Modèles dyadiques

Terence Tao

2007.

L'un des plus anciens et des plus fondamentaux concepts en mathématiques est la *droite*. Dépendant exactement des structures mathématiques que nous voulons étudier (algébriques, géométriques, topologiques, de la théorie de l'ordre, etc.), nous modélisons les droites de nos jours par une variété d'objets standards mathématiques, tels que la droite réelle $\mathbb{R}$, la droite complexe $\mathbb{C}$, la droite projective $\mathbb{RP}^1$, la droite réelle étendue $[-\infty, +\infty]$, la droite affine $\mathbb{A}^1$, le continuum c, la droite longue L, etc. Nous avons également des versions discrètes de la droite, telles que les nombres naturels $\mathbb{N}$, les entiers $\mathbb{Z}$, et les ordinaux ω, ainsi que des versions compactes de la droite, telles que l'intervalle unité $[0, 1]$ ou le cercle unité $\mathbb{T} := \mathbb{R}/\mathbb{Z}$. Finalement, nous avons des versions discrètes et compactes de la droite, comme les groupes cycliques $\mathbb{Z}/N\mathbb{Z}$ et les intervalles discrets $\{1, \ldots, N\}$ et $\{0, \ldots, N-1\}$. En prenant les produits cartésiens, nous obtenons alors des objets de dimension supérieure comme l'espace Euclidien $\mathbb{R}^n$, le réseau standard $\mathbb{Z}^n$, le tore standard $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$, et etc. Ces objets bien sûr forment le support sur lequel une très grande partie des mathématiques modernes est établie.

D'une manière générale, la droite a trois familles principales de structures sur elle :

Les structures géométriques, comme la métrique ou la mesure, la complétude, les échelles (grossières ou fines), les mouvements rigides (la translation et la symétrie), les similitudes (la dilatation, les applications affines), et les structures différentielles (faisceau tangent, etc.);

Les structures algébriques, tels que les groupes, les anneaux, ou les structures de corps, et toutes les autres choses qui viennent de ces catégories (e.g. les sous-groupes, les homomorphismes, les involutions, etc.) ; et

Les structures à une dimension, comme l'ordre, la structure de l'espace de longueur (en particulier, la structure de la connectivité des chemins), un générateur singleton, la propriété archimédienne, la capacité d'utiliser l'induction mathématique (i.e. le bon ordre), la convexité, ou la possibilité de déconnecter la droite en enlevant un seul point.

Bien sûr, ces structures sont entremêlées, et c'est un phénomène important qu'un concept mathématique qui semble natif à une struture, puisse souvent être défini de façon équivalente en fonction d'autres structures. Par exemple, la valeur absolue $|n|$ d'un entier n peut être définie géométriquement comme la distance de 0 à n, algébriquement comme l'indice du sous-groupe $\langle n \rangle = n \cdot \mathbb{Z}$ des entiers $\mathbb{Z}$ engendré par n, ou *en dimension 1* comme le nombre d'entiers entre 0 et n (en incluant 0, mais en excluant n). Cette équivalence des définitions devient importante quand on veut travailler dans des contextes plus généraux dans lesquels une ou plusieurs des structures ci-dessus manque ou bien est affaiblie.

Ce dont je souhaite parler aujourd'hui, c'est d'un modèle jouet pour la droite (dans n'importe laquelle de ses incarnations), dans lequel les structures géométriques et algébriques sont améliorées

Traduction par Denise Vella-Chemla (13.4.2022) de l'article "*Dyadic models*" du blog *What's new ?* de Terence Tao https://terrytao.wordpress.com/2007/07/27/dyadic-models/

(et deviennent soigneusement imbriquées et récursives), au dépend de la structure à une dimension (qui est complètement détruite). Ce modèle a de nombreuses appelaltions différentes, dépendantes du domaine des mathématiques dans lequel on travaille et des structures par lesquelles on est intéressé. En analyse harmonique, on l'appelle le modèle dyadique, le modèle de Walsh, ou le modèle du groupe de Cantor ; en théorie des nombres et en géométrie arithmétique, il est connu sous le nom de modèle du corps des fonctions ; en topologie, c'est le modèle de l'espace de Cantor ; en probabilités, c'est le modèle de la martingale ; en géométrie métrique, c'est le modèle ultramétrique, arborescent, ou non-archimédien ; en géométrie algébrique, c'est le modèle des séries de Puiseux ; en combinatoire additive, c'est le modèle de torsion borné ou le modèle du corps fini ; en informatique et en théorie de l'information, c'est le modèle du cube de Hamming ; en théorie de la représentation, c'est le modèle du cristal de Kashiwara. Permettez-moi de choisir arbitrairement l'un de ces termes, et de faire référence à tous ces termes comme aux *modèles dyadiques* pour la droite (ou pour tous les objets dérivés de la droite). Alors qu'il n'y a souvent pas de lien direct entre un modèle dyadique et un modèle non-dyadique, les modèles dyadiques servent de laboratoires incroyablement utiles dans lesquels on peut avoir un aperçu et l'intuition des modèles non-dyadiques du "monde réel", parce qu'on a une structure algébrique et géométrique beaucoup plus puissante et élégante avec laquelle jouer dans un tel paradigme (bien que la perte de la structure à une dimension puisse être une préoccupation importante). Peut-être que l'exemple le plus surprenant de cela est la preuve en trois lignes de l'hypothèse de Riemann dans le modèle du corps de fonctions des entiers, dont je discuterai un petit peu plus tard.

