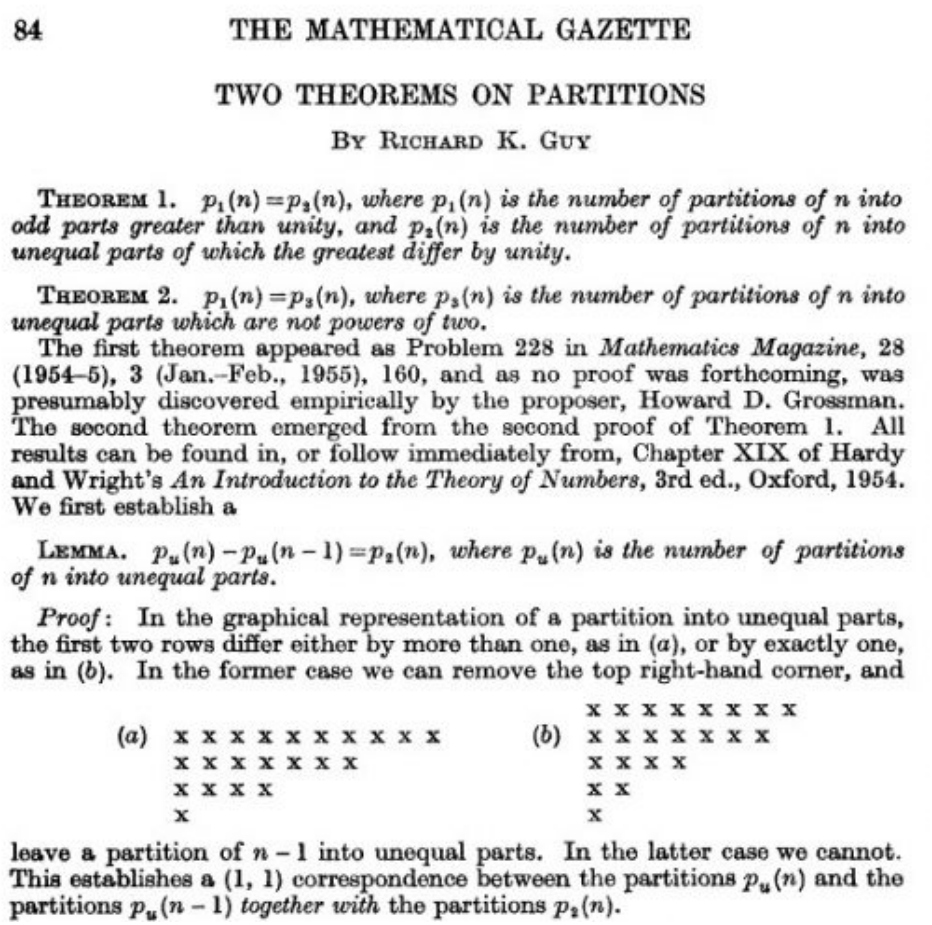
Richard Guy et la théorie des nombres

Richard Kenneth Guy (1916-2020)

Septembre 2020 (tome 52, no. 4)

M. J. Jacobson Jr., R. Scheidler and H. C. Williams

Même comme jeune enfant, Richard Guy était fasciné par les nombres. À l'âge de 17 ans, il acheta une copie du volume encyclopédique de Dickson *History of the Theory of Numbers* [Dickson 66] et il n'a pas pu résister à l'appel. Le coût `a l'époque était de 6 guinées, un gros montant d'argent—plus que ce qu'il a déboursé pour son diplôme de maîtrise à Cambridge. L'Histoire de Dickson a continué à avoir une grande influence sur Richard durant toute sa vie académique. Il publia son premier article important en théorie des nombres en 1958 [Guy 58]. C'est peut-être discutable, mais aucune œuvre de Richard ne fait preuve de son amour des nombres plus que son merveilleux *Book of Numbers*, écrit conjointement avec John H. Conway [Conway and Guy 96]. Le volume substantiel sur Richard faisant état de ses publications en Théorie des nombres fait mention d'environ 50 coauteurs, dont Elwin Berlekamp, John Conway, Paul Erdös, Derrick Lehmer, Yuri Matiyasevich, Alexander Oppenheim, John Selfridge et Daniel Shanks. Son intérêt prédominant en théorie des nombres était les suites d'entiers de toute forme et de tout contenu, incluant leur apparition en combinatoire, en géométrie et dans des problèmes Diophantiens. Les contributions de Richard dans le domaine sont trop nombreuses pour nous permettre de faire ici un compte-rendu complet; c'est pourquoi nous exhiberons seulement des exemples de ses travaux, avec une attention spéciale pour les recherches qu'il a effectuées depuis l'âge de 90 ans.



