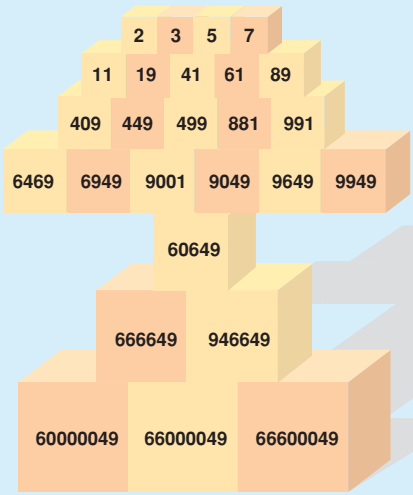


Nombres premiers inévitables et pyramidaux

JEAN-PAUL DELAHAYE

Nouveautés et divertissements à propos des toujours étonnants nombres premiers.

Les êtres humains ont pris conscience de l'existence de nombres particuliers il y a plus de deux mille ans, nombres qui sont à la fois très simples et infiniment complexes et c'est pourquoi les passionnés les étudient avec assiduité et obstination, tentant d'en percer les mystères, ou parfois uniquement pour se divertir. Ces nombres, ce sont, bien sûr, les nombres premiers qui, comme 2, 3, 5, 7, 11, 13, 17, 19, ne sont divisibles – c'est leur définition – que par 1 et eux-mêmes. Leur magie va, une fois encore, nous étonner, car plusieurs résultats, récemment découverts, concernent des propriétés remarquables de ces nombres.

LES NOMBRES PREMIERS INÉVITABLES

Jeffrey, Shallit de l'Université canadienne de Waterloo, a introduit une notion simple et naturelle qui l'a conduit à un théorème étrange et à une multitude de questions dont certaines sont, sans doute, difficiles.

Le mot MATHÉMATIQUE contient le mot AMIE (en parcourant les lettres de MATHÉMATIQUE on trouve dans l'ordre les lettres de AMIE). De même, un nombre premier peut en contenir un autre : le nombre premier 150967 contient le nombre premier 1597, qui lui-même contient les nombres premiers 17, 19, 59 et 97.

La question que s'est posée J. Shallit est : «Peut-on trouver une famille de nombres premiers $q_1, q_2, \ldots q_k, \ldots$ telle que tout nombre premier contienne (au moins) *l'un* des q_i?» Une telle famille serait en quelque sorte «inévitable». Pour qu'elle soit intéressante, il faudrait qu'on ne puisse pas la simplifier, c'est-à-dire il faudrait que, dès que l'on enlève un des q_i , alors la famille ne soit plus inévitable. C'est ce qu'on appellera une famille *inévitable minimale* de nombres premiers.

La famille 17 et 19 n'est pas une famille inévitable, car le nombre premier 13 ne contient aucun d'eux. Il semblerait qu'une famille inévitable soit difficile à construire. Il n'en est rien : un petit moment de réflexion vous fera découvrir une méthode infaillible pour construire une telle famille inévitable minimale de nombres premiers.

En effet, partons de la suite infinie complète des nombres premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61… Cette famille est inévitable (tous les nombres premiers sont dans la liste et donc chaque nombre premier considéré est contenu dans un élément de la liste, qui est ainsi inévitable…), mais elle n'est pas minimale, car on peut lui enlever 13 (au moins). En effet, si un nombre contient 13, il contient 3, donc en gardant 3 dans la liste et en enlevant 13, il est certain qu'on ne change pas le caractère inévitable de la famille. En revanche, on ne peut pas enlever 3 ni aucun des nombres précédents 13. Si on enlevait 3 ou 7 par exemple, la famille ne serait plus inévitable, car 3 et 7, ne contiendraient aucun nombre de la liste restante.

Ces considérations montrent que pour trouver une famille inévitable minimale de nombres premiers, on envisage les nombres premiers les uns après les autres dans l'ordre et pour chacun d'eux on décide de le garder ou non selon qu'il contient un nombre déjà sélectionné.

Parcourons les nombres premiers à partir du début : 2 est sélectionné ; puis 3, puis 5, puis 7, puis 11 ; 13 est supprimé, car il contient 3 ; 17 est supprimé, car il contient 7 ; 23 est supprimé, car il contient 2 et 3 ; 29 est supprimé, car il contient 2 ; 31 et 37 sont supprimés, car ils contiennent 3 ; 41 est sélectionné (aucun des nombres premiers retenus avant lui n'est contenu dans 41) ; 43, 47, 53, 59 sont supprimés ; 61 est sélectionné, etc.

Très bien, mais cette histoire nous fait entrer dans un calcul infini, puisque nous n'obtiendrons notre famille inévitable minimale qu'après avoir parcouru toute la suite des nombres premiers (dont on sait, merci Euclide, qu'elle est infinie). Nous n'aurons donc la réponse à notre question qu'au bout d'un temps infini. Si nous utilisions un ordinateur cela ne changerait rien : au bout de 1 000 heures de calcul il proposerait une liste de nombres premiers sélectionnés, mais vous ne sauriez pas s'il lui manque des éléments.

