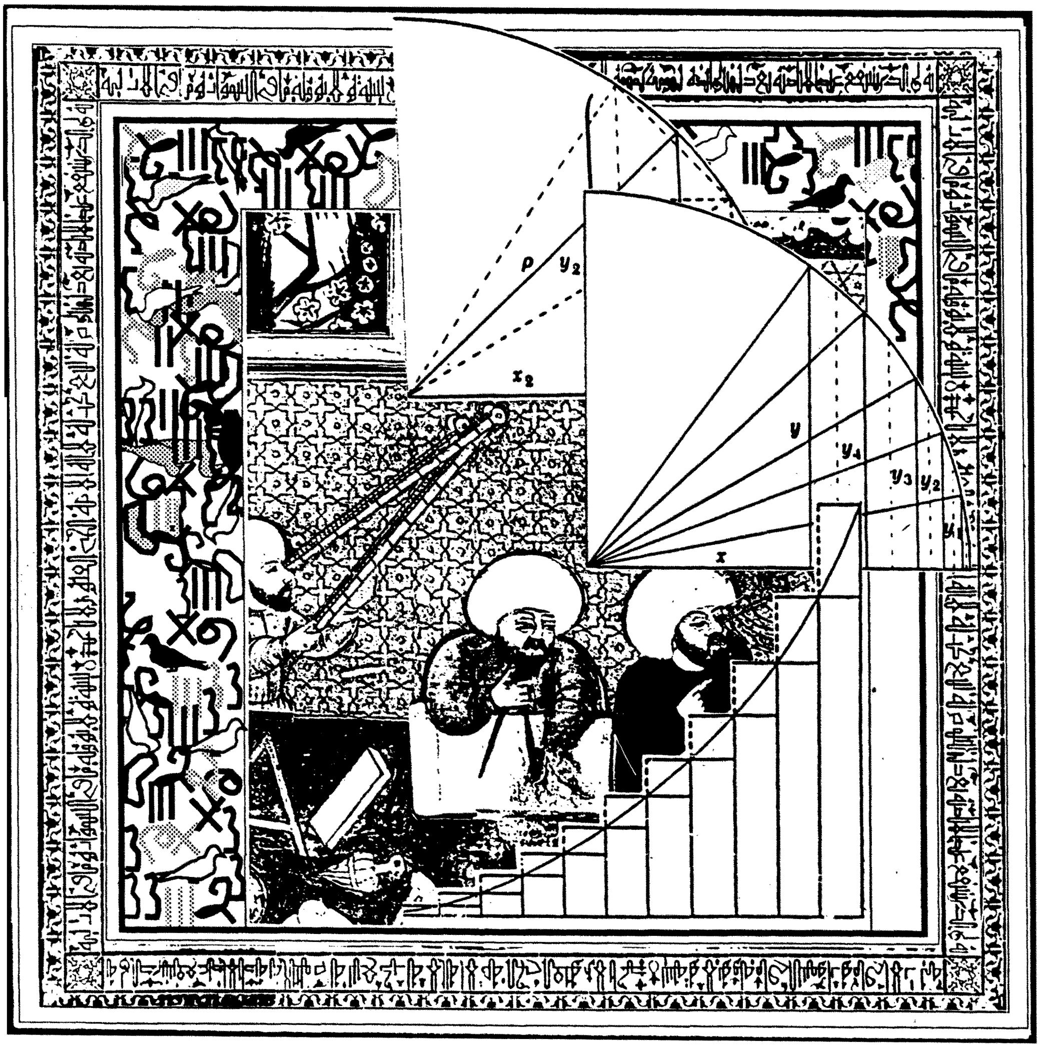
Vol. 68, No. 3 June 1995

MATHEMATICS MAGAZINE



- Ideas of Calculus in Islam and India
- Selling Primes
- Derivatives of Noninteger Order

An Official Publication of The MATHEMATICAL ASSOCIATION OF AMERICA

EDITORIAL POLICY

The aim of *Mathematics Magazine* is to provide lively and appealing mathematical exposition. This is not a research journal and, in general, the terse style appropriate for such a journal (lemma-theorem-proof-corollary) is not appropriate for an article for the *Magazine*. Articles should include examples, applications, historical background, and illustrations, where appropriate. They should be attractive and accessible to undergraduates and would, ideally, be helpful in supplementing undergraduate courses or in stimulating student investigations. Articles on pedagogy alone, unaccompanied by interesting mathematics, are not suitable. Neither are articles consisting mainly of computer programs unless these are essential to the presentation of some good mathematics. Manuscripts on history are especially welcome, as are those showing relationships between various branches of mathematics and between mathematics and other disciplines.

The full statement of editorial policy appears in this *Magazine*, Vol. 64, pp. 71–72, and is available from the Editor. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, nor published by another journal or publisher.

Send new manuscripts to: Paul Zorn, Editor-Elect, Department of Mathematics, St. Olaf College, 1520 St. Olaf Avenue, Northfield, MN 55057-1098. Manuscripts should be typewritten and double spaced and prepared in a style consistent with the format of *Mathematics Magazine*. Authors should submit the original and two copies and keep one copy. In addition, authors should supply the full five-symbol Mathematics Subject Classification number, as described in *Mathematical Reviews*, 1980 and later. Illustrations should be carefully prepared on separate sheets in black ink, the original without lettering and two copies with lettering added. Do not use staples.

Cover illustration: Carolyn Westbrook. Exterior border from mosaics in Hakim Bey Mosque, Konya. Astronomers from a 16th-century Persian illumination, in *Mathematics*, Time, Inc., NY, 1963, p. 71.

AUTHORS

Victor J. Katz has been solving problems for the MAA during the 1994–95 academic year. Normally, he is professor of mathematics at the University of the District of Columbia. Although he received his Ph.D. from Brandeis University in algebraic number theory, he has long been interested in the history of mathematics and its use in the teaching of mathematics. He has recently written the textbook *A History of Mathematics: An Introduction* (HarperCollins, 1993) and, since 1989, has edited the *Newsletter* of the International Study Group on the Relations Between History and Pedagogy of Mathematics, an affiliate of the International Commission on Mathematics Instruction.

Paulo Ribenboim, born in Reofe, Brazil, received his B.Sc. degree in mathematics at age 20 at the University of Rio de Janeiro. His first paper had already appeared in 1949, while studying ordered structures with A. Monteiro. He received his Ph.D. at the University of Sao Paulo in 1957, the same year he became one of the first research professors at the IMPA (in Rio de Janeiro) and the youngest fellow of the Brazilian Academy of Sciences. Recipient of a Fullbright Fellowship in 1959, he was appointed visiting associate professor at the University of Illinois at Urbana. In 1962, he began teaching at Queen's University in Kingston, Ontario, where he stayed for 32 years until his recent retirement. In 1969, he was elected to the Royal Society of Canada and, in 1977, he received an honorary degree from the Universit de Calm (France).

Kenneth S. Miller received his Ph.D. from Columbia University in 1950 and did his post-doctoral work at the Institute for Advanced Study in Princeton, NJ. During this time, his interests shifted from differential equations to mathematical machines to multivariate distributions to complex stochastic processes. Through a convoluted sequence of coincidences that spanned 30 years, he came to know Bertram Ross (late professor of mathematics at the University of New Haven). This relationship sparked an interest in the fractional calculus, of which this paper is one product.

Vol. 68, No. 3 June 1995

MATHEMATICS MAGAZINE

The *MATHEMATICS MAGAZINE* (ISSN 0025-570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, D.C. 20036 and Montpelier, VT, bimonthly except July/August.
The annual subscription price for the MATHEMATICS MAGAZINE to an individual member of the Association is $16 included as part of the annual dues. (Annual dues for regular members, exclusive of annual subscription prices for MAA journals, are $64. Student and unemployed members receive a 66% dues discount; emeritus members receive a 50% discount; and new members receive a 40% dues discount for the first two years of membership.) The nonmember/library subscription price is $68 per year.
Subscription correspondence and notice of change of address should be sent to the Membership/Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036. Microfilmed issues may be obtained from University Microfilms International, Serials Bid Coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

Advertising correspondence should be addressed to Ms. Elaine Pedreira, Advertising Manager, The Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036.

Second class postage paid at Washington, D.C. and additional mailing offices.

Postmaster: Send address changes to Mathematics Magazine Membership/Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036-1385.

PRINTED IN THE UNITED STATES OF AMERICA

ARTICLES

Ideas of Calculus in Islam and India

VICTOR J. KATZ
University of the District of Columbia
Washington, DC 20008

Introduction

Isaac Newton created his version of the calculus during the years from about 1665 to 1670. One of Newton's central ideas was that of a power series, an idea he believed he had invented out of the analogy with the infinite decimal expansions of arithmetic [**9**, Vol. III, p. 33]. Newton, of course, was aware of earlier work done in solving the area problem, one of the central ideas of what was to be the calculus, and he knew well that the area under the curve $y = x^n$ between $x = 0$ and $x = b$ was given by $b^{n+1}/(n+1)$. (This rule had been developed by several mathematicians in the 1630s, including Bonaventura Cavalieri, Gilles Persone de Roberval, and Pierre de Fermat.) By developing power series to represent various functions, Newton was able to use this basic rule to find the areas under a wide variety of curves. Conversely, the use of the area formula enabled him to develop power series. For example, Newton developed the power series for $y = \arcsin x$, in effect by defining it in terms of an area and using the area formula. He then produced the power series for the sine by solving the equation $y = \arcsin x$ for $x = \sin y$ by inversion of the series. What Newton did not know, however, was that both the area formula—which he believed had been developed some 35 years earlier—and the power series for the sine had been *known for hundreds of years* elsewhere in the world. In particular, the area formula had been developed in Egypt around the year A.D. 1000 and the power series for the sine, as well as for the cosine and the arctangent, had been developed in India, probably in the fourteenth century. It is the development of these two ideas that will be discussed in this article.

Before going back to eleventh-century Egypt, however, we will first review the argument used both by Fermat and Roberval in working out their version of the area formula in 1636. In a letter to Fermat in October of that year, Roberval wrote that he had been able to find the area under curves of the form $y = x^k$ by using a formula—whose history in the Islamic world we will trace—for the sums of powers of the natural numbers: "The sum of the square numbers is always greater than the third part of the cube which has for its root the root of the greatest square, and the same sum of the squares with the greatest square removed is less than the third part of the same cube; the sum of the cubes is greater than the fourth part of the fourth power and with the greatest cube removed, less than the fourth part, etc." [**5**, p. 221]. In other words, finding the area of the desired region depends on the formula

$$\sum_{i=1}^{n-1} i^k < \frac{n^{k+1}}{k+1} < \sum_{i=1}^{n} i^k.$$

Fermat wrote back that he already knew this result and, like Roberval, had used it to determine the area under the graph of $y = x^k$ over the interval $[0, x_0]$. Both men saw that if the base interval was divided into n equal subintervals, each of length x_0/n, and if over each subinterval a rectangle whose height is the y-coordinate of the right endpoint was erected (see FIGURE 1), then the sum of the areas of these N circumscribed rectangles is

$$\frac{x_0^k}{n^k}\frac{x_0}{n} + \frac{(2x_0)^k}{n^k}\frac{x_0}{n} + \cdots + \frac{(nx_0)^k}{n^k}\frac{x_0}{n} = \frac{x_0^{k+1}}{n^{k+1}}(1^k + 2^k + \cdots + n^k).$$

Similarly, they could calculate the sum of the areas of the inscribed rectangles, those whose height is the y-coordinate of the left endpoint of the corresponding subinterval. In fact, if A is the area under the curve between 0 and x_0, then

$$\frac{x_0^{k+1}}{n^{k+1}}\left(1^k + 2^k + \cdots + (n-1)^k\right) < A < \frac{x_0^{k+1}}{n^{k+1}}(1^k + 2^k + \cdots + n^k).$$

The difference between the outer expressions of this inequality is simply the area of the rightmost circumscribed rectangle. Because x_0 and $y_0 = x_0^k$ are fixed, Fermat knew that the difference could be made less than any assigned value simply by taking n sufficiently large. It follows from the inequality cited by Roberval that both the area A and the value $x_0^{k+1}/(k+1) = x_0y_0/(k+1)$ are squeezed between two values whose difference approaches 0. Thus Fermat and Roberval found that the desired area was $x_0y_0/(k+1)$.

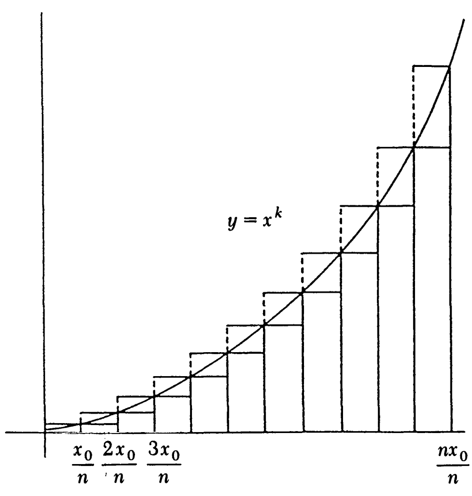


FIGURE 1

The obvious question is how either of these two men discovered formulas for the sums of powers. But at present, there is no answer to this question. There is nothing extant on this formula in the works of Roberval other than the letter cited, and all we have from Fermat on this topic, in letters to Marin Mersenne and Roberval, is a general statement in terms of triangular numbers, pyramidal numbers, and the other numbers that occur as columns of Pascal's triangle. (We note that Fermat's work was done some twenty years before Pascal published his material on the arithmetical triangle; the triangle had, however, been published in many versions in China, the Middle East, North Africa, and Europe over the previous 600 years. See [4], pp. 191–192; 241–242; 324–325.) Here is what Fermat says: "The last side multiplied by the next greater makes twice the triangle. The last side multiplied by the triangle of the next greater side makes three times the pyramid. The last side multiplied by the pyramid of the next greater side makes four times the triangulotriangle. And so on by the same progression in infinitum" [5, p. 230]. Fermat's statement can be written using the modern notation for binomial coefficients as

$$n\binom{n+k}{k} = (k+1)\binom{n+k}{k+1}.$$

We can derive from this formula for each k in turn, beginning with $k = 1$, an explicit formula for the sum of the kth powers by using the properties of the Pascal triangle. For example, if $k = 2$, we have

$$n\binom{n+2}{2} = 3\binom{n+2}{3} = 3\sum_{j=2}^{n+1}\binom{j}{2}$$
$$= 3\sum_{j=2}^{n+1}\frac{j(j-1)}{2} = 3\sum_{i=1}^{n}\frac{i(i+1)}{2} = 3\sum_{i=1}^{n}\frac{i^2+i}{2}.$$

Therefore,

$$2\frac{n}{3}\frac{(n+2)(n+1)}{2} - \sum_{i=1}^{n} i = \sum_{i=1}^{n} i^2$$

and

$$\sum_{i=1}^{n} i^2 = \frac{n^3+3n^2+2n}{3} - \frac{n^2+n}{2} = \frac{2n^3+3n^2+n}{6} = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}.$$

In general, the sum formula is of the form

$$\sum_{i=1}^{n} i^k = \frac{n^{k+1}}{k+1} + \frac{n^k}{2} + p(n),$$

where $p(n)$ is a polynomial in n of degree less than k, and Roberval's inequality can be proved for each k. We do not know if Fermat's derivation was like that above, however, because he only states a sum formula explicitly for the case $k = 4$ and gives no other indication of his procedure.

Sums of Integer Powers in Eleventh-Century Egypt

The formulas for the sums of the kth powers, however, at least through $k = 4$, as well as a version of Roberval's inequality, were developed some 650 years before the mid-seventeenth century by Abu Ali al-Hasan ibn al-Hasan ibn al-Haytham (965–1039), known in Europe as Alhazen. The formulas for the sums of the squares and cubes were stated even earlier. The one for squares was stated by Archimedes around 250 B.C. in connection with his quadrature of the parabola, while the one for cubes, although it was probably known to the Greeks, was first explicitly written down by Aryabhata in India around 500 [2, pp. 37–38]. The formula for the squares is not difficult to discover, and the one for cubes is virtually obvious, given some experimentation. By contrast, the formula for the sum of the fourth powers is not obvious. If one can discover a method for determining this formula, one can discover a method for determining the formula for the sum of any integral powers. Ibn al-Haytham showed in fact how to develop the formula for the kth powers from $k = 1$ to $k = 4$; all his proofs were similar in nature and easily generalizable to the discovery and proof of formulas for the sum of any given powers of the integers. That he did not state any such generalization is probably due to his needing only the formulas for the second and fourth powers to solve the problem in which he was interested: computing the volume of a certain paraboloid.

Before discussing ibn al-Haytham's work, it is good to briefly describe the world of Islamic science. (See [1] for more details.) During the ninth century, the Caliph al-Ma'mun established a research institute, the House of Wisdom, in Baghdad and invited scholars from all parts of the caliphate to participate in the development of a scientific tradition in Islam. These scientists included not only Moslem Arabs, but also Christians, Jews, and Zoroastrians, among others. Their goals were, first, to translate into Arabic the best mathematical and scientific works from Greece and India, and, second, by building on this base, to create new mathematical and scientific ideas. Although the House of Wisdom disappeared after about two centuries, many of the rulers of the Islamic states continued to support scientists in their quest for knowledge, because they felt that the research would be of value in practical applications.

Thus it was that ibn al-Haytham, born in Basra, now in Iraq, was called to Egypt by the Caliph al-Hakim to work on a Nile control project. Although the project never came to fruition, ibn al-Haytham did produce in Egypt his most important scientific work, the *Optics* in seven books. The *Optics* was translated into Latin in the early thirteenth century and was studied and commented on in Europe for several centuries thereafter. Ibn al-Haytham's fame as a mathematician from the medieval period to the present chiefly rests on his treatment of "Alhazen's problem," the problem of finding the point or points on some reflecting surface at which the light from one of two points outside that surface is reflected to the other. In the fifth book of the *Optics* he set out his solutions to this problem for a variety of surfaces, spherical, cylindrical, and conical, concave and convex. His results, based on six separately proved lemmas on geometrical constructions, show that he was in full command of both the elementary and advanced geometry of the Greeks.

The central idea in ibn al-Haytham's proof of the sum formulas was the derivation of the equation

$$(n+1)\sum_{i=1}^{n} i^k = \sum_{i=1}^{n} i^{k+1} + \sum_{p=1}^{n}\left(\sum_{i=1}^{p} i^k\right). \qquad (*)$$

Naturally, he did not state this result in general form. He only stated it for particular integers, namely $n = 4$ and $k = 1, 2, 3$, but his proof for each of those k is by induction on n and is immediately generalizable to any value of k. (See [7] for details.) We consider his proof for $k = 3$ and $n = 4$:

$$\begin{aligned}(4+1)(1^3+2^3+3^3+4^3) &= 4(1^3+2^3+3^3+4^3) + 1^3+2^3+3^3+4^3\\ &= 4\cdot 4^3 + 4(1^3+2^3+3^3) + 1^3+2^3+3^3+4^3\\ &= 4^4 + (3+1)(1^3+2^3+3^3) + 1^3+2^3+3^3+4^3.\end{aligned}$$

Because equation $(*)$ is assumed true for $n = 3$,

$$(3+1)(1^3+2^3+3^3) = 1^4+2^4+3^4 + (1^3+2^3+3^3) + (1^3+2^3) + 1^3.$$

Equation $(*)$ is therefore proved for $n = 4$. One can easily formulate ibn al-Haytham's argument in modern terminology to give a proof for any k by induction on n.

Ibn al-Haytham now uses his result to derive formulas for the sums of integral powers. First, he proves the sum formulas for squares and cubes:

$$\sum_{i=1}^{n} i^2 = \left(\frac{n}{3}+\frac{1}{3}\right)n\left(n+\frac{1}{2}\right) = \frac{n^3}{3}+\frac{n^2}{2}+\frac{n}{6}$$

$$\sum_{i=1}^{n} i^3 = \left(\frac{n}{4}+\frac{1}{4}\right)n(n+1)n = \frac{n^4}{4}+\frac{n^3}{2}+\frac{n^2}{4}.$$

We will not deal with these proofs here, but only with the derivation of the analogous result for the fourth powers. Although ibn al-Haytham himself derives this result only for $n=4$, he asserts it for arbitrary n. We will therefore use modern techniques modeled on ibn al-Haytham's method to derive it for that case. We begin by using the formulas for the sums of squares and cubes to rewrite equation $(*)$ in the form

$$\begin{aligned}(n+1)\sum_{i=1}^{n} i^3 &= \sum_{i=1}^{n} i^4 + \sum_{p=1}^{n}\left(\frac{p^4}{4}+\frac{p^3}{2}+\frac{p^2}{4}\right)\\ &= \sum_{i=1}^{n} i^4 + \frac{1}{4}\sum_{i=1}^{n} i^4 + \frac{1}{2}\sum_{i=1}^{n} i^3 + \frac{1}{4}\sum_{i=1}^{n} i^2.\end{aligned}$$

It then follows that

$$\begin{aligned}(n+1)\sum_{i=1}^{n} i^3 &= \frac{5}{4}\sum_{i=1}^{n} i^4 + \frac{1}{2}\sum_{i=1}^{n} i^3 + \frac{1}{4}\sum_{i=1}^{n} i^2\\ \frac{5}{4}\sum_{i=1}^{n} i^4 &= \left(n+1-\frac{1}{2}\right)\sum_{i=1}^{n} i^3 - \frac{1}{4}\sum_{i=1}^{n} i^2\\ \sum_{i=1}^{n} i^4 &= \frac{4}{5}\left(n+\frac{1}{2}\right)\sum_{i=1}^{n} i^3 - \frac{1}{5}\sum_{i=1}^{n} i^2\\ &= \frac{4}{5}\left(n+\frac{1}{2}\right)\left(\frac{n}{4}+\frac{1}{4}\right)n(n+1)n - \frac{1}{5}\left(\frac{n}{3}+\frac{1}{3}\right)n\left(n+\frac{1}{2}\right)\\ &= \left(\frac{n}{5}+\frac{1}{5}\right)\left(n+\frac{1}{2}\right)n(n+1)n - \left(\frac{n}{5}+\frac{1}{5}\right)\left(n+\frac{1}{2}\right)n\cdot\frac{1}{3}.\end{aligned}$$

Ibn al-Haytham stated his result verbally in a form we translate into modern notation as

$$\sum_{i=1}^{n} i^4 = \left(\frac{n}{5}+\frac{1}{5}\right)n\left(n+\frac{1}{2}\right)\left[(n+1)n-\frac{1}{3}\right].$$

The result can also be written as a polynomial:

$$\sum_{i=1}^{n} i^4 = \frac{n^5}{5}+\frac{n^4}{2}+\frac{n^3}{3}-\frac{n}{30}.$$

It is clear that this formula can be used as Fermat and Roberval used Roberval's inequality to show that

$$\lim_{n\to\infty}\frac{\sum_{i=1}^{n} i^4}{n^5} = \frac{1}{5}.$$

Ibn al-Haytham used his result on sums of integral powers to perform what we would call an integration. In particular, he applied his result to determine the volume of the solid formed by rotating the parabola $x = ky^2$ around the line $x = kb^2$, perpendicular to the axis of the parabola, and showed that this volume is 8/15 of the volume of the cylinder of radius kb^2 and height b. (See FIGURE 2.) His formal argument was a typical Greek-style exhaustion argument using a double *reductio ad absurdum*, but in essence his method involved slicing the cylinder and paraboloid into n disks, each of thickness $h = b/n$, and then adding up the disks. The ith disk in the paraboloid has radius $kb^2 - k(ih)^2$ and therefore has volume $\pi h(kh^2n^2 - ki^2h^2)^2 = \pi k^2h^5(n^2 - i^2)^2$. The total volume of the paraboloid is therefore approximated by

$$\pi k^2 h^5 \sum_{i=1}^{n-1} (n^2 - i^2)^2 = \pi k^2 h^5 \sum_{i=1}^{n-1} (n^4 - 2n^2i^2 + i^4).$$

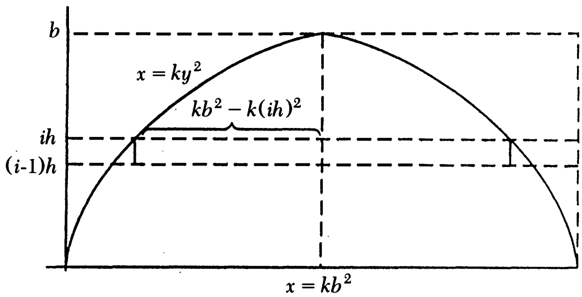


FIGURE 2

But since ibn al-Haytham knew the formulas for the sums of integral squares and fourth powers, he could calculate that

$$\sum_{i=1}^{n-1} (n^4 - 2n^2i^2 + i^4) = \frac{8}{15}(n-1)n^4 + \frac{1}{30}n = \frac{8}{15}n \cdot n^4 - \frac{1}{2}n^4 - \frac{1}{30}n$$

and therefore that

$$\frac{8}{15}(n-1)n^4 < \sum_{i=1}^{n-1} (n^2 - i^2)^2 < \frac{8}{15}n \cdot n^4.$$

But the volume of a typical slice of the circumscribing cylinder is $\pi h(k b)^2)^2 = \pi k^2h^5n^4$, and therefore the total volume of the cylinder is $\pi k^2h^5n \cdot n^4$, while the volume of the cylinder less its "top slice" is $\pi k^2h^5(n-1)n^4$. The inequality then shows that the volume of the paraboloid is bounded between 8/15 of the cylinder less its top slice and 8/15 of the entire cylinder. Because the top slice can be made as small as desired by taking n sufficiently large, it follows that the volume of the paraboloid is exactly 8/15 of the volume of the cylinder as asserted.

Ibn al-Haytham's formula for the sum of fourth powers shows up in other places in the Islamic world over the next few centuries. It appears in the work of Abu-l-Hasan ibn Haydur (d. 1413), who lived in what is now Morocco, and in the work of Abu Abdallah ibn Ghazi (1437–1514), who also lived in Morocco. (See [3] for details.) Furthermore, one also finds the formula in *The Calculator's Key* of Ghiyath al-Din Jamshid al-Kashi (d. 1429), a mathematician and astronomer whose most productive years were spent in Samarkand, now in Uzbekistan, in the court of Ulugh Beg. We do not know, however, how these mathematicians learned of the formula or for what purpose they used it.

Trigonometric Series in Sixteenth-Century India

The sum formulas for integral powers surface in sixteenth-century India and they are used to develop the power series for the sine, cosine, and arctangent. These power series appear in Sanskrit verse in the *Tantrasangraha-vyakhya* (of about 1530), a commentary on a work by Kerala Gargya Nilakantha (1445–1545) of some 30 years earlier. Unlike the situation for many results of Indian mathematics, however, a detailed derivation of these power series exists, in the *Yuktibhasa*, a work in Malayalam, the language of Kerala, the southwestern region of India. This latter work was written by Jyesthadeva (1500–1610), who credits these series to Madhava, an Indian mathematician of the fourteenth century.

Even though we do not know for sure whether Madhava was the first discoverer of the series, it is clear that the series were known in India long before the time of Newton. But why were the Indians interested in these matters? India had a long tradition of astronomical research, dating back to at least the middle of the first millennium B.C. The Indians had also absorbed Greek astronomical work and its associated mathematics during and after the conquest of northern India by Alexander the Great in 327 B.C. Hence the Indians became familiar with Greek trigonometry, based on the chord function, and then gradually improved it by introducing our sine, cosine, and tangent. Islamic mathematicians learned trigonometry from India, introduced their own improvements, and, after the conquest of northern India by a Moslem army in the twelfth century, brought the improved version back to India. (See [4] for more details.)

The interaction of astronomy with trigonometry brings an increasing demand for accuracy. Thus Indian astronomers wanted an accurate value for π (which comes from knowing the arctangent power series) and also accurate values for the sine and cosine (which comes from their power series) so they could use these values in determining planetary positions. Because a recent article [8] in this MAGAZINE discussed the arctangent power series, we will here consider only the sine and cosine series.

The statement of the Indian rule for determining these series is as follows: "Obtain the results of repeatedly multiplying the arc $[s]$ by itself and then dividing by $2, 3, 4, \ldots$ multiplied by the radius $[\rho]$. Write down, below the radius (in a column) the even results [i.e. results corresponding to $n = 2, 4, 6$ in $s^n/n!\rho^{n-1}$], and below the radius (in another column) the odd results [corresponding to $n = 3, 5, 7, \ldots$ in $s^n/n!\rho^{n-1}$]. After writing down a number of terms in each column, subtract the last term of either column from the one next above it, the remainder from the term next above, and so on, until the last subtraction is made from the radius in the first column and from the arc in the second. The two final remainders are respectively the cosine and the sine, to a certain degree of approximation." [6, p. 3] These words can easily be translated into the formulas:

$$x = \cos s = \rho - \frac{s^2}{2!\rho} + \frac{s^4}{4!\rho^3} - \cdots + (-1)^n \frac{s^{2n}}{(2n)!\rho^{2n-1}} + \cdots$$

$$y = \sin s = s - \frac{s^3}{3!\rho^2} + \frac{s^5}{5!\rho^4} - \cdots + (-1)^n \frac{s^{2n+1}}{(2n+1)!\rho^{2n}} + \cdots$$

(These formulas reduce to the standard power series when ρ is taken to be 1.)

The Indian derivations of these results begin with the obvious approximations to the cosine and sine for small arcs and then use a "pull yourself up by our own bootstraps" approach to improve the approximation step by step. The derivations also make use of the notion of differences, a notion used in other aspects of Indian mathematics as well. In our discussion of the Indian method, we will use modern notation to enable the reader to follow these sixteenth-century Indian ideas.

