## LES « PIROGUES » DU GRAND OCÉAN

***Chez les peuples les plus sauvages, ce qui a rapport à la navigation dénote un degré d'intelligence que l'on chercherait souvent en vain dans la manière dont ils bâtissent leurs habitations ou subviennent à leurs premiers besoins.***

**Amiral Pâris, 1843**

On ne se lance pas dans de grandes traversées sans embarcations sûres et rapides, remontant bien au vent. Les Océaniens avaient atteint un haut degré de perfectionnement dans l'art de la construction navale, encore en partie inégalé. Ils ont construit toutes sortes de navires, tant pour les coques que pour les gréements ou l'agencement des voilures, que l'on peut regrouper en deux catégories : les pirogues à balancier simple ou double (trimaran) et les pirogues doubles (catamarans), à l'exclusion notable de tout monocoque.

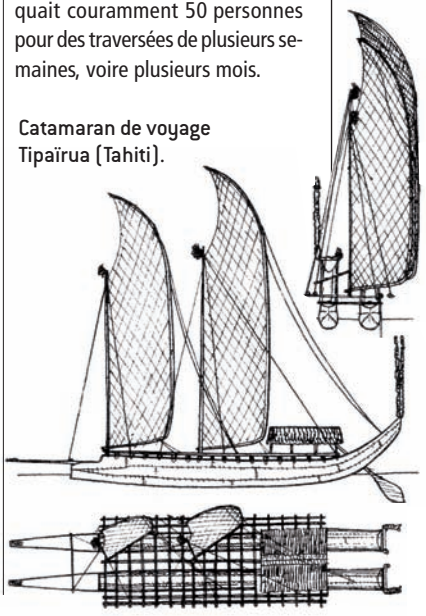
Avant l'arrivée des Européens, tous ces navires étaient construits avec des outils en pierre, le métal étant inconnu. Sur les plus grands, on assemblait les différentes pièces de bois, très soigneusement taillées, avec des cordages de coco. Le calfatage était traité par la bourre de coco enduite de gommes végétales.

Les coques étaient toutes d'une finesse et d'une légèreté inconcevables en Occident. Elles ne comportaient aucun appendice fixe sous l'eau (pas de quilles ni de gouvernail). Même avec l'usage actuel de matériaux composites, le poids des monocoques et des multicoques occidentaux modernes excède encore celui des réalisations océaniennes de longueur équivalente, notamment à cause des quilles lestées.

Les gréements étaient d'une grande variété. Il n'y avait jamais de foc, ce qui permettait des mâtures sans étai, légères et réglables. Enverguées sur au moins deux côtés, les voiles étaient en végétaux tissés assez rigides (pandanus). Leurs formes aérodynamiques permettaient dans bien des cas de dépasser la vitesse du vent. Les voiles de type aile rigide étaient les plus répandues à Tahiti au XVIII[e] siècle.

Les pirogues à balancier nommées praos volants dépassaient couramment les 20 nœuds. Certaines étaient amphidromes (capables de se déplacer dans les deux sens : avant et arrière identiques), naviguant toujours balancier au vent, avec des coques souvent dissymétriques sur le plan longitudinal pour contrer les effets de la dérive.

Les pirogues doubles étaient constituées soit de deux coques identiques (navire monodrome), soit de deux coques de tailles différentes (navire amphidrome). Les coques étaient proches l'une de l'autre pour bénéficier d'un effet d'accélération de la veine fluide entre les coques. L'équipage et les passagers vivaient sur la plateforme au ras de l'eau, sans aucune protection particulière. Les grands catamarans de voyage mesuraient entre 15 et 25 mètres, parfois plus de 30 mètres. On embarquait couramment 50 personnes pour des traversées de plusieurs semaines, voire plusieurs mois.



