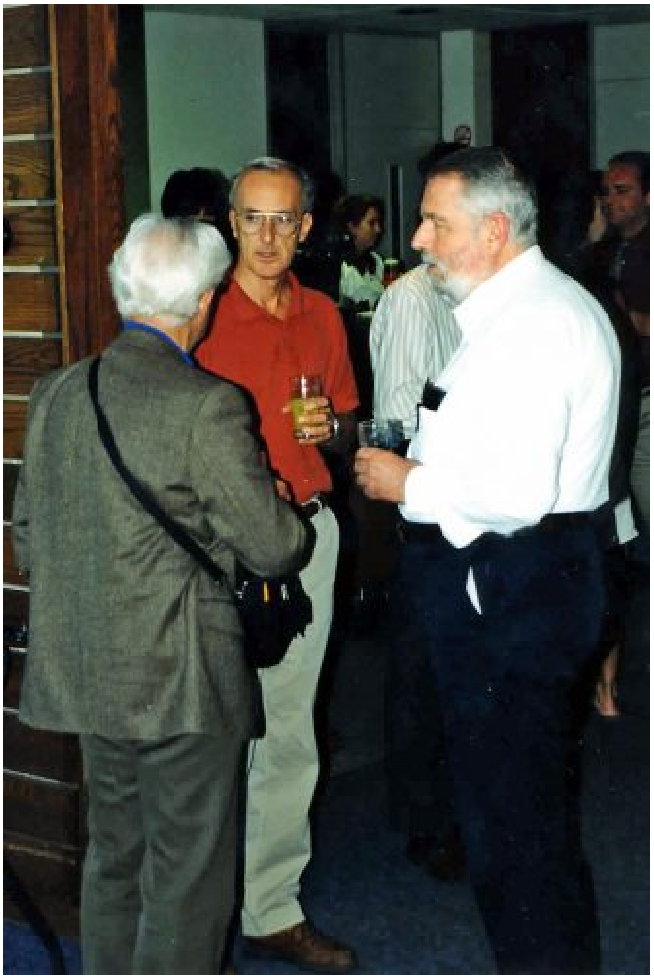
Richard Guy and Number Theory

Richard Kenneth Guy (1916 - 2020)

September 2020 (Vol. 52, No. 4)

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

Even as a small child Richard Guy was fascinated by numbers. When he was 17, he purchased a copy of Dickson's encyclopaedic *History of the Theory of Numbers* [Dickson 66] and fell under its spell. The cost of this book at the time was 6 guineas, a lot of money—more than he paid for his Master's degree from Cambridge. Dickson's history continued to exert a strong influence on Richard throughout his academic life. He published his first significant paper in number theory in 1958 [Guy 58]. Arguably, no work of Richard's exemplifies his love of numbers more than his wonderful *Book of Numbers*, joint with John H. Conway [Conway and Guy 96]. Richard's substantial volume of published works in number theory include some 50 coauthors, among them Elwin Berlekamp, John Conway, Paul Erdös, Derrick Lehmer, Yuri Matiyasevich, Alexander Oppenheim, John Selfridge, and Daniel Shanks. His predominant number theoretic interest was in integer sequences in any form or context, including their appearance in combinatorics, geometry and Diophantine problems. Richard's contributions to the field are too numerous to allow a complete account here, so we only provide some examples of his work, with special attention to research he conducted in his late 90s and beyond.



Richard, Andrew Bremner and John Selfridge at CNTA-VI, Winnipeg, 2006

> *Arguably, no work of Richard's exemplifies his love of numbers more than his wonderful Book of Numbers, joint with John H. Conway*

Tweet

Aliquot sequences were a particular life-long passion of Richard's. These are iterates n, $s(n)$, $s(s(n))$, … , $s^{(k)}(n)$ of the sum of proper (or aliquot) divisors function $s(n) = \sigma(n) - n$, for n a positive integer. Catalan [Catalan 88], later corrected by Dickson [Dickson 13], conjectured that all aliquot sequences terminate or become periodic and are hence bounded. The smallest integer for which this conjecture remains unsettled is $n = 276$; as of the time of writing this article, its aliquot sequence has been computed to 2139 terms and the 2140th term is composite and known to have a(n as yet unfactored) divisor of 213 decimal digits. In a series of reports published in the 1970s, Richard and John Selfridge discovered that under certain conditions aliquot sequences can become quite long. This led them to propose a counter-conjecture in 1975 [Guy and Selfridge 75] that many, perhaps almost all, sequences for even n diverge. The question of which conjecture is correct remains unresolved.