We first consider the circle of FIGURE 3 with a small arc $\alpha = \widehat{AC} \approx AC$. From the similarity of triangles AGC and OEB, we get

$$\frac{x_1 - x_2}{\alpha} = \frac{y}{\rho} \quad \text{and} \quad \frac{y_2 - y_1}{\alpha} = \frac{x}{\rho}$$
$$\text{or} \quad \frac{\alpha}{\rho} = \frac{x_1 - x_2}{y} = \frac{y_2 - y_1}{x}.$$

In modern terms, if $\angle BOF = \theta$ and $\angle BOC = \angle AOB = d\theta$, these equations amount to

$$\sin(\theta + d\theta) - \sin(\theta - d\theta) = \frac{y_2 - y_1}{\rho} = \frac{\alpha x}{\rho^2} = \frac{2\rho\, d\theta}{\rho} \cos\theta = 2\cos\theta\, d\theta$$

and

$$\cos(\theta + d\theta) - \cos(\theta - d\theta) = \frac{x_2 - x_1}{\rho} = -\frac{\alpha y}{\rho^2} = -\frac{2\rho\, d\theta}{\rho} \sin\theta = -2\sin\theta\, d\theta.$$

Now, suppose we have a small arc s divided into n equal subarcs, with $\alpha = s/n$. For simplicity we take $\rho = 1$, although the Indian mathematicians did not. By applying the previous results repeatedly, we get the following sets of differences for the y's (FIGURE 4) (where $y_n = y = \sin s$):

$$\Delta_n y = y_n - y_{n-1} = \alpha x_n$$
$$\Delta_{n-1} y = y_{n-1} - y_{n-2} = \alpha x_{n-1}$$
$$\cdots$$
$$\Delta_2 y = y_2 - y_1 = \alpha x_2$$
$$\Delta_1 y = y_1 - y_0 = y_1 = \alpha x_1.$$

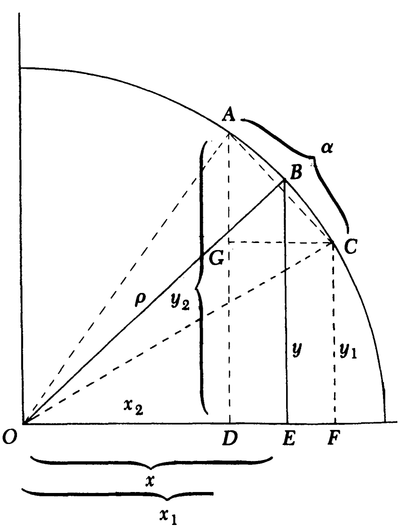


FIGURE 3

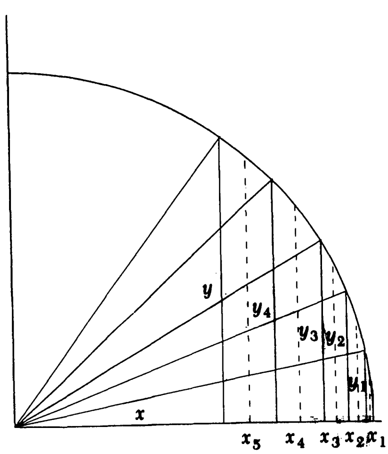


FIGURE 4

Similarly, the differences for the x's can be written

$$\begin{aligned}\Delta_{n-1}x &= x_n - x_{n-1} = -\alpha y_{n-1}\\ &\cdots\\ \Delta_2 x &= x_3 - x_2 = -\alpha y_2\\ \Delta_1 x &= x_2 - x_1 = -\alpha y_1.\end{aligned}$$

We next consider the second differences on the y's:

$$\Delta_2 y - \Delta_1 y = y_2 - y_1 - y_1 + y_0 = \alpha(x_2 - x_1) = -\alpha^2 y_1.$$

In other words, the second difference of the sines is proportional to the negative of the sine. But since $\Delta_1 y = y_1$, we can write this result as

$$\Delta_2 y = y_1 - \alpha^2 y_1.$$

Similarly, since

$$\Delta_3 y - \Delta_2 y = y_3 - y_2 - y_2 + y_1 = \alpha(x_3 - x_2) = -\alpha^2 y_2,$$

it follows that

$$\Delta_3 y = \Delta_2 y - \alpha^2 y_2 = y_1 - \alpha^2 y_1 - \alpha^2 y_2,$$

and, in general, that

$$\Delta_n y = y_1 - \alpha^2 y_1 - \alpha^2 y_2 - \cdots - \alpha^2 y_{n-1}.$$

But the sine equals the sum of its differences:

$$\begin{aligned}y = y_n &= \Delta_1 y + \Delta_2 y + \cdots + \Delta_n y\\ &= n y_1 - [y_1 + (y_1 + y_2) + (y_1 + y_2 + y_3) + \cdots + (y_1 + y_2 + \cdots + y_{n-1})]\alpha^2.\end{aligned}$$

Also, $s/n \approx y_1 \approx \alpha$, or $ny_1 \approx s$. Naturally, the larger the value of n, the better each of these approximations is. Therefore,

$$y \approx s - \lim_{n\to\infty}\left(\frac{s}{n}\right)^2 [y_1 + (y_1 + y_2) + \cdots + (y_1 + y_2 + \cdots + y_{n-1})].$$

Next we add the differences of the x's. We get

$$x_n - x_1 = -\alpha(y_1 + y_2 + \cdots + y_{n-1}).$$

But $x_n \approx x = \cos s$ and $x_1 \approx 1$. It then follows that

$$x \approx 1 - \lim_{n\to\infty}\left(\frac{s}{n}\right)(y_1 + y_2 + \cdots + y_{n-1}).$$

To continue the calculation, the Indian mathematicians needed to approximate each y_i and use these approximations to get approximations for $x = \cos s$ and $y = \sin s$. Each new approximation in turn is placed back in the expressions for x and y and leads to a better approximation. Note first that if y is small, y_i can be approximated by is/n. It follows that

$$\begin{aligned}x &\approx 1 - \lim_{n\to\infty}\left(\frac{s}{n}\right)\left[\frac{s}{n} + \frac{2s}{n} + \cdots + \frac{(n-1)s}{n}\right]\\ &= 1 - \lim_{n\to\infty}\left(\frac{s}{n}\right)^2 [1 + 2 + \cdots + (n-1)]\end{aligned}$$

$$= 1 - \lim_{n\to\infty} \frac{s^2}{n^2}\left[\frac{(n-1)n}{2}\right]$$

$$= 1 - \frac{s^2}{2}.$$

Similarly,

$$y \approx s - \lim_{n\to\infty}\left(\frac{s}{n}\right)^2\left[\frac{s}{n} + \left(\frac{s}{n} + \frac{2s}{n}\right) + \cdots + \left(\frac{s}{n} + \frac{2s}{n} + \cdots + \frac{(n-1)s}{n}\right)\right]$$

$$= s - \lim_{n\to\infty}\frac{s^3}{n^3}\left[1 + (1+2) + (1+2+3) + \cdots + (1+2+\cdots+(n-1))\right]$$

$$= s - \lim_{n\to\infty}\frac{s^3}{n^3}\left[n(1+2+\cdots+(n-1)) - \left(1^2+2^2+\cdots+(n-1)^2\right)\right]$$

$$= s - s^3\lim_{n\to\infty}\left[\frac{\sum_{i=1}^{n-1} i}{n^2} - \frac{\sum_{i=1}^{n-1} i^2}{n^3}\right]$$

$$= s - s^3\left(\frac{1}{2} - \frac{1}{3}\right)$$

$$= s - \frac{s^3}{6},$$

and there is a new approximation for y and therefore for each y_i. Note that in the transition from the second to the third lines of this calculation the Indians used ibn al-Haytham's equation $(*)$ for the case $k = 1$. Although the Indian mathematicians did not refer to ibn al-Haytham or any other predecessor, they did explicitly sketch a proof of this result in the general case and used it to show that, for any k, the sum of the kth powers of the first n integers is approximately equal to $n^{k+1}/(k+1)$. This result was used in the penultimate line of the above calculation in the cases $k = 1$ and $k = 2$ and in the derivation of the power series for the arctangent as discussed in [8].

To improve the approximation for sine and cosine, we now assume that $y_i \approx (is/n) - (is)^3/(6n^3)$ in the expression for $x = \cos s$ and use the sum formula in the case $k = 3$ to get

$$x \approx 1 - \lim_{n\to\infty}\frac{s}{n}\left[\frac{s}{n} - \frac{s^3}{6n^3} + \frac{2s}{n} - \frac{(2s)^3}{6n^3} + \cdots + \frac{(n-1)s}{n} - \frac{((n-1)s)^3}{6n^3}\right]$$

$$= 1 - \frac{s^2}{2} + \lim_{n\to\infty}\frac{s^4}{6n^4}\left[1^3 + 2^3 + \cdots + (n-1)^3\right]$$

$$= 1 - \frac{s^2}{2} + \frac{s^4}{6}\lim_{n\to\infty}\frac{\sum_{i=1}^{n-1} i^3}{n^4}$$

$$= 1 - \frac{s^2}{2} + \frac{s^4}{6}\cdot\frac{1}{4}$$

$$= 1 - \frac{s^2}{2} + \frac{s^4}{24}.$$

Similarly, ibn al-Haytham's formula for the case $j=3$ and the sum formula for the cases $j=3$ and $j=4$ lead to a new approximation for $y=\sin s$:

$$y \approx s - \frac{s^3}{6} + \lim_{n\to\infty}\left(\frac{s}{n}\right)^2\left[\frac{s^3}{6n^3} + \left(\frac{s^3}{6n^3} + \frac{(2s)^3}{6n^3}\right) + \cdots + \left(\frac{s^3}{6n^3} + \frac{(2s)^3}{6n^3} + \cdots + \frac{((n-1)s)^3}{6n^3}\right)\right]$$

$$= s - \frac{s^3}{6} + \lim_{n\to\infty}\frac{s^5}{6n^5}\left[1^3 + (1^3+2^3) + \cdots + \left(1^3+2^3+\cdots+(n-1)^3\right)\right]$$

$$= s - \frac{s^3}{6} + \lim_{n\to\infty}\frac{s^5}{6n^5}\left[n\left(1^3+2^3+\cdots+(n-1)^3\right) - \left(1^4+2^4+\cdots+(n-1)^4\right)\right]$$

$$= s - \frac{s^3}{6} + \frac{s^5}{6}\lim_{n\to\infty}\left[\frac{\sum_{i=1}^{n-1} i^3}{n^4} - \frac{\sum_{i=1}^{n-1} i^4}{n^5}\right]$$

$$= s - \frac{s^3}{6} + \frac{s^5}{6}\left(\frac{1}{4} - \frac{1}{5}\right)$$

$$= s - \frac{s^3}{6} + \frac{s^5}{120}.$$

Because Jyesthadeva considers each new term in these polynomials as a correction to the previous value, he understood that the more terms taken, the more closely the polynomials approach the true values for the sine and cosine. The polynomial approximations can thus be continued as far as necessary to achieve any desired approximation. The Indian authors had therefore discovered the sine and cosine power series!

Conclusion

How close did Islamic and Indian scholars come to inventing the calculus? Islamic scholars nearly developed a general formula for finding integrals of polynomials by A.D. 1000—and evidently could find such a formula for any polynomial in which they were interested. But, it appears, they were not interested in any polynomial of degree higher than four, at least in any of the material which has so far come down to us. Indian scholars, on the other hand, were by 1600 able to use ibn al-Haytham's sum formula for arbitrary integral powers in calculating power series for the functions in which they were interested. By the same time, they also knew how to calculate the differentials of these functions. So some of the basic ideas of calculus were known in Egypt and India many centuries before Newton. It does not appear, however, that either Islamic or Indian mathematicians saw the necessity of connecting some of the disparate ideas that we include under the name calculus. There were apparently only specific cases in which these ideas were needed.

There is no danger, therefore, that we will have to rewrite the history texts to remove the statement that Newton and Leibniz invented the calculus. They were certainly the ones who were able to combine many differing ideas under the two unifying themes of the derivative and the integral, show the connection between them, and turn the calculus into the great problem-solving tool we have today. But what we do not know is whether the immediate predecessors of Newton and Leibniz, including in particular Fermat and Roberval, learned of some of the ideas of the Islamic or Indian mathematicians through sources of which we are not now aware.

The entire question of the transmission of mathematical knowledge from one culture to another is a matter of current research and debate. In particular, with more medieval Arabic manuscripts being discovered and translated into European languages, the route of some mathematical ideas can be better traced from Iraq and Iran into Egypt, then to Morocco and on into Spain. (See [3] for more details.) Medieval Spain was one of the meeting points between the older Islamic and Jewish cultures and the emerging Latin-Christian culture of Europe. Many Arabic works were translated there into Latin in the twelfth century, sometimes by Jewish scholars who also wrote works in Hebrew. But although there is no record, for example, of ibn al-Haytham's work on sums of integral powers being translated at that time, certain ideas he used do appear in both Hebrew and Latin works of the thirteenth century. And since the central ideas of his work occur in the Indian material, there seems a good chance that transmission to India did occur. Answers to the questions of transmission will require much more work in manuscript collections in Spain and the Maghreb, work that is currently being done by scholars at the Centre National de Recherche Scientifique in Paris. Perhaps in a decade or two, we will have evidence that some of the central ideas of calculus did reach Europe from Africa or Asia.

Acknowledgement. I want to thank the referee for thoughtful comments and suggestions on the original version of this paper.

REFERENCES

1. J. L. Berggren, *Episodes in the Mathematics of Medieval Islam*, Springer-Verlag, New York, 1986.
2. Walter E. Clark, *The Aryabhatiya of Aryabhata* University of Chicago Press, Chicago, 1930.
3. Ahmed Djebbar, *Enseignement et Recherche Mathématiques dans le Maghreb des XIII^e – XIV^e Siecles* (Publications Mathématiques D'Orsay No. 81-02) Université de Paris-Sud, Orsay, France, 1981.
4. Victor Katz, *A History of Mathematics: An Introduction*, Harper Collins Publishers, New York, 1993.
5. Michael Mahoney, *The Mathematical Career of Pierre de Fermat 1601–65*, Princeton University Press, Princeton, NJ, 1973.
6. C. T. Rajagopal and A. Venkataraman, The sine and cosine power-series in Hindu mathematics, *J. of the Royal Asiatic Society of Bengal—Science* 15 (1949), 1–13.
7. Roshdi Rashed, Ibn al-Haytham et la measure du paraboloide, *J. for the History of Arabic Science* 5 (1981), 262–291.
8. Ranjan Roy, The discovery of the series formula for π by Leibniz, Gregory and Nilakantha, this MAGAZINE 63 (1990), 291–306.
9. Derek Whiteside, *The Mathematical Papers of Isaac Newton*, Cambridge University Press, Cambridge, 1967–1981.

Selling Primes

PAULO RIBENBOIM*
Queen's University
Kingston, Ontario, Canada, K7L 3N6

I am a big shot in a factory that produces primes.

And I will tell you an interesting dialogue with a buyer, coming from an exotic country.

The Dialogue

—Buyer: I wish to buy some primes.

—I (generously): I can give to you, free of charge, many primes: 2, 3, 5, 7, 11, 13, 17, 19,... .

—Buyer (interrupting my generous offer): Thank you, sir; but I want primes with 100 digits. Do you have these for sale?

—I: In this factory we can produce primes as large as you wish. There is in fact an old method of Euclid, which you may have heard about. If I have any number n of primes, say $p_1, p_2, \ldots, p_n$, we multiply them and add 1, to get the number $N = p_1 p_2 \cdots p_n + 1$. Either N is a prime or, if it is not a prime, we pick any prime dividing N. In this way, it is easy to see that we get a prime, which is different from the ones we mixed. Call it p_{n+1}. If we now mix $p_1, p_2, \ldots, p_n, p_{n+1}$ as I already said, we get still another prime p_{n+2}. Repeating this procedure we get as many primes as we wish and so, we are bound to get primes as large as we wish, for sure with at least 100 digits.

—Buyer: You are very nice to explain your procedure. Even in my distant country, I have heard about it. It gives primes that may be arbitrarily large. However, I want to buy primes that have exactly 100 digits, no more, no less. Do you have them?

—I: Yes. Long ago—at the beginning of last century—Bertrand observed that between any number $N > 1$ and its double $2N$, there exists at least one prime number. This experimental observation was confirmed by a rigorous proof by Chebyshev. So I can find the primes p_1, p_2, p_3 where

$$10^{99} < p_1 < 2 \times 10^{99}$$

$$2 \times 10^{99} < p_2 < 4 \times 10^{99}$$

$$4 \times 10^{99} < p_3 < 8 \times 10^{99}.$$

—Buyer: This means that you have guaranteed 3 primes with 100 digits, and perhaps a few more. But I want to buy many primes with 100 digits. How many can you produce?

—I: I have never counted how many primes of 100 digits could eventually be produced. I have been told that my colleagues in other factories have counted the total number of primes up to 10^{17}. We usually write $\pi(N)$ to denote the number of primes up to the number N. Thus, the count I mentioned has given:

$$\pi(10^8) = 5{,}761{,}455$$

$$\pi(10^9) = 50{,}847{,}534$$

*Lecture at the University of Augsburg, June 23, 1992.

$$\pi(10^{12}) = 37{,}607{,}912{,}018$$
$$\pi(10^{17}) = 2{,}625{,}557{,}157{,}654{,}233.$$

Even though all primes up to 10^{17} have not yet been produced by any factory, the count of $\pi(10^{17})$ is exact.

—Buyer (a bit astonished). If you cannot—as I understand—know how many primes of each large size there are in stock, how can you operate your factory and guarantee delivery of the merchandise?

—I: Your country sells oil, does it not? You can estimate the amount of oil at shallow depths quite accurately, but you cannot measure exactly the entire amount underground. It is just the same with us.

Gauss, one of the foremost scientists, discovered that

$$\pi(N) \sim \frac{N}{\log N}$$

for large values of N. This was confirmed, almost a century ago, by a proof given by Hadamard and de la Vallée Poussin.

—Buyer: Do you mean that $\pi(N)$ is approximately equal to $N/\log N$, with a small error?

—I: Yes. To be more precise, the relative error, namely the absolute value of the difference $|\pi(N) - N/\log N|$, divided by $\pi(N)$, tends to 0, as N increases indefinitely.

—Buyer: Then, because of the error, you cannot be very specific in your estimate. Unless you estimate the error.

—I: Correct (the buyer is not stupid...). Chebyshev showed, even before the prime number theorem was proved, that if N is large, then

$$0.9\frac{N}{\log N} < \pi(N) < 1.1\frac{N}{\log N}.$$

To count primes with 100 digits:

$$0.9\frac{10^{99}}{99\log 10} < \pi(10^{99}) < 1.1\frac{10^{99}}{99\log 10}$$
$$0.9\frac{10^{100}}{100\log 10} < \pi(10^{100}) < 1.1\frac{10^{100}}{100\log 10}.$$

It is easy to estimate the difference $\pi(10^{100}) - \pi(10^{99})$, which gives the number of primes with exactly 100 digits:

$$3.42 \times 10^{97} < \pi(10^{100}) - \pi(10^{99}) < 4.38 \times 10^{97}.$$

—Buyer: You are rich! I think you have more primes than we have oil. But I wonder how your factory produces the primes with 100 digits. I have an idea but I'm not sure how efficient my method would be.

1°) Write all the numbers with 100 digits.
2°) Cross out, in succession, all the multiples of 2, of 3, of 5, ..., of each prime p less than 10^{99}. For this purpose, spot the first multiple of p, then cross out every pth number.

What remains are the primes between 10^{99} and 10^{100}, that is, the primes with exactly 100 digits.

—I: This procedure is correct and was already discovered by Eratosthenes (in the 3rd century B.C.). In fact, you may stop when you have crossed out the multiples of all the primes less than 10^{50}.

However, this method of production is too slow. This explains why the archeologists never found a factory of primes amongst the Greek ruins, but just temples to Apollo, statues of Aphrodite (known as Venus, since the time of Romans), and other ugly remains, which bear witness to a high degree of decadence.

Even with computers this process is too slow to be practical. Think of a computer that writes 10^6 digits per second.

- There are $10^{100} - 10^{99} = 10^{99} \times 9$ numbers with 100 digits.
- These numbers have a total of $10^{101} \times 9$ digits.
- One needs $10^{95} \times 9$ seconds to write these numbers, that is about 1.5×10^{94} minutes, that is about 25×10^{92} hours, so more than 10^{91} days, that is of the order of 3×10^{88} years, that is 3×10^{86} centuries!

And after writing the numbers (if there is still an After...) there is much more to be done!

Before the buyer complained, I added:

—I: There are shortcuts, but even then the method would still be too slow. So, instead of trying to list the primes with 100 digits, our factory uses fast algorithms to produce enough primes to cover our orders.

—Buyer: I am amazed. I never thought how important it is to have a fast method. Can you tell me the procedure used in your factory? I am really curious. [Yes, this buyer was being too nosy. Now I became convinced that he was a spy.]

—I: When you buy a Mercedes, you don't ask how it was built. You choose your favorite color, pink, purple, or green with orange dots, you drive it and you are happy, because everyone else is envious of you.

Our factory will deliver the primes you ordered and we do better than Mercedes. We support our product with a lifetime guarantee. Goodbye, sir.

[He may have understood: Good buy, sir...]

After the Dialogue

I hope that after the dialogue with the spy-buyer, you became curious to know about our fast procedure to produce large primes. I shall tell you some of our most cherished secrets. In our factory there are two main divisions.

1) Production of primes.

2) Quality control.

Production of Primes

One of the bases of our production methods was discovered long ago by Pocklington [4]. I will state and prove his theorem, in the particular situation adapted to our production requirements. Then, I shall discuss how it may be used to obtain, in a surprisingly short time, primes with the required number of digits.

CRITERION OF POCKLINGTON. *Let p be an odd prime, let k be a natural number such that p does not divide k and $1 \leq k < 2(p+1)$; and let $N = 2kp + 1$. Then the following conditions are equivalent:*

1) *N is a prime.*
2) *There exists a natural number* a, $2 \le a < N$, *such that*

$$a^{kp} \equiv -1 (\bmod N)$$

and

$$\gcd(a^k + 1, N) = 1.$$

Proof. $1 \Rightarrow 2$. Assume that N is a prime. As it is known, there is some integer a, $1 < a < N$, such that $a^{N-1} \equiv 1(\bmod N)$, but $a^m \not\equiv 1(\bmod N)$ if $1 < m < N-1$; such a number a is called a *primitive root modulo N*. Thus $a^{2kp} \equiv 1(\bmod N)$, but $a^{kp} \not\equiv 1(\bmod N)$; then $a^{kp} \equiv -1(\bmod N)$. Also $a^k \not\equiv -1(\bmod N)$ otherwise $a^{2k} \equiv 1(\bmod N)$, which is not true; so $\gcd(a^k + 1, N) = 1$.

$2 \Rightarrow 1$. In order to show that N is a prime, we shall prove: If q is any prime dividing N, then $\sqrt{N} < q$. It follows that N cannot have two (equal or distinct) prime factors, so N is a prime.

So, let q be any prime factor of N. Then $a^{kp} \equiv -1(\bmod q)$ and $a^{2k} \equiv 1(\bmod q)$. Hence $\gcd(a, q) = 1$. Let e be the order of a modulo q, hence e divides $q-1$, by Fermat's little theorem. Similarly, e divides $2kp = N-1$, because $a^{2kp} \equiv 1(\bmod q)$. Note that $a^k \not\equiv 1(\bmod q)$, otherwise $a^{kp} \equiv 1(\bmod q)$; from $a^{kp} \equiv -1(\bmod q)$, it follows that $q = 2$ and N would be even, which is false.

From $\gcd(a^k + 1, N) = 1$, it follows that $a^k \not\equiv -1(\bmod q)$. Hence $a^{2k} \not\equiv 1(\bmod q)$, thus $e \nmid 2k = (N-1)/p$. But $e \mid N-1$, so $(N-1)/e$ is an integer, hence $p \nmid (N-1)/e$. Since $N - 1 = e\ (N - 1/e)$ and $p \mid N-1$, then $p \mid e$, thus $p \mid q-1$. Also $2 \mid q-1$, hence $2p \mid q-1$, so $2p \le q-1$ and $2p+1 \le q$. It follows that $N = 2kp + 1 < 2 \times 2(p+1)p + 1 = 4p^2 + 4p + 1 = (2p+1)^2 \le q^2$, therefore $\sqrt{N} < q$. This concludes the proof.

The criterion of Pocklington is applied as follows to obtain primes of a required size, say with 100 digits.

First step: Choose, for example, a prime p_1 with $d_1 = 5$ digits. Find $k_1 < 2(p_1 + 1)$ such that $p_2 = 2k_1p_1 + 1$ has $d_2 = 2d_1 = 10$ digits or $d_2 = 2d_1 - 1 = 9$ digits and there exists $a_1 < p_2$ satisfying the conditions $a_1^{k_1p_1} \equiv -1(\bmod p_2)$ and $\gcd(a_1^{k_1} + 1, p_2) = 1$. By Pocklington's criterion, p_2 is a prime.

Subsequent steps: Repeat the same procedure starting with the prime p_2 to obtain the prime p_3, etc... In order to produce a prime with 100 digits, the process must be iterated five times. In the last step, k_5 should be chosen so that $2k_5p_5 + 1$ has 100 digits.

Feasibility of the Algorithm

Given p and k, with $1 \le k < 2(p+1)$, k not a multiple of p, if $N = 2kp + 1$ is a prime, then it has a primitive root. It would be much too technical to explain in detail the following results, some known to experts, others still unpublished. It follows from a generalized form of the Riemann hypothesis, that if x is a large positive real number and the positive integer a is not a square, then the ratio

$$\frac{\#\{\text{primes } q \le x \text{ such that } a \text{ is a primitive root modulo } q\}}{\#\{\text{primes } q \le x\}}$$

converges; if a is a prime, the limit is at least equal to Artin's constant

$$\prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) \approx 0.37.$$

Better, given positive integers, a, b, which are not squares and a large prime q, the probability that a or b is a primitive root modulo q, is much larger. Taking $a = 2$, $b = 3$, it is at least 58%. The corresponding probability increases substantially when taking three positive integers a, b, c that are not squares.

This suggests that we proceed as follows. Given the prime p, choose k, not a multiple of p, $1 \leq k < 2(p+1)$. If $N = 2kp + 1$ is a prime, then very likely 2, 3, or 5 is a primitive root modulo N. If this is not the case, it is more practical to choose another integer k', like k, and investigate whether $N' = 2k'p + 1$ is a prime.

The question arises: What are the chances of finding k such that N is a prime? I now discuss this point.

1°) According to a special case of Dirichlet's famous theorem (see **[5]**, **[6]**), given p, there exist infinitely many integers $k \geq 1$ such that $2kp + 1$ is a prime. This may be proved in elementary way.

2°) How small may k be, so that $2kp + 1$ is a prime? A special case of a deep theorem of Linnik asserts:
For every sufficiently large p, in the arithmetic progression with first term 1 and difference $2p$, there exists a prime $p_1 = 2kp + 1$ satisfying $p_1 \leq (2p)^L$; here L is a positive constant, (that is, L is independent of p) (see **[5]**).

3°) Recently, Heath-Brown has shown that $L \leq 5.5$.

4°) In Pocklington's criterion, it is required to find $k < 2(p+1)$ such that $p_1 = 2kp + 1$ is a prime. This implies that $p_1 < (2p+1)^2$. No known theorem guarantees that such small values of k lead to a prime.

5°) Recent work of Bombieri, Friedlander and Iwaniec deals with primes p for which there are small primes $p_1 = 2kp + 1$. Their results, which concern averages, point to the existence of a sizable proportion of primes p with small prime $p_1 = 2kp + 1$.

The problems considered above are of great difficulty. In practice, we may ignore these considerations and find, with a few trials, the appropriate value of k.

Estimated Time to Produce Primes with 100 Digits

The time required to perform an algorithm depends on the speed of the computer and on the number of bit operations (i.e., operations with digits) that are necessary.

As a basis for this discussion, we may assume that the computer performs 10^6 bit operations per second. If we estimate an upper bound for the number of bit operations, dividing by 10^6 gives an upper bound for the number of seconds required.

A closer look at the procedure shows that it consists of a succession of the following operations on natural numbers: multiplication ab modulo n, power a^b modulo n, calculation of greatest common divisor.

It is well known (see **[1]**, **[2]**) and not difficult to show that for each of the above operations there exist $C > 0$ and an integer $e \geq 1$ such that the number of bit operations required to perform the calculation is at most Cd^e, where d is the maximum of the number of digits of the numbers involved. Combining these estimates gives an upper bound of the same form Cd^e *for the method* ($C > 0$, $e \geq 1$

and d is the maximum of the number of digits of all integers involved in the calculation).

It is not my purpose to give explicit values for C and e when p, k, a are given. Let me just say that C, e are rather small, so the algorithm runs very fast. I stress that in this estimate the time required in the search for k, a is not taken into account.

The above discussion makes clear that much more remains to be understood in the production of primes and the feasibility of the algorithm. This task is delegated to our company's division of research and development, and I admire our colleagues in the research subdivision who face the deep mysteries of prime numbers.

Before I rapidly tour our division of quality control, I would like to make a few brief comments about our preceding considerations. They concern the complexity of an algorithm.

An algorithm A, performed on natural numbers, is said to run in *polynomial time* if there exist positive integers C, e (depending on the algorithm) such that the number of bit operations (or equivalently, the time) required to perform the algorithm on natural numbers with at most d digits is at most Cd^e.

An algorithm that does not run in polynomial time is definitely too costly to implement and is rejected by our factory. It is one of the main subjects of research to design algorithms that run in polynomial time. The algorithm to produce primes of a given size, for all practical purposes, runs in polynomial time, even though this has not yet been supported by a proof.

Quality Control

The division of quality control in our factory watches that the primes we sell are indeed primes. When Pocklington's method is used we only need to worry if no silly calculation error was made, because it leads automatically to prime numbers. If other methods are used, as I shall soon invoke, there must be a control. The division of quality control also engages in consulting work. A large number N is presented, with the question: Is N a prime number?

Thus, our division of quality control also deals with tests of primality. Since this is a cash rewarding activity, there are now many available tests of primality. I may briefly classify them from the following three points of view:

1. Tests for generic numbers.
   Tests for numbers of special forms, like $F_n = 2^{2^n} + 1$ (Fermat numbers), $M_p = 2^p - 1$, (p prime, Mersenne numbers), etc....
2. Tests fully justified by theorems.
   Tests based on justification that depends on forms of Riemann's hypothesis of the zeros of the zeta function, or on heuristic arguments.
3. Deterministic tests.
4. Probabilistic or Monte Carlo tests.

A deterministic test applied to a number N will certify that N is a prime or that N is a composite numbers. A Monte Carlo test applied to N will certify either that N is composite, or that, with a large probability, N is a prime.

Before I proceed, let me state that the main problem tempting the researchers is the following: Will it be possible to find a fully justified and deterministic test of primality for generic numbers, which runs in polynomial time? Or will it be proven that there cannot exist a deterministic, fully justified test of primality that runs in polynomial time, when applied to any natural number?

This is a tantalizing and deep problem.

It would be long-winded and complex even to try to describe all the methods and algorithms used in primality testing. So, I shall concentrate only on the strong pseudoprime test, which is of Monte Carlo type.

Pseudoprimes Let N be a prime, let a be such that $1 < a < N$. By Fermat's little theorem, $a^{N-1} \equiv 1 (\bmod N)$.

However, the converse is not true. The smallest example is $N = 341 = 11 \times 31$, with $a = 2$, $2^{340} \equiv 1 (\bmod 341)$.

The number N is called a *pseudoprime in base* a, where $\gcd(a, N) = 1$, if N is composite and $a^{N-1} \equiv 1 (\bmod N)$. For each $a \geq 2$, there are infinitely many pseudoprimes in base a. Now observe that every odd prime N satisfies the following property:

> For any a, $2 \leq a < N$, with $gcd(a, N) = 1$, writing $N - 1$ in the form $N - 1 = 2^s d$ (where $1 \leq s$, d is odd), either $a^d \equiv 1 (\bmod N)$ or there exists r, $0 \leq r < s$, such that $a^{2^r d} \equiv -1 (\bmod N)$. (*)

Again, the converse is not true, as illustrated by $N = 2047 = 23 \times 89$, with $a = 2$.

The number N is called a *strong pseudoprime in base* a, where $\gcd(a, N) = 1$, if N is composite and the condition (*) is satisfied.

It has been shown by Pomerance, Selfridge, and Wagstaff that for every $a \geq 2$ there exist infinitely many strong pseudoprimes in base a.

The strong pseudoprime test The main steps in the strong pseudoprime test for a number N are the following:

1°) Choose $k > 1$ numbers a, $2 \leq a < N$, such that $\gcd(a, N) = 1$. This is easily done by trial division and does not require knowledge of the prime factors of N. If $\gcd(a, N) > 1$ for some a, $1 < a < N$, then N is composite.

2°) For each chosen base a, check if the condition (*) is satisfied.

If there is a such that (*) is not satisfied, then N is composite. Thus, if N is a prime, then (*) is satisfied for each base a. The events that condition (*) is satisfied for different bases may be legitimately considered as independent if the bases are randomly chosen.

Now, Rabin proved (see [5]): Let N be composite. Then the number of bases a for which N is a strong pseudoprime in base a is less than $\frac{1}{4}(N-1)$. Thus, if N is composite, the probability that (*) is satisfied for k bases is at most $1/4^k$. Hence, certification that N is a prime when (*) is satisfied for k distinct bases is incorrect in only one out of 4^k numbers; for example, if $k = 30$, the certification is incorrect only once in every 10^{18} numbers.

The strong pseudoprime test runs in polynomial time and it is applicable to any number.

If a generalized form of Riemann's hypothesis is assumed to be true, Miller showed (see [5]): If N is composite, there exists a base a, with $\gcd(a, N) = 1$, such that $a < (\log N)^{2+\varepsilon}$, for which (*) is not satisfied.

A new production method We may use Rabin's test to produce numbers with 100 digits that may be certified to be prime numbers, with only very small probability of error.

1°) Pick a number N with 100 digits. Before doing any hard work, it is very easy, with trial division, to find out if this number does, or does not have, any prime factor less than, say, 1000. In the latter case, keep this number; in the first case, discard N, pick another number N', and proceed similarly.

2°) Use $k = 30$ small numbers a, prime to N, as bases to verify if condition (*) is satisfied. Discard N if, for some base a, the condition (*) is not satisfied and repeat the process with some other number N'. If (*) is satisfied for all a then, according to Rabin's calculation, we may certify that N is prime; in doing so, we are incorrect only in at most one out of 10^{18} numbers. How unlucky can we be and choose, in succession, numbers which are composite? According to the inequalities of Chebyshev already indicated, the proportion of numbers with 100 digits that are prime is not less than $\frac{3.42}{9 \times 10^2} \approx \frac{1}{260}$ and not more than $\frac{4.38}{9 \times 10^9} \approx \frac{1}{205}$. Unintelligent employees who would pick even numbers, or numbers divisible by $3, 5, \ldots,$ or small primes (say up to 1000) are sure to be fired. Thus the luck of picking a prime increases and it becomes quite reasonable to use Rabin's method of production.

We may sell the number N as if it were a prime, even with a "money back guarantee" because the probability that we are selling a composite number is only 1 in every 1,000,000,000,000,000,000 sales! This is a better guarantee than anyone can get in any deal. We are sure that our company will not be bankrupt and will continue to support generously my trips to advertise our products—all complemented by lavish dinners and the finest wines, to help convince our customers that primes are the way of life.

Appendix

Here is an example of a prime with 100 digits that was calculated by L. Roberts, using the method of Pocklington.