84 THE MATHEMATICAL GAZETTE

TWO THEOREMS ON PARTITIONS

BY RICHARD K. GUY

THEOREM 1. $p_1(n) = p_3(n)$, *where* $p_1(n)$ *is the number of partitions of* n *into odd parts greater than unity, and* $p_2(n)$ *is the number of partitions of* n *into unequal parts of which the greatest differ by unity.*

THEOREM 2. $p_1(n) = p_3(n)$, *where* $p_3(n)$ *is the number of partitions of* n *into unequal parts which are not powers of two.*

The first theorem appeared as Problem 228 in *Mathematics Magazine*, 28 (1954–5), 3 (Jan.–Feb., 1955), 160, and as no proof was forthcoming, was presumably discovered empirically by the proposer, Howard D. Grossman. The second theorem emerged from the second proof of Theorem 1. All results can be found in, or follow immediately from, Chapter XIX of Hardy and Wright's *An Introduction to the Theory of Numbers*, 3rd ed., Oxford, 1954. We first establish a

LEMMA. $p_u(n) - p_u(n-1) = p_2(n)$, *where* $p_u(n)$ *is the number of partitions of* n *into unequal parts.*

Proof: In the graphical representation of a partition into unequal parts, the first two rows differ either by more than one, as in (*a*), or by exactly one, as in (*b*). In the former case we can remove the top right-hand corner, and

(*a*)

x x x x x x x x x x
x x x x x x x
x x x x
x

(*b*)

x x x x x x x x
x x x x x x x
x x x x
x x
x

leave a partition of $n-1$ into unequal parts. In the latter case we cannot. This establishes a (1, 1) correspondence between the partitions $p_u(n)$ and the partitions $p_u(n-1)$ *together with* the partitions $p_2(n)$.

Le premier article théorique de Richard, paru en 1958

> *C'est peut-être discutable, mais aucune œuvre de Richard ne fait preuve de son amour des nombres plus que son merveilleux Book of Numbers, écrit conjointement avec John H. Conway*

Tweet

Une passion toute particulière de Richard pendant toute sa vie, fut les *suites aliquotes*. Elles consistent à itérer $n, s(n), s(s(n)), \ldots, s^{(k)}(n)$ via la somme des diviseurs propres (aliquotes) de la fonction $s(n) = \sigma(n) - n$, lorsque n est un entier positif. Catalan [Catalan 88], corrigé par la suite par Dickson [Dickson 13], a conjecturé que toutes les suites aliquotes ou bien s'arrêtent ou bien deviennent périodiques, et ainsi sont bornées. Le plus petit entier pour lequel cette conjecture n'est pas prouvée ou contredite est $n = 276$; en date de la rédaction de cet article, sa suite aliquote contient 2139 termes et le 2140e terme est un nombre composé et connu pour posséder un diviseur de 213 chiffres décimaux. Dans une série de rapports publiés dans les années 1970, Richard et John Selfridge ont trouvé que sous certaines conditions les suites aliquotes peuvent être très longues. Ceci les incita à proposer en 1975 une contre-conjecture

[Guy and Selfridge 75] à l'effet que plusieurs de ces suites, peut-être presque toutes, divergent pour tout entier pair n. La question de savoir quelle conjecture est correcte est encore sans réponse.

