LES NOMBRES ENTIERS : DES AMIS QUI NOUS POSENT DES PROBLEMES[1]

Par M. Jean-Baptiste Hiriart-Urruty[2]

Résumé. A l'aide de quelques exemples bien choisis, nous illustrons les problèmes d'énoncé simple mais difficiles à résoudre que posent les nombres entiers. En plus de cela, nous expliquons deux avancées majeures sur les nombres premiers qui ont été effectuées par des mathématiciens professionnels en 2013.

Abstract. With the help of some examples, we illustrate the problems, easy to state but difficult to solve, that integers can pose. Moreover, we explain two major advances on prime numbers made by professional mathematicians during the 2013 year.

Resumen. Con la ayuda de unos pocos ejemplos bien elegidos, ilustramos problemas faciles de enunciar pero difíciles de resolver relativos a los números enteros. Además, discutimos dos importantes avances acerca de los números primos obtenidos por los matemáticos profesionales en 2013.

Introduction. Les nombres *entiers naturels*, ou les entiers naturels, ou simplement les entiers, sont les plus simples des nombres : 1, 2, 3, ... En anglais, on les dénomme *integers*, faisant écho à la même racine latine ; ne dit-on pas un homme entier ou un homme intègre (même si ça n'est pas tout à fait la même chose) ? Si on « casse » ces nombres en petits morceaux, on obtient 1/2, 1/4, 2/5, ... c'est-à-dire des *fractions*, d'où l'explication de cette appellation. Les nombres ainsi obtenus par cassures sont appelés *rationnels*. Le calcul mathématique ne s'en contente pas puisqu'il a fallu aller considérer des nombres tels que $\sqrt{2}$, appelés *irrationnels*, littéralement : « qui échappent à la raison ». Mais, nous allons en rester aux nombres entiers naturels, de bons amis mais qui nous posent bien des problèmes. Voici deux citations de mathématiciens célèbres :

---

[1] Communication a l'Académie des Sciences, Inscriptions et Belles-Lettres de Toulouse le 12 juin 2014.

[2] Institut de mathématiques
Universite Paul Sabatier de Toulouse
E-mail : jbhu@math.univ-toulouse.fr
www.math.univ-toulouse.fr/ ~jbhu/

- *« Dieu a créé les nombres entiers, l'homme a fait le reste»*,

Leopold Kronecker (1823-1891).

- *« Si les nombres ne sont pas beaux, alors j'ignore ce qui l'est »*

Paul Erdös (1913-1996).

Commençons par des choses simples, les particularités d'un nombre (26 en l'occurrence), puis continuons par les nombres dits premiers, sources d'innombrables problèmes et conjectures.

1. chaque nombre a sa particularité... le cas de 26.

Lors d'une séance de l'Académie des Sciences, Inscriptions et Belles-Lettres de Toulouse à laquelle j'assistais, un confrère (plutôt du monde littéraire) évoquait le nombre entier 26 comme un nombre particulier, utilisé comme symbole par des sectes (les cathares ?) et il mentionnait un résultat dont l'origine remonterait jusqu'à P. Fermat : 26 serait **le seul nombre entier coincé entre un carré** ($25 = 5^2$) **et un cube** ($27 = 3^3$). Ne connaissant pas ce résultat, ou l'ayant oublié, j'étais un peu surpris. J'ai voulu en avoir le cœur net : était-ce bien vrai ? Si oui, comment le démontre-t-on ? Une rapide consultation auprès de mes collègues mathématiciens me conforta dans ma première impression, à savoir que ce n'était ni un résultat très connu ni facile à appréhender au premier abord. Les recueils de particularités des nombres entiers (exemple [1]) ne le mentionnaient pas non plus ; il a fallu attendre le tout récent ouvrage [2] pour qu'il en soit ainsi. Deux collègues de mon université, spécialistes de théorie des nombres, m'apprirent qu'il s'agissait d'un résultat dû à P. Fermat qui, comme à son habitude, l'avait posé comme défi aux anglais, en indiquant que le résultat était vrai mais sans en donner une démonstration... Cette propriété de 26 est tout de même curieuse : imaginez un peigne infini dans lequel vous enlevez toutes les dents sauf celles correspondant à des carrés d'entiers (4, 9, 16, 25, ...), puis un autre peigne infini où vous faites la même chose avec les dents placées en des positions différentes des cubes d'entiers (8, 27, 64, ...) ; vous positionnez ensuite les deux peignes l'un sur l'autre, et le seul cheveu (= l'entier) que vous arrivez à coincer entre deux dents est 26 !