Heureusement la théorie des langages (un domaine de l'informatique théorique) va nous aider. On sait, grâce à un résultat de M. Lothaire, que pour tout ensemble E d'entiers donnés (pas nécessairement des nombres premiers) écrits en base 10 (le résultat se généralise à toute base), il existe un ensemble inévitable minimal fini d'éléments de E. Autrement dit l'algorithme de sélection décrit précédemment appliqué à n'importe quel ensemble E ne retient plus rien à partir d'un certain moment.

Pour des ensembles E particuliers, ce résultat est facile à vérifier. Par exemple, pour l'ensemble des nombres pairs, voyons quel est l'ensemble inévitable minimal, c'est-à-dire l'ensemble des nombres pairs contenus dans tous les nombres pairs. Pour cet ensemble {0, 2, 4, 6, 8, 10, 12,…}, la procédure infinie décrite au-dessus ne garde que {0, 2, 4, 6, 8} et ensuite enlève tout, conduisant donc à l'ensemble inévitable minimal de nombres pairs {0, 2, 4, 6, 8}. Le raisonnement montrant qu'on ne retiendra rien de plus est évident, tout nombre pair se termine par 0, 2, 4, 6 ou 8 donc à partir de 8 plus aucun nombre pair supplémentaire n'est retenu.

Pour l'ensemble E des nombres multiples de 4, on trouve l'ensemble inévitable

minimal : {0, 4, 8, 12, 16, 32, 36, 52, 56, 72, 76, 92, 96}. Là encore un raisonnement simple assure qu'aucun nombre ne sera retenu au-delà de 96 et permet donc d'arrêter la recherche.

Pour l'ensemble des nombres multiples de 3, il est bien moins facile de trouver l'ensemble inévitable minimal. Cherchez-le si vous en avez le loisir et le goût, la solution est donnée à la fin de cet article.

Revenons aux nombres premiers. Au bout d'un certain temps, en appliquant l'algorithme d'élimination décrit au-dessus, vous enlèverez tout, car vous aurez obtenu l'ensemble inévitable minimal des nombres premiers. Le résultat de M. Lothaire vous indique que cela va se produire, mais malheureusement ne vous dit pas quand ! Vous êtes certain d'arriver au bon résultat, mais quand cela se produira vous ne le saurez pas, à moins de découvrir un raisonnement comme pour les multiples de 2, 3 ou 4. Pour les nombres premiers, le raisonnement est assez difficile, pourtant Jeffrey Shallit a réussi à le formuler – il occupe deux pages de son article – et établit que l'ensemble minimal inévitable des nombres premiers écrits en base 10 est : {2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991,6469, 6949, 9001, 9049, 9649, 9949, 60649, 666649, 946649, 60000049, 66000049, 66600049}.

Tout nombre premier écrit en base 10 contient donc l'un de ces 26 nombres premiers, et cet ensemble de nombres premiers est le plus petit qui soit inévitable en base 10. Pourquoi ces nombres premiers-là ? Qu'ont-ils de particulier qui les désigne ainsi ? Mystère. Le résultat de Jeffrey Shallit n'est-il pas un étrange et beau résultat !

Si on utilise une autre base que la base décimale, on obtient d'autres ensembles inévitables minimaux de nombres premiers *(voir la figure 1)*. Signalons que J. Shallit a aussi démontré que l'ensemble inévitable minimal des nombres composés écrits en base 10 est : {4, 6, 8, 9, 10, 12, 15, 20, 21, 22, 25, 27, 30, 32, 33, 35, 50, 51, 52, 55, 57, 70, 72, 75, 77, 111, 117, 171, 371, 711, 713, 731}.

Il conjecture aussi sans avoir réussi à en trouver de démonstration que {1, 2, 4, 8, 65536} est l'ensemble inévitable minimal des puissances de 2 écrites en base 10.

Un fait remarquable et intéressant dans le calcul des ensembles inévitables minimaux est que l'ordinateur propose un résultat qui, si vous l'avez fait tourner assez longtemps, a de bonnes chances d'être celui que vous cherchez, mais la seule façon de savoir si l'ensemble qu'il vous propose est vraiment complet (c'est-à-dire si aucun autre nombre ne sera retenu quand vous prolongerez le calcul une heure, une journée, une semaine etc.) est de raisonner. L'ordinateur propose, le mathématicien – s'il y arrive – dispose et c'est de leur association que naissent les résultats sur les ensembles inévitables minimaux.

