5. ATTENTION AUX GÉNÉRALISATIONS HÂTIVES

De nombreuses fois dans l'histoire des mathématiques, des propriétés constatées sur un petit nombre de cas ont été conjecturées «vraies dans tous les cas». Voici quelques exemples de situations qui montrent qu'il faut se méfier de telles généralisations.

(a) Pierre de Fermat considère l'expression $F_n = 2^{2^n}+1$ et, après le calcul de F_0, F_1, F_2, F_3, F_4, constate qu'il s'agit toujours de nombres premiers. Il en tire la conjecture que F_n est toujours un nombre premier. Le grand Leonhard Euler découvre plus tard que F_5 n'est pas premier. Pire : aujourd'hui, après avoir évalué et testé les valeurs suivantes de F_n, on n'a trouvé que des nombres composés. On se demande donc si, au-delà de F_5, tous les F_n ne seraient pas composés ! Si c'est le cas, ce sera l'exemple extrême de la conjecture fausse : non seulement elle possède un contre-exemple, mais tout nombre plus grand que 5 est un contre-exemple !

(b) Plus récemment, on a remarqué que :

3! – 2! + 1! = 5 : premier
4! – 3! + 2! – 1! = 19 : premier
5! – 4! + 3! – 2! + 1! = 101 : premier
6! – 5! + 4! – 3! + 2! – 1! = 619 : premier
7! – 6! + 5! – 4! + 3! – 2! + 1! = 4 421 : premier
8! – 7! + 6! – 5! + 4! – 3! + 2! – 1! = 35 899 : premier

En conclut-on que $n!$ – $(n–1)!$ + ... + $(–1)^n$ 2! – $(–1)^n$ 1! est toujours un nombre premier ?

Non : 9! – 8! + 7! – 6! + 5! – 4! + 3! – 2! + 1! = 326 981 = 79 × 4 139.

(c) Plus étonnant encore est l'exemple suivant. Les nombres n^{17} + 9 et $(n + 1)^{17}$ + 9 n'ont pas de facteurs communs si n = 1, n = 2, n = 3, etc. Vous pouvez vérifier cela jusqu'à 100, jusqu'à 1 000, jusqu'à un milliard, jusqu'à mille milliards de milliards, et même jusqu'à huit millions de milliards de milliards de milliards de milliards de milliards. Pourtant, un peu plus loin, pour :

n = 8 424 432 925 592 889 329 288 197 322 308 900 672 459 420 460 792 433 ≃ 8,424 10^{52}, vous rencontrerez une exception : parfois n^{17} + 9 et $(n+1)^{17}$ + 9 ont des facteurs communs.

(d) Il est des situations plus étranges encore, où seul le raisonnement permet de savoir qu'une propriété toujours testée vraie en pratique est fausse en général.

L'exemple le plus connu est celui qui concerne l'approximation de Pi*(m)* le nombre de nombres premiers inférieurs à m. On sait que ce nombre vaut à peu près :

$$\mathrm{Li}(m) = \int_2^m 1/\log(x)\,dx\ .$$

On constate en pratique que Pi*(m)* ≤ Li*(m)*, et l'on ne connaît aucune exception à cette inégalité. Cependant le mathématicien Littlewood a prouvé en 1914 que la quantité Pi*(m)* – Li*(m)* changeait de signe une infinité de fois, et donc qu'il n'est pas vrai que Pi*(m)* ≤ Li*(m)* pour tout m. En 1933, S. Skewes a établi que le premier changement de signe se produit avant $10^{10^{10^{34}}}$ (quatre niveaux d'exposant). Cette majoration a été améliorée par H. te Riele, en 1987, par 10^{371}, mais c'est encore au-delà de ce qu'on peut atteindre numériquement : aujourd'hui, on sait qu'il existe un m tel que Pi*(m)* > Li*(m)*, mais on n'en connaît aucun.

```
    if d*d>p then k:=k+1;fi;
   od;
   p;
  fi;
 end:
```

Ce qui tient sur cinq lignes :

```
premier := proc(n) local p,k,d;if n=1 then 2 else p:=1;k:=1;while k<>n do p:=p+2;d:=2;while(d*d<=p)and(p mod d <> 0)do d:=d+1;od;if d*d>p then k:=k+1;fi;od;p;fi;end;
```

Explications : proc est un mot convenu pour indiquer qu'on définit une procédure, c'est-à-dire une fonction ; local sert à préciser les variables qu'on utilisera dans le calcul ; if C then A1 else A2 fi est la structure de contrôle qui, lorsque la condition C est satisfaite, exécute l'action A1 et qui, sinon, exécute l'action A2 ; while C do A od est la structure de contrôle qui, tant que la condition C est satisfaite, exécute de manière répétée l'action A ; end indique la fin de la définition de la procédure.

