Changer l'ordre sur les entiers naturels pour comprendre le partage des décomposants Goldbach

Denise Vella

Octobre 2007

1 Introduction

La conjecture de Goldbach (1742) énonce que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers.
Cette note présente un nouvel ordre sur les entiers, basé sur un système de numération par les restes modulaires découlant du théorème des restes chinois, qui vise à faire appréhender la façon dont les nombres pairs partagent des décomposants Goldbach[1].
Je remercie Denis Guedj d'avoir fait "revivre Cantor" par son livre "Villa des hommes" paru en septembre 2007 et Nathalie Charraud pour la même raison par son livre "Infini et Inconscient : essai sur Georg Cantor".

2 Deux anecdotes en école élémentaire

La première anecdote est inventée ; la seconde est vécue[2].

Imaginons une maîtresse de CP qui demande à un élève de ranger un ensemble de formes géométriques selon leur couleur. Après une réalisation laborieuse de la consigne par l'élève, elle lui demande "Combien y-a-t-il de rectangles ?" L'élève est en droit de se rebeller : "Comment ? On me demande un classement. Je m'attends à une question en relation avec le classement effectué du style "combien y-a-t-il de formes de couleur bleue par exemple ?" et on me pose au lieu de cela une question qui m'oblige à littéralement "bouleverser" mon classement". Dans la suite de cette note, j'ai postulé que l'on n'arrivait pas à prouver la conjecture de Goldbach car on n'avait pas utilisé encore le bon "classement" des entiers naturels.

Deuxième exemple, vécu cette fois. Il peut arriver, en classe de CE2, lorsqu'on introduit les milliers en numération que des élèves qui ont à ranger des nombres dans l'ordre croissant écrivent par mégarde que 1236 est plus petit que 702. L'explication de ce fait peut être que l'ordre lexicographique du dictionnaire qu'ils ont acquis se "télescope" alors avec l'ordre engendré par le système de numération décimale et les élèves appliquent la règle "j'ordonne les mots (là, il

[1] On appelle décomposant Goldbach d'un nombre pair donné un nombre premier qui est terme d'une somme de deux nombres premiers de valeur égale au nombre pair en question.

[2] Après 8 années d'ingéniorat d'informatique, je me suis reconvertie professeur des écoles.

s'agit de nombres) en observant leur première lettre (là, il s'agit de chiffres) ; s'il y a égalité, je m'occupe de la deuxième lettre, etc". Et ils oublient de regarder en premier lieu et tout simplement le "nombre" de chiffres des nombres à comparer. Dans le dictionnaire, le mot "alphabet" est avant le mot "bol" par exemple, bien que comptant beaucoup plus de lettres que ce dernier car a est avant b dans l'ordre alphabétique et donc cela peut ne pas être choquant pour un élève que 1236 soit inférieur à 702 dans la mesure où 1 est inférieur à 7[3].

Dans la suite, on introduira un ordre lexicographique (utilisant d'ailleurs la notion de préfixe) dans un système de représentation des entiers naturels par leurs restes chinois.

3 Théorème des restes chinois et système de numération par n-uplets de restes

J'ai dans un premier temps voulu ordonner lexicographiquement les entiers de 0 à 210 (qui est le produit des quatre premiers nombres premiers 2, 3, 5 et 7) en les représentant chacun par leurs quatre restes dans les divisions par ces nombres premiers. J'ai obtenu l'ordre suivant, étonnant, dû au théorème des restes chinois. Les résultats sont présentés dans deux tableaux (le tableau correspondant aux nombres pairs s'obtient par complémentarité à 209), un pour les nombres pairs, et un pour les nombres impairs. Les en-têtes des lignes fournissent les restes des divisions des nombres se trouvant dans les cases du tableau par 2, 3 et 5 (ou classes d'équivalences modulo 2, 3 ou 5), et les en-têtes de colonnes fournissent le reste de la division des nombres des cases de la colonne par 7 (ou classe d'équivalence modulo 7). On a coloré les nombres premiers en bleu.

	$(---6)$	$(---5)$	$(---4)$	$(---3)$	$(---2)$	$(---1)$	$(---0)$
$(124-)$	0	89	179	59	149	29	119
$(123-)$	83	173	53	143	23	113	203
$(122-)$	167	47	137	17	107	197	77
$(121-)$	41	131	11	101	191	71	161
$(120-)$	125	5	95	185	65	155	35
$(114-)$	139	19	109	199	79	169	49
$(113-)$	13	103	193	73	163	43	133
$(112-)$	97	187	67	157	37	127	7
$(111-)$	181	61	151	31	121	1	91
$(110-)$	55	145	25	115	205	85	175
$(104-)$	69	159	139	129	9	99	189
$(103-)$	153	33	123	33	93	183	63
$(102-)$	27	117	207	87	177	57	147
$(101-)$	111	201	81	171	51	141	21
$(100-)$	195	75	165	45	135	15	105

L'énoncé du théorème des restes chinois (qui date du troisième siècle et a été développé par le mathématicien chinois Sun Tzu) est le suivant :

[3]Concernant le traitement de l'erreur en didactique des mathématiques, on consultera "l'âge du capitaine" de Stella Baruk [22].

$$\begin{array}{l} \textit{Soient } k \textit{ nombres entiers naturels } m_1,\ m_2,\ ...,\ m_k \\ \qquad\qquad \textit{premiers entre eux deux à deux} \\ \quad \textit{et } k \textit{ entiers } r_1,\ r_2,\ ...,\ r_k, \\ \textit{le système de congruence} \begin{cases} x \equiv r_1\ (mod\ m_1) \\ x \equiv r_2\ (mod\ m_2) \\ ... \\ x \equiv r_k\ (mod\ m_k) \end{cases} \\ \textit{admet une unique solution modulo } M = m_1 m_2 ... m_k \end{array}$$

A cause du théorème des restes chinois, chaque entier est solution d'une infinité de systèmes de congruences.
Par exemple, l'entier 26 est solution du système :

$$\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \end{cases}$$

mais également du système :

$$\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \\ x \equiv 1\ (mod\ 5) \end{cases}$$

ou encore du système :

$$\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 2\ (mod\ 3) \\ x \equiv 1\ (mod\ 5) \\ x \equiv 5\ (mod\ 7) \\ x \equiv 4\ (mod\ 11) \\ x \equiv 0\ (mod\ 13) \\ x \equiv 9\ (mod\ 17) \\ x \equiv 7\ (mod\ 19) \\ x \equiv 3\ (mod\ 23) \\ x \equiv 26\ (mod\ 29) \\ x \equiv 26\ (mod\ 31) \\ x \equiv 26\ (mod\ 37) \end{cases}$$

On peut donc associer à tout entier plusieurs représentations par des n-uplets de restes. En l'occurence, on pourrait associer à 26 les représentations par n-uplets de restes suivantes : $(0, 2)$ ou $(0, 2, 1)$ ou $(0, 2, 1, 5, 4, 0, 9, 7, 3, 26, 26, 26)$.
Un tel système de numération[4] permet de représenter un grand nombre entier par un ensemble d'entiers plus petits et est notamment utilisé en cryptographie.