Après enquête, il s'avère : oui, le résultat est vrai ; j'en ai trouvé une démonstration dans le livre référencé en [3], attribuée à P. Fermat. La démonstration en question consiste à faire de l'arithmétique dans l'anneau euclidien (et donc factoriel) $\mathbb{Z}[i\sqrt{2}]$... le fil y conduisant est l'équation $y^2 = x^3 - 2$; le groupe de Mordell & Weil de cette équation est cyclique infini ; il se trouve qu'il y a une infinité de solutions rationnelles à cette équation, mais seulement deux solutions entières $(x, y) = (3, \pm 5)$. On démontre qu'il n'y a pas non plus, parmi les entiers naturels, de solutions à l'équation $y^2 = x^3 + 2$. Ce qui répond à notre interrogation... J'en ai fait une note ([4]), diffusée auprès de mes collègues, dont est extrait le présent compte rendu.

Mais comment Fermat a-t-il « intuité le résultat » (comme on dit en

Midi-Pyrénées) ? En avait-il vraiment une démonstration ? On n'en sait rien... Sa correspondance avec des scientifiques en France et en Europe est truffée de questions et défis du même calibre ; celui concernant ce qui s'appelle « le grand théorème de Fermat »[3] a émergé, mais il y en a bien d'autres.

Généralisons la question : l'écart de 2 entre un carré et un cube d'entiers est-il particulier ? Voici ce qu'on peut dire à propos d'écarts valant 0 ou 1 :

- Il y a une infinité de carrés d'entiers qui valent des cubes d'entiers, un exemple en est $4^3 = 8^2$.
- Il n'y a qu'un seul cas où un carré d'entier et un cube d'entier sont consécutifs (en excluant l'intervention de l'entier 1, bien sùr) : $8 = 2^3$ suivi de $9 = 3^2$.
- Un résultat assez extraordinaire, conjecturé par le mathématicien belge E. Catalan en 1844 et démontré par P. Mihailescu en 2002 seulement, affirme que l'équation en nombres entiers

$$|x^m - y^n| = 1 \qquad (1)$$

n'a que la solution du dessus ; bref, **les seules puissances parfaites consécutives sont 8 et 9** (toujours en excluant l'intervention de l'entier 1).

Chaque entier a ses particularités, la récente compilation [2] en présente une multitude, *ad nauseam*... Des qualificatifs tout aussi savoureux les uns que les autres les accompagnent : (nombre entier) apocalyptique, brésilien, chanceux, fortuné, frugal, idéal, narcissique, obstiné, puissant, sociable, vampire, etc.

L'Arithmétique ou la Théorie des nombres (appellation plus moderne) est la partie des mathématiques qui s'occupe des propriétés des nombres ; elle est très ancienne, autant que sa consœur la Géométrie ; dans ses formes actuelles, elle se conjugue sous différentes rubriques : la théorie algébrique des nombres, la théorie analytique des nombres, la théorie « computationnelle » (on dit aussi algorithmique) des nombres. Il y a des mathématiciens professionnels de ces questions dans toutes les grandes universités ; celle de Bordeaux en a été et reste toujours une place forte, celle de Toulouse à un degré moindre. J'ai gardé un souvenir personnel de quand j'arrivais à l'université de Bordeaux pour mes études dites de troisième cycle et de préparation à l'agrégation de mathématiques. Au détour d'un couloir du bâtiment de mathématiques (toujours en place), une petite affichette accolée à une porte avec un simple

