Introduction

L'arithmétique, c'est être capable de compter jusqu'à vingt sans enlever ses chaussures.

Walt Disney

Lorsque je commençais sérieusement à écrire *Promenades Mathématiques* vers le début de l'année 2001, dans une autre vie, j'avais bon nombre d'idées sur ce que je voulais développer et montrer à mes lecteurs futurs, mais j'étais bien loin d'imaginer ce qui m'attendait…

En effet le hasard a voulu, ou peut-être la providence, que je découvre à cette occasion un certain nombre d'ouvrages de vulgarisation, principalement les livres de Ian Stewart, et qu'à travers ces diverses lectures je me rende compte de mon immense ignorance dans de nombreux domaines des mathématiques...

La lecture assidue de (très) nombreux ouvrages m'a amené dans des directions extrêmement variées et surtout à me pencher sur des questions que personne ne m'avait présentées réellement à l'Université ni même suggéré d'explorer et ceci particulièrement dans deux domaines qui traversent une grande partie des mathématiques : les Fonctions d'une Variable Complexe, ce qui s'appelle encore parfois Théorie des Fonctions, et l'Arithmétique ou Théorie des Nombres.

Pour ce qui est de la Théorie des Fonctions j'avais bien quelques vagues souvenirs d'un enseignement universitaire de Maîtrise (apparition subliminale d'un professeur tout seul au fond de son amphi de cinq-cent places et trois malheureux étudiants s'essayant à déchiffrer des trucs que lui seul comprenait) et certains sont remontés à la surface (enfin, très vaguement, faut pas exagérer non plus), mais l'ensemble restait bien nébuleux… Aussi me suis-je lancé dans l'écriture de quelques textes destinés au site des *Promenades Mathématiques* à propos de diverses fonctions comme la Fonction Gamma ou les Fonctions de Bessel ou même l'Analyse Hilbertienne. Puis un texte plus général sur les Fonctions Complexes a vu le jour et, bien que n'étant ni un spécialiste de la question, ni un universitaire aux diplômes reconnus, tous ces textes sont devenus des espèces de références sur le Web.

Dans les divers domaines en question revenait comme une litanie la référence aux Intégrales Abéliennes, aux Intégrales Elliptiques puis aux Fonctions Elliptiques…[1], et là par contre ça ne me disait pratiquement rien (j'avais peut-être mal écouté à l'Université…) : j'ai donc empoigné le livre de Dieudonné sur l'histoire des mathématiques ([Die]) où les chapitres consacrés à ces questions sont extrêmement

[1] De même d'ailleurs dans la résolution d'équations différentielles ou d'intégrales dans Maple où les explications données sont fort succintes… mais incitent à aller y regarder de plus près.

touffus et difficiles à lire du fait de l'évolution rapide des idées (et des notations) dans ce domaine. Il n'empêche, j'ai mordu à l'hameçon et j'ai commencé à me documenter plus avant : les références les plus accessibles au premier abord sont en fait des textes du début du 19e siècle avec Legendre et Abel, assez difficiles à lire, puis des textes du début du 20e siècle (Greenhill ou Halphen par exemple) qui, même s'ils sont surtout tournés vers les applications mécaniques, donnent de très nombreuses idées et développements. Enfin, par le plus grand des hasards je suis tombé sur le MacKean & Moll ([Mck]) qui, sous des dehors « charmants » s'avère franchement redoutable au bout d'un moment...

Mais le déclic est vraiment venu quand j'ai découvert les divers liens cachés avec les grands thèmes arithmétiques du 20e siècle : Dernier théorème de Fermat-Wiles, fonctions modulaires, cryptographie, fonction Zêta, par exemple, et là j'ai commencé à vraiment travailler. Ça fait maintenant cinq ans que je suis là-dessus comme une bernique accrochée à son rocher, que mes livres de chevet sont « Elliptic Curves », « Multiplicative number theory », « Cours d'arithmétique », « An invitation to modern number theory », etc., que parfois je me prends pour André Weil ou Geoffrey Hardy (enfin, de très très très loin) et que je me dis que je vais prouver l'Hypothèse de Riemann (ah, ah, ah, …), bref tout ceci a envahi mon esprit et si je n'avais pas fait une pause d'un an je ne serais certainement pas là pour écrire ces lignes.

