

grande ressemblance avec la formule de Riemann pour la fonction $\pi(x)$ et qui permettent de prouver un analogue de la conjecture de Riemann pour une autre sorte de fonctions ζ . Mais en ce qui concerne l'hypothèse de Riemann elle-même, ce type de tentatives n'avait jusqu'à présent fourni aucun résultat.

Depuis 2000, sur la base d'une idée de Jon Keating et Nina Snaith, de l'université de Bristol, on utilise des matrices aléatoires pour modéliser la fonction ζ sur la droite critique. En se fondant sur l'analogie entre ces objets complètement différents, les mathématiciens formulent des conjectures qui, espère-t-on, fourniront d'autres pistes pour apporter une réponse définitive à la conjecture de Riemann.

Une autre tentative un peu plus facile à saisir fait appel à une étonnante propriété d'approximation de la fonction ζ . En 1975, le mathématicien russe Serguei Voronin prouva que la fonction ζ peut approcher aussi précisément qu'on le veut n'importe quelle fonction (suffisamment régulière) sur un petit domaine. C'est le célèbre théorème d'universalité de Voronin. Explicitons un peu ce résultat spectaculaire.

Soit une fonction $f(s)$ définie sur un petit disque K , situé n'importe où dans la moitié droite de la bande critique. Supposons que f n'ait aucun zéro dans K et qu'elle y soit analytique (développable en série de puissances entières). Alors pour tout $\epsilon > 0$, aussi petit soit-il, il existe un nombre réel $t > 0$ tel que la différence entre $\zeta(s+it)$ et $f(s)$ soit inférieure à ϵ en valeur absolue, et ce pour tout s de K . En d'autres termes, on peut trouver t tel que $\zeta(s+it)$ soit aussi proche que l'on veut de $f(s)$.

UNE PORTE VERS L'UNIVERSALITÉ

On montre même qu'il existe une infinité de nombres t vérifiant cette approximation pour une fonction f et un nombre ϵ donnés. En quelque sorte, la fonction ζ contient donc dans ses valeurs des informations sur toutes ces fonctions f . Un peu comme s'il s'agissait d'un atlas contenant toutes les cartes possibles... C'est pourquoi on résume le théorème d'universalité de Voronin en disant : « Qui connaît la fonction ζ connaît le monde. »

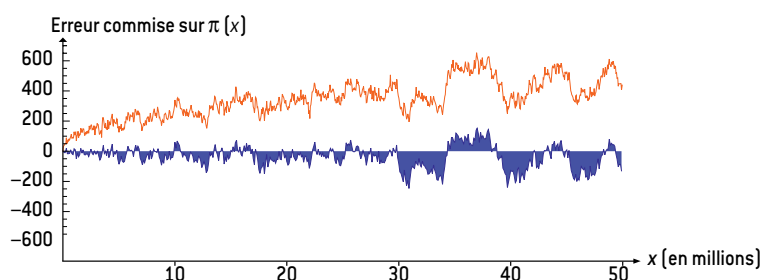
Cette propriété d'universalité fournit en retour des renseignements sur la fonction ζ elle-même. Si en effet la conjecture de Riemann est correcte, c'est-à-dire que tous les zéros non triviaux de $\zeta(s)$ se trouvent sur la droite critique, on peut appliquer le théorème d'universalité à $\zeta(s)$ et il en résulte que la fonction ζ s'approxime elle-même – on en déduit qu'elle est autosimilaire, comme le sont les fractales (figures géométriques qui, quel que soit le grossissement choisi, gardent le même aspect). Réciproquement, si on prouvait que la fonction ζ est autosimilaire, la validité de la conjecture de Riemann en découlerait.