---

[3] L'équation de Fermat $x^n + y^n = z^n$, où la puissance n est un entier ≥ 3 et où les inconnues x, y, z sont des entiers positifs est sans doute la plus célèbre de la Théorie des nombres et a donné du fil à retordre à des générations de mathématiciens. Curieusement, une équation très voisine, $x^n + y^n = z^{n+1}$, elle, ne pose pas de difficultés : à partir de n'importe quels entiers positifs a et b, on en construit des solutions qui sont $x = a(a^n + b^n)$, $y = b(a^n + b^n)$, $z = a^n + b^n$.

adhésif mentionnait «Laboratoire de théorie des nombres»... Un flash traversa alors mon esprit, j'imaginais des éprouvettes dans lesquelles on mélangait des nombres et on faisait des expériences avec... Comme tout étudiant de l'époque, et d'aujourd'hui dans une grande mesure, j'ignorais qu'on pouvait faire de la recherche professionnelle et contemporaine sur les nombres entiers. Plus tard, au début de ma carrière universitaire, j'ai essayé de garder un contact avec ce domaine, qui n'était pas celui de mes recherches personnelles, en consultant les revues et en lisant des comptes rendus, mais j'ai dû abandonner assez vite : suivre l'évolution d'un domaine de recherche requiert une attention continue et demande du temps.

En tout cas, la théorie des nombres se prête bien à l'énoncé de conjectures, facilement compréhensibles même par un non spécialiste, nous en avons évoqué un exemple plus haut avec la conjecture de Catalan. Comment ne pas repenser ici à l'une des plus célèbres, celle du « grand théorème de Fermat ? ». Nous en évoquerons d'autres.

Mais qu'est-ce qu'exactement une conjecture ? Si on ouvre un dictionnaire quelconque à ce mot, voici la définition qu'on trouve : hypothèse formulée sur l'exactitude ou l'inexactitude d'un énoncé dont on ne connaît pas encore la démonstration. En d'autres termes, c'est une « question ouverte » pour laquelle une affirmation a été prononcée : « oui, je pense que cette assertion est vraie », ou, ce qui a la même force logique, « non, je conjecture que cet énoncé est faux ». En mathématiques, comme dans d'autres sciences, les conjectures ont toujours joué un rôle de stimulant. Qu'est-ce qu'une conjecture célèbre ? C'est, me semble t-il, une affirmation qui vérifie les trois propriété suivantes :

- l'énoncé en est simple, compréhensible par le plus grand nombre de mathématiciens, voire de non mathématiciens ;
- avoir résisté (assez) longtemps aux assauts des mathématiciens professionnels ;
- avoir engendré de nouvelles mathématiques à travers les différentes tentatives de résolution.

L'image (de jeux de fêtes foraines ou de casinos) qui me vient à l'esprit est celle de certaines machines à sous, où l'objectif est de faire tomber des pièces de monnaie à partir de présentoirs où elles sont disposées (sous verre), à l'aide de quelques mouvements autorisés (et commandées de l'extérieur de l'appareil). Lorsqu'on voit ça, la première réaction est de se dire : «Je vois comment faire, je vais y arriver...». En conséquence, on joue, on insiste, on s'énerve... et on abandonne. La personne qui vous suit a la même réaction que la vôtre initiale : « Il s'y est mal pris, moi je vois comment faire... » ; à son tour, il joue en essayant autre chose, insiste, et finit par abandonner...

2. Les nombres dits premiers

Certains nombres entiers peuvent être factorisés, d'autres pas, par exemple : 6 peut être factorisé, c'est-à-dire être écrit comme le produit d'autres nombres entiers, $6 = 2 \times 3$; 5 ne peut être factorisé (autrement que de manière triviale, $5 = 1 \times 5$). Les nombres entiers $n > 1$ qui n'ont comme diviseurs que les évidents 1 et n sont appelés **premiers**, les autres sont appelés **composés**. La série des nombres premiers débute donc par : 2, 3, 5, 7, 11..., celle des nombres composés par 4, 6, 8, 9, 10... L'étude des nombres premiers a fasciné des générations et des générations de mathématiciens, professionnels ou amateurs, et ça continue de nos jours. Voici quelques appréciations de contemporains :

- *«En observant les nombres premiers, on éprouve le sentiment d'être en présence d'un des plus inexplicables secrets de la création»*

