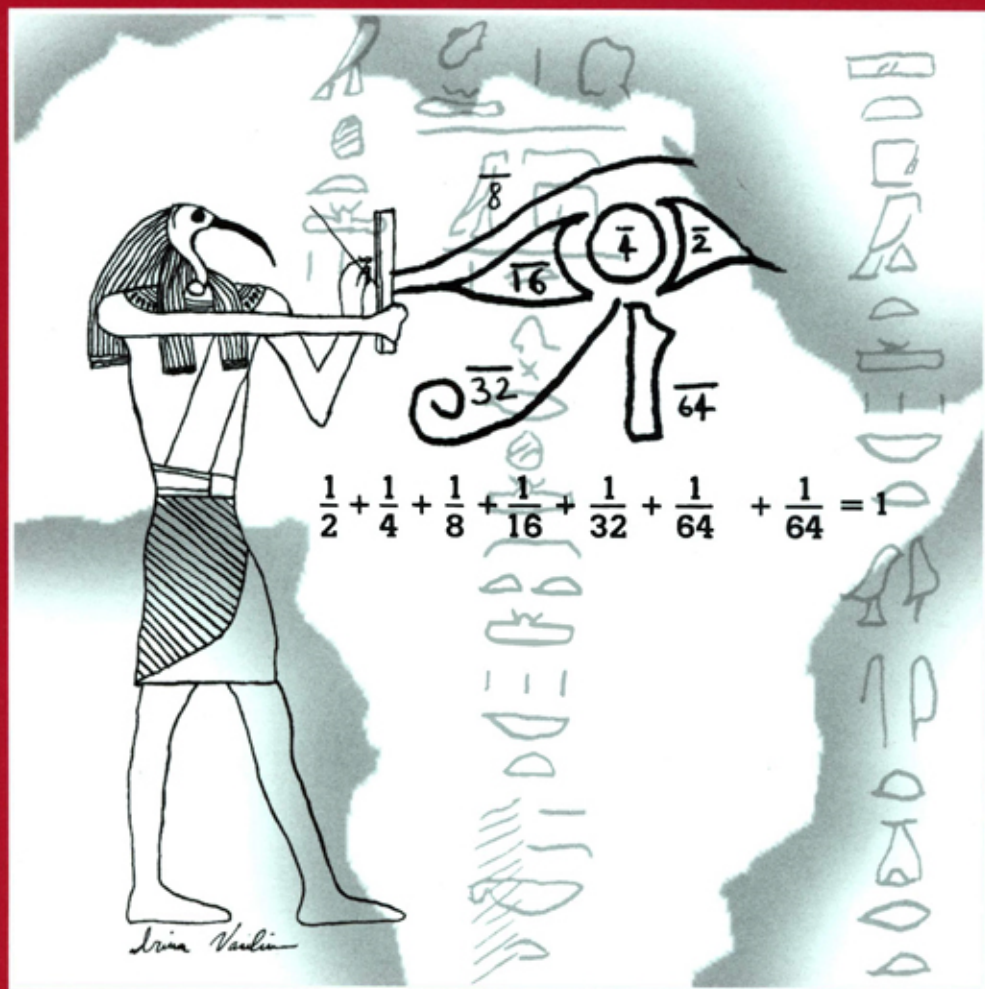




MATHEMATICS MAGAZINE



- Znam's Problem
- The Josephus Problem: Once More Around
- A Brief History of Factoring and Primality Testing B. C. (Before Computers)

EDITORIAL POLICY

Mathematics Magazine aims to provide lively and appealing mathematical exposition. The *Magazine* is not a research journal, so the terse style appropriate for such a journal (lemma-theorem-proof-corollary) is not appropriate 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. Manuscripts on history are especially welcome, as are those showing relationships among various branches of mathematics and between mathematics and other disciplines.

A more detailed statement of author guidelines appears in this *Magazine*, Vol. 74, pp. 75–76, and is available from the Editor or at www.maa.org/pubs/mathmag.html. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, or published by another journal or publisher.

Submit new manuscripts to Frank A. Farris, Editor, *Mathematics Magazine*, Santa Clara University, 500 El Camino Real, Santa Clara, CA 95053-0373. Manuscripts should be laser printed, with wide line spacing, and prepared in a style consistent with the format of *Mathematics Magazine*. Authors should mail three copies and keep one copy. In addition, authors should supply the full five-symbol 2000 Mathematics Subject Classification number, as described in *Mathematical Reviews*.

Cover image: *Thoth Bestows Mathematics upon Humankind*, by Jason Challas, who bestows instruction in computer art at Santa Clara University. Drawing of Thoth by Irina Vasiliu.

AUTHORS

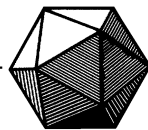
Lawrence Brenton received his Bachelor of Arts degree in 1968 from the University of Pennsylvania and earned his Ph.D. from the University of Washington in 1974. He held posts as a post-doctoral research fellow at the University of Bonn, Germany, and as a visiting professor at Tulane University before joining the faculty of Wayne State University, where he has served for twenty-six years. His research interests are several complex variables and algebraic geometry, especially the theory of singularities of analytic varieties. His current passion is directing the Wayne State University Undergraduate Research Program.

Ana Vasiliu was a participant in the WSU Undergraduate Research Program and worked on Znam's problem together with others under the supervision of Professor Brenton. She is currently working towards a Master's degree at Oklahoma State University.

Richard A. Mollin received his Ph.D. in 1975 in mathematics from Queen's University, Kingston, Ontario, Canada, where he was born. He is now a full professor in the Mathematics Department at the University of Calgary, with over 150 publications in algebra, number theory, and computational mathematics to his credit. The development behind the ideas for this article was an inspiration for the writing of his latest book, *An Introduction to Cryptography* (Chapman and Hall/CRC Press). He resides in Calgary with his wife Bridget and two cats. When not engaged in mathematics or entertaining mathematical visitors at Mollin Manor, he and Bridget enjoy hiking in the Rockies.

Peter Schumer received his B.S. and M.S. from Rensselaer Polytechnic Institute and his Ph.D. from University of Maryland, College Park. Since 1983 he has been a member of the mathematics faculty at Middlebury College in Vermont. His main mathematical interests include elementary number theory, combinatorics, and the history of mathematics. He has written a textbook, *Introduction to Number Theory* (PWS Publishing) and was the 2000 recipient of the MAA's Trevor Evans Award for the article, "The Magician of Budapest." His interests in mathematics and the game of *go* have been amicably combined during several sabbaticals to California and to Japan.

Vol. 75, No. 1, February 2002



MATHEMATICS MAGAZINE

EDITOR

Frank A. Farris
Santa Clara University

ASSOCIATE EDITORS

Glenn D. Appleby
Santa Clara University

Arthur T. Benjamin
Harvey Mudd College

Paul J. Campbell
Beloit College

Annalisa Crannell
Franklin & Marshall College

David M. James
Howard University

Elgin H. Johnston
Iowa State University

Victor J. Katz
University of District of Columbia

Jennifer J. Quinn
Occidental College

David R. Scott
University of Puget Sound

Sanford L. Segal
University of Rochester

Harry Waldman
MAA, Washington, DC

EDITORIAL ASSISTANT

Martha L. Giannini

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 *MATHEMATICS MAGAZINE* to an individual member of the Association is \$131, which includes annual dues. Student and unemployed members receive a 66% dues discount; emeritus members receive a 50% discount; and new members receive a 20% dues discount for the first two years of membership.

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 Dave Riska (driska@maa.org), Advertising Manager, the Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036.

Copyright © by the Mathematical Association of America (Incorporated), 2002, including rights to this journal issue as a whole and, except where otherwise noted, rights to each individual contribution. Permission to make copies of individual articles, in paper or electronic form, including posting on personal and class web pages, for educational and scientific use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear the following copyright notice:

Copyright the Mathematical Association of America 2002. All rights reserved.

