle immédiatement. $\square$

On termine cette section par une démonstration du théorème A.

Preuve du théorème A : La fonction

$$f(z) = {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix} ; z\right] {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix} ; \frac{z}{z-1}\right] (1-z)^{N/2}$$

est un polynôme de degré N, et par conséquent, $f(z) = f(\vec{v}; z)$ pour un certain vecteur $\vec{v} \in \mathbb{C}^{N+1}$.

Par le théorème 3.6 et le théorème 2.4, le vecteur $\vec{v}$ est un vecteur propre de J_N avec comme valeur propre associée $\dfrac{N^2+N}{2}$.

Finalement, par le théorème 2.7, on sait que $\vec{v}$ est un vecteur propre de T_N de valeur propre 1. $\square$

3.2 Compter des points dans des corps finis

Il s'avère que la fonction génératrice du vecteur propre de valeur propre 1

$$f(z) = {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix} ; z\right] {}_2F_1\left[\begin{matrix} -N/2 & N/2+1 \\ & -N \end{matrix} ; \frac{z}{z-1}\right] (1-z)^{N/2}$$

possède de nombreuses symétries modulo p.

En particulier, on peut vérifier que

$$f(z) = f(1-z) = f\left(\frac{1}{z}\right) = f\left(\frac{1}{1-z}\right) = f\left(1-\frac{1}{z}\right) = f\left(\frac{z-1}{z}\right),$$

pour tout $z \in \mathbb{F}_p$ avec $z \neq 0, 1$.

L'ensemble des transformations de Möbius

$$G = \left\{ z, 1-z, \frac{1}{z}, \frac{1}{1-z}, 1-\frac{1}{z}, \frac{z-1}{z} \right\}$$

définit un sous-groupe de $\mathrm{PGL}_2(\mathbb{Z})$.

Ce groupe est très lié à la famille de Legendre des courbes elliptiques

$$E_z : y^2 = x(x-1)(x-z)$$

sur $\mathbb{F}_p$.

En particulier, deux courbes E_z et E_w sont isomorphes si et seulement si $w = \chi(z)$ pour un certain $\chi \in G$.

Par conséquent, la valeur $f(z)$ devrait être invariante par un certain isomorphisme de la courbe elliptique E_z.

Dans cette section, on prouve exactement cela. Notamment, on prouve le théorème C qui énonce que

$$f(z) \equiv (\#E_z(\mathbb{F}_p) - 1)^2 \mod p.$$

Un résultat bien connu de théorie des nombres est que $\#E_z(\mathbb{F}_p) - 1$ modulo p est donné (au signe près) par le polynôme d'Igusa

$$H_p(z) = \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 z^k.$$

En particulier, cela amène au critère de Deuring-Hasse que E_z est super-singulière si et seulement si $H_p(z) \equiv 0 \mod p$ [10, 16].

Théorème 3.7 : (Hasse [10]) *Soit $p > 2$ un nombre premier et $z \in \mathbb{F}_p$ avec $z \neq 0, 1$. Alors*

$$(-1)^{(p-1)/2} H_p(z) \equiv 1 - \#E_z(\mathbb{F}_p) \mod p.$$

Lemme 3.8 : Soit $N = p - 1$ pour un nombre premier impair p. Alors

$${}_2F_1\left[\begin{matrix} -N/2 \;\; N/2+1 \\ -N \end{matrix}; z\right] \equiv {}_2F_1\left[\begin{matrix} -N/2 \;\; N/2+1 \\ -N \end{matrix}; z/(z-1)\right](1-z)^{N/2} \mod p.$$

Preuve : en utilisant l'identité de Pfaff et le fait que $N \equiv -1 \mod p$, on a

$$\begin{aligned} {}_2F_1\left[\begin{matrix} -N/2, N/2+1 \\ -N \end{matrix}; z/(z-1)\right](1-z)^{N/2} &= {}_2F_1\left[\begin{matrix} -N/2, -3N/2-1 \\ -N \end{matrix}; z\right] \\ &= \sum_{k=0}^{N} \frac{(-N/2)_k(-3N/2-1)_k}{(-N)_k}\frac{z^k}{k!} \\ &\equiv \sum_{k=0}^{N} \frac{(-N/2)_k(N/2+1)_k}{(-N)_k}\frac{z^k}{k!} \mod p \\ &= {}_2F_1\left[\begin{matrix} -N/2, N/2+1 \\ -N \end{matrix}; z\right]. \end{aligned}$$

□

Lemme 3.9 : Soit $N = p - 1$ pour un nombre premier impair p. Alors

$$H_p(z) \equiv {}_2F_1\left[\begin{matrix} -N/2 \;\; N/2+1 \\ -N \end{matrix}; z\right] \mod p.$$

Preuve : Puisque $(-N)_k \equiv k! \mod p$ et puisque

$$\begin{aligned}\binom{N/2}{k} &= \frac{(N/2)(N/2-1)\dots(N/2-k+1)}{k!}\\ &\equiv \frac{(-1/2)(-1/2-1)\dots(-1/2-k+1)}{k!} \mod p = (-1)^k\frac{(1/2)_k}{k!},\end{aligned}$$

on calcule

$$\begin{aligned}H_p(z) &\equiv \sum_{k=0}^{N/2}\frac{(1/2)_k(1/2)_k}{(-N)_k}\frac{z^k}{k!} \mod p\\ &\equiv {}_2F_1\left[\begin{matrix}-N/2, N/2+1\\ -N\end{matrix};z\right] \mod p.\end{aligned}$$

□

L'énoncé du théorème C est simplement la combinaison du théorème de Hasse et des deux lemmes précédents.