Le programme, si n vaut 1, donne 2. Sinon, en parcourant les entiers de 2 en 2 (variable p), le programme recherche les nombres premiers et les compte avec la variable k, jusqu'à en avoir trouvé n. Le programme rend alors le résultat p, qui à cet instant, contient bien le n-ième nombre premier.

On peut faire encore plus court, mais cette définition possède plusieurs avantages sur la définition mathématique précédente de p_n ou sur une définition plus courte en Maple : elle se comprend immédiatement pour qui possède quelques connaissances du langage Maple, elle est fondée sur l'idée la plus naturelle qu'on puisse avoir ; elle permet de calculer en quelques secondes le centième nombre premier, et même le millième.

La recherche de formules n'utilisant qu'un symbolisme mathématique limité est un jeu un peu gratuit que les mathématiciens professionnels regardent le plus souvent avec amusement sans le prendre au sérieux (ce qui n'empêche pas que d'éminents mathématiciens comme G. Hardy ou E. Wright s'y soient adonnés).

6. FORMULES SIMPLES DONNANT DE GRANDES QUANTITÉS DE NOMBRES PREMIERS

Certaines formules, sans donner tous les nombres premiers, ni même ne donner que des nombres premiers, en donnent une grande quantité en suivant. C'est le cas de la formule d'Euler $f(n) = n^2 – n + 41$, qui donne des nombres premiers pour toutes les valeurs de n allant de 0 à 40.

Les polynômes suivants battent le record d'Euler :

$103n^2 – 3945n + 34381$ est premier pour n = 0, 1, ..., 42 (R. Ruby).

$47n^2 – 1701n + 10181$ est premier pour n = 0, 1, ..., 42 (G. Fung).

$36n^2 – 810n + 2753$ est premier pour n = 0, 1, ...,44 (R. Ruby).

Une conjecture très vraisemblable (car liée à une autre bien testée) est qu'aussi grand que soit A on peut trouver un polynôme de la forme $n^2 + n + B$ qui donne des nombres premiers pour n = 0, ..., A. On sait cependant que B sera nécessairement très grand : la valeur de B correspondant à A = 41 est plus grande que 10^{18}, mais reste inconnue.

7. a^b EST DIOPHANTIEN

La découverte de Matiiassevitch en 1970, qui résout le dixième problème de Hilbert, fut le couronnement d'une longue série de progrès commencée par la formulation, dans les années 1930, d'une définition de la notion générale d'algorithmes par A. Church et A. Turing : pour démontrer qu'aucun algorithme ne peut traiter le problème des équations diophantiennes, il faut d'abord disposer d'une définition satisfaisante de la notion d'algorithme !

De nombreuses avancées conduisirent à une situation en 1970 où, pour établir l'indécidabilité du dixième problème de Hilbert, seule restait à prouver que a^b est diophantien, c'est-à-dire qu'il existe une équation $P(a, b, c, x_1, x_2,..., x_n) = 0$, P polynôme, possédant des solutions entières $x_1, x_2,..., x_n$, si et seulement si $a^b = c$.

Ce problème en apparence élémentaire est en fait extrêmement difficile. Comme le caractère diophantien de a^b entraîne l'existence d'un polynôme dont les valeurs positives sont les nombres premiers – chose jugée invraisemblable à l'époque – nombreux furent les mathématiciens (dont le grand logicien polonais Alfred Tarski) qui concluaient à tort que a^b n'était pas diophantien.

Le jeune mathématicien Youri Matiiassevitch, alors chercheur à l'Institut Sketlov de Leningrad, travailla avec obstination plusieurs années de suite sur la preuve du caractère diophantien de l'exponentielle. Il crut avoir trouvé une solution, mais, au moment même où il en faisait l'exposé devant ses collègues, il découvrit une erreur. Enfin il trouva seul une solution, au début du mois de janvier 1970. Quelques jours avant sa découverte, absorbé dans des pensées qui allaient résoudre un problème vieux de 70 ans, il avait quitté la soirée de fête du Nouvel An en enfilant par distraction le manteau de son oncle, d'une taille franchement inadéquate...

LE DIXIÈME PROBLÈME DE HILBERT

Pourtant ce sont les mathématiciens professionnels, à l'occasion d'un défi lancé par David Hilbert en 1900, qui ont obtenu le plus surprenant résultat concernant les formules simples définissant l'ensemble des nombres premiers.

