Une autre idée suivit dans la foulée : il s'aperçut qu'avec quelques ajustements, les théories qu'il avait développées sur les formes modulaires pouvaient être de puissants outils non seulement pour vérifier les énoncés de Ramanujan, mais aussi pour mettre au jour des propriétés plus profondes de la fonction $p(n)$.

Multiples congruences...

K. Ono parvint ainsi à prouver que les congruences des nombres de partitions des entiers ne sont pas rares du tout. Les mathématiciens avaient supposé qu'il y en avait peu au-delà de 5, 7 et 11. En fait, comme le découvrit K. Ono, il en existe une infinité.

Les collègues de K. Ono saluèrent cette découverte, mais cela ne lui suffit pas pour être satisfait. Il avait beau avoir prouvé que les congruences des nombres de partitions des entiers sont partout, il n'était pas en mesure de déterminer où précisément.

Quand K. Ono bute sur un problème, il le met de côté avec d'autres problèmes non résolus jusqu'à ce qu'il refasse naturellement surface. Le problème de la prédiction des congruences des nombres de partitions resta ainsi en sommeil pendant cinq ans, jusqu'à l'arrivée du postdoctorant Zachary Kent à l'Université Emory, au printemps de 2010. Il surgit alors un jour au hasard d'une conversation, et bientôt ils ne parlèrent plus que de cela – dans leurs bureaux, à la pause café et lors de longues promenades dans les bois au Nord d'Atlanta.

Petit à petit, ils ont mentalement construit une superstructure labyrinthique où les nombres de partitions peuvent être parfaitement rangés. Pour ce faire, ils ont fait appel à des méthodes p-adiques, où l'on considère les objets arithmétiques à des multiples près des puissances successives d'un nombre premier p (par exemple 13, 13^2, 13^3 et ainsi de suite). Or les nombres ainsi obtenus obéissent à une structure fractale : ils se répètent selon des motifs presque identiques à différentes échelles, comme les branches successives d'un cristal de glace. Ce résultat montre que les nombres de partitions des entiers ne sont pas simplement une séquence aléatoire de nombres avec des symétries fortuites ici ou là. Au contraire, ces nombres ont « une structure interne d'une grande beauté », explique K. Ono, qui les rend prévisibles et bien plus fascinants à étudier.

Il fallut plusieurs mois à K. Ono, Z. Kent et leur collaboratrice Amanda Folsom de

Formes modulaires et fonctions thêta

Les formes modulaires et les fonctions thêta sont des fonctions de variables complexes vérifiant certaines relations fonctionnelles ; elles incarnent de multiples phénomènes liés à la géométrie algébrique, l'arithmétique et la théorie des groupes.

Plusieurs des grands noms des mathématiques du XIX^e siècle leur sont associés : Gotthold Eisenstein, Carl Gustav Jacobi, Henri Poincaré, Bernhard Riemann... De nos jours, ces fonctions et leurs généralisations interviennent dans la théorie des représentations des groupes, des courbes elliptiques et des variétés abéliennes, domaines importants des mathématiques du XX^e siècle.

Notons $\Sigma_{n \geq 0}$ l'opération de somme sur tous les entiers n positifs ou nuls. Une forme modulaire en la variable complexe z peut être vue comme une série infinie $f(z) = \Sigma_{n \geq 0} a_n q^n$ où $q = e^{2\pi i z}$, convergente quand la partie imaginaire de z est strictement positive (donc pour $|q| < 1$), et qui, principalement, obéit à l'équation fonctionnelle :

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

pour des entiers a, b, c, d vérifiant $ad - bc = 1$ et des propriétés de congruence telles que, par exemple, « N divise c ». L'entier N est le « niveau » et k est le « poids » de la forme modulaire. Les formes modulaires de poids 2 ont joué un rôle fondamental dans la preuve par Andrew Wiles du grand théorème de Fermat, en 1994 (théorème selon lequel il n'existe pas d'entiers positifs x, y et z tels que $x^n + y^n = z^n$, dès que l'entier n est supérieur à 2).

Le lien des formes modulaires avec les courbes elliptiques peut être illustré avec l'exemple de la courbe $y^2 - y = x^3 - x$.

Pour tout nombre premier p, notons N_p le nombre de solutions de cette équation modulo p (c'est-à-dire à un multiple de p près) et posons : $a(p) = p - N_p$.