On trouve dans [3] quelques points forts de l'histoire du théorème chinois des restes (notamment sa première formulation dans le traité classique de Sunzi, puis son apparition dans les Neufs Chapitres[5] ou dans le Liber Abbaci de Fibonnacci ; le théorème des restes chinois a été également présenté par Euler, ou

[4] appelé RNS dans la littérature anglo-saxonne pour Residue Numeration System.

[5] Mon nom d'épouse est Chemla ; ce nom est également celui d'une mathématicienne et épistémologue française renommée qui a réalisé un travail considérable d'analyse des Neufs Chapitres. Cela fait au moins deux personnes nommées Chemla et s'intéressant au théorème des restes chinoisn !

bien de façon plus contemporaine par Shockley, Prather, ou Weiss).
Notons ici qu'on le trouve également dans le paragraphe 38 des Recherches Arithmétiques de Gauss mais reformulé par des congruences (que Gauss a inventéees). Si l'on considère chaque congruence comme représentant un ensemble d'entiers naturels, on peut dire que chaque entier est solution d'une multitude de systèmes de congruence correspondant à différents ensembles de nombres auxquels il appartient (éventuellement "inclus" les uns dans les autres).

Une formulation m'intéresse parmi toutes celles présentées par Davis et Hersh ; elle est d'abord présentée succinctement, puis analysée précisément un peu plus loin. Il s'agit de la formulation du théorème des restes chinois par Prather, un "savant informaticien contemporain".

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ *est la décomposition de l'entier n en facteurs premiers* $(p_i^{\alpha_i} = q_i)$
alors le groupe cyclique Z_n *a la représentation produit* $Z_{q_1} \times Z_{q_2} \times ... \times Z_{q_r}$.

L'analyse extraite de "l'Univers mathématique" de Davis et Hersh de la formulation par Prather du théorème des restes chinois est fournie en annexe 2.

Ma formation initiale est une formation en informatique[6]. Cette formation incluait notamment un cours de théorie des langages et automates[7].
Dans cette théorie, on définit un alphabet A comme un ensemble fini non vide de symboles. On appelle monoïde libre engendré par A l'ensemble A* muni de la concaténation des mots[8]. Enfin, on appelle langage sur l'alphabet A ou langage de A* tout ensemble de mots de A*. Autrement dit, un langage sur A est un sous-ensemble de A*.

Nous avons choisi de représenter les entiers par des n-uplets de restes. Cela présente deux particularités, si l'on considère les représentations par restes comme les mots d'un langage dans la théorie des langages :

- l'alphabet d'appartenance des lettres des mots est infini, c'est $\mathbb{N}$,
- à chaque entier pourrait être associée une infinité dénombrable de mots en bijection avec $\mathbb{N}$ selon la longueur du n-uplet de représentation que l'on choisit.

Pour pallier au deuxième inconvénient, on va choisir d'associer à chaque entier un unique n-uplet le représentant, en ne s'intéressant qu'aux modules premiers inférieurs à sa racine. On considère ainsi l'unique système de congruences selon les nombres premiers inférieurs à la racine du nombre que l'on veut représenter[9].
Fournissons quelques exemples de représentations :
14 et 20 ont pour représentations (0,2).
38 a pour représentation (0, 2, 3).
76 a pour représentation (0,1,1,6).

[6] J'ai obtenu un DEA d'intelligence artificielle en 1987.
[7] Le paragraphe suivant présentant des définitions est extrait du livre [2].
[8] A* consiste à introduire le mot particulier appelé "mot vide" de longueur nulle.
[9] Delahaye présente ce "système de numération en nombres premiers" (page 72 de son livre "Merveilleux nombres premiers").

4 Hilbert, Cantor et la notion d'ordre sur les entiers

Dans une biographie de Hilbert, on trouve que "Hilbert affirme la résolubilité de tout problème mathématique". Il écrit "Jamais le mathématicien ne sera réduit à dire Ignorabimus". Cette conviction lui fait dire à Klein : "Il vous faut avoir un problème. Choisissez un objectif déterminé et marchez franchement vers lui. Vous pourrez ne jamais atteindre le but mais vous trouverez sûrement quelque chose d'intéressant en chemin."

La conjecture de Goldbach, comme la conjecture des nombres premiers jumeaux ou essentiellement l'hypothèse de Riemann, fait partie du huitième problème de la liste de 23 problèmes exposée en 1900 par Hilbert. Hilbert avait placé en tête de ses 23 problèmes celui de l'hypothèse du continu de Cantor[10].

Enfin, Hilbert écrit ceci de l'ordre sur les entiers : "l'ordre dit naturel des nombres d'un système est celui où l'on regarde un plus petit nombre comme précédant un plus grand qui sera de son côté regardé comme suivant le premier. Il y a, c'est facile à voir, une infinité d'autres manières d'ordonner les nombres d'un système". Hilbert dit également "Nul ne doit nous exclure du paradis que Cantor a créé".

Cantor a créé la théorie des ensembles, a inventé les nombres "transfinis". Si l'on souhaite avoir des détails sur les avancées majeures qu'il a apportées aux mathématiques, on consultera les références [4], [5], [6] et [14] ainsi que ses oeuvres sur Gallica. Il est à l'origine de l'idée de modifier l'ordre sur les entiers. Citons une phrase de Cantor illustrant sa prise de conscience du bouleversement qu'il introduit : "Ce-disant, je ne dissimule en aucune façon que par cette entreprise, j'entre en opposition, dans une certaine mesure, avec des conceptions largement répandues concernant l'infini mathématique et avec les points de vue que l'on a fréquemment adoptés sur l'essence de la grandeur numérique.".