**Catamaran de voyage Tipaïrua (Tahiti).**

l'observation directe : l'étoile n'est pas exactement dans la direction de l'île, le vent et le courant entraînent des dérives, l'azimut de l'astre varie au cours du temps, etc. La ligne directe entre le départ et l'île est connue, et l'art du pilote consiste à apprécier l'écart entre cette direction théorique et la route réelle, lorsqu'il navigue face au vent en tirant des bords. Il utilise notamment des astres guides à tribord et à bâbord, qui servent de garde-fous lorsque des nuages masquent les étoiles de l'avant ou de l'arrière. Le pilote expérimenté sait aussi reconnaître un astre qui apparaît seul au milieu d'un ciel voilé et l'utiliser pour maintenir son cap.

Certaines pratiques se sont perpétuées, mais leur secret est bien gardé. Par exemple, on utilise encore en Micronésie une méthode de navigation fort ancienne, caractérisée par le fractionnement de la route à suivre en plusieurs segments successifs, dénommés *etak*. Le navigateur a recours à un point de référence, réel ou imaginaire, situé au large de sa route. Ce point sert d'axe autour duquel pivotent les différents repères directionnels qu'il va successivement utiliser. Le premier azimut de référence du voyage est celui qui relie le point de départ à une certaine étoile se levant à l'horizon, en passant par le point pivot. À la fin du premier segment de route – *etak* –, le navigateur verra une deuxième étoile se lever à l'horizon, dans l'alignement du point de référence, et ainsi de suite.

Pour mémoriser ces routes maritimes, les navigateurs ont associé à chaque *etak* des images de la vie en mer – un banc de thons jaunes, un vol de frégates, un croisement de houles… L'ensemble constitue un récit de voyage ponctué d'événements réels ou imaginaires. Simplifiés et chantés en cœur par les équipages, ces récits rythment les efforts et marquent les principaux changements de cap, sans dévoiler aux non-initiés les secrets de la route maritime…

### BIBLIOGRAPHIE


E. Desclèves, **Le peuple de l'Océan,** L'Harmattan, 2010.

M.-F. Péteuil, **Ciel d'îles,** *Journal de la Société des Océanistes*, 2003.

B. Finneys, **Voyagers into Ocean Space,** University of California Press, 1985.

J. Neyret, **Pirogues océaniennes,** Association des amis du musée de la Marine, 1976.

D. Lewis, **We, the Navigators,** University of Hawaï, 1972.

E. Dodd, **Polynesian Seafaring,** Dodd, Mead & Company, 1972.

A. Gerbault, **Un paradis se meurt,** Self, 1949.

LOGIQUE & CALCUL

# La maîtrise des nombres premiers

*Comme l'eau et le feu, les polynômes et les nombres premiers se rencontrent et donnent naissance à un violent bouillonnement... mathématique.*

**Jean-Paul DELAHAYE**

Les polynômes, tels $n \to 2n + 1$, $n \to n^2$, $n \to 5n^3 - 35n^2 + 11$, etc., sont les plus simples des fonctions. Ils représentent l'« ordre mathématique » et ce qui se calcule facilement. Parfois, ils servent d'échelle pour mesurer la difficulté des problèmes.

Les nombres premiers (2, 3, 5, 7, 11, 13, 17, ...) se situent à l'opposé : ce sont des êtres mathématiques délicats, récalcitrants, incontrôlables, et dont la nature ne sera sans doute jamais entièrement élucidée. Il en résulte que la confrontation entre polynômes et nombres premiers ne peut que produire des idées stimulantes et soulever des problèmes passionnants et difficiles. C'est à ces sujets et à certains résultats nouveaux que nous consacrons cette rubrique.