LA FORMULE DE RIEMANN POUR $\pi(x)$

$$\pi(x) + \sum_{n=2}^{\infty} \frac{1}{n} \pi\left(x^{\frac{1}{n}}\right) = \text{li}(x) - \sum_{\rho} \left(\text{li}(x^{\rho}) + \text{li}(x^{1-\rho})\right) + \int_x^{\infty} \frac{du}{u(u^2-1) \ln u} - \ln 2$$

Cette formule relative au nombre $\pi(x)$ de nombres premiers inférieurs à x est valable pour tout $x \geq 2$ qui n'est pas une puissance d'un nombre premier p (dans ce cas particulier, on doit ajouter à gauche $1/(2k)$ pour la contribution de $x=p^k$). La somme dans le membre de droite est à effectuer sur tous les zéros ρ non triviaux de la fonction ζ ayant une partie imaginaire positive. La somme dans le membre de gauche est en réalité finie, car dès que la n -ième racine de x est inférieure à 2, le n -ième terme est nul (ainsi que les termes suivants).

Si l'on veut vraiment calculer $\pi(x)$ à l'aide de cette formule (avec un ordinateur), on doit remplacer les deux sommes par des sommes partielles ne contenant qu'un nombre fini de termes. Or même lorsqu'on ne prend en compte que les 10 premières valeurs de n et les 30 premiers zéros de la fonction ζ , on obtient une excellente approximation de $\pi(x)$ (voir le graphique ci-dessous). L'écart entre cette approximation et la valeur exacte (en bleu) est à peine supérieur à 200, même autour de $x=50$ millions. En revanche, l'approximation donnée par la formule de Gauss (en rouge) devient de plus en plus mauvaise à mesure que x augmente.



© Peter Meier

Le mathématicien danois Harald Bohr (frère du physicien Niels Bohr) est à l'origine de cette observation, dans les années 1920. Mais, faute du théorème d'universalité, il n'avait pu en donner une preuve. Celle-ci a été fournie par le mathématicien indien Bhaskar Bagchi au début des années 1980.

Beaucoup d'autres reformulations de la conjecture de Riemann sont aujourd'hui connues, mais une preuve semble pourtant toujours aussi éloignée. Bien sûr, si la conjecture était fautive, il suffirait de trouver un seul contre-exemple. Les mathématiciens cherchent aussi dans cette direction. Andrew Odlyzko, à l'université du Minnesota, Herman te Riele, au centre de recherche en informatique d'Amsterdam, et d'autres ont calculé jusqu'à présent plus de 100 milliards de zéros de la fonction ζ : ils se trouvent tous sur la droite critique $\text{Re}(s)=1/2$.

Mais ces vérifications numériques ne constituent pas une preuve de l'hypothèse de Riemann. Face à l'infinité des nombres, ce à quoi le raisonnement humain et l'ordinateur peuvent accéder n'est qu'une minuscule goutte dans l'immensité de l'océan. Le million de dollars attend toujours son destinataire, mais cette somme ne représentera pas grand-chose comparée à la satisfaction d'avoir résolu le problème. ■

L'ESSENTIEL

● Comment déterminer les nombres premiers ? Depuis l'Antiquité, plusieurs formules ont été proposées pour les calculer.

● Certaines sont élégantes, d'autres plus complexes, mais elles ont souvent pour défaut de ne donner que quelques nombres premiers.

● D'autres encore donnent une infinité (théorique) de nombres premiers, mais les valeurs qu'ils prennent croissent trop vite.

● On peut néanmoins s'en inspirer pour faire mieux, notamment en ajustant très finement les paramètres des formules.

L'AUTEUR



SIMON PLOUFFE
professeur à l'IUT Informatique
de Nantes, coauteur de
l'Encyclopédie en ligne des suites
de nombres entiers (OEIS).

Un record pour les nombres premiers

Depuis des millénaires, les mathématiciens conçoivent des formules pour calculer des nombres premiers. En janvier 2019, une formule élaborée par l'auteur a généré une séquence de 100 nombres premiers. C'est un record ! Explications.