Richard was keenly interested in evangelizing his conjecture and continued to work on it to the end. A 2012 result of Bosma and Kane [Bosma and Kane 12] shows that the geometric mean (over all n) of the *amplification* $s(2n)/2n$ is less than 1, thus suggesting that the terms of an aliquot sequence tend to decrease on average. Richard believed that this finding does not capture the true nature of aliquot sequences because it does not take into account how frequently (if ever) an integer occurs as a value $s(2n)$, and it fails to account for the *guides* and *drivers* described in [Guy and Selfridge 75]. These are certain divisors of $s^{(k)}(n)$ that persist from one term to another with high probability and that in almost all cases cause the sequence to increase. Indeed, Pomerance [Pomerance 18] showed that the geometric mean of $s(n)/n$ for $n \equiv 2 \pmod 4$ is less than 1, whereas it exceeds 1 for $n \equiv 0 \pmod 4$.

With further analytic results seemingly out of reach for the time being, Richard instead turned to a quest for stronger numerical evidence supporting his point of view. Mike Jacobson recounts how Richard began to subtly recruit him to join in this cause, beginning with an e-mail with the rather cryptic subject line "Would you like to factor a number?" The number was of course factored, and when asked what this was about, Richard gladly offered an explanation that began as follows:

> *I'm calculating an aliquot sequence. This is rather a lost cause, but it has grabbed me from even before a bright young undergrad named Jeff Lagarias was introduced to me by Danny Kleitman long years ago at MIT. Selfridge and I devoted thousands of hours on two Olivettis, and Mike Williams used a more sophisticated machine down in the basement of this building [the Mathematical Sciences building at the University of Calgary], when it was only four stories high.*

Jacobson describes how at any time, Richard's office computer showed at least one open window actively computing terms of some aliquot sequence and performing the necessary factorizations. At the time of the initial request to Jacobson, Richard was using Pari/GP to manually iterate the aliquot sequence for n = 99225 because, again in his words, "the smallest odd number which shows any signs of getting to infinity is 99225". He had extended this sequence to well over 700 terms and regularly needed to factor integers of over 100 decimal digits. Jacobson eventually automated the factorization process for Richard and helped him extend the sequence to more than 3400 terms, which led to an even more ambitious project. In 1976, Richard had written a survey of then state-of-the-art integer factorization methods [Guy 76] that became very influential with the advent of the RSA cryptosystem in 1978. Following earlier computations undertaken by Richard's former Master's student Stan Devitt in 1976 [Devitt 76] that were surely inspired by Richard's survey, Richard, Jacobson and then Calgary students Kevin Chum and Anton Mosunov performed extensive computations of the geometric mean of $s(n)/n$ by modeling an aliquot sequence as a Markov chain [Chum et. al. 18]. To Richard's delight, along with a variety of other related numerical results capturing data of actual aliquot sequences, these computations provide empirical evidence that the geometric mean of $s(n)/n$ in fact exceeds 1, exactly as he had hoped and predicted. Work on the Guy-Selfridge conjecture by Jacobson and his students is ongoing.

Richard was fond of finding arrangements of numbers subject to certain constraints governing neighbour relationships. He was intrigued by the simplicity of such questions and the frequent immense difficulty of proving even the simplest existence or counting results on such arrangements. Richard was convinced that for all sufficiently large n, there exist permutations of the integers 1, 2, … , n such that any two adjacent entries sum to a square, cube, triangular or pentagonal number, or any "reasonable" polynomial in n. The square case was only recently settled by R. Gerbitz [Gerbitz 2018] who established an affirmative answer for all $n \geq 25$ ($n \geq 32$ for circular arrangements). All other cases remain wide open. In a delightful manuscript entitled "Fibonacci plays Billiards" [Berlekamp and Guy 03], Elwin Berlekamp and Richard gave a complete characterization of values n that admit permutations of the first n positive integers such that any two neighbours sum to a Fibonacci or Lucas number. The title stems from a methodology that facilitates the search for number arrangements by placing the numbers 1, 2, … , n on the perimeter of a billiard table and considering paths of billiard balls as they bounce off the corresponding points on its cushions at a 45 degree angle. In the summer of 2017, then centenarian Richard, with help from Calgary colleague Renate Scheidler, recruited Ethan White, an undergraduate student at the time, to look into analogous problems where sums are replaced by absolute differences. Eventually, they settled on the question of circular arrangements where the absolute difference of any two adjacent terms takes on one of two fixed given values a or b. Aided by White's computations, they employed Richard's number wall [Conway and Guy 96, pp. 85-89] to try to discover linear recurrences for the counts $N_{a,b}(n)$ of such arrangements of length n. They found explicit recurrence relations for the pairs (a,b) = (1,2), (1,3), (2,3), (1,4) and eventually employed the graph theoretic transfer matrix method to prove that $N_{a,b}(n)$ satisfies a linear recurrence relation whenever such arrangements exist for a given pair (a,b) [White et al 20].

