Ci-dessous les idées qui m'ont amenée aux miennes (DV, 25/4/2014)

- la manière dont Gauss met les nombres tête-bêche : pour trouver la formule de la somme des n premiers entiers, ou bien pour voir comment "tombent en face" ou "pas en face" les résidus quadratiques d'un nombre premier suivant qu'il est de la forme $4k+1$ ou $4k+3$. La lecture intensive des sections 1, 2, 3 et 4 des Recherches arithmétiques ;

- la notion d'invariant informatique qui intervient dans le modèle de preuves de programmes de Hoare ;

- toutes les conférences d'Alain Connes, notamment son insistance sur la notion de permutations de lettres, qu'il présente dans ses conférences sur la théorie de l'ambiguité de Galois ;

- les notions de permutations qui interviennent dans le jeu du taquin, auquel j'ai souvent joué ;

- la recherche intensive d'anagrammes depuis mai 2013 ;

- le fait qu'Alain Connes ait dit en conférence que les algèbres non-commutatives si complexes qu'ils étudiaient pouvaient trouver leur illustration dans la très simple structure de monoïde, cumulé au fait que la concaténation des mots est non-commutative ; ces notions m'étaient familières pour avoir suivi plusieurs cours de théorie des langages lors de mes études universitaires ;

- le fait que la structure *chaîne de caractères* (string) soit une structure de données essentielle en informatique et que la concaténation des mots, ainsi que toute autre opération sur les chaînes (reconnaissance de sous-chaînes, comptage de lettres, etc) soit un concept sous-jacent à toute l'idée de programmation informatique ;

- le fait que la notion d'*échange* (*swap*) soit une action essentielle en informatique (elle est enseignée en tout début de formation, lorsque est présenté le piège de l'échange brutal de deux variables, sans en passer par une troisième pour échanger, et qui fait perdre un contenu) ; elle est réutilisée intensivement en algorithmique, dans les algorithmes de tris par exemple ;

- la notion de machine de Turing avec son ruban de booléens plutôt qu'un ruban de lettres, dont la tête de lecture lit les éléments et agit en fonction de leur valeur et de sa liste d'instructions qui est exactement ce qui intervient ici dans la notion de règles de réécriture sous-jacentes à la composition des mots, ces idées ayant été ravivées lors de la conférence récente de Bernard Chazelle et par la lecture de la biographie de Turing d'Andrew Hodges ;

- ma redécouverte du petit livre de Trathenbrot et ses invariants qui interviennent dans le problème des mots ;

- l'impossibilité de lire des articles de géométrie non-commutative ou de mathématiques en général qui m'a fait prendre la décision de revenir à mes fondamentaux à Noël 2013 : la programmation, les instructions, les variables, les booléens, les invariants de Hoare ;

- la rencontre d'Yves Meyer qui donnait une conférence à des lycéens au sujet de la preuve d'Helfgott de la conjecture ternaire de Goldbach ; cela m'a amenée à lire et visionner des articles sur la théorie des ondelettes utilisée dans la compression d'images ; mais par une curieuse coïncidence, peu de temps avant que je ne le rencontre, des articles sont sortis sur une nouvelle méthode révolutionnaire de compression d'images, qui utilise le fait que l'information est condensée dans certains pixels (i.e. on peut retrouver toute l'information en ne conservant que les pixels en question, et en déduisant de celle-ci toutes les autres). Cela m'a confortée dans l'idée, que j'avais déjà d'ailleurs à cause de la programmation de la fonction somme des diviseurs d'Euler, que des booléens codant seulement l'information premier-composé devaient pouvoir suffire à mener le raisonnement (sans en passer comme je l'avais toujours fait jusque-là, par les restes dans les différents corps premiers) ;

- la lecture d'articles sur les groupes de tresses avec là-encore, permutations de variables et invariants ;

- le fait d'avoir lu que les pavages de Penrose peuvent être étudiés en utilisant des chaînes de booléens telles que $x_n = 1 \implies x_{n+1} = 0$, ce qui est exactement ce qui se produit dans le cas de la divisibilité

d'entiers successifs par un certain nombre ;

- le fait d'avoir, par formation initiale, une manière de penser calculatoire : Richard Karp, éminent informaticien américain, présente dans la dernière partie de sa conférence à la fondation Simons, ce qui distingue les mathématiciens des informaticiens : ils diffèrent dans leur manière d'aborder les problèmes ; selon Karp, un informaticien regarde les processus, les changements, la dynamique : il cherche ce qui change tandis qu'un mathématicien regarde les objets décrits par un ensemble fixe d'axiomes et peut prouver l'existence de solutions d'une manière non forcément constructive. La notion importante, selon lui, pour les informaticiens, est celle de calcul effectif et de processus dynamiques ; Karp ne parle pas de mathématiciens qui se préoccupent de la notion de temps ;

- la lecture de livres de vulgarisation de mécanique quantique : les équations de Bell, qui lient entre elles des variables ; et l'intrication de q-bits dans le cadre de la communication codée d'Alice et Bob ;

- l'écoute des conférences d'Alain Aspect et Serge Haroche, qui expliquent l'intrication des photons, dans le cadre de l'expérience des fentes de Young entre autres ;

- l'article de Rosser et Schoenfeld qui fournit des minorations et majorations pour $\pi(x)$ ou $\pi(2x)-\pi(x)$, mais sans lui, on sait que les nombres premiers vont se raréfiant tandis que les nombres composés sont de plus en plus nombreux par le Théorème des Nombres Premiers conjecturé par Gauss et prouvé par Hadamard et De La Vallée-Poussin ;

- le fait d'avoir reçu, de 1968 à 1975, une éducation élémentaire aux mathématiques par la méthode dite des "mathématiques modernes" : ensembles, bijections, tableaux à double entrée, numération et comptage dans différentes bases ;

- le fait d'avoir eu, toute petite, deux jeux extra : la maison aux clefs géométriques, et le puzzle de Notre-Dame de Paris.