D. Zagier (1977), mathématicien.

- *«Les amateurs de nombres premiers sont de grands enfants, et la fascination qu'exercent sur eux ces entiers sans facteurs triviaux les a conduits à s'intéresser à une multitude de nombres particuliers dont l'intérêt n'est ni mathématique, ni pratique. Animés par l'amour pur, obsessionnel, voire fétichiste des chiffres et de leurs figures, ils dépensent un temps considérable à imaginer des bizarreries numériques et à lancer des ordinateurs à leur recherche. Ne boudons pas notre plaisir dans cette foire aux nombres... Peut-être découvrira-t-on un jour, parmi ces trésors de pacotille, une méthode, un problème ou un nombre patiemment calculé et soigneusement conservé pour la simple joie d'un collectionneur, qui ouvrira une porte. D'une telle découverte pourrait naître une application inattendue, dans un domaine où personne, aujourd'hui, ne soupçonne que les nombres premiers puissent jouer un rôle, comme cela s'est produit en cryptographie en 1975»*

J.-P. Delahaye ([6, chapitre 9], grand vulgarisateur des mathématiques et de l'informatique.

- *«Je me suis surpris à effleurer des vertiges métaphysiques en dévorant le livre de M. du Sautoy ([7]) sur les nombres premiers»*

Umberto Eco

Même les titres des livres sur le sujet traduisent l'émerveillement ou la perplexité des auteurs, voir par exemple les références [6], [7] et [8].

La première propriété des nombres premiers, connue depuis la Grèce antique au moins (avec Euclide), est qu'*ils sont en nombre infini*.... Ca ne s'arrête jamais : prenez un nombre aussi grand que vous voulez, il y aura toujours un nombre premier plus grand que lui. Oui mais, en a-t-on une écriture explicite ? Comme pour les records, le plus grand nombre premier connu évolue au cours des années ; cela est dû à la puissance de calcul

croissante des ordinateurs et de l'amélioration des tests de primalité (c'est-à-dire des méthodes permettant d'affirmer qu'un nombre est premier ou ne l'est pas). A ce jour (depuis 2013), voici le plus grand nombre premier connu, c'est

$$\mathbf{2^{57\,885\,161}-1} \qquad (2)$$

qui s'écrit avec 17 425 170 chiffres décimaux. Si on écrivait à la suite tous les chiffres de ce développement décimal avec, disons, 2 chiffres par centimètre, l'écriture de ce nombre s'étendrait sur plus de 87 kilomètres ! ([9]). On remarquera que le nombre entier figurant en (2) est de la forme $2^p - 1$, avec p nombre premier ; on les appelle **nombres de** MERSENNE[4] **premiers.** Certes, ils ne sont pas tous premiers, mais presque tous les records de plus grands nombres premiers (en fait, tous les récents) ont été atteints avec ce type de nombres.

Une deuxième chose importante sur les nombres premiers est qu'ils constituent les «briques» de base permettant de factoriser n'importe quel entier ; c'est ce qu'on appelle *le théorème fondamental de l'arithmétique*, connu depuis notre passage au collège. La possibilité ou non de factoriser des nombres entiers les plus grands possibles, et dans un temps acceptable (via des calculs sur ordinateurs), est la base de la science moderne du cryptage et décryptage. La sécurisation de nos cartes de paiement, ainsi que d'autres procédés de cryptage utilisés couramment, se basent sur l'impossibilité, en pratique, de factoriser de très grands nombres. La fiabilité d'une technique de cryptage est sans cesse remise en cause par les progrès de la puissance informatique ([10]). Comme pour les plus grands nombres premiers connus, il existe un site web qui offre une mise à jour des différents records de factorisation des entiers.