Richard avec ses collègues et ses étudiant.e.s à Math Lounge de l'Université de Calgary, 2011

Richard était vivement intéressé à évangéliser sa conjecture et a continué à y travailler jusqu'à la fin. Un résultat de Bosma et Kane [Bosma and Kane 12] montre que la moyenne géométrique (sur tous les n) de *l'amplification* $s(2n)/2n$ prend une valeur plus petite que 1, ce qui nous incite à croire que les termes d'une suite aliquote ont tendance à décroître en moyenne. Richard a cru que cette découverte ne capture pas la vraie essence des suites aliquotes parce que cela ne prend pas en compte la fréquence éventuelle d'un entier comme valeur $s(2n)$, de sorte que cela ne contribue pas au décompte dans le cas des *guides* et des *conducteurs*, deux objets décrits dans l'article de Guy et Selfridge [Guy and Selfridge 75]. Ce sont des diviseurs de $s^{(k)}(n)$ qui persistent à réapparaître d'un terme à l'autre avec une forte probabilité et qui la plupart du temps font augmenter la longueur de la suite. En fait, Pomerance [Pomerance 18] a montré que la moyenne géométrique des $s(n)/n$ est plus petite que 1 pour $n \equiv 2 \pmod 4$, et dépasse 1 pour $n \equiv 0 \pmod 4$.

Car d'autres résultats analytiques semblaient hors de porté pour le moment, Richard fit le choix de chercher des évidences numériques supportant son point de vue. Mike Jacobson nous raconte comment Richard commença subtilement à le recruter pour le joindre à sa cause, en écrivant d'abord un message électronique dont le sujet avait une saveur cryptique: " *Would you like to factor a number?* " La factorisation du dit nombre était obtenue, et lorsque Mike s'enquit de quoi Richard en retournait, ce dernier offrit avec un grand plaisir une explication débutant de la façon suivante (traduction libre):

> *Je suis en train de calculer une suite aliquote. C'est plutôt une cause perdue d'avance, mais je suis devenu intoxiqué, et cela remonte bien avant l'époque où un jeune étudiant brillant sous-gradué portant le nom de Jeff Lagarias me fut présenté par Danny Kleitman il y plusieurs années à MIT. Selfridge et moi-même avions investi des milliers d'heures sur deux Olivettis, pendant que Mike Williams utilisait une machine plus sophistiquée ici au sous-sol de cet édifice [the Mathematical Sciences building à l'Université de Calgary], à l'époque où il n'y avait que 4 étages.*

Jacobson décrit comment à n'importe quel moment de la journée, l'ordinateur du bureau de Richard montrait au moins une fenêtre ouverte qui calculait activement les termes d'une suite aliquote et qui effectuait les factorisations requises. À l'époque de cette requête auprès de Jacobson, Richard utilisait Pari/GP pour itérer manuellement les termes de la suite

aliquote pour $n = 99225$ parce que, toujours selon ses mots, " le plus petit nombre impair qui donne des signes de convergence vers l'infini, c'est 99225 ". Il a étendu cette suite bien au-delà de 700 termes et avait fréquemment besoin de factoriser des entiers de plus de 100 chiffres décimaux. Jacobson a éventuellement automatisé le processus de factorisation pour Richard et l'aida à étendre la suite à plus de 3400 termes, ce qui donna naissance à un projet plus ambitieux. En 1976, Richard avait écrit un survol faisant état des connaissances de l'époque sur les méthodes de factorisation [Guy 76], un survol qui devint très populaire avec la venue du cryptosystème RSA en 1978. Suite à des calculs préalables entrepris par l'ancien étudiant à la maîtrise Stan Devitt de Richard en 1976 [Devitt 76], qui assurément furent inspirés par le survol de Richard, il s'avère que Richard, Jacobson et les étudiants de Calgary, Kevin Chum et Anton Mosunov, performèrent des calculs poussés sur la moyenne géométrique de $s(n)/n$ en modélisant une suite aliquote comme une chaîne de Markov [Chum et al. 18]. Pour le plus grand plaisir de Richard, grâce à une floppée d'autres résultats numériques sur les suites aliquotes, ces résultats fournissent une évidence empirique que la moyenne géométrique des $s(n)/n$ dépasse 1, comme Richard l'espérait et le prédisait. Jacobson et ses étudiants poursuivent leurs travaux sur la conjecture de Guy-Selfridge.