Existe-t-il une formule polynomiale donnant les nombres premiers ? Une telle formule ne peut donner tous les nombres premiers, ni même ne donner *que* des nombres premiers. Les mathématiciens ont en effet démontré que : *Si un polynôme P(n) à coefficients entiers n'est pas constant, alors il existe une infinité de valeurs entières de n telles que P(n) n'est pas un nombre premier.*

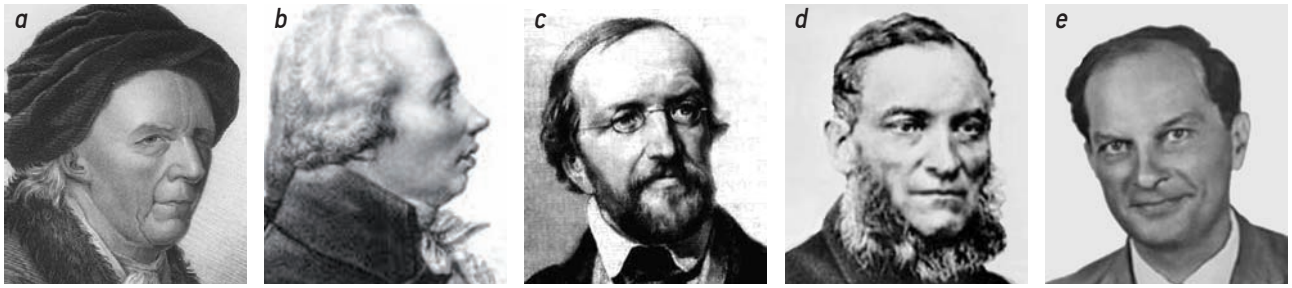
Plus puissant, le résultat qui suit, démontré par Robert Buck en 1946, enlève tout espoir de faire produire uniquement des nombres premiers à une fonction polynomiale ou même à un quotient de fonctions polynomiales : *Si un quotient de deux polynômes à coefficients entiers P(n)/Q(n) donne des nombres dont la valeur absolue est première pour les valeurs entières de n, alors P(n)/Q(n) est constant...* et donc sans intérêt.

## Un polynôme qui fait illusion

Ces résultats et quelques autres du même type montrent que les polynômes sont trop simples pour engendrer les nombres premiers. Ils ne contredisent pas le résultat suivant : le polynôme P de degré 25 à 26 variables *(voir la figure 2)* est tel qu'il y a identité entre l'ensemble des valeurs positives qu'il prend pour des valeurs entières de ses variables et l'ensemble des nombres premiers. En bref : ses valeurs positives sont les nombres premiers.

Ce polynôme construit en 1976 par James Jones, Daihachiro Sato, Hideo Wada et Douglas Wiens résulte du codage de la définition de l'ensemble des nombres premiers sous la forme d'un système d'équations, qui ensuite a été réduit à une seule équation. De tels codages sont possibles pour tous les ensembles de nombres dont on connaît un algorithme qui en calcule les éléments les uns après les autres. On sait produire ces polynômes grâce aux méthodes que Yuri Matiyasevich a élaborées pour la résolution du dixième problème de Hilbert et qui a conduit à l'affirmation : *Il n'existe aucun algorithme général pour connaître les solutions entières des équations de la forme* P = 0, *où* P *est un polynôme à coefficients entiers d'une ou plusieurs variables.*

Malheureusement, le polynôme de 1976 produit aussi des nombres négatifs qui ne




**1. CONTRIBUTEURS** à la théorie des nombres premiers mettant en jeu des polynômes. L. Euler (1707-1783, *a*) a montré que le polynôme $n^2 + n + 41$ donne des nombres premiers pour $n = 0, 1, 2, ..., 39$. A.-M. Legendre (1752-1833, *b*) s'est intéressé à $n^2 - n + 41$, qui donne des nombres premiers pour $n = 1, 2, ..., 40$. G. Dirichlet (1805-1859, *c*) a démontré le résultat conjecturé par Legendre : si *a* et *b* sont premiers entre eux, il existe une infinité de nombres premiers de la forme $an + b$. V. Bunyakovsky (1804-1889, *d*) a conjecturé que, sauf pour les cas faciles à repérer, toute formule polynomiale de degré 2 engendre une infinité de nombres premiers. S. Ulam (1909-1984, *e*) a trouvé des spirales où les alignements correspondent aux suites de nombres premiers. Y. Matiyasevich *(f)* a montré comment produire des polynômes dont les valeurs positives sont des

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 $\pi$) 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


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

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 $n = -24, -23, \ldots, 0, 1, \ldots, 18$.