$p_1 = 2333$ $\quad k_1 = 2001$ $\quad a_1 = 2$

$p_2 = 9336667$ $\quad k_2 = 9336705$ $\quad a_2 = 3$

$p_3 = 174347410924471$ $\quad k_3 = 174347410924479$ $\quad a_3 = 2$

$p_4 = 607940393921354891483080 51219$

$k_4 = 60794039392135489148308051256$ $\quad a_4 = 3$

$p_5 = 7391830451225043189805749502951935872607026673729850562129$

$k_5 = 5000000000000000000000000000000000000000137$ $\quad a_5 = 2$

$p_6 = 739183045122504318980574950295193587260905203527348622396300677536$
$3808830429094325308601979054023347$

Acknowledgement to Bart Braden for friendly style suggestions.

REFERENCES

1. Le Veque, W. J. (editor) *Studies in Number Theory*, MAA, Washington, 1975.
2. Mignotte, M. *Mathematics for Computer Algebra*, Springer-Verlag New York, 1991.
3. Plaisted, D. A. Fast verification, testing and generation of large primes, *Theor. Comp. Sci.* 9 (1979), 1–16.
4. Pocklington, H. C. The determination of the prime or composite nature of large numbers by Fermat's theorem, *Proc. Cambridge Phil. Soc.* 18 (1914/ 16), 29–30.
5. Ribenboim, P. *The Book of Prime Number Records*, 2nd edition, Springer-Verlag New York, 1989.
6. Ribenboim, P. *The Little Book of Big Primes*, Springer-Verlag New York, 1991.

Derivatives of Noninteger Order

KENNETH S. MILLER
25 Bonwit Road
Rye Brook, NY 10573

1. Introduction

The purpose of this paper is to introduce the reader to the subject of the fractional calculus and fractional differential equations. We define integrals and derivatives of noninteger order and study some of their elementary properties. In the final section we examine fractional differential equations.

We shall indicate differentiation by the operator D. Thus

$$D^n f(t), \qquad n = 1, 2, \dots$$

represents the nth derivative of $f(t)$. The particular n-fold integral

$$\int_0^t dt_1 \int_0^{t_1} dt_2 \int_0^{t_2} dt_3 \cdots \int_0^{t_{n-1}} f(\xi)\, d\xi \tag{1.1}$$

of $f(t)$ will be denoted by $D^{-n} f(t)$.

We shall give meaning to the symbol $D^\nu f(t)$ where ν is not necessarily an integer. Our results are true for any ν that is not purely imaginary (and even this case may be treated, [1]). For simplicity, and with little loss of generality, we shall assume v to be real. The study of operators of the form D^ν constitutes the content of the subject called *fractional calculus* (even though ν need not be rational).

The higher transcendental function $E_t(\nu, a)$ introduced in Section 2 plays a prominent role in the theory of fractional linear differential equations. We devote Section 3 to an analysis of some of its elementary properties.

While the formula

$$D^n[D^m f(t)] = D^{n+m} f(t) = D^m[D^n f(t)]$$

is certainly true for suitable functions f in the case n and m are positive integers; it may *not* be true if n and m are *not* positive integers. Certain aspects of this problem are examined in Section 4.

2. Fractional Integrals and Derivatives

It is convenient to define first the fractional integral $D^{-\nu} f(t)$, $\nu > 0$, and *then* define the fractional derivative $D^\mu f(t)$, $\mu > 0$, in terms of the fractional integral, Let I be the closed interval $[0, X]$ where $X > 0$, and let f be continuous on I. Then

$$D^{-1} f(t) = \int_0^t f(\xi)\, d\xi \tag{2.1}$$

exists for all t in I; see (1.1).

In our attempt to make a suitable definition of $D^{-\nu} f(t)$ for $\nu > 0$, we first establish the formula

$$D^{-n} f(t) = \frac{1}{(n-1)!} \int_0^t (t-\xi)^{n-1} f(\xi)\, d\xi \tag{2.2}$$

for $n = 1, 2, \dots$. The proof is by induction on n. Certainly (2.2) is true if $n = 1$. Let us assume that it is true for $n = N$. Then

$$D^{-(N+1)}f(t) = D^{-1}\left[\frac{1}{(N-1)!}\int_0^t (t-\xi)^{N-1} f(\xi)\, d\xi\right]$$
$$= \int_0^t \left[\frac{1}{(N-1)!}\int_0^x (x-\xi)^{N-1} f(\xi)\, d\xi\right] dx.$$

Interchanging the order of integration leads to

$$D^{-(N+1)}f(t) = \frac{1}{N!}\int_0^t (t-\xi)^N f(\xi)\, d\xi, \tag{2.3}$$

and our proof is complete.

We are prepared now to define the fractional integral. Equation (2.2) may be written as

$$D^{-n}f(t) = \frac{1}{\Gamma(n)}\int_0^t (t-\xi)^{n-1} f(\xi)\, d\xi, \tag{2.4}$$

where we have replaced $(n-1)!$ by the equivalent representation in terms of the Gamma function. Now the right-hand side of (2.4) is valid, not just for n a positive integer, but for *any* positive number n. Thus if $\nu > 0$ and if f is continuous on $I' = (0, X]$ and integrable on every finite subinterval of $I = [0, X]$, we call

$$D^{-\nu}f(t) = \frac{1}{\Gamma(\nu)}\int_0^t (t-\xi)^{\nu-1} f(\xi)\, d\xi, \qquad t \in I' \tag{2.5}$$

the *fractional integral* of f of order ν.

Of course we could have defined the fractional integral of f of order ν as just the right-hand side of (2.5). However, the analysis leading to (2.4) provides some motivation for making this definition.

Let us consider an example. Suppose

$$f(t) = t^{\lambda}, \qquad \lambda > -1. \tag{2.6}$$

Then (2.5) is essentially a Beta function, and a trivial integration yields

$$D^{-\nu}t^{\lambda} = \frac{\Gamma(\lambda+1)}{\Gamma(\lambda+1+\nu)} t^{\lambda+\nu}, \qquad t \in I', \quad \lambda > -1, \quad \nu > 0. \tag{2.7}$$

Unfortunately, except for polynomials, the fractional integral of practically every other simple function we can think of leads to a nonelementary function. For example, let us attempt to find the fractional integral of e^{at} where a is a constant. From (2.5)

$$D^{-\nu}e^{at} = \frac{1}{\Gamma(\nu)}\int_0^t (t-\xi)^{\nu-1} e^{a\xi}\, d\xi, \qquad \nu > 0,$$

and if we make the trivial change of variable $x = t - \xi$,

$$D^{-\nu}e^{at} = \frac{1}{\Gamma(\nu)} e^{at}\int_0^t x^{\nu-1} e^{-ax}\, dx. \tag{2.8}$$

We shall call the right-hand side of (2.8) $E_t(\nu, a)$ so that

$$D^{-\nu}e^{at} = E_t(\nu, a). \tag{2.9}$$

The function $E_t(\nu, a)$ is especially useful in our study of fractional differential equations. In the next section we shall examine some properties of this important function.

Let us turn now to the problem of defining the fractional derivative. We can *not* use (2.5). That is, we may not write

$$D^{\mu}f(t) = \frac{1}{\Gamma(-\mu)}\int_0^t (t-\xi)^{-\mu-1} f(\xi)\, d\xi, \qquad \mu > 0$$

since the integral does not converge (unless f has compact support contained in $[0, t)$). Therefore we resort to the following artifice. Let $\mu > 0$ and let m be the smallest integer exceeding μ. Then we define the *fractional derivative* of f of order μ (if it exists) as

$$D^{\mu}f(t) = D^{m}\left[D^{-(m-\mu)}f(t)\right]. \tag{2.10}$$

For example, if f is given by (2.6), then from (2.7)

$$D^{-(m-\mu)}t^{\lambda} = \frac{\Gamma(\lambda+1)}{\Gamma(\lambda+1+m-\mu)} t^{\lambda+m-\mu}$$

and thus

$$\begin{aligned} D^{\mu}t^{\lambda} &= \frac{\Gamma(\lambda+1)}{\Gamma(\lambda+1+m-\mu)} D^{m} t^{\lambda+m-\mu} \\ &= \frac{\Gamma(\lambda+1)}{\Gamma(\lambda+1-\mu)} t^{\lambda-\mu}, \qquad t \in I'; \quad \lambda > -1, \quad \mu > 0. \end{aligned}$$

We may use (2.10) to verify that the fractional derivative of order μ is the ordinary derivative of order μ when μ is a positive integer. For suppose $\mu = p$ (a positive integer). Then $m = p + 1$, and if f has a pth derivative, (2.10) implies

$$D^{p}f(t) = D^{p+1}\left[D^{-1}f(t)\right];$$

see (2.1).

3. Some Special Functions

We already have used the Gamma function in the previous section. The reader recalls that if $\nu > 0$, it has the integral representation

$$\Gamma(\nu) = \int_0^{\infty} x^{\nu-1}e^{-x}\, dx. \tag{3.1}$$

Now from (2.8) and (2.9) we may write $E_t(\nu, a)$ as

$$E_t(\nu, a) = t^{\nu}e^{at}\gamma^*(\nu, at) \tag{3.2}$$

where

$$\gamma^*(\nu, at) = \frac{1}{\Gamma(\nu)(at)^{\nu}}\int_0^{at} \xi^{\nu-1}e^{-\xi}\, d\xi, \qquad \nu > 0$$

is the incomplete Gamma function [**2**, page 337]. A comparison with (3.1) demonstrates the aptness of the name.

Let us look more closely at $\gamma^*(\nu,t)$. It may be represented by the infinite series

$$\gamma^*(\nu,t)=e^{-t}\sum_{k=0}^{\infty}\frac{t^k}{\Gamma(\nu+k+1)} \tag{3.3}$$

and is an entire function of both ν and t. This form of $\gamma^*(\nu,t)$ is useful in deducing certain formulae involving $E_t(\nu,a)$. In particular some simple properties of the $E_t(\nu,a)$ function we shall need are the recursion relation

$$E_t(\nu,a)=aE_t(\nu+1,a)+\frac{t^\nu}{\Gamma(\nu+1)}, \tag{3.4}$$

the differentiation formula

$$D^pE_t(\nu,a)=E_t(\nu-p,a),\qquad p=0,1,\ldots, \tag{3.5}$$

and the special value

$$E_t(0,a)=e^{at}. \tag{3.6}$$

To prove (3.4) we see from (3.3) that

$$\begin{aligned}\gamma^*(\nu+1,t)&=e^{-t}\sum_{k=0}^{\infty}\frac{t^k}{\Gamma(\nu+k+2)}=e^{-t}\sum_{j=1}^{\infty}\frac{t^{j-1}}{\Gamma(\nu+j+1)}\\&=e^{-t}t^{-1}\left[\sum_{j=0}^{\infty}\frac{t^j}{\Gamma(\nu+j+1)}-\frac{1}{\Gamma(\nu+1)}\right]\\&=t^{-1}\left[\gamma^*(\nu,t)-\frac{e^{-t}}{\Gamma(\nu+1)}\right],\end{aligned}$$

and using (3.2) we get (3.4).

To prove (3.5) we see that

$$\begin{aligned}\frac{\partial^p}{\partial t^p}E_t(\nu,a)&=\frac{\partial^p}{\partial t^p}\sum_{k=0}^{\infty}\frac{a^kt^{k+\nu}}{\Gamma(\nu+k+1)}=\sum_{k=0}^{\infty}\frac{a^kt^{k+\nu-p}}{\Gamma(\nu+k-p+1)}\\&=E_t(\nu-p,a),\end{aligned}$$

which is (3.5). Trivially, see (3.3),

$$E_t(0,a)=e^{at}\gamma^*(0,at)=\sum_{k=0}^{\infty}\frac{(at)^k}{\Gamma(k+1)}=e^{at},$$

which is (3.6).

4. The Law of Exponents

If α and β are any real numbers, then for suitable functions we may compute $D^{\alpha+\beta}f(t)$. We use (2.10) if $\alpha+\beta>0$ and we use (2.5) if $\alpha+\beta<0$. However, in general, the law of exponents

$$D^{\mu}D^{\nu}=D^{\mu+\nu} \tag{4.1}$$

is *not* necessarily valid without additional caveats. (By (4.1) we mean, of course,

$D^{\mu}[D^{\nu}f(t)] = D^{\mu+\nu}f(t)$). For example, if f is continuous on I, then indeed

$$D[D^{-1}f(t)] = f(t) \tag{4.2}$$

(or symbolically $DD^{-1} = D^{1-1} = D^0$) is true by the Fundamental Theorem of the Integral Calculus. But $D^{-1}[Df(t)]$ is not necessarily equal to $f(t)$. For, let $f(t) = 1$. Then $D^{-1}f(t) = t$ and $D[D^{-1}f(t)] = 1$; but $D^{-1}[Df(t)] = 0$.

However, we shall show that

$$D^{-\mu}[D^{-\nu}f(t)] = D^{-(\mu+\nu)}f(t) \tag{4.3}$$

is true for all *positive* μ and ν, and continuous f. Fortunately this is the only portion of the general law of exponents that we need for our present investigations.

In an attempt to prove (4.3) we write

$$\begin{aligned} D^{-\mu}[D^{-\nu}f(t)] &= \frac{1}{\Gamma(\mu)}\int_0^t (t-\xi)^{\mu-1}[D^{-\nu}f(\xi)]\,d\xi \\ &= \frac{1}{\Gamma(\mu)}\int_0^t (t-\xi)^{\mu-1}\,d\xi \frac{1}{\Gamma(\nu)}\int_0^{\xi}(\xi-x)^{\nu-1}f(x)\,dx. \end{aligned} \tag{4.4}$$

One is then tempted to interchange the order of integration as we did in (2.3) to obtain

$$D^{-\mu}[D^{-\nu}f(t)] = \frac{1}{\Gamma(\mu+\nu)}\int_0^t (t-x)^{\mu+\nu-1}f(x)\,dx. \tag{4.5}$$

We recognize the right-hand side of (4.5) as $D^{-(\mu+\nu)}f(t)$.

Of course the fly in the ointment is: How do we justify the interchange of order of integration? If $G(\xi, x)$ is jointly continuous on $I \times I$, then there is no problem. We know that

$$\int_0^t d\xi \int_0^{\xi} G(\xi, x)\,dx = \int_0^t dx \int_x^t G(\xi, x)\,d\xi.$$

If G is not continuous, but if the integrals $\int_0^{\xi} G\,dx$ and $\int_x^t G\,d\xi$ both exist as ordinary or as improper integrals, then general conditions under which the order of integration may be interchanged are difficult to obtain. And in our problem the integrand is not continuous if μ and/or ν is less than one.

Fortunately, *Dirichlet's formula* may be used to justify the passage from (4.4) to (4.5). A special case of this formula states that if g is continuous on $I \times I$, and if $\mu > 0$, $\nu > 0$, then

$$\begin{aligned} &\int_0^t (t-\xi)^{\mu-1}\,d\xi \int_0^{\xi}(\xi-x)^{\nu-1}g(\xi,x)\,dx \\ &\quad = \int_0^t dx \int_x^t (t-\xi)^{\mu-1}(\xi-x)^{\nu-1}g(\xi,x)\,d\xi. \end{aligned}$$

A proof may be found in [5, page 77].

As an application of (4.3) we shall show that

$$D^{\rho}E_t(\nu, a) = E_t(\nu-\rho, a),\ \nu > 0 \tag{4.6}$$

for all ρ, positive or negative. To do this we see from (2.9) that

$$D^{-\nu}e^{at} = E_t(\nu, a),\ \nu > 0. \tag{4.7}$$

Thus (4.3) implies that for $\mu > 0$

$$D^{-\mu}E_t(\nu, a) = D^{-(\mu+\nu)}e^{at}. \tag{4.8}$$

But from (4.7) we see that the right-hand side of (4.8) is $E_t(\mu + \nu, a)$. Thus we have shown that

$$D^{-\mu}E_t(\nu, a) = E_t(\mu + \nu, a). \tag{4.9}$$

Let us now calculate the fractional derivative of $E_t(\nu, a)$. By definition, see (2.10),

$$D^{\mu}E_t(\nu, a) = D^m\left[D^{-(m-\mu)}E_t(\nu, a)\right]$$

(where $\mu > 0$ and m is the smallest integer greater than μ) is the fractional derivative of $E_t(\nu, a)$ of order μ. Since $D^{-(m-\mu)}E_t(\nu, a) = E_t(\nu + m - \mu, a)$, by (4.9) we have

$$D^{\mu}E_t(\nu, a) = D^m\left[E_t(\nu + m - \mu, a)\right].$$

Equation (3.5) thus establishes the fundamental and useful result that

$$D^{\mu}E_t(\nu, a) = E_t(\nu - \mu, a), \ \mu > 0 \tag{4.10}$$

is the fractional derivative of $E_t(\nu, a)$ of order μ. Combining (4.9) and (4.10) demonstrates the truth of (4.6).

5. Fractional Differential Equations

An ordinary differential equation is an equation involving derivatives of a function, and the basic problem is to find a function that satisfies this equation. For example,

$$[D^2 + aD + bD^0]y(t) = 0 \tag{5.1}$$

(where a and b are constants) is a second-order ordinary linear differential equation with constant coefficients. The problem is to find nonidentically zero functions $y(t)$ that identically satisfy (5.1). Therefore it should come as no surprise that we define a fractional differential equation as an equation involving fractional derivatives of a function. In particular, if n and q are positive integers and $v = 1/q$, then we call

$$\mathscr{E} = D^{nv} + a_1 D^{(n-1)v} + \cdots + a_n D^0 \tag{5.2}$$

a *fractional differential operator of order* (n, q). We shall assume that the a_i are constants. Of course there exist more complicated fractional differential operators, but (5.2) is more than sufficiently complex. Although we can solve the general equation $\mathscr{E}y(t) = 0$, in this elementary treatment we shall focus our attention on equations of order $(2, q)$, that is, on equations of the form

$$[D^{2v} + aD^v + bD^0]y(t) = 0. \tag{5.3}$$

Our problem, of course, is to find a function $y(t)$ that satisfies (5.3). (The fractional Green's function may be used to solve the nonhomogeneous equation $\mathscr{E}y(t) = x(t)$; but we shall not discuss it here, see [3].)

In order to find a viable approach let us briefly review some results in ordinary differential equation theory that may give us a hint as how to proceed. Toward this end, we consider the ordinary differential equation of (5.1). The standard gambit in attempting to find a solution is to apply the differential operator $D^2 + aD + bD^0$ to the exponential function e^{ct} where c is an arbitrary constant. Then

$$[D^2 + aD + bD^0]e^{ct} = (c^2 + ac + b)e^{ct}.$$

Now the above expression will vanish if $c^2 + ac + b = 0$. Thus we see that if $c = \alpha$ where α is a zero of the indicial polynomial P,

$$P(\lambda) = \lambda^2 + a\lambda + b = (\lambda - \alpha)(\lambda - \beta), \tag{5.4}$$

then $e^{\alpha t}$ is a solution of (5.1). Of course, so is $e^{\beta t}$, and if $\alpha \neq \beta$, we have two linearly independent solutions. If $\alpha = \beta$, then α is a double root of $P(\lambda) = 0$ and $e^{\alpha t}$ and $te^{\alpha t}$ are linearly independent solutions of (5.1).

Let us now attempt to use the above arguments in attacking (5.3). We have seen in (3.6) that

$$E_t(0, c) = e^{ct},$$

and using (4.6) we readily compute

$$\begin{aligned} D^v E_t(0, c) &= E_t(-v, c) \\ D^v E_t(-v, c) &= E_t(-2v, c) \\ &\vdots \\ D^v E_t(-(q-1)v, c) &= E_t(-qv, c). \end{aligned}$$

But $qv = 1$, and from (3.4)

$$E_t(-1, c) = cE_t(0, c) + \frac{t^{-1}}{\Gamma(0)}.$$

Since $\Gamma(0) = \infty$ we see that

$$E_t(-1, c) = cE_t(0, c).$$

The significance of these manipulations is that if we apply the operator D^v to $E_t(0, c), E_t(-v, c), \dots, E_t(-(q-1)v, c)$, we get a cyclic permutation of the same functions. That is, no new functions are introduced.

Therefore we shall choose a linear combination of these functions as a candidate for a solution of (5.3), say

$$y(t) = B_0 E_t(0, c) + B_1 E_t(-v, c) + B_2 E_t(-2v, c) + \cdots + B_{q-1} E_t(-(q-1)v, c) \tag{5.5}$$

where $B_0, B_1, \dots, B_{q-1}$ as well as c are arbitrary constants for the moment. From our preceding arguments

$$\begin{aligned} D^v y(t) = {} & cB_{q-1}E_t(0, c) + B_0 E_t(-v, c) + B_1 E_t(-2v, c) \\ & + \cdots + B_{q-2} E_t(-(q-1)v, c). \end{aligned} \tag{5.6}$$

Now if $D^{2v}y(t)$ has the same cyclic property, we may calculate $[D^{2v} + aD^v + bD^0]y(t)$. It will be a linear combination of $E_t(0, c), E_t(-v, c), \dots, E_t(-(q-1)v, c)$ whose coefficients are functions of the B's and c. Then perhaps we can choose $B_0, B_1, \dots, B_{q-1}, c$ such that the coefficients of the $E_t(-kv, c)$ functions vanish. If so, we shall have a solution of (5.3).

Let us therefore start by calculating $D^{2v}y(t)$. Again from (4.6)

$$D^{2v}y(t) = B_0E_t(-2v,c) + B_1E_t(-3v,c) + \cdots + B_{q-2}E_t(-qv,c) + B_{q-1}E_t(-(q+1)v,c).$$

Now, as before, $E_t(-qv,c) = E_t(-1,0) = cE_t(0,c)$. Also

$$E_t(-(q+1)v,c) = E_t(-1-v,c). \tag{5.7}$$

To simplify this expression we again invoke (3.4) with $\nu = -1-v$ and $a = c$. Then

$$E_t(-1-v,c) = cE_t(-v,c) + \frac{t^{-1-v}}{\Gamma(-v)},$$

and (5.7) becomes

$$E_t(-(q+1)v,c) = cE_t(-v,c) + \frac{t^{-1-v}}{\Gamma(-v)}.$$

So while we still have our cyclical property, that is, only terms of the form $E_t(-kv,c)$, $k = 0,1,\ldots,q-1$, appear, we also have the unwanted term $t^{-1-v}/\Gamma(-v)$. Well, let's worry about this term later. For the present we may write $D^{2v}y(t)$ as

$$D^{2v}y(t) = cB_{q-2}E_t(0,c) + cB_{q-1}E_t(-v,c) + B_0E_t(-2v,c) + \cdots + B_{q-3}E_t(-(q-1)v,c) + B_{q-1}\frac{t^{-1-v}}{\Gamma(-v)}. \tag{5.8}$$

Now from (5.5), (5.6), and (5.8) we may compute $[D^{2v} + aD^v + bD^0]y(t)$. If we do so, collecting coefficients of the $E_t(-kv,c)$ terms, we get

$$\begin{aligned}[D^{2v} + aD^v + bD^0]y(t) &= [cB_{q-2} + acB_{q-1} + bB_0]E_t(0,c)\\ &\quad + [cB_{q-1} + aB_0 + bB_1]E_t(-v,c)\\ &\quad + \sum_{k=0}^{q-3}[B_k + aB_{k+1} + bB_{k+2}]E_t(-(k+2)v,c)\\ &\quad + B_{q-1}\frac{t^{-1-v}}{\Gamma(-v)}.\end{aligned} \tag{5.9}$$

Since α is a root of the indicial equation $P(\lambda) = 0$ (see (5.4)),

$$\alpha^2 + a\alpha + b \equiv 0. \tag{5.10}$$

Thus if we compare (5.10) with the terms under the summation sign in (5.9), we see that if the B_k represent decreasing powers of α, then all these terms will vanish. Let us therefore choose B_k as

$$B_k = A\alpha^{-k}$$

where A is an arbitrary nonzero factor independent of k. (For the moment we are assuming that $\alpha \neq 0$.) Then from (5.9)

$$\begin{aligned}B_k + aB_{k+1} + bB_{k+2} &= A(\alpha^{-k} + a\alpha^{-k-1} + b\alpha^{-k-2})\\ &= A\alpha^{-k-2}(\alpha^2 + a\alpha + b)\\ &= 0.\end{aligned}$$

We therefore have reduced (5.9) to

$$\begin{aligned}[D^{2v}+aD^{v}+bD^{0}]y(t) = {} & A[c\alpha^{-q+2}+ac\alpha^{-q+1}+b]E_t(0,c)\\ & +A[c\alpha^{-q+1}+a+b\alpha^{-1}]E_t(-v,c)\\ & +A\alpha^{-q+1}\frac{t^{-1-v}}{\Gamma(-v)}.\end{aligned}$$

But the constant c is still at our disposal. If we let $c=\alpha^q$, then the above expression reduces to

$$[D^{2v}+aD^{v}+bD^{0}]y(t) = A\alpha^{-q+1}\frac{t^{-1-v}}{\Gamma(-v)}. \tag{5.11}$$

Since A is arbitrary, we shall choose it as α^{q-1} so that the term on the right-hand side of (5.11) is independent of α.

With these choices of $B_0, B_1, \ldots, B_{q-1}, c, A$ we may write $y(t)$ (see (5.5)) as

$$e_\alpha(t) = \sum_{k=0}^{q-1}\alpha^{q-k-1}E_t(-kv,\alpha^q)$$

and (5.11) may be written as

$$[D^{2v}+aD^{v}+bD^{0}]e_\alpha(t) = \frac{t^{-1-v}}{\Gamma(-v)}, \tag{5.12}$$

where α is a zero of $P(\lambda)$. If $\alpha=0$ we choose $e_\alpha(t)$ as

$$e_0(t) = \frac{t^{-1+v}}{\Gamma(v)}.$$

Of course $e_\alpha(t)$ is not a solution of (5.3) since we still have the $t^{-1-v}/\Gamma(-v)$ term on the right-hand side of (5.12). But we are getting close. We recall that P has two zeros. Let $\lambda=\beta$ be the other zero. Then similar arguments show that

$$[D^{2v}+aD^{v}+b]e_\beta(t) = \frac{t^{-1-v}}{\Gamma(-v)},$$

where of course

$$e_\beta(t) = \sum_{k=0}^{q-1}\beta^{q-k-1}E_t(-kv,\beta^q).$$

Thus

$$\psi(t) = e_\alpha(t) - e_\beta(t) \tag{5.13}$$

is the solution of (5.3).

If $\alpha\neq\beta$ then (5.13) represents a nonidentically zero solution of (5.3). Of course if $\alpha=\beta$ we have the trivial solution $\psi(t)\equiv 0$. However, we recall the same phenomenon in ordinary differential equation theory. If $\alpha=\beta$, then $te^{\alpha t}$ is a solution of (5.1).

Using a similar but more sophisticated argument one can show that if $\alpha=\beta\neq 0$, that is if the zeros of the indicial polynomial P are equal and nonzero, then

$$\psi(t) = \sum_{k=-(q-1)}^{q-1} \alpha^k (q - |k|) D^{1-(k+1)v}(te^{\alpha^q t})$$

is a nontrivial solution of (5.3).

If $\alpha = 0 = \beta$, then (5.3) becomes

$$D^{2v}y(t) = 0$$

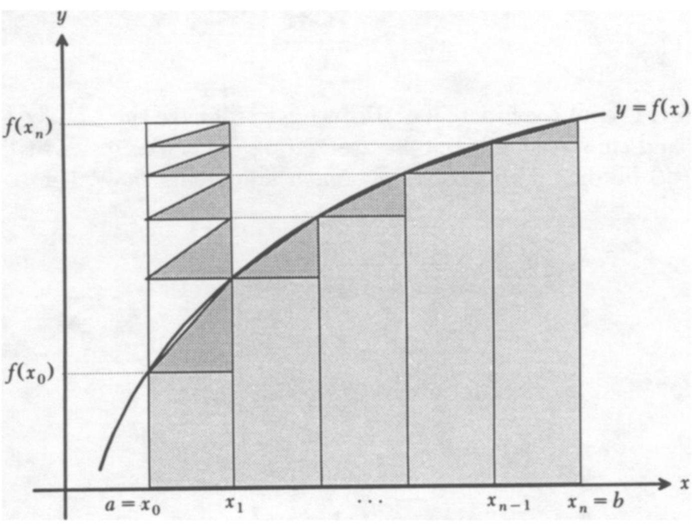
whose solution is

$$y(t) = \frac{t^{2v-1}}{\Gamma(2v)}.$$

REFERENCES

1. E. R. Love, Fractional derivatives of imaginary order, *J. London Math. Soc.* (2) 3 (1971), 241–259.
2. W. Magnus, F. Oberhettinger and R. P. Soni, *Formulas and Theorems for the Special Functions of Mathematical Physics*, Springer-Verlag New York, 1966.
3. K. S. Miller and B. Ross, Fractional Green's functions, *Indian J. Pure Appl. Math.* 22 (1991), 763–767.
4. K. B. Oldham and J. Spanier, *The Fractional Calculus*, Academic Press, New York, 1974.
5. E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge University Press, Cambridge, 1965.

Proof without Words: The Trapezoidal Rule (for Increasing Functions)



$$\int_a^b f(x)\,dx \cong \sum_{i=0}^{n-1} f(x_i)\frac{b-a}{n} + \frac{1}{2}[f(x_n) - f(x_0)]\frac{b-a}{n}$$

—Jesús Urías
Comunicación Optica, UASLP
78000, San Luis Potosí, SLP, México

$$\psi(t) = \sum_{k=-(q-1)}^{q-1} \alpha^k (q - |k|) D^{1-(k+1)v}(te^{\alpha^q t})$$

is a nontrivial solution of (5.3).

If $\alpha = 0 = \beta$, then (5.3) becomes

$$D^{2v} y(t) = 0$$

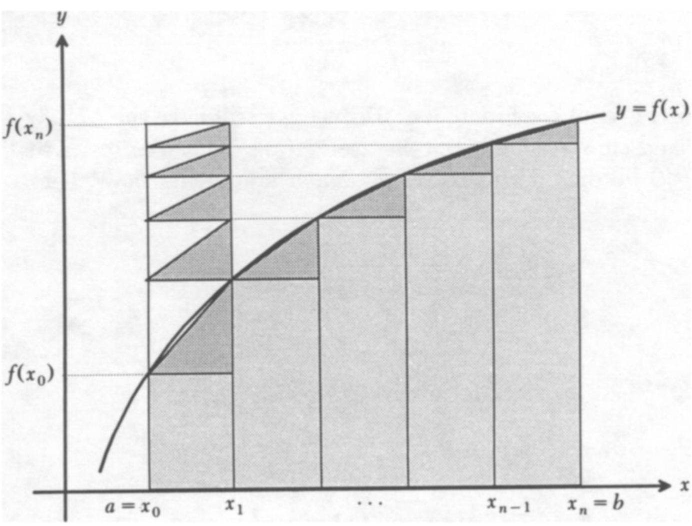
whose solution is

$$y(t) = \frac{t^{2v-1}}{\Gamma(2v)}.$$

REFERENCES

1. E. R. Love, Fractional derivatives of imaginary order, *J. London Math. Soc.* (2) 3 (1971), 241–259.
2. W. Magnus, F. Oberhettinger and R. P. Soni, *Formulas and Theorems for the Special Functions of Mathematical Physics*, Springer-Verlag New York, 1966.
3. K. S. Miller and B. Ross, Fractional Green's functions, *Indian J. Pure Appl. Math.* 22 (1991), 763–767.
4. K. B. Oldham and J. Spanier, *The Fractional Calculus*, Academic Press, New York, 1974.
5. E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge University Press, Cambridge, 1965.

Proof without Words: The Trapezoidal Rule (for Increasing Functions)



$$\int_a^b f(x)\,dx \cong \sum_{i=0}^{n-1} f(x_i)\frac{b-a}{n} + \frac{1}{2}[f(x_n) - f(x_0)]\frac{b-a}{n}$$

—Jesús Urías
Comunicación Optica, UASLP
78000, San Luis Potosí, SLP, México

NOTES

Copulas, Characterization, Correlation, and Counterexamples

ROGER B. NELSEN
Lewis and Clark College
Portland, OR 97219-7899

1. Copulas Copulas are functions that join univariate distribution functions to form multivariate distribution functions. They were first introduced in 1959 by A. Sklar **[10]** to answer some questions posed by M. Fréchet concerning the relationship between a multidimensional probability distribution function and its lower dimensional marginals. Over the past 30 years or so, copulas have played an important role in several areas of probability and statistics, including multivariate distribution theory, nonparametric statistics, and Markov processes; but only recently have they come to the attention of the general statistical and mathematical communities. In this paper, we will survey some of the important properties of copulas, and demonstrate ways in which copulas can be employed in probability and mathematical statistics courses to enhance and illuminate the presentation of a number of topics. Specifically, we will show how copulas can be used in statistics i) to characterize some dependence concepts for two random variables; ii) to obtain a geometric interpretation of the population version of a nonparametric correlation coefficient, and to illustrate how that coefficient measures dependence; and iii) to facilitate the generation of counterexamples.