Étendons la suite des $a(p)$ à tous les entiers positifs (premiers ou non) par les règles $a(p^m) - a(p)\,a(p^{m-1}) + p\,a(p^{m-2}) = 0$ et $a(n\,m) = a(n)\,a(m)$ pour n et m premiers entre eux. Alors d'après un cas particulier du théorème de A. Wiles, la fonction $f = \Sigma a(n)\,q^n$ est une forme modulaire de poids 2 et de niveau 37.

Quant aux fonctions thêta, la fonction typique est la fonction de deux variables suivante :

$\theta(u, z) = \Sigma_{n \in \mathbb{Z}} q^{n^2} t^n$

REPRÉSENTATION DE LA partie réelle d'une fonction modulaire liée aux « fonctions elliptiques de Weierstrass », sur le disque $|q| < 1$ (nombres complexes q dont le module est inférieur à 1). Les régions où la partie réelle de la fonction est nulle sont en noir (les valeurs sont croissantes du bleu-vert au jaune-rouge).

avec $q = e^{2\pi i z}$ et $t = e^{2\pi i u}$ et où $\Sigma_{n \in \mathbb{Z}}$ désigne la somme sur tous les entiers relatifs n (négatifs et positifs).

En tant que fonction de u, la fonction θ vérifie :
$\theta(u + az + b) = e(z, u)\,\theta(u, z)$,
où $e(z, u)$ est un facteur non nul ayant une expression simple.

En prenant $u = 0$, la fonction $\theta_0(z) = \Sigma_{n \in \mathbb{Z}} q^{n^2}$ est une forme modulaire « tordue » de poids 1/2 ; elle vérifie notamment :
$\theta_0(-1/z) = \alpha\, z^{1/2}\,\theta_0(z)$
où $\alpha = e^{-i\pi/4}$.

Les fonctions thêta recèlent une foule d'informations arithmétiques. On a par exemple remarqué que
$\theta_0{}^4(z) = 1 + \Sigma_{n>1} r(n)\,q^n$
où $r(n)$ est le nombre de représentations de l'entier n comme somme de quatre carrés d'entiers ; cela a permis à Jacobi de démontrer que $r(n)$ est égal à huit fois la somme des diviseurs de n si n est impair, et à 24 fois la somme des diviseurs impairs de n si n est pair.

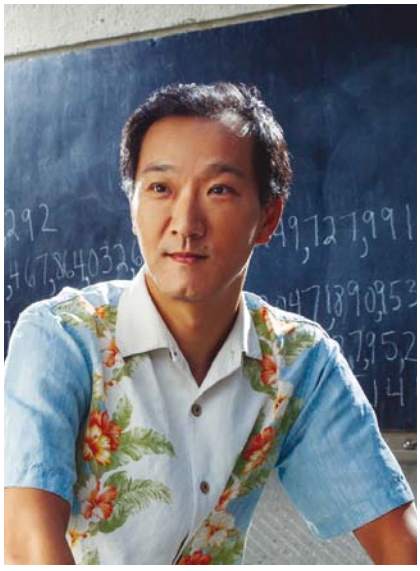
– Marc Hindry
Institut de mathématiques de Jussieu – Paris Rive Gauche

l'Université Yale pour démêler tous les fils de leur nouvelle théorie. Mais ils réussirent à prouver que les congruences des nombres de partitions apparaissent de façon calculable. Il en existe pour tous les nombres premiers et leurs puissances. Mais au-delà de 11, les motifs deviennent beaucoup plus complexes, ce qui explique probablement pourquoi Ramanujan ne les a jamais déterminées. K. Ono et ses collègues présentèrent leurs résultats à un symposium spécialement organisé à l'Université Emory en 2011.

De puissants outils

L'exploration des intuitions de Ramanujan a conduit K. Ono à d'autres développements qui pourraient un jour trouver une utilité hors des mathématiques. En mêlant la prescience de Ramanujan avec les mathématiques actuelles, K. Ono et ses collègues ont mis au point de puissants outils de calcul, utiles en mathématiques pures, mais qui pourraient aussi déboucher sur de meilleures méthodes de cryptage des données informatiques et aider à étudier les trous noirs.