Mais revenons à l'idée de départ du livre : contrairement à ce qui s'était passé pour les Fonctions Analytiques, je n'ai pas mis en ligne les textes que j'écrivais au fur et à mesure et ceci pour une raison simple : il y a trop de choses à découvrir, à maîtriser, à comprendre et petit à petit cent cinquante puis deux cent pages se sont remplies où je complétais telle ou telle partie avec des résultats que je découvrais dans tel ou tel ouvrage, où je tentais une approche informatique d'une hypothèse non démontrée, où le fil et l'aiguille s'entremêlaient chez Eric Weisstein (MathWorld), sur Wikipedia, sur Chronomath, et plein d'autres activités très prenantes. Par exemple le chapitre sur les Fractions continues a nécessité pratiquement trois ans de travail (discontinu heureusement)… et je n'en suis pas pleinement satisfait d'ailleurs, loin s'en faut (à supposer qu'on puisse se satisfaire d'un tel sujet en évolution permanente).

Dans mon esprit il fallait que ces efforts débouchent sur un livre de « vulgarisation » abordant toutes ces questions, et ce d'autant plus qu'il n'y a pas beaucoup d'ouvrages généraux (et encore moins d'ouvrages écrits en français) essayant de mettre à la portée du plus grand nombre ces notions sans lesquelles de grands pans des mathématiques actuelles sont incompréhensibles et ne seraient certainement pas ce qu'elles sont[1]. Par ailleurs ayant déjà traité quelques questions d'Arithmétique dans *Promenades*, je suis reparti sur cette base : le niveau de lecture nécessaire ici suppose que le lecteur a déjà acquis l'essentiel des connaissances des *Promenades*, particulièrement en Analyse et Arithmétique.

Ce manque dans la littérature est d'autant plus étonnant d'ailleurs qu'une grande quantité d'idées modernes en Algèbre sont issues de questions d'Arithmétique (les groupes, les corps, les anneaux, les idéaux sont des outils de base en Arithmétique et ont souvent été créés pour répondre à un besoin de ce domaine) ; de même certaines questions d'Analyse comme les nombres p-adiques ou l'approximation des réels, pour

[1] Je n'ai aucune prétention à me mesurer avec des savants de stature internationale comme Marc Hindry, Henri Cohen ou Gérald Tennenbaum pour ne citer que des auteurs de langue française, mais je souhaitais simplement aborder des questions et des méthodes que tout étudiant de Licence devrait sinon maîtriser, du moins connaître, me semble-t-il, et ceci sans autre prétention que le plaisir de la découverte et de la vulgarisation. Dans le même registre que ce livre on pourra lire [Gross] qui est un bon complément.

ne citer que ces thèmes, sont fondamentaux en Arithmétique et en sont un des principaux domaines de recherche actuellement.

Un autre aspect plus visible, si on peut dire, concerne plus précisément la Cryptographie et ses usages modernes à travers la protection des données et de la vie privée des personnes : les théorèmes actuels de Cryptographie ne donnent pratiquement jamais la certitude que l'on serait en droit d'attendre, à savoir que rien ne permet d'affirmer l'inviolabilité d'un cryptage, et ce thème reste un objet de recherche très disputé.