Richard aimait trouver des arrangements de nombres assujettis à certaines contraintes sur leurs relations avec leurs voisins. Il était intrigué par la simplicité de telles questions et par l'immense difficulté, ce qui était fréquemment le cas, de prouver l'existence de tels arrangements ou même de les dénombrer. Richard était convaincu que pour tout n suffisamment grand, il existe des permutations des entiers $1, 2, \ldots, n$ telles que la somme de deux termes consécutifs est un carré, un cube, un nombre triangulaire ou pentagonal ou un polynôme " raisonnable " en n. Le cas d'être un carré n'a été résolu que récemment par R. Gerbitz [Gerbitz 2018] qui a établi une réponse affirmative pour tout $n \geq 25$ ($n \geq 32$ pour des arrangements circulaires). Tous les autres cas sont encore des problèmes ouverts. Dans un merveilleux article dont le titre est "Fibonacci plays Billiards" [Berlekamp and Guy 03], Elwin Berlekamp et Richard ont donné une caractérisation complète des valeurs de n qui admettent des permutations des n premiers entiers positifs telles que la somme de deux voisins quelconques est un nombre de Fibonacci ou un nombre de Lucas. Le titre de l'article est né de la méthodologie qui a été utilisée et qui facilite la recherche d'arrangements de nombres en plaçant les nombres $1, 2, \ldots, n$ sur le périmètre d'une table de billiard et en considérant le parcours des balles de billiard lorsqu'elles rebondissent sur les rebords coussinés avec un angle de 45 degrés.

Pendant l'été de 2017, le centenaire Richard, avec l'aide de sa collègue de Calgary, Renate Scheidler, recruta Ethan White, un étudiant sous-gradué à l'époque, pour considérer des problèmes analogues où les sommes sont remplacées par des différences en valeurs absolues. À un moment donné, ils ont résolu la question des arrangements circulaires où les différences en valeurs absolues de deux termes adjacents prennent l'une des deux valeurs de l'ensemble $\{a, b\}$. Aidés par les calculs de White, ils ont utilisé le "mur des nombres" de Richard [Conway and Guy 96, pp. 85-89] pour essayer de découvrir des récurrences linéaires pour les décomptes $N_{a,b}(n)$ de tels arrangements de longueur n. Ils ont trouvé des relations explicites pour les paires $(a, b) = (1, 2), (1, 3), (2, 3), (1, 4)$ et ont éventuellement employé la méthode " graph theoretic transfer matrix " pour prouver que $N_{a,b}(n)$ satisfait une relation de récurrence linéaire lorsque de tels arrangements existent pour une paire donnée (a, b) [White et al. 20].

Richard s'intéressait aussi aux problèmes Diophantiens, particulièrement à la question de savoir si des entiers peuvent être représentés par certains types d'équations. Une *équation Diophantienne* est une équation pour laquelle les solutions sont restreintes aux entiers ou aux nombres rationnels. Par exemple, $(x, y) = (8, 3)$ est une solution de l'équation Diophantienne $x^2 - 7y^2 = 1$. Richard démarra dans ce domaine une collaboration de longue durée avec Andrew Bremner à la fin des années 1980 qui dura plus de 15 ans. En 1993, Bremner, Richard et Richard Nowakowski ont résolu la question, posée pour la première fois par Melvyn J. Knight, de déterminer les entiers n qui peuvent être représentés sous la forme

$$n = (x + y + z)(1/x + 1/y + 1/z),$$

avec des entiers x, y, z [Bremner et al. 93]. Par exemple, pour $n = 62$, on a la solution $x = 5075$, $y = 128050$, $z = 160602$. Ils ont trouvé que cette question se ramène au problème de trouver les points entiers d'une certaine courbe elliptique dont la 2-torsion est rationnelle et ils ont calculé le rang de Mordell-Weil de cette courbe pour tout n avec $|n| \leq 1000$.

Les suites d'entiers dans le contexte de la géométrie attirait aussi Richard. Un exemple d'une question avec cette saveur est le problème de paver un rectangle $4 \times (n - 1)$ avec des dominos ou des tuiles 1×2. Richard savait que la suite $(A_n)_{n \geq 0}$ représentant le nombre de ces pavages distincts satisfait une récurrence linéaire d'ordre 4:

$$A_k = A_{k-1} + 5A_{k-2} + A_{k-3} - A_{k-4}$$

avec $A_0 = 0$, $A_1 = 1$, $A_2 = 1$, $A_3 = 5$, $A_4 = 11$, $A_5 = 36$, etc. Il nota que la suite $(A_n)_{n \geq 0}$ semblait être une suite de divisibilités: A_n divise A_m chaque fois que n divise m. Cette observation engendra une collaboration avec Hugh Williams et son ancien étudiant au doctorat Eric Roettger qui produisit une série d'articles [Roettger et al. 13, Roettger et al. 15, Williams and Guy 15], culminant avec une solution du problème ouvert de Lucas consistant à généraliser les suites de Lucas au niveau des récurrences linéaires d'ordre supérieur.