Présentons maintenant un exemple classique de bouleversement de l'ordre sur les entiers que Cantor propose et qui va nous amener à définir un ordre qui semble pertinent pour comprendre la conjecture de Goldbach. D'ailleurs, Cantor s'est intéressé à la conjecture de Golbach en 1894 et en a publié une table de vérification jusqu'à 1000 au congrès de l'AFAS.

Si par exemple, on décide de réordonner les entiers en énumérant dans un premier temps tous les entiers pairs puis tous les entiers impairs, les entiers seront énumérés selon l'ordre suivant :

$$0, 2, 4, 6, 8, ..., 1, 3, 5, 7, ...$$

(et 1 non seulement se retrouvera à la position $\omega + 1$ où ω désigne le nombre d'éléments d'un ensemble infini dénombrable, en l'occurence l'ensemble des nombres pairs, en bijection avec $\mathbb{N}$, mais de surcroît, 1 n'aura pas de prédécesseur ; cela semble vertigineux et l'on se demande dans quelle mesure on

[10] Cohen a démontré l'indécidabilité de cette hypothèse.

peut s'acclimater à ces sortes d'ordres tant ils ne nous sont pas "naturels"). Dans [5], N. Charraud nous explique que Cantor, grâce à ses ordres, peut faire des rapprochements inattendus et démontre que divers objets peuvent se trouver comparables. Pour illustrer ses types d'ordre, il montre même comment associer un type d'ordre à une peinture ou à une symphonie. Il se place ainsi en précurseur de la numérisation de l'information qui envahit tous les champs de connaissance actuellement.

N. Charraud signale également le souci du style de présentation des résultats et de la transmission qui motive Cantor. Il insiste en effet sur "l'effort de présenter le cheminement de pensée aussi clairement que possible" et admire particulièrement les exposés d'Hermite pour leur limpidité : "Le style personnel de Cantor va avec le souci de communiquer de la façon la plus transparente possible le processus et les étapes de sa découverte".

Ce souci de limpidité se retrouve chez Hilbert, dans un extrait de sa conférence de 1900 : "On peut néammoins se demander s'il n'existe pas des attributs généraux caractérisant un bon problème de mathématiques. Un mathématicien français des temps passés a dit : "une théorie mathématique ne doit être regardée comme parfaite que si elle a été rendue tellement claire qu'on puisse la faire comprendre au premier individu rencontré dans la rue". Cette clarté, cette limpidité si énergiquement exigée ici d'une théorie mathématique, je l'exigerai encore davantage d'un problème mathématique parfait ; ce qui est clair et limpide nous attire en effet, ce qui est embrouillé nous rebute".

Il y a un an quand j'ai lu la biographie de Cantor par J.P.Belna [14], j'ai essayé d'utiliser la notion de bijection entre ensembles pour accéder à la conjecture de Goldbach ; j'étais partie de la façon suivante : l'ensemble des nombres pairs ayant l'une de leurs décompositions Goldbach faisant intervenir 3 est infini dénombrable (3+3=6, 3+5=8, 3+7=10, 3+11=14,...). De même, l'ensemble des nombres pairs faisant intervenir 5 dans l'une des décompositions Goldbach est également infini dénombrable : 5+5=10, 5+7=12, 5+11=16,...). Et de même pour chacun des ensembles de nombres pairs engendrables par chacun des nombres premiers qui sont en nombre infini. Si on fait l'union de tous ces ensembles infinis dénombrables, on obtient un ensemble infini dénombrable, qu'on peut mettre en bijection avec $\mathbb{N}$, l'ensemble des entiers naturels. Les intersections de ces ensembles sont parfois non vides : 3+7=5+5, par exemple. D'autre part, l'ensemble des nombres pairs est aussi en bijection avec l'ensemble des entiers naturels. Pour autant, cela ne me permettait pas d'assurer que l'on ne "ratait" aucun entier.

5 Un ordre inhabituel sur les entiers

Selon Hermann Weyl, il revient à chaque utilisateur de créer son propre ensemble de nombres selon la réalité qu'il souhaite modéliser. Une excellente présentation de la façon dont l'homme a "construit les différentes sortes de nombres" est à trouver dans l'ouvrage de Claude-Paul Bruter [1].

En ce qui concerne une justification éventuelle de la conjecture de Goldbach, citons un extrait de [3] : "l'ordre à partir du chaos n'est pas toujours arrivé à si bon compte. Suivant une conjecture non encore prouvée (1984) de Goldbach

(1690 - 1764), tout nombre pair est la somme de deux nombres premiers. Par exemple, $24 = 5 + 19$. Ceci peut se produire de plusieurs manières différentes : $24 = 7 + 17 = 11 + 13$. La liste suivante obtenue par ordinateur[11] donne la décomposition de nombres pairs en somme de deux nombres premiers, où le premier terme est le plus petit possible (et le second, le plus grand possible). Le chaos est clair. Mais quel est l'ordre sous-jacent ? La démonstration de la conjecture de Goldbach, si jamais elle arrive, peut apporter de l'ordre dans ce chaos".

Reprenons ici les mots de l'article d'Euler "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs" : Les mathématiciens ont tâché jusqu'ici en vain à découvrir quelque ordre dans la progression des nombres premiers, et on a lieu de croire que c'est un mystère auquel l'esprit humain ne sauroit jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers, que quelques-uns se sont donnés la peine de continuer au-delà de cent mille et on s'apercevra qu'il n'y règne aucun ordre ni règle".

Si l'on observe finement la liste de décompositions fournie par Davis et Hersh[12], on constate une coïncidence troublante qui fait penser à un "motif" de nombres premiers qui se répètent (en l'occurrence 3, 5, 3, 5, 7, 13, 11, 13, 19, 17, 19, 3) et qui sont décomposants Goldbach des nombres 20902 et suivants et des nombres 20962 et suivants (je les ai positionnés en regard les uns des autres en annexe 1). Les tables de nombres premiers nous ont habitués à une présentation si chaotique, "sans schéma discernable de régularité" qu'on a beaucoup de mal à penser que la répétition d'un tel "motif" soit absolument accidentelle. On va imaginer comment un nouvel ordre sur les entiers pourrait expliquer cette coïncidence.