A (two-dimensional) *copula* is a function $C: \mathbf{I}^2 \to \mathbf{I} = [0,1]$ with the following properties:

(i) $C(0,t) = C(t,0) = 0$ and $C(1,t) = C(t,1) = t$ for all t in $\mathbf{I}$; and (1.1)
(ii) $C(u_2,v_2) - C(u_1,v_2) - C(u_2,v_1) + C(u_1,v_1) \geq 0$ for all u_1,u_2,v_1,v_2 in $\mathbf{I}$ such that $u_1 \leq u_2$ and $v_1 \leq v_2$.

It follows that C is nondecreasing in each variable (let $v_1 = 0$ or $u_1 = 0$ above) and continuous (since (1.1) implies that C satisfies the Lipschitz condition $|C(u_2,v_2) - C(u_1,v_1)| \leq |u_2 - u_1| + |v_2 - v_1|$). If one thinks of $C(u,v)$ as assigning a number in $\mathbf{I}$ to the rectangle $[0,u] \times [0,v]$ then part (ii) of (1.1) gives an "inclusion-exclusion"-type formula for the number assigned by C to each rectangle $[u_1,u_2] \times [v_1,v_2]$ in $\mathbf{I}^2$, and states that the number so assigned must be nonnegative.

The importance of copulas to mathematical statistics is described in

SKLAR'S THEOREM. *Let H be a two-dimensional distribution function (d.f.) with marginal d.f.'s F and G. Then there exists a copula C such that $H(x,y) = C(F(x),G(y))$. Conversely, for any univariate d.f.'s F and G and any copula C, the function H defined above is a two-dimensional d.f. with marginals F and G. Furthermore, if F and G are continuous, C is unique.*

Thus a copula "couples" a bivariate d.f. to its one-dimensional marginal d.f.'s. A proof of Sklar's theorem may be found in [8]. In addition, a copula is itself a bivariate distribution function with marginals uniform on $\mathbf{I}$.

As noted by M. Fréchet [1], it is an elementary exercise to show that any bivariate d.f. H with marginal d.f.'s F and G satisfies

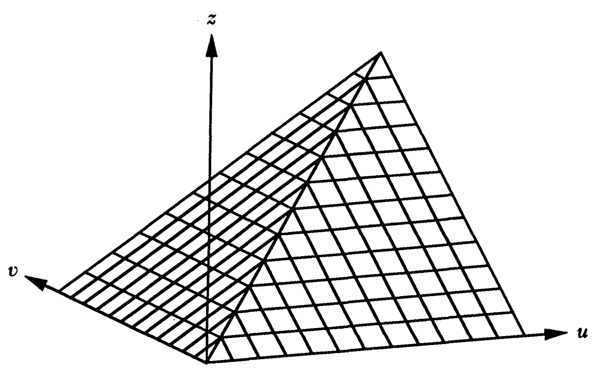
$$\max\{F(x)+G(y)-1,0\}\leq H(x,y)\leq \min\{F(x),G(y)\}. \qquad (1.2)$$

To see this, observe that: $H(x,y)=\Pr\{X\leq x, Y\leq y\}\leq \Pr\{X\leq x\}=F(x)$; similarly $H(x,y)\leq G(y)$; and $1\geq \Pr\{X\leq x \text{ or } Y\leq y\}=F(x)+G(y)-H(x,y)$. The bounds in (1.2) for bivariate d.f.'s are often referred to as the lower and upper *Fréchet bounds, and are themselves bivariate d.f.'s. In terms of copulas, (1.2) is*

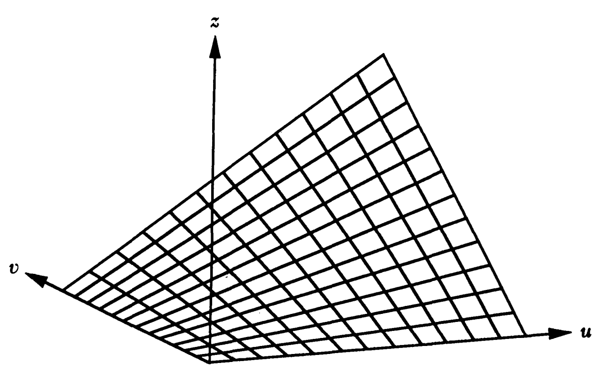
$$\max\{u+v-1,0\}\leq C(u,v)\leq \min\{u,v\} \quad \text{for all } u,v\in \mathbf{I}, \qquad (1.3)$$

and the lower and upper bounds in (1.3) are the copulas for the Fréchet bounds in (1.2).

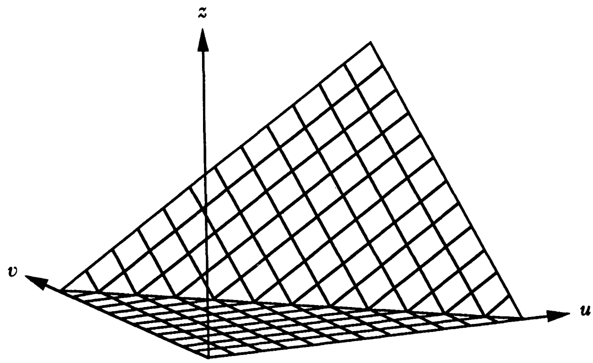
Several of our applications involve the shape of the graph of a copula, i.e., of the surface $z=C(u,v)$. It follows from (1.1) that the graph of any copula is a continuous surface whose boundary is the skew quadrilateral with vertices (0,0,0), (0,1,0), (1,1,1), and (1,0,0); and from (1.3) that this graph lies between the surfaces $z=\max\{u+v-1,0\}$ and $z=\min\{u,v\}$. In the figures we display the graphs of the copulas $\max\{u+v-1,0\}$ and $\min\{u,v\}$ for the Fréchet bounds, and the important intermediate case, $z=C(u,v)=uv$. Alternatively, the graph of a copula can be viewed as the graph of the joint d.f. $z=H(x,y)$ in which the x and y axes have been relabelled in units of $u=F(x)$ and $v=G(y)$. For a complete historical discussion of copulas and an extensive bibliography, see [7].



$z=\min\{u,v\}$



$z=uv$



$z = \max\{u + v - 1, 0\}$

2. Characterization In this section and the next, let X and Y be continuous random variables (r.v.'s) with joint d.f. H, marginal d.f.'s, F and G, respectively, and copula C. Many properties of the pair X, Y may be succinctly expressed as properties of the corresponding copula C. Independence is one such property: in terms of d.f.'s X and Y are independent if, and only if, $H(x, y) = F(x)G(y)$. So, as a consequence of Sklar's theorem, every pair of independent r.v.'s has the same copula, or

(a) X and Y are independent if, and only if, $C(u, v) = uv$.

At the other extreme, monotone functional dependence of r.v.'s can also be shown to be a property of the copula: Specifically,

(b) Y is almost surely an increasing function of X if, and only if, $C(u, v) = \min\{u, v\}$; and

(c) Y is almost surely a decreasing function of X if, and only if, $C(u, v) = \max\{u + v - 1, 0\}$.

These last two results are usually attributed to Fréchet. For a recent proof, see **[3]**.

Another statistical concept similar to but weaker than independence is *exchangeability*. A (finite) set of r.v.'s is exchangeable if the individual r.v.'s are identically distributed; every pair of r.v.'s has the same joint distribution as every other pair; and so on. Whereas independent r.v.'s are exchangeable, exchangeable r.v.'s need not be independent. For example, sampling with replacement from a finite population yields observations that are independent and exchangeable, sampling without replacement yields observations that are exchangeable but not independent. In the bivariate setting, X and Y are exchangeable if the vectors (X, Y) and (Y, X) have the same distribution. So exchangeability of r.v.'s is essentially equivalent to symmetry of their copula, or:

(d) X and Y are exchangeable if, and only if, $F = G$ and $C(u, v) = C(v, u)$.

In a number of statistical situations, it may be desirable to describe qualitatively the statement that "large values of Y occur with large values of X, and small values of Y occur with small values of X." For example, if X and Y denote a student's percentile scores on two achievement tests, then X and Y may tend to be simultaneously high or simultaneously low. One such "positive dependence property" is *positive quadrant dependence* **[2]**: X and Y are positively quadrant dependent if their joint distribution is such that the probability that they are simultaneously "small" is at least as great as it would be were they independent r.v.'s; that is, $\Pr\{X \le x, Y \le y\} \ge \Pr\{X \le x\}\Pr\{Y \le y\}$ for all x and y. Since this is equivalent to $H(x, y) \ge F(x)G(y)$, it readily follows that

(e) X and Y are positively quadrant dependent if, and only if, $C(u, v) \ge uv$ for all $u, v \in \mathbf{I}$. A geometric interpretation of positive quadrant dependence is immediate: X

and Y are positively quadrant dependent if, and only if, the graph of $z = C(u, v)$ lies on or above the graph of $z = uv$.

For a discussion of several other dependence concepts in terms of copulas and their corresponding geometric interpretations, see [4].

3. Correlation As we've seen in the preceding section, a property of r.v.'s that doesn't depend on the form of the marginal distributions can often be expressed in terms of the copula. Indeed, it can be shown [9] that if f and g are strictly increasing (almost surely) on the ranges of X and Y, respectively, then the copula of the r.v.'s $f(X)$ and $g(Y)$ is the same as the copula of X and Y. In other words, while almost surely strictly increasing functions of the r.v.'s will alter the marginal and joint d.f.'s, they leave the copula unchanged. Thus it is the copula that expresses the "nonparametric" or "distribution-free" properties of the joint distribution of X and Y, i.e., those properties (such as positive, quadrant dependence) that are invariant under almost surely strictly increasing transformations. Hence one might suspect that the population analog of a nonparametric correlation coefficient such as Spearman's rho (ρ_s) would be expressible in terms of the copula. Such is indeed the case, and the result yields a nice geometric interpretation of ρ_s.

Spearman's ρ_s, introduced by the psychologist C. Spearman in 1904, is also known as the grade correlation coefficient, a term introduced by K. Pearson. The population version of Spearman's ρ_s can be defined as the ordinary Pearson product-moment correlation coefficient, applied not to the r.v.'s X and Y, but to their "grades" $U = F(X)$ and $V = G(Y)$. Since U and V are uniform on $\mathbf{I}$ (note that $F(x) = \Pr\{X \le x\} = \Pr\{U \le F(x)\}$), we have $E(U) = E(V) = 1/2$ and $\operatorname{Var}(U) = \operatorname{Var}(V) = 1/12$. The joint d.f. of U and V is C, and thus

$$\rho_s = \frac{E(UV) - 1/4}{1/12} = 12E(UV) - 3 = 12\int\int_{\mathbf{I}^2} uv\, dC - 3.$$

But if (U', V') is any other pair of r.v.'s independent of (U, V), each uniform on $(0, 1)$ with joint d.f. C', then $\int\int_{\mathbf{I}^2} C(u, v)\, dC' = \int\int_{\mathbf{I}^2} C'(u, v)\, dC$ since

$$\Pr\{U \le U', V \le V'\} = \int\int_{\mathbf{I}^2} \Pr\{U \le u, V \le v\}\, dC' = \int\int_{\mathbf{I}^2} C(u, v)\, dC',$$

and

$$\begin{aligned}\Pr\{U' \ge U, V' \ge V\} &= \int\int_{\mathbf{I}^2} \Pr\{U' \ge u, V' \ge v\}\, dC \\ &= \int\int_{\mathbf{I}^2} [1 - u - v + C'(u, v)]\, dC = \int\int_{\mathbf{I}^2} C'(u, v)\, dC.\end{aligned}$$

Thus $\int\int_{\mathbf{I}^2} uv\, dC = \int\int_{\mathbf{I}^2} C\, du dv$ and hence

$$\rho_s = 12\int\int_{\mathbf{I}^2} C\, du dv - 3 = 12\int\int_{\mathbf{I}^2} [C(u, v) - uv]\, du dv. \tag{3.1}$$

From (3.1) we obtain simple geometric interpretations of Spearman's ρ_s. Since $\int\int_{\mathbf{I}^2} C\, du dv$ represents the volume of the portion of the unit cube below the graph of $z = C(u, v)$, we see from (1.3) that the value of this integral lies between $1/6$ and $1/3$. Thus ρ_s can be viewed as the volume under the graph of $z = C(u, v)$ over $\mathbf{I}^2$, scaled to lie between -1 and $+1$, or as the (scaled) signed volume between the surfaces $z = C(u, v)$ and $z = uv$. Indeed, any measure of distance between these surfaces is a measure of dependence. See [9] for further examples.

In the previous section we observed that X and Y are positively quadrant dependent if, and only if, $C(u,v) \geq uv$ on $\mathbf{I}^2$. So, in a sense, the quantity $C(u,v) - uv$ is a measure of "local" positive (and negative) quadrant dependence, and thus $\rho_s/12 = \int\int_{\mathbf{I}^2}[C(u,v) - uv]\ dudv$ can be interpreted as a measure of "average" quadrant dependence.

Similar results exist for the population version of another nonparametric correlation coefficient, Kendall's tau. For details, see [5].

4. Counterexamples When the student of probability and statistics encounters a statement, the task usually is (as in other branches of mathematics) to either provide a proof if it is true or find a counterexample if it is false. In this final section we will illustrate the ease with which copulas can be used to construct counterexamples. Of course, other examples for each of the following situations exist; see, for example, [6] and [11].

For the first five examples, consider the copula formed by averaging the two copulas for the Fréchet bounds, i.e., $C_1(u,v) = (1/2)(\max\{u+v-1,0\} + \min\{u,v\})$. Let U and V be r.v.'s with joint d.f. C_1. This copula concentrates the probability mass uniformly on the two diagonals of $\mathbf{I}^2$, i.e., $(U-V)(U+V-1) = 0$ holds almost surely. Whenever there is at least one relationship $\varphi(U,V) = 0$ that holds with probability 1 on $\mathbf{I}^2$ (but φ not identically 0 on $\mathbf{I}^2$), we call the distribution (and the copula) *singular*. We note that the Fréchet bounds are singular as well.

Example 1. There exist exchangeable random variables that are not independent. Note that U and V have the same marginal distribution and that $C_1(u,v) = C_1(v,u)$. But more is true—U and V are also uncorrelated, since $\mathrm{Cov}(U,V) = E(UV) - E(U)E(V) = 1/4 - (1/2)^2 = 0$.

Example 2. There is a bivariate distribution without a density but whose marginals possess densities (note that $\partial^2 C_1(u,v)/\partial u \partial v = 0$ almost everywhere).

For the next three examples, let X and Y be standard normal r.v.'s with d.f. Φ.

Example 3. There exist bivariate distributions with normal marginals that are not bivariate normal. Indeed, if $N_\rho(x,y)$ denotes a standard bivariate normal d.f. with (Pearson) correlation coefficient ρ for some $\rho \in (-1,1)$, then *any* copula *except* one of the form $C(u,v) = N_\rho(\Phi^{-1}(u), \Phi^{-1}(v))$ will suffice!

Example 4. There exist uncorrelated normal random variables that are not independent (note that $E(XY) = 0$ but $C_1(u,v) \neq uv$). Recall that if X and Y are bivariate normal, then X and Y are independent if, and only if, they are uncorrelated—and this example shows that this conclusion need not hold when the joint d.f. is not a bivariate normal.

Example 5. Two normal random variables may have a sum that is not normal (note that $\Pr\{X+Y=0\} = 1/2$). Again, if X and Y are bivariate normal, then the sum (or any other linear combination) is also normal.

For the final four examples, let U and V be r.v.'s uniform on $\mathbf{I}$, but satisfying $V = |2U-1|$, and let C_2 denote their copula. To find an expression for C_2, we evaluate $C_2(u,v) = \Pr\{U \leq u, V \leq v\}$ where $V = 1-2U$ when $u \in [0,1/2]$ and $V = 2U-1$ when $u \in (1/2,1]$. This yields

$$C_2(u,v) = \begin{cases} \max\left\{u + \frac{1}{2}(v-1), 0\right\}, u \in \left[0, \frac{1}{2}\right], \\ \min\left\{u + \frac{1}{2}(v-1), v\right\},\ u \in \left(\frac{1}{2}, 1\right]. \end{cases}$$

This copula, again singular, concentrates the probability uniformly on the polygonal line in $\mathbf{I}^2$ that joins $(0,1)$ to $(1/2,0)$ to $(1,1)$, i.e., the graph of $v = |2u-1|$ for $u \in \mathbf{I}$.

Example 6. Two r.v.'s can be uncorrelated although one can be predicted perfectly from the other ($\mathrm{Cov}(U,V)=0$ but $V=|2U-1|$).

Example 7. Two r.v.'s may be identically distributed and uncorrelated but not exchangeable (C_2 is not symmetric in u and v).

Example 8. There exist identically distributed r.v.'s whose difference is not symmetric about 0 (note that $\Pr\{U-V>0\} = \Pr\{U>1/3\} = 2/3$).

Example 9. There exist pairs of r.v.'s each symmetric about 0, but whose sum is not symmetric about 0 (Let $X=2U-1$ and $Y=2V-1$ so that X and Y are uniform on $(-1,1)$, then note that $\Pr\{X+Y>0\} = \Pr\{U+V>1\} = \Pr\{U>2/3\} = 1/3$).

REFERENCES

1. M. Fréchet, Sur les tableaux de corrélation dont les marges sont données, *Annales de l'Université de Lyon*, 9 (1951), Sect. A, 53–77.
2. E. L. Lehmann, Some concepts of dependence, *Annals of Mathematical Statistics*, 37 (1966), 1137–1153.
3. P. Mikusiński, H. Sherwood, and M. D. Taylor, The Fréchet bounds revisited, *Real Analysis Exchange*, 17 (1991-92), 759-764.
4. R. B. Nelsen, Copulas and association, in *Advances in Probability Distributions with Given Marginals*, eds. G. Dall'Aglio, S. Kotz and G. Salinetti; Kluwer Academic Publishers, Dordrecht (1991), 51–74.
5. R. B. Nelsen, On measures of association as measures of positive dependence, *Statistics & Probability Letters* 14 (1992), 269–274.
6. J. P. Romano and A. F. Siegel, *Counterexamples in Probability and Statistics*, Wadsworth and Brooks/ Cole, Pacific Grove, CA (1986).
7. B. Schweizer, Thirty years of copulas, in *Advances in Probability Distributions with Given Marginals*, eds. G. Dall'Aglio, S. Kotz and G. Salinetti; Kluwer Academic Publishers Dordrecht (1991), 13–50.
8. B. Schweizer and A. Sklar, *Probabilistic Metric Spaces*, Elsevier Science Publishing Co., New York, 1983.
9. B. Schweizer and E. F. Wolff, On nonparametric measures of dependence for random variables, *Annals of Statistics*, 9 (1981), 879–885.
10. A. Sklar, Fonctions de répartition à n dimensions et leurs marges, *Publications de l'Institut Statistique de l' Université de Paris*, 8 (1959), 229–231.
11. J. M. Stoyanov, *Counterexamples in Probability*, John Wiley & Sons, Inc., New York, 1987.

An Amazing Identity of Ramanujan

MICHAEL D. HIRSCHHORN
University of New South Wales
Kensington, N.S.W., Australia 2033

In the so-called "lost notebook" of Ramanujan ([1], p. 341), one finds the following amazing statement:

If

$$\frac{1+53x+9x^2}{1-82x-82x^2+x^3} = \sum_{n>0} a_n x^n,$$

$$\frac{2-26x-12x^2}{1-82x-82x^2+x^3} = \sum_{n\geqslant 0} b_n x^n$$

and

$$\frac{2+8x-10x^2}{1-82x-82x^2+x^3} = \sum_{n\geqslant 0} c_n x^n,$$

then

$$a_n^3 + b_n^3 = c_n^3 + (-1)^n.$$

What is amazing about this result is not only that it is true, but that anyone could think of it at all. The purpose of this note is twofold: to show that the result is true, and to show how Ramanujan may have found it.

It is easy enough to show via partial fractions that

$$a_n = \frac{1}{85}\left\{(64+8\sqrt{85})\alpha^n + (64-8\sqrt{85})\beta^n - 43(-1)^n\right\},$$

$$b_n = \frac{1}{85}\left\{(77+7\sqrt{85})\alpha^n + (77-7\sqrt{85})\beta^n + 16(-1)^n\right\},$$

$$c_n = \frac{1}{85}\left\{(93+9\sqrt{85})\alpha^n + (93-9\sqrt{85})\beta^n - 16(-1)^n\right\},$$

where $\alpha = \dfrac{83+9\sqrt{85}}{2}$, $\beta = \dfrac{83-9\sqrt{85}}{2}$.

It follows that

$$\begin{aligned} a_n^3 = \frac{1}{85^3}\Big\{&(1306624+141824\sqrt{85})\alpha^{3n} + (1306624-141824\sqrt{85})\beta^{3n} \\ &-(1230144+132096\sqrt{85})(-\alpha^2)^n - (1230144-132096\sqrt{85})(-\beta^2)^n \\ &+(96960+12120\sqrt{85})\alpha^n + (96960-12120\sqrt{85})\beta^n + 267245(-1)^n\Big\}; \end{aligned}$$

$$\begin{aligned} b_n^3 = \frac{1}{85^3}\Big\{&(1418648+153664\sqrt{85})\alpha^{3n} + (1418648-153664\sqrt{85})\beta^{3n} \\ &+(484512+51744\sqrt{85})(-\alpha^2)^n + (484512-51744\sqrt{85})(-\beta^2)^n \\ &+(466620+42420\sqrt{85})\alpha^n + (466620-42420\sqrt{85})\beta^n + 173440(-1)^n\Big\}; \end{aligned}$$

$$c_n^3 = \frac{1}{85^3}\Big\{(2725272+295488\sqrt{85})\alpha^{3n} + (2725272-295488\sqrt{85})\beta^{3n}.$$
$$-(745632+80352\sqrt{85})(-\alpha^2)^n - (745632-80352\sqrt{85})(-\beta^2)^n$$
$$+(563580+54540\sqrt{85})\alpha^n + (563580-54540\sqrt{85})\beta^n - 173440(-1)^n\Big\},$$

and $a_n^3 + b_n^3 - c_n^3 = (-1)^n$.

How did Ramanujan discover the result? I believe he did the following.

He started with an identity such as

$$(A^2+7AB-9B^2)^3 + (2A^2-4AB+12B^2)^3$$
$$= (2A^2+10B^2)^3 + (A^2-9AB-B^2)^3.$$

(Several similar identities appear in Ramanujan's work.) Now define the sequence $\{h_n\}$ by

$$h_0 = 0,\ h_1 = 1,\ h_{n+2} = 9h_{n+1} + h_n.$$

Then

$$h_{n+1}^2 - h_{n+2}h_n = (-1)^n.$$

Set

$$A = h_{n+1},\ B = h_n.$$

Then

$$A^2 - 9AB - B^2 = h_{n+1}^2 - h_n(9h_{n+1} + h_n)$$
$$= h_{n+1}^2 - h_n h_{n+2} = (-1)^n.$$

Let

$$a_n = A^2 + 7AB - 9B^2 = h_{n+1}^2 + 7h_{n+1}h_n - 9h_n^2,$$
$$b_n = 2A^2 - 4AB + 12B^2 = 2h_{n+1}^2 - 4h_{n+1}h_n + 12h_n^2, \text{ and}$$
$$c_n = 2A^2 + 10B^2 = 2h_{n+1}^2 + 10h_n^2.$$

Then

$$a_n^3 + b_n^3 = c_n^3 + (-1)^n.$$

Now it can easily be shown that

$$h_n = \frac{1}{\sqrt{85}}\left\{\left(\frac{9+\sqrt{85}}{2}\right)^n - \left(\frac{9-\sqrt{85}}{2}\right)^n\right\},$$

and hence that

$$h_n^2 = \frac{1}{85}\left\{\left(\frac{83+9\sqrt{85}}{2}\right)^n + \left(\frac{83-9\sqrt{85}}{2}\right)^n - 2(-1)^n\right\},$$

$$h_{n+1}^2 = \frac{1}{85}\left\{\left(\frac{83+9\sqrt{85}}{2}\right)^{n+1} + \left(\frac{83-9\sqrt{85}}{2}\right)^{n+1} + 2(-1)^n\right\},$$

and

$$h_n h_{n+1} = \frac{1}{85}\left\{\left(\frac{9+\sqrt{85}}{2}\right)\left(\frac{83+9\sqrt{85}}{2}\right)^n + \left(\frac{9-\sqrt{85}}{2}\right)\left(\frac{83-9\sqrt{85}}{2}\right)^n - 9(-1)^n\right\}$$

It follows that

$$\sum_{n\geqslant 0} h_n^2 x^n = \frac{x-x^2}{1-82x-82x^2+x^3},$$

$$\sum_{n\geqslant 0} h_{n+1}^2 x^n = \frac{1-x}{1-82x-82x^2+x^3},$$

and

$$\sum_{n\geqslant 0} h_n h_{n+1} x^n = \frac{9x}{1-82x-82x^2+x^3},$$

and hence that

$$\sum_{n\geqslant 0} a_n x^n = \frac{(1-x)+7(9x)-9(x-x^2)}{1-82x-82x^2+x^3} = \frac{1+53x+9x^2}{1-82x-82x^2+x^3},$$

$$\sum_{n\geqslant 0} b_n x^n = \frac{2(1-x)-4(9x)+12(x-x^2)}{1-82x-82x^2+x^3} = \frac{2-26x-12x^2}{1-82x-82x^2+x^3},$$

and

$$\sum_{n\geqslant 0} c_n x^n = \frac{2(1-x)+10(x-x^2)}{1-82x-82x^2+x^3} = \frac{2+8x-10x^2}{1-82x-82x^2+x^3},$$

as stated by Ramanujan.

REFERENCE

1. S. Ramanujan Aiyangar, *The Lost Notebook and Other Unpublished Papers*, New Delhi, Narosa, 1988.

Convergence of Complex Continued Fractions

JOHN MARAFINO
TIMOTHY J. McDEVITT
James Madison University
Harrisonburg, VA 22801

I. Introduction Our major goal in this paper is to use a variety of techniques available to the advanced undergraduate in the study of the convergence and divergence of a particular complex continued fraction. The material was actually presented to an independent study group and touches upon several areas:

a) analysis—using the derivative to determine the convergence of an iterative sequence;
b) algebra—the use of finitely generated groups in the study of the divergence of periodic sequences;
c) number theory—how counting functions can determine the size of certain groups;
d) topology—changing the setting of a problem to one that easily lends itself to the study of our problem; and
e) complex variables—using properties of Moebius transformations when examining the iterates of a function.

The problem before us is to determine those complex numbers c, for which the continued fraction

$$\cfrac{1}{1+\cfrac{c}{1+\cfrac{c}{\ddots}}} \tag{1}$$

converges. By considering iterates of the function

$$f_c(z) = \frac{1}{1+cz} \tag{2}$$

evaluated at zero; that is, by considering the sequence $f_c(0)$, $f_c(f_c(0)) = f_c^2(0), f_c(f_c(f_c(0))) = f_c^3(0), \dots, f_c^n(0), \dots,$ it will be shown that the complex fraction (1) converges for all complex numbers $\mathbb{C}$ except those on the real line less than $-1/4$. We will do this in two ways; in Section II we will use techniques that illustrate (a) and (e), and in Section III we will use techniques illustrating (b), (c), and (d).

The earliest record of real continued fractions is contained in the works of Bombelli and Cataldi [**9**, p. 1] and dates back to the latter half of the 1500s. However, it wasn't until the 1700s that a systematic treatment of continued fractions was presented by Euler [**7**] in his book *Introduction to Analysis of the Infinite*. The first known result for complex continued fractions, which includes the type we are examining, dates back to Worpitzky [**9**, p. 10] in 1865. His theorem dealt with circular regions of convergence. A more generalized statement of the problem, its different cases, and more complete solutions were formalized around the early 1900s by Van Vleck [**9**, p. 10], Pringsheim [**9**, p. 46], and others [**9**, p. 46]. We choose not to deal with the problem in its complete generality for a number of reasons. First, it is not how mathematics is usually done. Generalizations follow from the special cases, and so it would be misleading to the student to do otherwise. Second, generalizations often cloud the picture. The essential ideas in the proof are often buried somewhere in the generalized argument. Third, it makes exploring other techniques of proof and applying them to our setting more difficult.

In addition to the convergence problem, we will also consider what happens to those c-values in $(-\infty, -1/4)$, for which the iterates of $f_c(0)$ diverge. In this interval we define for each $k = 2, 3, \ldots,$ a set D_k, which contains those values of c for which the sequence $\{f_c^n(0)\}$ has k convergent subsequences $\{f_c^{nk+j}(0)\}$, $j = 1, 2, \ldots, k$, each with a distinct limit. It will be shown that the D_k's have a finite number of elements and that their union is dense on $(-\infty, -1/4)$. Major work in the divergence of iterates was done by Julia and Fatou in the 1920s, and with the use of high-power computers continues to be an open and exciting area of study in dynamical systems [3], [5], [6].

II. The derivative and iterates of $f_c(z)$ The techniques we use in the proofs of this section are motivated by the paper of Baker and Rippon [2] in which the convergence of $a, a^a, a^{a^a}, \ldots, a \in \mathbb{C}$, is considered.

THEOREM 1. *If $f_c^n(0)$ converges as $n \to \infty$, then*

$$c \in D = \{t^2 + t : \mathrm{Re}(t) > -1/2\} \cup \{-1/4\}.$$

Note that $D = \mathbb{C} \setminus (-\infty, -1/4)$.

Proof. If $c = 0$, then $f_c^n(0) = 1$ for all n. Hence, $\{f_c^n(0)\}$ converges and $c \in D$. Suppose $c \neq 0$ and let $w = \lim_{n \to \infty} f_c^n(0)$. Then w is a fixed point of $f_c(z)$, so $w = 1/(1 + cw)$. Letting $t = cw$ we have $w = 1/(1+t)$ and $c = t^2 + t$. Because $f_c(z)$ is one-to-one and $w \neq 0$ is a fixed point, $f_c^n(0) \neq w$ for every n, and

$$\lim_{n \to \infty} \left(\frac{f_c^{n+1}(0) - w}{f_c^n(0) - w} \right) = \lim_{n \to \infty} \left(\frac{f_c(f_c^n(0)) - f_c(w)}{f_c^n(0) - w} \right) = f_c'(w) = \frac{-t}{t+1}.$$

Since $\{f_c^n(0)\}$ converges, it must be that $|-t/(t+1)| \leq 1$. Otherwise, one can show that there exists a $\lambda > 1$ such that for n sufficiently large, $|f_c^{n+1}(0) - w| > \lambda |f_c^n(0) - w|$, and this implies that the sequence does not converge to w. Therefore, $|-t/(t+1)| \leq 1$, and this is equivalent to $\mathrm{Re}(t) \geq -1/2$.

We now show that the assumption $\{f_c^n(0)\}$ converges implies that either $\mathrm{Re}(t) > -1/2$ or $t = -1/2$. Suppose to the contrary that $\mathrm{Re}(t) = -1/2$ and $\mathrm{Im}(t) \neq 0$. Then c is real, and $c < -1/4$. Since w is a fixed point of $f_c(z)$, $f_c(w) = w = 1/(1 + cw)$ and it follows that

$$cw^2 + w - 1 = 0, \tag{3}$$

which in turn implies

$$w = \frac{-1 \pm \sqrt{1 + 4c}}{2c}. \tag{4}$$

Thus, w has a nonzero imaginary part. But because c is real-valued, $\{f_c^n(0)\}$ must be contained in $\mathbb{R}$ and so must its limit point, w. This is a contradiction. Hence, our claim is established and the theorem follows.

In our proof the assumption of convergence of the iterates placed a bound less than one on the magnitude of the derivative. Can we argue the result in the other direction? The answer is yes and is the central idea in the proof of the converse of

Theorem 1. We also take advantage of the following properties of Moebius transformations:

i) The composition of Moebius transformations is a Moebius transformation [1, p. 77].
ii) A Moebius transformation has at most two fixed points, unless it is the identity function [1, p. 78].