L

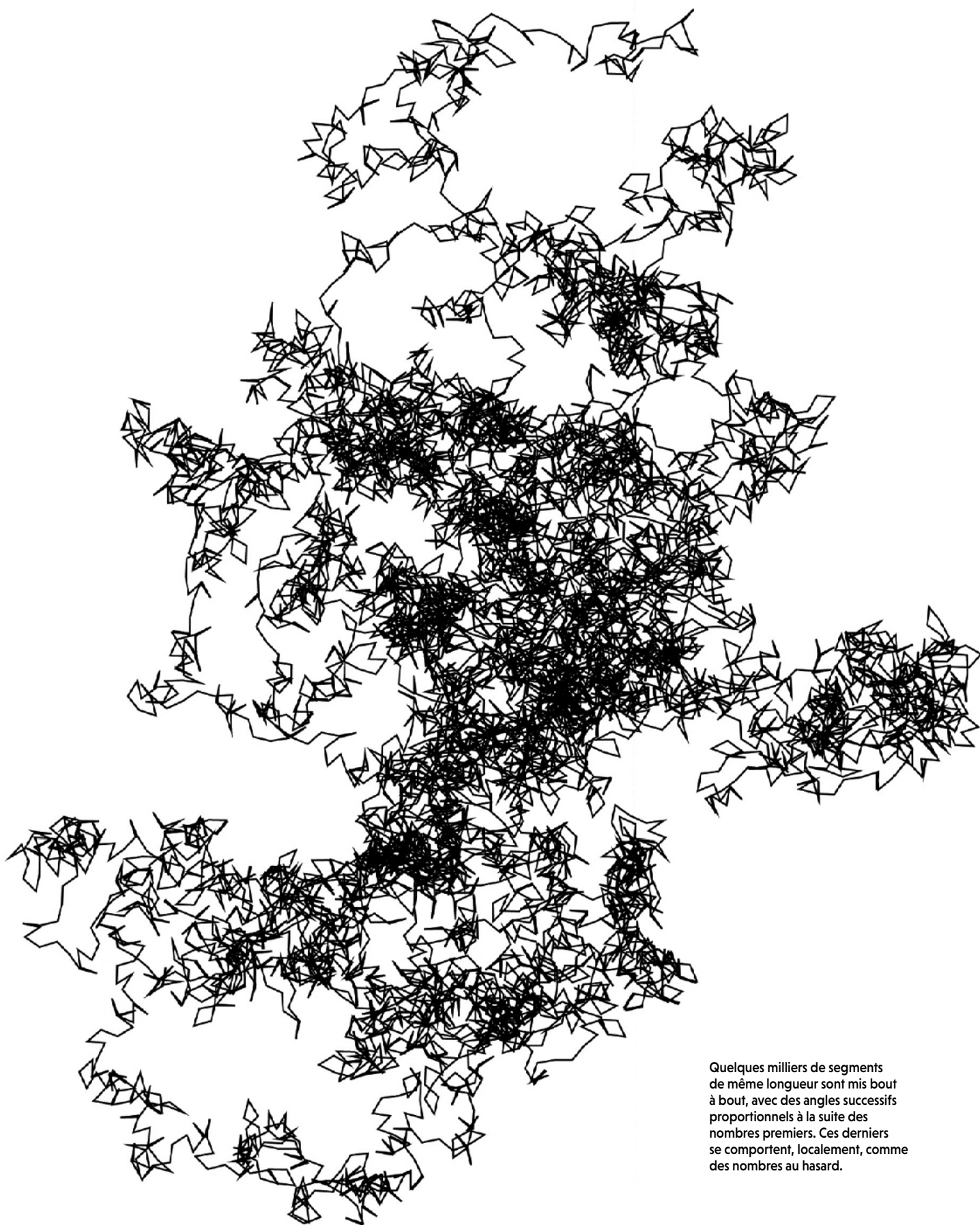
e 7 décembre 2018, un record été battu, celui du plus grand nombre premier connu. $2^{82589933} - 1$, qui comporte près de 25 millions de chiffres en écriture décimale. On doit cette performance (la vérification est en cours) au *Gimps*, le *Great Internet Mersenne Prime Search*. Ce projet fondé par George Woltman réunit des

volontaires mettant à disposition leur ordinateur pour un calcul, distribué, des nombres premiers dits de Mersenne (voir l'encadré page 79), c'est-à-dire de la forme $2^p - 1$, p étant un nombre premier. On disposerait donc d'une formule pour déterminer les nombres premiers ?