Choisissons comme "bon ordre" l'ordre lexicographique sur les représentations par les restes. Selon cet ordre, tous les entiers pairs sont plus petits que 1 puisque le n-uplet représentant chacun d'eux a 0 comme première coordonnée alors que celui de 1 a 1 comme première coordonnée. Mais ce qui est troublant, c'est que 6 est plus petit que 2 car 2 est congru à 2 (modulo 3) alors que 6 est congru à 0 (modulo 3). On définit la relation d'ordre suivant :

$$
\begin{array}{ll}
 & a < b \\
\iff & \textit{la représentation par restes de a est un préfixe de la représentation par restes de b} \\
 & (\textit{i.e. il y a partage de toutes les coordonnées communes}).
\end{array}
$$

Pour chercher des décomposants Goldbach partagés, on s'intéressera dans un premier temps aux préfixes les plus longs possibles, c'est à dire dont la représentation par les restes a seulement une lettre en moins que celle du mot auquel on s'intéresse.

[11] Je reproduis cette liste en annexe 1.

[12] voir annexe 1.

Ci-dessous, fournissons les représentations par restes des nombres de 6 à 100.

$6 : (0)$	$54 : (0, 0, 4, 5)$
$8 : (0)$	$56 : (0, 2, 1, 0)$
$10 : (0, 1)$	$58 : (0, 1, 3, 2)$
$12 : (0, 0)$	$60 : (0, 0, 0, 4)$
$14 : (0, 2)$	$62 : (0, 2, 2, 6)$
$16 : (0, 1)$	$64 : (0, 1, 4, 1)$
$18 : (0, 0)$	$66 : (0, 0, 1, 3)$
$20 : (0, 2)$	$68 : (0, 2, 3, 5)$
$22 : (0, 1)$	$70 : (0, 1, 0, 0)$
$24 : (0, 0)$	$72 : (0, 0, 2, 2)$
$26 : (0, 2, 1)$	$74 : (0, 2, 4, 4)$
$28 : (0, 1, 3)$	$76 : (0, 1, 1, 6)$
$30 : (0, 0, 0)$	$78 : (0, 0, 3, 1)$
$32 : (0, 2, 2)$	$80 : (0, 2, 0, 3)$
$34 : (0, 1, 4)$	$82 : (0, 1, 2, 5)$
$36 : (0, 0, 1)$	$84 : (0, 0, 4, 0)$
$38 : (0, 2, 3)$	$86 : (0, 2, 1, 2)$
$40 : (0, 1, 0)$	$88 : (0, 1, 3, 4)$
$42 : (0, 0, 2)$	$90 : (0, 0, 0, 6)$
$44 : (0, 2, 4)$	$92 : (0, 2, 2, 1)$
$46 : (0, 1, 1)$	$94 : (0, 1, 4, 3)$
$48 : (0, 0, 3)$	$96 : (0, 0, 1, 5)$
$50 : (0, 2, 0, 1)$	$98 : (0, 2, 3, 0)$
$52 : (0, 1, 2, 3)$	$100 : (0, 1, 0, 2)$

Voyons les relations d'ordre entre les nombres maintenant :
10, 12, 14, 16, 18, 20, 22 et 24 ont tous pour préfixes 6 ou 8 et ils partagent tous un décomposant Goldbach avec au moins l'un des deux.
26, 32, 38 et 44 ont pour préfixes 14 ou 20 et le partage d'au moins un décomposant Goldbach a systématiquement lieu.
28, 34, 40 et 46 ont pour préfixes 10, 16 ou 22 et on parvient à la même conclusion au niveau des partages de décomposants.
On va dans la section suivante essayer d'expliquer du mieux possible ce partage des décomposants.

6 Partage des décomposants Goldbach

Dans une note précédente, on a constaté que tout nombre inférieur à x et dont les restes de divisions euclidiennes par les nombres de 2 à x sont différents un à un des restes de $2x$ par ces mêmes divisions a son complémentaire à $2x$ qui est premier. Ecrivons cela en utilisant une notation en langage mathématique :

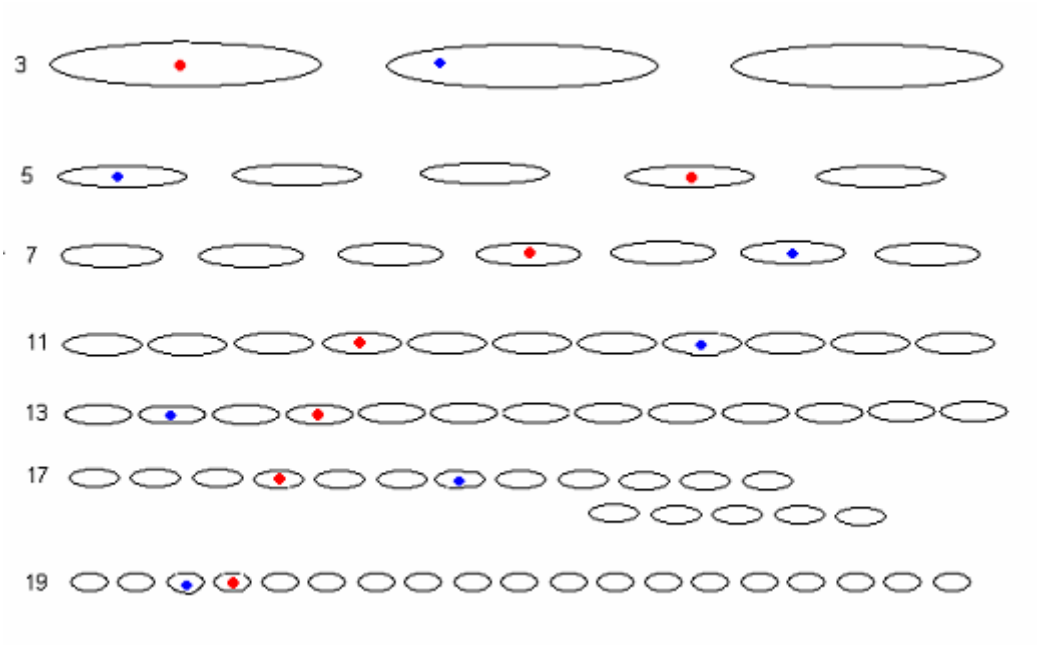
$\forall\ 2x$
$\forall\ p_1$ *premier impair inférieur ou égal à* x
$\forall\ q$ *premier impair inférieur ou égal à* x,
$2x \not\equiv p_1\ (mod\ q) \iff p_2 = 2x - p_1$ *premier impair supérieur ou égal à* x
$(2x = p_1 + p_2$ *est appelée une décomposition Goldbach de* $2x)$.