Abstracting with credit is permitted. To copy otherwise, or to republish, requires specific permission of the MAA's Director of Publication and possibly a fee.

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

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

Printed in the United States of America

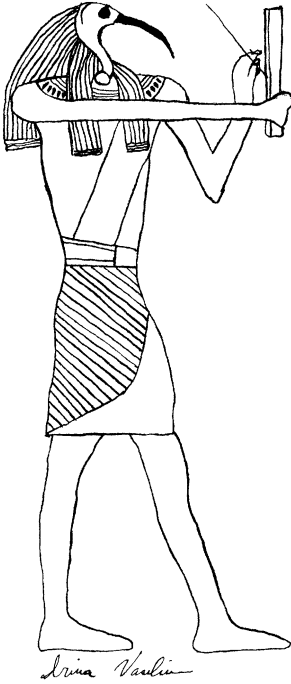
Znam's Problem

LAWRENCE BRENTON

Wayne State University
Detroit, Michigan 48202

ANA VASILIU

Oklahoma State University
Stillwater, Oklahoma 74075

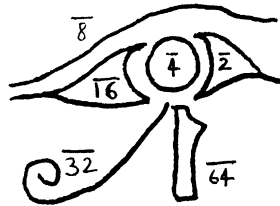


The mysterious science of mathematics was bestowed upon humankind as a gift from the benevolent ibis-headed god Thoth in prehistoric times. So asserts the Egyptian Book of the Dead, a compilation of myths and incantations from the oldest civilization of which we have a substantial body of reliable historical documents [17]. According to legend, the evil god Seth damaged the eye of Horus, son of Isis and Osiris. The Eye of Horus had mystical significance, as each of its parts was associated with a fraction of the form $1/2^n$.

Thoth is credited with restoring the eye “by the touch of his finger,” making it whole. Later scholars interpreted this story as an allegorical reference to the geometric sum

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \frac{1}{64}. \quad (1)$$

This sum is “made whole” (that is, it sums to 1) by the addition of one more “finger” (one counting unit, or $1/64$ in this example).



Fractional expressions of this sort occurred naturally within the Egyptian system of arithmetic. The mathematician-scribes of dynastic Egypt denoted rational numbers by strings of *unit fractions*—fractions whose numerators are 1. What we would think of as a subtraction problem, for instance, $1 - 1/3 - 1/4 - 1/8 - 1/10 - 1/30 - 1/45$, was posed in Egyptian mathematical texts in the form of “completion to unity”: given the unit fraction sum

$$\frac{1}{3} + \frac{1}{4} + \frac{1}{8} + \frac{1}{10} + \frac{1}{30} + \frac{1}{45},$$

what unit fractions must be added in order to obtain one? This is problem 23 in the famous Ahmose papyrus (1500 BCE; also called the Rhind mathematical papyrus [20]), which derives the solution

$$\frac{1}{3} + \frac{1}{4} + \frac{1}{8} + \frac{1}{10} + \frac{1}{30} + \frac{1}{45} + \frac{1}{9} + \frac{1}{40} = 1$$

Thoth's sum (1) has the additional feature that the missing part is "as small as possible." That is, if we are given any sum $\sum_{i=1}^k 1/n_i < 1$ then the missing part $1 - \sum_{i=1}^k 1/n_i$ is equal to $D/\text{lcm}(n_1, n_2, \dots, n_k)$ for some positive integer D , where lcm is the least common multiple. If we want to make our fraction whole "by the touch of one finger," we must have $D = 1$. Thus, we wish to investigate solutions to the fractional Diophantine equation

$$\frac{1}{n_1} + \frac{1}{n_2} + \dots + \frac{1}{n_k} + \frac{1}{\text{lcm}(n_1, n_2, \dots, n_k)} = 1. \quad (2)$$

This equation has been given an amusing interpretation as an inheritance problem [1].

Equally interesting is the companion equation

$$\frac{1}{n_1} + \frac{1}{n_2} + \dots + \frac{1}{n_k} - \frac{1}{\text{lcm}(n_1, n_2, \dots, n_k)} = 1 \quad (3)$$

(cf. Borwein [2]). For instance, for $k = 3$ we have the following relation between solutions of equation (3) and the geometry of the five regular polyhedra (Platonic solids). For a fixed regular polyhedron, denote by F , E , and V the number of faces, edges, and vertices, respectively, let S be the number of sides of each face, and let R be the number of rays that meet at each vertex. Since each edge adjoins exactly two faces and produces exactly two rays, we have the relations

$$E = \frac{1}{2}VR = \frac{1}{2}FS. \quad (4)$$

Now consider the Euler formula $V - E + F = 2$, valid for any sphere-like polyhedron, regular or not. From (4) we have $2E/R - E + 2E/S = 2$, or

$$\frac{1}{R} - \frac{1}{2} + \frac{1}{S} = \frac{1}{E} \quad (5)$$

and thus

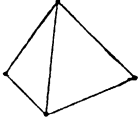
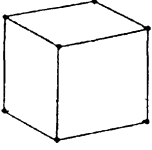
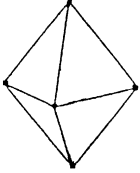
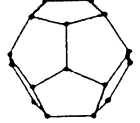
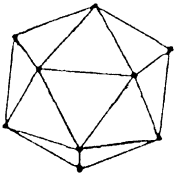
$$\frac{1}{2} + \frac{1}{R} + \frac{1}{S} - \frac{1}{E} = 1. \quad (6)$$

We claim that $E = \text{lcm}(2, R, S)$. To see this, first, from geometric symmetry considerations, observe that F , E , and V are all even. Thus, (4) shows that E is a common multiple of 2, R , and S . But by (5), E is also a divisor of $\text{lcm}(2, R, S)$. Thus $E = \text{lcm}(2, R, S)$, and equation (7) is revealed as a special case of our equation (3).

In fact, every solution of length 3 to equation (3) arises in this way, except for the infinite family $(2, 2, 2n)$, $n = 1, 2, \dots$. We do not know any deep geometric explanation of this observation; perhaps it is merely a coincidence based on the fact that there are only a few solutions to the inequality

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} > 1.$$

TABLE 1:

$\frac{1}{2} + \frac{1}{3} + \frac{1}{3} - \frac{1}{6} = 1$		Tetrahedron: triangles meeting 3 at a point.
$\frac{1}{2} + \frac{1}{3} + \frac{1}{4} - \frac{1}{12} = 1$		Cube: squares meeting 3 at a point.
$\frac{1}{2} + \frac{1}{4} + \frac{1}{3} - \frac{1}{12} = 1$		Octahedron: triangles meeting 4 at a point.
$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} - \frac{1}{30} = 1$		Dodecahedron: pentagons meeting 3 at a point.
$\frac{1}{2} + \frac{1}{5} + \frac{1}{3} - \frac{1}{30} = 1$		Icosahedron: triangles meeting 5 at a point.

For $k > 3$ the first systematic search for solutions to equations (2) and (3) was undertaken in the 1880s by J. J. Sylvester [22], a founder of the American Mathematical Society. Sylvester considered the sequence $\{2, 3, 7, 43, \dots\}$ defined recursively by $A_1 = 2, A_{n+1} = 1 + \prod_{i=1}^n A_i$. It is easy to check that for each k , the finite sequence $\{A_1, \dots, A_k\}$ is a solution to equation (2). Similarly, two infinite sets of solutions to equation (3) are given by $\{A_1, \dots, A_{k-1}, A_k - 2\}$, $3 \leq k < \infty$, and $\{A_1, \dots, A_{k-2}, 2A_{k-1} - 3, 2A_{k-1} - 1\}$, $4 \leq k < \infty$.