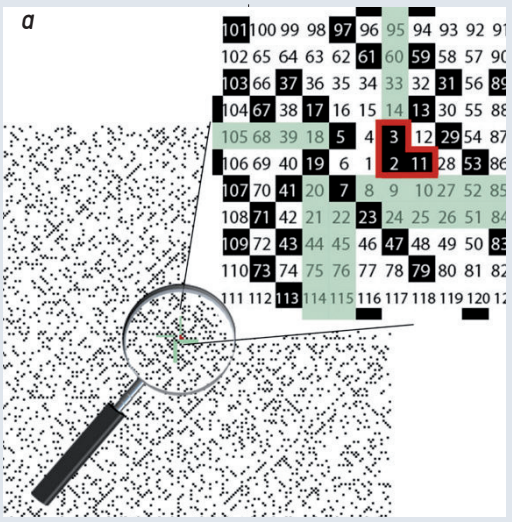
R. Ruby, 1988 : $103n^2 + 31n - 3391$ produit 43 nombres premiers, pour $n = -23, -22, \ldots, 0, 1, \ldots, 19$.

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

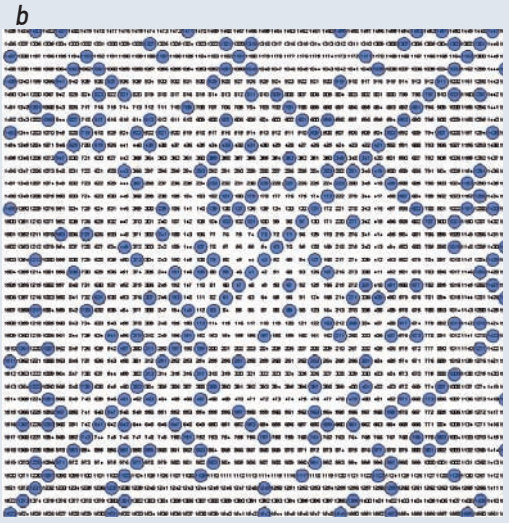
Les polynômes de degré 2 donnant beaucoup de nombres premiers expliquent en partie pourquoi dans la spirale de Stanislas Ulam *(a)* (les entiers écrits en spirale en noircissant les nombres premiers), on voit de nombreux alignements rectilignes diagonaux de points noirs. D'ailleurs, en faisant partir 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.

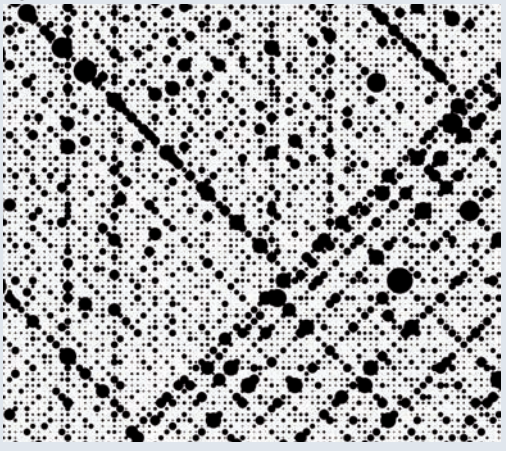
*a*




*b*



*c*

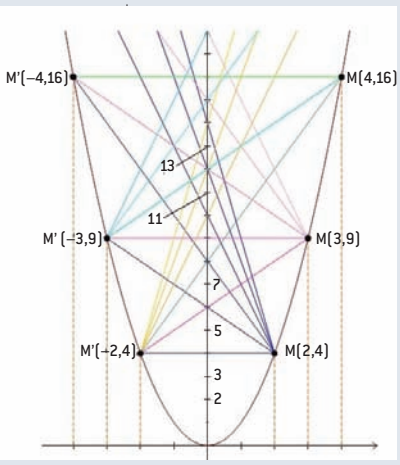


## 5. Un crible géométrique

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 $a + b, a^2 + b, \ldots, a^n + b$.