LES PYRAMIDES DE NOMBRES PREMIERS PALINDROMES

Les amateurs de nombres premiers sont aussi des collectionneurs et leurs recherches regorgent de défis. Les pyramides de nombres premiers sont un de leurs sujets favoris, dont G.L. Honaker et Chris Caldwell sont des spécialistes. Examinons certaines découvertes récentes.

Partant d'un nombre premier, 2 par exemple, on cherche un nombre premier palindrome (c'est-à-dire qui est le même quand on le lit à l'envers) contenant 2 en son centre, 929 par exemple. On recherche alors un autre nombre premier palindrome de 5 chiffres contenant 929 en son milieu 39293 convient, etc. Partant de 2, les plus hautes pyramides qu'on peut construire ont pour hauteur 5. Il y en a exactement 2 que voici :

1. LES ENSEMBLES INÉVITABLES MINIMAUX DE NOMBRES PREMIERS EN DIFFÉRENTES BASES

La notion d'ensemble inévitable minimal de nombres premiers dépend de la base de numération avec laquelle on écrit les nombres. En base 10, Jeffrey Shallit a montré que l'ensemble inévitable minimal est : {2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991, 6469, 6949, 9001, 9049, 9649, 9949, 60649, 666649, 946649, 60000049, 66000049, 66600049}.

Cela signifie que tout nombre premier comporte dans ses chiffres au moins un de ces nombres premiers (l'ensemble est inévitable) et qu'on ne peut pas faire plus petit (l'ensemble inévitable est minimal). Exemples : le nombre premier 4606669 contient 409 ; le nombre premier 906601 contient 9001; le nombre premier 6000004000000009 contient 60000049.

Base 2. En base 2, le résultat prend une forme plus simple. La suite des nombres premiers s'écrit : 10, 11, 101, 111, 1011, 1101, 10001, 10011, 10111, 11101, ... et il est évident donc que tout nombre premier contient 10 ou 11. L'ensemble des deux nombres premiers {10, 11} (en écriture décimale {2, 3}) est donc l'ensemble inévitable minimal des nombres premiers écrits en base 2.

Base 3. En base 3, le résultat reste assez simple. La suite des nombres premiers s'écrit : 2, 10, 12, 21, 102, 111, 122, 201, 212, 1002, 1011, 1101, 1112, 1121, 1202, 1222, 2012, 2021, 2111, 2122... On trouve l'ensemble inévitable minimal {2, 10, 111} (en écriture décimale {2, 3,13}).

Base 4. En base 4, le résultat reste une dernière fois assez simple. La suite des nombres premiers est : 2, 3, 11, 13, 23, 31, 101, 103, 113, 131, 133, 211, 221, 223, 233, 311, 323, 331, 1003, 1013... On trouve l'ensemble inévitable minimal {2, 3, 11} (en écriture décimale {2, 3, 5}).

Base 5. En base 5, tout se complique. La suite des nombres premiers est : 2, 3, 10, 12, 21, 23, 32, 34, 43, 104, 111, 122, 131, 133, 142, 203, 214, 221, 232, 241, 243, 304, 313, 324, 342, 401, 403, 412, 414, 423...

En appliquant la méthode de sélection jusqu'à 10000, on trouve : {2, 3, 10, 111, 401, 414, 14444, 44441} (soit en écriture décimale : {2, 3, 5, 31, 101, 109, 1249, 3121}). Reste à démontrer que l'on n'a rien oublié.

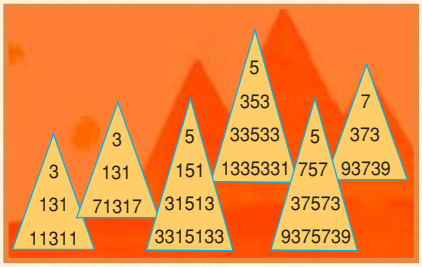
Base 6. En base 6, le même genre de problème se pose. La suite des nombres premiers est : 2, 3, 5, 11, 15, 21, 25, 31, 35, 45, 51, 101, 105, 111, 115, 125, 135,141, 151, 155, 201, 211, 215, 225, 241, 245, 251, 255, 301, 305, ... En appliquant la méthode de sélection jusqu'à 10000, on trouve : {2, 3, 5, 11, 4401, 4441, 40041} (soit en écriture décimale {2, 3, 5, 7, 1009, 1033, 5209}).

Base 7. La suite des nombres premiers en base 7 est : 2, 3, 5, 10, 14, 16, 23, 25, 32, 41, 43, 52, 56, 61, 65, 104, 113,115, 124, 131, 133, 142, 146, 155, 166, 203, 205, 212, 214, 221, ... En appliquant la méthode de sélection jusqu'à 10000, on trouve : {2, 3, 5, 10, 14,16, 41, 61, 11111} (soit en écriture décimale {2, 3, 5, 7, 11, 13,29, 43, 2801}).