- Entiers dyadiques et réels -

Très grossièrement, un des avantages-clefs que les modèles dyadiques offrent sur les modèles non-dyadiques est qu'ils n'ont aucune "retenue" d'une échelle à l'autre. Cette retenue nous est enseignée dès l'école primaire, quand nous apprenons les algorithmes de la notation arithmétique décimale : de longues additions, de longues soustractions, de longues multiplications, et de longues divisions. En notation décimale, la notion d'échelle nous est donnée par les puissances de dix (avec des puissances plus grandes correspondant à des échelles grossières et des puissances plus petites correspondent à des échelles fines), mais pour faire de l'arithmétique proprement avec cette notation, on doit constamment "emporter" des chiffres d'une échelle vers l'échelle suivante plus grossière, ou inversement, "ramener" des chiffres d'une échelle à l'échelle suivante plus fine. Ces interactions entre des chiffres d'échelles adjacentes (qui en terminologie moderne, serait décrite comme des cocycles) fait que les opérations arithmétiques semblent plutôt compliquées en notation décimale, bien qu'on puisse au moins isoler le comportement à des échelles fines du comportement à des échelles grossières (mais pas vice versa) par l'arithmétique modulaire. (Pour décrire cela d'une façon un peu plus algébrique, les entiers ou les nombres réels peuvent quotienter les échelles grossières via les sous-groupes normaux (ou les idéaux) comme $N \cdot \mathbb{Z}$, mais n'ont pas un sous-groupe normal correspondant ou un idéal pour quotienter les échelles fines.)

Il est donc naturel de chercher des modèles de l'arithmétique dans lesquels ce débordement (phénomène des retenues) n'est pas présent. On est d'abord exposé à de tels modèles au lycée, quand l'arithmétique des polynômes en une inconnue t est introduite (i.e. on travaille avec des anneaux tels que $\mathbb{Z}[t]$ ou $\mathbb{R}[t]$ plutôt que $\mathbb{Z}$ ou $\mathbb{R}$). Par exemple, pour quotienter un polynôme par un autre, on utilise l'algorithme de longue division polynomiale (ou la division synthétique), qui est formellement identique à la longue division pour les entiers en notation décimale mais sans tout cet ennui d'une

échelle à la suivante. Ici les échelles sont représentées par des puissances de t, plutôt que par des puissances de 10. Comme avec les réels ou les entiers, les échelles grossières peuvent être contenues dans des sous-groupes normaux (et des idéaux) tels que $t^d \cdot \mathbb{R}[t]$, mais maintenant les échelles précises peuvent aussi être contenues dans des sous-groupes normaux (bien que non pas idéals) tels que $\langle 1, t, \ldots, t^{d-1} \rangle$, le groupe engendré par $1, t, \ldots, t^{d-1}$ (i.e. le groupe des polynômes de degré inférieur à d). (Du point de vue de la théorie des catégories, les choses sont mieux ici parce que diverses séquences exactes courtes faisant intervenir les échelles sont maintenant séparées.)

Maintenant, les anneaux de polynômes tels que $\mathbb{Z}[t]$ ou $\mathbb{R}[t]$ sont un peu "trop grands" pour servir de modèles pour $\mathbb{Z}$ ou $\mathbb{R}$ (à moins qu'on ne leur adjoigne quelques infinitésimaux, mais c'est une autre histoire), puisqu'ils ont une dimension de plus. On peut obtenir un modèle plus précis en considérant à nouveau la représentation décimale, qui identifie les nombres naturels à des polynômes sur l'espace des chiffres $\{0, 1, \ldots, 9\}$. Cet espace n'est pas fermé selon l'addition (qui est ce qui cause le phénomène de retenue en premier lieu) ; mais l'on peut remédier à cela en remplaçant cet espace de chiffres par le groupe cyclique $\mathbb{Z}/10\mathbb{Z}$. Cela nous donne le modèle $(\mathbb{Z}/10\mathbb{Z})[t]$ pour les entiers ; c'est la représentation décimale sans l'opération de retenue. Si nous suivons la notation décimale usuelle et que nous identifions les polynômes dans $(\mathbb{Z}/10\mathbb{Z})[t]$ avec les chaînes de chiffres de la manière habituelle (e.g. en identifiant 3 dizaines $+2$ avec 32) alors nous obtenons un systéme de numération qui est similaire, mais pas tout à fait identique, aux entiers. Par exemple, $66 + 77$ est maintenant égal à 33 plutôt qu'à 143 ; 25×4 maintenant est égal à 80 plutôt qu'à 100 ; et etc. Notons que contrairement aux nombres naturels, l'espace des polynômes est déjà fermé selon la négation et par conséquent, il n'y a pas de nécessité d'introduire les nombres négatifs ; par exemple, dans ce système, on a $-12 = 98$. Je ferai référence à $(\mathbb{Z}/10\mathbb{Z})[t]$ en le désignant comme le modèle des "dyadiques en base 10" pour les entiers (ce qui est un peu ennuyeux, le terme "10-adique" étant déjà utilisé pour signifier quelque chose de légèrement différent).