En collaboration avec Jan Bruinier, de l'Université technique de Darmstadt en Allemagne, K. Ono a établi une formule permettant de calculer rapidement et avec précision les nombres de partitions des grands entiers, le graal que Ramanujan n'avait jamais atteint. K. Ono surnomme sa formule « l'Oracle ». En plus de calculer les nombres de partitions, dit-il, elle pourrait servir à étudier certains types de « courbes elliptiques » – des objets géométriques définis par une certaine classe d'équations polynomiales et qui sont dotées de remarquables propriétés arithmétiques.



Audra Melton

3. LES TRAVAUX DE KEN ONO, mathématicien à l'Université Emory, à Atlanta aux États-Unis, confirment et généralisent certains des résultats figurant dans les notes de Ramanujan.

Les cryptographes utilisent les courbes elliptiques pour réaliser certains algorithmes de cryptage. Le succès d'un tel algorithme repose sur la capacité de ce dernier à engendrer, pour qui veut décrypter le message codé, un problème mathématique impossible à résoudre en un temps raisonnable. Par exemple, un algorithme de cryptage répandu nommé RSA repose sur la difficulté à décomposer un très grand nombre en ses facteurs premiers. Des méthodes plus récentes font appel à des points sur une courbe elliptique, dont les relations sont encore plus difficiles à déchiffrer. Si l'Oracle ou les découvertes associées peuvent éclairer d'autres propriétés plus insaisissables, les cryptographes pourraient potentiellement les exploiter pour concevoir des systèmes de cryptage plus robustes.

Les travaux de K. Ono ont également dévoilé l'un des plus grands mystères de l'héritage mathématique de Ramanujan. Trois mois avant de mourir, cloué au lit par la fièvre et la douleur, le mathématicien indien écrivit à la hâte une dernière missive à Hardy. « Je suis tout à fait désolé de ne pas t'avoir écrit une seule lettre jusqu'à maintenant », s'excusait-il. « J'ai récemment découvert des fonctions très intéressantes que j'appelle "fausses" fonctions thêta [...]. Elles s'inscrivent dans les mathématiques aussi élégamment que les fonctions thêta ordinaires ».

Les fonctions thêta sont essentiellement des formes modulaires *(voir l'encadré page 53)*. Ramanujan supposait qu'il est possible de décrire de nouvelles fonctions (les fausses fonctions thêta, ou fonctions mock-thêta, le terme anglais *mock* signifiant faux) qui ne ressemblent en rien à des formes modulaires et qui pourtant se comportent de la même façon en des points particuliers nommés singularités. À l'approche de ces points, la valeur prise par

Généraliser les identités de Rogers-Ramanujan

La lettre adressée par Ramanujan à G. H. Hardy en 1913 incluait deux identités, initialement découvertes en 1894 par le mathématicien britannique Leonard James Rogers, et désormais connues sous le nom d'identités de Rogers-Ramanujan. Elles portent sur deux séries infinies, notées $G(q)$ et $H(q)$, et les identifient à des produits infinis :

$$G(q) = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(1-q)\dots(1-q^n)} = \prod_{n=0}^{\infty} \frac{1}{(1-q^{5n+1})(1-q^{5n+4})}$$

$$H(q) = \sum_{n=0}^{\infty} \frac{q^{n^2+n}}{(1-q)\dots(1-q^n)} = \prod_{n=0}^{\infty} \frac{1}{(1-q^{5n+2})(1-q^{5n+3})}$$

Ces identités sont utilisées aujourd'hui dans plusieurs domaines des mathématiques et de la physique théorique. La lettre de Ramanujan contenait une troisième formule montrant que leur quotient $H(q)/G(q)$ a des propriétés remarquables. Notamment, selon les valeurs de q, ce quotient donne aisément des nombres algébriques (nombres qui sont solution d'une équation polynomiale à coefficients entiers, comme le nombre d'or $(1+\sqrt{5})/2$, qui est la solution positive de l'équation $x^2 - x - 1 = 0$).

Ces formules de Ramanujan ont longtemps intrigué les mathématiciens, qui s'interrogeaient sur leur origine et les raisons profondes de leur validité. Tout récemment, Ole Warnaar, de l'Université du Queensland en Australie, en collaboration avec K. Ono et Michael Griffin de l'Université Emory, ont découvert que ces identités constituent des cas particuliers d'une famille infinie d'identités de nature et de propriétés similaires, ce qui permet d'intégrer les identités de Rogers-Ramanujan dans un cadre théorique plus vaste.