Znam's problem

Slovak mathematician Stefan Znam is credited with posing the following problem in the theory of systems of congruences: find all sequences $\{n_1, \dots, n_k\}$ of integers ≥ 2 with the property that for each i , n_i properly divides $1 + \prod_{j \neq i} n_j$. Here $\prod_{j \neq i} n_j$ denotes the deleted product $n_1 n_2 \dots n_{i-1} n_{i+1} \dots n_k$.

For example, $\{2, 3, 11, 23, 31\}$ is a solution to Znam's problem, because

- (leave out 2) $1 + 3 \times 11 \times 23 \times 31 = 23530$, which is divisible by 2.
- (leave out 3) $1 + 2 \times 11 \times 23 \times 31 = 15687$, which is divisible by 3.
- (leave out 11) $1 + 2 \times 3 \times 23 \times 31 = 4279$, which is divisible by 11.
- (leave out 23) $1 + 2 \times 3 \times 11 \times 31 = 2047$, which is divisible by 23.
- (leave out 31) $1 + 2 \times 3 \times 11 \times 23 = 1519$, which is divisible by 31.

All known solutions to Znam's problem produce solutions to equation (2), but a more exact relationship is not known. Suppose that n_1, \dots, n_k is a fixed solution to Znam's problem, and for $1 \leq i \leq k$, put $X_i = \prod_{j \neq i} n_j$. First, it is clear that the n_i s are relatively prime in pairs, because if $d > 1$ were a common divisor of n_i and n_j , then, since n_i divides $1 + X_i$, so does d . But by definition n_j is one of the factors of X_i , so we conclude that d divides both X_i and $1 + X_i$, an impossibility.

Now consider the integer $N = 1 + \sum_{i=1}^k X_i$. As above, for each i , n_i divides N , since for $j \neq i$ the term X_j contains n_i as a factor, while by assumption n_i also divides $1 + X_i$. Thus, since the n_i s are relatively prime, $\prod_{i=1}^k n_i$ also divides N . If we write $N = r \prod_{i=1}^k n_i$ and divide by $\prod_{i=1}^k n_i$, we obtain the unit fraction equation

$$\sum_{i=1}^k \frac{1}{n_i} + \frac{1}{\prod_{i=1}^k n_i} = r. \quad (7)$$

Now $\text{lcm}(n_1, n_2, \dots, n_k) = \prod_{i=1}^k n_i$ for relatively prime n_i , so if $r = 1$ then these integers satisfy the unit fraction equation (2).

Can $r > 1$ ever occur? This is an unsolved problem. No solution to (7) is known in integers $n_i \geq 2$ for $r > 1$. If n_1, \dots, n_k is such a solution, then, again since the n_i s are relatively prime, the largest possible value of $\sum_{i=1}^k 1/n_i + 1/\prod_{i=1}^k n_i$ is the corresponding sum for the first k primes:

$$\sum_{i=1}^k \frac{1}{n_i} + \frac{1}{\prod_{i=1}^k n_i} \leq \sum_{i=1}^k \frac{1}{p_i} + \frac{1}{\prod_{i=1}^k p_i},$$

where p_i is the i th prime. This sum is less than 2 for $k \leq 58$ ($\sum_{i=1}^{58} \frac{1}{p_i} = 1.998740043 \dots$). Thus without loss of generality we may take $r = 1$ in equation (7) when searching for solutions to Znam's problem of small length:

$$\sum_{i=1}^k \frac{1}{n_i} + \frac{1}{\prod_{i=1}^k n_i} = 1. \quad (8)$$

This is the special case of Horus' equation (2) in which the n_i s are relatively prime. (If all of the n_i s happen to be prime then the resulting product $N = \prod_{i=1}^k n_i$ is called a *primary pseudoperfect number* [8].)

Conversely, any solution $n_1 < n_2 < \dots < n_k$ of equation (8) is a solution to Znam's problem unless $n_k = 1 + \prod_{i=1}^{k-1} n_i$, in which case n_k does not *properly* divide this last expression as required in Znam's original formulation of the problem.

Modern history

Znam posed his problem in 1972. In 1983, Sun [21] proved that there are infinitely many solutions to Znam's problem. The proof is as follows: Consider again the Sylvester sequence $2, 3, 7, 43, 1807, 3263443, \dots, A_n, A_{n+1} = 1 + \prod_{i=1}^n A_i, \dots$. First we claim that for all $n \geq 1$, A_{2n} ends in a 3 and A_{2n+1} ends in a 7, which is easy to prove by induction. For $n = 1$, we have $A_2 = 3$ and $A_3 = 7$. Now let $n > 1$ and assume that the claim is true for all $i < n$. Then computing mod 10 we have

$$A_{2n} = 1 + \prod_{i=1}^{2n-1} A_i \equiv 1 + 2 \times 3^{n-1} \times 7^{n-1} \equiv 1 + 2 \times 21^{n-1}$$

$$\equiv 1 + 2 \times 1^{n-1} \equiv 3 \pmod{10}; \quad \text{and}$$

$$A_{2n+1} = 1 + \prod_{i=1}^{2n} A_i \equiv 1 + 2 \times 3^n \times 7^{n-1} \equiv 1 + 6 \times 21^{n-1} \equiv 1 + 6 \equiv 7 \pmod{10},$$

as required.

From this it follows that $\prod_{i=1}^{2n-1} A_i = A_{2n} - 1$ ends in a 2, and hence the integer $1 + \prod_{i=1}^{2n-1} A_i^2 \equiv 1 + 2^2 \pmod{10}$, ends in a 5. Thus the rational expression $(1 + \prod_{i=1}^{2n-1} A_i^2)/5$ is actually an integer. Sun then proceeded to show that for all $n > 1$ the sequence $\{A_1, A_2, \dots, A_{2n-1}, B_n, C_n\}$ is a solution to Znam's problem for

$$B_n = 5 + \prod_{i=1}^{2n-1} A_i, C_n = \prod_{i=1}^{2n-1} A_i + \left(1 + \prod_{i=1}^{2n-1} A_i^2\right)/5.$$

To see this, we use the fact that the first $2n - 1$ terms of the Sylvester sequence satisfy equation (8):

$$\sum_{i=1}^{2n-1} \frac{1}{A_i} + \frac{1}{\prod_{i=1}^{2n-1} A_i} = 1.$$

Now put $P = \prod_{i=1}^{2n-1} A_i$ and compute

$$\begin{aligned} & \sum_{i=1}^{2n-1} \frac{1}{A_i} + \frac{1}{B_n} + \frac{1}{C_n} + 1/B_n C_n \prod_{i=1}^{2n-1} A_i \\ &= 1 - \frac{1}{P} + \frac{1}{P+5} + \frac{1}{P+(1+P^2)/5} + \frac{1}{P(P+5)(P+(1+P^2)/5)} \\ &= 1 - \frac{1}{P} + \frac{1}{P+5} + \frac{5}{P^2+5P+1} + \frac{5}{P(P+5)(P^2+5P+1)} \\ &= 1 + \frac{-(P+5)(P^2+5P+1) + P(P^2+5P+1) + 5P(P+5) + 5}{P(P+5)(P^2+5P+1)} = 1. \end{aligned}$$

Thus $\{A_1, \dots, A_{2n-1}, B_n, C_n\}$ is a solution to Znam's problem, as claimed. The first solution of this type is $\{2, 3, 7, 5 + 2 \times 3 \times 7, 42 + (1 + 42^2)/5\} = \{2, 3, 7, 47, 395\}$. The second ($n = 3$) is $\{2, 3, 7, 43, 1807, 3263447, 2130014000915\}$.

In 1978 Janek and Skula found all solutions to Znam's problem of length $k \leq 6$. They are

$k = 5$	$k = 6$
2, 3, 7, 47, 395	2, 3, 7, 47, 3952, 3, 7, 43, 1823, 193667
2, 3, 11, 23, 31	2, 3, 11, 23, 312, 3, 7, 47, 403, 19403
	2, 3, 7, 47, 415, 8111
	2, 3, 7, 47, 583, 1223
	2, 3, 7, 55, 179, 24323

After several new solutions of length 7 were found by Cao, Liu, and Zhang [10], the list of all solutions of length 7 was published by Brenton and Hill [6]. Another geometric application is given by Brenton and Hill in the same paper, this time to the subject of the topological structure of four-dimensional singularities (see also [3]). Further applications in number theory and graph theory appear in [7].