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).

À l'origine de beaucoup de ces travaux se trouve la remarque formulée en 1772 par Euler que le polynôme $n^2+n+41$ donne des nombres premiers pour $n = 0, 1, 2, 3, ..., 39$. Legendre proposa en 1798 le polynôme $n^2-n+41$ qui donne des nombres premiers pour $n = 1, ..., 40$. Dans les deux cas, on a 40 valeurs consécutives d'un polynôme de degré 2 produisant un nombre premier.

Le polynôme d'Euler a l'avantage, sur celui de Legendre, qu'il peut se généraliser d'une étonnante manière. Richard Mollin a en effet prouvé que si $M$ est un entier fixé (aussi grand qu'on le veut), il existe un entier $k$ tel que le polynôme $n^2 + n + k$ donne des nombres premiers pour $n = 0, 1, 2, ..., M$. Autrement dit, si vous voulez un polynôme de degré 2 qui donne un million de nombres premiers quand la variable $n$ va de un à un million, c'est possible et le polynôme peut avoir la forme très simple $n^2 + n + k$.

On doit formuler plusieurs réserves sur ce beau résultat de R. Mollin. Une fois encore, elles nous font prendre conscience que l'écart entre la théorie et la pratique est parfois très grand. D'une part, le résultat de R. Mollin est démontré en utilisant une conjecture assez forte qui généralise la conjecture des nombres premiers jumeaux (celle-ci affirme qu'il existe une infinité de paires de nombres premiers espacés de 2, comme 11 et 13, 17 et 19, 41 et 43). Cette conjecture, même si elle est vraisemblable et bien testée expérimentalement, ne semble pas à la portée des mathématiques d'aujourd'hui et le résultat de R. Mollin reste donc incertain.

D'autre part, la constante $k$ qu'il faut utiliser dans la définition du polynôme $n^2+n+k$ prend des valeurs considérables si l'on veut que le polynôme donne beaucoup d'entiers premiers : pour obtenir plus de 40 nombres premiers, $k$ doit dépasser $10^{18}$. Enfin, et c'est le pire, la méthode de démonstration utilisée par R. Mollin n'est pas constructive : elle ne permet pas en pratique de trouver $k$ !

Pour pallier ce défaut de la théorie qui nous suggère que sont vraies certaines choses qu'elle ne sait pas montrer, d'autres mathématiciens s'occupent de trouver « pour de vrai » des polynômes qui produisent beaucoup de nombres premiers. Leurs résultats, obtenus bien sûr à l'aide d'astucieux programmes informatiques et de longues heures de calcul, sont de nature variée : recherche de longues progressions arithmétiques de nombres premiers, recherche de polynômes de bas degré donnant beaucoup de valeurs premières consécutives ou une grande proportion de nombres premiers dans un intervalle, etc.

Comme ils ne réussissent pas à trouver de polynôme de degré 2 donnant plus de 43 nombres premiers différents pour des valeurs successives de $n$, les mathématiciens ont essayé avec des polynômes de degré 3 ou plus.