Base 8. La suite des nombres premiers est : 2, 3, 5, 7, 13, 15, 21, 23, 27, 35, 37, 45,51, 53, 57, 65, 73, 75, 103, 107, 111, 117, 123, 131, 141, 145, 147, 153, 155, 161... La méthode de sélection donne {2, 3, 5, 7, 111, 141, 161, 401, 661, 4611, 6101, 6441,60411}, soit en écriture décimale, {2, 3, 5, 7, 73, 97, 113, 257, 433, 2441, 3137, 3361, 24841}.

Base 9. La suite des nombres premiers est : 2, 3, 5, 7, 12, 14, 18, 21, 25, 32, 34, 41,45, 47, 52, 58, 65, 67, 74, 78, 81, 87, 102, 108, 117, 122, 124, 128, 131, 135... La sélection donne {2, 3, 5, 7, 14, 18, 41, 81, 601, 661, 1011, 1101}, soit en décimal, {2, 3, 5, 7, 13, 17, 37, 73, 487, 541, 739, 811}. Les résultats pour les bases 5, 6, 7, 8, 9 sont expérimentaux et n'ont pas été démontrés.

Si au lieu de placer un 2 au sommet on place un autre chiffre premier (3, 5 ou 7), les plus hautes pyramides qu'on obtient sont les suivantes :



Ces résultats sont définitifs, car les programmes utilisés pour trouver ces records ont exploré toutes les alternatives possibles : par exemple placer 727, qui est premier, sous le 2 à la place de 929, oblige à placer ensuite 37273, mais aucune suite n'est alors possible, car 1372731, 2372732, 3372733, 4372734, 5372735, 6372736, 7372737, 8372738, 9372739 sont tous des nombres composés.

Peut-on trouver de plus hautes pyramides en plaçant au sommet des nombres premiers de plusieurs chiffres (qui conduisent donc à des pyramides tronquées), ou en allongeant les lignes de plusieurs chiffres à la fois au lieu d'un seul (toujours en exigeant bien sûr d'avoir des nombres premiers palindromes à chaque niveau)?

La plus haute pyramide tronquée avec des marches de largeur 1, trouvée à l'heure actuelle est due à Felice Russo la voici :

Comme il y a une infinité de points de départ possibles, il est vraisemblable que ce record sera amélioré. Un lecteur essaiera-t-il?

Si maintenant nous recherchons des pyramides de sommet 2 ayant des marches de largeur 2 (chaque nouveau nombre allonge le précédent de deux chiffres en avant et de deux chiffres en arrière) le record de hauteur est alors 26. Il y a deux pyramides record dont la première est représentée ci-contre à droite.

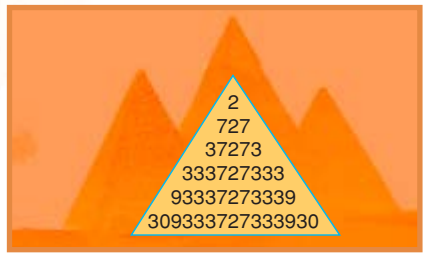
Si à la place du sommet 2, nous choisissons 3, la hauteur maximale est 28 (trois pyramides différentes ont cette hauteur). Avec 5 et 7, la hauteur maximale est 29 et dans chaque cas une seule pyramide a été trouvée.

Comme pour les pyramides aux marches de largeur 1 partant de 2, 3, 5 ou 7, les calculs ont été menés de façon systématique et on est donc certain que l'on ne pourra pas améliorer ces records qui sont donc définitifs.

Pour construire ces pyramides, il faut que l'on sache déterminer si un nombre est premier ou non. Pour cela, la méthode la plus simple consiste à rechercher des diviseurs de n : on fait la division de n par tous les nombres jusqu'à la racine carrée de n (car si n possède un diviseur autre que 1 et lui-même, il en possède un inférieur ou égal à sa racine carrée), et si aucune division ne tombe juste on sait que n est premier. Cette méthode des divisions ne marche pas pour des nombres longs : par cette méthode, au-delà de 40 chiffres, même le plus puissant ordinateur (ou réseaux d'ordinateurs) ne peut tester la primalité d'un nombre. On doit donc utiliser d'autres techniques dont les plus faciles à programmer sont probabilistes, ce qui veut dire qu'elles produisent leur conclusion avec un certain risque d'erreur *(voir figure 2)*. Cependant en s'y prenant bien, le risque peut être minimisé (inférieur à 10^{-6} ou même inférieur à 10^{-12}) et donc en pratique tous les résultats obtenus, même quand on utilise des tests de primalité probabilistes, sont corrects. Les chercheurs de pyramides de nombres premiers utilisent ces méthodes probabilistes.