Sur plusieurs dizaines d'années, quasi-simultanément à la conception et la rédaction du célèbre *Triangle book* de John Conway [Conway and Sigur 15], Richard compila et prouva une quantité de résultats dans une monographie intitulé simplement *The Triangle* [Guy 20]. En plus d'une riche quantité de propriétés des triangles d'un point de vue de la géométrie et de la théorie des nombres, ce travail de 240 pages contient une collection de figures exquises toutes méticuleusement conçues de main de maître grâce au talent de sorcier de Richard et à sa maîtrise de LaTeX. Richard était en particulier captivé par la construction expliquée et joliment illustrée aux page 43 et suivante [Guy 20]. À partir d'un triangle ABC, prenez n'importe quel point P sur son cercle circonscrit et considérez sa réflexion sur le côté BC pour obtenir un point A' qui permet de définir un nouveau triangle $A'BC$. Intersectez la perpendiculaire sur le côté BC avec le cercle circonscrit de ce nouveau triangle pour obtenir un point P'. De façon semblable, prenez la réflexion de P sur les côtés AB et BC pour obtenir les triangles $AB'C$ and ABC' et les points Q', R'. Les trois points P', Q', R' sont sur une *droite de Steiner* parallèle à la *droite de Wallace* de P à une distance de P deux fois plus grande. Répétez tout le processus avec les points P', Q', R' pour générer 9 points supplémentaires, etc. Richard compare la construction permettant de calculer les multiples scalaires d'un point fixe donné d'une courbe elliptique et il était curieux d'en connaître plus sur le comportement de cette tri-suite (*tri-séquence*), en particulier sur la possibilité de périodicité. Richard accorde à Andrew Bremner le crédit de la découverte de quatre 3-cycles et par la suite à Alex Fink, dont il était le mentor pendant ses années comme étudiant sous-gradué à Calgary, pour avoir observé que chaque point P de départ mène à trois 6-cycles.

Richard avait un don phénoménal gour reconnaître les motifs et une habileté étrange pour séparer le bon grain d'une belle structure de théorie des nombres de l'ivraie des similarités accidentelles. Dans le cours de ses investigations sur différentes suites, Richard a découvert ce qu'il a appelé avec beaucoup d'esprit " *La loi forte des petits nombres* " ("*The Strong Law of Small Numbers*"). Dans un article très engagé et ayant un grand impact, portant le même titre [Guy 88], il commenta 35 exemples de motifs (patterns) qui semblent apparaître quand on considère de petites valeurs de n. Certains fonctionnent, mais plusieurs ne tiennent pas la route. Il conclua qu'il n'y a pas suffisamment de petits nombres pour répondre à de nombreuses demandes qui en étaient faites. Il donna une suite à cet article deux ans plus tard avec sa seconde loi [Guy 90], laquelle affirme " *Quand deux nombres semblent égaux, ce n'est pas nécessairement le cas.* " (" *When two numbers look equal it ain't necessarily so* ". On devrait obliger tout étudiant gradué en mathématiques à lire ces deux articles.

L'une des contributions de Richard en mathématiques appelées à défier le temps est sa monographie *Unsolved Problems in Number Theory* [Guy 04]. C'est une merveilleuse compilation de problèmes en Théorie des nombres avec des commentaires qui en est à sa troisième édition et qui nous contamine (positivement au sens figuré). Ce volume remarquable a stimulé des théoriciens des nombres en puissance, parmi lesques plusieurs sont devenus des étoiles et continue d'être une source d'inspiration pour les érudits du domaine.