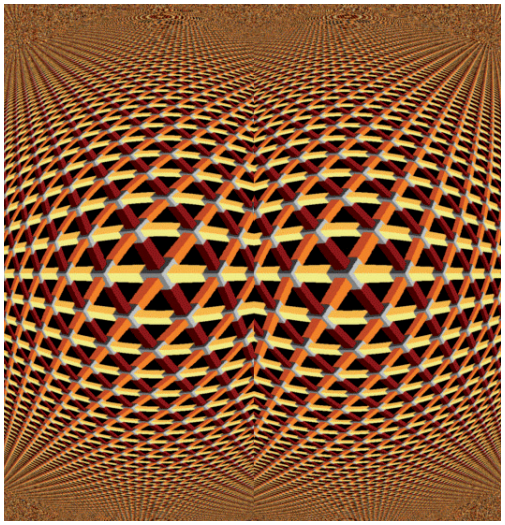
## Au-delà du degré 2

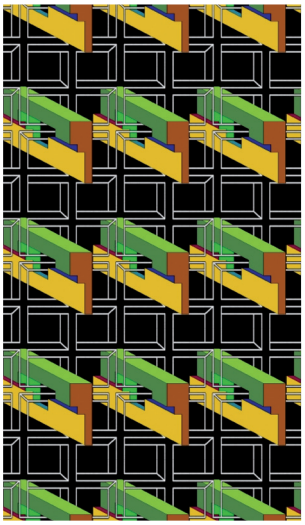
De nombreux records sont dus à F. Dress et B. Landreau. Pour le degré 3, le polynôme $66n^3 + 83n^2 + 13\,735n + 30139$ donne 46 nombres premiers différents pour $n = -26, -25, ..., 0, 1, ..., 18, 19$ (record en 2000). Degré 4, record en 2002 : le polynôme $3/4n^4+1/2n^3-4\,323/4n^2+34\,415/2n-62\,099$ donne 49 nombres premiers différents pour $n = -16, -15, ..., 31, 32$. Degré 5, record en 2002 : le polynôme $1/4n^5+1/2\,n^4-345/4\,n^3 + 879/2\,n^2 + 17\,500\,n + 70\,123$ donne 57 nombres premiers différents, pour $n = -27, -26, ..., 28, 29$. Degré 6, record en 2010 : $1/72\,n^6 + 1/24\,n^5 - 1\,583/72\,n^4 - 3\,161/24\,n^3 + 200807/36\,n^2 + 97973/3\,n - 11\,351$ donne 58 nombres premiers différents, pour $n = -45, -44, ..., 11, 12$. C'est le record absolu pour un polynôme de petit degré.

En augmentant le degré, on sait de façon certaine, grâce à un théorème de Lagrange, que l'on pourra obtenir des polynômes donnant autant de nombres premiers différents que l'on veut pour des valeurs consécutives de la variable.

Les mathématiciens combinent deux notions mathématiques difficilement miscibles et découvrent un trésor de problèmes et de résultats, quelques joyaux de pure théorie... et parfois des théorèmes illusoires. Ce trésor s'enrichit des trouvailles autorisées par les calculs colossaux sur ordinateur qui guident les mathématiciens dans leur exploration du monde des entiers.

### FIGURES IMPOSSIBLES ET INFINIES





À la suite de l'article de mai 2011, Jean-François Colonna m'a proposé de nouveaux dessins infinis et impossibles *(ci-dessus à droite)*, dont plusieurs autostéréogrammes. Il me signale qu'il avait conçu l'idée des dessins impossibles infinis dès 1974 et en avait réalisé quelques-uns (voir son site Internet http://www.lactamme.polytechnique.fr/). Dominique Caudron m'a aussi envoyé des images impossibles infinies intéressantes. Il a en particulier réalisé le stéréogramme ci-dessus, à gauche, d'une figure infinie impossible (voir son site http://oncle.dom.pagesperso-orange.fr/art/index.htm).

ART & SCIENCE

# Donner à voir les mathématiques

*Une exposition se propose de rendre perceptibles les mathématiques et l'esprit de ceux qui les font : pour cela, mathématiciens et artistes se sont associés pour transformer des idées abstraites en œuvres d'art.*

**Loïc MANGIN**

Comment rendre compte des mathématiques ? Comment concilier l'art avec la pensée abstraite des mathématiciens ? Comment représenter leurs idées, leurs intuitions, leur création ? La *Fondation Cartier pour l'art contemporain*, à Paris, à travers son directeur, Hervé Chandès, a voulu relever le défi. Il s'est tourné vers un lieu d'excellence de cette discipline, l'Institut des hautes études scientifiques (IHÉS), à Bures-sur-Yvette, pour réfléchir à une façon artistique d'exposer les mathématiques en restant au plus près d'elles. Il s'agissait d'instaurer un dialogue entre artistes et mathématiciens. Le résultat de cette collaboration est l'exposition *Mathématiques, un dépaysement soudain*, un titre qui reprend une expression du mathématicien Alexandre Grothendieck.