La répartition des nombres premiers parmi les entiers naturels a été et est toujours une préoccupation des mathématiciens. Il existe une multitude de résultats et de conjectures à leur sujet. Voici un résultat, facile à expliquer à un élève de lycée : l'écart entre deux nombres premiers consécutifs peut être aussi grand que l'on veut. Prenons les entiers $n! + 1$ et $n! + n + 1$; il y a exactement $n - 1$ entiers entre les deux, et pourtant aucun de ces entiers intermédiaires n'est premier ; en effet[5] :

$$\begin{aligned} n! + 2 &= n \times (n-1)... \times 3 \times 2 \times 1 + 2 \text{ est un multiple de } 2\,; \\ n! + 3 &= n \times (n-1)... \times 3 \times 2 \times 1 + 3 \text{ est un multiple de } 3\,; \\ &\cdots\cdots\cdots\cdots \\ n! + n &= n \times (n-1)... \times 3 \times 2 \times 1 + n \text{ est un multiple de } n. \end{aligned}$$

[4] . Le père MERSENNE a joué un rôle important dans la diffusion des mathématiques au temps de FERMAT ; dans le jargon administratif actuel de la recherche, on l'appellerait un «facilitateur».

[5] . n!, qui se lit «factorielle n» est une écriture ramassée du nombre entier n×(n–1)×(n–2)....×3×2×1.

Parmi les conjectures les plus récentes concernant les écarts entre nombres premiers consécutifs, j'ai une faiblesse particulière pour celle du mathématicien roumain D.Andrica (1986). En voici son énoncé : Si $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, ..., p_n, p_{n+1}$ ... est la suite croissante des nombres premiers, alors

$$\sqrt{p_{n+1}} - \sqrt{p_n} < \mathbf{1}. \qquad (3)$$

Etonnante par la simplicité de son énoncé, cette conjecture a été vérifiée jusqu'au maximum des possibilités (mathématiques et informatiques) actuelles... Il n'en reste pas moins qu'on ne sait pas si cette inégalité est vraie en toute généralité, ou si un contre-exemple (suffisamment grand) existe pour la contredire.

3. Les nombres premiers dits jumeaux

Il y a quelque temps, pas très longtemps à vrai dire, des collègues ont illustré l'affiche annonçant un jubilé en mon honneur par la formule suivante :

$$11 + 13 + 17 + 19 = 60. \qquad (4)$$

Si je voyais la signification de la somme (c'était pour mes 60 ans), je ne percevais pas la signification des nombres 11, 13, 17, 19... et les collègues se gardaient bien de me la donner. Finalement, j'ai percé le mystère : 11 et 13 sont des nombres premiers qui se suivent, de même 17 et 19. «Se suivent» ne signifie pas «se suivent immédiatement» puisqu'après un nombre premier qui est toujours impair (à part le premier d'entre eux, 2) il y a un nombre pair qui, lui, n'est pas premier (puisque divisible par 2). Ces nombres premiers qui se suivent sont qualifiés de *jumeaux* ; bref, il s'agit de nombres premiers dont la différence est 2. Dans notre exemple, 60 est la somme de deux couples de nombres jumeaux, (11, 13) et (17, 19) ; de fait, il est aussi somme de deux autres nombres premiers jumeaux, 29 et 31. La question est : y en a-t-il une infinité ou bien s'arrête-t-on à partir d'un certain moment (au-delà d'un entier assez grand) ? C'est la conjecture sur l'infinitude des nombres premiers jumeaux (*i.e.,* de la forme n et $n + 2$) : **«Il y a une infinité de nombres premiers** n **tels que** $n+2$ **soit aussi premier»**. La question est toujours sans réponse... depuis qu'elle fut formulée, entre autres, par le mathématicien français A.de Polignac en 1849[6]. Les deux plus grands nombres jumeaux connus à ce jour (le record date de décembre 2011) sont :

$$\mathbf{3\,756\,801\,695\,685} \times \mathbf{2}^{\mathbf{666\,669}} \pm \mathbf{1} \; ; \qquad (5)$$

pour leur écriture décimale, ils nécessitent 200 700 chiffres. Les plus récents nombres premiers jumeaux marquant une année furent 1997 et 1999 ; quant

[6] A vrai dire, la conjecture de Polignac est plus générale : Pour tout entier naturel pair 2k, c'est- à-dire 2, 4, 6, ... il existe une infinité de paires de nombres premiers consécutifs dont la différence vaut 2k. Autre manière de dire les choses : Tout nombre pair 2k s'écrit une infinité de fois comme la différence de deux nombres premiers consécutifs. Le cas qui nous préocupe ici est celui de 2k = 2.