En s'autorisant des marches de largeur constante plus grande (par exemple 3), on découvre des pyramides plus hautes (c'est logique, car à chaque étape un plus grand nombre de possibilités est offert). Mais peut-on trouver une pyramide de hauteur infinie? G. L.Honaker et C. Caldwell pensent que non et c'est pourquoi ils ont formulé la conjecture suivante : *Quel que soit le nombre premier palindrome choisi comme sommet et quel que soit le nombre fixé pour la largeur des marches, une pyramide de palindromes premiers a une hauteur finie.* Bien sûr cette conjecture attend une démonstration.

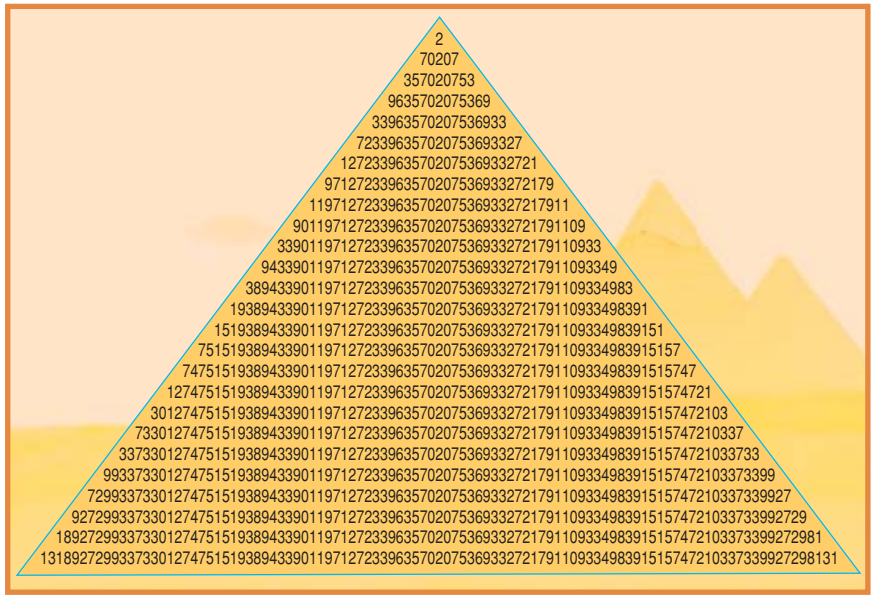
Mais que se passe-t-il si on autorise la largeur des marches à être variable comme pour la pyramide suivante?



La possibilité d'utiliser des marches de toute largeur conduit vraisemblablement à des pyramides infinies. Personne néanmoins n'a su le démontrer aujourd'hui!

En s'imposant d'utiliser à chaque fois le plus petit nombre palindrome qui convienne pour obtenir l'étage suivant et partant de 2, une pyramide de hauteur 58 a été calculée par F. Russo. Son sommet est la pyramide précédente. Nous la décrivons en ne donnant que l'extension nécessaire pour passer d'un étage à celui juste au-dessous : 2, 7, 3, 33, 9, 30, 18, 92, 3, 133, 18, 117, 17, 15, 346, 93, 33, 180, 120,194, 126, 336, 331, 330, 95, 12, 118, 369, 39, 32, 165, 313, 165, 134, 13,149, 195, 145, 158, 720, 18, 396, 193, 102, 737, 964, 722, 156, 106, 395,945, 303, 310, 113, 150, 303, 715, 123. Il semble assez clair qu'on doit pouvoir la poursuivre indéfiniment, mais cela reste à prouver. Il faudra démontrer aussi, par des méthodes non probabilistes, que chacun des étages est bien un nombre premier.

Terminons ce petit voyage par une nouvelle conjecture proposée par Harvey Dubner et qui fait joliment la synthèse de deux conjectures anciennes.



JUMEAUX + GOLDBACH

Depuis 250 ans, on pense que tout nombre pair plus grand que 2 est somme de deux nombres premiers (4 = 2+2, 6 = 3+3, 8 = 5+3, 10 = 5+5, etc.). Il s'agit de la conjecture de Christian Goldbach pour laquelle un prix de un million de dollars avait été proposé en 2000. L'offre n'était valable que pour les années 2000 et 2001 et personne ne l'a emportée. La conjecture a été vérifiée jusqu'à 400 000 000 000 000.

On pense aussi depuis bien longtemps qu'il existe une infinité de paires de nombres premiers jumeaux, c'est-à-dire espacés de 2 unités comme 11 et 13, ou comme 17 et 19, ou comme 2027 et 2029 (les plus proches années à venir qui seront des nombres premiers jumeaux). Le début de la suite des nombres premiers jumeaux est : (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73),(101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227,229), (239, 241)…

La proportion de nombres premiers jumeaux parmi les nombres premiers diminue quand on progresse vers l'infini : les nombres premiers jumeaux sont de plus en plus rares et beaucoup plus rares que les nombres premiers. Plus précisément, alors que la densité des nombres premiers autour de n est environ $1/ln(n)$ (c'est le fameux résultat prouvé simultanément par Hadamard et de la Vallée Poussin en 1896), on conjecture que la densité des nombres premiers jumeaux vaut $2{,}64/[ln(n)]^2$, ce qui – si la conjecture est vraie – signifie que les nombres premiers jumeaux sont de plus en plus rares parmi les nombres premiers, leur proportion tendant vers 0 à l'infini.