THEOREM 2. *If* $c \in D = \{t^2 + t\colon \operatorname{Re}(t) > -1/2\} \cup \{-1/4\}$, *then the sequence* $\{f_c^n(0)\}$, $n = 1, 2, 3, \ldots$ *converges.*

Proof. If $c = 0$, then $f_c^n(0) = 1$ for all n, so the sequence converges. If $c = -1/4$, then

$$f_c(z) = \frac{1}{1 - \frac{1}{4}z}$$

has one fixed point at $z = 2$. Consider the real-valued function

$$F(x) = \frac{1}{1 - \frac{1}{4}x}.$$

Clearly, $F^n(0) = f_c^n(0)$ for all n. Since $F(x)$ is increasing on $(-\infty, 4)$ we have that $F^n(0) < F^n(2) = 2$ for every n. In addition, $F(0) = 1 < 4/3 = F^2(0)$ and so $F^n(0) < F^{n+1}(0)$ for all n. Hence, the sequence $\{F^n(0)\}$ converges. Suppose λ is the limit of this bounded increasing sequence. This gives

$$\lambda = \lim_{k\to\infty} f_c^{k+1}(0) = \lim_{k\to\infty} f_c(f_c^k(0)) = f_c\Big(\lim_{k\to\infty} f_c^k(0)\Big) = f_c(\lambda).$$

Since there is only one fixed point, we conclude $\lambda = 2$. Therefore, the sequence converges to the point $\lambda = 2$.

Suppose $c \neq 0$ and $c \neq -1/4$. There is exactly one t such that $c = t^2 + t$ and $\operatorname{Re}(t) > -1/2$; hence $f_c(z)$ has two distinct fixed points at $1/(1+t)$ and $-(1/t)$. Let $\Omega = \{z\colon \exists\delta > 0 \ni f_c^n$ converges uniformly to $1/(1+t)$, a constant function, on $N_\delta(z)\}$, where $N_\delta(z)$ denotes an open disk about z of radius δ. Observe that Ω is open. Since $w = 1/(1+t)$ is a fixed point and $|f_c'(w)| = \eta < 1$, one can find a $\delta > 0$ so that when $z \in N_\delta(w)$, $|f_c^n(z) - w| = |f_c^n(z) - f_c^n(w)| < \eta^n|z - w| < \eta^n\delta$. It follows that f_c^n converges uniformly to w in $N_\delta(z)$. Thus, $w = 1/(1+t) \in \Omega$ and obviously $-(1/t) \notin \Omega$.

Let $g_c(z) = (1 - z)/cz$ be the inverse of $f_c(z)$. Since the singularity of $f_c(z)$ is $-(1/c)$, the singularity of $f_c^{n+1}(z)$, which is also a Moebius transformation, is $g_c^n(-(1/c))$. We now show that

$$\lim_{n\to\infty} g_c^n\left(-\frac{1}{c}\right) = -\frac{1}{t}.$$

(We will need this result later.) Let $c_n = g_c^n(-(1/c))$ for each n. Using (i) we can express $f_c^n(z)$ in the form

$$f_c^n(z) = A_n + \frac{B_n}{z - c_{n-1}}, \tag{5}$$

and since $1/(1+t)$ and $-1/t$ are fixed points of f_c^n, we have

$$A_n = -\frac{1}{t} + \frac{1}{t+1} - c_{n-1} \quad \text{and} \quad B_n = \left(\frac{1}{t} + c_{n-1}\right)\left(\frac{1}{t+1} - c_{n-1}\right).$$

In addition,

$$|f_c^{n'}(1/(1+t))| = |f_c'(1/(1+t))|^n = |(-t/(1+t))|^n \to 0 \text{ as } n \to \infty.$$

If we use (5) in this last expression, then

$$\left|\frac{-B_n}{\left(\dfrac{1}{1+t} - c_{n-1}\right)^2}\right| = \frac{\left|\dfrac{1}{t} + c_{n-1}\right|}{\left|\dfrac{1}{1+t} - c_{n-1}\right|} \to 0 \text{ as } n \to \infty.$$

This shows c_n converges to $-1/t$ as $n \to \infty$.

We use this last result to argue that $\Omega = \mathbb{C}\setminus\{-(1/t)\}$. Let $\varepsilon > 0$ be given and consider $K_\varepsilon \equiv \mathbb{C}\setminus\overline{N}_\varepsilon(-(1/t))$, where the bar denotes closure. Since the sequence $\{c_n\}$ converges to $-(1/t)$, $\{A_n\}$ and $\{B_n\}$ converge respectively to $1/(1+t)$ and 0 as $n \to \infty$. So by choosing $N > 0$ such that $|c_n - (-(1/t))| < \varepsilon/2$ for $n > N$, it follows that for any $z \in K_\varepsilon$, $|z - c_n| > \varepsilon/2$ for $n > N$. From (5) and the above comments, we conclude

$$\left|f_c^n(z) - \frac{1}{1+t}\right| \text{ converges uniformly to 0 on } K_\varepsilon,$$

and so $K_\varepsilon \subseteq \Omega$. Upon letting $\varepsilon \to 0$, we see that $\Omega = \mathbb{C}\setminus\{-(1/t)\}$; consequently $0 \in \Omega$ and $\{f_c^n(0)\}$ converges.

The combination of Theorems 1 and 2 insures $\{f_c^n(0)\}$ converges if, and only if, $c \in D = \{t^2 + t\colon \mathrm{Re}(t) > -1/2\} \cup \{-1/4\}$.

We now turn our attention to the sets D_k, $k = 2,3,\ldots$. Recall, D_k is the set of real numbers c less than $-1/4$ for which the k subsequences, $\{f_c^{nk+j}(0)\}$, $j = 1,2,\ldots,k$ as $n \to \infty$, converge to distinct limits. We have the following result.

THEOREM 3. *For each $k \geq 2$, D_k is finite.*

Proof. We first show that D_2 is empty. Suppose not, and let $c \in D_2$. Then $\{f_c^{2n}(0)\}$ converges to a point w, which is a fixed point of $f_c^2(z)$. Since $c \in \mathbb{R}$, $\{f_c^{2n}(0)\} \subseteq \mathbb{R}$, and therefore, w must also be real-valued. But, upon inspection, $w = f_c^2(w)$ implies Equations (3) and (4). Thus, w has a nonzero imaginary part, which is a contradiction. Therefore, D_2 is empty.

Since $f_c^k(z)$ is a Moebius transformation, it has at most two fixed points. Now for each c in D_k, $k > 2$, $\{f_c^n(0)\}$ has k convergent subsequences $\{f_c^{nk+j}(0)\}$, $j = 1,2,\ldots,k$, each having a distinct limit. These k limits are fixed points of $f_c^k(z)$. By (ii), we must have $f_c^k(z) \equiv z$. In the case that $c \in D_3$,

$$f_c^3(z) = \cfrac{1}{1 + \cfrac{c}{1 + \cfrac{c}{1+cz}}} = z, \quad \forall z.$$

This simplifies to $(c+1)(cz^2 + z - 1) = 0$ for all z. Since the second factor cannot be 0 for all z, it follows that $c = -1$ and so $D_3 = \{-1\}$. In general, if $c \in D_k$, then $f_c^k(z) = z$ for all z. Rewriting this as $f_c(f_c^{k-1}(z)) = z$, using (5) on $f_c^{k-1}(z)$, and the expressions for A_{k-1} and B_{k-1}, one can show with a little bit of algebraic manipulation that the equation $f_c^k(z) = z$ for all z is equivalent to $-c_{k-2}(cz^2 + z - 1) = 0$ for all z, where $c_{k-2} = g_c^{k-2}(-1/c)$. This implies that $c_{k-2} = 0$. Thus, the set D_k is contained in the set of c values that make the equation $c_{k-2} = 0$ true. Since c_{k-2} is a rational function of c, there are only a finite number of solutions to this equation. So D_k is finite.

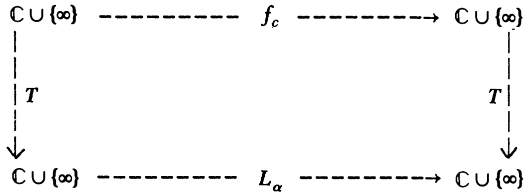


FIGURE 1

We note that if c is a root of the equation, $c_{k-2}=0$, the sequences $\{f_c^{nk+j}(0)\}$, $j=0,1,\ldots,k-1$ do not necessarily have k distinct limits.

III. Changing the setting The arguments used in Section II illustrate the power of complex analysis, but they are not very efficient. We will show how changing the setting of the problem results in a more concise proof of Theorem 2 and a more precise statement and proof of Theorem 3. In addition, we will be able to show that the union of the D_k's is dense on $(-\infty, -1/4)$. Our approach is motivated by a study of the work done by earlier mathematicians [**9**, p. 46–56] and more recently by [**3**, p. 1–48], [**5**, p. 1–60] and [**6**, p. 1–24, p. 57–74, p. 75–106].

For each $c=t^2+t$, $\mathrm{Re}(t)\geq -1/2$, $t\neq 0$, $t\neq -1/2$, $f_c(z)$ has exactly two fixed points, $1/(1+t)$ and $-(1/t)$. Let

$$T(z)=\frac{z+\dfrac{1}{t}}{z-\dfrac{1}{1+t}}. \tag{6}$$

Then,

$$T^{-1}(z)=\frac{\dfrac{1}{1+t}z+\dfrac{1}{t}}{z-1}. \tag{7}$$

Set $L_\alpha(z)=Tf_cT^{-1}(z)=\alpha z$, where $\alpha=(1+t)/-t$. FIGURE 1 displays the relationship among f_c, T, and L_α.

Note that $1/(1+t)$, $-(1/t)$, and $-(1/c)$ are mapped under $T(z)$ to the point at infinity, zero, and $-t/(1+t)$, respectively. Hence, instead of considering f_c, its iterates, and the parameter c-plane, we consider the linear map L_α, its iterates, and the parameter α-plane. We display the relationship between the two parameters in FIGURE 2. In the figure, $c=t^2+t$ is a one-to-one analytic map from $\{t\colon \mathrm{Re}(t)>-1/2\}$ onto $\mathbb{C}\backslash\{x\colon x\in\mathbb{R} \text{ and } x\leq -1/4\}$, and $\alpha=(1+t)/-t$ is a one-to-one analytic map of $\{t\colon \mathrm{Re}(t)>-1/2\}\backslash\{0\}$ onto the exterior of the unit disk. Thus, the relationship between α and c given by

$$c(\alpha)=\frac{1}{\alpha+1}\left(\frac{1}{\alpha+1}-1\right),\ |\alpha|>1,$$

is one-to-one and analytic. (Complex analysts will immediately observe that $c(\alpha)$ is the extremal function for the Bieberbach Conjecture [**8**, p. 189].) When $\mathrm{Re}(t)=-1/2$, $c=t^2+t$ maps $-1/2+iy$ and $-1/2-iy$ to $-1/4-y^2$, a point on the real line less than or equal to $-1/4$. Also, $\alpha=(1+t)/-t$ maps the line $\mathrm{Re}(t)=-1/2$ one-to-one and onto $\{|z|=1\}\backslash\{-1\}$. It follows that $c(\alpha)$ is a continuous, one-to-one map from the upper half (or lower half) of the unit circle onto the real numbers less than $-1/4$.

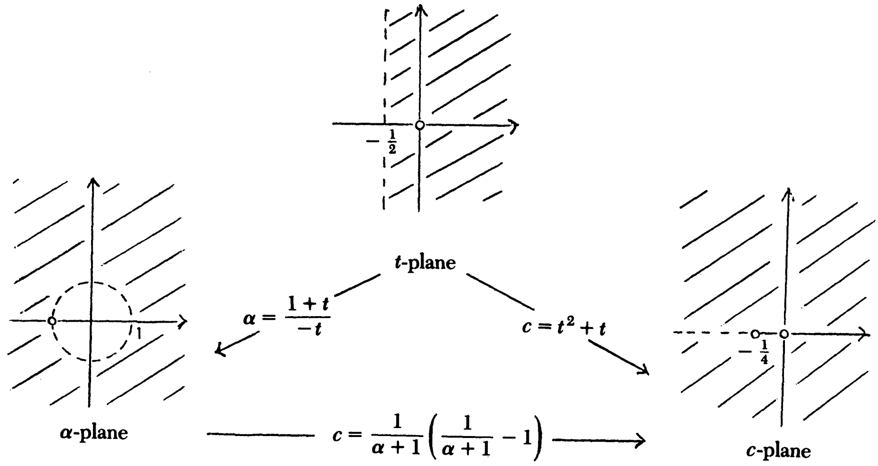


FIGURE 2

We now consider the iterates of $L_\alpha(z)$. If $c = t^2 + t$ where $\text{Re}(t) > -1/2$ and $t \neq 0$, then $|\alpha| = |(1+t)/-t| > 1$. Hence, for all $z \in \mathbb{C}\setminus\{0\}$, $L_\alpha^n(z) = \alpha^n z$ converges to the point at infinity as $n \to \infty$. Since $f_c = T^{-1}L_\alpha T$, we have for all $z \in \mathbb{C}\setminus\{-(1/t)\}$, $f_c^n(z)$ converges to $1/(1+t)$ as $n \to \infty$. Since $0 \neq -(1/t)$, the sequence $\{f_c^n(0)\}$ converges. The cases where $t = -1/2$ and $t = 0$ are handled as before. Thus, *we have a concise proof of Theorem* 2.

Recall that the singularities of $f_c^n(z)$, $n = 1, 2, \dots,$ are the iterates of $-(1/c)$ under the inverse map $g_c(z)$. Under T, this corresponds to considering the iterates of $-t/(1+t)$ under the map $L_\alpha^{-1}(z) = (1/\alpha)z$. Clearly, these iterates converge to zero, and so the iterates of $g_c^n(-(1/c))$, $n = 1, 2, \dots,$ converge to $-(1/t)$.

In the case $c = t^2 + t$ where $\text{Re}(t) = -1/2$ and $t \neq -1/2$, c is a point on the real line less than $-1/4$ and $|\alpha| = |(1+t)/-t| = 1$. We would like to determine those α on the unit disk such that $c(\alpha) \in D_k$. If $k \geq 3$, then we have $f_c^k(z) \equiv z$ as argued earlier and hence $L_\alpha^k(z) \equiv z$. Thus $\alpha^k = 1$ and so α is a kth root of unity. Under complex multiplication the kth roots of unity form a cyclic group with generator $\alpha_0 = e^{i(2\pi/k)}$, the principal kth root of unity. We denote this group by $G_k(\alpha_0)$. Using T and the definition of D_k, it follows that if $c(\alpha) \in D_k$, then the k subsequences $\{L_\alpha^{nk+j}((1+t)/-t)\}$ $j = 1, 2, \dots, k$, each have distinct limits, which respectively are $L(\alpha) = \alpha^2$, $L^2(\alpha) = \alpha^3, \dots, L^k(\alpha) = \alpha$. This implies that α must be a generator of $G_k(\alpha_0)$. We know [4, p. 71] that $\alpha = \alpha_0^s$ is a generator of $G_k(\alpha_0)$ if, and only if, $(s, k) = 1$. For a given k the number of such generators is $\varphi(k)$, where φ is the Euler totient function [4, p. 146]. Finally, we note that if α is a generator of $G_k(\alpha_0)$, then its inverse, which in this setting is the conjugate of α, is also a generator of $G_k(\alpha_0)$. Hence, there is an even number of generators of $G_k(\alpha_0)$, half of which are in the upper half-circle, the other half on the lower half-circle. We conclude that the generators of $G_k(\alpha_0)$ lying in the upper half-circle are mapped by $c(\alpha)$ one-to-one and onto D_k, and so the number of elements in D_k is given by $\varphi(k)/2$. We have a more precise proof of Theorem 3 that leads to the following result.

THEOREM 4. *The union of the D_k's is dense on* $(-\infty, -1/4)$.

Proof. Suppose $\delta > 0$ and let $\alpha = e^{i\theta}$ be any point in the upper half of the unit circle. Since the rationals are dense in $\mathbb{R}$, there exists a rational number m/k,

$(m,k)=1$, such that $(\theta-\delta)/2\pi<m/k<(\theta+\delta)/2\pi$. This implies that $e^{i(2m\pi/k)}$ lies on the arc connecting $e^{i(\theta-\delta)}$ and $e^{i(\theta+\delta)}$ taken in the counterclockwise direction. Since $e^{i(2m\pi/k)}$ is a kth root of unity and a generator of $G_k(\alpha_0)$, we have that $\bigcup_{k=3}^{\infty}\{\alpha$ such that α is a generator of $G_k(\alpha_0)\}$ is dense on the unit circle.

Now let $\varepsilon>0$ and c be such that the interval $(c-\varepsilon,c+\varepsilon)$ is contained in the interval $(-\infty,-1/4)$. Since $c(\alpha)$ is a one-to-one, continuous map of the upper half-circle onto the half-line, there exists an $\alpha=e^{i\theta}$ and $\delta>0$ such that $c(\alpha)=c$, and the arc from $e^{i(\theta-\delta)}$ to $e^{i(\theta+\delta)}$ is mapped under $c(\alpha)$ into the interval $(c-\varepsilon,c+\varepsilon)$. Since we can find on the arc a kth root of unity that is a generator of the kth roots of unity, denoted α_k, its image, $c(\alpha_k)$, is a point of D_k in the interval. Hence, our theorem is established.

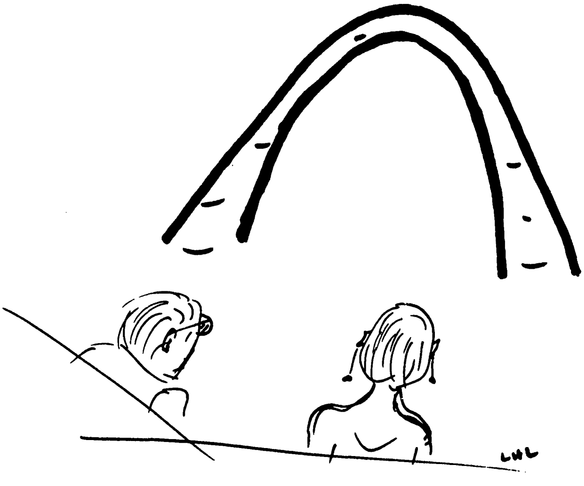
REFERENCES

1. Lars V. Ahlfors, *Complex Analysis*, 3rd edition, McGraw Hill Book Co., New York, 1979.
2. I.N. Baker and P. J. Rippon, A note on complex iteration, *Amer. Math. Monthly*, August-September, 1985, 501–504.
3. Alan F. Beardon, *Iteration of Rational Functions*, Springer-Verlag New York, 1991.
4. Elwyn H. Davis, *Introductory Modern Algebra*, Charles E. Merrill Publishing Co. / Bell and Howell Company, Columbus, OH, 1974.
5. Robert L. Devaney, *Chaotic Dynamical Systems*, 2nd edition, Addison-Wesley Publishing Co., Inc., Reading, MA, 1989.
6. Robert L. Devaney and Linda Keen, *Chaos and Fractals, The Mathematics Behind the Computer Graphics*, Proceedings of Symposia in Applied Mathematics, Volume 39, Amer. Math. Society, 1989.
7. Leonard Euler, *Introduction to Analysis of the Infinite, Book 1*, Springer-Verlag New York, 1988.
8. G. M. Goluzin, *Geometric Theory of Functions of a Complex Variable*, Translations of Mathematical Monographs, Vol. 26, Amer. Math. Society, 1969.
9. William B. Jones and W. J. Thron, Continued fractions, analytic theory and applications, *Encyclopedia of Mathematics and Its Applications*, Volume 11, Addison-Wesley Publishing Co., Reading, MA, 1980.
10. H. S. Wall, *Analytic Theory of Continued Fractions*, Chelsea Publishing Co., Bronx, NY, 1967.

Two Mathematikers at the Gateway Arch in St. Louis

"*Cosh*, it's beautiful!"

"Yessiree. 1/2 (e^u + e^{-u}), for sure!"



—LESTER H. LANGE
308 ESCALONA DRIVE
CAPITOLA, CA 95010

$(m,k)=1$, such that $(\theta-\delta)/2\pi<m/k<(\theta+\delta)/2\pi$. This implies that $e^{i(2m\pi/k)}$ lies on the arc connecting $e^{i(\theta-\delta)}$ and $e^{i(\theta+\delta)}$ taken in the counterclockwise direction. Since $e^{i(2m\pi/k)}$ is a kth root of unity and a generator of $G_k(\alpha_0)$, we have that $\bigcup_{k=3}^{\infty}\{\alpha$ such that α is a generator of $G_k(\alpha_0)\}$ is dense on the unit circle.

Now let $\varepsilon>0$ and c be such that the interval $(c-\varepsilon, c+\varepsilon)$ is contained in the interval $(-\infty,-1/4)$. Since $c(\alpha)$ is a one-to-one, continuous map of the upper half-circle onto the half-line, there exists an $\alpha=e^{i\theta}$ and $\delta>0$ such that $c(\alpha)=c$, and the arc from $e^{i(\theta-\delta)}$ to $e^{i(\theta+\delta)}$ is mapped under $c(\alpha)$ into the interval $(c-\varepsilon, c+\varepsilon)$. Since we can find on the arc a kth root of unity that is a generator of the kth roots of unity, denoted α_k, its image, $c(\alpha_k)$, is a point of D_k in the interval. Hence, our theorem is established.

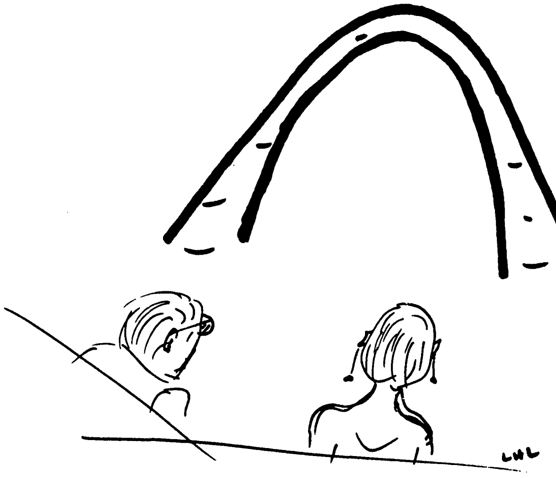
REFERENCES

1. Lars V. Ahlfors, *Complex Analysis*, 3rd edition, McGraw Hill Book Co., New York, 1979.
2. I.N. Baker and P. J. Rippon, A note on complex iteration, *Amer. Math. Monthly*, August-September, 1985, 501–504.
3. Alan F. Beardon, *Iteration of Rational Functions*, Springer-Verlag New York, 1991.
4. Elwyn H. Davis, *Introductory Modern Algebra*, Charles E. Merrill Publishing Co. / Bell and Howell Company, Columbus, OH, 1974.
5. Robert L. Devaney, *Chaotic Dynamical Systems*, 2nd edition, Addison-Wesley Publishing Co., Inc., Reading, MA, 1989.
6. Robert L. Devaney and Linda Keen, *Chaos and Fractals, The Mathematics Behind the Computer Graphics*, Proceedings of Symposia in Applied Mathematics, Volume 39, Amer. Math. Society, 1989.
7. Leonard Euler, *Introduction to Analysis of the Infinite, Book 1*, Springer-Verlag New York, 1988.
8. G. M. Goluzin, *Geometric Theory of Functions of a Complex Variable*, Translations of Mathematical Monographs, Vol. 26, Amer. Math. Society, 1969.
9. William B. Jones and W. J. Thron, Continued fractions, analytic theory and applications, *Encyclopedia of Mathematics and Its Applications*, Volume 11, Addison-Wesley Publishing Co., Reading, MA, 1980.
10. H. S. Wall, *Analytic Theory of Continued Fractions*, Chelsea Publishing Co., Bronx, NY, 1967.

Two Mathematikers at the Gateway Arch in St. Louis

"*Cosh*, it's beautiful!"

"Yessiree. 1/2 ($e^u + e^{-u}$), for sure!"



—Lester H. Lange
308 Escalona Drive
Capitola, CA 95010

The Cardinality of Sets of Functions

PIOTR ZARZYCKI
University of Gdańsk
80-952 Gdańsk, Poland

In introducing cardinal numbers and applications of the Schröder-Bernstein Theorem, we find that the determination of the cardinality of sets of functions can be quite instructive. Recall that the Schröder-Bernstein Theorem (SBT) states that *if* $n \leq m \leq n$, *then* $m = n$. The letters m and n denote cardinal numbers. We let $N = \{1, 2, \dots\}$ and Y^Y = the set of all functions from Y into itself. The cardinality of X is denoted $|X|$ and we assume that $|X| = m \geq \aleph_0$.

Problems Find the cardinality of the following sets of functions:

$$A_1 = \{f \in N^N: \ f \textit{ is not surjective}\}$$
$$A_2 = \{f \in N^N: \ f \textit{ is not injective}\}$$
$$A_3 = \{f \in N^N: \ f \textit{ is surjective}\}$$
$$A_4 = \{f \in N^N: \ f \textit{ is injective}\}$$
$$A_5 = \{f \in N^N: \ f \textit{ is bijective}\}$$
$$B_1 = \{f \in X^X: \ f \textit{ is not surjective}\}$$
$$B_2 = \{f \in X^X: \ f \textit{ is not injective}\}$$
$$B_3 = \{f \in X^X: \ f \textit{ is surjective}\}$$
$$B_4 = \{f \in X^X: \ f \textit{ is injective}\}$$
$$B_5 = \{f \in X^X: \ f \textit{ is bijective}\}$$

Solutions The proofs of $|A_1| = |A_2| = 2^{\aleph_0}$ and $|B_1| = |B_2| = 2^m$ are routine.

If $f(N) \subset N - \{1\}$, then $f \in A_1$ and $|(N - \{1\})^N| \leq |A_1| \leq |N^N|$.

If f: $N \to N$ and $f(1) = f(2)$, then $f \in A_2$, and

$$|N^{N-\{1,2\}}| \leq |A_2| \leq |N^N|.$$

Similarly one can prove that $|B_1| = |B_2| = 2^m$. Here and elsewhere we use the well-known relation for cardinal numbers (see for instance [3], chapter XVI; see also [2], exercise 4 p. 47):

$$\textit{If } m \geq \aleph_0, \textit{ then } m^m = 2^m.$$

We give the proofs of $|A_3| = |A_4| = |A_5| = 2^{\aleph_0}$ and $|B_3| = |B_4| = |B_5| = 2^m$. Actually, it follows from $A_5 \subset A_3, A_4$ and $B_5 \subset B_3, B_4$ and from SBT that it is sufficient to show that $|A_5| = 2^{\aleph_0}$ and $|B_5| = 2^m$. We give the argument for A_4 because of its cleverness. Let us notice that if $f \in N^N$, then we can identify f with the sequence $(a_1, a_2, \dots)$, where $f(i) = a_i$. To show that $|A_4| = 2^{\aleph_0}$ it is enough to produce $2^{\aleph_0}$ injective sequences $(a_1, a_2, \dots)$.

Proof 1. $|A_4| = |A_5| = 2^{\aleph_0}$

Let us take any x from the interval $(0,1)$. The element x has the decimal expansion $x = 0.a_1a_2\ldots$. To x we assign the sequence $(1a_1, 1a_1a_2, 1a_1a_2a_3, \ldots)$, where $1a_1$ is a natural number with the first digit equal to 1 and the second digit equal to a_1, and so on. The assignment $x \mapsto (1a_1, 1a_1a_2, 1a_1a_2a_3, \ldots)$ is obviously injective and $(1a_1, 1a_1a_2, 1a_1a_2a_3, \ldots) \in A_4$. If we take the assignment

$$x \mapsto (1,2,\ldots,9,1a_1,\ldots,99,1a_1a_2,\ldots,999,\ldots)$$

we get $2^{\aleph_0}$ bijective sequences from A_5. (In the group $1a_1, \ldots, 99$ there are all 2-digit numbers, in the group $1a_1a_2, \ldots, 999$—all 3-digit numbers, and so on.)

Proof 2. $|A_4| = 2^{\aleph_0}$.
The assignments

$$x = 0.a_1a_2 \cdots \mapsto (a_1+1, a_1+a_2+2, a_1+a_2+a_3+3, \ldots)$$

$$x = 0.a_1a_2 \cdots \mapsto (a_1+1, (a_1+1)(a_2+2), (a_1+1)(a_2+2)(a_3+3), \ldots)$$

are injective.

Proof 3. $|A_4| = 2^{\aleph_0}$.
To any $A \subset N$ we assign the function $f_A\colon N \to N$ defined by

$$f_A(n) = \begin{cases} 2|A \cap \{1,2,\ldots,n\}| + 2n & \text{if } n \in A, \\ 2|A \cap \{1,2,\ldots,n\}| + 2n - 1 & \text{if } n \notin A. \end{cases}$$

The assignment $A \mapsto f_A$ is injective. Obviously $f_A \in A_4$. As there are $2^{\aleph_0}$ subsets of N we get $|A_4| = 2^{\aleph_0}$.

Proof 4. $|B_5| = 2^m$.
Our method of producing many bijections $f\colon X \to X$ is nonconstructive and differs from the cases of A_4 and A_5, where we used the arithmetic structure of N.

Let $P(X)$ be a set of all subsets of X. It is well known that $|P(X)| = 2^{|X|} > |X| = m$ (Cantor's theorem). It is easy to see that if $P_0(X) = \{F \subset X\colon F \text{ is finite}\}$, then $|P_0(X)| = m$ (see [3], p. 146 or [4], exercise 14.36). Thus, if $\mathfrak{F} = \{Y \subset X\colon Y \text{ is infinite}\}$, then $|\mathfrak{F}| = 2^m$. Here we have also used an important result from the arithmetic of cardinal numbers [1, pp. 96–97], [3, chapter XVI].

If $m \geq n \geq \aleph_0$, *then* $m + n = m$.

To any $Y \in \mathfrak{F}$ we assign the function $f_Y \in B_5$ in the following way:

The set Y can be represented as a sum of two disjoint sets Y_1, Y_2 of equal cardinality (this property follows from $|Y \times N| = |Y|$) and let f_1 be any bijection from Y_1 onto Y_2.
We put

$$f_Y(x) = \begin{cases} x & \text{if } x \in X - Y, \\ f_1(x) & \text{if } x \in Y_1, \\ f_1^{-1}(x) & \text{if } x \in Y_2. \end{cases}$$

FIGURE 1 shows f_Y. The assignment $Y \mapsto f_Y$ is injective: If $Y \neq Y'$, then there exists $x \in Y - Y'$ or $x \in Y' - Y$. In the first case $f_Y(x) \neq x$, $f_{Y'}(x) = x$. In the second case $f_Y(x) = x$, $f_{Y'}(x) \neq x$. Obviously $f_Y \in B_5$.

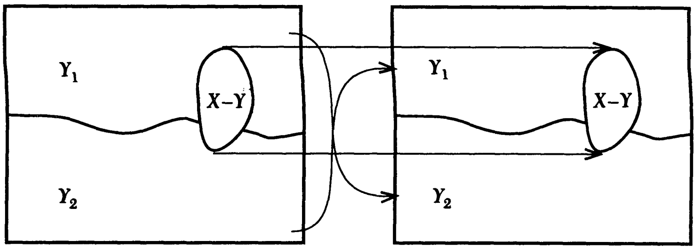


FIGURE 1

REFERENCES

1. P. Halmos, *Naive Set Theory*, Springer-Verlag New York, 1974.
2. I. Kaplansky, *Set Theory and Metric Spaces*, Allyn and Bacon, Boston, 1975.
3. W. Sierpiński, *Cardinal and Ordinal Numbers*, Państwowe Wydawnictwo Naukowe, Warszawa, 1958.
4. L. E. Sigler, *Exercises in Set Theory*, Springer-Verlag New York, 1976.

Oscillating Sawtooth Functions

FREDERICK HARTMANN
DAVID SPROWS
Villanova University
Villanova, PA 19085

Ideally every discussion of a theorem in mathematics should contain some comment about its converse. Two important theorems in elementary calculus are:

(1) If f has a derivative, then f is continuous.
(2) If f is continuous, then f is a derivative.

Most calculus books contain a number of counterexamples to the converse of (1), but the converse of (2) is usually not discussed in any detail. In this note we will consider a class of functions that can be used to supply counterexamples to the converse of (2).

One approach to developing an example of a discontinuous derivative is to first consider the function $f(x)=x^2\sin(\frac{1}{x})$ for $x\neq 0$ with $f(0)=0$. Since $-x^2\leq f(x)\leq x^2$, the derivative of f at 0 exists and is equal to 0. For $x\neq 0$, the derivative of f is given by $2x\sin(\frac{1}{x})-\cos(\frac{1}{x})$. Thus $f'(x)=g(x)-h(x)$ where $g(x)=2x\sin(\frac{1}{x})$ for $x\neq 0$ with $g(0)=0$ and $h(x)=\cos(\frac{1}{x})$ for $x\neq 0$ with $h(0)=0$. Since $g(x)$ is continuous and $h(x)$ is not continuous, it follows that $f'(x)$ is not continuous. (For another version of this approach see [1] and [2].)

In this note we will consider an alternate approach to finding counterexamples to the converse of (2) that uses "sawtooth functions." Although largely ignored by many calculus texts, "sawtooth functions" are a rich source of interesting examples. In particular, these functions can be used in a direct and elementary way to obtain examples of non-continuous derivatives.