The main purpose of this paper is to extend these results to the case $k = 8$. There are exactly 119 solutions of length 8 to equation (8), of which 93 are solutions to Znam's problem. They are listed on our website at www.dept.math.wayne.edu/ugresearch.

There is also considerable interest in finding exotic solutions of greater length. For instance, all solutions of length ≤ 9 are known to start with $n_1 = 2$. (All but six have $n_1 = 2$ and $n_2 = 3$ [7].) But in 1996 Rolland Girgensohn [12] discovered the remarkable solution,

{3, 4, 5, 7, 29, 41, 67, 89701, 230865947737, 5726348063558735709083, 172509500849902989281836693100308633431804359, 428596832385786878003 379724333422434733374132288492887588514414196525736338894723726187, 4754717350939481607957800419492385085075824146211772113509986641996 6609382912418290571285921576904572237676355786179525975342527449296 80110197649133558287624332177380360519}.

It remains an open question whether there is a solution in all odd numbers.

The search for solutions

Sun's method illustrated above also suggests a technique for an exhaustive computer search for solutions for fixed k . Let $n_1 < n_2 < \cdots < n_{k-2}$ be a sequence of relatively prime integers such that $\sum_{i=1}^{k-2} 1/n_i < 1$. We wish to "complete the expression to unity" by finding integers $x = n_{k-1}$ and $y = n_k$ such that

$$\sum_{i=1}^{k-2} \frac{1}{n_i} + \frac{1}{x} + \frac{1}{y} + \frac{1}{xy \prod_{i=1}^{k-2} n_i} = 1.$$

Denote $\prod_{i=1}^{k-2} n_i$ by P and define D by requirement $1 - \sum_{i=1}^{k-2} 1/n_i = D/P$. Clearing denominators, this gives $yP + xP + 1 = Dxy$. Multiplying by D and rearranging, $D^2xy - PDx - PDy = D$. This quadratic form can be solved by completing the square

$$\begin{aligned} 0 &= D^2xy - DPx - DPy + P^2 - P^2 - D \\ &= Dx(Dy - P) - P(Dy - P) - P^2 - D \\ &= (Dx - P)(Dy - P) - P^2 - D. \end{aligned}$$

That is,

$$(Dx - P)(Dy - P) = D + P^2.$$

Thus for every way to factor $D + P^2 = F \times G$ we obtain candidates for x and y by putting $Dx - P = F$, $Dy - P = G$. This gives the rational solution $x = (F + P)/D$, $y = (G + P)/D$. In order to obtain a solution in *integers*, D must divide $F + P$ and $G + P$. That is, using the language of congruences, the factors F and G must satisfy $F, G \equiv -P \pmod{D}$. For the examples of Sun, $D = 1$, $F = 5$, and $G = (1 + P^2)/5$. It can also be shown [6] that if $n_1 < n_2 < \cdots < n_k$ is a solution to Znam's problem then for each $i \leq k - 2$, n_i falls in the range

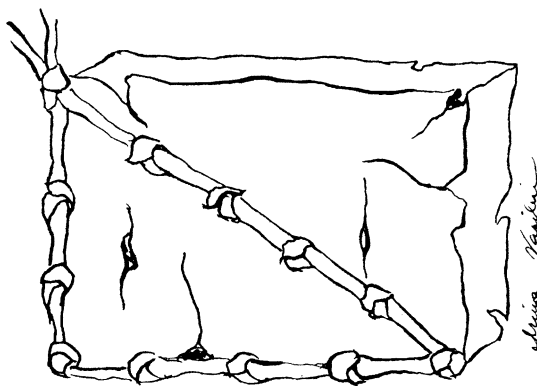
$$\left(1 - \sum_{j=1}^{i-1} \frac{1}{n_j}\right)^{-1} < n_i < (k - i) \left(1 - \sum_{j=1}^{i-1} \frac{1}{n_j}\right)^{-1}.$$

Thus for fixed k there are only finitely many initial sequences n_1, n_2, \dots, n_{k-2} that can be completed in two steps to a solution to Znam's problem. To find the missing two terms, compute $D + P^2$ and factor it. If $D + P^2$ has any divisor $F \equiv -P \pmod{D}$, then (and only then) we obtain a new solution.

For $k = 8$ the Wayne State University Undergraduate Research Group worked on this problem for several months, using a program written in *Maple* running on a system of Sun Sparc stations. We have recently completed this investigation. The list of all solutions to Znam's problem of length ≤ 8 may be found at our website [23]. The last several solutions completing the list were discovered by Blake Spraggins and Ana Vasiliu in the summer of 1998, and were presented at the 9th Annual Argonne Symposium for Undergraduates in Science, Engineering and Mathematics, Argonne National Laboratory, November 6 and 7, 1998, by Vanessa Stachel and Ana Vasiliu.

Application

A thousand years before Pythagoras, the Egyptians knew that $3^2 + 4^2 = 5^2$ and understood the significance of this relation for right triangles. Indeed, there are apocryphal stories that Egyptian architectural engineers used this result to make sure that stones used for building purposes were cut perfectly square. Supposedly, the special assistants to the mathematician-scribes called "rope-stretchers" carried a closed loop of rope in which 12 equally spaced knots were tied. To test whether a quarried block was square, the rope was stretched across a corner. If it fit, the angle was exactly 90 degrees.



Similarly, we have $3^3 + 4^3 + 5^3 = 6^3$ as another example of a curious relation among powers of consecutive integers.

In 1950 Paul Erdős conjectured that the equation

$$1^n + 2^n + \dots + m^n = (m+1)^n \quad (9)$$

has no solution in positive integers (n, m) except for the trivial solution $1 + 2 = 3$. It was shown by Leo Moser [16] that if (n, m) is a solution then the prime factors p_i of m satisfy equation (7). Cao Zhenfu [9] used our derivation of all solutions to Znam's problem of length 8 to prove that in any solution to the Erdős-Moser equation, m must have at least 9 prime factors. This result can be substantially improved as follows. Applying the technique of Moser, our colleagues William Butske, Linda Jaje, and Daniel Mayernik [8] showed that

$$m > 10^{9321155}.$$

By a result conjectured by Kellogg [15] and proved by Curtiss [11] (and independently by Tanzo Takenouchi), the Sylvester solution $\{2, 3, 7, 43, 1807, \dots, A_k\}$ maximizes the product $n_1 n_2 n_3 \dots n_k$ among all solutions of equation (8) of length k . Thus if we have a solution m to equation (6) with k prime factors then

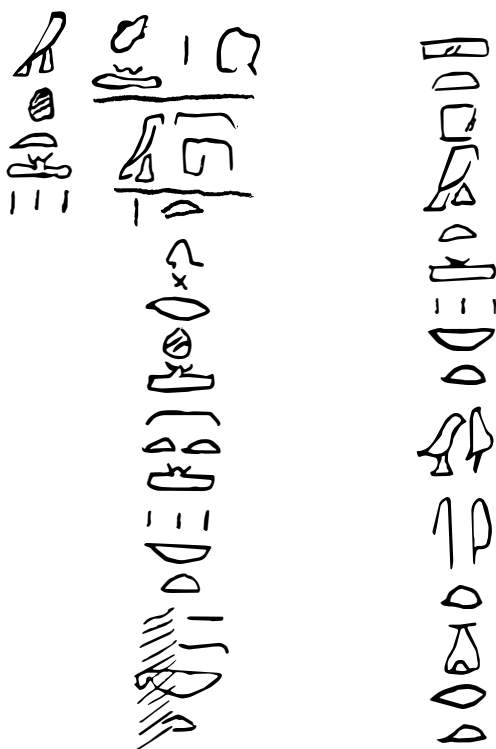
$$m \leq 2 \times 3 \times 7 \times \dots \times A_k = A_{k+1} - 1 < (1.066 \times 10^{13})^{2^{(k-6)}}.$$

Hence

$$(1.066 \times 10^{13})^{2^{(k-6)}} > 10^{9321155}$$

and solving for k gives $k > 25.44$.