Il y a également un modèle dyadique en base 10 pour les nombres réels, dans lequel on autorise un nombre infini de puissances négatives de t mais seulement un nombre fini de puissances positives de t ; en d'autres termes, c'est le modèle $(\mathbb{Z}/10\mathbb{Z})((1/t))$, l'anneau des séries formelles de Laurent en $1/t$. Cet anneau à nouveau diffère légèrement des réels ; par exemple, $0.999\ldots$ n'est maintenant plus égal à $1.000\ldots$ (en fait, ils diffèrent de $1.111\ldots$). Ainsi, la notation décimale envoie $(\mathbb{Z}/10\mathbb{Z})((1/t))$ sur l'axe réel positif $\mathbb{R}^+$, mais il y a un petit peu de non-injectivité causée par cette application.

Les modèles dyadiques en base 10 pour les réels et les entiers ne sont pas particulièrement précis, cela est dû à la présence de diviseurs nuls dans l'anneau de base sous-jacent $\mathbb{Z}/10\mathbb{Z}$. Par exemple, on a $2 \times 5 = 0$ dans ce modèle. On peut faire beaucoup mieux en travaillant sur un corps fini F, comme le corps $\mathbb{F}_2$ à deux éléments Cela nous donne les modèles dyadiques $F[t]$ et $F((1/t))$ pour les entiers et les réels respectivement qui s'avèrent des analogues beaucoup plus proches que le modèle dyadique en base 10. Par exemple, $F[t]$, comme les entiers, est un domaine euclidien, et $F((1/t))$ est un corps. (Dans le cas binaire $F = \mathbb{F}_2$, l'opération d'addition est juste le XOR (ou exclusif) bit à bit, et la multiplication est la convolution bit à bit). Nous pouvons également modéliser de nombreux autres objets non-dyadiques, comme l'illustre la table suivante :

Non-dyadique	Dyadique
Entiers $\mathbb{Z}$	Polynômes $F[t]$
Rationnels $\mathbb{Q}$	Fonctions rationnelles $F(t)$
Réels $\mathbb{R}$	Polynômes de Laurent $F((1/t))$
Cercle unité $\mathbb{R}/\mathbb{Z}$	$F((1/t))/F[t] \equiv \frac{1}{t}F[\frac{1}{t}]$
$\lvert F\rvert^d \cdot \mathbb{Z}$	$t^d \cdot F[t]$
Groupe cyclique $\mathbb{Z}/\lvert F\rvert^d \cdot \mathbb{Z}$	Espace vectoriel F^d
Corps fini $\mathbb{Z}/p \cdot \mathbb{Z}$	Corps fini $F[t]/p(t) \cdot F[t]$
Valeur absolue	(Exponentielle de) degré
Onde plane	Fonction de Walsh
Ondelettes	Ondelettes de Haar
Gaussien	Fonction en escalier
Boule	Intervalle dyadique
Opérateurs de chaleur	Espérances conditionnelles de martingales
À bande limitée	Localement constant
Intervalle / progression arithmétique	Sous-espace / sous-groupe
Ensemble de Bohr	Hyperplan

Rappelons que nous pouvons définir la valeur absolue (ou norme) d'un entier n comme l'indice du sous-groupe $\langle n \rangle$ des entiers. Exactement la même définition peut être appliquée au modèle dyadique $F[t]$ des entiers ; la valeur absolue d'un élément $n \in F[t]$ peut alors être vue comme étant égale à $|n| = |F|^{\deg(n)} \in \mathbb{Z}^+$, où $\deg(n)$ est le degré de t dans n (avec la convention que 0 a un degré de $-\infty$ et ainsi une valeur absolue égale à 0). Par exemple, dans le cas binaire, $t^3 + t + 1$ (ou 1011) a une norme égale à 8[1]. Comme la valeur absolue sur les entiers, la valeur absolue sur le modèle dyadique $F[t]$ des entiers est multiplicative et obéit à l'inégalité triangulaire, permettant d'avoir une métrique sur $F[t]$ par la formule habituelle $d(n, m) := |n - m|$. En fait, nous avons quelque chose de mieux qu'une métrique, qu'on appelle une ultramétrique ; dans le monde dyadique, l'inégalité

[1] 11 ?

