Le nombre 19 m'intrigue

Michel Mizony(*)

Voici le texte d'une intervention donnée à l'antenne de Bourg-en-Bresse de l'IUFM de Lyon, lors d'un colloque (Le Rallye Mathématique Transalpin) réunissant des instituteurs et professeurs de collège de trois pays (Italie, France et Suisse) ; ce colloque avait pour thème « Qu'est-ce qu'un bon problème de rallye ? ».

Il m'a été demandé de donner un témoignage de mathématicien-chercheur sur son travail, à l'occasion de ce colloque. Dur dur, car autant de mathématiciens, autant de manières différentes de se poser et d'aborder des problèmes, qui sont de plus pour la plupart très, très abstraits.

Actuellement mes centres d'intérêts en recherche sont les théories de la gravitation [2] (c'est de l'analyse sur des variétés) et la modélisation mathématique (rapports des mathématiques avec les autres disciplines scientifiques). Mais, comme beaucoup de chercheurs, je m'intéresse aussi à des problèmes abordables par un public moins restreint. Ainsi je vais vous parler du nombre 19, nombre intriguant.

Depuis quelques années, je cherche des propriétés particulières du nombre premier 19. C'est un nombre qui pour moi est plein de mystères.

En effet dans le cadre d'une recherche internationale, nous avons trouvé, en 1997 et 1998, d'abord huit nombres premiers consécutifs en progression arithmétique, puis neuf, puis dix [1]. À noter que ce résultat est le fruit d'une recherche collective entre mathématiciens de plusieurs pays.

Rappel : une progression arithmétique est une suite de nombres dans laquelle on passe de l'un au suivant en ajoutant toujours le même nombre, appelé « raison ».

Ce dix-uplet (comme on le dit dans notre jargon) est formé de nombres de 93 chiffres, la raison provient de 210 ($210 = 2 \times 3 \times 5 \times 7$ est la raison minimale d'après un théorème dû à Cantor) et surtout ces nombres sont égaux à 19 modulo 30 ($30 = 2 \times 3 \times 5$).

Rappel : Calcul modulo n : dans une « division avec reste » ou en restant dans les nombres entiers, être égal à 19 modulo 30 signifie obtenir un reste de 19 dans la division par 30.

Ces résultats furent obtenus grâce à l'utilisation d'un grand nombre d'ordinateurs. Notre algorithme ne permet pas de trouver un 11-uplet (qui doit être de raison 2 310), car l'algorithme est trop lent. Or, pour l'initialisation de l'algorithme qui a permis de trouvé le dix-uplet, j'avais proposé, après de multiples tests sur ordinateurs, de partir des nombres 19 et 199 pour des raisons intuitives, et le résultat est venu 100 fois plus vite que ne le laissaient prévoir les probabilités (il existe beaucoup de théorèmes de nature probabiliste en théorie des nombres). Pourquoi, je ne sais pas. De ce fait le nombre 19 m'intrigue.

(*) Directeur de l'IREM de Lyon. mél : mizony@univ-lyon1.fr

Alors voici quelques propriétés que j'ai glanées ou trouvées (retrouvées ?), qui sont suffisamment élémentaires pour être éventuellement utilisables par des professeurs de mathématiques. J'ai déjà fait plusieurs interventions dans des classes de lycées de l'académie de Lyon sur ce thème (en particulier sur le principe algorithmique de Nelson [1] qui permet de trouver rapidement des 3-uplets et 4-uplets avec les calculatrices programmables), mais les lemmes (résultats) que je vous livre aujourd'hui datent de ce mois d'Août 2004. Pré-requis : la définition du calcul modulo n.

Remarque de départ : $n = 30$ est le plus petit entier tel qu'il existe un nombre k premier vérifiant $k^2 \equiv 1$ modulo 30 et admettant une ou plusieurs racines carrées modulo 30.

Exercice 1 :
– Établir un algorithme qui permette de trouver ces premières paires (k, n).
On doit obtenir (19, 30), (17, 32), (29, 35), …, (199, 330), …
– Trouver les racines carrées de 19 modulo 30.

19 est racine carrée de 1 modulo 30, car $19^2 = 361 \equiv 1$ (modulo 30) et est carré de nombres obtenus en lui ajoutant un multiple de 30, comme $7^2 = 49$ (30 +19), $13^2 = 169$ (150 + 19). Les nombres $17 = 30 - 13$ et $23 = 30 - 7$ sont aussi des racines carrées de 19 modulo 30.
Ainsi, 19 est racine carré de 1 et carré de nombres (modulo 30) !