Enfin de nombreux problèmes envahissent la recherche mathématique moderne à partir de questions essentielles comme la Géométrie Combinatoire, descendante directe de la « Géométrie des Nombres » de Hermann Minkowski, la Théorie des Graphes, les Codes (dont le traitement fait appel à de nombreuses notions d'Algèbre), etc. Et puis les recherches arithmétiques ont croisé par hasard la Mécanique Quantique vers 1960 : les zéros de la fonction *Zêta* sont visiblement liés aux valeurs propres de matrices aléatoires modélisant des observables quantiques, laissant entrevoir diverses directions pour des explorations futures.[1]

Bref, la formation de l'honnête femme ou homme à la recherche de connaissances accessibles avec un minimum de savoir reste mon objectif principal et préféré : pas la peine de (trop) réviser ses classiques d'Algèbre ou d'Analyse, les trois-quarts du livre doivent être accessibles avec un niveau de Terminale Scientifique… Je triche un peu mais, même si ce n'est pas tout à fait vrai le niveau étant plutôt L2 ou L3, j'ai essayé de limiter au maximum les connaissances nécessaires tout en offrant un grand choix de parcours accessibles dans cette jungle moderne que sont les mathématiques actuelles.

* *
*

L'architecture du livre ne suit pas forcément une démarche chronologique, la séparation se faisant plutôt entre Arithmétique Classique et Théorie des Nombres : les neuf premiers chapitres traitent de questions où l'utilisation de l'Analyse Complexe n'est pas indispensable ; il n'empêche que, même à ce premier niveau de complexité, de nombreuses questions restent ouvertes et j'ai essayé d'en détailler quelques unes. Par ailleurs divers problèmes d'Analyse ou d'Algèbre apparaissent de manière structurante au fil des situations comme par exemple les *formes quadratiques*, l'*approximation*, les *fonctions arithmétiques*.

Les trois chapitres suivants traitent des Fonctions Analytiques ainsi que des deux grands exemples que sont la fonction *Gamma* d'Euler et la fonction *Zêta* de Riemann, ce chapitre étant naturellement suivi par le *Théorème des Nombres Premiers*. Une troisième partie s'intéresse aux bases des *Fonctions Elliptiques*, des *Fonctions Thêta* et des *Formes Modulaires* qui décrivent de manière intime la structure profonde des relations entre les nombres ; ces chapitres sont relativement lourds d'un point de vue calculatoire malgré mes efforts pour élaguer au maximum ; enfin quelques thèmes transversaux comme

[1] Évidemment, dans un ouvrage tel que celui-ci, il est hors de question d'être exhaustif et divers problèmes importants ne sont qu'effleurés, mais j'ai essayé d'aller le plus loin possible dans la plupart des questions soulevées. Comme par ailleurs je fournis toujours les références d'ouvrages permettant de développer tel ou tel point, j'ose espérer que les lecteurs ne m'en tiendront pas rigueur.

Partitio Numerorum ou *Formes Quadratiques* viennent mettre une touche provisoirement finale à ce tableau.

En fait la deuxième moitié du livre est presque plus analytique qu'arithmétique, mais dans ce domaine, même si on arrive parfois à des résultats sans passer par la Théorie des Fonctions, comme par exemple la démonstration du Théorème des Nombres Premiers par des méthodes « élémentaires », on voit bien que certains objets basiques font partie des éléments constitutifs de l'Arithmétique et des fondements des mathématiques.

Les lecteurs attentifs remarqueront immédiatement qu'il n'est pas question du *Théorème de Fermat-Wiles*, tarte à la crème des ouvrages de vulgarisation : c'est totalement volontaire car la filiation de ce théorème n'est pas très conséquente et même si sa démonstration a permis diverses avancées très importantes, la technicité des questions posées m'interdit pratiquement d'en parler autrement que de manière « journalistique », chose déjà faite dans *Promenades*. De même je n'ai que peu abordé les problèmes diophantiens à part l'équation de Pell-Fermat et quelques situations liées aux courbes elliptiques, chaque problème demandant un traitement quasiment individuel. A contrario on peut se demander si les *Suites de Farey* qui occupent un bon chapitre méritaient autant d'honneur… En fait oui, bizarrement, car on va les retrouver au carrefour de diverses questions dont les *Fractions Continues* et l'*Hypothèse de Riemann* !