Le problème posé par David Hilbert en 1900 (parmi 23 problèmes) était de trouver une méthode générale et systématique pour étudier les équations diophantiennes, c'est-à-dire les équations polynomiales à coefficients entiers, comme l'équation $X^2 + Y^3 = Z^5$. On savait que la recherche des solutions entières de ce type d'équations était difficile ; Hilbert pensait d'ailleurs qu'aucune méthode systématique n'existait. La démonstration de cette conjecture sera terminée en 1970 par le mathématicien Youri Matiiassevitch, qui prouva qu'une certaine équation polynomiale paramétrée ne pouvait pas être résolue pour toutes les valeurs de ses paramètres à l'aide d'une seule méthode (autrement dit, à l'aide d'un seul algorithme).

Le travail fait pour élaborer cette équation aboutissait à une autre conclusion remarquable : à tout ensemble de nombres entiers dont les éléments peuvent être énumérés par un programme (l'ensemble des nombres premiers en est un) correspond une fonction polynôme dont les valeurs positives, lorsque les variables prennent des valeurs positives, constituent exactement les éléments de cet ensemble. Il existe donc une fonction polynôme (à plusieurs variables) qui, lorsque les variables prennent des valeurs positives, prend des valeurs positives et négatives, l'ensemble de celles qui sont positives étant exactement l'ensemble des nombres premiers.

Cela ne contredit pas les énoncés cités au début, qui indiquaient seulement que ne pouvait exister une fonction polynôme à plusieurs variables qui, lorsque ses variables prennent des valeurs positives, ne prend que des valeurs positives, l'ensemble des valeurs prises étant exactement l'ensemble des nombres premiers.

L'écart entre le résultat positif et le résultat négatif est mince comme une feuille de papier à cigarette et, à vrai dire, a profondément étonné les mathématiciens. Il fallut sept ans pour que le polynôme dont l'existence résulte du résultat de Matiiassevitch soit élaboré explicitement et publié en 1976 par J. Jones, D. Sato, H. Wada et D. Wiens. Le voici :

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

Quand les 26 variables $a,b,c,...,z$ prennent toutes les valeurs de l'ensemble des nombres entiers positifs, l'expression prend des valeurs positives et négatives. L'ensemble des valeurs positives prises est l'ensemble des nombres premiers.

L'éminent mathématicien soviétique You Linnik, à qui un collègue apprenait l'existence de ce polynôme inattendu, s'écria : «C'est merveilleux, très bientôt nous allons sans doute apprendre une quantité de choses nouvelles sur les nombres premiers.» On lui précisa alors qu'il existait un polynôme analogue pour tout ensemble de nombres énumérables par programme. «C'est lamentable, dit alors Linnik. Très probablement nous n'allons rien apprendre de nouveau sur les nombres premiers.»

Il est vrai que le polynôme est très décevant, car il ne prend que très rarement des valeurs positives (les seules intéressantes !) et, à moins d'étudier soigneusement la façon dont il a été construit, on ne réussit à tirer aucun nombre premier de ce polynôme qui, en théorie, les donne tous ! Il y a quelques années, je l'avais mentionné dans cette chronique, et plusieurs lecteurs m'avaient fait part de leur désillusion et même de leur doute concernant les propriétés annoncées. Je veux les rassurer : il n'y a aucune erreur, le polynôme possède bien les propriétés annoncées, mais il n'est pas plus utile pour calculer les nombres premiers que la formule de Willans. Les formules vraiment utiles, répétons-le, correspondent à des programmes et, parce qu'on ne leur impose pas un carcan artificiel par limitation du symbolisme, sont efficaces.

Jean-Paul DELAHAYE est professeur à l'Université de Lille. e-mail : delahaye@lifl.fr

Une feuille de calcul *Maple* associée à cet article, rédigée par Eric Wegrzynowski, est mise à la disposition des lecteurs à l'adresse : http:/ /www.lifl.fr/ ~wegrzyno/ FormPrem.html.

C. BOXA, *A Note on Diophantine Representation*, in *The American Mathematical Monthly*, pp. 138-143, février 1993.

C. CALDWELL, *The Prime Pages*. http:/ /www.utm.edu/ research/ primes/ .

G. HARDY et E. WRIGHT, *An Introduction to the Theory of Numbers*, Oxford Science Publications, Clarendon Press, Oxford, cinquième édition, 1979.

Y. MATIIASSEVITCH, *Le dixième problème de Hilbert. Son indécidabilité*, Masson, Paris, 1995.

P. RIBENBOIM, *Nombres premiers : mystères et records*, Presses universitaires de France, 1994.

***Le secret des nombres* (arithmétique pour l'enseignement de spécialité de terminale S), ouvrage collectif des Éditions Archimède, ISSN 0987-0806, *Tangente*, hors série n° 6, 1998.**