En effet,

$$
\begin{aligned}
& 2x \not\equiv p_1 \ (mod\ q) \\
\iff\ & 2x - p_1 \not\equiv 0 \ (mod\ q) \\
\iff\ & 2x - p_1 \textit{ est un nombre premier car il n'est divisible par aucun autre nombre premier } q
\end{aligned}
$$

On fournissait l'exemple du nombre pair 40 : les nombres impairs inférieurs à 20 qui sont incongrus à 40 selon tout nombre premier inférieur à 20 sont les nombres 3, 9, 11 et 17. Tous ces nombres ont leur complémentaire à 40 qui est premier. On constate que l'ensemble des nombres qui ont leur complémentaire à $2x$ qui est premier peut à la fois contenir des nombres premiers et des nombres composés.

L'énoncé présenté ci-dessus est vrai. Cependant, il pourrait être vrai par vacuité, c'est à dire vrai alors qu'il n'existerait aucun p_1 le vérifiant. Démontrer la conjecture de Goldbach consiste à démontrer que cet énoncé ne peut jamais être vrai par vacuité.
Représentons cela dans la théorie des ensembles. Ci-dessous sont dessinés les résidus possibles selon chaque nombre premier inférieur à 20 (3 classes de congruence modulo 3, 5 classes de congruence modulo 5, etc). Par convention, on dessine la classe 0 à l'extrême-gauche du dessin. Les points bleus représentent l'appartenance de 40. 3 permet de trouver une décomposition Goldbach de 40 car 3 n'est jamais dans le même ensemble de congruence que 40. Démontrer la conjecture de Goldbach consiste donc à démontrer qu'il existe toujours un nombre premier qui ne partage aucune classe de congruence avec 2x. Les nombres impairs inférieurs à 20 qui ne partagent aucune classe de congruence avec 40 ont leur complémentaire à 40 qui est premier (ce sont ici 3, 9, 11 et 17).



Un professeur a insisté sur le fait qu'il fallait que j'adopte une méthode constructiviste. J'ai donc essayé de trouver comment un nombre pair pourrait

"hériter" ses décomposants Goldbach d'autres nombres pairs plus petits que lui (et d'ailleurs, du coup, les transmettre à des nombres pairs plus grands que lui).

7 Descente infinie de Fermat

Quand cet été, j'ai décidé de me "fixer" définitivement sur la numération par restes pour étudier le partage des décomposants Goldbach[13], j'étais persuadée qu'il fallait suivre la recommandation de Poincaré et essayer d'établir une démonstration par récurrence. Mais le problème est que rien ne lie les décompositions Goldbach de deux entiers successifs car les décomposants devant être incongrus selon tous les modules inférieurs à x au nombre pair $2x$ considéré, tout distingue deux entiers successifs représentés par leurs restes modulaires puisqu'ils n'ont aucun reste en commun ; le mode de raisonnement par récurrence semblait donc très mal adapté. Le fait de choisir plutôt comme ordre l'ordre lexicographique des représentations par restes des entiers fait que l'on ne se place plus dans l'axiomatique de Peano. Je crois qu'associé à l'idée de nouvel ordre sur les entiers, le raisonnement appelé "descente infinie de Fermat" est plus adapté à la conjecture de Goldbach.

On trouve par exemple dans [4] une présentation de ce mode de raisonnement ; il repose sur le fait qu'il n'existe pas de suite infinie strictement décroissante d'entiers positifs.

L'ensemble $\mathbb{N}$ des entiers naturels et toutes ses parties propres non vides possèdent une propriété remarquable : ils admettent un plus petit élément.
Imaginons que nous voulions démontrer qu'une certaine propriété $P(n)$ est impossible (n est un entier naturel). On raisonne par l'absurde en supposant $P(n)$ vraie pour un certain entier n (la partie E de $\mathbb{N}$ où $P(n)$ est vraie est donc non vide). Si nous sommes capables de montrer que P est alors vraie pour un entier strictement inférieur à n, nous aboutirons à une contradiction. En effet, si a désigne le plus petit élément de E, on a simultanément $P(a)$ vraie et $P(b)$ vraie avec $b < a$. L'entier b appartient donc à E et est strictement plus petit que le plus petit élément de E. D'où la contradiction.

Puisqu'il semble qu'un entier "partage" toujours ses décomposants avec des nombres entiers plus petits que lui au sens du nouvel ordre que nous avons défini sur les entiers, si un nombre pair ne vérifiait pas Goldbach, il y aurait un nombre entier plus petit que lui (au moins) qui ne la vérifierait pas non plus mais cela est impossible puisqu'il n'existe pas de suite strictement décroissante infinie d'entiers naturels. Donc la conjecture de Goldbach doit être vraie.

8 Les chemins empruntés, les souvenirs engrangés

Depuis deux ans, j'ai emprunté de multiples chemins, pour essayer de comprendre la conjecture de Goldbach. Au début, je l'ai lue autrement : "tout nombre entier supérieur ou égal à 2 est moyenne de deux nombres premiers (ou bien est à égale distance de deux premiers)". Peu après, j'en ai trouvé une

[13] J'avais écrit une note à Noël 2006 qui s'appelait "propriétés de symétrie d'une table de congruence" et qui utilisait déjà cette représentation.

