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.

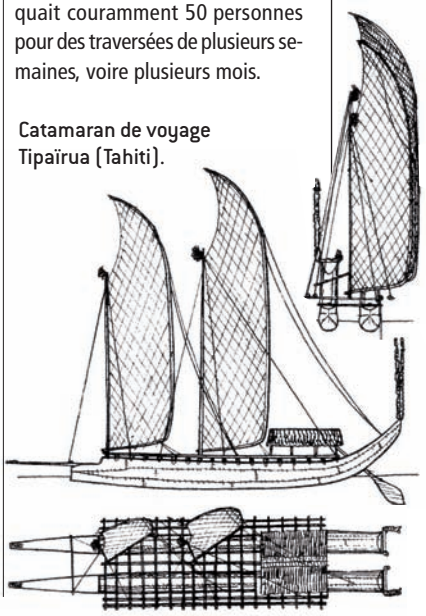
Avant l'arrivée des Européens, tous ces navires étaient construits avec des outils en pierre, le métal étant inconnu. Sur les plus grands, on assemblait les différentes pièces de bois, très soigneusement taillées, avec des cordages de coco. Le calfatage était traité par la bourre de coco enduite de gommes 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 π) qui se trouve donc codé par la donnée d'un nombre fini d'entiers.

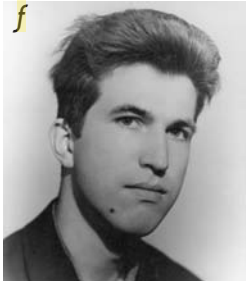
2. Le polynôme de Jones

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

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 $n = 0, 1, 2, \ldots, M$. 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.