Rappel : Les mathématiciens appellent nombres premiers jumeaux deux nombres premiers qui diffèrent de 2 comme 3 et 5, 5 et 7, 11 et 13, 17 et 19, 29 et 31, 41 et 43, 71 et 73, …

Lemme 1 : Soit $(k - 2, k)$ une paire de nombres premiers jumeaux. Si k se termine par 9 en base 10 (de manière plus intrinsèque $k \equiv 9$ modulo 10), alors, en posant $n = \frac{5}{3}(x-1)$, on a $k^2 \equiv 1$ modulo n et $(k-2)^2 \equiv k$ modulo n.

Exemple : pour $k = 109$, $n = \frac{5}{3} \times 108 = 180$ et $107^2 = 11\,449 \equiv 109$ modulo 180.
C'est un cas particulier du résultat plus général suivant.

Lemme 2 : Tous les nombres x de la forme $x = 19 + 30 \times n$ vérifient $x^2 \equiv 1$ modulo $n = \frac{5}{3}(x-1)$ et $(x-2)^2 \equiv x$ modulo $n = \frac{5}{3}(x-1)$.

Exemple : pour $x = 49$, $\frac{5}{3} \times 48 = 80$ et $47^2 = 2\,209 \equiv 49$ modulo 80.

Exercice 2 :

– Établir des algorithmes qui permettent de vérifier ces lemmes (un premier algorithme permettant de trouver les premières paires de premiers jumeaux, un deuxième testant la véracité du lemme 2).

– (Pour les professeurs) démontrer ces lemmes (on pourra utiliser le fait que $x - 1$ est divisible par 6).

Considérons maintenant les suites de quatre nombres premiers les plus proches possibles ; elles sont formées de deux paires de premiers jumeaux.

Définition : On appelle quadruplet de nombres premiers toute suite de la forme $(x - 8, x - 6, x - 2, x)$, où chacun des nombres est premier.

On pense qu'il existe une infinité de telles suites, mais ce n'est pas encore démontré.

Exercice 3 :

– Établir un algorithme qui permette de trouver les premiers quadruplets de nombres premiers (on doit trouver les quadruplets (5, 7, 11, 13), (11, 13, 17, 19), puis (101, 103, 107, 109), (191, 193, 197, 199), …).

– Montrer qu'en dehors du quadruplet (5, 7, 11, 13), tous les autres vérifient $x \equiv 19$ modulo 30.

Notes : Il y a toujours des propriétés que l'on utilise implicitement. J'en citerai deux que j'utilise beaucoup.

Tout nombre premier (en dehors de 2 et 3) est nécessairement de la forme $6n + 1$ ou $6n - 1$.

Le calcul modulo n est un calcul dans l'anneau $\mathbf{Z}/n\mathbf{Z}$, en particulier le groupe des éléments inversibles pour la multiplication dans $\mathbf{Z}/n\mathbf{Z}$ donne des indications sur les nombres premiers. Étudier les inversibles de $\mathbf{Z}/30\mathbf{Z}$ puis de $\mathbf{Z}/(2 \times 3 \times 5 \times 7\mathbf{Z})$. Pour une bibliographie, il existe pas mal de livres sur la théorie des nombres ; ceux disponibles ([3], [4], [5]) dans les bibliothèques des IREM ou des préparations au Capes ou à l'Agrégation de mathématiques sont amplement suffisants.

Conclusion : 19 est un drôle de nombre.

Je continue ma quête d'autres propriétés (arithmétiques) de ce nombre et je suis preneur de toute idée (c'est une remarque sur le $18 = 19 - 1$ que m'a donnée Georges, un animateur de l'IREM de Lyon, qui m'a permis de rédiger les lemmes 1 et 2). Le nombre 19 m'intrigue toujours dans la mesure où je ne sais pas encore répondre à la question initiale sur la rapidité de la découverte d'une suite de dix nombres premiers consécutifs en progression arithmétique.

Alors, « Qu'est-ce qu'un bon problème pour un mathématicien ? ». C'est d'abord et avant tout quelque chose qui intrigue ; l'essentiel de la recherche va consister à transformer ce « quelque chose qui intrigue » en un (ou plusieurs) problème(s) bien posé(s) puis il ne reste plus qu'à démontrer, suivant l'adage : « un problème bien posé est à moitié résolu ».

(suite page 415)

(suite de la page 412)

Bibliographie

[1] Harvey Dubner, Tony Forbes, Nik Lygeros, Michel Mizony et Paul Zimmermann. Ten consecutive primes in arithmetic progression, *Math. of Comp*. Volume 71, Number 239, pages 1323-1328, 2002.

[2] *La relativité générale aujourd'hui ou l'observateur oublié*, Éditions Aléas, 2003.

[3] Jean-Marie De Koninck et Armel Mercier. *Introduction à la théorie des nombres*, Modulo Éditeur, 1994.

[4] Sabah Al Fakir. *Algèbre et théorie des nombres*, Ellipses, 2003.

[5] Pierre Samuel. *Théorie algébrique des nombres*, Hermann, Paris, 1971.