triangulaire

$$d(x,z) \leq d(x,y) + d(y,z)$$

peut être renforcée pour devenir l'inégalité ultra-triangulaire

$$d(x,z) \leq \max(d(x,y), d(y,z)).$$

On peut alors étendre de manière unique cette valeur absolue multiplicativement vers le modèle dyadique $F((1/t))$ des réels, qui est donné par la même formule $|n| = |F|^{\deg(n)} \in \mathbb{R}^+$, où $\deg(n)$ est maintenant compris comme étant la plus grande puissance de t qui apparaît dans la factorisation de n (ou $-\infty$ si aucune telle puissance n'est présente). Ainsi par exemple, dans le cas binaire $1/t + 1/t^2 + 1/t^3 + \ldots$ (ou $0.111\ldots$) a une norme de $1/2$. Comme avec la droite réelle, cette valeur absolue transforme la droite réelle dyadique $F((1/t))$ en un espace métrique complet. L'espace métrique engendre alors les boules $B(x,r) := \{y \in F((1/t)) : |y-x| < r\}$, qui dans le cas binaire sont identifiables avec les intervalles dyadiques. Le fait qu'on ait une ultramétrique plutôt qu'une métrique signifie que les boules bénéficient d'une *propriété de nidification* très utile, qui n'est pas présente dans le paradigme non-dyadique : si deux boules s'intersectent, alors la plus grande doit nécessairement contenir la plus petite.

D'un autre côté, toute la structure "à une dimension" de la droite réelle est perdue quand on passe au modèle dyadique. Par exemple, la droite réelle dyadique est encore localement compacte, mais non pas localement connectée ; la topologie est plutôt localement celle d'un espace de Cantor. Il n'y a pas de notion naturelle d'ordre sur les entiers dyadiques ou sur la droite réelle, et la métrique est non-archimédienne. En lien avec cela, l'indiçage mathématique ne s'applique plus aux entiers dyadiques. Cependant, et en quelque sorte de façon contre-intuitive, on peut aller relativement loin dans l'imitation de nombreuses caractéristiques des entiers et des réels sans utiliser aucune structure à une dimension. J'essaierai d'illustrer cela dans un certain nombre de contextes.

- Modèles dyadiques et analyse harmonique -

Comparons d'abord l'analyse harmonique des modèles dyadique et non-dyadique. La mesure de Lebesgue dx est l'unique mesure de Haar de la droite réelle qui assigne une mesure de 1 à l'intervalle unité $[0,1]$. Similairement, pour la droite réelle dyadique $F((1/t))$, il y a une unique mesure de Haar dx qui assigne une mesure de 1 à la boule unité $B(0,1)$. En effet, cette mesure peut être définie en ramenant la mesure de Lebesgue sur l'axe positif réel $\mathbb{R}^+$ via l'application décimale qui envoie les éléments de $F((1/t))$ sur l'expansion de la base correspondante $|F|$ dans les réels (e.g. dans le cas binaire, $t^2 + 1/t$ serait envoyé sur $100.1_2 = 4.5$).

La théorie générale de l'analyse harmonique sur les groupes abéliens localement compacts montre alors qu'il y a une théorie de la transformation de Fourier sur la droite réelle $F((1/t))$, qui s'avère être très analogue à celle de la droite réelle non-dyadique $\mathbb{R}$. (Il y a aussi une théorie de Fourier reliant les entiers dyadiques $F[t]$ avec le cercle unité dyadique $F((1/t))/F[t] \equiv \frac{1}{t} \cdot F[\frac{1}{t}]$, que nous laissons à la lectrice). Rappelons que la transformation de Fourier sur la droite réelle est construite à partir du caractère 1-périodique $e : \mathbb{R} \to \mathbb{C}$ défini par $e(x) := e^{2\pi i x}$ par la formule

$$\hat{f}(\xi) := \int_{\mathbb{R}} f(x) e(-x\xi)\ dx$$

pour toutes les $f : \mathbb{R} \to \mathbb{C}$ au bon comportement (e.g. les f partout intégrables). Similairement, la transformation de Fourier sur $F((1/t))$ (en supposant que F est un corps premier $F = \mathbb{F}_p \equiv \mathbb{Z}/p\mathbb{Z}$ pour faire simple) peut être construite à partir du caractère 1-périodique $e_p : F((1/t)) \to \mathbb{C}$ défini par

$$e_p(\sum_{j=-\infty}^{d} a_j t^j) := e(a_{-1}/p)$$

(qui serait une onde carrée dans le cas binaire) en utilisant presque la même formule, notamment