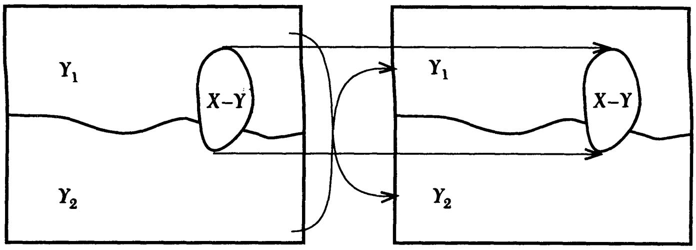


FIGURE 1

REFERENCES

1. P. Halmos, *Naive Set Theory*, Springer-Verlag New York, 1974.
2. I. Kaplansky, *Set Theory and Metric Spaces*, Allyn and Bacon, Boston, 1975.
3. W. Sierpiński, *Cardinal and Ordinal Numbers*, Państwowe Wydawnictwo Naukowe, Warszawa, 1958.
4. L. E. Sigler, *Exercises in Set Theory*, Springer-Verlag New York, 1976.

Oscillating Sawtooth Functions

FREDERICK HARTMANN
DAVID SPROWS
Villanova University
Villanova, PA 19085

Ideally every discussion of a theorem in mathematics should contain some comment about its converse. Two important theorems in elementary calculus are:

(1) If f has a derivative, then f is continuous.
(2) If f is continuous, then f is a derivative.

Most calculus books contain a number of counterexamples to the converse of (1), but the converse of (2) is usually not discussed in any detail. In this note we will consider a class of functions that can be used to supply counterexamples to the converse of (2).

One approach to developing an example of a discontinuous derivative is to first consider the function $f(x)=x^2\sin(\frac{1}{x})$ for $x\neq 0$ with $f(0)=0$. Since $-x^2\leq f(x)\leq x^2$, the derivative of f at 0 exists and is equal to 0. For $x\neq 0$, the derivative of f is given by $2x\sin(\frac{1}{x})-\cos(\frac{1}{x})$. Thus $f'(x)=g(x)-h(x)$ where $g(x)=2x\sin(\frac{1}{x})$ for $x\neq 0$ with $g(0)=0$ and $h(x)=\cos(\frac{1}{x})$ for $x\neq 0$ with $h(0)=0$. Since $g(x)$ is continuous and $h(x)$ is not continuous, it follows that $f'(x)$ is not continuous. (For another version of this approach see [1] and [2].)

In this note we will consider an alternate approach to finding counterexamples to the converse of (2) that uses "sawtooth functions." Although largely ignored by many calculus texts, "sawtooth functions" are a rich source of interesting examples. In particular, these functions can be used in a direct and elementary way to obtain examples of non-continuous derivatives.

Given a sequence $\{x_k\}$ with $x_k > x_{k+1} > 0$ for all k such that $\lim x_k = 0$, the *oscillating sawtooth function* $f(x)$ associated with $\{x_k\}$ is first defined on each subinterval $[x_{n+1}, x_n]$. The graph of f on $[x_{n+1}, x_n]$ consists of the sides of an isosceles triangle of height one. These triangles are taken to be above the x-axis if n is odd and below the x-axis if n is even. The definition of f is then extended to the entire real line by setting $f(0)=0$, $f(x)=0$ if $x > x_1$, and $f(x)=f(-x)$ if $x<0$.

In more detail, for each k, let $f(x_k)=0$ and $f(\bar{x}_k)=(-1)^{k+1}$ where $\bar{x}_k = (x_k + x_{k+1})/2$. Extend f to $(0, x_1]$ by connecting $(x_k, 0)$ to $(\bar{x}_k, (-1)^{k+1})$ and $(\bar{x}_k, (-1)^{k+1})$ to $(x_{k+1}, 0)$ by straight lines for each k. For example, if $\bar{x}_k < x < x_k$, then $f(x) = (-1)^{k+1}(1 + (x - \bar{x}_k)/(\bar{x}_k - x_k))$. Next extend f to $[0, \infty)$ by setting $f(0)=0$ and $f(x)=0$ for $x > x_1$. Finally extend f to the entire real line by setting $f(x)=f(-x)$ for $x<0$.

Example 1. To illustrate a specific example of a sawtooth function that gives a counterexample to the converse of (2), we let f denote the oscillating sawtooth function corresponding to $x_n = 1/n$. A partial picture of the graph of f is given in FIGURE 1.

If f were continuous, then by the Fundamental Theorem of Calculus an antiderivative of f would be given by $F(x) = \int_0^x f(t)\,dt$ for $x \geq 0$ and $F(x) = F(-x)$ for $x<0$. Since f is not continuous at 0, to show F is an antiderivative of f we must show that $F'(0)$ exists and $F'(0) = f(0) = 0$. By symmetry this reduces to showing that

$$\lim_{x \to 0+} \frac{F(x)}{x} = 0.$$

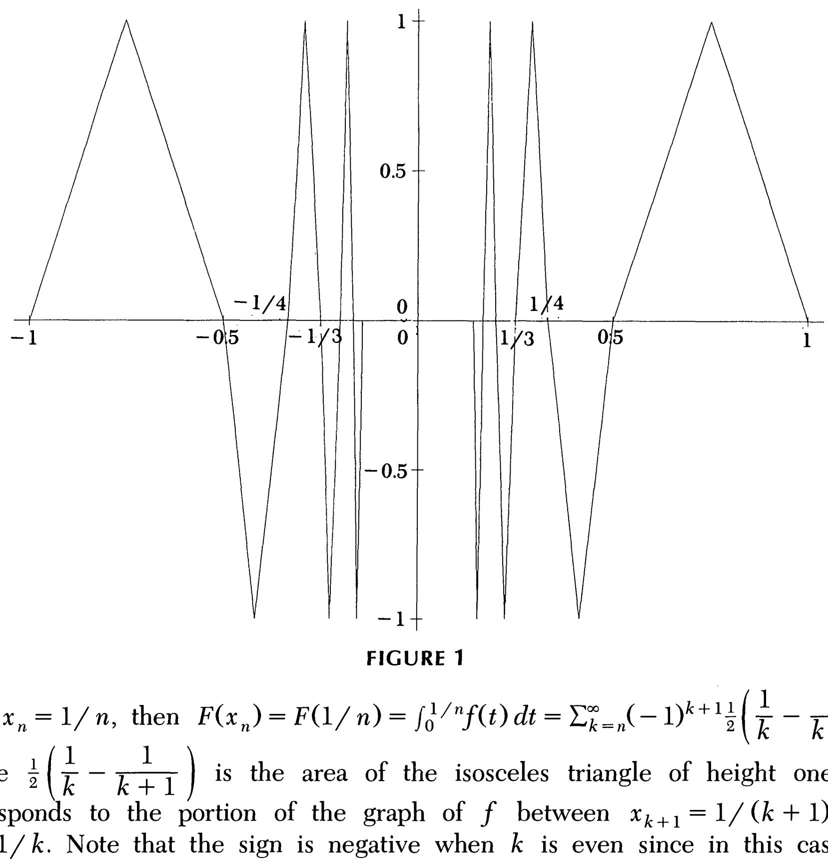


FIGURE 1

If $x_n = 1/n$, then $F(x_n) = F(1/n) = \int_0^{1/n} f(t)\,dt = \sum_{k=n}^{\infty} (-1)^{k+1} \frac{1}{2}\left(\frac{1}{k} - \frac{1}{k+1}\right)$ where $\frac{1}{2}\left(\frac{1}{k} - \frac{1}{k+1}\right)$ is the area of the isosceles triangle of height one that corresponds to the portion of the graph of f between $x_{k+1} = 1/(k+1)$, and $x_k = 1/k$. Note that the sign is negative when k is even since in this case the corresponding triangle is below the x-axis.

Since $F(1/n)$ is represented by the alternating series

$$\sum_{k=n}^{\infty}(-1)^{k+1}\frac{1}{2}\frac{1}{k(k+1)},$$

we have $|F(1/n)| \le (1/2)[1/n(n+1)]$. For arbitrary x, there are two possibilities for $F(x)$. If x is in the interval $[1/(n+1), 1/n]$ where n is odd, then $0 \le F(x) \le F(\frac{1}{n})$. If n is even, then $F(\frac{1}{n}) \le F(x) \le 0$. In either case, $|F(x)| \le |F(\frac{1}{n})|$. Since $x \ge 1/(n+1)$, we have

$$\left|\frac{F(x)}{x}\right| \le \left|\frac{F(\frac{1}{n})}{1/(n+1)}\right| \le \frac{1}{2n},$$

which implies

$$\lim_{x\to 0+}\frac{F(x)}{x} = 0.$$

Essentially the same argument as given above can be used to show that the oscillating sawtooth function corresponding to $x_n = 1/n^r$ for any $r > 0$ is a discontinuous derivative. However, not every oscillating sawtooth function can be used as a counterexample to the converse of (2) as can be seen by the following example.

Example 2. Let f be the oscillating sawtooth function corresponding to $x_n = 1/2^n$. This function does not have an antiderivative since in this case we have

$$\begin{aligned} F(x_n)/x_n &= 2^n\sum_{k=n}^{\infty}(-1)^{k+1}\frac{1}{2}\left(\frac{1}{2^k}-\frac{1}{2^{k+1}}\right) \\ &= 2^n\sum_{k=n}^{\infty}(-1)^{k+1}\frac{1}{2^{k+2}} = \frac{(-1)^{n+1}2^n}{3\cdot 2^{n+1}} = \frac{(-1)^{n+1}}{6}, \end{aligned}$$

so the limit as $n\to\infty$ does not exist. Hence $F'(0)$ does not exist.

The above examples are valuable to calculus students not only as a means of gaining insight into the Fundamental Theorem of Calculus and its converse, but also as a way of showing how basic concepts involving the integral, infinite series and the definition of the derivative can be blended together to determine the behavior of certain types of functions.

REFERENCES

1. J. Klippert, On the right-hand derivative of a certain integral function, *Amer. Math Monthly* 98 (1991), 751–752.
2. S. Ricci, Solution to proposed problem problem 1112, this MAGAZINE 55 (1982), 48.

The Generalized Fermat's Point

JINGCHENG TONG
YAP S. CHUA
University of North Florida
Jacksonville, FL 32224

In the 17th century, Fermat proposed and Torricelli solved the problem of determining a point P in a given acute triangle ABC such that the sum $PA + PB + PC$ of the distances from P to the vertices of the triangle is the minimum. The first proof was published in 1659, and the point P is called *Fermat's point* in the literature.

There is a very natural generalization of Fermat's problem. Let l, m, n be three positive real numbers. Find a point P in a given triangle ABC such that $l \cdot PA + m \cdot PB + n \cdot PC$ is a minimum. This generalization was considered in two articles in this journal [2], [3]. The method in [2] is complicated, while the method in [3] does not use synthetic geometry. In this note, using the idea in the proof of the existence of Fermat's point [1], we give a proof for the generalized case. This proof is just a slight modification of the old one.

Let us recall the proof of the existence of Fermat's point. On the sides of AB, BC, CA of triangle ABC, erect externally the equilateral triangles ABC', $A'BC$, and $AB'C$. Draw lines CC' and AA' to intersect at P. Then the point P is Fermat's point. The proof is based on the fact that a line segment is the shortest path between two points. Here is the outline of the proof in [1].

1. $\triangle ABA' \cong \triangle C'BC$, so $\measuredangle BAP = \measuredangle BC'P$.
2. Pick point D on CC' such that $C'D = AP$ and connect BD and BP.
3. $\triangle BC'D \cong \triangle BAP$. Hence $\measuredangle DBC' = \measuredangle PBA$ and $BD = BP$.
4. $\measuredangle PBD = 60^\circ$, $\triangle DBP$ is equilateral, so $DP = BP$.
5. Hence $C'C = C'D + DP + PC = PA + PB + PC$.
6. Now suppose P' is any (other) point inside $\triangle ABC$. Rotate $\triangle AP'B$ counterclockwise 60°. Then P' maps to D', $\triangle BC'D' \cong \triangle BAP'$ and $\triangle BP'D'$ is an equilateral triangle. Hence
$$P'A + P'B + P'C = C'D' + D'P' + P'C \geq C'C = PA + PB + PC.$$
7. Similarly we can prove that
$$BB' = PA + PB + PC = AA' = CC'.$$

Now we follow this same outline to give a proof of the generalized case, to find a point P in a given triangle ABC such that $l \cdot PA + m \cdot PB + n \cdot PC$ is a minimum. We first consider the case where $l \geq m + n$. Then

$$\begin{aligned} lPA + mPB + nPC &\geq m(PA + PB) + n(PA + PC) \\ &\geq mAB + nAC. \end{aligned}$$

so P must be A and we are done.

In the sequel, without loss of generality, we may require that $l < m + n$, $m < n + l$, and $n < l + m$, that is, l, m, n are the lengths of the sides of a triangle. So, on sides AB, BC, AC of triangle ABC, erect externally three directly similar triangles $BCA', BC'A, B'CA$ as in FIGURE 1 such that

$$BC : A'C : BA' = BC' : AC' : BA = B'C : AC : B'A = l : m : n.$$

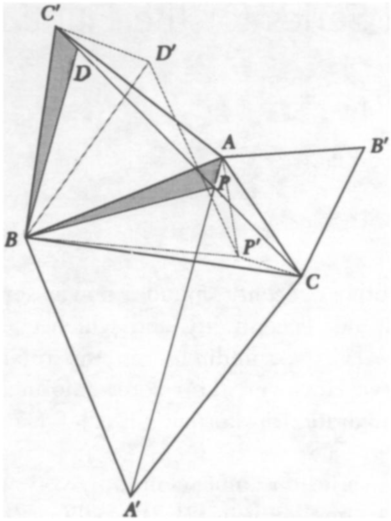


FIGURE 1

Draw CC' and AA' to intersect at P. We will show that P is the desired point, the generalized Fermat's point.

1. We have $\triangle ABA' \sim \triangle C'BC$ since $\measuredangle ABA' = \measuredangle C'BC$ and $BC : BA' = BC' : BA = l : n$. Hence $\measuredangle BAP = \measuredangle BC'P$.
2. Pick point D on CC' such that $C'D = (l/n)AP$ and connect BD and BP.
3. Now $\triangle BC'D \sim \triangle BAP$ since $\measuredangle BC'P = \measuredangle BAP$ and $BC' : BA = l/n = C'D : AP$.
4. Hence $\measuredangle DBC' = \measuredangle PBA$ and $C'D : AP = BD : BP = l/n$.
5. We have $\measuredangle PBD = \measuredangle PBA + \measuredangle ABD = \measuredangle DBC' + \measuredangle ABD = \measuredangle ABC'$ and $BD : BP = BC' : BA = l/n$, so that $\triangle PBD \sim \triangle ABC'$ and $DP : PB = m/n$. Now
$$CC' = C'D + DP + P'C = (l \cdot PA + m \cdot PB + n \cdot PC)/n$$
and
$$l \cdot PA + m \cdot PB + n \cdot PC = n \cdot CC'.$$
6. Now suppose P' is any (other) point inside $\triangle ABC$. Pick point D' so that $\measuredangle P'BD' = \measuredangle ABC'$ and $BD' : P'B = l/n$. Then $\triangle C'BD' \sim \triangle ABP'$ and $\triangle P'BD' \sim \triangle ABC'$. Now $C'D' : P'A = l/n$ and $D'P' : P'B = m/n$, so then
$$C'C \leq C'D' + D'P' + P'C = (l \cdot P'A + m \cdot P'B + n \cdot P'C)/n,$$
so that
$$l \cdot P'A + m \cdot P'B + n \cdot PC \geq n \cdot CC' = l \cdot PA + m \cdot PB + n \cdot PC,$$
and P is the sought point.
7. Similarly we can prove that $CC' : AA' : BB' = l : m : n$.

REFERENCES

1. H. S. M. Coxeter, *Introduction to Geometry*, John Wiley & Sons, Inc., New York, 1961.
2. I. Greenberg and R. A. Robertello, The three factory problem, this MAGAZINE 38 (1965), 67–72.
3. W. J. Van de Lindt, A geometrical solution of the three factory problem, this MAGAZINE 39 (1966), 162–165.

An Overlooked Series for the Elliptic Perimeter

CARL E. LINDERHOLM
ARTHUR C. SEGAL
University of Alabama at Birmingham
Birmingham, AL 35294-1170

1. Introduction The authors recently found a power series for the perimeter of an ellipse whose variable is not eccentricity and which converges considerably faster than the standard series [1]. Not finding it in the references available to us, we imagined it might be new. However, the referee informed us that we had rediscovered one of Kummer's quadratic transformations [5] of Gauss's hypergeometric series, dating back to 1837.

This "Gauss-Kummer" series does not seem to be very well known, although a very general form of it appears implicitly in [2]. We believe that in its explicit form it is highly accessible to nonspecialists and merits much wider notice than it currently receives. Section two indicates the relatively elementary route by which we arrived at it. Our proof of its validity in section three is straightforward, and independent of the original results and methods of Gauss and Kummer. Paying our respects to them, we show in section four how the series fits into the hypergeometric system.

Recall that the integral for the perimeter p of an ellipse with semiaxes $a > b$ and eccentricity ε is

$$p = 4a\int_0^{\pi/2}\sqrt{1-\varepsilon^2\cos^2 t}\,dt = 4a\int_0^{\pi/2}\sqrt{1-\varepsilon^2\sin^2 t}\,dt. \tag{1}$$

With the factor $4a$ deleted, the integral is called the complete elliptic integral of the second kind, $E(m)$, where $m = \varepsilon^2$, and is tabulated in [1, Table 17.1, p. 609].

Evaluation of (1) yields the standard series [1, Formula 17.3.12, p. 591],

$$p = 2\pi a\left[1 - \left(\frac{1}{2}\right)^2\frac{\varepsilon^2}{1} - \left(\frac{1\cdot 3}{2\cdot 4}\right)^2\frac{\varepsilon^4}{3} - \left(\frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\right)^2\frac{\varepsilon^6}{5} - \cdots\right]. \tag{2}$$

Unfortunately, for ellipses that are not very round, the standard series converges quite slowly. For example, let $a = 4/3$, $b = 2/3$; then $\varepsilon^2 = 1 - b^2/a^2 = 0.75$. Five terms of (2) give 6.48854898, which is about 0.458% greater than the actual perimeter $p \cong 6.45896548$ computed from Table 17.1 of [1].

2. Approximations We rediscovered the Gauss-Kummer series via the intuitive approximation scheme outlined here. By analogy with the radius of a circle, we define the *effective radius* of an ellipse as $r = p/2\pi$. Two natural first approximations to r are the linear (or arithmetic) mean and the quadratic (or gaussian) mean of the semiaxes:

$$r_1 = \frac{a+b}{2}, \qquad r_2 = \left(\frac{a^2+b^2}{2}\right)^{1/2}.$$

Table 1 displays their values for the previous example ($a = 4/3$, $b = 2/3$). Since r_1 underestimates r and r_2 overestimates it, we tried their linear and quadratic means:

$$r_3 = \frac{r_1+r_2}{2}, \qquad r_4 = \left(\frac{r_1^2+r_2^2}{2}\right)^{1/2}.$$

TABLE 1

$r = 1.02797628$
$r_1 = 1$
$r_2 = 1.05409255$
$r_3 = 1.02704628$
$r_4 = 1.02740233$
$r' = 1.02778514$

Unfortunately, both of these are (not bad) underestimates, so averaging them was of no help in improving the approximation.

Instead of dealing with linear and quadratic means, we next considered the 3/2 mean

$$r' = \left(\frac{a^{3/2} + b^{3/2}}{2}\right)^{2/3}$$

We see in Table 1 that r' is still an underestimate, but significantly better than the others. In fact, r' in this example is only about 0.0186% less than r. What makes r' such a good approximation?

In order to explore the 3/2 mean, we first normalized the ellipse so that $a + b = 2$. We let $a = 1 + h$ and $b = 1 - h$ ($h = 1/3$ in our previous example). Averaging the binomial expansions of $(1+h)^{3/2}$ and $(1-h)^{3/2}$, we have

$$r' = \left(1 + \frac{3}{8}h^2 + \frac{3}{128}h^4 + \frac{7}{1024}h^6 + \cdots\right)^{2/3} = 1 + c_1h^2 + c_2h^4 + c_3h^6 + \dots,$$

where c_1, c_2, c_3 are undetermined coefficients. Cubing both sides, we find $c_1 = 1/4$, $c_2 = 0$, $c_3 = 1/192$. Hence

$$r' = 1 + \frac{1}{4}h^2 + \frac{1}{192}h^6 + \dots.$$

The absence of an h^4 term in r' made us suspect that most of the (small) difference between r and r' could be accounted for by such a term; that is, $r - r' \cong k_1h^4$. Using the data of Table 1 and $h = 1/3$, we computed $k_1 \cong 1/64.59$. This was close enough to $1/64$ to lead us to conjecture that

$$r = 1 + \frac{1}{4}h^2 + \frac{1}{64}h^4 + k_2h^6 + \dots.$$

Repeating the numerical estimation, $k_2 \cong 1/245$, which is close to another perfect square, $1/256$. Our refined conjecture for the effective radius of a normalized ellipse was thus

$$r = 1 + \left(\tfrac{1}{2}\right)^2h^2 + \left(\tfrac{1}{8}\right)^2h^4 + \left(\tfrac{1}{16}\right)^2h^6 + \dots. \tag{3}$$

We then recognized these coefficients as the squares of the binomial coefficients in the expansion of $(1+x)^{1/2}$. If the fifth term of (3) follows this pattern, it would be $(5/128)^2h^8$. Again using $h = 1/3$, these five terms sum to within 10^{-8} of the r-value of Table 1. Clearly, our (then conjectured) series (3) converges *much faster* than the standard series (2). As we later learned from the referee, (3) is one of Kummer's quadratic transformations [5] of 1837, applied to series (2). See section four for details.

If we remove the normalization $a+b=2$, then for an arbitrary ellipse $h=(a-b)/(a+b)$, and therefore the (conjectured) perimeter is

$$p=\pi(a+b)\left\{1+\frac{1}{4}\left(\frac{a-b}{a+b}\right)^2+\frac{1}{64}\left(\frac{a-b}{a+b}\right)^4+\frac{1}{256}\left(\frac{a-b}{a+b}\right)^6+\frac{25}{16{,}384}\left(\frac{a-b}{a+b}\right)^8+\cdots\right\}. \tag{4}$$

3. Proof of validity We begin with the usual parametrization of an ellipse, $x=a\cos\theta$, $y=b\sin\theta$, with normalization $a=1+h$, $b=1-h$, $0<h<1$. Using symmetry,

$$\begin{aligned} p&=4\int_0^{\pi/2}\sqrt{dx^2+dy^2}=4\int_0^{\pi/2}\sqrt{a^2\sin^2\theta+b^2\cos^2\theta}\,d\theta\\ &=4\int_0^{\pi/2}\sqrt{\tfrac{1}{2}(a^2+b^2)-\tfrac{1}{2}(a^2-b^2)\cos 2\theta}\,d\theta\\ &=2\int_0^{\pi}\sqrt{1+h^2-2h\cos\phi}\,d\phi,\quad\text{where }\phi=2\theta. \end{aligned} \tag{5}$$

We now introduce the complex parameters $z=he^{i\phi}$, $\bar{z}=he^{-i\phi}$. Then $z\bar{z}=h^2$, $z+\bar{z}=2h\cos\phi$ and hence (5) becomes

$$p=2\int_0^{\pi}\sqrt{1+z\bar{z}-(z+\bar{z})}\,d\phi=2\int_0^{\pi}\sqrt{1-z}\sqrt{1-\bar{z}}\,d\phi, \tag{6}$$

where square roots are evaluated on the principal branch, which is analytic except on the negative real axis.

Note next that $|z|=|\bar{z}|=h<1$, and so the two series

$$\sqrt{1-z}=\sum_{m=0}^{\infty}\binom{\frac{1}{2}}{m}(-z)^m=\sum_{m=0}^{\infty}\binom{\frac{1}{2}}{m}(-h)^m e^{im\phi},$$

$$\sqrt{1-\bar{z}}=\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}(-\bar{z})^n=\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}(-h)^n e^{-in\phi}\quad.$$

converge absolutely and uniformly in ϕ. Accordingly, so does their product, and equation (6) becomes

$$p=2\int_0^{\pi}\sum_{m,n=0}^{\infty}\binom{\frac{1}{2}}{m}\binom{\frac{1}{2}}{n}(-h)^{m+n}e^{i(m-n)\phi}\,d\phi. \tag{7}$$

For $m\neq n$, the two terms in (7) indexed by (m,n) and (n,m) add up to $2\binom{\frac{1}{2}}{m}\binom{\frac{1}{2}}{n}(-h)^{m+n}\cos(m-n)\phi$. Recalling that $\int_0^{\pi}\cos k\phi\,d\phi=0$ for integers $k\neq 0$, we see that any such pair of terms integrates to zero. Therefore, all that remains of series (7) are the $m=n$ terms, namely

$$p=2\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}^2(-h)^{2n}\int_0^{\pi}d\phi=2\pi\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}^2h^{2n}=2\pi r, \tag{8}$$

which completes our proof of the validity of the Gauss-Kummer series (3) for the effective radius $r=p/2\pi$ of a normalized ellipse.

We remark that the series (8) even converges for $h = 1$, and to the correct value. That is, if $h = 1$, then $a = 2$, $b = 0$ and the "flattened" ellipse has obvious perimeter 8. The series

$$\sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n}^2 = \frac{4}{\pi} \tag{9}$$

is known [4, Formula 274, p. 50], and indeed, equations (8) and (9) give $p = 2\pi(4/\pi) = 8$ as desired.

4. Hypergeometric series In this section we show that the Gauss-Kummer series (3) is just one component of the large and intricate class of hypergeometric series. These are complex solutions of the hypergeometric equation that are regular at the origin [2, Chapter II]. They can be expressed as a three-parameter family

$$F[\alpha, \beta; \gamma; z] = \sum_{n=0}^{\infty} \frac{(\alpha)_n (\beta)_n}{(\gamma)_n n!} z^n,$$

where the Pochhammer symbol $(\alpha)_n$ is defined as follows: $(\alpha)_0 = 1$, and for $n = 1, 2, 3, \ldots$, $(\alpha)_n = \alpha(\alpha+1)(\alpha+2)\cdots(\alpha+n-1) = \Gamma(\alpha+n)/\Gamma(\alpha)$. Many elementary functions can be expressed in this fashion, e.g., $\tan^{-1} z = zF[\frac{1}{2}, 1; \frac{3}{2}; -z^2]$.

Examples more relevant for our purposes are

$$F\left[-\frac{1}{2}, \frac{1}{2}; 1; \varepsilon^2\right] = 1 - \frac{1}{4}\varepsilon^2 - \frac{3}{64}\varepsilon^4 - \frac{5}{256}\varepsilon^6 - \ldots, \tag{10}$$

which is recognizable as the standard series (2) for $p/2\pi a$, and

$$F\left[-\tfrac{1}{2}, -\tfrac{1}{2}; 1; h^2\right] = 1 + \frac{1}{4}h^2 + \frac{1}{64}h^4 + \frac{1}{256}h^6 + \ldots, \tag{11}$$

which is recognizable as the Gauss-Kummer series (3) for $p/2\pi$ in a normalized ellipse ($a = 1 + h$). We are about to see that the two series (10) and (11) are closely related.

In 1813 Gauss published a lengthy article on hypergeometric series [3]. In it, he included a few special quadratic transformations, i.e., those involving z^2. Expanding on the work of Gauss, Kummer published additional quadratic transformations in his long paper of 1837 [5]. The specific one that concerns us here is [2, p. 64, eq. 24]

$$F\left[\alpha, \beta; 2\beta; \frac{4z}{(1+z)^2}\right] = (1+z)^{2\alpha} F\left[\alpha, \alpha + \frac{1}{2} - \beta; \beta + \frac{1}{2}; z^2\right]. \tag{12}$$

Now recall that for a normalized ellipse,

$$\varepsilon^2 = 1 - \frac{b^2}{a^2} = 1 - \frac{(1-h)^2}{(1+h)^2} = \frac{4h}{(1+h)^2}.$$

Hence we can apply (12) with $\alpha = -1/2$ and $\beta = 1/2$ to obtain

$$F\left[-\frac{1}{2}, \frac{1}{2}; 1; \frac{4h}{(1+h)^2}\right] = (1+h)^{-1} F\left[-\frac{1}{2}, -\frac{1}{2}; 1; h^2\right]. \tag{13}$$

Therefore (13) converts (10), the standard series for $p/2\pi a$, into (11), the Gauss-Kummer series for $p/2\pi(1+h)$ in a normalized ellipse.

In closing, the authors wish to thank Michael I. Rosen of Brown University for calling our attention to (9). We had already discovered (3), (4), (8) and a very complicated proof when Professor Rosen's communication gave us a clue to the much better one presented in section three. We are also indebted to the referee for many helpful comments.

REFERENCES

1. Abramowitz, Milton and Stegun, Irene A., *Handbook of Mathematical Functions*, National Bureau of Standards, Washington, 1964.
2. Erdélyi, Arthur, et al., *Higher Transcendental Functions*, McGraw-Hill, New York, 1953.
3. Gauss, Carl Friedrich, *Disquisitiones Generales Circa Seriem Infinitam*

$$1+\left[\frac{\alpha\beta}{1\cdot\gamma}\right]x+\left[\frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot 2\cdot\gamma(\gamma+1)}\right]x^2+\left[\frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{1\cdot 2\cdot 3\cdot\gamma(\gamma+1)(\gamma+2)}\right]x^3+\text{etc.},$$

Pars Prior. Commentationes Societatis Regiae Scientiarum Gottingensis Recentiores, Vol. II, 1813.
4. Jolley, L. B. W., *Summation of Series*, Dover Publications, Inc., Mineola, NY, 1961.
5. Kummer, Ernst Eduard, Über die Hypergeometrische Reihe, *Journal für die Reine und Angewandte Mathematik* 15 (1837), 39–83 and 127–172.

Dropping Scores

STEPHEN R. SHALOM
William Paterson College
Wayne, NJ 07470

1. Introduction Making up an exam for a course I teach on Social Science Research Methods, I was trying to devise a question that would test whether students had an intuitive understanding of variance as a measure of dispersion. The question I came up with was: "An instructor tells a class that they may drop their lowest of 10 test grades. For any particular student, what will happen to the variance of his or her grades when the lowest grade is dropped?" Just before making multiple copies of the exam, however, I discovered that in fact it is *not* the case that dropping the lowest score invariably lowers the variance, even leaving aside the trivial case where all the scores are equal. This led me to investigate the impact of dropping both the highest and lowest scores simultaneously, and again I found some counter-intuitive results.

This article discusses the effect on the variance of dropping the lowest score or the lowest and the highest scores. We use the common formulas for variance:

$$\sigma^2=\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n}=\frac{\sum x_i^2}{n}-\left(\frac{\sum x_i}{n}\right)^2, \tag{1}$$

and

$$s^2=\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n-1}=\frac{\sum x_i^2}{n-1}-\frac{\left(\sum x_i\right)^2}{n(n-1)}, \tag{2}$$

where $x_1,\dots,x_n$ denote the n scores, $\bar{x}$ denotes their mean, and the sums are taken from 1 to n.

In closing, the authors wish to thank Michael I. Rosen of Brown University for calling our attention to (9). We had already discovered (3), (4), (8) and a very complicated proof when Professor Rosen's communication gave us a clue to the much better one presented in section three. We are also indebted to the referee for many helpful comments.

REFERENCES

1. Abramowitz, Milton and Stegun, Irene A., *Handbook of Mathematical Functions*, National Bureau of Standards, Washington, 1964.
2. Erdélyi, Arthur, et al., *Higher Transcendental Functions*, McGraw-Hill, New York, 1953.
3. Gauss, Carl Friedrich, *Disquisitiones Generales Circa Seriem Infinitam*

$$1+\left[\frac{\alpha\beta}{1\cdot\gamma}\right]x+\left[\frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot 2\cdot\gamma(\gamma+1)}\right]x^2+\left[\frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{1\cdot 2\cdot 3\cdot\gamma(\gamma+1)(\gamma+2)}\right]x^3+\text{etc.},$$

Pars Prior. Commentationes Societatis Regiae Scientiarum Gottingensis Recentiores, Vol. II, 1813.
4. Jolley, L. B. W., *Summation of Series*, Dover Publications, Inc., Mineola, NY, 1961.
5. Kummer, Ernst Eduard, Über die Hypergeometrische Reihe, *Journal für die Reine und Angewandte Mathematik* 15 (1837), 39–83 and 127–172.

