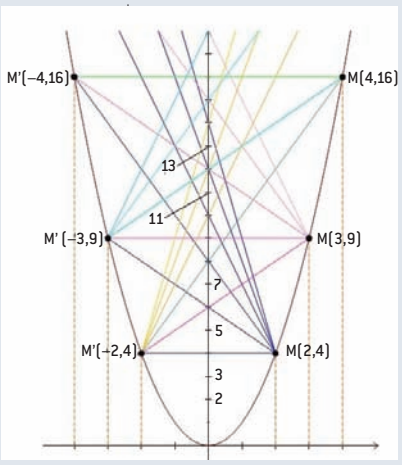
5. Un crible géométrique

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.

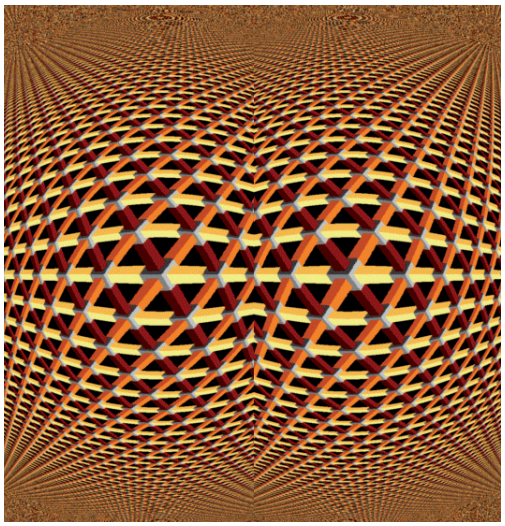
Au-delà du degré 2

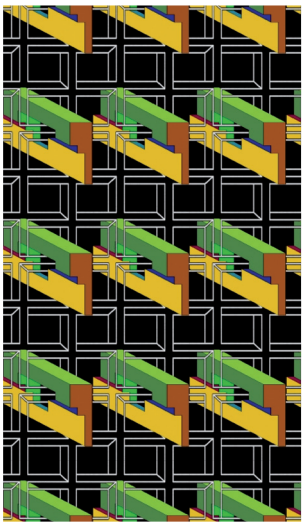
De nombreux records sont dus à F. Dress et B. Landreau. Pour le degré 3, le polynôme $66n^3 + 83n^2 + 13\,735n + 30139$ donne 46 nombres premiers différents pour $n = -26, -25, ..., 0, 1, ..., 18, 19$ (record en 2000). Degré 4, record en 2002 : le polynôme $3/4n^4+1/2n^3-4\,323/4n^2+34\,415/2n-62\,099$ 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).