$$\hat{f}(\xi) := \int_{F((1/t))} f(x) e_p(-x\xi)\ dx$$

pour toutes les $f : F((1/t)) \to \mathbb{C}$ au bon comportement. On peut alors montrer que cette transformation de Fourier dyadique (appelée transformation de Walsh-Fourier dans le cas binaire) a toutes les propriétés algébriques usuelles que la transformation de Fourier non-dyadique a - par exemple, elle réagit à la convolution, la translation, la modulation, et la dilatation exactement de la même façon que sa contrepartie non-dyadique, et on peut aussi montrer qu'elle a un parfait analogue du théorème de Plancherel. (Elle a aussi un algorithme plus agréable de transformation de Fourier rapide que sa contrepartie non-dyadique, parce qu'on n'a plus besoin de l'étape additionnelle pour faire attention à la retenue d'une échelle à la suivante). En fait, la structure dyadique rend l'analyse harmonique sur $F((1/t))$ en quelque sorte plus simple que celle sur $\mathbb{R}$, à cause de la possibilité d'avoir *une localisation parfaite de l'espace des phases*. Dans la droite réelle, il est bien connu qu'une fonction et sa transformée de Fourier ne peuvent pas être simultanément à support compact sans s'évanouir complètement (parce que si une fonction était à support compact, alors sa transformée de Fourier serait une fonction analytique réelle, qui ne peut être à support compact sans s'évanouir complètement, du fait du prolongement analytique). Pourtant, le prolongement analytique est une propriété hautement "à une dimension" (elle exploite la connectivité). De plus, ça n'est pas une propriété robuste, et il est possible d'avoir des fonctions f sur la droite réelle telles que f et sa transformée de Fourier sont "presque à support compact", ou plus précisément rapidement décroissante ; la fonction gaussienne $f(x) = \exp(-\pi|x|^2)$, qui est sa propre transformée de Fourier, en est un particulièrement bon exemple. Dans le monde dyadique, l'analogue de la fonction gaussienne est la fonction en escalier $1_{B(0,1)}$, qui est aussi sa propre transformée de Fourier, et démontre ainsi qu'il est possible qu'une fonction et sa transformée de Fourier soient toutes les deux à support compact. Plus généralement, il est possible pour une fonction $f : F((1/t)) \to \mathbb{C}$ d'être à support sur un intervalle dyadique I, et pour sa transformée de Fourier d'être de suppport un autre intervalle dyadique J, tant que le principe d'incertitude $|I||J| \geq 1$ est respecté. On peut utiliser ces "paquets d'ondes de Walsh" (qui incluent les ondelettes de Haar et les fonctions de Radamacher comme cas parti-
culiers) pour réaliser de façon élégante et efficace une analyse en temps-fréquence dans le paradigme dyadique. Ce paradigme s'est avéré être un modèle inestimable de travail avant de s'attaquer aux problèmes temps-fréquence les plus intéressants dans le paradigme non-dyadique (tels que ceux liés au théorème de Carleson, ou à plusieurs intégrales singulières multilinéaires), car de nombreuses prises de tête techniques sont absentes dans le paradigme dyadique, alors que la combinatoire temps-fréquence (qui est vraiment le cœur du sujet) reste largement intacte. (Pour donner seulement un exemple, le théorème d'échantillonage de Shannon s'effondre, dans le paradigme dyadique, en l'énoncé trivial qu'une fonction qui est localement constante sur des intervalles dyadiques de longueur 2^{-n}, peut être reconstruite exactement en échantillonant cette fonction sur des intervalles

de 2^{-n}). Voir les notes de cours de Pereyra ou de moi-même pour de plus amples discussions. Dans certains cas, on peut en fait déduire un résultat d'analyse harmonique non-dyadique directement d'un résultat dyadique à travers une sorte d'argument de moyenne (ou la ruse de la translation de 1/3 de Michael Christ, qui est l'observation que tout intervalle non-dyadique (dans, disons, $[0,1]$) est contenu soit dans un intervalle dyadique de taille comparable, soit dans la translation de 1/3 d'un intervalle dyadique de taille comparable). En particulier, l'approche "fonction de Bellman" de l'analyse harmonique procède souvent par calcul de la moyenne, car la méthode de la fonction de Bellman nécessite une structure dyadique récursive (ou une structure continue de type noyau de la chaleur) pour fonctionner correctement. En général, pourtant, l'argument dyadique sert seulement de modèle de "carte routière" pour l'argument non-dyadique, plutôt que d'être un composant formel. Il y a seulement peu de cas connus où un résultat dyadique en analyse harmonique n'a pas montré la route vers une preuve de l'analogue non-dyadique ; une de ces exceptions est le problème d'établir un analogue non linéaire du théorème de Carleson, qui a été réalisé dans le paradigme dyadique mais reste ouvert dans le paradigme non-dyadique.

- Modèles dyadiques dans les EDP[2] -

Laissons maintenant l'analyse harmonique et tournons nous vers les modèles dyadiques et non-dyadiques d'autres parties des mathématiques. Je parlerai rapidement des EDP, qui sont un domaine dans lequel les modèles dyadiques ont prouvé qu'ils n'avaient qu'un impact limité (bien que le modèle dyadique de Katz-Pavlovic pour les équations d'Euler et Navier-Stokes soit peut-être un contre-exemple). Cela est en partie dû au fait que, contrairement à l'analyse harmonique, l'analyse des EDP exploite lourdement la dimension 1 de la droite réelle (et en particulier, l'axe temporel), par exemple à travers l'utilisation d'arguments de continuité ou de formules de monotonie. Cependant, on peut encore obtenir quelques analogues partiels de nombreux objets EDP, plus particulièrement ceux reliés à l'équation de la chaleur, si tant est que l'on veuille travailler avec des notions dyadiques pour le temps. Par exemple, dans le cas binaire $F = \mathbb{F}_2$, l'analogue dyadique de l'opérateur de la chaleur $e^{t\Delta}$ quand $t = 2^{2n}$ (une puissance de 4) serait l'opérateur d'espérance conditionnelle de la σ-algèbre engendrée par des intervalles dyadiques de longueur 2^n. Ces espérances conditionnelles sont nichées dans n, amenant une structure de martingale. Il y a en fait une très forte (et bien connue) analogie entre les opérateurs de la chaleur et les espérances conditionnelles selon une martingale ; pour donner seulement un exemple, l'inégalité stricte de Young sur la droite réelle prouvée par une méthode de flot de chaleur (assurant qu'une certaine expression multilinéaire est monotone le long du flot de chaleur), et l'inégalité stricte de Young sur $F((1/t))$ ou F^n peuvent être similairement prouvées (avec une preuve légèrement plus courte) par un argument imbriqué d'espérance conditionnelle.