Au final le domaine abordé pourrait sembler colossal et c'est d'ailleurs vrai, la littérature sur toutes ces questions représentant une partie significative de la production mathématique passée, présente et probablement à venir ; mais j'ai essayé de faire des choix de « cœur » plutôt que de raison, gardant toujours à l'esprit les possibilités du calcul et de l'informatique, la visualisation plutôt que l'aridité de la présentation formelle, les applications plutôt que la théorie, et j'espère, chère lectrice, cher lecteur, te faire partager un petit peu du plaisir et du désir qui s'emparent de l'âme quand la beauté du raisonnement, la finesse de l'hypothèse, la subtilité du calcul donnent accès au paradis caché des mathématiciens.

* *
*

Quelques remarques techniques : dans la mesure du possible un certain nombre de questions supplémentaires sont traitées sur le site http://promenadesmaths.free.fr ; des sujets comme l'équirépartition, les nombres premiers dans les suites arithmétiques, l'approche probabiliste, … étant trop longs à traiter ici, nous les proposons sur le Web.

Les références et les liens cités dans le corps du livre ne sont pas forcément pérennes, ils sont disponibles sur le site et j'essaie de les garder actifs ou de trouver l'équivalent s'ils viennent à disparaître ; les liens de la bibliographie quand à eux sont de deux ordres : ceux vers des sites « lourds » comme Gallica, MathWorld, Wikipedia, Numdam, … ne risquent pas vraiment de disparaître, par contre pour nombre d'autres liens il peut y avoir un doute, aussi les fichiers correspondants sont stockés sur le site, ils sont signalés dans la bibliographie par ce symbole : 🗁.

Les illustrations proviennent de plusieurs logiciels : Maple ®, Geogebra ®, Excel ® : les fichiers originaux, comme pour *Promenades Mathématiques*, sont également disponibles sur le site. La bibliographie étant plutôt vaste, je fournis une liste d'ouvrages de base à lire pour chaque chapitre ; les liens vers Wikipedia et MathWorld fournissent également souvent des références, malheureusement il est difficile de connaître précisément l'intérêt d'un ouvrage rien qu'à son titre ou à quelques pages de présentation, les critiques de livres de mathématiques n'étant pas légion. De plus la majorité des

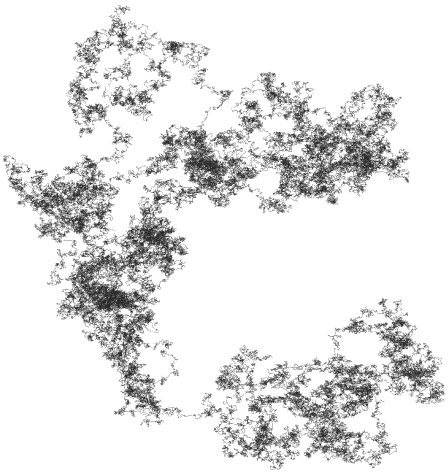
ouvrages cités sont en anglais et bien que disponibles par internet interposé ou dans les bonnes bibliothèques universitaires, leur achat peut vite s'avérer dispendieux...