UNE FORMULE, MAIS LAQUELLE ?

Ce n'est pas aussi simple, notamment parce que tous les nombres premiers ne sont pas de la forme de Mersenne, tant s'en faut. La question se pose donc toujours : y a-t-il une formule pour les nombres premiers ? La réponse est... oui et non.

Et d'abord qu'entend-on par formule ? Par exemple, ce peut être une formule dite close comme celle trouvée par le Suisse Leonhard Euler en 1772 : $p(n) = n^2 + n + 41$. Pour n entre 0 >



Quelques milliers de segments de même longueur sont mis bout à bout, avec des angles successifs proportionnels à la suite des nombres premiers. Ces derniers se comportent, localement, comme des nombres au hasard.

$$\frac{n^6}{72} - \frac{5n^5}{24} - \frac{1493n^4}{72} + \frac{1027n^3}{8} + \frac{100471n^2}{18} - \frac{11971n}{6} - 57347$$

➤ et 39, elle délivre 40 nombres premiers d'affilée : 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 et 1601. De plus, la formule est élégante et simple, mais elle a ses limites. Pour $n = 40$, on trouve 1681... qui est 41^2 .

En 2010, François Dress et Bernard Landreau en ont trouvé une meilleure, mais plus compliquée (voir ci-dessus). Avec ce polynôme, on obtient des nombres premiers pour n compris entre -42 et 15 . La recherche de ce polynôme a tout de même demandé six mois d'efforts avec une batterie d'ordinateurs.

Est-ce donc si difficile de produire une formule qui donnerait quantité de nombres premiers ? La question a été close une bonne fois pour toutes en 1947, quand William Mills a publié

Par tous les moyens, on cherche à calculer les nombres premiers, avec une fortune diverse.

une formule qui peut donner un nombre arbitraire de nombres premiers. Si $A = 1,3063778838630806904686144926...$ alors $\lfloor A^{3^n} \rfloor$ donne une suite arbitraire de nombres tous premiers. Ici $\lfloor x \rfloor$ indique que l'on prend la partie entière du nombre x . La suite débute ainsi : 2, 11, 1361, 2521008887... Cependant, les valeurs augmentent très vite, le 8^e terme a déjà 762 chiffres, et le 20^e environ six milliards !

En 1951, le Britannique Edward Wright en proposait une autre, si $g_0 = \alpha = 1,9287800...$ et $g_{n+1} = 2^{g_n}$ alors $\lfloor g_{n+1} \rfloor = \lfloor 2^{2^{g_n}} \rfloor$ est toujours premier. Les nombres premiers consécutifs sont uniquement représentés par α . La suite obtenue est 3, 13, 16381... le 4^e terme a plus de 4932 chiffres et personne n'a osé calculer le 5^e...

Ainsi, ces deux suites produisent bien une infinité de nombres premiers, mais le taux de croissance décourage les plus téméraires. Peut-on élaborer des formules fournissant une suite de nombres premiers de longueur arbitraire, mais avec un taux de croissance raisonnable ?

LE TABLEAU DE CHASSE

Le « tableau de chasse » ci-contre récapitule des formules et des procédés pour les nombres premiers. L'infini calculable mentionné signifie que le calcul ou procédé peut se dérouler jusqu'à ce que les ressources s'épuisent. Par exemple, le programme Primesieve est le plus rapide. Il peut produire tous les nombres premiers jusqu'à 1000 milliards en 52 minutes sur un ordinateur moyen. Dans sa version courante, la liste peut aller jusqu'à 2^{64} , soit $1,844 \times 10^{19}$, mais les nombres réclament 4,1 exaoctets d'espace pour être stockés... Ce programme est fondé sur le crible d'Ératosthène, du nom d'un mathématicien grec du III^e siècle avant notre ère. Cet algorithme procède par élimination : on supprime parmi les nombres de 2 à N tous les multiples d'un entier de sorte qu'à la fin il ne reste que les nombres premiers.