Dropping Scores

STEPHEN R. SHALOM
William Paterson College
Wayne, NJ 07470

1. Introduction Making up an exam for a course I teach on Social Science Research Methods, I was trying to devise a question that would test whether students had an intuitive understanding of variance as a measure of dispersion. The question I came up with was: "An instructor tells a class that they may drop their lowest of 10 test grades. For any particular student, what will happen to the variance of his or her grades when the lowest grade is dropped?" Just before making multiple copies of the exam, however, I discovered that in fact it is *not* the case that dropping the lowest score invariably lowers the variance, even leaving aside the trivial case where all the scores are equal. This led me to investigate the impact of dropping both the highest and lowest scores simultaneously, and again I found some counter-intuitive results.

This article discusses the effect on the variance of dropping the lowest score or the lowest and the highest scores. We use the common formulas for variance:

$$\sigma^2=\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n}=\frac{\sum x_i^2}{n}-\left(\frac{\sum x_i}{n}\right)^2, \tag{1}$$

and

$$s^2=\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n-1}=\frac{\sum x_i^2}{n-1}-\frac{\left(\sum x_i\right)^2}{n(n-1)}, \tag{2}$$

where $x_1,\dots,x_n$ denote the n scores, $\bar{x}$ denotes their mean, and the sums are taken from 1 to n.

2. Main results *Dropping the lowest (or highest) score does not necessarily lower the variance.* Consider the set of scores {0, 1, 11}. We find that $\sigma^2 = 74/3$, and when the lowest score, 0, is dropped, $\sigma^2 = 25$.

Since adding a constant to each observation does not alter the variance, other counterexamples can readily be generated. Moreover, these same counter-examples apply if one calculates s^2. Similar counter-examples for $n > 3$ can also be found.

Of course, dropping the lowest score does not always increase the variance. The last section of this article will show the conditions under which the variance will increase, decrease, or remain unchanged.

Deleting the lowest and the highest scores simultaneously will decrease σ^2 except in two cases: (a) *when all the scores are the same, in which case the variance is zero and remains unchanged*; *and* (b) *where n is even and one-half of the scores are equal to one value and the other half equal to another value, in which case the variance is unchanged.* Assume there is some set of n scores, n > 2, such that the variance does not decrease when the highest and the lowest scores are removed. Since this property of the set will not be affected by any linear transformation on the set of scores, the problem can be simplified by subtracting the lowest score from each of the scores and then dividing all of them by the resulting highest score. (We exclude the case where all the scores are equal; when this is so, the variance will be 0 before removing the two scores and 0 after.) The new set of transformed scores will range from 0 to 1.

Let S and SS denote the sum and the sum of the squares, respectively, of all the scores. The sum and sum of the squares of all the scores excluding the highest and lowest will then be $S - 1$ and $SS - 1$, respectively. Let σ_0^2 = variance of the original data and σ_t^2 = variance of the trimmed data. When is $\sigma_0^2 \le \sigma_t^2$? We require

$$\frac{SS}{n} - \frac{S^2}{n^2} \le \frac{SS-1}{n-2} - \frac{(S-1)^2}{(n-2)^2}. \tag{3}$$

Expanding and combining terms yields

$$4(n-1)S^2 - 2n^2S + n^2(n-1) \le 2n(n-2)SS. \tag{4}$$

Since for all $i, 0 \le x_i \le 1$, it follows that $x_i^2 \le x_i$. Therefore, $SS \le S$. In fact, $SS = S$ only when $x_i^2 = x_i$ for all i, which occurs only when every x_i is equal to 0 or 1. Temporarily leaving aside this case, $SS < S$.

Therefore, $2n(n-2)SS < 2n(n-2)S$. Using this fact, the inequality in (4) becomes

$$4(n-1)S^2 - 2n^2S + n^2(n-1) < 2n(n-2)S,$$

and (recall that $n > 2$) we see that $4S^2 - 4nS + n^2 < 0$, and $(2S - n)^2 < 0$. Therefore, we have reached a contradiction, and equation (3) is false, except for the case where all the x_i's are equal to 0 or 1. In this case, since $x_i = x_i^2$ for all i, $S = SS$. Substituting into equation (4) gives $(2S - n)^2 \le 0$, and, $S = n/2$.

Therefore, $\sigma_0^2 \ge \sigma_t^2$ unless $x_1 = x_i^2$ for all i. In that case, $\sigma_t^2 \ge \sigma_0^2$ when n is even, and exactly half the scores are 0 and half are 1. Thus, if the set of scores is evenly split with only two values, then $\sigma_0^2 = \sigma_t^2$.

Deleting the lowest and highest scores simultaneously will not necessarily decrease the sample variance using formula (2), *even aside from the two special cases above.* When we use formula (2) for variance, this same proof by contradiction fails, and in fact it is rather easy to show examples for all n where dropping the highest and the lowest scores increases the variance. Consider the set of n scores (n even) where the lowest score is zero, the highest is one, half of the rest are equal to A and half equal to B, where $A+B=1$, and where $0<A<B<1$. Then, using formula (2), removing the highest and lowest score will increase the variance whenever:

$$s_0^2 = \frac{\left(\frac{n-2}{2}\right)(A^2+B^2)+1}{n-1} - \frac{\left[\left(\frac{n-2}{2}\right)+1\right]^2}{n(n-1)}$$

$$< \frac{\left(\frac{n-2}{2}\right)(A^2+B^2)}{(n-3)} - \frac{\left(\frac{n-2}{2}\right)^2}{(n-2)(n-3)} = s_t^2. \tag{5}$$

Simplifying, recalling $B=1-A$, and solving for A taking only the smaller root since $A<B$), yields:

$$A < \frac{n-2-\sqrt{(n-2)(n-3)}}{2(n-2)}.$$

Thus for any n, we can choose an A sufficiently small to satisfy equation (5). For $n=4$, for example, A must be less than .1464 and the set of scores $(0,.1,.9,1)$ will have its sample variance, s^2, increased from .27 to .32 when the high and low scores are removed. Likewise, for odd $n \geq 5$, we can take the set of scores where there are single scores equal to zero, one, and .5; half of the rest are equal to A and half equal to B, where $A+B=1$, and where $0<A<B<1$. This time, as long as we choose an A less than

$$\frac{2(n-2)-\sqrt{2(3n-13)(n-2)}}{4(n-2)},$$

removing the highest and lowest scores will increase s^2.

3. Characterizing the impact of excluding one extreme observation In this section, we will characterize the nature of the change in variance when an extreme observation is deleted.

Consider a set of n scores $x_1,\dots,x_n$; $x_1 \leq x_2 \leq \cdots \leq x_n$. Transform the scores by subtracting the score to be removed from all the other scores. If zero is the highest score, multiply all the scores by -1. Now zero is the score to be removed and all other scores are greater than or equal to zero. Write the transformed scores $y_1, y_2, \dots, y_n$. Let

$$S' = \sum_{i=1}^{n} y_i = \sum_{i=2}^{n} y_i \quad \text{and} \quad (SS)' = \sum_{i=1}^{n} y_i^2 = \sum_{i=2}^{n} y_i^2.$$

Removing the lowest score will *increase* the variance σ^2 whenever:

$$\sigma_0^2 = \frac{(SS)'}{n} - \frac{(S')^2}{n^2} < \frac{(SS)'}{n-1} - \frac{(S')^2}{(n-1)^2} = \sigma_t^2.$$

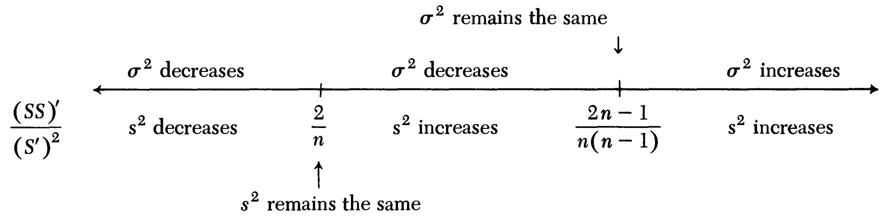
Expanding and combining terms reveals that the variance σ^2 increases if

$$\frac{(SS)'}{(S')^2} > \frac{2n-1}{n(n-1)} = \frac{2}{n} + \frac{1}{n(n-1)} > \frac{2}{n}.$$

Removing the lowest score will increase the sample variance s^2 whenever the following relationship holds:

$$s_0^2 = \frac{(SS)'}{(n-1)} - \frac{(S')^2}{n(n-1)} < \frac{(SS)'}{n-2} - \frac{(S')^2}{(n-2)(n-3)} = s_t^2.$$

Expanding and combining terms gives: $\frac{(SS)'}{(S')^2} > \frac{2}{n}$. The effect on the variance of removing the lowest score is illustrated in the following chart, where the axis represents the value of $(SS)'/(S')^2$:



Acknowledgement. The author thanks Eswar G. Phadia for helpful comments.

REFERENCES

1. David, H. A. General bounds and inequalities in order statistics, *Comm. Statist.-Theory Meth.* 17 (1988), 2119–2134.
2. Groeneveld, R. A. Best bounds for order statistics and their expectations in range and mean units with applications, *Comm. Statist.-Theory Meth.* 11 (1982), 1809–1815.

PROBLEMS

LOREN C. LARSON, *editor*
St. Olaf College

GEORGE T. GILBERT, *associate editor*
Texas Christian University

Proposals

To be considered for publication, solutions should be received by November 1, 1995.

1474. *Proposed by G. A. Edgar, The Ohio State University, Columbus, Ohio.*

Consider triangle ABC with sides lengths $a = BC$, $b = AC$, and $c = AB$. Suppose r, r', and r'' are positive numbers satisfying

$$r' \leq a, \qquad r'' \leq b \leq r'' + r, \qquad r' \leq c \leq r' + r,$$
$$r' \geq 2r, \qquad r'' \geq 2r, \qquad r'' \leq \tfrac{4}{3}r'.$$

What is the least possible measure of angle A?

1475. *Proposed by Peter J. Ferraro, Roselle Park, New Jersey.*

Show that

$$\lfloor\sqrt{\alpha}\rfloor + \lfloor\sqrt{\beta}\rfloor + \lfloor\sqrt{\alpha+\beta}\rfloor \geq \lfloor\sqrt{2\alpha}\rfloor + \lfloor\sqrt{2\beta}\rfloor$$

for all real numbers α and β, $\alpha \geq 1$ and $\beta \geq 1$. ($\lfloor x\rfloor$ denotes the greatest integer not exceeding x.)

1476. *Proposed by Hugh Thurston, University of British Columbia, Vancouver, British Columbia, Canada.*

Is there a curve and a point P on the curve such that as Q approaches P on the curve, the limit

$$\lim_{Q\to P}\left(\frac{\text{arc } PQ}{\text{chord } PQ}\right)$$

exists but does not equal 1?

1477. *Proposed by Wu Wei Chao, He Nan Normal University, Xin Xiang City, Ne Nan Province, China.*

Show that $\dfrac{1+\sqrt{1-x}}{2x} < \cot x$ for all x in the open interval $(0,1)$.

ASSISTANT EDITORS: CLIFTON CORZAT, BRUCE HANSON, RICHARD KLEBER, KAY SMITH, *and* THEODORE VESSEY, *St. Olaf College and* MARK KRUSEMEYER, *Carleton College. We invite readers to submit problems believed to be new and appealing to students and teachers of advanced undergraduate mathematics. Proposals should be accompanied by solutions, if at all possible, and by any other information that will assist the editors and referees. A problem submitted as a Quickie should have an unexpected, succinct solution. An asterisk (*) next to a problem number indicates that neither the proposer nor the editors supplied a solution.*

Solutions should be written in a style appropriate for Mathematics Magazine. Each solution should begin on a separate sheet containing the solver's name and full address.

Solutions and new proposals should be sent to George T. Gilbert, Problems Editor, Department of Mathematics, Box 32903, Texas Christian University, Fort Worth, TX 76129 or mailed electronically to g.gilbert@tcu.edu. Electronic submission of TeX input files is acceptable. Readers who use e-mail should also provide an e-mail address.

1478. *Proposed by Piotr Zarzycki, University of Gdańsk, Gdańsk, Poland.*

Let $C[0,1]$ denote the ring of continuous real-valued functions on the closed interval $[0,1]$. Is the set $I = \{f \in C[0,1]\colon f(0)=0 \text{ and } f'_+(0)=0\}$ a countably generated ideal of $C[0,1]$?

Quickies

Answers to the Quickies are on page 231.

Q835. *Proposed by Erwin Just (Emeritus), Bronx Community College, New York, New York.*

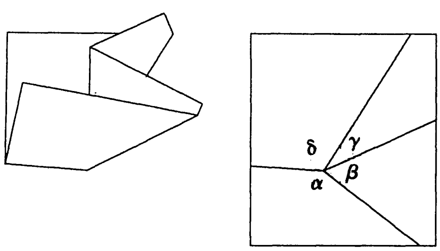
Find all positive integer solutions to $(x+2)^n - x^n = 3^n + 5^n$?

Q836. *Proposed by George Mackiw, Loyola College in Maryland, Baltimore, Maryland.*

Suppose O is a real orthogonal matrix whose eigenvalues include neither 1 nor -1. Replace all the entries of any single row of O by their negatives. Show that the resulting orthogonal matrix has both 1 and -1 as eigenvalues.

Q837. *Proposed by Scott Coble, Gonzaga University, Spokane, Washington.*

A banquet problem: A sheet of paper is folded flat in such a way that when the paper is unfolded, the creases form four rays with a common endpoint. Given the measures of any two adjacent angles formed by these rays, find the measures of the other two.



Solutions

A Linear Congruence Equation **June 1994**

1448. *Proposed by Daniel P. Moore, Alexander Consulting Group, Chicago, Illinois.*

Let $q_1, q_2, \ldots, q_n$ be odd integers, $n \geq 2$. Prove or disprove the following. There are integers $d_1, d_2, \ldots, d_n$, each equal to 0, 1, or -1, but not all zero, such that

$$\sum_{i=1}^{n} d_i q_i \equiv 0 \pmod{2^n}.$$

Solution by Thomas Jager, Calvin College, Grand Rapids, Michigan.

More generally, there is a solution $d_1, \ldots, d_n$ unless the q_i's are distinct $(\bmod 2^n)$ and exactly one of the q_i's is odd.

We proceed by induction on n, the case $n=2$ following easily. Assume the claim for $n-1$ elements. Clearly, a solution exists if the q_i's are not distinct. Suppose the q_i's are distinct and no solution of d_i's exists. In what follows all calculations are assumed to be taken modulo 2^n.

For each set P of q_i's, let ΣP be the sum of the q_i's in P. Suppose $P_1 \neq P_2$. Then if $\Sigma P_1 \equiv \Sigma P_2$, we get a solution by taking $d=+1$ for q_i's in $P_1-(P_1 \cap P_2)$, $d=-1$ for q_i's in $P_2-(P_1 \cap P_2)$, and $d=0$ for the remaining q_i's. Hence $P_1 \neq P_2$ implies $\Sigma P_1 \neq \Sigma P_2$, and since there are 2^n sets of q_i's, each value in $\mathbf{Z}_{2^n}$ is a sum ΣP for exactly one set P. Because $\mathbf{Z}_{2^n}$ contains odd values, at least one q_i, say $q=q_1$, is odd.

Let $S_q=\{\Sigma P: q \in P\}$ and $S'_q=\{\Sigma P: q \notin P\}$. Then S_q and S'_q partition $\mathbf{Z}_{2^n}$. Clearly, $S'_q+q=S_q$. Further, since S_q and S'_q are disjoint, S_q+q and S_q are disjoint, so that $S_q+q=S'_q$. Hence $S_q+2q=S_q$. It follows that all the members of S_q are odd and all the members of S'_q are even. Apply the inductive hypothesis to the set $\frac{1}{2}S'_q$ to prove the claim for n and complete the solution.

Since each non-negative integer has a unique binary representation, $\{1,2,4,\ldots,2^{n-1}\}$ is a set with exactly one odd value for which no solution of d's exists.

Also solved by Paul R. Abad, The Aetna Dungeon Group, Armstrong State College Problem Group, Con Amore Problem Group (Denmark), Gregory T. Lee (Canada), O. P. Lossers (The Netherlands), Michael Reid, John S. Sumner and Keven L. Dove, Van Ha Vu, and the WMC Problems Group.

An Infinite Product for e **June 1994**

1449. *Proposed by Paul Bracken, University of Waterloo, Waterloo, Ontario, Canada.*

Let $a_1=1$, and $a_n=n(a_{n-1}+1)$ for $n>1$. Compute the product

$$\prod_{n=1}^{\infty}\left(1+a_n^{-1}\right).$$

Solution by Chris Hill, student, University of Illinois at Urbana-Champaign, Champaign, Illinois.

Let P_N denote the Nth partial product of the given infinite product, and write the recurrence relation in the form

$$\frac{a_n+1}{n+1}=a_n+1, \qquad n \geqslant 1. \tag{1}$$

Then

$$P_N=\prod_{n=1}^{N}\frac{a_n+1}{a_n}=\prod_{n=1}^{N}\frac{a_{n+1}}{(n+1)a_n}=\frac{a_{N+1}}{(N+1)!}, \qquad N \geq 1. \tag{2}$$

Replacing n by N in (1) and dividing by $N!$, and then using (2), we find that

$$P_N=P_{N-1}+\frac{1}{N!}, \qquad N \geq 2.$$

Thus, $P_N-P_{N-1}=1/N!$ for $N \geq 2$, and since $P_1=2$ we have

$$\begin{aligned} P_N &= (P_N-P_{N-1})+(P_{N-1}-P_{N-2})+\cdots+(P_2-P_1)+P_1 \\ &= \frac{1}{N!}+\frac{1}{(N-1)!}+\cdots+\frac{1}{2!}+\frac{1}{1!}+\frac{1}{0!}, \qquad N \geq 1. \end{aligned}$$

Thus,

$$\lim_{N \to \infty} P_N=\sum_{n=0}^{\infty}\frac{1}{n!}=e.$$

Also solved by Paul R. Abad, Casey Abell, The Aetna Dungeon Group, Robert A. Agnew, Anchorage Math Solutions Group, John Andraos and Don Mills (Canada), Michael H. Andreoli, Armstrong State College Problem Group, Philipp Batchelor (Switzerland), Rich Bauer, J. C. Binz (Switzerland), T. Biyikoglu (student, Austria), Stanford Bonan, Stan Byrd, Michael P. Chernesky, John Christopher, Jay H. Chyung, Sally Cockburn, Con Amore Problem Group (Denmark), Charles K. Cook, Bill Correll, Jr. (student), Ernie Croot (student), David Doster, Robert L. Doucette, Steve Edwards, Mordechai Falkowitz (Israel), J. S. Frame, Zachary Franco, Robert Geretschläger (Austria), Michael Golomb, Joseph F. Grimland, Jr. and Samuel R. Glidewell, Richard Heeg, Francis M. Henderson, Laurent Hodges, Richard Holzsager, R. Daniel Hurwitz, Theodore Hwa, Paul Irwin, Thomas Jager, Alexander Kain, Hans Kappus (Switzerland), Murray S. Klamkin, Emil F. Knapp, Pavlos B. Konstadinidis (student), Kee-Wai Lau (Hong Kong), Detlef Laugwitz (Germany), Kwok-Shing Leung, Carl Libis, Peter A. Lindstrom, Nick Lord (England), O. P. Lossers (The Netherlands), Sergey Lototsky (student), David E. Manes, Jerry Maples (student), Mathers of Invention, Janice A. Meegan, Gary Miller (Canada), Can A. Minh (student), William A. Newcomb, Stephen Noltie, Cornel G. Ormsby, Jeremy Ottenstein (Israel), P. J. Pedler (Australia), J. L. Pietenpol, Michael Reid, F. C. Rembis, Jeffrey Schwartz and Andrea Shoff and Jennifer Young (students), Allen J. Schwenk, Heinz-Jürgen Seiffert (Germany), The Shreveport Problem Group, Nicholas C. Singer, John S. Sumner, Nora S. Thornber, Michael Vowe (Switzerland), Van Ha Vu, Robert J. Wagner, Harry Weingarten, Doug Wilcock, WMC Problems Group, Yongzhi Yang and Peter J. Costa, Ki Jun Yi and Byoung Soo Kim (Korea), Harald Ziehms (Germany), and the proposer. There were one unsigned solution and two incorrect solutions.

Pietenpol pointed out that this infinite product for e has probably been known for a long time; he had discovered it some 35 years ago, and published it as Problem E1330 in the August–September 1958 issue of the *American Mathematical Monthly*. The solution appears in the March 1959 issue (Vol. 66, No. 3, p. 237). *Laugwitz* showed that if $a_1 = 1/a > 0$, then the infinite product is equal to e^a.

A Characterization of Even Permutations **June 1994**

1450. *Proposed by John O. Kiltinen, Northern Michigan University, Marquette, Michigan.*

Which permutations in S_n, the group of all permutations on the set $\{1, 2, \dots, n\}$, can be expressed as a product of two n-cycles?

Solution by Fred Galvin, University of Kansas, Lawrence, Kansas.

The answer is "the even ones." In fact, we show that (i) every even permutation in S_n is the product of two n-cycles, and (ii) every odd permutation in S_n is the product of an n-cycle and an $(n-1)$-cycle. (The converse statements are trivial.)

We prove (i) by induction on n. The cases $n=1$ and $n=2$ are trivial. Suppose $n>2$, and let π be an even permutation of $\{1, \dots, n\}$. Without loss of generality, we may assume that $\pi(1) \neq n$; let $x = \pi(1)$ and let $\pi' = (1, n)\pi(x, n)$ (composition of permutations is from left to right). Then π' is an even permutation leaving n fixed. By the induction hypothesis, $\pi' = \alpha\beta$ where α and β are $(n-1)$-cycles leaving n fixed. Then $\pi = (1, n)\alpha\beta(x, n)$ where $(1, n)\alpha$ and $\beta(x, n)$ are n-cycles.

For the proof of (ii), let π be an odd permutation of $\{1, \dots, n\}$. Without loss of generality, we may assume that $\pi(1) = n$. Then $\pi' = (1, n)\pi$ is an even permutation leaving n fixed. By (i) we have $\pi' = \alpha\beta$ where α and β are $(n-1)$-cycles leaving n fixed. Then $\pi = (1, n)\alpha\beta$ where $(1, n)\alpha$ is an n-cycle and β is an $(n-1)$-cycle.

Also solved by The Aetna Dungeon Group, Anchorage Math Solutions Group, Pralay Chatterjee and V. Kannan (India), D. K. Cohoon, Con Amore Problem Group (Denmark), Thomas Jager, Carlton Kellogg, David E. Manes, Allen J. Schwenk, WMC Problems Group, and the proposer.

Kellogg notes that this result is in an article by D. W. Walkup, "How many ways can a permutation be factored into 2 n-cycles?", *Discrete Mathematics*, Vol. 28, 1979, 315–319.

A Functional Equation **June 1994**

1451. *Proposed by Barry Cipra, Northfield, Minnesota.*

Let f be an entire function such that $f(z) + f(z+1) = f(2z)$ and $f(0) = 0$. Prove that f is identically zero.

I. *Solution by A. R. Sourour, University of Victoria, Victoria, British Columbia, Canada.*

Upon taking derivatives, we get $2f'(2z) = f'(z) + f'(z+1)$, and hence $|f'(2z)| \leq \max\{|f'(z)|, |f'(z+1)|\}$. Now if D is any closed disk with center at 0 and radius at least 4, then the last inequality implies that the maximum of $|f'|$ on D is assumed at a point in the interior of D, since if $2z$ is on the boundary, then z and $z+1$ are both in the interior. By the maximum modulus principle, f' is a constant on D. Since this is true for every such disk, f' is a constant function, and hence $f(z) = az + b$, for constants a and b. It is easily seen that this satisfies the given functional equation if, and only if, $a = -b$, that is, $f(z) = f(0)(1-z)$.

II. *Solution by Rudolf Rupp, Universität Karlsruhe, Mathematisches Institut I, Karlsruhe, Germany.*

Differentiating the identity twice shows that

$$f''(z) + f''(z+1) = 4f''(2z).$$

In the closed unit disk $\{|z| \leq 1\}$ this implies $4M \leq 2M$, where we have set $M = \max\{|f''(z)|: |z| \leq 2\}$. Since $M \geq 0$, we must have $M = 0$; that is, f'' vanishes identically. Thus, $f(z) = az$. Inserting this into the original equation proves that f must vanish identically.

Comment. This method of proof is known as the "trick of Herglotz" (see Reinheld Remmert, *Theory of Complex Functions*, Springer-Verlag New York, 1989, p. 328.)

Also solved by Seung-Jin Bang (Korea), Soon-Yeong Chung (Korea), John Cobb, Con Amore Problem Group (Denmark), Robert L. Doucette, Mordechai Falkowitz (Israel), Zachary Franco, Michael Golomb, Chris Hill (student), Michael Hoffman and Richard Katz, Richard Holzsager, L. Huang, Thomas Jager, Kee-Wai Lau (Hong Kong), Detlef Laugwitz (Germany), Nick Lord (England), O. P. Lossers (The Netherlands), Arijit Mahalanabis, José Humberto Ferreira Rosa, Van Ha Vu, and the proposer.

Golomb and *Rupp* show that the same result holds when the hypothesis that f is an entire function is replaced by f is analytic in the disk $D = \{z \in \mathbf{C}: |z| \leq 2\}$. *Hoffman and Katz* prove the following proposition: Suppose c, a, and λ are in $\mathbf{C}$ with $|c| > 1$, and $f: \mathbf{C} \to \mathbf{C}$ is an entire function satisfying the functional equation $f(cz) = \lambda f(z) + f(z+a)$ for all $z \in \mathbf{C}$. If there is a nonnegative integer d such that $c^d = 1 + \lambda$, then there is a unique monic polynomial of degree d that satisfies the given functional equation, and all other entire solutions are scalar multiples of this polynomial. If there is no such d, then f must be identically 0.

Concurrent Lines in a Triangle **June 1994**

1452. *Proposed by John Frohliger and Adam Zeuske (student), St. Norbert College, DePere, Wisconsin.*

Let ABC be a given triangle and θ an angle between $-90°$ and $90°$. Let A', B', C' be points on the perpendicular bisectors of BC, CA, and AB, respectively, so that $\angle BCA'$, $\angle CAB'$, and $\angle ABC'$ all have measure θ. Prove that the lines AA', BB', and CC' are concurrent, provided that points A', B', C' are not equal to A, B, C, respectively.

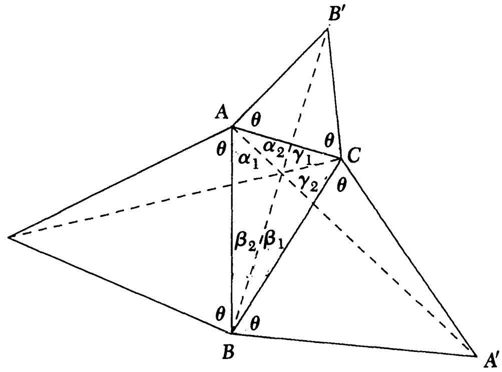
I. *Solution by Michael Vowe, Therwil, Switzerland.*

From the figure (for $\theta \neq \pm 90°$) and the law of sines, we obtain

$$\frac{\sin\alpha_1}{A'B} = \frac{\sin(\beta+\theta)}{AA'}, \qquad \frac{\sin\alpha_2}{A'C} = \frac{\sin(\gamma+\theta)}{AA'},$$

and hence

$$\frac{\sin\alpha_1}{\sin\alpha_2} = \frac{\sin(\beta+\theta)}{\sin(\gamma+\theta)}.$$



In the same manner we have,

$$\frac{\sin\alpha_1}{\sin\alpha_2}\frac{\sin\beta_1}{\sin\beta_2}\frac{\sin\gamma_1}{\sin\gamma_2}=\frac{\sin(\beta+\theta)}{\sin(\gamma+\theta)}\frac{\sin(\gamma+\theta)}{\sin(\alpha+\theta)}\frac{\sin(\alpha+\theta)}{\sin(\beta+\theta)}=1,$$

and the converse of Ceva's theorem (in trigonometric form) proves that the three lines AA', BB', and CC' are concurrent.

II. *Solution by Murray S. Klamkin, University of Alberta, Edmonton, Alberta, Canada.*
Since $BA' = CA' = \frac{1}{2}a\sec\theta$, it follows that the areal coordinates of A' are

$$\tfrac{1}{4}\big(a^2\tan\theta, ab\sec\theta\sin(C-\theta), ac\sec\theta\sin(B-\theta)\big).$$

If $\mathbf{V}$ denotes a vector from a given origin to a point V, then the vector representation of A' is given by

$$\mathbf{A}' = \tfrac{1}{4}\big(\mathbf{A}a^2\tan\theta + \mathbf{B}ab\sec\theta\sin(C-\theta) + \mathbf{C}ac\sec\theta\sin(B-\theta)\big).$$

It now follows that the line AA' intersects BC in a point A'' such that

$$\frac{BA''}{A''C}=\frac{c\sin(B-\theta)}{b\sin(C-\theta)}$$

and similarly for the other two lines (by cyclic interchange). Then since

$$\frac{c\sin(B-\theta)}{b\sin(C-\theta)}\frac{a\sin(C-\theta)}{c\sin(A-\theta)}\frac{b\sin(A-\theta)}{a\sin(B-\theta)}=1,$$

it follows by Ceva's theorem that the lines AA', BB', and CC' are concurrent, provided the points A', B', C' are not equal to A, B, C, respectively.

The two angles of θ that must be excluded are $-90°$ and $90°$.

III. *Solution by the Anchorage Math Solutions Group, University of Alaska, Anchorage, Alaska.*

In trilinear coordinates, the lines AA', BB', and CC' are given by

$$\begin{aligned}
&& \sin(B-\theta)\beta - \sin(C-\theta)\gamma &= 0\\
-\sin(A-\theta)\alpha && + \sin(C-\theta)\gamma &= 0\\
\sin(A-\theta)\alpha & - \sin(B-\theta)\beta && = 0
\end{aligned}$$

so the condition for concurrence of these lines is that

$$\det\begin{pmatrix} 0 & \sin(B-\theta) & -\sin(C-\theta) \\ -\sin(A-\theta) & 0 & \sin(C-\theta) \\ \sin(A-\theta) & -\sin(B-\theta) & 0 \end{pmatrix} = 0.$$

Concurrence at an ideal point is Euclidean parallelism in the exceptional cases.

Also solved by Con Amore Problem Group (Denmark), Milton P. Eisner, H. Skelter, and the proposer.

Convexity in Towers of Powers **June 1994**

1453*. *Proposed by Murray S. Klamkin, University of Alberta, Edmonton, Alberta, Canada.*

Let $E_{n+1} = x^{E_n}$ where $E_0 = 1$, $n = 0, 1, \ldots$, and $x \geq 0$ ($E_1 = x$, $E_2 = x^x$, etc.). It is easy to show that for $x \geq 1$, E_n ($n \geq 1$) is a strictly increasing convex function. Prove or disprove each of the following.

(i) E_{2n} is a unimodal convex function for $n > 1$ and all $x \geqslant 0$.

(ii) E_{2n+1} is an increasing function for $x \geq 0$, and is concave in a small enough interval $[0, \varepsilon(n)]$.

Composite analysis by Richard Holzsager, The American University, Washington, DC, and George Gilbert, Texas Christian University, Fort Worth, Texas.

Neither statement gives the correct concavity. For instance, one can set up a recursion and let the computer calculate that $E''_{10}(.02) \approx -15.5$. Also, a straightforward calculation shows that $\lim_{x \to 0^+} E''_3(x) = \infty$, so that E_3 cannot be concave in any interval containing 0.

In fact, the function E_n is convex in some interval of the form $[0, \varepsilon_n)$ for $n > 1$. To see this, call a function f "small of order r" near 0 if, for any $\delta > 0$, $f(x)/x^{r-\delta} \to 0$ as $x \to 0^+$. Note that $x^r \ln^k x$ is small of order r for all k. Let κ_r stand for any function that is small of order r. The convexity follows once we establish that, for $n \geq 1$,

$$E_{2n} = 1 + x\ln x + \kappa_2, \qquad E'_{2n} = \ln x + 1 + \kappa_1, \qquad E''_{2n} = 1/x + \kappa_0, \tag{1}$$

$$E_{2n+1} = x + x^2\ln^2 x + \kappa_3, \qquad E'_{2n+1} = 1 + 2x\left(\ln^2 x + \ln x\right) + \kappa_2$$

$$E''_{2n+1} = 2\left(\ln^2 x + 3\ln x + 1\right) + \kappa_1. \tag{2}$$

From $E_{n+1} = x^{E_n}$, we find that

$$E'_{n+1} = E_{n+1}\left(\frac{E_n}{x} + E'_n \ln x\right)$$

and

$$E''_{n+1} = E_{n+1}\left(\frac{E_n^2}{x^2} + \frac{2E_nE'_n\ln x}{x} + E_n'^2\ln^2 x - \frac{E_n}{x^2} + \frac{2E'_n}{x} + E''_n \ln x\right).$$

It is easy to show that these formulas hold for $n = 1$. Furthermore, one finds that $(1)_n$ implies $(2)_n$, and $(2)_n$ implies $(1)_{n+1}$, so, by induction, (1) and (2) hold for all $n \geq 1$. This completes the proof of our claim.