à cette année, 2014 n'est pas un nombre premier puisque pair ; nous devons attendre 2027 et 2029 pour la prochaine paire de nombres premiers jumeaux.

Des avancées notables sur le sujet ont été faites très récemment, en 2013 ([11]) ; en voici une synthèse.

Dans les cinquante pages d'un article accepté pour publication en mai 2013, YITANG ZHANG (enseignant-chercheur de l'université de New Hampshire aux Etats-Unis, d'origine chinoise) a démontré qu'il existe une infinité de paires de nombres premiers consécutifs dont l'écart est inférieur ou égal à n_0, et ce n_0 est 70 millions ([12]). En termes mathématiques, cela s'écrit :

$$\liminf_{n\longrightarrow+\infty}(p_{n+1}-p_n)<7\times10^7. \tag{6}$$

Au cours de l'été 2013, un projet collaboratif (dénommé Polymath 8, voir [13]) orchestré par le médaillé FIELDS T. TAO aboutit à l'amélioration du résultat de ZHANG, réduisant l'écart n_0 à 4680. Encore plus récemment, en début 2014, l'écart n_0 a été abaissé à 270. L'objectif est de diminuer encore ce n_0 avant la fin de l'année 2014. C'est encore loin de ce qu'on attend : selon la conjecture énoncée plus haut, l'écart entre deux nombres consécutifs de la liste des nombres premiers devrait être 2 une infinité de fois ; en termes mathématiques, cela s'écrirait :

$$\liminf_{n\longrightarrow+\infty}\ (p_{n+1}-p_n)=2. \tag{7}$$

En somme, l'étau se resserre !

Du point de vue théorie mathématique, on sait un certain nombre de choses importantes sur la suite des nombres premiers jumeaux, par exemple :

- mis à part la paire de démarrage (3, 5), ils sont tous de la forme $(6n-1, 6n+1)$;
- à la différence de la série des inverses des nombres premiers qui diverge (c'est-à-dire, $\sum_{n=1}^{+\infty}\frac{1}{p_n}=+\infty$) la série des inverses des nombres premiers jumeaux converge,

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\ldots.=:B<+\infty. \tag{8}$$

C'est un résultat assez étonnant, dû au mathématicien norvégien V. BRUN en 1919 ; malheureusement il ne permet pas de conclure à la finitude ou à l'infinitude des nombres premiers jumeaux. La quantité B au-dessus a été calculé numériquement de manière très précise, elle est de l'ordre de 1, 90...

4. La conjecture de Goldbach

La conjecture de C.GOLDBACH (1742) s'énonce comme suit : «Tout entier pair strictement supérieur à 2 peut s'écrire comme somme de deux nombres

premiers (le même nombre premier pouvant être utilisé deux fois) » ; sous une forme plus imagée : **« Tout entier strictement supérieur à 2 est la moyenne arithmétique de deux nombres premiers »**. Une majorité des mathématiciens spécialistes du sujet pensent que c'est vrai. Il y a des frémissements de temps en temps, des annonces parfois intempestives puis démenties, mais rien de définitif et de sûr. Néanmoins, l'année 2013 a été marquée par une avancée majeure sur le sujet, en voici un résumé. Commençons par dire que, de nos jours, on a l'habitude de diviser la conjecture en deux :

- la conjecture de Goldbach *faible*, ou ternaire, qui dit que **tout entier impair strictement supérieur à** 5 **peut s'écrire comme la somme de trois nombres premiers** ;

- la conjecture de Goldbach *forte*, ou binaire, la vraie en fait, celle énoncée plus haut, qui dit que **tout entier pair strictement supérieur à** 2 **peut s'écrire comme somme de deux nombres premiers**.

Comme leurs qualificatifs peuvent le sugérer, la conjecture forte implique la conjecture faible ; de manière immédiate, enlevez 3 à votre entier impair n, et ensuite exprimez $n - 3$ comme la somme de deux nombres premiers.