L'infini calculable du crible d'Ératosthène, à l'époque de son inventeur, était d'un autre ordre, et relevait plus du calcul manuel. La même chose s'applique pour le petit théorème de Fermat selon lequel si p est un nombre premier et si a est un entier non divisible par p , alors $a^{p-1} - 1$ est un multiple de p . Les nombres premiers produits par ce théorème sont probables et faibles. Si p est très grand, il constitue néanmoins un test probabiliste pratique de la primalité d'un nombre candidat.

Quant aux nombres de Mersenne (de la forme $2^p - 1$), ils sont limités par la taille de p . Pour tester un seul exposant dans la liste des candidats, un voire deux mois de calcul intensif sur

Auteur(s)	Année	Commentaire	Efficacité	Nombres calculés
Ératosthène	-276 à -194	Crible d'exclusion	Pratique	Infini calculable
Mersenne	1536	Nombres premiers de la forme $2^p - 1$.	Pratique, exact	51
Fermat	1640	Petit théorème de Fermat	Produit des premiers probables faibles	Infini calculable
Euler	1772	Polynôme du second degré	Pratique	40
Mills	1947	Double exponentielle	Pratique	Moins de 10
Wright	1951	Super exponentielle	Pratique	Moins de 5
Wilson	vers 1780	Formule qui utilise $p!$	Théorique	Très peu
Jones, Sato, Wada et Wiens	1976	Polynôme de degré 25 à 26	Théorique	Très peu
John H. Conway	1987	Fractran	Théorique	Très peu
Rowland	2008	Récurrance	Théorique	Très peu
F. Dress et B. Landreau	2010	Polynôme de degré 6	Pratique	58
Benoît Perichon et al.	2010	26 premiers en progression arithmétique	Pratique	26
Tomás Oliveira e Silva et al.	2019	Programme Primesieve : crible d'Ératosthène optimisé	Le plus rapide connu	Infini calculable sur un ordinateur actuel

POUR LA SCIENCE HORS-SÉRIE N° 103 / Mai-Juin 2019 / 79

2
3
5
11
37
223
3 331
192 271
84 308 429
774 116 799 347
681 098 209 317 971 743
562 101 323 304 225 290 104 514 179
13 326 678 220 145 859 782 825 116 625 722 145 759 009
1 538 448 162 271 607 869 601 834 587 431 948 506 238 982 765 193 425 993 274 489

> Avec un exposant égal à $3/2$ et $a_0 = 2,038239154782...$ on obtient la suite de nombres premiers ci-dessus.

C'est désormais la suite A323611. Un autre exemple livre les petits nombres premiers. Avec $a_0 = 3,34683553593243081...$ et un exposant égal à $1,251295195638...$ la suite (A323065) est: 3, 5, 7, 11, 19, 41, 103, 331, 1423, 8819, 86477, 1504949...

En choisissant a_0 assez grand, on peut utiliser un exposant très petit, comme $101/100$. Si $a_0 = 10^{500} + 961,4993763378507...$ on obtient une suite de 100 nombres premiers, le dernier n'ayant que 1340 chiffres. Elle bat ainsi les records de 2010 (58 nombres premiers avec un polynôme et 26 avec une progression arithmétique). Notons

néanmoins que lorsque leur taille dépasse 20 chiffres, les nombres obtenus ne sont que des premiers probables. Si a_0 est bien choisi, on conjecture que l'exposant peut être aussi près de 1 qu'on le souhaite (pour limiter la croissance).

OBTEINIR TOUS LES NOMBRES PREMIERS ?

Avec des formules de ce type, peut-on obtenir tous les nombres premiers? Pour y parvenir, on pourrait par exemple partir d'un nombre premier arbitraire et descendre jusqu'à 2. C'est possible avec un procédé inverse en utilisant $1/\alpha$, α étant l'exposant. Ainsi, en partant du nombre premier $10^{100} + 267$ et avec $\alpha = 0,38562256415290...$ on obtient 742 123 524 365 563, 542 489, 163, 7, 2.

On retrouve la suite inverse en partant à 2 avec $a_0 = 2,1322219996628413452...$ et l'exposant $1/\alpha = 2,5932092490404286167308...$ Le principe fonctionne dans les deux sens!