Remerciements : Le travail de recherche de W.R.C. a été financé par une récompense pour l'amélioration de la recherche AMS-Simons.

Références

[1] B. Bakalov, E. Horozov, M. Yakimov, *General methods for constructing bispectral operators*, Phys. Lett. A **222** (1996), 59–66.

[2] Brawer, Robert, Magnus Pirovino. *The linear algebra of the Pascal matrix,* Linear Algebra and Its Applications 174 (1992) : 13-23.

[3] W. R. Casper, F. A. Grünbaum, M. Yakimov, I. Zurrián, *Matrix valued discrete-continuous functions with the prolate spheroidal property*, Commun. Math. Phys. **405** (2024), No. 3, Paper No. 69, 36 p.

[4] W. R. Casper, M. Yakimov, *Integral operators, bispectrality and growth of Fourier algebras*, J. Reine Angew. Math. **766** (2020), 151–194.

[5] W. R. Casper, I. Zurrián, *The Pascal Matrix, Commuting Tridiagonal Operators and Fourier Algebras*, arXiv :2407.21680.

[6] A. Connes, H. Moscovici, *The UV prolate spectrum matches the zeros of zeta*, Proc. Natl. Acad. Sci. U.S.A. **119**, e2123174119 (2022).

[7] J. J. Duistermaat, F. A. Grünbaum, *Differential equations in the spectral parameter*, Comm. Math. Phys. **103** (1986), 177–240.

[8] B. Dwork, *Lectures on p-adic differential equations*, Vol. 253. Springer Science and Business Media, 2012.

[9] A. Edelman, G. Strang, *Pascal Matrices*, American Mathematical Monthly **111** (2004), no. 3, 189–197.

[10] Helmut Hasse. *Zur Theorie der abstrakten elliptischen Funktionenkörper. III. Die Struktur des Meromorphismenringes. Die Riemannsche Vermutung*, J. Reine Angew. Math. 175 (1936), 193–208.

[11] J. Fuselier, L. Long, R. Ramakrishna, H. Swisher, Fang-Ting Tu *Hypergeometric functions over finite fields*, Vol. 280. No. 1382. American Mathematical Society, 2022.

[12] K. Kedlaya, *p-adic Differential Equations*, Cambridge University Press, 2022.

[13] H. J. Landau, H. O. Pollak, *Prolate spheroidal wave functions, Fourier analysis and uncertainty. II*, Bell System Tech. J. **40** (1961), 65–84.

[14] Sir Thomas Muir, *Theory of Determinants : In the Historical Order of Development*, Vol. III, Macmillan, London, 1920.

[15] Morris Newman, Matrix computations, in Survey of Numerical Analysis (John Todd, Ed.), McGraw-Hill, New York, 1962.

[16] Silverman, Joseph H. *The arithmetic of elliptic curves*, Graduate Texts in Mathematics Vol. 106. New York : Springer, 2009.

[17] Michael F. Singer *Solving homogeneous linear differential equations in terms of second order linear differential equations*, American Journal of Mathematics 107.3 (1985) : 663-696.

[18] Michael F. Singer, Felix Ulmer. *Galois groups of second and third order linear differential equations*, Journal of Symbolic Computation 16.1 (1993) : 9-36.

[19] D. Slepian, *Prolate spheroidal wave functions, Fourier analysis and uncertainity. IV. Extensions to many dimensions ; generalized prolate spheroidal functions*, Bell System Tech. J. **43** (1964), 3009–3057.

[20] D. Slepian, H. O. Pollak, *Prolate spheroidal wave functions, Fourier analysis and uncertainty. I*, Bell System Tech. J. **40** (1961), 43–63.

[21] N. Strauss, *Jordan form of a binomial coefficient matrix over H*, Linear Algebra Appl. 9065-72 (1987).

[22] C. A. Tracy, H. Widom, *Fredholm determinants, differential equations and matrix models*, Comm. Math. Phys. **163** (1994), 33–72.

[23] C. A. Tracy, H. Widom, *Level-spacing distributions and the Airy kernel*, Comm. Math. Phys. **159** (1994), 151–174.

[24] Waterhouse, William C. *The map behind a binomial coefficient matrix over* $\mathbb{Z}/p\mathbb{Z}$, Linear Algebra Appl. 105 (1988) : 195-198.