Thus any counterexample to Erdős' conjecture must be the product of at least 26 prime factors. This is a modern result whose proof lends support to the claim of the scribe Ahmose (1500 BCE) that the study of unit fractions will reveal



(“Rules for enquiring into nature, and for knowing all that exists, [every] mystery, ... every secret.” —translation by Peet [18].)

Acknowledgments. Pictures of Thoth and the brick are by Irina Vasiliu. We would like to thank the referees for suggesting improvements to the original version of this paper, especially to the section on regular polyhedra.

REFERENCES

1. P. Anne, Egyptian fractions and the inheritance problem, *College Math. J.* **29** (1998), 296–300.
2. D. Borwein, J. Borwein, P. Borwein, and R. Girgensohn, Giuga's conjecture on primality, *Amer. Math. Monthly* **103** (1996), 40–50.

3. L. Brenton, Homologically simple singularities, *Classical and Quantum Gravity* **18** (2001), 325–340.
4. L. Brenton and R. Bruner, On recursive solutions of a unit fraction equation, *J. Austral. Math. Soc. (Ser. A)* **57** (1994), 341–356.
5. L. Brenton and D. Drucker, On the number of solutions of $\sum_{j=1}^s (1/x_j) + 1/(x_1 \dots x_s) = 1$, *J. Number Theory* **44**:1 (1993), 25–29.
6. L. Brenton and R. Hill, On the Diophantine equation $1 = \sum (1/n_i) + 1/(\prod n_j)$ and class of homologically trivial complex surface singularities, *Pacific J. Math.* **133**:1 (1988), 41–67.
7. L. Brenton and L. Jaje, Perfectly weighted graphs, to appear in *Graphs and Combinatorics*.
8. W. Butske, L. Jaje, and D. Mayernik, On the equation $\sum_{p|N} \frac{1}{p} + \frac{1}{N} = 1$, pseudoperfect numbers and perfectly weighted graphs, *Math. of Comp.* **69** (2000), 407–420.
9. Z. Cao, Harbin Inst. of Tech., Harbin, China, personal communication (1999).
10. Z. Cao, R. Liu, and L. Zhang, On the equation $\sum_{j=1}^s (1/x_j) + 1/(x_1 \dots x_s) = 1$ and Znam's problem, *J. Number Theory* **27**:2 (1987), 206–211.
11. D. Curtiss, On Kellogg's Diophantine problem, *Amer. Math. Monthly* **29** (1922), 380–387.
12. R. Girgensohn, Medizinische Univ. Lubeck, Lubeck, Germany, personal communication (1996).
13. M. Henle, *A Combinatorial Introduction to Topology*, Dover Publications, Inc., New York, 1979.
14. J. Janak and L. Skula, On the integers x_i for which $x_i | x_1 \dots x_{i-1} x_{i+1} x_n + 1$ holds, *Math. Slovaca* **28**:3 (1978), 305–310.
15. O. Kellogg, On a Diophantine equation, *Amer. Math. Monthly* **28** (1921), 300–303.
16. L. Moser, On the Diophantine equation $1^n + 2^n + 3^n + \dots + (m-1)^n = m^n$, *Scripta Math.* **19** (1953), 84–88.
17. K. Paul, *The Book of the Dead; an English Translation of the Chapters, Hymns, etc., of the Theban Recession*, E. P. Dutton & Co., New York, 1928.
18. E. Peet, *The Rhind Mathematical Papyrus*, British Museum 10057 & 10058, Hadder & Stoughton Limited, London, 1923.
19. L. Pisano, *Scritti (Liber Abaci)*, Vol. 1, B. Boncompagni, Rome (1857).
20. G. Robins and C. Shute, *The Rhind Mathematical Papyrus, an Ancient Egyptian Text*, British Museum Publications, London, 1987.
21. Q. Sun, On a problem of Znam, *Sichuan Daxue Xuebao* **4** (1983), 9–11.
22. J. Sylvester, On a point in the theory of vulgar fractions, *Amer. J. Math* **3** (1880), 332–335, 388–389.
23. *The Wayne State University Undergraduate Research Group*, www.dept.math.wayne.edu/ugresearch.

Letter to the Editor

Dear Editor:

A. A. Kosinski provided some interesting and valuable information about Gabriel Cramer in “Cramer’s Rule is Due to Cramer” (this MAGAZINE, October 2001). However, the note did not address the most controversial and bitter question: Is the man’s name pronounced CRAY-mer or krah-MARE? The MARE party believes that the CRAY people are displaying typical Anglo-Saxon uncultured illiteracy. The CRAYs say that the MAREs are displaying pretentious ignorance, like those Z-phobes who insist on referring to the composers Boulez and Glazunov as boo-LAY and Glottsanoff. Each party accuses the other of confusing the eighteenth century Cramer with the twentieth century Swedish statistician H. Cramer, whose name (allegedly) is really pronounced the other way. Can Professor Kosinski, or anybody else authoritatively settle this issue? It is encrusted with about as much pseudoinformation as Nobel’s relationship to Mittag-Leffler.

S. A. Fulling
Texas A&M University
College Station, TX 77843-3368

The Josephus Problem: Once More Around

PETER SCHUMER

Department of Mathematics and Computer Science
Middlebury College
Middlebury, VT 05753
schumer@middlebury.edu

The Jewish soldier and historian Josephus Flavius (ca. 37 CE–ca. 95 CE) lived an exciting and tumultuous life and inspired an interesting set of mathematical problems.

Born in Jerusalem, Joseph ben Matthias studied Hebrew and Greek literature as a young child and then spent three years (from the ages of 16 to 19) living an ascetic lifestyle with a fellow hermit in the desert. After further study as a member of the Pharisee sect, he served as delegate to Nero, was chosen governor of Galilee, and rose to the rank of general to help lead the Jewish revolt against Rome in the year 66.

A year later, he was a member of the resistance at the siege of Jotapata that held out for 47 days. According to Josephus [5], the doomed soldiers decided to take their own lives rather than be captured by the Romans and suffer an uncertain and inglorious future. Josephus exclaimed, “Let us commit our mutual deaths to determination by lot. He whom the lot falls to first, let him be killed by him that hath the second lot, and thus fortune shall make its progress through us all.” By chance or fate or providence, “[Josephus] with another was left to last. And as [Josephus] was very desirous neither to be condemned to the lot, nor, if he had been left to the last, to imbrue his right hand in the blood of his countryman, [Josephus] persuaded him to trust the Roman assurances, and to live as well as himself” [5]. Josephus surrendered to Vespasian, traveled extensively with him, and served under Vespasian when the latter became emperor. Josephus also served under the next emperor, Titus, the son of Vespasian, and took his family name of Flavius as his own.

Josephus was in Jerusalem (as a Roman citizen) during the bloodiest battles in the year 70, traveled to Rome for the beginning of the construction of the Coliseum, survived a tragic ship wreck, was married at least three times, and lived a life full of excitement and intrigues. More importantly, he wrote several books including *A History of the Jewish War*, *Contra Apionem* (a response to the anti-Semitic agitator Apion), *Antiquities of the Jews*, and an *Autobiography*.