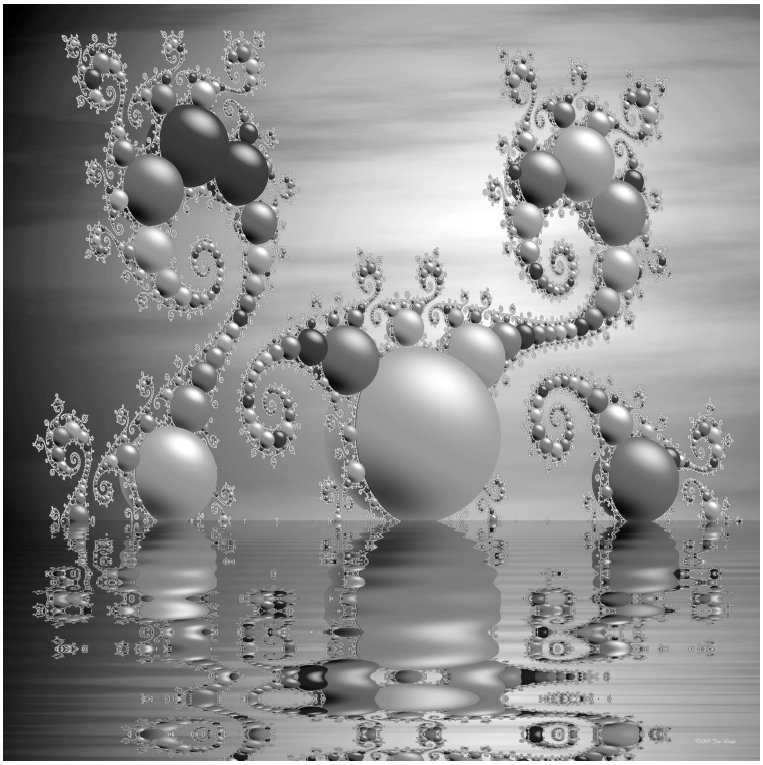
Dans le texte les références bibliographiques sont parfois accompagnées de l'emplacement exact dans l'ouvrage cité : par exemple [Har, 6.22] renvoie au chapitre 6, §22. J'ai adopté cette manière de faire car il peut y avoir des rééditions ou des traductions non paginées de la même manière suivant les versions ; c'était par ailleurs indispensable dans la mesure ou je ne démontre pas tous les résultats utilisés.

Un dernier point qui peut sembler mineur mais ne l'est absolument pas, ni dans mon esprit, ni dans la réalité, est l'interpellation régulière du « lecteur » : ce dernier peut aussi bien être une femme qu'un homme, mais les habitudes et le machisme de la langue française font que le terme masculin prend habituellement le dessus. Aussi à chaque fois que cela s'est présenté ai-je tiré à pile ou face pour savoir à qui je m'adressais… Le résultat du tirage est que sur 36 « lecteurs » il y a finalement 17 lectrices et 19 lecteurs.

Je tiens enfin à exprimer ma profonde reconnaissance à toutes celles et ceux qui m'ont aidé et soutenu : mon épouse Christine, d'une infinie patience, Corinne Baud, toujours aussi efficace, Christian Leboeuf, sans qui ce livre n'existerait même pas, Jos Leys, Jean-François Colonna et Géraud Bousquet qui m'ont autorisé à utiliser les magnifiques images qu'ils produisent et bien sûr toutes les lectrices et tous les lecteurs de *Promenades* qui m'ont montré que ce que je faisais pouvait présenter quelqu'intérêt.

Montpellier, avril 2010





Groupe de Klein (Jos Leys)

1. Brève histoire des débuts de l'Arithmétique

> *Le discours mathématique est extrêmement codifié ; c'est d'ailleurs son aspect formel que cette expression évoque en premier lieu. C'en est sa raison d'être : le rôle du formalisme est (ne devrait être que) la validation du discours. Mais ce discours est signifiant. La forme, aussi sophistiquée soit-elle, ne créée pas plus le sens que la synthèse des molécules, aussi complexes soient-elles, n'engendre la vie.*
>
> Jean-Marc Deshouillers[1]

L'Arithmétique, comme son nom l'indique (du grec *arithmos=nombre*), est l'étude des nombres. Les nombres sont entiers naturels dans $\mathbb{N}$, entiers relatifs dans $\mathbb{Z}$, ou rationnels dans $\mathbb{Q}$; ils peuvent également être réels dans $\mathbb{R}$, voire complexes dans $\mathbb{C}$ ou pire encore (quaternions, octonions, etc.) mais le traitement de ces derniers ne fait pas à proprement parler partie de l'Arithmétique. La Théorie des Nombres est la même chose, mais en plus élaboré…

Tout au long de son développement historique, ses frontières avec l'Algèbre et l'Analyse ont été mouvantes et souvent imprécises ; une séparation assez naturelle s'est d'ailleurs établie chez les Grecs entre arithmétique pratique (le calcul ou *logistique*) et arithmétique théorique, distinction que l'on retrouve toujours plus ou moins.