Esquisses biographiques

Michael J. Jacobson, Jr. *est professeur au département d'informatique à l'Université de Calgary, effectuant de la recherche en cryptographie et en théorie calculatoire des nombres avec une emphase particulière sur les algorithmes dans les corps globaux.*

Hugh C. Williams *est professeur émérite au département de mathématiqes et de statistique et il a détenu la chaire iCORE en théorie algorithmique des nombres et en cryptographie à l'Université de Calgary. Il est aussi professeur émérite au départment d'informatique à l'Université du Manitoba. Ses intérêts en recherche incluent la théorie calculatoire des nombres, la cryptographie, l'histoire des mathématiques et les calculs sur l'ordinateur.*

Références

[Berlekamp and Guy 03] E. Berlekamp and R. K. Guy, Fibonacci plays Billiards, arXiv:2002.03705 [math.HO].

[Bosma and Kane 12] W. Bosma and B. Kane, The aliquot constant, *Quart. J. Math*. 63 (2012), no. 2, 309-323.

[Bremner et al 93] A. Bremner, R. K. Guy and R. J. Nowakowski, Which integers are representable as the product of the sum of three integers with the sum of their reciprocals? *Math. Comp*. **61** (1993), no. 203, 117-130.

[Catalan 88] E. Catalan, Propositions et questions diverses, *Bull. Soc. Math. France* **16** (1888), 128-129.

[Chum et. al. 18] K. Chum, R. K. Guy, M. J. Jacobson, Jr. and A. S. Mosunov, Numerical and Statistical Analysis of Aliquot Sequences, *Experim. Math.*, DOI:10.1080/10586458.2018.1477077 (2018)

[Conway and Guy 96] J. H. Conway and R. K. Guy, *The Book of Numbers*, Springer, 1996.

[Conway and Sigur 15] J. H. Conway and S. Sigur, *The Triangle Book*, A K Peters 2015.

[Devitt 76] J. S. Devitt, Aliquot Sequences, Master's thesis, University of Calgary 1976.

[Dickson 13] L. E. Dickson, Theorems and Tables on the Sums of Divisors of a Number, *Quart. J. Math*. **44** (1913), 264-296.

[Dickson 66] L. E. Dickson, *History of the Theory of Numbers*, Volumes I-III, Reprintings of the originals, Chelsea Publishing Co., New York 1966.

[Guy 58] R. K. Guy, Two theorems on partitions. *Math. Gaz*. **42** (1958), 84-86.

[Guy 76] R. K. Guy, How to factor a number. Proc. Fifth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1975), pp. 49-89. *Congressus Numerantium* **XVI**, Utilitas Math. Publ., Winnipeg, Man., 1976.

[Guy 88] R. K. Guy, The strong law of small numbers, *Amer. Math. Monthly* **95** (1988), no. 8, 697-712.

[Guy 90] R. K. Guy, The second strong law of small numbers. *Math. Mag*. **63** (1990), no. 1, 3-20.

[Guy 04] R. K. Guy, *Unsolved Problems in Number Theory*, third ed., Problem Books in Mathematics. Springer, New York, 2004.

[Guy 20] R. K. Guy, The Triangle, arXiv:1910.03379v1 [math.HO].

[Guy and Selfridge 75] R. K. Guy and J. L. Selfridge, What drives an aliquot sequence? *Math. Comp*. **29** (1975), no. 129, 101-107.

[Pomerance 18] C. Pomerance, The first function and its iterates, In: *Connections in Discrete Mathematics: A Celebration of the Work of Ron Graham* (S. Butler, J. Cooper, G. Hurlbert, eds), pp. 125-138, Cambridge University Press, 2018.

[Roettger et al 13] E. L. Roettger, H. C. Williams and R. K. Guy, Some extensions of the Lucas functions, in: *Number theory and related fields*, 271-311, Springer Proc. Math. Stat., 43, Springer, New York, 2013.

[Williams and Guy 15] H. C. Williams and R. K. Guy, Odd and even linear divisibility sequences of order 4, *Integers* **15** (2015), Paper No. A33.

[Roettger et al 15] E. L. Roettger, H. C. Williams and R. K. Guy, Some primality tests that eluded Lucas. *Des. Codes Cryptogr*. 77 (2015), no. 2-3, 515-539.

[White et al 20] E. White, R. K. Guy and R. Scheidler, Difference Necklaces, arXiv:2006.15250 [math.CO].

[Yoshihara 04] N. Yoshigahara, *Puzzles 101: A Puzzlemaster's Challenge*, A K Peters, Natick MA, 2004.