Differing accounts and new problems

The details of exactly how Josephus’s life was spared vary greatly from one source to another. In [4] it is stated, “In the Jewish revolt against Rome, Josephus and thirty-nine of his comrades were holding out against the Romans in a cave. With defeat imminent, they resolved that, like the rebels at Masada, they would rather die than be slaves to the Romans. They decided to arrange themselves in a circle. One man was designated as number one, and they proceeded clockwise around the circle of forty men, killing every seventh man. Josephus . . . instantly figured out where he ought to sit to be the last to go.” (You may wish to verify that he should place himself in position number 24.) In another source [6], there are 41 men and every third man in turn is killed. Josephus must figure out immediately where he and a close friend must stand to be the last two chosen. (In this case, the solution is to stand in positions 16 and 31.)

A Medieval version of the “Josephus problem” is recounted [6] in which “15 Turks and 15 Christians are on board a storm-ridden ship which is certain to sink unless half

the passengers are thrown overboard.” All 30 stand in a circle and decide that every ninth person will be tossed to sea. The problem is to determine where the Christians should stand to ensure that all the Turks are first to go.

The most intricate variation of the Josephus problem appears in the Japanese text, *Treatise on Large and Small Numbers* (1627), by Yoshida Koyu. According to [1], in this version of the problem there is a family of 30 children, half from a former marriage. To choose one child to inherit the parent’s estate, they are arranged in a circle with every tenth child eliminated. The current wife arranges things so that all fifteen children from the first marriage are taken out first. However, after fourteen children are thus eliminated, the father catches on and decides to reverse the order and count in a counterclockwise direction. Even so, a child from the first marriage is eventually chosen.

Some version of the mathematical Josephus problem dates back to Abraham ibn Ezra (ca. 1092–1167), the prolific Jewish scholar and author of works on astrology, the cabala, philosophy, and mathematics. As reported by Smith [7], a work from this period entitled *Ta’hbula* contains the Josephus problem and is presumed to be written by Abraham ibn Ezra. Even so, despite the antiquity of the problem, not much attention was paid to mathematical versions of the Josephus problem until the late nineteenth century and scant reference is made to this intriguing problem in modern textbooks.

One very notable exception is a text by Graham, Knuth, and Patashnik, *Concrete Mathematics: A Foundation for Computer Science* [3], which makes a thorough study of the “standard” Josephus problem and then extends it in order to discuss general recurrence relations. The standard Josephus problem is to determine where the last survivor stands if there are n people to start and every second person is eliminated. If we let $J(n)$ be the position of the last survivor, the result is that if $n = 2^a + t$, where $0 \leq t < 2^a$, then $J(n) = 2t + 1$. The proof is as elegant as the result and is a very nice application of mathematical induction.

More generally (and less violently), suppose n people numbered one through n stand around a circle. Person number q knows some gossip and tells it to the person q spaces ahead clockwise around the circle, who then tells it to the next person remaining q spaces ahead, etc. In fact, q may be larger than n , in which case the person numbered d is actually numbered d (modulo n). Here we let $J(n, q)$ denote the position of the last person to hear the latest scoop. (So for example, $J(n) = J(n, 2)$.) Calculation of $J(n, q)$ for various values of n and q can be time-consuming and there doesn’t appear to be a nice closed formula in general. However, the following result is most useful.

PROPOSITION 1. For $n \geq 1$, $q \geq 1$, $J(n + 1, q) \equiv J(n, q) + q \pmod{n + 1}$.

Proof. Consider $n + 1$ people in a circle with every q th being eliminated in turn. The first person eliminated is person $q \pmod{n + 1}$. Now we have reduced the problem to the $J(n, q)$ problem, except that the people are numbered $q + 1$, $q + 2$, etc. rather than 1, 2, etc. Hence, $J(n + 1, q) \equiv J(n, q) + q \pmod{n + 1}$. ■

For the standard Josephus problem, $q = 2$, and so Proposition 1 implies that $J(n + 1) \equiv J(n) + 2 \pmod{n + 1}$, an interesting way to interpret the result stated earlier [3]. Note that we use the complete set of residues $\{1, 2, \dots, n + 1\}$ modulo $n + 1$.

Here is another example showing the utility of Proposition 1. Suppose we wish to make a chart of $J(n, 5)$ for various values of n , starting with 1. We do not need to draw circle after circle (in some sense reinventing the wheel), one for each successive value of n . Instead, since $J(1, 5) = 1$, we can apply Proposition 1 repeatedly to obtain $J(2, 5) \equiv 1 + 5 \equiv 2 \pmod{2}$, $J(3, 5) \equiv 2 + 5 \equiv 1 \pmod{3}$, $J(4, 5) \equiv 1 + 5 \equiv 2 \pmod{4}$, and so on. See TABLE 1.

TABLE 1:

n	1	2	3	4	5	6	7	8	9	10	11	12
$J(n, 5)$	1	2	1	2	2	1	6	3	8	3	8	1

Proposition 1 can be easily extended. Let $J(n, q, k)$ denote the position of the k th from last person to be chosen when there are n people and every q th person is eliminated. So $J(n, q, 1) = J(n, q)$. Then

PROPOSITION 2. For $n \geq 1, q \geq 1$: $J(n + 1, q, k) \equiv J(n, q, k) + q \pmod{n + 1}$.

The proof is identical to the proof of Proposition 1.

By way of illustration, TABLE 2 gives the positions of the second from last person to be eliminated when $q = 3$.

TABLE 2:

n	2	3	4	5	6	7	8	9	10	11	12	13
$J(n, 3, 2)$	1	1	4	2	5	1	4	7	10	2	5	8

Josephus permutations

There are a host of interesting variations and questions relating to the Josephus problem. Let us begin by defining the Josephus permutation $P(n, q)$ as the permutation on the numbers 1 through n created by applying the Josephus elimination procedure to every q th number. Alternatively, we can think of this as a “Josephus shuffle” where we take n cards numbered 1 through n and place every q th card face down on a table. The resulting ordering of the cards is the appropriate Josephus permutation.

For example,

$$P(7, 2) = \left(\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 5 & 3 & 7 \end{array} \right) \quad \text{and}$$
$$P(8, 9) = \left(\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 6 & 4 & 5 & 2 & 7 & 8 \end{array} \right).$$

Are all permutations of 1 to n realizable as Josephus permutations for appropriate q ? A simple counting argument shows otherwise. Of course there are $n!$ distinct permutations of the numbers $1, \dots, n$. However, there are precisely $L(n) = \text{lcm}[1, 2, 3, \dots, n]$ distinct Josephus permutations. To see this note that $P(n, q) = P(n, q + L(n))$ since at each step (say k) of the elimination ($1 \leq k \leq n$), we simply spin around the circle $L(n)/(n + 1 - k)$ times before moving q places beyond our previous position. Furthermore, if $q \not\equiv q' \pmod{L(n)}$, then $P(n, q)$ is not the same as $P(n, q')$. To see this note that there is a k with $1 \leq k \leq n$ such that $q \not\equiv q' \pmod{k}$. But then on the $(n + 1 - k)$ th step with k people remaining, $P(n, q)$ and $P(n, q')$ will differ. In any event, since $n! > L(n)$ for all $n > 3$, there are some permutations which are not Josephus permutations.

More concretely, notice that $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ is not a Josephus permutation $J(4, q)$ for any q . If it were, then $q \equiv 2 \pmod{4}$, $q \equiv 1 \pmod{3}$, and $q \equiv 1 \pmod{2}$. But the first and third congruences would imply that q were simultaneously even and odd respectively, a contradiction.

Subsets marked for elimination

Other variations of the Josephus problem involve eliminating a prescribed half of the participants first. For example, if n is even, say $n = 2k$, can we eliminate the first k people leaving the second k intact? This is easy of course—just let $q = 1$.

Well then, given $n = 2k$ people, can we find a value of q that eliminates the second half of the circle first? This is not as simple, but if we let

$$q = L(n) = \text{lcm}[1, 2, \dots, n], \quad \text{then} \quad P(n, q) = \begin{pmatrix} 1 & 2 & \cdots & 2k-1 & 2k \\ 2k & 2k-1 & \cdots & 2 & 1 \end{pmatrix}$$

and so the people are eliminated in reverse order, thus removing the second half of the circle first.