représentation géométrique dont j'espérais qu'elle serait fructueuse. Après cela, je me suis intéressée aux séquences de valuations p-adiques, qui sont autant de séquences fractales d'entiers. En additionnant les exposants intervenant dans les factorisations des entiers successifs, j'obtenais une séquence fractale d'entiers dont les $log(n)$ premiers éléments ayant 1 pour image étaient d'indices premiers. En représentant graphiquement les empilements de valuations p-adiques, je suis "tombée" sur une courbe logarithmique (que je me suis outrancièrement expliquée par le TNP d'Hadamard et La Vallée-Poussin). J'ai découvert une note de Laisant dans le Bulletin de la SMF (tome 25 de l'année 1897) avec qui je partageais une vision, selon laquelle les nombres premiers effectuaient une sorte de danse de salon les uns en face des autres (pour Laisant, c'était des tirettes que l'on faisait coïncider [21]). Puis j'ai fait un détour par la théorie des graphes, toujours sans aucun succès. Alors, lors de l'été 2006, j'ai découvert les groupes et Galois, sous prétexte que l'on pouvait associer certaines décompositions Goldbach aux sommets de polyèdres imaginaires. Enfin, aux environs de Noël 2006, j'ai cru en avoir terminé car j'avais alors trouvé que la conjecture de Goldbach peut être reformulée de la façon suivante : quelque soit $2x$ un nombre pair, il existe une suite décroissante de $x-1$ entiers successifs et inférieurs strictement à $2x-1$ qui ne sont pas divisibles un à un par les éléments de la suite croissante des nombres entiers de 2 à x mais cela restait à établir. Je trouvais qu'il suffisait (sic) d'associer à tout entier un certain nombre de fractions rationnelles dont il s'agissait de tester le caractère entier ou non...
Pendant tout ce temps, je me suis servie de l'informatique pour vérifier mes idées (autant que faire se peut dans la mesure où l'infini informatique est une poussière devant l'infini mathématique) ; j'adoptais une démarche expérimentale, par essais et erreurs. Le programme le plus intéressant intellectuellement a été celui du calcul de la somme des diviseurs des entiers, par un algorithme récursif inventé par Euler et qui est en relation avec son théorème pentagonal. L'article *"Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs"* [10] décrit cet algorithme et est très impressionnant. L'émerveillement du mathématicien devant la "magie" des nombres s'en dégage de façon intemporelle. On programme donc récursivement le calcul de la somme des diviseurs mais la formule reste hermétiquement incompréhensible[14]. Tout au long de ce travail, j'ai échangé souvent avec quelques professeurs qui ont été bienveillants à mon égard et je les en remercie.

9 Conclusion

Citons Henri Cohen : "à la différence de l'hypothèse de Riemann, la conjecture de Goldbach n'a pas d'intérêt en soi, outre le pur défi qu'elle pose". La légende court selon laquelle Gauss aurait dit à propos de la conjecture de Goldbach ou d'une conjecture similaire qu'il pouvait en écrire de nombreuses du même genre et que cela ne présentait pas d'intérêt de résoudre de tels problèmes. Gauss a entre autres inventé le langage des congruences, a conjecturé le TNP, a prouvé le théorème fondamental de l'algèbre, a démontré de multiples façons la loi de réciprocité quadratique. Quant à Cantor, on sait qu'il s'est intéressé à la

[14]Il y a peut-être une formule récursive semblable qui lie entre elles les décompositions Goldbach de certains entiers ou les nombres de telles décompositions.

conjecture de Goldbach et on peut se demander si c'est elle qui l'a amené à définir ses types d'ordre[15]. Le travail présenté ici illustre en quelque sorte une fable dont le titre pourrait être "les géants et la fourmi" ou bien "les théoriciens et l'ingénieur" au sens où je n'ai fait qu'essayer d'utiliser les outils théoriques qu'ils avaient élaborés pour résoudre ce problème que je me suis approprié.
Je ne sais pas si les idées qui ont été présentées pourraient servir à mener à bien une démonstration de la conjecture de Goldbach. Ma promenade promet d'être encore longue et pour la première fois depuis deux ans, j'ai l'impression d'avoir enfin emprunté le bon chemin. J'aime beaucoup le titre d'un livre de Hawking qui est "Sur les épaules des géants". Par la lecture de tous ces ouvrages de vulgarisation, j'ai le sentiment d'avoir quelque peu cotoyé ces personnes éminemment intéressantes qu'ont été Cantor, Hilbert, Gauss, Galois et même si je n'aboutis pas, les avoir "rencontrées" aura été un enrichissement humain[16].
Pour terminer, je citerai une anecdote : un jour, un enfant me proposa de me "montrer l'infini"... Il sortit un miroir de poche et le plaça face à un miroir accroché au mur. La suite de miroirs de plus en plus petits semblait ne jamais s'arrêter et l'enfant était émerveillé. Je continue de partager son sentiment après deux ans de promenade autour de la conjecture de Goldbach.

Bibliographie

(1) C.P. Bruter, *La construction des nombres*, Ed. Ellipses, 2000.
(2) T. Brugère et A. Mollard, *Mathématiques à l'usage des informaticiens*, Ed. Ellipses, 2003.
(3) P.J. Davis, R.Hersh, *l'Univers mathématique*, Ed. Gauthier-Villars, 1985
(4) *L'infini (le fini, le discret et le continu)*, Hors série n° 13, Ed. Bibliothèque Tangente, 2006.
(5) N. Charraud, *Infini et Inconscient, essai sur Georg Cantor*, Ed. Anthropos, 1994.
(6) D. Guedj, *Villa des hommes*, Ed. Robert Laffont, 2007
(7) D. Nordon, M.Mendès-France (illustrations), *Les mathématiques pures n'existent pas !*, Ed. Actes Sud, 1985.
(8) D. Nordon, *Les obstinations d'un mathématicien*, Ed. Belin Pour La Science, 2003.
(9) A. Doxiadis, *Oncle Pétros et la conjecture de Goldbach*, Ed. Points, 2002.
(10) L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Commentatio 175 indicis Enestroemiani, Bibliothèque impartiale 3, 1751, p.10-31.
(11) P. Damphousse, *Découvrir l'arithmétique*, Ed. Ellipses, 2000.
(12) A. Astruc, *Evariste Galois*, Ed. Grandes biographies, 1999.
(13) M. Du Sautoy, *La symphonie des nombres premiers*, Ed. Eloïse d'Ormesson, 2005.
(14) J.P. Belna, *Cantor*, Ed. Les belles lettres, 2000.
(15) J.P. Delahaye, *Merveilleux nombres premiers*, Ed. Belin Pour La Science,

[15] Je suis née en 1965 et tout mon apprentissage des mathématiques en école élémentaire s'est fait par les ensembles d'une part et par la représentation des nombres dans des systèmes de numération multi-bases d'autre part, ce que l'on a appelé les "mathématiques modernes".

[16] En annexe 3, sont présentées très succinctement d'autres références trouvées çà et là qui pourraient être mises à profit pour comprendre la conjecture de Goldbach.

