sont généralement pas l'opposé de nombres premiers. Pire, il est presque impossible de lui faire produire des nombres positifs sans comprendre la façon dont il a été construit. Par conséquent, si vous procédez au hasard, ne soyez pas étonné de ne tomber que sur des nombres négatifs et... composés !

En considérant l'expression : $Q = 2 + (P - 2 + |P - 2|)/2$ qui vaut P quand $P > 2$ et 2 quand $P < 2$, on obtient une fonction qui est polynomiale à l'exception de l'utilisation de la valeur absolue. Cette expression « quasi polynomiale » ne donne que des nombres premiers et les donne tous, ce qui est assez remarquable. Malheureusement, elle donne 2 le plus souvent, et lui faire produire d'autres nombres premiers est aussi difficile que faire produire des nombres premiers à P : en procédant au hasard, vous tomberez presque toujours sur $Q = 2$.

En 2003, Nachiketa Gupta, de l'Université de Pennsylvanie, a étudié comment on peut produire des nombres premiers avec ce type de polynômes. Son mémoire de thèse se termine par le traitement du cas 2, c'est-à-dire par la détermination des valeurs des 26 variables qui permettent d'avoir $P = 2$.

L'existence du polynôme de Jone-Sato-Wada-Wiens, inutile en pratique, a une conséquence théorique intéressante. Il est possible de vérifier qu'un nombre n est premier en opérant au plus 87 additions et multiplications, car s'il l'est, il existe un jeu de valeurs pour les 26 variables du polynôme qui donne n.

En pratique, cependant, trouver les bonnes valeurs des 26 variables conduisant à n sera très long : contrairement à ce que pensent de nombreux mathématiciens, trouver une preuve courte est parfois un jeu inutile et maladroit.

Ce dernier point est confirmé par le résultat suivant, obtenu par des méthodes du même type. Si un système S de démonstration est donné (par exemple la théorie des ensembles de Zermelo-Fraenkel, système suffisant pour pratiquement toutes les mathématiques), alors on peut trouver un polynôme associé au système S tel que, quelle que soit la longueur de la démonstration d'une formule F de S, il existe une démonstration de l'affirmation que « F est un théorème de S » faisable en 100 additions et multiplications. Autrement dit, celui qui reste dans le système S est parfois obligé de faire de très longues démonstrations, mais celui qui calcule le polynôme associé à S dispose, lui, de la possibilité – théorique – d'établir tout résultat démontré par S à l'aide d'une série de 100 opérations arithmétiques au plus.

Ce jeu avec les polynômes a conduit récemment Christoph Baxa à écrire explicitement un polynôme à coefficients entiers dont les valeurs indiquent toutes les décimales du nombre e (ou du nombre π) qui se trouve donc codé par la donnée d'un nombre fini d'entiers.

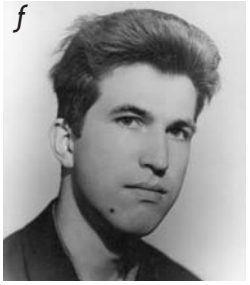
2. Le polynôme de Jones

$$P = (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2-[2n+p+q+z-e]^2$$
$$-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2$$
$$-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2$$
$$-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2$$
$$-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}$$

Des algorithmes polynomiaux

Puisque les polynômes sont des fonctions lentement croissantes (comparées aux fonctions exponentielles $n \to 2^n$, $n \to n!$, $n \to n^n$, etc.), la question de savoir s'il est difficile ou non de tester la primalité (c'est-à-dire la nature première ou non d'un entier) se formule ainsi : existe-t-il un algorithme indiquant si OUI ou NON l'entier n est un nombre premier, et dont le temps de calcul pour n est inférieur à la valeur d'un polynôme dont la variable est la longueur de l'écriture de n ? Plus brièvement : existe-t-il des tests de primalité polynomiaux ?

On a longtemps pensé que la réponse était positive, sans réussir à le démontrer. Ce n'est qu'en 2002 qu'une équipe de trois mathématiciens indiens, Manindra Agrawal, Neeraj Kayal, Nitin Saxena, a réglé le problème affirmativement en proposant un test


f


g


h


i


j

nombres premiers. T. Tao *(g)* a prouvé avec B. Green que pour tout entier k, il existe une infinité de suites arithmétiques de longueur k, composées uniquement de nombres premiers. R. Mollin *(h)* a généralisé le polynôme d'Euler et démontré, sous réserve d'une conjecture vraisemblable, que si M est un entier fixé (aussi grand qu'on le désire), il existe un entier k tel que le polynôme $n^2 + n + k$ donne des nombres premiers pour $n = 0, 1, 2, ..., M$. M. Agrawal *(i)* a prouvé avec ses collègues N. Kayal et N. Saxena qu'il existe des tests de primalité polynomiaux. Ch. Mauduit *(j)* a démontré avec J. Rivat que, dans les progressions arithmétiques de Dirichlet, il y a autant de nombres premiers dont la somme des chiffres de leur écriture décimale est paire, que de nombres premiers dont la somme des chiffres est impaire.

3. Records de progressions arithmétiques de nombres premiers

Les trois nombres premiers les plus grands en progression arithmétique :
$9\,094\,283\,341\,425 \times 2\,666\,669 - 1 + n \times 32\,289\,41\,5\,560\,495 \times 2\,666\,666$ pour $n = 0, 1, 2$.

Le premier terme possède 200 701 chiffres décimaux. Cette progression a été trouvée en mars 2011 par David Broadhurst. Il est bien sûr plus difficile de trouver quatre nombres premiers en progression arithmétique que d'en trouver trois. Il y a donc aussi un record pour quatre, cinq, etc.