- Modèles dyadiques en combinatoire additive -

Tournons-nous maintenant vers la combinatoire additive. Ici, il est souvent pratique pour des raisons combinatoires de travailler non pas sur un groupe additif infini tel que $\mathbb{R}$ or $\mathbb{Z}$, mais sur un groupe additif fini. Dans le paradigme non-dyadique, on utilise habituellement un groupe cyclique tel que $\mathbb{Z}/N\mathbb{Z}$; dans le paradigme dyadique, on utilise un espace vectoriel tel que F^n (on devrait

[2]EDP = Équations différentielles partielles.

penser à F comme étant fixé, e.g. $F = \mathbb{F}_2$ ou $F = \mathbb{F}_3$, et n grand). Une philosophie générale est que tant que ces deux groupes ont à peu près la même taille (i.e. $N \approx |F|^n$), alors la combinatoire additive de ces deux groupes sera à peu près analogue, même si algébriquement les groupes sont plutôt différents (le premier peut être engendré par un seul générateur, mais la plupart des éléments ont un grand ordre, alors que le second peut nécessiter de nombreux générateurs, mais tous les éléments ont un petit ordre). Mais le modèle dyadique tend à être significativement plus traitable pour un certain nombre de raisons. De façon plus évidente, le groupe F^n est aussi un espace vectoriel, et ainsi on peut appliquer les outils puissants de l'algèbre linéaire. Un groupe cyclique a seulement quelques analogues (désordonnés) d'outils algébriques linéaires ; par exemple, dans les groupes cycliques, les progressions arithmétiques généralisées sont en quelque sorte analogues aux espaces vectoriels étendus par un ensemble de vecteurs et ont beaucoup de sous-groupes ; de façon duale, les ensembles de Bohr (les ensembles de niveau de un ou plusieurs caractères) jouent le rôle des groupes cycliques analogues à l'intersection d'un ou plusieurs hyperplans dans F^n. Voir le papier de survol de Green pour une discussion plus approfondie. Une autre caractéristique du groupe F^n est la présence de drapeaux de sous-espaces, e.g. le drapeau de coordonnée

$$\{0\} = F^0 \subset F^1 \subset \ldots \subset F^n$$

qui permet dans certains cas de prouver des faits combinatoires dans F^n par une induction sur la dimension, et d'utiliser les outils reliés à de tels drapeaux comme la technique combinatoire de la *compression*. (se reporter à ce post précédent https://terrytao.wordpress.com/2007/03/22/freimans-theorem-in-finite-fields-via-extremal-set-theory/pour quelques exemples de cela).

Très récemment, pourtant, Ben Green et moi avons découvert que le manque de 1-dimensionnalité dans le modèle du corps fini peut rendre ce modèle *moins* traitable que le modèle du groupe cyclique dans certains sens techniques. Par exemple, la célèbre démonstration de Gowers du théorème de Szemerèdi ne fonctionne pas dans les modèles des corps finis à cause de ce petit pli. Cela semble avoir quelque chose à voir avec la (encore peu comprise) analogie entre les séquences nulles du paradigme non-dyadique, et les polynômes du paradigme dyadique. Nous espérons que nous aurons davantage à dire sur ce sujet dans le futur.

- Modèles dyadiques en combinatoire algébrique -

J'évoquerai brièvement le rôle des modèles dyadiques en combinatoire algébrique. Ici il semblerait que de nombreuses questions algébriques qui sont posées sur le corps $\mathbb{R}$ ou $\mathbb{C}$ s'effondrent en des questions purement combinatoires une fois qu'on "tropicalise" en passant au modèle dyadique, tel que le domaine des séries de Puiseux $\mathbb{C}\{t\}$. De plus (et plutôt de façon miraculeuse), certaines questions ont des réponses *identiques* dans les paradigmes dyadique et non-dyadique, nous autorisant à utiliser des gadgets combinatoires pour résoudre des problèmes algébriques. Par exemple, la question de comprendre les relations possibles entre les valeurs propres d'une somme $A + B$ de matrices hermitiennes, avec les valeurs propres de A et B séparément, est un problème algébrique non trivial ; mais en passant au modèle dyadique des séries de Puiseux et en extrayant les exposants dominants (ce qui n'affecte pas la réponse finale), il a été montré par Speyer que le problème s'effondre en celui de localiser un nid d'abeille entre trois ensembles de valeurs propres potentielles. (Ce fait, ainsi que celui décrit ci-dessous, a été établi plus tôt par Knutson et moi-même mais par une méthode plus indirecte). Il y a également une contrepartie discrète (en théorie

