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

plus de deux fois. La condition nécessaire est aussi suffisante. Si a et b sont premiers entre eux, alors il existe une infinité de nombres premiers de la forme $an + b$.

Ce célèbre résultat, conjecturé par Adrien-Marie Legendre, a été prouvé par Gustav Dirichlet en 1838. Depuis, beaucoup de travail a été fait pour préciser comment les nombres premiers se répartissent quand a est fixé et que l'on fait varier b. Par exemple, il est intéressant de comparer les nombres d'entiers premiers produits par les polynômes $4n + 1$ et $4n + 3$ quand n varie jusqu'à M.

Les deux formules sont aussi efficaces l'une que l'autre : le rapport du nombre d'entiers premiers produits par la première, sur le nombre d'entiers premiers produits par la seconde, tend vers 1 quand M tend vers l'infini. Un examen numérique de la question montre cependant que $4n + 3$ surpasse légèrement $4n + 1$. Donner un sens précis à cette domination et la prouver mathématiquement a été un long travail qui n'a abouti qu'en 1994, avec les résultats obtenus par Michael Rubinstein et Peter Sarnak, sous réserve de conjectures vraisemblables. Des détails sur ces compétitions numériques figurent dans la rubrique de mars 2010 (*Un terrain de course numérique*, *Pour la Science*, n°389, mars 2010).

Suites de Dirichlet : de beaux résultats

En 2010, Christian Mauduit et Joël Rivat, de l'Institut de mathématiques de Luminy, ont démontré un résultat attendu depuis longtemps sur les chiffres des nombres premiers dans des progressions arithmétiques de Dirichlet. L'une des conséquences, exprimée en langage simple, est la suivante : 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. Le résultat se généralise dans toute base de numération. Il est valable aussi quand on s'intéresse aux nombres premiers (en nombre infini) dont la somme des chiffres vaut 0, 1, 2, ..., $k - 1$ modulo k.

Parmi les plus beaux résultats sur les suites arithmétiques de nombres premiers, le théorème de Ben Green et Terence Tao

4. Les polynômes de degré 2 et la spirale d'Ulam

Le polynôme $n^2 + n + 41$ découvert par Euler donne des nombres premiers (distincts) pour $n = 0, 1, 2, 3, \ldots, 39$. Celui de Legendre, $n^2 - n + 41$, en donne pour $n = 1, 2, \ldots, 40$. Y a-t-il mieux ? La théorie indique que probablement oui, mais ne propose rien de concret. Ce sont les ordinateurs qui ont permis de faire mieux.

Voici ce que la recherche d'un polynôme de degré 2 donnant des suites de nombres premiers, pour des valeurs successives de sa variable, a donné.

G. Fung, 1988 : $47n^2 + 9n - 5209$ produit 43 nombres premiers, pour $n = -24, -23, \ldots, 0, 1, \ldots, 18$.

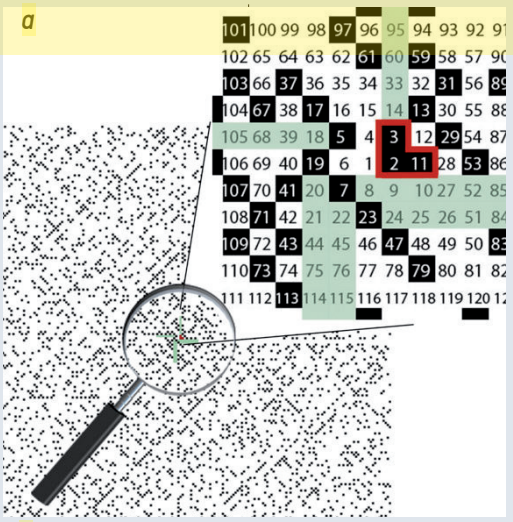
R. Ruby, 1988 : $103n^2 + 31n - 3391$ produit 43 nombres premiers, pour $n = -23, -22, \ldots, 0, 1, \ldots, 19$.