Tous ces calculs décrits sont empiriques. En pratique, on arrive à générer un nombre arbitraire de nombres premiers avec une croissance minimale de la suite. Les formules sont bien plus économes que celles Mills et Wright. À partir d'un nombre premier donné, on peut descendre jusqu'à 2 et à partir de 2 on peut obtenir une famille de suites infinies de nombres premiers.

Les records sont faits pour être battus, et avec un matériel informatique adéquat, et un certain temps de calcul, la suite de 100 nombres premiers peut être étendue jusqu'à 1 000 000 de chiffres. Mieux, lorsque l'exposant est $3/2$, on conjecture que tous les nombres premiers peuvent être générés. Reste à le démontrer... ■

UN PROGRAMME MAISON

L'algorithme mis au point procède en trois étapes. D'abord, on choisit la valeur de départ a_0 et l'exposant α , préférablement une fraction simple. Puis on lance un algorithme qui associe la technique de Monte-Carlo (fondée sur des processus aléatoires) et le principe du recuit simulé. Ce principe est inspiré de la métallurgie où l'on alterne les cycles de refroidissement lent et de réchauffage (recuit) afin de minimiser l'énergie d'un matériau. Cette technique évite que l'écart entre chaque nombre premier

ne croisse trop vite. Une fois quatre ou cinq valeurs trouvées, on passe à l'étape 3. On utilise une formule qui permet d'aller soit vers l'avant soit vers l'arrière. Vers l'avant, on cherche le plus petit nombre premier après $\{a_p^{\alpha}\}$. C'est assez facile en quelques minutes, même s'il a des milliers de chiffres, grâce à des logiciels, comme Maple ou PFGW. On rebrousse chemin pour vérifier que la formule fonctionne. Pour ce faire, on doit résoudre pour x avec $x^{\alpha} = S_{n+1}$. Ici S_{n+1} est le prochain nombre premier candidat. C'est ici qu'un α rationnel facilite le calcul.

Des nombres et des énigmes

La suite des énigmes concoctées
par Ana Retchman et Sébastien Kernivinen.

La fin page 105. Solutions page 106.

Ana
Retchman



Sébastien
Kernivinen



ÉNIGME 5

Trouver tous les entiers strictement positifs x et y tels que $6 \times (x! + 3) = y^2 + 5$ (ou $x!$ désigne le produit $1 \times 2 \times 3 \dots \times x$).

ÉNIGME 6

Trouvez les chiffres a et b de sorte que le nombre à cinq chiffres $32a1b$, soit divisible par 156.