Finally, we show that E_{2n+1} is increasing for $x \geq 0$. We need only consider $0 < x < 1$. For such x's, $a < b$ implies $x^b < x^a$, and applying this repeatedly, we see that, for $0 < x < 1$,

$$x = E_1 < E_3 < \cdots < E_{2n+1} < \cdots < E_{2n} < \cdots < E_2 < E_0 = 1.$$

Repeated application of the recurrence $E_n' = E_n(E_{n-1}/x + E_{n-1}' \ln x)$, yields

$$E_n' = \frac{E_n E_{n-1}}{x}\left(1 + E_{n-2} \ln x + E_{n-2}E_{n-3} \ln^2 x + \cdots + E_{n-2}E_{n-3} \cdots E_0 \ln^{n-1} x\right).$$

For a given x in $(0,1)$,

$$E_{2n+1}' = \frac{E_{2n+1}E_{2n}}{x}\big[(1 + E_{2n-1}\ln x) + E_{2n-1}E_{2n-2}\ln^2 x(1 + E_{2n-3}\ln x) + \cdots$$
$$+ E_{2n-1} \cdots E_2 \ln^{2n-2} x(1 + E_1 \ln x) + E_{2n-1} \cdots E_0 \ln^{2n} x\big]$$

is positive unless $1 + E_{2j+1} \ln x < 0$ for some j. However, in this case $1 + E_{2k} \ln x < 0$ for all k, hence rearranging

$$E_{2n+1}' = \frac{E_{2n+1}E_{2n}}{x}\big[1 + E_{2n-1}\ln x(1 + E_{2n-2}\ln x)$$
$$+ \cdots + E_{2n-1} \cdots E_1 \ln^{2n-1} x(1 + E_0 \ln x)\big],$$

we see that each summand is positive, proving that E_{2n+1} is increasing.

The second step of iterating the recurrence yields

$$E_{2n+2}' = E_{2n+2}E_{2n+1}\left[\frac{(1 + E_{2n}\ln x)}{x} + E_{2n}' \ln^2 x\right].$$

Note that $x^x > 1/e$ and the $x^{x^{1/e}}$ decreases on $(0, e^{-e})$. If $E_{2n} > 1/e$ on $(0, e^{-e})$, then also

$$E_{2n+2} > x^{x^{E_{2n}}} > x^{x^{1/e}} > \left(e^{-e}\right)^{(e^{-e})^{1/e}} = \frac{1}{e}.$$

It follows that $1 + E_{2n} \ln x < 0$ on $(0, e^{-e})$, hence that $E_{2n}' < 0$ on $(0, e^{-e})$ for all $n \geq 1$. If E_{2n} were convex for $x \geq e^{-e}$, unimodality would be established. One final observation: Because $1 + E_{2n} \ln x$ increases with n, if $E_{2n}'(x) > 0$ for a given x, then $E_{2n+2k}'(x) > 0$ for all integers $k > 0$.

Similar analyses were received from Con Amore Problem Group (Denmark), and Zachary Franco.

Answers

Solutions to the Quickies on page 225.

A835. If x is odd, then $x \equiv \pm 1 \pmod 4$. If $x \equiv 1 \pmod 4$, the given equation yields $-1 \equiv 1 \pmod 4$, and if $x \equiv -1 \pmod 4$, it yields $-(-1)^n \equiv (-1)^n \pmod 4$. In either case, we have a contradiction so there is no solution.

Assume x is even. If there exists a solution, then $3^n + 5^n \equiv 0 \pmod{2^n}$. An examination of $3^n + 5^n$, however, reveals that $3^n + 5^n \not\equiv 0 \pmod{2^4}$. Therefore, there exists no solution for $n \geq 4$. Clearly there are no solutions when $n \leq 1$. When $n = 2$, we obtain $(x + 2)^2 - x^2 = 3^2 + 5^2$, which requires that $x = 15/2$. Thus, no solution exists when $n = 2$. If $n = 3$, however, we have $(x + 2)^3 - x^3 = 3^3 + 5^3$ or $x^2 + 2x - 24 = 0$ with roots 4 and -6. It follows that $n = 3$, $x = 4$ is the only solution in positive integers.

Alternate Solution. If n is even, $3^n + 5^n \equiv 2 (\bmod 8)$, while $(x+2)^n - x^n \equiv 0 (\bmod 4)$, a contradiction. If n is odd, $3^n + 5^n = (4-1)^n + (4+1)^n = 2 \cdot 4^n + 2\binom{n}{2}4^{n-2} + \cdots + 2\binom{n}{n-1}4 \equiv 8 (\bmod 16)$. If x is odd, $(x+2)^n - x^n \equiv (x+2) - x = 2 (\bmod 8)$, a contradiction. If x is even, $(x+2)^n - x^n \equiv 0 (\bmod 2^n)$, forcing $n = 1$ or 3. Inspection yields $n = 3$, $x = 4$ as the only solution.

A836. The eigenvalues of O have absolute value 1, so if ± 1 are not eigenvalues, the characteristic polynomial, $p(\lambda) = |\lambda I - O| = \lambda^n + \cdots + (-1)^n |O|$, has no real roots. When we multiply a row of O by -1, the constant term of the characteristic polynomial changes sign, hence has both positive and negative roots; that is, ± 1 are eigenvalues.

A837. From the unfolded paper we have $\alpha + \beta + \gamma + \delta = 2\pi$. From the folded paper we have $\alpha - \beta + \gamma - \delta = 0$. Adding the two equations reveals that opposite pairs of angles are supplementary.

Algorithms

Years ago, in grade school,
Teacher used to say,
"For every problem there's a rule,
So do it just that way."

But when I got to college
They said I always must
Apply my basic knowledge,
Since rules are to distrust.

The New Math thought that every kid
Should give real thought a try.
It didn't matter what you did
Just so you told them why.

Then the computers came along,
And algorithms, too,
Constructed so you can't go wrong
No matter what you do.

An algorithm? That's a rule
For doing something. Back to school!

From *Lion Hunting and Other Mathematical Pursuits, A Collection of Mathematics, Verse, and Stories by Ralph P. Boas, Jr.*, Gerald L. Alexanderson and Dale H. Mugler, eds., MAA, Washington, DC, 1995.

REVIEWS

PAUL J. CAMPBELL, *editor*
Beloit College

Assistant Editor: Eric S. Rosenthal, West Orange, NJ. Articles and books are selected for this section to call attention to interesting mathematical exposition that occurs outside the mainstream of the mathematics literature. Readers are invited to suggest items for review to the editors.

Steinbock, Oliver, Ágota Tóth, and Kenneth Showalter, Navigating complex labyrinths: Optimal paths from chemical waves, *Science* 267 (10 February 1995) 868–871.

The era of computing with chemicals is upon us. Last year, Leonard Adleman (University of Southern California) solved a directed hamiltonian path problem using molecules of DNA. Now three chemists have used the Belousov-Zhabotinsky reaction and time-lapse imaging to find optimal paths in mazes. "A single propagating wave generates a map for the optimal path from every point of the system to a target point."

Stewart, Ian, Juggling by numbers, 145 *New Scientist* (18 March 1995) (No. 1969) 34–38.

Mathematics is the science of patterns, and some mathematicians are keen jugglers; so it is perhaps surprising that only recently is there a mathematical theory of juggling. A juggling pattern can be described by a sequence of integers that represent the heights of the throws and measure the time between successive throws of a particular ball. Mathematical theorems tell from the repeat unit for a pattern how many balls the pattern needs and whether it is jugglable, as well as how many patterns there are for a given number of balls and a set period. For mathematical details, see Joe Buhler *et al.*, Juggling drops and descents, *American Mathematical Monthly* 101 (6) (June-July 1994) 507–519.

Peterson, Ivars, Paper folds, creases, and theorems, *Science News* 147 (21 January 1995) 44.

Origami is regarded as a geometric mathematical recreation, but little has been done to analyze mathematically how the crease patterns are related to the resulting forms. Thomas C. Hull (University of Rhode Island) is pursuing such an analysis by thinking of the crease pattern as a graph but with specific angles between the edges. His findings, and those of Japanese colleagues, have inspired new origami creations, much as mathematical analysis of juggling in recent years has inspired new juggling routines.

Peterson, Ivars, The Codemart catalog: arranging points on a sphere for fun and profit, *Science News* 147 (4 March 1995) 140, 142.

What is the optimal way to arrange n points on a sphere? It depends on what you want to do: Maximize the minimum distance between pairs of points, minimize the average distance from any point on the sphere to one of the placed points, or any of half a dozen other criteria. The optimal arrangement is usually different for one criterion than another, and each criterion corresponds to a class of practical problems. (Sample: Laser beams are used to destroy a tumor; how should you arrange the beams to minimize intersection except at the target?) N.J.A. Sloane and Ronald H. Hardin (Bell Labs) and Warren D. Smith (NEC Research Laboratory, Princeton, NJ) have built up tables of "nice" arrangements of points on spheres. Their catalog is available by sending the message `send index for att/math/sloane/packings` to the address `netlib@research.att.com`.

Long, Suzanne, Fuzzy logic in focus, *Hemispheres* (December 1994) 101–104.

This article in an airline magazine is short on theory but notes applications of fuzzy logic in the Mars land rover and other space projects, the 1994 GM Saturn's automatic transmission (it shifts smoothly to accommodate the driver's bad acceleration habits), and Whirlpool's new refrigerators (the defrost cycle adjusts to the residents' door-opening habits). Students at many levels would enjoy and be motivated by further details on any of these. The details, however, are no doubt proprietary.

Stewart, Ian, Daisy, Daisy, give me your answer, do, *Scientific American* 272 (1) (January 1995) 96–99.

Stewart describes, in his customary dialogue fashion, the latest explanation for the appearance of the Fibonacci numbers in phyllotaxis. This new theory, by Stéphane Douady and Yves Couder (Laboratory of Statistical Physics, Paris), shows how the dynamics of plant growth produces the golden angle between successive primordia. This angle allows the seed of a sunflower to pack most efficiently, because "the most irrational number is the golden number"—meaning that the difference between successive approximants tends to zero as slowly as possible.

Cutler, Alan, Notes from the underground, *The Sciences* 35 (1) (January/February 1995) 36–40.

If the dinosaurs died out suddenly 65 million years ago, why isn't there a peak of discovered dinosaur bones of that age? Some insight can be gained by conceiving of the fossil record as a signal, to which signal-processing techniques—low-pass filters, convolution, deconvolution, etc.—can be applied. Mathematical modeling of dinosaur extinction shows that, for any reasonable estimates of parameters for mortality and bone burial, time averaging—corresponding to mixing of sediments as they are deposited—completely swamps the extinction spike in the fossil record. However, properly calibrated deconvolution can recover the original spike from the "smeared" record.

Honsberger, Ross, *Episodes in Nineteenth and Twentieth Century Euclidean Geometry*, MAA, 1995; xiii + 174 pp, \$28.50 (\$22 to MAA members) (P). ISBN 0–88385–639–5.

Books like this one are very rare. It visits modern results in Euclidean plane geometry, arriving at them through synthetic methods (as opposed to analytic geometry). A high-school background suffices, though the reader is referred to other sources for the proofs of the basic properties of the nine-point circle. A few exercises are included for most chapters, along with solutions. The book does not give references to the original papers for the results.

Alexanderson, Gerald L. and Dale H. Mugler, *Lion Hunting and Other Mathematical Pursuits: A Collection of Mathematics, Verse, and Stories by Ralph P. Boas, Jr.*, MAA, 1995; xii + 308 pp, \$35 (\$25 to MAA members) (P). ISBN 0–88385–323–X.

This tribute to Ralph Boas includes biographical and bibliographical information, reminiscences, and nontechnical papers on a variety of subjects, as well as epimathematical works (e.g., the world's most complete collection devoted to the mathematics of big-game hunting). "His wit, humor, and humanity emanate from every page," concludes the back cover, after samples that should convince you that this book will make light and delightful bedtime reading.

Shin, Sun-Joo, *The Logical Status of Diagrams*, Cambridge University Press, 1995; xi + 197 pp, $39.95.

This MAGAZINE publishes a regular feature entitled "Proof without Words." Are the diagrams presented really proofs? Should you trust them? "[A] negative attitude toward diagrams has been prevalent among logicians and mathematicians. They consider any non-linguistic form of representation to be a heuristic tool only. No diagram or collection of diagrams is considered a valid proof at all. ...[N]obody has shown any legitimate justification for this attitude ...." Author Shin traces "this prejudice" to "the limitation of diagrams in representing knowledge" but mainly to the possibility of their misdirecting reasoning. He argues that diagrams are not inherently misleading, nor does misuse of them justify the prejudice. To substantiate his case, he carries out a case study of Venn diagrams as a formal system, showing that "they form a sound and complete system independent of Boolean algebra."

Cipra, Barry, At math meetings, enormous theorem eclipses Fermat, *Science* 267 (10 February 1995) 794–795.

The "enormous theorem" of the title of this article is the classification theorem for finite simple groups. Richard Lyons (Rutgers University) and Ron Solomon (Ohio State University) have taken on the task of providing a "second-generation" proof of this result. Any finite group can be built up from finite simple groups, and the theorem says that any finite simple group either belongs to one of the infinite families of cyclic, alternating, or Lie-type groups, or else is one of 28 sporadic groups. The current proof, completed in 1980, is scattered across a thousand journal articles and 15,000 pages. Who could check such a result? The projected second-generation proof will be shorter—between 3,000 and 5,000 pages. Will there some day be a 50-page proof? Don't count on it.

Cipra, Barry, A visit to Asymtopia yields insight into set structures, *Science* 267 (17 February 1995) 964–965.

"Suppose you want to throw a party ...[Y]ou want people to mix, so you don't want to wind up with any 'triangles' consisting of three people each of whom already knows the other two. On the other hand, you don't want to wind up with any large groups of complete strangers, so you decide to require that among any, say, five people, at least two should know each other." Ramsey's theorem implies that for any k (e.g., $k = 5$), every graph with more than a certain number of vertices must contain at least one triangle (three vertices adjacent in pairs) or k independent vertices (none adjacent to any of the others). So, there is a maximum size, denoted $R(3,5)$, for the party (in fact, $R(3,5) = 14$). The exact values of $R(3,k)$ are known only for k up through 9. Jeong-Hon Kim (Bell Labs) took a new approach by letting the number of vertices grow arbitrarily large and searching for asymptotic results. Viewing the addition of an edge as an infinitesimal change "allows him to describe the process of adding edges by a differential equation," which can be solved to show that $R(3,k)$ is $\Theta(k^2/\log k)$ (i.e., it is bounded between two multiples of $k^2/\log k$).

Pool, Robert, Putting game theory to the test, *Science* 267 (17 March 1995) 1591–1593.

Evolutionary biologists have been testing specific game-theory models by making field observations and doing lab experiments. They have found good agreement between theory and practice, in spiders fighting over web sites, egrets killing their siblings, naked mole rats being lazy, bower birds destroying rivals' bowers, and small fish scouting out approaching larger fish. In each case, the animal behavior reflects an evolutionarily stable strategy.

Gardner, Martin, *My Best Mathematical and Logic Puzzles*, Dover, 1994; vii + 82 pp, $3.95 (P). ISBN 0-486-28152-3. Wells, David, *The Penguin Book of Curious and Interesting Puzzles*, Penguin, 1992; viii + 382, $12 (P). ISBN 0-14-014875-2. Slocum, Jerry, and Jack Botermans, *The Book of Ingenious and Diabolical Puzzles*, Times Books, 1995; viii + 152 pp, $19.50. ISBN 0-8129-2153-4.

Most of Gardner's 66 puzzles in this book are taken from his first three collections of Mathematical Games columns in *Scientific American*, but the last 12 are from two articles in *Games* magazine. While Gardner avoids the classics by Dudeney, Loyd, and Phillips, Wells samples those authors and others (it would be easier to tell just who if the book had a decent table of contents). Attributions are cited for most of Wells's 568 puzzles, and that feature plus a good index make his book a useful reference. Slocum and Botermans offer another of their beautiful coffee-table puzzle books; beautiful photographs of antique physical (not necessarily mathematical) puzzles are accompanied by some history of them. (I was pleased to learn so much about tangrams and their varieties.)

Wagon, Stan, *The Power of Visualization: Notes from a Mathematica Course*, Front Range Press (P.O. Box 3162, Copper Mountain, CO 80443-3162; outside U.S.A., 26 Temple Lane, Dublin 2, Ireland), 1994; iii + 117 pp, $25. ISBN 0-9631678-3-9. Supplementary diskette (IBM or Macintosh) $25. Book with either diskette $35.

This book contains the lecture notes from a 1994 summer course in Mathematica for college instructors with some prior experience with the package. Wagon is the author of *Mathematica in Action* (W.H. Freeman, 1991) and co-author of *Animating Calculus* (W.H. Freeman, 1994), where further details on many of the examples of this book can be found. One-week introductory and intermediate courses will be offered in July 1995.

Halmos, Paul R., *Linear Algebra Problem Book*, MAA, 1995; xiii + 366 pp, $35 ($25 to MAA members) (P). ISBN 0-88385-322-1.

Thirty years ago or so, Halmos's *Finite-Dimensional Vector Spaces* set a standard (since then greatly relaxed) for the undergraduate linear algebra course. This new book of his "largely" follows the organization of that classic and is a worthy supplement for any linear algebra course that is more than just matrix algebra. Unlike most problem books, the problems and their extensive motivations take up an equal number of pages with the hints and solutions.

Moore, A.W., A brief history of infinity, *Scientific American* 272 (4) (April 1995) 112–116.

Infinity is an "evergreen" subject for a popular science magazine, as philosophers are wont to say. Here one describes Archimedes' method of exhaustion and Cantor's theory of infinite cardinality. Author Moore concludes by suggesting that Cantor did not "dispel all doubt about mathematical dealings with infinity" but "may have reinforced that doubt," and by urging "mathematicians and other scientists to use more caution than usual when assessing how Cantor's results bear on traditional conceptions of infinity"!

Stewart, Ian, Paradox of the spheres, *New Scientist* 145 (14 January 1995) (No. 1960) 28–31.

Stewart offers a pleasant exposition of the Banach-Tarski paradox ("not a true paradox, being counterintuitive rather than self-contradictory").

NEWS AND LETTERS

TWENTYTHIRD ANNUAL USA MATHEMATICAL OLYMPIAD

PROBLEMS AND SOLUTIONS

1. Let $k_1 < k_2 < k_3 < \cdots$ be positive integers, no two consecutive, and let $s_m = k_1+k_2+\cdots+k_m$ for $m = 1, 2, 3, \ldots$. Prove that, for each positive integer n, the interval $[s_n, s_{n+1})$ contains at least one perfect square.

Solution. The interval $[s_n, s_{n+1})$ contains a perfect square if and only if $[\sqrt{s_n}, \sqrt{s_{n+1}})$ contains an integer, so it suffices to prove that $\sqrt{s_{n+1}} - \sqrt{s_n} \geq 1$ for each $n \geq 1$. Substituting $s_n + k_n$ for s_{n+1}, we see that the desired inequality is $s_n + k_{n+1} \geq (\sqrt{s_n} + 1)^2$ or $k_{n+1} \geq 2\sqrt{s_n} + 1$. Since $k_{m+1} - k_m \geq 2$ for each m, we have

$$\begin{aligned} s_n &= k_n + k_{n-1} + k_{n-2} + \cdots + k_1 \\ &\leq k_n + (k_n - 2) + \cdots + l_n \end{aligned}$$

where $l_n = 2$ if k_n is even and $l_n = 1$ if k_n is odd. Thus

$$\begin{aligned} s_n &\leq \begin{cases} \dfrac{k_n(k_n+2)}{4} & \text{if } k_n \text{ is even} \\ \dfrac{(k_n+1)^2}{4} & \text{if } k_n \text{ is odd} \end{cases} \\ &\leq \frac{(k_n+1)^2}{4}. \end{aligned}$$

Hence $(k_n + 1)^2 \geq 4s_n$, and $k_{n+1} \geq k_n + 2 \geq 2\sqrt{s_n} + 1$.

2. The sides of a 99-gon are initially colored so that consecutive sides are red, blue, red, blue, ..., red, blue, yellow. We make a sequence of modifications in the coloring, changing the color of one side at a time to one of the three given colors (red, blue, yellow), under the constraint that no two adjacent sides may be the same color. By making a sequence of such modifications, is it possible to arrive at the coloring in which consecutive sides are red, blue, red, blue, red, blue, ..., red, yellow, blue?

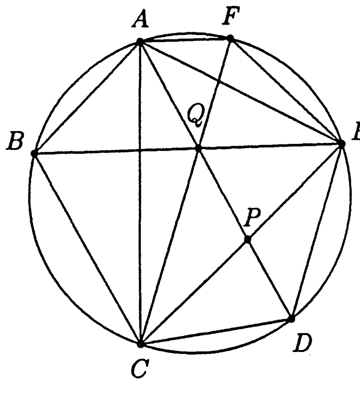
Solution. Given a coloring of a polygon with an odd number of sides, assign to each vertex of the polygon a *score* by the following rule. If, reading clockwise, two adjacent sides have coloring (red, blue), (blue, yellow), or (yellow, red), then the score of the intermediate vertex is $+1$; if the clockwise coloring is (blue, red), (yellow, blue) or (red, yellow) then the score of this vertex is -1. The *total score* of the colored polygon is the sum of the scores of its vertices. It is easy to see that the score of the (clockwise) coloring (red, blue, red, blue, ..., red, blue, yellow) is $+3$ and the score of (red, blue, red, blue, ..., red, yellow, blue) is -3. The only allowed modifications are those in which the side to be re-colored is initially one color, the two adjacent sides are both a second color, and the modified side is then given the third color. When such an operation is performed, the score of one incident vertex changes $+1$ to -1 while the score of the other incident vertex changes from -1 to $+1$. These modifications preserve the total score. Thus it is impossible to arrive at the coloring (red, blue, red, blue, ..., red, yellow, blue) starting from (red, blue, red, blue, ..., red, blue, yellow).

Note. It is clear that in giving the intial and final colorings of the sides, the proposer conceived of the sides being listed in some fixed cyclic order, with the same starting point and in the same direction around the polygon. Otherwise, a trivial affirmative solution exists.

3. A convex hexagon $ABCDEF$ is inscribed in a circle such that $AB = CD = EF$ and diagonals AD, BE, and CF are concurrent. Let P be the intersection of AD and CE. Prove that $CP/PE = (AC/CE)^2$.

Solution. Since $CD = EF$, the lines $\overleftrightarrow{CF}$ and $\overleftrightarrow{DE}$ are parallel. Hence $\Delta CPQ \sim \Delta EPD$ and

$$\frac{CP}{PE} = \frac{CQ}{DE}.$$



Note that $\angle QDE \cong \angle ACE$ since these angles subtend the same arc, and $\angle QED \cong \angle AEC$ since these angles subtend arcs of equal length ($\overset{\frown}{BD}$ and $\overset{\frown}{AC}$). It follows that $\Delta QDE \sim \Delta ACE$. By the same argument, $\angle QDC \cong \angle AEC$ and $\angle DCQ \cong \angle CAE$ so $\Delta CQD \sim \Delta ACE$. Therefore, by the similar triangles $\Delta QDE \sim \Delta ACE \sim \Delta CQD$, we have

$$\frac{CP}{PE} = \frac{CQ}{DE} = \frac{CQ}{DQ}\frac{DQ}{DE} = \left(\frac{AC}{CE}\right)^2.$$

4. Let $a_1, a_2, a_3, \ldots$ be a sequence of positive real numbers satisfying $\sum_{j=1}^{n} a_j \geq \sqrt{n}$ for all $n \geq 1$. Prove that, for all $n \geq 1$,

$$\sum_{j=1}^{n} a_j^2 > \frac{1}{4}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right).$$

Solution. The desired inequality is a consequence of the following result.

Proposition *Suppose $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are positive numbers such that*

$$b_1 > b_2 > \cdots > b_n, \qquad (1)$$

and for $k = 1, 2, \ldots, n$

$$\sum_{j=1}^{k} b_j \leq \sum_{j=1}^{k} a_j. \qquad (2)$$

Then

$$\sum_{j=1}^{n} b_j^2 \leq \sum_{j=1}^{n} a_j^2. \qquad (3)$$

Proof. Let $b_{n+1} = 0$. Using (1) and (2), we obtain

$$\sum_{k=1}^{n}(b_k - b_{k+1})\sum_{j=1}^{k} b_j \leq \sum_{k=1}^{n}(b_k - b_{k+1})\sum_{j=1}^{k} a_j,$$

$$\sum_{j=1}^{n} b_j \sum_{k=j}^{n}(b_k - b_{k+1}) \leq \sum_{j=1}^{n} a_j \sum_{k=j}^{n}(b_k - b_{k+1}),$$

and thus

$$\sum_{j=1}^{n} b_j^2 \leq \sum_{j=1}^{n} a_j b_j.$$

Squaring both sides and using Cauchy's inequality,

$$\left(\sum_{j=1}^{n} a_j b_j\right)^2 \leq \left(\sum_{j=1}^{n} a_j^2\right)\left(\sum_{j=1}^{n} b_j^2\right),$$

we have

$$\sum_{j=1}^{n} b_j^2 \leq \sum_{j=1}^{n} a_j^2.$$

To complete the solution of the problem, for $j = 1, 2, \ldots, n$ let

$$b_j = \sqrt{j} - \sqrt{j-1} = \frac{1}{\sqrt{j} + \sqrt{j-1}}.$$

Then (1) and (2) are satisfied, so

$$\begin{aligned} \sum_{j=1}^{n} a_j^2 &\geq \sum_{j=1}^{n} \frac{1}{(\sqrt{j} + \sqrt{j-1})^2} \\ &> \sum_{j=1}^{n} \frac{1}{(2\sqrt{j})^2} \\ &= \frac{1}{4}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right). \end{aligned}$$

Note. Equality holds in (3) if and only if $a_j = b_j$ ($j = 1, 2, \ldots, n$).

5. Let $|U|$, $\sigma(U)$ and $\pi(U)$ denote the number of elements, the sum, and the product, respectively, of a finite set U of positive integers. (If U is the empty set, $|U| = 0$, $\sigma(U) = 0$, $\pi(U) = 1$.) Let S be a finite set of positive integers. As usual, let $\binom{n}{k}$ denote $\frac{n!}{k!(n-k)!}$. Prove that

$$\sum_{U \subseteq S} (-1)^{|U|} \binom{m - \sigma(U)}{|S|} = \pi(S)$$

for all integers $m \geq \sigma(S)$.

Solution. The identity follows by counting (in two ways) certain sequences of zeros and ones. Suppose $S = \{a_1, a_2, \ldots, a_n\}$ and $m \geq \sigma(S)$. For 0-1 sequences of length m, call the first a_1 positions *block 1*, the next a_2 positions *block 2* and so on. How many of the 2^m sequences contain exactly n ones altogether and have no such block consisting entirely of zeros?

The first count is by a direct argument. Since there are n ones and n identified blocks, each block must have a single 1, and there are thus a_1 choices for the position of the 1 in the first block, a_2 for the second, and so on. Thus the total number of such sequences is $a_1 a_2 \cdots a_n = \pi(S)$.

The second count makes use of the principle of inclusion-exclusion. Let X be a finite set and let $X_1, X_2, \ldots, X_n$ be (not necessarily distinct) subsets of X. Denote the complements of these sets by $\overline{X}_1, \overline{X}_2, \ldots, \overline{X}_n$, respectively. Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. The inclusion-exclusion formula counts the number of elements of X not belonging to any X_i:

$$\left|\bigcap_{i=1}^{n} \overline{X}_i\right| = \sum_{Q \subseteq [n]} (-1)^{|Q|} \left|\bigcap_{i \in Q} X_i\right|. \quad (1)$$

Let X be the set of all 0-1 sequences of length m containing exactly n ones, and let X_i be the subset in which block i consists entirely of zeros. For each $U \subseteq S$, let $Q(U) = \{i \mid a_i \in U\}$. If a 0-1 sequence belongs to X_i for each $i \in Q(U)$, then there are $\sigma(U)$ positions consisting entirely of zeros, and the n ones must be chosen from the $m - \sigma(U)$ remaining positions. Hence

$$\left|\bigcap_{i \in Q(U)} X_i\right| = \binom{m - \sigma(U)}{n}.$$

By the one-to-one correspondence between $U \subseteq S$ and $Q(U) \subseteq [n]$, the inclusion-exclusion sum (1) may be written as a sum over all $U \subseteq S$. Thus the number of 0-1 sequences of length m in which there are exactly n ones and in which none of the identified blocks consists entirely of zeros is

$$\sum_{U \subseteq S} (-1)^{|U|} \binom{m - \sigma(U)}{|S|}.$$

Equating this count to the previous one, we have the desired identity.

Note. Define

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}.$$

With this interpretation, the result is a polynomial identity and thus holds not only for integer m satisfying $m \geq \sigma(S)$, but for arbitrary real or complex values of m.

Solutions were prepared by Cecil Rousseau, Memphis State University, Memphis, TN 38152.

Dear Editor,

In "An Advanced Calculus Approach to Finding the Fermat Point" (Feb. 1994), Hajja quotes Kay that "any attempt to solve this by means of calculus would most probably end in considerable frustration" and, then gives a calculus-based solution of this problem a.k.a. Steiner's problem. A much shorter solution of this problem appeared in this MAGAZINE, Vol. 40 (1967), p. 273.

Prem N. Bajaj
The Wichita State University
Wichita, KS 67260-0033

Dear Editor,

In "The Product of Chord Lengths of a Circle" (Feb. 1995), by Mazzoleni and Shen, Residue Theory is used to prove that we have

$$\prod_{k=2}^{n} \left|1 - e^{\frac{2\pi i(k-1)}{n}}\right| = n$$

(which holds for $n \geq 2$, even without taking absolute values).

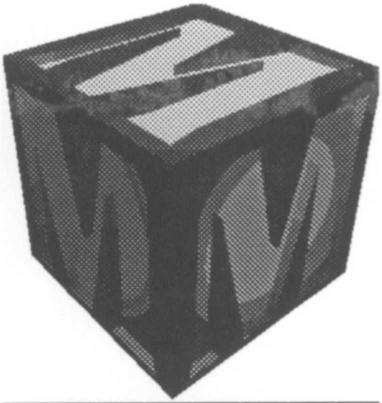
We present a more elementary proof of the same result:

Let $p_k = e^{\frac{2\pi i(k-1)}{n}}$ for $k = 1, \cdots, n$ be the nth roots of 1. As $z^n - 1 = (z-1)(z^{n-1} + \cdots + 1)$ we have $\prod_{k=2}^{n} (z - p_k) = z^{n-1} + \cdots + 1$ and the result follows if we take $z = 1$.

See *Complex Analysis* by J. Bak & J. Newman, Springer 1983 (11, 12, p. 16), and *Complex Numbers & Geometry* by L. Hahn, MAA 1994 (49, p. 53).

Jorge-Nuno Siva
University of California
Berkeley, CA 94720

The proof presented by Dr. Silva is our Reference [2]. It was explicitly included in an earlier draft, but was eliminated during the editing process. --Andre Mazzoleni



"One of the best uses of multimedia I have ever seen for the instructional market."

-- *Stacy Prassas,*
Vice President,
Willow New Media Services

"I love this program! The step-by-step methods really help me in understanding functions."

-- *Jamille Hicks*
Undergradutate Student
Biology

"Congratulations on producing the first really creative math CD-ROM."

-- *Dr. Mary Winter*
Professor of Mathematics
Michigan State University

MULTIMEDIA MATH

functions

A New Era in Learning

Multimedia Math: Functions (M^3: Functions) is designed to enhance the quality of undergraduate mathematics teaching and learning through the introduction of multimedia technology.

It is the first of its kind, utilizing digital audio and video, graphics, and animation to teach the mathematical topic of "Functions" — a central concept and the primary content of precalculus math courses.

Best of all, it allows students to learn at their own pace, while ensuring that they understand a concept before proceeding to a more difficult level.

Usage

M^3: Functions can be used in many different ways:

- Resource for independent study in a learning lab
- Supplement to a mathematics class
- Stand-alone course with database and record-keeping system

M^3: Functions is designed to run stand-alone from a CD-ROM on a MPCII compliant computer or with multiple users on a network.

For more information contact

The University of Alabama
Center for Teaching and Learning
Box 870304
Tuscaloosa, Alabama
35487-0304

Phone (205)348-2424
Fax (205)348-2754

E-mail M3SALES@BAMANET.UA.EDU

CONTENTS

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, NW
Washington, D.C. 20036