Écrire un nombre pair sous la forme d'une somme de deux nombres premiers jumeaux est donc plus difficile que de l'écrire sous la forme d'une somme de deux nombres premiers. Pourtant 6 = 3+3, 8 = 3+5, 10 = 5+5, 12 = 5+7, 14 = 7+7, 16 = 13+3,18 = 13+5, 20 = 13+7, 22 = 19+3, 24 = 19+5, 26 = 13+13. Il semble bien qu'on puisse toujours écrire un nombre pair comme la somme de deux nombres premiers jumeaux. Une recherche systématique montre en réalité qu'il existe des exceptions : 94 par exemple ne peut pas s'écrire comme somme de deux nombres premiers jumeaux. Un calcul par ordinateur conduit à la liste d'exceptions suivantes : 94, 96, 98, 400, 402, 404, 514, 516, 518, 784, 786, 788,904, 906, 908, 1114, 1116, 1118, 1144, 1146, 1148, 1264, 1266, 1268, 1354,1356, 1358, 3244, 3246, 3248, 4204, 4206, 4208.

Plus intéressant, aucune autre exception n'a été trouvée en explorant tous les nombres pairs jusqu'à 20 000 000 000, d'où la conjecture de Harvey Dubner : *Tout*

2. ALGORITHMES PROBABILISTES POUR LA PRIMALITÉ

Pour trouver des nombres premiers de plusieurs dizaines ou plusieurs centaines de chiffres, la méthode des divisions n'est pas utilisable. On peut cependant procéder de la manière suivante qui conduira non pas à une certitude, mais à une forte présomption (ce sont des algorithmes probabilistes).

Pour savoir si n est premier :

– on choisit un nombre a entre 2 et $n-1$ et on calcule par une série de multiplications et divisions a^2 mod n (c'est-à-dire le reste de la division de a^2 par n), puis a^4 mod n, a^8 mod n, a^{16} mod n, etc.

– en multipliant entre eux certains des résultats de l'étape précédente, on calcule : a^{n-1} mod n. Par exemple, si $n = 13$, on doit calculer a^{12} mod 13 qu'on obtient en multipliant (a^4 mod 13) par (a^8 mod 13).

– si le résultat obtenu est différent de 1, d'après le petit théorème de Fermat, cela signifie que n n'est pas premier (dans ce cas, il n'y a pas d'incertitude) ;

– sinon, on a un indice que n pourrait être premier, et essayant une autre valeur de a et en arrivant à nouveau au résultat 1, on diminuera le risque de se tromper.

Su Hee Kim et Carl Pomerance ont calculé les probabilités d'erreur de cette méthode. On sait par exemple que si vous choisissez au hasard un nombre n de cent chiffres ou moins, que vous choisissez au hasard un nombre a entre 2 et $n-1$, et que vous trouvez que $a^{n-1} = 1$ mod n, alors la probabilité pour que n soit premier est supérieure à 99,9999972%. Voici quelques autres majorations du risque d'erreur r de cette méthode :

– pour 60 chiffres, risque d'erreur $r < 7{,}2 \times 10^{-2}$,
– pour 80 chiffres, risque d'erreur $r < 8{,}5 \times 10^{-5}$,
– pour 100 chiffres, risque d'erreur $r < 2{,}8 \times 10^{-8}$,
– pour 200 chiffres, risque d'erreur $r < 3{,}9 \times 10^{-27}$,
– pour 1000 chiffres, risque d'erreur $r < 1{,}2 \times 10^{-123}$,
– pour 10000 chiffres, risque d'erreur $r < 1{,}6 \times 10^{-1331}$.

3. AVEC DES MARCHES DE LARGEUR 3 ON BUTE SUR L'IMPOSSIBLE CALCULATOIRE.

Si, partant du sommet 2, on cherche à construire une pyramide de nombres premiers palindromes ayant des marches de largeur 3 (à chaque étape, on prolonge les nombres précédents de 3 chiffres en avant et de trois chiffres en arrière), Honaker et Caldwell ont évalué qu'on devrait pouvoir trouver une pyramide de hauteur 193 environ (ayant donc une base constituée d'un nombre de 1153 chiffres). Malheureusement la recherche de cette pyramide record est impossible à mener systématiquement (même en utilisant des tests de primalité probabilistes), car il faudrait envisager 10^{30} pyramides environ. En menant un calcul partiel, ils ont cependant trouvé une pyramide intéressante de hauteur 94 dont le dernier nombre est le nombre premier palindrome suivant de 559 chiffres :

36111974471735117172375698479939699398670294872076673738872570975933036936694591471136170275296690097813090393814299595293030317076035718632439535136131237879832196339678074474010296492097573093813312017933390112092138018139630234276013533095170197012074071138190030076093033030020030330390670030091831170470210791071590335310672432036931810831290211093339710213318390375790294692010474470876933691238978732131631535934236817530670713030392595992418393090318790096692572071631174195496639630339579075278837376670278492076893996939974896573271711537174479111 63.

