

7. a^b EST DIOPHANTIN

La découverte de Matiassevitch 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 $P(a, b, c, x_1, x_2, \dots, x_n) = 0$, P polynôme, possédant des solutions entières $x_1, x_2, \dots, x_n$, 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 Matiassevitch, 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 Matiassevitch, 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 Matiassevitch soit élaboré explicitement et publié en 1976 par J. Jones, D. Sato, H. Wada et D. Wiens. Le voici : $(1 - (vz + h + j - q)^2 - ((gk + 2g + k + 1)(h + j) + h - z)^2 - (2n + p + q + z - e)^2 - (16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f^2)^2 - (e^3(e + 2)(a + 1)^2 + 1 - o^2)^2 - ((a^2 - 1)y^2 + 1 - x^2)^2 - (16r^2y^4(a^2 - 1) + 1 - u^2)^2 - ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2)^2 - (n + l + v - y)^2 - ((a^2 - 1)^2 + 1 - m^2)^2 - (ai + k + 1 - j)^2 - (p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m)^2 - (q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x)^2 - (z + pl(a - p) + t(2ap - p^2 - 1 - pm)^2)(k + 2)$.

Quand les 26 variables $a, b, c, \dots, z$ 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@lil.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.lil.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/primel/>.

G. HARDY et E. WRIGHT, *An Introduction*

to the Theory of Numbers, Oxford Science Publications, Clarendon Press, Oxford, cinquième édition, 1979.

Y. MATIASSEVITCH, *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.