En mai 2013, le même mois que pour le résultat sur l'écart entre les nombres premiers (*cf.* paragraphe précédent), M.H. Helfgott (du département de mathématiques de l'Ecole Normale Supérieure de Paris) annonce qu'il a résolu la conjecture de Goldbach ternaire. Le travail, déposé sous forme de prépublication ([14]), est en cours de vérification ; le cheminement de la démonstration est expliqué par l'auteur lui-même en [15]. En fait, il démontre (mathématiquement) le résultat pour les entiers $n \geq 10^{30}$; la vérification numérique avait été faite pour tous les entiers impairs jusqu'à cette borne, et même bien au-delà, jusqu'à $8,875 \times 10^{30}$.

Selon lui, la conjecture forte reste encore bien loin des possibilités et connaissances actuelles.

Plus forte que les conjectures exposées aux paragraphes 3 et 4 est ladite conjecture de H.Dubner (en 2000) : *« Tout entier pair supérieur à* 4208 *est la somme de deux nombres premiers ayant un jumeau »*. Elle a été vérifiée pour tous les nombres pairs jusqu'à 4×10^{11} . La démontrer ou la réfuter semble hors d'atteinte aujourd'hui.

5. Conjecture (ou Hypothèse) de Riemann

Mais la conjecture la plus célèbre, celle qui domine toutes les autres (au moins selon certains mathématiciens), qui assurera célébrité et fortune à celui qui y répondra est la conjecture de G.Riemann (1859) (on dit aussi, et plus fréquemment, « l'hypothèse de Riemann »). Sous sa forme basique, elle

exprime que la fonction de ζ RIEMANN (prolongement analytique en une fonction holomorphe définie pour tout nombre complexe z autre que 1, de la fonction de la variable complexe $z \mapsto \zeta(z) := \sum_{n=1}^{\infty} \frac{1}{n^z}$) a tous ses zéros non triviaux situés sur la droite d'équation $\mathcal{R}e(z) = \frac{1}{2}$. Un des côtés fascinants de cette conjecture est qu'elle peut être reliée à divers domaines des mathématiques, comme cela est bien expliqué dans l'excellent article de synthèse [16]. Un autre aspect est qu'elle a été vérifiée pour les premiers millions de zéros de ζ (les 10^{23} premiers zéros en fin 2004, probablement bien plus aujourd'hui). On raconte que le mathématicien HILBERT, interrogé sur la première chose qu'il demanderait après un sommeil de plus de cinq cents ans, répondit que ce serait : «Quelqu'un a-t-il résolu la conjecture de RIEMANN ?». Tout aussi étonnantes sont les formes diverses *équivalentes* que peut prendre la conjecture de RIEMANN, dans pratiquement tous les domaines des mathématiques. Notre forme équivalente favorite est celle de J.C. LAGARIAS ([17]) ; nous ne résistons pas au plaisir de la présenter.

Soit

$$H_n = \sum_{k=1}^{n} \frac{1}{k} \quad \text{(appelés parfois nombres réels harmoniques) ;}$$

$$\sigma(n) = \sum_{d \text{ divise } n} d, \text{ la somme de tous les diviseurs de } n \ (\sigma(6) = 12 \text{ par exemple}).$$

Alors :

Forme équivalente de la conjecture de Riemann :

$$\text{Pour tout } n \geq 1,\ \sigma(n) \leq H_n + \exp(H_n)\ln(H_n),$$
$$\text{avec égalité seulement pour } n = 1. \qquad (9)$$

Bien sûr, il y a tout un travail profond de mathématiques pour en arriver là, le travail de toute une vie de mathématicien par exemple. Reconnaissons que (9) est très facile à comprendre, même pour un étudiant en mathématiques débutant ; il n'en demeure pas moins qu'y répondre est hors d'atteinte pour l'instant.

La conjecture de RIEMANN est la première sur la liste des sept défis mathématiques posés en 2000 par l'Institut Mathématique CLAY. Chaque résolution (vérifiée) est dotée d'un récompense de 1 million de dollars. A ce jour (juin 2014), seule une des conjectures, celle de H. POINCARÉ, a été résolue (en 2003).