de la représentation) à ce phénomène ; la question du calcul des multiplicités du produit tensoriel pour le groupe unitaire $U(n)$ est aussi un problème algébrique non trivial, en grande partie dû au "mélange" entre des éléments de base des représentations irréductibles quand on prend les produits tensoriels et qu'on les décompose à nouveau en représentations irréductibles (dans le cas où $n = 2$, ce mélange est décrit par les coefficients de Clebsch-Gordan ; la situation est plus compliquée pour les grandes valeurs de n du fait des multiplicités dans la décomposition). Mais si on remplace la notion d'une représentation par le modèle "dyadique" d'une représentation cristalline, le mélange est éliminé (sans affecter les multiplicités), et il a été montré par Henriques et Kamnitzer que le problème de calculer les multiplicités du produit tensoriel s'effondre à nouveau en un problème de nid d'abeille. Il serait intéressant d'obtenir une explication plus générale de la raison pour laquelle ces phénomènes adviennent.

- Modèles dyadiques en théorie des nombres -

Finalement, je souhaite discuter du rôle des modèles dyadiques en théorie des nombres - un sujet qui a été en fait le sujet d'au moins un texte de diplôme. Par contraste avec les autres domaines discutés ci-dessus, il y a une fantastique disparité en théorie des nombres entre notre compréhension du modèle dyadique et celle du modèle non-dyadique ; plusieurs des plus célèbres problèmes en théorie des nombres non-dyadiques (e.g. l'hypothèse de Riemann, le dernier théorème de Fermat, la conjecture des nombres premiers jumeaux, la conjecture abc, la factorisation de grands nombres) sont de façon surprenante faciles à résoudre dans le monde dyadique (voir e.g. l'exposé de Zhang pour la version du dernier théorème de Fermat), mais personne ne sait comment convertir les arguments dyadiques dans le paradigme non-dyadique (bien que l'étape inverse de convertir des arguments non-dyadiques en arguments dyadiques soit habituellement plutôt évidente). Une exception notable ici est le problème de la parité, qui a résisté aux progrès à la fois dans le paradigme dyadique et dans le paradigme non-dyadique.

Venons maintenant à l'hypothèse de Riemann. De façon classique, la théorie des nombres s'est concentrée sur la structure multiplicative de l'anneau des entiers $\mathbb{Z}$. Après avoir factorisé le groupe des unités $\{-1, +1\}$, on restreint habituellement son attention aux entiers positifs $\mathbb{Z}^+$. Dans le modèle dyadique, on étudie la structure multiplicative de l'anneau $F[t]$ des polynômes pour un certain corps fini F. Après avoir factorisé le groupe $F^\times$ des unités, on peut restreindre son attention aux polynômes unitaires $F[t]_m$. Comme l'anneau des polynômes est un domaine euclidien, il a une factorisation unique, et en particulier, tout polynôme unitaire peut être exprimé de manière unique (à permutation près) comme le produit de polynômes unitaires irréductibles, que nous appellerons des polynômes premiers. On peut analyser le problème de compter les nombres premiers dans $F[t]$ en utilisant les fonctions zeta, en analogie complète avec le cas entier. La fonction zeta de Riemann est bien sûr donnée par

$$\zeta(s) := \sum_{n \in \mathbb{Z}^+} \frac{1}{n^s}$$

(pour $\mathrm{Re}(s) > 1$) et on introduit la fonction analogue zeta

$$\zeta_{F[t]}(s) := \sum_{n \in F[t]_m} \frac{1}{|n|^s}.$$

Dans les entiers, la factorisation unique donne l'identité

$$\log n = \sum_{d|n} \Lambda(d)$$

où $\Lambda(d)$ est la fonction de von Mangoldt, définie comme étant égale à $\log p$ quand d est la puissance d'un nombre premier p et 0 sinon. En prenant la transformation de Mellin de cette identité, nous concluons que

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n \in \mathbb{Z}^+} \frac{\Lambda(n)}{n^s},$$

qui est l'identité fondamentale reliant les zéros de la fonction zeta à la distribution des nombres premiers. On peut faire la même chose dans le cas dyadique, en obtenant l'identité

$$-\frac{\zeta'_{F[t]}(s)}{\zeta_{F[t]}(s)} = \sum_{n \in F[t]_m} \frac{\Lambda_{F[t]}(n)}{|n|^s}, (1)$$

où la fonction de von Mangoldt $\Lambda_{F[t]}(n)$ pour $F[t]$ est définie comme $\log |p|$ quand n est la puissance d'un polynôme premier p, et 0 sinon.