R. Ruby, 1989 : $36n^2 + 18n - 1801$ produit 45 nombres premiers, pour $n = -33, -32, \ldots, 0, \ldots, 11$.

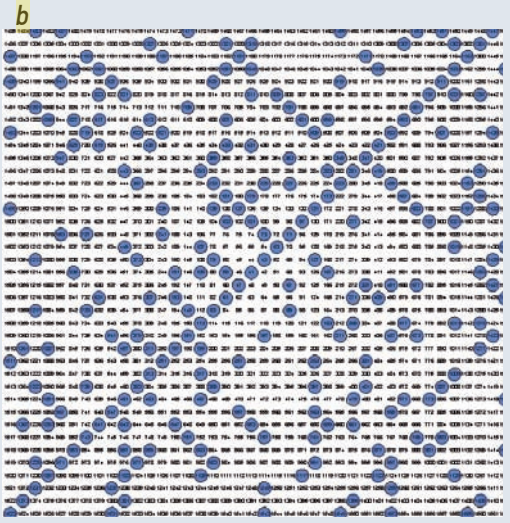
Les polynômes de degré 2 donnant beaucoup de nombres premiers expliquent en partie pourquoi dans la spirale de Stanislas Ulam *(a)* (les entiers écrits en spirale en noircissant les nombres premiers), on voit de nombreux alignements rectilignes diagonaux de points noirs. D'ailleurs, en faisant partir la spirale d'Ulam non pas de 1, mais de 41 *(b)*, les nombres premiers donnés par la formule d'Euler s'alignent.

Selon une variante de la spirale d'Ulam proposée par Jean-François Colonna, on dispose les entiers en spirale comme précédemment, puis on dessine autour de chaque entier n un cercle dont le rayon est proportionnel au nombre de diviseurs de n. Des alignements obliques apparaissent *(c)*, qui, cette fois, ne représentent plus les nombres premiers, mais les nombres ayant de nombreux diviseurs.

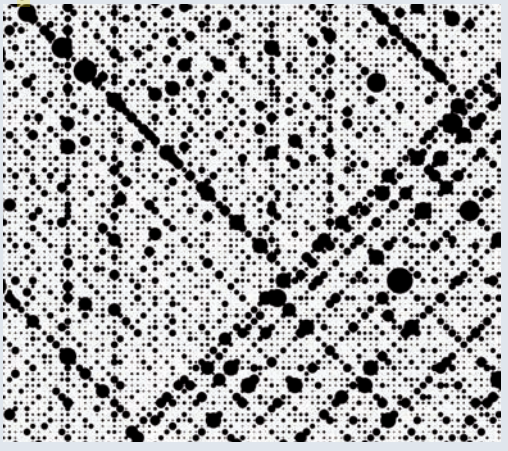
a



b



c

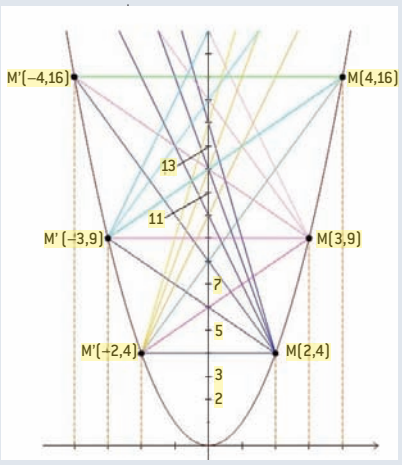


5. Un crible géométrique

Une des plus étranges façons de relier polynômes et nombres premiers a été proposée par Yuri Matiyasevich. À partir du simple polynôme $P(n) = n^2$, il explique comment un tracé de segments de droites conduit directement à l'ensemble des nombres premiers.

On part de la parabole $y = x^2$. On y repère les points d'abscisse entière ayant une valeur absolue supérieure à 2, à savoir les abscisses 2, −2, 3, −3, 4, −4, etc. Ce sont les points : M(2, 4), M'(–2, 4), M(3, 9), M'(–3, 9), M(4, 16), M'(–4, 16), etc.