With n even, can we eliminate all the even-numbered people first without disturbing any of the odd-numbered people? Again the solution is straightforward, just let $q = 2$, as we have discussed previously.

But what if $n = 2k$ and we want to eliminate all the odd-numbered people first? This is more interesting. If we want to eliminate the odd-numbered people in ascending order, then for $n = 4$, we immediately discover $P(4, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$. But if $P(6, q)$ were to be of the form $P(6, q) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & E & E & E \end{pmatrix}$ where E stands for an unspecified even number, it must be the case that $q \equiv 1 \pmod{6}$, $q \equiv 2 \pmod{5}$, and $q \equiv 2 \pmod{4}$. Then q is both odd and even, an impossibility. Yet we can still eliminate the odd numbers first as demonstrated by $P(6, 19) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 6 & 2 \end{pmatrix}$. Similarly, one can discover “by hand” that $P(8, 27) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 7 & 4 & 2 & 6 & 8 \end{pmatrix}$ and $P(10, 87) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 3 & 1 & 5 & 9 & 2 & 8 & 6 & 10 & 4 \end{pmatrix}$. In fact, we have given the smallest value of q that does the trick for each appropriate n . Since there are $k!$ ways to permute the k odd numbers $1, 3, 5, \dots, 2k-1$, and many permutations lead to contradictory congruences for q , the situation quickly becomes computationally more difficult. Even so, let’s go a bit further.

With some work, for the case $n = 12$, we discover that $q \equiv 5 \pmod{12}$, $q \equiv 8 \pmod{11}$, $q \equiv 5 \pmod{10}$, $q \equiv 2 \pmod{9}$, $q \equiv 5 \pmod{8}$, and $q \equiv 5 \pmod{7}$ is consistent in that it follows that $q \equiv 1 \pmod{2}$, $q \equiv 2 \pmod{3}$, and $q \equiv 1 \pmod{4}$. The Chinese remainder theorem guarantees a unique solution modulo $\text{lcm}[12, 11, 10, 9, 8, 7] = L(12) = 27,720$. In fact, $q = 16,805$ works. The resulting permutation is

$$P(12, 16805) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 1 & 7 & 9 & 3 & 11 & 8 & 6 & 10 & 2 & 4 & 12 \end{pmatrix}.$$

Similarly, for the case $n = 14$, requiring $q \equiv 13 \pmod{14}$, $q \equiv 8 \pmod{13}$, $q \equiv 9 \pmod{12}$, $q \equiv 2 \pmod{11}$, $q \equiv 5 \pmod{10}$, $q \equiv 3 \pmod{9}$, and $q \equiv 1 \pmod{4}$ leads to a consistent set of simultaneous congruences that together eliminate all odd numbered positions first. Here we get $q = 167,565 \pmod{360,360}$. The resulting permutation is

$$P(14, 167565) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 13 & 7 & 3 & 5 & 11 & 1 & 9 & 6 & 12 & 10 & 14 & 8 & 2 & 4 \end{pmatrix}.$$

In the last two examples, there was no guarantee that the values of q found were the smallest values that would eliminate all the odd numbers first. My colleague at Middlebury College, Frank Swenton, made a computer search to find just that. His initial results are shown in TABLE 3.

In fact, there is a complete solution to the problem of eliminating all odd numbers first if we aren’t concerned with finding the smallest solution. If $n = 2k$, the

TABLE 3:

n	smallest q that eliminates odds first
2	1
4	5
6	19
8	27
10	87
12	989
14	3,119
16	5,399
18	8,189
20	99,663
22	57,455
24	222,397
26	2,603,047
28	8,476,649
30	117,917,347
32	290,190,179
34	360,064,247
36	1,344,262,919
38	3,181,391,639
40	? (larger than 10 billion)

idea is to find a value of q for which $q \equiv -1 \pmod{2k}$, $q \equiv -1 \pmod{2k-1}$, $q \equiv -1 \pmod{2k-2}$, \dots , $q \equiv -1 \pmod{k+1}$. Such a value of q would have the effect of eliminating all the odd numbers in descending order beginning with $2k-1$ before eliminating any even numbers.

PROPOSITION 3. Given $n = 2k$, let $q = L(n) - 1$ where $L(n) = \text{lcm}[1, 2, \dots, n]$. Then

$$P(n, q) = \begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots & 2k \\ 2k-1 & 2k-3 & \dots & 1 & E & \dots & E \end{pmatrix}.$$

Proof. Let d denote the d th stage of the Josephus process for $1 \leq d \leq k$. We use induction on d . The first number eliminated is $2k-1$ and so the result holds for $d=1$. Assume it holds for all values up to some value d . At this point we last eliminated the odd number $2k-2d+1$, all larger odd numbers have been eliminated, and all other numbers between 1 and $2k$ inclusive remain. The q th number is now two places behind the last number removed and so the $(d+1)$ st number eliminated is $2k-2(d+1)+1$ as required. ■

For example, if $n = 16$ then $q = L(16) - 1 = 720,719$ and

$$P(16, 720719) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 15 & 13 & 11 & 9 & 7 & 5 & 3 & 1 & 14 & 10 & 6 & 2 & 12 & 4 & 8 & 16 \end{pmatrix}.$$

Of course the even-numbered people might collapse from exhaustion before ever being chosen.

Another interesting question is this: Given n (the total number of people) and m (the position you find yourself), is there always a q for which $J(n, q) = m$? In other words, can you always save yourself if you are allowed to specify the value of q ?

The answer is yes and the solution can be found in [3]. Briefly the solution goes as follows: Let $L(n) = \text{lcm}[1, \dots, n]$ as before. Assume (for now) that $m > n/2$. By Bertrand's Postulate (conjectured by Bertrand in 1845 and proved by Chebyshev in 1850), there is a prime p with $n/2 < p < n$. Choose q with $q \equiv 1 \pmod{L/p}$ and $q \equiv m + 1 - n \pmod{p}$. Since p and L/p are relatively prime, by the Chinese remainder theorem, there is a simultaneous solution mod L . For this value of q , the Josephus process removes the people in the order $1, 2, \dots, n - p$, and then everyone else starting at person $m + 1$ and moving clockwise around the circle, hence ending at person m . (A slight modification can be made to handle the case when $m \leq n/2$.)

Further circlings

The Josephus problem and its many variants would make a nice chapter in many mathematics and computer science courses. The standard Josephus problem ($q = 2$) has a very elegant interpretation in terms of the binary representation of n . Take a moment to discover it for yourself.

The Josephus permutations are beautiful and concrete examples of permutations in an abstract algebra course. It may be of interest to note that the set of such permutations form a subgroup of the full symmetric group on n for $n = 3, 4$, and 5 . However, Frank Swenton again, has confirmed that this pattern does not carry over beyond $n = 5$. Even so, the cycle structure of $P(n, q)$ has been studied for some special cases (see Herstein and Kaplansky [4]).

Another question: how many fixed points can we expect in a Josephus permutation (equivalently, a Josephus shuffle)? If we randomly shuffle an n -card deck we expect to have one fixed point, that is, a single card remaining in its original position. To see this, let the random variable X_i be 1 if after shuffling the i th card ends up in the i th place and 0 if the i th card ends up elsewhere. Then the expected value of X_i is simply $E(X_i) = 1(1/n) + 0(1 - 1/n) = 1/n$. Since expectation is linear, $E(\sum X_i) = \sum E(X_i)$, and we have that $E(\sum X_i) = n(1/n) = 1$.

However, in the Josephus shuffle we can set things up so that there are no fixed points for arbitrarily large values of n —just let $q = L(n)$ for even n resulting in the cards' order being completely reversed. In the other direction, the example $P(8, 9)$ given earlier had five fixed points. For $q > 1$ (and not congruent to 1 modulo $L(n)$), how large (relative to n) can the number of fixed points be? There are lots of interesting combinatorial and number theoretic problems circling around for the mathematically brave!