Richard was also interested in Diophantine problems, particularly the question of whether integers could be represented by certain types of equations. A *Diophantine equation* is an equation for which solutions are restricted to the integers or rational numbers; for example, $(x,y) = (8,3)$ is a solution to the Diophantine equation $x^2 - 7y^2 = 1$. Richard began a long-term collaboration in this area with Andrew Bremner in the late 1980s that lasted more than 15 years. In 1993 Bremner, Richard and Richard Nowakowski settled the question, first posed by Melvyn J. Knight, of which integers n can be represented in the form

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

with integers x, y, z [Bremner et al 93]. For example, for $n = 62$, we have the solution $x = 5075$, $y = 128050$, $z = 160602$. They found that this question reduces to the problem of finding integer points on a certain elliptic curve with rational 2-torsion and computed the Mordell-Weil rank of this curve for all n with $|n| \leq 1000$.

Integer sequences in the context of geometry also appealed to Richard. An example of a question of this flavour is the problem of tiling a 4× (n-1) rectangle with dominos (1×2 tiles). Richard knew that the sequence $(A_n)_{n \geq 0}$ representing the number of distinct such tilings satisfies the fourth order linear recurrence

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

with $A_0 = 0$, $A_1 = 1$, $A_2 = 1$, $A_3 = 5$, $A_4 = 11$, $A_5 = 36$, etc. He noticed that the sequence $(A_n)_{n \geq 0}$ seemed to be a divisibility sequence (A_n divides A_m whenever n divides m). This observation led to a collaboration with Hugh Williams and his former doctoral student Eric Roettger that produced a series of papers [Roettger et al 13, Roettger et al 15, Williams and Guy 15], culminating with a solution to Lucas' unsolved problem of generalizing the Lucas sequences to the setting of higher order recurrences.

Over several decades, somewhat simultaneously with the conception and writing of John Conway's renowned *Triangle Book* [Conway and Sigur 15], Richard compiled and proved a comprehensive body of results in a monograph simply entitled *The Triangle* [Guy 20]. In addition to a wealth of number theoretic and geometric facts about triangles, this 240 page work contains a collection of exquisite figures, all meticulously produced through Richard's wizard mastery of LaTeX. Richard was captivated in particular by the following construction, explained and beautifully illustrated on pp. 43 ff [Guy 20]. For a triangle *ABC*, take any point *P* on its circumcircle and reflect it on the edge *BC* to obtain a point *A'* that defines a new triangle *A'BC*. Intersect the perpendicular to the edge *BC* with the circumcircle of this new triangle to obtain a point *P'*. Similarly, reflect *P* on the edges *AB* and *BC* to obtain triangles *AB'C* and *ABC'* and points *Q'*, *R'*. The three points *P'*, *Q'*, *R'* lie on a *Steiner line* parallel to the *Wallace line* of *P* and twice its distance to *P*. Repeat the entire process starting with *P'*, *Q'*, *R'* to generate 9 further points etc. Richard likened this construction to computing scalar multiples of a given fixed point on an elliptic curve and was curious about the behaviour of this *trisequence*, particularly the possibility of periodicity. Richard credits Andrew Bremner with the discovery of four 3-cycles and subsequently Alex Fink, whom he mentored during Alex's undergraduate years at Calgary, for observing that every starting point *P* leads to three 6-cycles.

The University of Calgary's Department of Mathematics and Statistics celebrates Richard's 100th birthday, 2016

Richard had a phenomenal gift for pattern recognition and an uncanny ability of separating the grain of beautiful number theoretic structure from the chaff of coincidental similarities. In the course of his investigations of various sequences, Richard discovered what he wittily referred to as "The Strong Law of Small Numbers". In his very engaging and influential paper of the same title [Guy 88], he discussed 35 examples of patterns that seem to appear when we check small values of *n*. Some work, but many don't. He concluded that there aren't enough small numbers to meet the many demands made of them. He followed this paper two years later with his second law [Guy 90] which states "When two numbers look equal it ain't necessarily so." Both these papers should be required reading by any graduate student of mathematics.

One of Richard's most lasting contributions to the field is his monograph *Unsolved Problems in Number Theory* [Guy 04]. A marvellous compilation of number theoretic problems and commentary that has gone through three editions and is instantly infectious, this remarkable book has stimulated generations of aspiring number theorists, several of whom have gone on to have stellar careers, and continues to be a source of inspiration for scholars and in the field.

Michael J. Jacobson, Jr. *is a Professor in the Department of Computer Science at the University of Calgary, conducting research in cryptography and computational number theory, with particular focus on algorithms in global fields.*

Hugh C. Williams *is a Professor Emeritus in the Department of Mathematics and Statistics and the former iCORE Chair in Algorithmic Number Theory and Cryptography at the University of Calgary as well as Professor Emeritus in the Department of Computer Science at the University of Manitoba. His research interests include computational number theory, cryptography and the history of mathematics and computation.*

[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.