Le sommet de cette pyramide est :

2
3002003
3303002003033
9303303002003033039
760930330302003033039067
30076093033030020030330390670003
900300760930330302003033039067003009
38190030076093033030020030330390670030091 83
7113819003007609303303002003033039067003009183117
740711381900300760930330302003033039067003009183117047
12074071138190030076093033030020030330390670030091831170 47021
970120740711381900300760930330302003033039067003009183117047021079
70197012074071138190030076093033030020030330390670030091831170 47021079107
9517019701207407113819003007609303303002003033039067003009183117047021079107159

4 NOMBRES PREMIERS JUMEAUX

Voici la liste des 100 premières paires de nombres premiers jumeaux : [3, 5], [5, 7], [11, 13], [17, 19], [29, 31], [41, 43], [59, 61], [71, 73], [101, 103], [107, 109], [137,139], [149, 151], [179, 181], [191, 193], [197, 199], [227, 229], [239,241], [269, 271], [281, 283], [311, 313], [347, 349], [419, 421], [431,433], [461, 463], [521, 523], [569,571], [599, 601], [617, 619], [641, 643], [659, 661], [809, 811], [821,823], [827, 829], [857, 859], [881, 883], [1019, 1021], [1031, 1033],[1049, 1051], [1061, 1063], [1091, 1093], [1151, 1153], [1229, 1231],[1277, 1279], [1289, 1291], [1301, 1303], [1319, 1321], [1427, 1429], [1451, 1453], [1481, 1483], [1487, 1489], [1607,1609], [1619, 1621], [1667, 1669], [1697, 1699], [1721, 1723], [1787,1789], [1871, 1873], [1877, 1879], [1931, 1933], [1949, 1951], [1997,1999], [2027, 2029], [2081, 2083], [2087, 2089], [2111, 2113], [2129, 2131], [2141, 2143], [2237, 2239], [2267,2269], [2309, 2311], [2339, 2341], [2381, 2383], [2549, 2551], [2591,2593], [2657, 2659], [2687, 2689], [2711, 2713], [2729, 2731], [2789,2791], [2801, 2803], [2969, 2971], [2999, 3001], [3119, 3121], [3167, 3169], [3251, 3253], [3257, 3259], [3299, 3301],[3329, 3331], [3359, 3361], [3371, 3373], [3389, 3391], [3461, 3463],[3467, 3469], [3527, 3529], [3539, 3541], [3557, 3559], [3581, 3583],[3671, 3673], [3767, 3769], [3821, 3823]

Tout nombre pair, sauf ceux de l'ensemble {94, 96,98, 400, 402, 404, 514, 516, 518, 784, 786, 788, 904, 906, 908, 1114, 1116,1118, 1144, 1146, 1148, 1264, 1266, 1268, 1354, 1356, 1358, 3244, 3246,3248, 4204, 4206, 4208}, s'écrit comme somme de deux nombres premiers jumeaux. Du moins c'est ce que l'on vérifie quand on essaye tous les nombres pairs jusqu'à 20 000 000000.

Voici par exemple la décomposition des nombres pairs entre 1000 et 1110 sous forme d'une somme de deux nombres premiers jumeaux.

1000 = 821+179	1002 = 823+179	1004 = 823+181
1006 = 857+149	1008 = 859+149	1010 = 859+151
1012 = 821+191	1014 = 823+191	1016 = 823+193
1018 = 881+137	1020 = 883+137	1022 = 1019+ 3
1024 = 1021+3	1026 = 1021+5	1028 = 1021+7
1030 = 1019+11	1032 = 1021+11	1034 = 1031+3
1036 = 1033+3	1038 = 1033+5	1040 = 1033+7
1042 = 1031+11	1044 = 1033+11	1046 = 1033+13
1048=1031+17	1050 = 1033,+17	1052 = 1049+3
1054 = 1051+3	1056 = 1051+5	1058=1051+7
1060 = 1049+11	1062=1051+11	1064 = 1061+3
1066 = 1063+3	1068 = 1063+5	1070 = 1063+7
1072 = 1061+11	1074 = 1063+11	1076 = 1063+13
1078 = 1061+7	1080 = 1063+17	1082 = 1063+19
1084 = 857+227	1086 = 859+227	1088 = 859+229
1090 = 1061+29	1092 = 1063+29	1094 = 1091+3
1096 = 1093+3	1098 = 1093+5	1100 = 1093+7

D'où la nouvelle conjecture de Dubner :

Tout nombre pair plus grand que 4208 est la somme de deux nombres premiers jumeaux.