6. En guise de conclusion.

Les nombres entiers sont certes des objets familiers, de bons amis de la vie quotidienne, mais ils peuvent donner lieu à des problèmes de nature mathématique très difficiles à résoudre : *« Any fool can ask questions about numbers, which even a thousand wise men cannot solve »,* paraphrase du point de vue de K.F. Gauss par P. Ribenboim (en 1984), grand vulgarisateur des problèmes relatifs aux nombres.

Répondre à une des conjectures importantes sur les nombres, telles que celles que nous avons évoquées, n'assurera pas la fortune mais au moins la célébrité à son auteur. D'une manière générale, les conjectures jouent un rôle de stimulation essentiel dans l'avancement des mathématiques, comme nous avons essayé de le montrer dans notre travail [18]. Souvent, elles n'ont pas d'applications directes immédiates, elles sont le reflet de la quête scientifique permanente des mathématiciens ; un de mes collègues de l'université de Bordeaux, spécialiste de la Théorie des nombres justement, résumait joliment cet objectif par le raccourci suivant : *« Gratter là où ça démange ».*

Références.

[1] F. Le Lionnais et J. Brette, *Nombres remarquables*, Hermann (1997).

[2] D. Lignon, *Dictionnaire de (presque) tous les nombres entiers*, Ellipses (2012).

[3] J.H. Silverman, *The arithmetic of elliptic curves,* Springer-Verlag (1986).

[4] J-B. Hiriart-urruty, *Sur une particularité de 26...* Revue Matapli, publiée par la SMAI, n° 82, pp.53-54 (2007).

[5] M. Mischler, *Le b.a.-ba pour comprendre Catalan-Mihailescu,* Quadrature, n° 78, pp.41-47 (2010).

[6] J.-P. Delahaye, *Merveilleux nombres premiers*, Editions Belin-Pour la Science (2000).

[7] M. du Sautoy, *La symphonie des nombres premiers*, Collection Points Sciences (2007).

[8] J. Derbyshire, *Dans la jungle des nombres premiers,* Collection Quai des sciences, Dunod (2007).

[9] M. Waldschmidt, *Le théorème de* Green-Tao *et autres secrets des nombres pre- miers*, in **Mathématiques, l'explosion continue**, Publications de la SMF-SMAI-SFdS (2013).

[10] J.-L. Nicolas et C. Delaunay, *Cryptage et décryptage : communiquer en toute sécurité*, in **Mathématiques, l'explosion continue**, Publications de la SMF-SMAI-SFdS (2013).

[11] P. Pajot, *Réduire l'écart entre les nombres premiers*, in La Recherche (numéro spécial) : **Le Top des 10 découvertes de l'année 2013** (janvier 2014).

[12] Y. Zhang, *Bounded gaps between primes,* Annals of Mathematics 179, n° 3, pp.1121- 1174 (mai 2014). Article reçu par le comité de rédaction le 17 avril 2013 et accepté pour publication, après lecture-arbitrage, le 21 mai 2013.

[13] R. de la Bretèche, *Petits écarts entre nombres premiers et Polymath : une nouvelle manière de faire de la recherche en mathématiques ?* Gazette des mathématiciens, publiée par la SMF (avril 2014).

[14] H.A. Helfgott, *Major arcs for Goldbach's problem*. Article de 130 pages, déposé sous forme de prépublication en mai 2013.

[15] H.A. Helfgott, *La conjecture de Goldbach ternaire*, Gazette des mathématiciens, publiée par la SMF (avril 2014).

[16] M. Balazard, *Un siècle et demi de recherches sur l'hypothèse de Riemann*, Gazette des mathématiciens n° 126, publiée par la SMF, pp.7-24 (octobre 2010).

[17] J.C. Lagarias, *An elementary problem equivalent to the Riemann hypothesis,* The American Mathematical Monthly, Vol. 109, pp.534-543 (2002).

[18] J.-B. Hiriart-Urruty, *Le rôle des conjectures dans l'avancement des mathématiques : tours et détours à l'aide d'exemples*, Quadrature, n° 83, pp.27-33 (2012).