Jusqu'à présent, les situations dyadique et non-dyadique sont analogues et très proches. Mais maintenant, nous pouvons faire quelque chose de spécial dans le monde dyadique : nous pouvons calculer la fonction zeta explicitement en sommant par degré. En effet, on a

$$\zeta_{F[t]}(s) = \sum_{d=0}^{\infty} \sum_{n \in F[t]_m : \deg(n) = d} \frac{1}{|F|^{ds}}.$$

Le nombre de polynômes unitaires de degré d est $|F|^d$. En sommant la série géométrique, on obtient une formule exacte pour la fonction zeta :

$$\zeta_{F[t]}(s) = (1 - |F|^{s-1})^{-1}.$$

En particulier, l'hypothèse de Riemann pour $F[t]$ est une trivialité - il n'y a clairement pas de zéro quels qu'ils soient ! En insérant cela en retour dans (1) et en comparant les coefficients, on se retrouve bientôt avec un théorème des nombres premiers exact pour $F[t]$:

$$\sum_{n \in F[t]_m : \deg(n) = d} \Lambda(n) = |F|^d \log |F|$$

qui implique rapidement que le nombre de polynômes premiers de degré d est $\frac{1}{d}|F|^d + O(|F|^{d/2})$. (On peut généraliser l'analyse ci-dessus à d'autres variétés sur les corps finis, aboutissant au final aux conjectures de Weil (non démontrées), qui incluent l'"hypothèse de Riemann pour les corps de fonctions".)

Un autre exemple d'un problème qui est difficile en théorie des nombres non-dyadique mais qui est trivial en théorie des nombres dyadique est celui de la *factorisation*. Dans les entiers, on ne sait pas si un nombre de n chiffres peut être factorisé (probabilistiquement) en temps polynômial en n[3]

[3]Note de la traductrice : "PRIMES is in P" de Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, 2004.

(le meilleur algorithme connu pour de grands n, le crible de corps de nombres, est en un peu plus que $\exp(O(\log^{1/3} n))$; en effet, la difficulté présumée de la factorisation sous-tend des protocoles très utilisés tels que RSA. Pourtant, dans $F[t]$ avec F fixé, un polynôme f de degré n peut être factorisé (probabilistiquement) en temps polynomial en n par l'algorithme suivant en trois étapes :

- Calculer le pgcd de f et sa dérivée f' en utilisant l'algorithme d'Euclide (qui est en temps polynomial du degré). Cela localise tous les facteurs répétés de f, et permet de se ramener rapidement au cas où f est sans carré. (Cette ruse est inutilisable dans le cas entier, du fait de l'absence d'une bonne notion de dérivée).

- Observer (à partir du théorème de Cauchy) que pour n'importe quel polynôme premier g de degré d, on a $t^{|F|^d} = t \bmod g$. Ainsi le polynôme $t^{|F|^d} - t$ contient le produit de tous les nombres premiers de la factorisation de ce degré (et de tous les nombres premiers divisant d) ; en effet, par le théorème exact des nombres premiers et un comptage du degré, ce sont les seuls facteurs possibles de $t^{|F|^d} - t$. Il est facile de calculer le reste de $t^{|F|^d} - t$ modulo f en temps polynomial, et alors on peut calculer le pgcd de f avec $t^{|F|^d} - t$ en temps polynomial également. Cela isole essentiellement les facteurs premiers d'un degré fixé, et permet rapidement de réduire le cas quand f est le produit de nombres premiers distincts de même degré d. (Ici, on a exploité le fait qu'il y a de nombreux nombres premiers ayant exactement la même norme - ce qui est bien sûr clairement faux dans le cas des entiers. C'est également le cas dans l'étape 3 ci-dessous.)

- Maintenant, on applique l'algorithme de Cantor-Zassenhaus. Supposons que $|F|$ est impair (le cas $|F| = 2$ peut être traité par une modification de cette méthode). En calculant $g^{(|F|^d-1)/2} \bmod f$ pour des g sélectionnés au hasard, on peut générer quelques racines carrées de l'unité au hasard modulo f (grâce au théorème de Cauchy et au théorème des restes chinois ; il y a aussi une petite chance que l'on génère un élément non inversible, mais on traite ce cas facilement). Ces racines carrées a seront soit $+1$ soit -1 modulo chacun des facteurs premiers de f. Si l'on prend le pgcd de f avec $a+1$ ou $a-1$, on a une forte probabilité de séparer les facteurs premiers de f ; en répétant cela quelques fois, on isole bientôt tous les facteurs premiers séparément.

- Conclusion -

Comme la promenade tourbillonante ci-dessus l'a, on l'espère, démontré, les modèles dyadiques pour les entiers, les réels, et les autres objets "linéaires" se rencontrent dans de nombreuses parties différentes des mathématiques. Dans certains domaines, ils sont un modèle jouet ultra-simplifié et trop facile ; dans d'autres domaines, ils atteignent le cœur de la matière en fournissant un modèle dans lequel toutes les technicités non pertinentes sont supprimées ; et dans d'autres champs encore, ils sont un composant crucial dans l'analyse du cas non-dyadique. Dans tous ces cas, pourtant, il semble que la contribution que les modèles dyadiques nous fournissent en nous aidant à comprendre le monde non-dyadique est immense.