2000.
(16) P. Hoffman, *Erdös, l'homme qui n'aimait que les nombres*, Ed. Belin, 2000.
(17) J. Hadamard, *Essai sur la psychologie de l'invention dans le domaine mathématique*, suivi de H. Poincaré, *L'invention mathématique*, Ed. Jacques Gabay, 2000.
(18) J.J.Gray, *Le défi de Hilbert*, Ed. Dunod, 2003.
(19) Collectif, Ebbinghaus et autres auteurs, *Les Nombres*, Ed. Vuibert, 1999.
(20) S. Hawking, *Et Dieu créa les nombres*, Ed. Dunod, 2006.
(21) C. Laisant, *Sur un procédé expérimental de vérification de la conjecture de Goldbach*, Bulletin de la SMF n°25 de 1897.
(22) S. Baruk, *L'âge du capitaine*, Ed. Seuil, 1998.
(23) G. Tenenbaum, M. Mendès-France, *Les nombres premiers*, Collection Que sais-je ?, PUF, 2000
(24) C.F. Gauss, *Recherches arithmétiques*, Ed. Jacques Gabay, 1801.

Enfin, toutes les notes de recherches et une bibliographie détaillée se trouve sur un site personnel à l'adresse http://denise.vella.chemla.free.fr.

Annexe 1 : la conjecture de Goldbach présentée dans le livre de Davis et Hersh

$20882 = 3 + 20879$ $20942 = 3 + 20939$
$20884 = 5 + 20879$ $20944 = 5 + 20939$
$20886 = 7 + 20879$ $20946 = 7 + 20939$
$20888 = 31 + 20857$ $20948 = 19 + 20929$
$20890 = 3 + 20887$ $20950 = 3 + 20947$
$20892 = 5 + 20887$ $20952 = 5 + 20947$
$20894 = 7 + 20887$ $20954 = 7 + 20947$
$20896 = 17 + 20879$ $20956 = 17 + 20939$
$20898 = 11 + 20887$ $20958 = 11 + 20947$
$20900 = 3 + 20897$ $20960 = 13 + 20947$
$20902 = 3 + 20899$ $20962 = 3 + 20959$
$20904 = 5 + 20899$ $20964 = 5 + 20959$
$20906 = 3 + 20903$ $20966 = 3 + 20963$
$20908 = 5 + 20903$ $20968 = 5 + 20963$
$20910 = 7 + 20903$ $20970 = 7 + 20963$
$20912 = 13 + 20899$ $20972 = 13 + 20959$
$20914 = 11 + 20903$ $20974 = 11 + 20963$
$20916 = 13 + 20903$ $20976 = 13 + 20963$
$20918 = 19 + 20899$ $20978 = 19 + 20959$
$20920 = 17 + 20903$ $20980 = 17 + 20963$
$20922 = 19 + 20903$ $20982 = 19 + 20963$
$20924 = 3 + 20921$ $20984 = 3 + 20981$
$20926 = 5 + 20921$ $20986 = 3 + 20983$
$20928 = 7 + 20921$ $20988 = 5 + 20983$
$20930 = 31 + 20899$ $20990 = 7 + 20983$
$20932 = 3 + 20929$ $20992 = 11 + 20981$
$20934 = 5 + 20929$ $20994 = 11 + 20983$
$20936 = 7 + 20929$ $20996 = 13 + 20983$
$20938 = 17 + 20921$ $20998 = 17 + 20981$
$20940 = 11 + 20929$ $21000 = 17 + 20983$

Annexe 2 : le théorème chinois pour l'informaticien Prather selon Davis et Hersh

Avant d'analyser la présentation du théorème chinois des restes par Prather l'informaticien, Davis et Hersh jugent la présentation de ce théorème par Shockley (dans son Introduction à la théorie des nombres de 1967). Ils expliquent : "la présentation de Shockley peut être appelée une version à la mode de ce qui figure dans les Disquisitiones Arithmeticae de Gauss (1801). La notation Gaussienne pour les congruences est pleinement établie et se prête à un degré d'élégance inconnu jusqu'alors [...] Cette formulation peut être considérée comme un sommet dans le cadre de la théorie des nombres algébrisée de manière classique.

La différence de ton entre les formulations de Prather et Shockley est intense. Nous avons chez Prather une réécriture complète du théorème sous l'influence de la conception structuraliste des mathématiques. L'ensemble fini des entiers naturels $0, 1, 2, ..., n-1$ considéré muni de l'addition modulo n (c'est à dire

négligeant les multiples de n) constitue ce qu'on appelle un groupe cyclique additif, noté Z_n. Le produit de deux tels groupes, $Z_4 \times Z_3$ par exemple, consiste en couples (a, b) d'entiers où le premier est un élément de Z_4 et le second un élément de Z_3. Ainsi, les éléments de $Z_4 \times Z_3$ sont les douze couples :

$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$

L'addition des éléments de $Z_4 \times Z_3$ est définie comme l'addition des entiers correspondants, la première étant effectuée modulo 4 et la seconde modulo 3. Ainsi, par exemple :

$$(2,2) + (3,2) \ = \ ((2+3) \ mod \ 4, \ (2+2) \ mod \ 3) \ = \ (1,1)$$

Chaque couple (a, b) peut être identifié avec l'unique nombre parmi $0, 1, ..., 11$ dont la division par 4 fournit a et dont la division par 3 fournit b. Avec cette identification, la table ci-dessus devient :

0	9	6	3
4	1	10	7
8	5	2	11

Ainsi, $(1, 1) = (2, 2) + (3, 2)$ se traduit par $1 = (2 + 11) \ mod \ 12$, ce qui est un exemple particulier de l'isomorphisme des deux tables suivant leurs définitions individuelles de $+$. La présente formulation du théorème chinois affirme que ce schéma est vrai dans le cas général de l'entier n, pourvu que nous décomposions n en ses facteurs premiers. Notons que cette formulation du théorème chinois nous donne à la fois plus et moins que la formulation précédente (par Shockley). Elle met l'accent sur la structure au détriment de l'algorithme. Elle fournit une analyse complète de l'addition modulaire dans Z_n, en termes d'additions plus simples dans (Z_{q_i}). Elle court-circuite la question de savoir comment établir l'identification de Z_n et de $Z_{q_1} \times ... \times Z_{q_r}$ (quoique cette identification intervienne au coeur de la démonstration) et elle ignore totalement la question, historiquement motivante, de savoir comment, les restes étant donnés, nous pouvons promptement calculer le nombre qui engendre ces restes. En un sens, il est très étrange de voir dans le commentaire de Prather à la fin de son exposé que le théorème chinois s'est montré utile dans la conception d'unités arithmétiques rapides pour les ordinateurs. On penserait que ceci appelle la connaissance d'un algorithme concret. Mais il est vrai que l'informatique dans sa formulation théorique est dominée par un esprit d'abstraction qui n'a rien à envier aux autres branches des mathématiques dans son fanatisme."

