

3. Records de progressions arithmétiques de nombres premiers

Les trois nombres premiers les plus grands en progression arithmétique :

$$9094283341425 \times 2666669 - 1 \\ + n \times 32289415560495 \times 2666666$$

pour $n = 0, 1, 2$.

Le premier terme possède 200 701 chiffres décimaux. Cette progression a été trouvée en mars 2011 par David Broadhurst. Il est bien sûr plus difficile de trouver quatre nombres premiers en progression arithmétique que d'en trouver trois. Il y a donc aussi un record pour quatre, cinq, etc.

Les quatre nombres premiers les plus grands en progression arithmétique :

$$1631979959 \times 225000 - 1 \\ + n \times (164196977 \times 280000$$

$$- 1631979959 \times 225000) \text{ pour } n = 0, 1, 2, 3.$$

Cette progression a été trouvée en 2010 par D. Broadhurst.

Les cinq nombres premiers les plus grands en progression arithmétique :

$$(82751511 + 20333209 \times n) \times 16229\# + 1$$

pour $n = 0, 1, 2, 3, 4$.

La notation $k\#$ désigne le produit de tous les nombres premiers inférieurs ou égaux à k (par exemple, $7\# = 2 \times 3 \times 5 \times 7 = 210$). Cette progression a été trouvée en 2009 par Ken Davis. Plus une progression arithmétique est longue,

plus elle est difficile à découvrir. Même si l'on sait, grâce au théorème de B. Green et T. Tao, qu'il existe des progressions arithmétiques de nombres premiers de toute longueur, le record actuel n'est que de 26.

La plus longue progression arithmétique de nombres premiers :

$$43142746595714191 + 23681770 \times 23\# \times n$$

pour $n = 0, 1, 2, 3, \dots, 25$.

Cette progression de 26 termes a été trouvée en 2009 par Benoît Perichon.

Pour une liste plus complète de tels records : <http://users.cybercity.dk/~dsl522332/math/aprecords.htm>

✓ BIBLIOGRAPHIE

G. Tenenbaum et M. Mendès France, *Les nombres premiers, entre l'ordre et le chaos*, Dunod, 2011.

T. Tao, *Structure and randomness in the prime numbers*, dans D. Schleicher et M. Lackmann (éds.), *An Invitation to Mathematics*, Springer-Verlag, 2011 (http://terrytao.files.wordpress.com/2009/09/primes_paper.pdf).

Ch. Mauduit et J. Rivat, *Sur un problème de Gelfond : la somme des chiffres d'un nombre premier*, *Annals of Mathematics*, vol. 171(3), pp. 1591-1646, 2010.

B. Green et T. Tao, *The primes contain arbitrarily long arithmetic progressions*, *Ann. of Math.*, vol. 167(2), pp. 481-547, 2008.

R. Crandall et C. Pomerance, *Prime Numbers : A Computational Perspective*, Springer-Verlag, 2005.

M. Agrawal et al., *PRIMES is in P*, *Ann. of Math.*, vol. 160(2), pp. 781-793, 2004.

P. Ribenboim, *The Little Book of Bigger Primes*, Springer-Verlag, 2004.

M. Dietzfelbinger, *Primality Testing in Polynomial Time*, Springer, 2004.

J.-P. Delahaye, *Merveilleux nombres premiers*, Belin/Pour la Science, 2000.

de primalité polynomial (voir *Pour la Science* n° 303, janvier 2003, pages 98-103).

Bien sûr, un algorithme dont le temps de calcul est un polynôme de degré 50 est moins intéressant qu'un algorithme dont le temps de calcul est un polynôme de degré 2. Une fois trouvé un test de primalité polynomial, le travail n'était donc pas terminé, et on a tenté d'obtenir des tests polynomiaux de degré aussi petit que possible.

L'analyse de l'algorithme des trois chercheurs indiens montre que leur test est de degré 12, ce qui est beaucoup. Mais en admettant une conjecture considérée comme probable, on établit que leur algorithme permet un test de degré 6.

On a d'abord trouvé une preuve, n'utilisant cette fois aucune conjecture, avec des polynômes de degré 11, puis 8. Une variante de l'algorithme a été proposée par Carl Pomerance et Henry Lenstra, et ils prouvèrent en 2005 que leur test est polynomial de degré 6. Une autre variante fut prouvée de degré 3, mais cette fois, sous réserve d'une conjecture assez risquée. Ce degré 3 ne doit donc pas être considéré comme acquis.

Enfin, un autre résultat établit que, sauf cas exponentiellement rares, la primalité est démontrable en temps polynomial de degré 4. On ne pense pas pouvoir faire mieux. Cela conduit à la conclusion suivante, probablement définitive : prouver qu'un entier n est premier exige un temps de calcul qui augmente comme un polynôme de degré 4 de la longueur de l'entier n auquel on s'intéresse.

Notons cependant que pour l'instant les algorithmes polynomiaux mis au point et prouvés tels ne sont pas aussi rapides que les anciens algorithmes (qui eux ne sont pas prouvés polynomiaux !). L'approche théorique n'est pas pour autant inutile, mais il faudra peut-être attendre un moment pour qu'elle ait des retombées pratiques.

Des suites arithmétiques

Abordons maintenant les suites arithmétiques de nombres premiers. Les plus simples des polynômes sont les formes linéaires : $n \rightarrow an + b$.

Nous avons vu qu'une telle expression ne donne pas des nombres premiers pour tout entier n (sauf si elle est constante et égale à un nombre premier). En revanche, il n'est pas interdit qu'elle donne une infinité de nombres premiers. L'une des plus simples questions liant nombres premiers et polynômes est ainsi celle de l'existence de paramètres a et b tels qu'il y ait une infinité de nombres premiers de la forme $an + b$ quand n prend des valeurs entières.

Bien sûr, il ne peut pas y avoir une infinité de nombres premiers de la forme $5n + 10$ puisque tout nombre de cette forme est multiple de 5 si n est entier. Plus généralement, si a et b sont multiples d'un même entier $k > 1$ (on dit qu'ils ne sont pas premiers entre eux), alors les nombres de la forme $an + b$ ne peuvent pas être premiers