Cette conjecture entraîne à la fois la conjecture de Goldbach (tout nombre pair plus grand que 2 est somme de deux nombres premiers) et la conjecture des nombres premiers jumeaux (il existe une infinité de nombres premiers jumeaux).

nombre pair plus grand que 4208 est la somme de deux nombres premiers jumeaux.

La démonstration de cette conjecture établirait à la fois la conjecture de Goldbach (car on a vérifié que tous les nombres pairs inférieurs à 4208 s'écrivent comme somme de deux nombres premiers) et la conjecture sur l'infinité des nombres premiers jumeaux (car une quantité finie de nombres premiers jumeaux ne peut suffire à exprimer tous les nombres pairs au-delà de 4208 comme somme de nombres premiers jumeaux). La conjecture de Dubner est plus difficile que les deux conjectures anciennes réunies et donc… elle est sans doute très loin d'être démontrée !

En même temps que notre connaissance des nombres premiers s'accroît, la quantité de questions non résolues qu'ils posent augmente. Pas d'inquiétude donc pour l'amateur de nombres premiers, il gardera de quoi s'occuper pour longtemps encore.

Solution au problème de la recherche de l'ensemble inévitable minimal des multiples de 3.

Cet ensemble *M* possède 280 éléments : *M*= {0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 42, 45, 48, 51, 54, 57, 72, 75, 78, 81,84, 87, 111, 114, 117, 141, 144, 147, 171, 174, 177, 222, 225, 228, 252, 255, 258, 282, 285, 288, 411, 414, 417, 441, 444, 447, 471,474, 477, 522, 525, 528, 552, 555, 558, 582, 585, 588, 711, 714, 717, 741,744, 747, 771, 774, 777, 822, 825, 828, 852, 855, 858, 882, 885, 888}.

On vérifie à la main (ou avec son ordinateur) qu'en appliquant la méthode générale de sélection jusqu'à 1 000, on arrive bien à *M*. Il faut alors raisonner pour prouver qu'on ne retient rien au-delà de 1 000. Soit un nombre de 4 chiffres ou plus retenu au-delà de 1 000 (on suppose qu'il en existe et on cherche une contradiction). Il s'écrit *abcd*… Aucun de ses chiffres n'est multiple de 3 (car sinon il ne serait pas retenu puisque 0, 3, 6 et 9 sont déjà retenus). Supposons que *a* soit congru à 1 modulo 3 (c'est-à-dire de la forme $3p + 1$), alors *b* aussi (sinon *b* serait congru à 2 modulo 3, et donc *ab* serait multiple de 3, or par construction tout multiple de 3 de deux chiffres contient un nombre de l'ensemble *M*). De même *c* serait congru à 1 modulo 3 (sinon *bc* serait multiple de 3). Donc *abc* serait multiple de 3, ce qui est impossible, car tout nombre de trois chiffres multiple de 3 contient un nombre de *M* (car *M* a été construit en appliquant la procédure de sélection jusqu'à 1 000). L'hypothèse que *a* est congru à 1 modulo 3 conduit donc à une impossibilité. De même l'hypothèse que *a* est congru à 2 modulo 3, implique que *b* est congru à 2 modulo 3 et que *c* est aussi congru à 2 modulo 3, donc que *abc* est multiple de 3 ce qui est impossible. Le chiffre *a* ne peut donc être ni multiple de 3, ni congru à 1 modulo 3, ni congru à 2 modulo 3. Donc aucun nombre au-delà de 1 000 ne sera retenu.

Jean-Paul DELAHAYE est professeur d'informatique à l'Université de Lille. Son dernier livre *L'intelligence et le calcul*, éditeur Belin-Pour la Science, est un recueil de chroniques parues dans *Pour la Science*. e-mail : delahaye@lifl.fr

R. CRANDAL et C. POMERANCE, *Primes Numbers : A Computational Perspective*, Springer, New York, 2001.

P. De GEEST *World of Number.* http://www.worldofnumbers.com/

J.-P. DELAHAYE, *Merveilleux nombres premiers*, Éditions Belin/Pour la science, 2000.

H. DUBNER, *Twin Prime Conjectures*, in *J. Recreational Mathematics*, vol. 30.3, pp. 199-205, 1999-2000.

G.L. HONAKER et Ch. CALDWELL. *Palindromic Prime Pyramids. J. Recreational Mathematics*, vol. 30.3, pp. 169-176, 1999-2000. http://www.utm.edu/~caldwell/supplements

C. RIVERA, *The Prime Puzzles & Problems.* http://www.primepuzzles.net/

J. SHALLIT, *Minimal Primes*, in *J. Recreational Math*, vol. 30.2, pp. 113-117, 1999-2000.