Annexe 3 : d'autres manières d'aborder la conjecture de Goldbach d'une grande complexité

Un extrait du livre collectif "les Nombres" aux éditions Vuibert [19], page 404, provenant de la section concernant les preuves d'indépendance logique :
"On peut mentionner la conjecture de Goldbach. Plus généralement, on peut penser à tout énoncé portant sur les nombres naturels et comprenant un ensemble fini de quantificateurs universels suivi d'un noyau sans quantificateur, ce qui

est par exemple le cas de toute équation diophantienne ou de sa négation. Tant qu'un tel problème n'est pas résolu, on peut se demander s'il est indépendant de ZFC[17]. Pour ce type de problème, un résultat d'indépendance a une signification très différente de ceux concernant l'hypothèse du continu ou l'hypothèse de Suslin : une preuve de son indépendance implique automatiquement sa vérité. Si par exemple, l'hypothèse de Riemann était fausse, il devrait y avoir un contre-exemple dont la validité pourrait être vérifiée, sur la base de ZFC. Ainsi, l'indépendance ne pourrait survenir que si la conjecture était vraie. Pour démontrer que Goldbach est vraie, il faudrait démontrer qu'elle n'est pas réfutable selon ZFC."

Un extrait du livre "le défi de Hilbert" de J.J.Gray [18]: Un autre problème, également mentionné par Hilbert, qui peut se ramener à une équation diophantienne, est la conjecture de Goldbach. Elle en devient l'affirmation qu'une certaine équation diophantienne n'a pas de solution. Si le dixième problème de Hilbert avait admis une réponse positive, la conjecture de Goldbach aurait été réfutée - une connexion que Hilbert n'avait certainement pas soupçonnée. Davis, Mattiassevitch et Robinson montrèrent que même l'hypothèse de Riemann peut être reformulée comme une question Diophantienne (ce qui ne la rend pas plus facile pour autant). Julia Robinson disait ceci à propos du dixième problème de Hilbert : "Je souhaitais toujours à chacun de mes anniversaires et d'année en année que le dixième problème de Hilbert soit résolu. Pas par moi, mais simplement qu'il soit résolu. J'avais le sentiment que je ne pourrais accepter de mourir sans connaître la réponse". On raconte d'autre part qu'Hadamard et la Vallée-Poussin qui ont prouvé indépendamment le TNP sont morts très âgés. Allez, je l'avoue, toutes ces recherches n'ont qu'un but : augmenter, autant que faire se peut, ma longévité !

Enfin, un extrait des oeuvres mathématiques d'Evariste Galois trouvées sur Gallica p.405 : "le principal avantage de la nouvelle théorie [18] que nous venons d'exposer est de ramener les congruences à la propriété (si utile dans les équations ordinaires) d'admettre précisément autant de racines qu'il y a d'unités dans l'ordre de leur degré. La méthode pour avoir toutes ces racines sera très simple. Premièrement, on pourra toujours préparer la congruence donnée $Fx = 0$, et le moyen de le faire est évidemment le même que pour les équations ordinaires. Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$. Si maintenant on veut avoir les solutions imaginaires du second degré, on cherchera le plus grand facteur commun à $Fx = 0$ et à $x^{p^\nu - 1} = 1$. C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux, comme je vais essayer d'en donner en deux mots une idée [...] Ainsi, pour chaque nombre de la forme p^ν, on pourra former un groupe de permutations tel que toute fonction des racines invariable par ces permutations devra admettre une valeur rationnelle quand l'équation de degré p^ν sera

[17] mis pour axiomatique de Zermelo-Fraenkel avec l'axiome du choix.

[18] consistant à associer à une équation ce que l'on appelle son groupe de Galois.

primitive et soluble par radicaux"[19].

Pour finir, je voudrais reproduire dans cette annexe un extrait d'une superbe biographie de Galois par Alexandre Astruc, publiée aux éditions Flammarion en 1994 car je crois que l'on gagnerait à faire circuler de telles phrases.

Astruc écrit que "communiquer ses découvertes, être reconnu par ses pairs, telles sont les idées fixes de tout savant, et Galois ne fait pas exception à cette règle". Un peu plus loin, il cite intégralement la préface de Galois à ses "deux mémoires d'analyse pure". La fin de cette préface préfigure le partage actuel de la connaissance via internet notamment et cette notion de partage m'est chère.

"On doit prévoir que, traitant des sujets aussi nouveaux, hasardé dans une voie aussi insolite, bien souvent des difficultés se sont présentées que je n'ai su vaincre. Aussi, dans ces deux mémoires et surtout dans le second qui est plus récent, trouvera-t-on souvent la formule : "Je ne sais pas." La classe des lecteurs dont j'ai parlé au commencement[20] ne manquera pas d'y trouver à rire. C'est que malheureusement on ne se doute pas que le livre le plus précieux du plus savant serait celui où il dirait tout ce qu'il ne sait pas, c'est qu'on ne se doute pas qu'un auteur ne nuit jamais tant à ses lecteurs que quand il dissimule une difficulté. Quand la concurrence, c'est à dire l'égoïsme, ne règnera plus dans les sciences, quand on s'associera pour étudier, au lieu d'envoyer aux Académies des paquets cachetés, on s'empressera de publier les moindres observations pour peu qu'elles soient nouvelles, et on ajoutera : "Je ne sais pas le reste.""

[19] J'aimerais vraiment qu'un professeur m'explique dans quelle mesure ces quelques lignes ne suffisent pas, à elles seules, à prouver la conjecture de Goldbach, dans la mesure où il y est question de solutions entières et de congruences et que la conjecture est formulable en ces termes.

[20] Ici, Galois veut parler des mathématiciens qui ont dénigré son travail à l'époque.