ÉNIGME 7

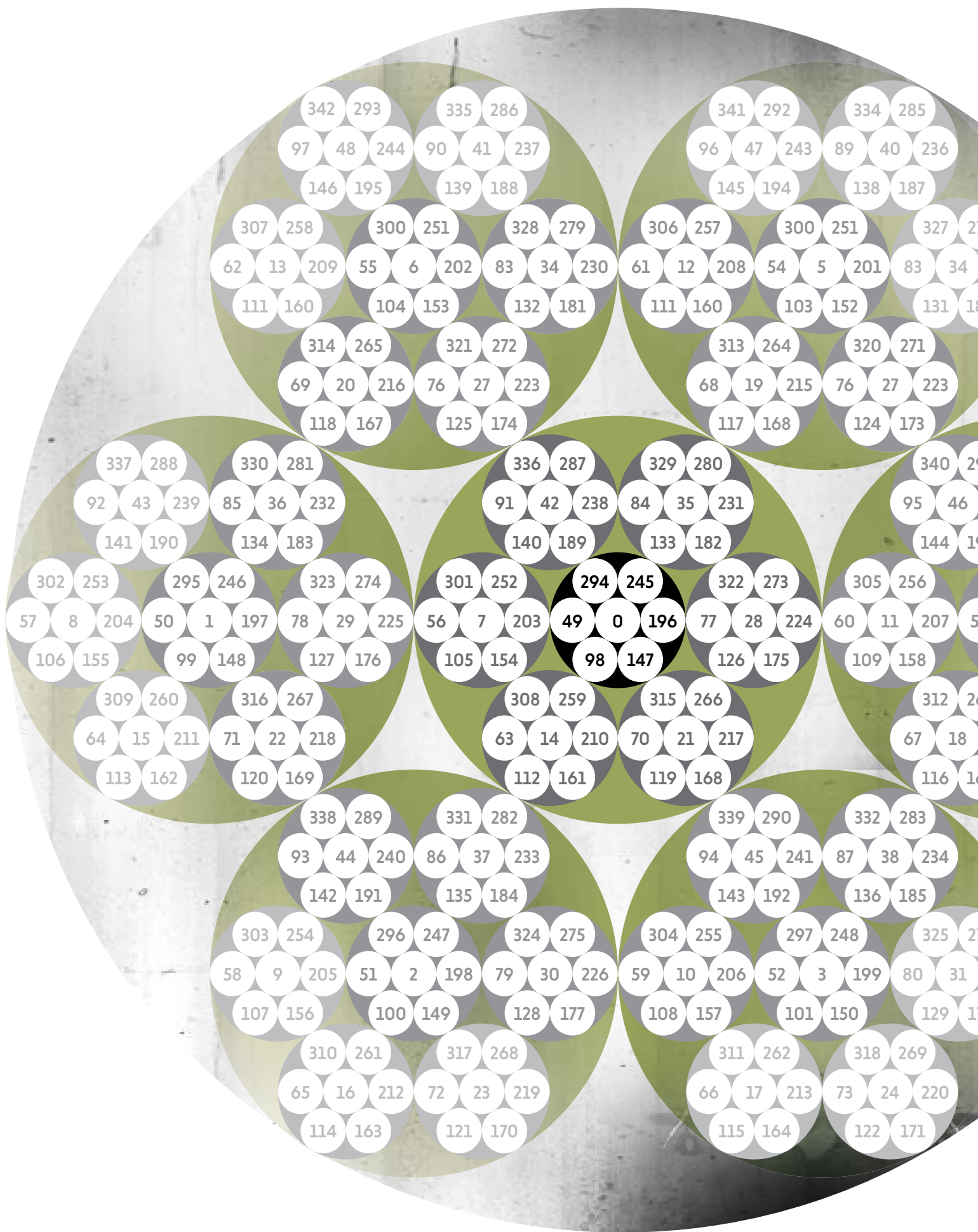
Quel est le plus grand nombre qu'on puisse obtenir en multipliant des nombres entiers positifs dont la somme vaut 8 ?

ÉNIGME 8

Si douze nombres strictement positifs $a_1 \leq a_2 \leq \dots \leq a_{12}$ sont tels que, dès qu'on en choisit trois quelconques parmi eux, on ne peut pas construire de triangle (non plat) dont les côtés aient pour longueurs ces trois nombres, quelle est la plus petite valeur possible de $\frac{a_{12}}{a_1}$?

ÉNIGME 9

La somme de deux nombres entiers positifs vaut 125. Si on multiplie le premier par 4 et qu'on divise le second par 4, on obtient la même somme. Quels sont les deux nombres initiaux ?





DES HOMMES ET DES NOMBRES

Parmi les résultats les plus importants obtenus en mathématiques ces dernières années, beaucoup concernent la théorie des nombres. Et derrière ces exploits se cachent des mathématiciens aux tempéraments variés, aux approches différentes... Mais tous ont en commun d'avoir pris à bras-le-corps des problèmes ardues et de les avoir explorés de façon nouvelle. Avec à la clé, pour ces hommes de nombres, les récompenses les plus prestigieuses, comme la médaille Fields ou le prix Abel.

Les nombres 7-adiques
(ici, les $7 \times 7 \times 7 = 343$ premiers)
sont arrangés de façon fractale
révélant leur proximité (cette notion
prend un sens différent de celui
qu'on lui connaît habituellement).
Dans le disque noir central,
on distingue les multiples
de $7 \times 7 = 49$, puis dans les disques
autour les entiers de la forme
 $n \times 7 \times 7 + 7$, $n \times 7 \times 7 + 14$...