On relie les points M avec les points M', ce qui donne des segments qui coupent l'axe Oy en des points d'ordonnée entière. Le segment reliant M(n, n^2) et M'(–m, m^2) coupe l'axe Oy en (0, nm). De ce fait, tous les nombres composés sont traversés par au moins deux segments. Les nombres premiers apparaissent donc sur l'axe Oy comme les points ayant une ordonnée entière et qui ne sont coupés par aucun segment. L'ensemble des nombres premiers a ainsi été déduit géométriquement du polynôme $P(n) = n^2$.



de 2004 indique que pour tout entier positif k, il existe une infinité de suites arithmétiques de longueur k composées uniquement de nombres premiers. On peut donc trouver des progressions arithmétiques de nombres premiers de toutes longueurs… cela même si on n'en connaît pour l'instant aucune de plus de 26 termes *(voir la figure 3)*.

En 2006, un perfectionnement des méthodes utilisées pour ce premier résultat a conduit T. Tao et Tamar Ziegler à l'énoncé remarquable suivant concernant les progressions polynomiales de nombres premiers : si $P_1, P_2, \ldots, P_n$ sont des polynômes sans terme constant (c'est-à-dire vérifiant $P_i(0) = 0$), alors on peut trouver un a et un b (et même une infinité de a et de b) tels que $P_1(a) + b$, $P_2(a) + b$, …, $P_n(a) + b$ soient tous des nombres premiers.

Avec $P_1(a) = a, P_2(a) = 2a, \ldots, P_n(a) = na$, on retrouve le résultat de B. Green et T. Tao qu'il existe des progressions arithmétiques de nombres premiers aussi longues qu'on le veut : $a + b$, $2a + b$, …, $na + b$.

Bien d'autres énoncés intéressants sur les suites polynomiales de nombres premiers en résultent. Par exemple, en prenant $P_1(a) = a, P_2(a) = a^2, \ldots, P_n(a) = a^n$, on obtient le résultat nouveau qu'il existe des suites de nombres premiers aussi longues qu'on le veut de la forme $a + b$, $a^2 + b$, …, $a^n + b$.

Ces résultats sont positifs : les mathématiciens savent trouver des nombres premiers ayant une forme donnée ou, au moins, réussissent à prouver qu'ils existent. Mais d'autres résultats sont moins brillants : nous restons bien ignorants des valeurs premières des polynômes les plus simples. Ainsi, bien que cela ait été conjecturé depuis longtemps, personne ne réussit à démontrer qu'il existe une infinité de nombres premiers de la forme $n^2 + 1$.

Un blocage pour $n^2 + 1$

Une conjecture de Viktor Bunyakovsky datant de 1857 affirme que, sauf si c'est impossible pour une raison simple *(voir plus bas)*, toute formule polynomiale de degré 2 engendre une infinité de nombres premiers. Selon cette conjecture, si $P(n)$ est un polynôme à coefficients entiers, alors deux cas sont possibles : *(a)* toutes ses valeurs sont multiples d'un entier $k > 1$; *(b)* $P(n)$ produit une infinité de nombres premiers.

Voyons deux exemples. Le polynôme $n^2 + n + 4$ ne donne que des nombres pairs (si n est pair, $n^2 + n + 4$ l'est aussi ; si n est impair, n^2 est impair et $n^2 + n + 4$ est alors pair), donc toutes ses valeurs sont multiples de 2 ; nous sommes dans le cas *(a)*.

En revanche, le polynôme $n^2 + 1$, pour les valeurs n = 1, 2, 3, 4, 5, donne 2, 5, 10, 17, 26 qui ne sont pas multiples d'un même nombre entier. D'après la conjecture de Bunyakovsky, nous sommes dans le cas *(b)* et le polynôme $n^2 + 1$ doit donner une infinité de nombres premiers.

Notons que la conjecture est démontrée dans le cas des polynômes de degré 1, car elle est alors équivalente au théorème de Dirichlet ; mais on ne sait la démontrer pour aucun autre polynôme. Pire, on ne sait même pas prouver que les polynômes qui, d'après la conjecture, doivent donner une infinité de nombres premiers, en donnent tous au moins un !

Parmi les cas délicats qui inquiètent sur la véracité de la conjecture, il y a le polynôme $n^{12} + 488\,669$ qui ne donne aucun nombre premier avant $n = 616\,980$.

L'AUTEUR

Jean-Paul DELAHAYE
est professeur à l'Université de Lille et chercheur au Laboratoire d'informatique fondamentale de Lille (LIFL).