Les quatre nombres premiers les plus grands en progression arithmétique :
$1\,631\,979\,959 \times 225\,000 - 1 + n \times (164\,196\,977 \times 280\,000 - 1\,631\,979\,959 \times 225\,000)$ pour $n = 0, 1, 2, 3$.

Cette progression a été trouvée en 2010 par D. Broadhurst.

Les cinq nombres premiers les plus grands en progression arithmétique :
$(82\,751\,511 + 20\,333\,209 \times n) \times 16229\# + 1$ pour $n = 0, 1, 2, 3, 4$.

La notation $k\#$ désigne le produit de tous les nombres premiers inférieurs ou égaux à k (par exemple, $7\# = 2 \times 3 \times 5 \times 7 = 210$). Cette progression a été trouvée en 2009 par Ken Davis. Plus une progression arithmétique est longue, plus elle est difficile à découvrir. Même si l'on sait, grâce au théorème de B. Green et T. Tao, qu'il existe des progressions arithmétiques de nombres premiers de toute longueur, le record actuel n'est que de 26.

La plus longue progression arithmétique de nombres premiers :
$43\,142\,746\,595\,714\,191 + 23\,681\,770 \times 23\# \times n$ pour $n = 0, 1, 2, 3, \ldots, 25$.

Cette progression de 26 termes a été trouvée en 2009 par Benoît Perichon.

Pour une liste plus complète de tels records : http://users.cybercity.dk/~dsl522332/math/aprecords.htm

BIBLIOGRAPHIE

G. Tenenbaum et M. Mendès France, **Les nombres premiers, entre l'ordre et le chaos**, Dunod, 2011.

T. Tao, **Structure and randomness in the prime numbers**, dans D. Schleicher et M. Lackmann (éds.), *An Invitation to Mathematics*, Springer-Verlag, 2011 (http://terrytao.files.wordpress.com/2009/09/primes_paper.pdf).

Ch. Mauduit et J. Rivat, **Sur un problème de Gelfond : la somme des chiffres d'un nombre premier**, *Annals of Mathematics*, vol. 171(3), pp. 1591-1646, 2010.

B. Green et T. Tao, **The primes contain arbitrarily long arithmetic progressions**, *Ann. of Math.*, vol. 167(2), pp. 481-547, 2008.

R. Crandall et C. Pomerance, **Prime Numbers : A Computational Perspective**, Springer-Verlag, 2005.

M. Agrawal *et al.*, **PRIMES is in P**, *Ann. of Math.*, vol. 160(2), pp. 781-793, 2004.

P. Ribenboim, **The Little Book of Bigger Primes**, Springer-Verlag, 2004.

M. Dietzfelbinger, **Primaly Testing in Polynomial Times**, Springer, 2004.

J.-P. Delahaye, **Merveilleux nombres premiers**, Belin/Pour la Science, 2000.

de primalité polynomial (*voir Pour la Science n° 303, janvier 2003, pages 98-103*).

Bien sûr, un algorithme dont le temps de calcul est un polynôme de degré 50 est moins intéressant qu'un algorithme dont le temps de calcul est un polynôme de degré 2. Une fois trouvé un test de primalité polynomial, le travail n'était donc pas terminé, et on a tenté d'obtenir des tests polynomiaux de degré aussi petit que possible.

L'analyse de l'algorithme des trois chercheurs indiens montre que leur test est de degré 12, ce qui est beaucoup. Mais en admettant une conjecture considérée comme probable, on établit que leur algorithme permet un test de degré 6.

On a d'abord trouvé une preuve, n'utilisant cette fois aucune conjecture, avec des polynômes de degré 11, puis 8. Une variante de l'algorithme a été proposée par Carl Pomerance et Henry Lenstra, et ils prouvèrent en 2005 que leur test est polynomial de degré 6. Une autre variante fut prouvée de degré 3, mais cette fois, sous réserve d'une conjecture assez risquée. Ce degré 3 ne doit donc pas être considéré comme acquis.

Enfin, un autre résultat établit que, sauf cas exponentiellement rares, la primalité est démontrable en temps polynomial de degré 4. On ne pense pas pouvoir faire mieux. Cela conduit à la conclusion suivante, probablement définitive : prouver qu'un entier n est premier exige un temps de calcul qui augmente comme un polynôme de degré 4 de la longueur de l'entier n auquel on s'intéresse.

Notons cependant que pour l'instant les algorithmes polynomiaux mis au point et prouvés tels ne sont pas aussi rapides que les anciens algorithmes (qui eux ne sont pas prouvés polynomiaux !). L'approche théorique n'est pas pour autant inutile, mais il faudra peut-être attendre un moment pour qu'elle ait des retombées pratiques.

Des suites arithmétiques

Abordons maintenant les suites arithmétiques de nombres premiers. Les plus simples des polynômes sont les formes linéaires : $n \to an + b$.

Nous avons vu qu'une telle expression ne donne pas des nombres premiers pour tout entier n (sauf si elle est constante et égale à un nombre premier). En revanche, il n'est pas interdit qu'elle donne une infinité de nombres premiers. L'une des plus simples questions liant nombres premiers et polynômes est ainsi celle de l'existence de paramètres a et b tels qu'il y ait une infinité de nombres premiers de la forme $an + b$ quand n prend des valeurs entières.

Bien sûr, il ne peut pas y avoir une infinité de nombres premiers de la forme $5n + 10$ puisque tout nombre de cette forme est multiple de 5 si n est entier. Plus généralement, si a et b sont multiples d'un même entier $k > 1$ (on dit qu'ils ne sont pas premiers entre eux), alors les nombres de la forme $an + b$ ne peuvent pas être premiers