Six mathématiciens ont accepté de se prêter à l'exercice : sir Michael Atiyah, Alain Connes, Nicole El Karoui, Mikhaïl Gromov, Don Zagier et Cédric Villani. Les artistes sollicités, des habitués de la *Fondation Cartier*, sont les cinéastes Raymond Depardon, Claudine Nougaret et David Lynch, la chanteuse Patti Smith, la peintre Beatriz Milhazes, le plasticien Jean-Michel Alberola et, enfin, le photographe et sculpteur Hiroshi Sugimoto. Voyons comment ce dernier s'est emparé des mathématiques à travers une sculpture *(voir la figure a)* et une photographie *(voir la figure b)*.

Il échange depuis 2004 avec Jean-Pierre Bourguignon, directeur de l'IHÉS et commissaire de l'exposition à venir (avec l'astrophysicien Michel Cassé). À cette époque, H. Sugimoto présentait une série de 19 photographies prises au musée de l'Université de Tokyo. J.-P. Bourguignon avait rédigé les notices de chacune d'elles. De fait, certaines représentent des modèles stéréométriques en plâtre destinés à faciliter la visualisation de fonctions mathématiques complexes. Man Ray avait fait de même au début du XX$^{e}$ siècle avec des objets conservés à l'Institut Henri Poincaré, à Paris.

**Hiroshi Sugimoto sculpte avec des outils perfectionnés, tels des robots, pour accéder à la rigueur mathématique.**

H. Sugimoto ne fait pas que photographier les objets mathématiques, il les sculpte aussi, à plus grande échelle. Pour ce faire, il utilise les outils perfectionnés d'aujourd'hui, tels des robots, pour coller au mieux à la précision et à la rigueur mathématiques du modèle. L'observation de la photographie et de la sculpture (de trois mètres de hauteur) révèle la différence. Le modèle mathématique illustré *via* ces deux médiums est une surface à courbure constante négative. Cet objet est défini par trois équations *(voir la figure c)* où $x$, $y$ et $z$ définissent l'objet dans l'espace à trois dimensions de la même façon que l'on peut définir une sphère (une surface) dans l'espace. Les paramètres $u$ et $v$ correspondent aux coordonnées nécessaires pour se repérer sur cette surface ; ils sont équivalents à la latitude et à la longitude utilisées sur une sphère.

Cette surface est la représentation d'une géométrie dite hyperbolique, car sa courbure est négative en tout point. Cela se traduit, pour tout triangle donné, à une somme des angles inférieure à 180 degrés. Rappelons que sur un plan euclidien, cette somme est égale à 180 degrés et que sur une surface à courbure positive, par exemple sphérique, elle est supérieure à 180 degrés.

Que pourra-t-on voir encore ? À partir de la bibliographie de Henri Poincaré, J.-M. Alberola a conçu une carte du ciel mathématique où des « constellations » réunissent des références partageant des thèmes communs. D. Lynch a mis en scène le rez-de-chaussée du bâtiment à partir d'une intense correspondance avec M. Gromov. Ce dernier a notamment proposé l'idée d'une bibliothèque « idéale » rassemblant un choix personnel de livres, des classiques de l'Antiquité à ceux plus récents, tels les ouvrages de Richard Feymann. Sur une idée d'A. Connes, R. Depardon et Cl. Nougaret ont filmé plusieurs mathématiciens qui, en quatre minutes, expliquent leur rapport aux mathématiques, leurs idées… Et bien d'autres choses qui permettront d'accéder à la magie des mathématiques à travers l'esthétique ! ■

***Mathématiques, un dépaysement soudain,*** *à la Fondation Cartier, du 21 octobre 2011 au 19 février 2012. http://fondation.cartier.com*