La première comprenait les diverses numérations parlées et écrites, la représentation des fractions et les techniques opératoires relatives aux quatre opérations élémentaires : addition, soustraction, multiplication et division. Quand à la deuxième ce sera l'objet de la majeure partie de ce livre…

1.1. Systèmes de numération écrite

Il y a quelque 40 000 ans, lorsqu'ils commencèrent à se civiliser, les premiers *Homo sapiens* ne connaissaient pas les chiffres. Il est probable qu'ils commencèrent à désigner des quantités avec leurs doigts puis qu'ils pensèrent à les « écrire » quelque part : certains signes peints font penser à des comptages de nombre d'animaux ou de lunaisons ou Dieu seul sait quoi…

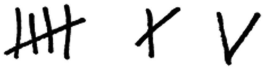
Par exemple, datant du Paléolithique moyen ($-300\,000$ à $-30\,000$), on a trouvé un os de loup comportant 55 encoches rangées en deux séries groupées par paquets de 5 ; sur

[1] J. M. Deshouillers, *Les Déchiffreurs* (ouvrage collectif), Belin, 2008.

un os vieux de 10 000 ans on peut voir l'image d'un sanglier avec 17 traits : le chasseur y décrit certainement ses chasses. Sur les galets peints ou gravés de la Grotte du Mas d'Azil[1] de nombreux points ou marques sont présents, marques calendaires ? comptages ? On ne sait.

Cette technique de traits fut longtemps employée car facile à réaliser et facile à comprendre, mais avec l'usage nos ancêtres se rendirent compte qu'avec de nombreux traits des erreurs apparaissent car notre capacité visuelle est limitée : lorsque le nombre de traits dépasse quatre, tout se brouille, on ne sait plus très bien où l'on en est. D'après Stanislas Dehaene l'homme, de même que la plupart des animaux, disposerait d'un accumulateur intégré qui lui permet de « peser » des quantités : deux zones spécialisées du cerveau sont sollicitées. Dans une zone du cortex frontal on compte de 1 à 4 directement ; lorsque les quantités considérées deviennent plus importantes une zone plus profonde intervient et prend le relais : on va s'attacher à estimer le résultat et non à compter directement.

La solution est venue il y a quelques milliers d'années : il s'agit d'éviter d'aligner plus de quatre traits successifs. Le nombre 5 devient quatre entailles traversées par une barre, puis une barre barrée puis un V.



Pour les autres nombres, on ajoute des traits que l'on barre, etc. ce que l'on fait encore, par exemple pour compter des bulletins de vote.

1.1.1. Égypte

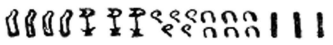
Les numérations parlées remontent partout aux époques les plus reculées : Aristote remarquait d'ailleurs que la plupart des peuples comptaient par dizaines à quelques exceptions près.

La numération écrite égyptienne est fondée sur la base 10 ; lorsqu'il s'agit de ce que l'on pourrait appeler la numération gravée (hiéroglyphes), chaque puissance de 10 possède un signe propre :

unité (un bâton), dizaine  (un arceau), centaine  (une spirale),

millier  (une fleur de lotus), dizaine de mille  (un doigt montrant le ciel),

centaine de mille  (un têtard, symbole du non-dénombrable : il y a beaucoup de têtards au bord du Nil) million  (le dieu de l'infini : oh, my God !).

Pour représenter un nombre on accole les symboles sans ordre bien établi, avec parfois des simplifications. Par exemple  représente 43563.

L'écriture hiératique amène également diverses solutions qui font penser aux numérations alphabétiques ultérieures (grecque, hébraïque et arabe).

[1] http://www.cerimes.fr/le-catalogue/galets-graves-aziliens-analyse-microscopique.html