REFERENCES

1. R. Cooke, *The History of Mathematics: A Brief Course*, Wiley, 1997, 247–248.
2. W. Durant, *The Story of Civilization III: Caesar and Christ*, Simon and Schuster, New York, 1944, 543–546.
3. R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison Wesley, 1989, 8–20.
4. I. N. Herstein, I. Kaplansky, *Matters Mathematical*, Harper and Row, 1974, 121–126.
5. F. Josephus, *The Great Roman-Jewish War: A.D. 66–70*, Peter Smith, Gloucester, 1970, 138–139.
6. J. R. Newman, *The World of Mathematics* (Vol. 4), Tempus, 1988, 4: 2403–2405.
7. D. E. Smith, *History of Mathematics* (Vol. 1), Dover, 1958, 207–208.

A Brief History of Factoring and Primality Testing B. C. (Before Computers)

RICHARD A. MOLLIN

University of Calgary
Calgary, Alberta
Canada T2N 1N4
ramollin@math.ucalgary.ca

Factoring and primality testing have become increasingly important in today's information based society, since they both have produced techniques used in the secure transmission of data. However, often lost in the modern-day shuffle of information are the contributions of the pioneers whose ideas ushered in the computer age and, as we shall see, some of whose ideas are still used today as the underpinnings of powerful algorithms for factoring and primality testing. We offer this brief history to help readers know more about these contributions and appreciate their significance.

Virtually everyone who has graduated from high school knows the definition of a prime number, namely a $p \in \mathbb{N} = \{1, 2, 3, 4, \dots\}$ such that $p > 1$ and if $p = \ell m$ where $\ell, m \in \mathbb{N}$, then either $\ell = 1$ or $m = 1$. (If $n \in \mathbb{N}$ and $n > 1$ is *not* prime, then n is called *composite*.) Although we cannot be certain, the concept of primality probably arose with the ancient Greeks over two and one-half millennia ago. The first *recorded* definition of prime numbers was given by Euclid around 300 BCE in his *Elements*. However, there is some indirect evidence that the concept of primality might have been known far earlier, for instance, to Pythagoras and his followers.

The Greeks of antiquity used the term *arithmetic* to mean what today we would call *number theory*, namely the study of the properties of the natural numbers and the relationships between them. The Greeks reserved the word *logistics* for the study of ordinary computations using the standard operations of addition/subtraction and multiplication/division, which we now call arithmetic. The Pythagoreans introduced the term *mathematics*, which to them meant the study of arithmetic, astronomy, geometry, and music. This curriculum became known as the *quadrivium* in the Middle Ages.

Although we have enjoyed the notion of a prime for millennia, only very recently have we developed *efficient* tests for primality. This seemingly trivial task is in fact much more difficult than it appears.

A *primality test* is an algorithm (a methodology following a set of rules to achieve a goal), the steps of which verify that given some integer n , we may conclude “ n is a prime number.” A *primality proof* is a successful application of a primality test.

Such tests are typically called *true primality tests* to distinguish them from *probabilistic primality tests* (which can only conclude that “ n is prime” up to a specified likelihood). We will not discuss such algorithms here (see [9] for these).

A concept used frequently in primality testing is the notion of a *sieve*. A “sieve” is a process to find numbers with particular characteristics (for instance primes) by searching among *all* integers up to a prescribed bound, and eliminating invalid candidates until only the desired numbers remain. Eratosthenes (ca. 284–204 BCE) proposed the first sieve for finding primes. The following example illustrates the *Sieve of Eratosthenes*.

EXAMPLE 1. Suppose that we want to find all primes less than 30. First, we write down all natural numbers less than 30 and bigger than 1. The first uncrossed number,

2, is a prime. We now cross out all numbers (bigger than 2) that are multiples of 2 (and hence composite).

$$\{2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, 21, \cancel{22}, \\ 23, \cancel{24}, 25, \cancel{26}, 27, \cancel{28}, 29, \cancel{30}\}.$$

The next uncrossed number, 3, must be a prime, so we cross out all numbers (bigger than 3) that are (composite) multiples of 3.

$$\{2, 3, 5, 7, \cancel{9}, 11, 13, \cancel{15}, 17, 19, \cancel{21}, 23, 25, \cancel{27}, 29\}.$$

Then 5 is the next uncrossed number, so we conclude it is prime, and we cross out all numbers (bigger than 5) that are multiples of 5.

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, \cancel{25}, 29\}.$$

(We need not check any primes bigger than 5 since such primes are larger than $\sqrt{30}$. An historical description of this fact follows.)

The set of primes less than 30 is what remains:

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}.$$

The Sieve of Eratosthenes represents the only known algorithm from antiquity that we would call a primality test, but it is highly inefficient and it could not come close to verifying some of the primes known today. The number $2^{6972593} - 1$, shown to be prime on June 1, 1999, has 2,098,960 decimal digits (see the discussion of Mersenne primes below). Using the Sieve of Eratosthenes to verify its primality would take longer than the life expectancy of our sun using the fastest computers known today. The modern techniques that yield such a spectacular primality proof as this one are based on the ideas of later pioneers, whose contributions we highlight in this article.

Arabs and Italians

Arabic scholars were primarily responsible for preserving much of the mathematics from antiquity, and they extended many ancient results. Indeed, it was said that Caliph al-Mamun (809–833) experienced a vision, which included a visit from Aristotle; after this epiphany, al-Mamun was driven to have all of the Greek classics translated into Arabic, including Euclid's *Elements*.

Under the caliphate of al-Mamun lived Mohammed ibn Musa al-Khowarizmi (Mohammed, son of Moses of Kharezmi, now Khiva), who was one of those to whom Europe owes the introduction of the Hindu-Arabic number system. Around 825 CE, he completed a book on arithmetic, which was later translated into Latin in the twelfth century under the title *Algorithmi de numero Indorum*. This book is one of the best-known works which introduced to Europe the Hindu-Arabic number system. This may account for the widespread, although mistaken, belief that our numerals are Arabic in origin. Not long after Latin translations of al-Khowarizmi's book were available in Europe, readers began to attribute the new numerals to him, and began contracting his name, in connection with these numerals, to *algorism*, and ultimately to *algorithm*.

Al-Khowarizmi also wrote a book on algebra, *Hisab al-jabr wa'lmuqābala*. The word *algebra* is derived from *al-jabr* or *restoration*. The term referred to the operation of removing a quantity that is subtracted on one side of an equation and "restoring" it

on the other side as an added quantity. In the Spanish work *Don Quixote*, which came much later, the term *algebrist* is used for a *bone-setter* or *restorer*.

As we observed, Eratosthenes did not discuss the issue of when his algorithm would terminate. However, Ibn al-Banna (ca. 1258–1339) appears to have been the first to observe that, in order to find the primes less than n using the sieve of Eratosthenes, one can restrict attention to prime divisors less than \sqrt{n} .

Fibonacci The resurrection of mathematical interest in Europe during the thirteenth century is perhaps best exemplified by the work of Leonardo of Pisa (ca. 1170–1250), better known as Fibonacci. While living in North Africa, where his father served as consul, Fibonacci was tutored by an Arab scholar. Thus, Fibonacci was well-educated in the mathematics known to the Arabs. Fibonacci's first book, and certainly his best known, is *Liber Abaci* or *Book of Calculation* first published in 1202, which continued to promote the use of the Hindu-Arabic number system in Europe. However, only the second edition, published in 1228 has survived.

In this work, Fibonacci gave an algorithm to determine if n is prime by dividing n by natural numbers up to \sqrt{n} . This represents the first recorded instance of a *deterministic algorithm* for primality testing, where *deterministic* means that the algorithm always terminates with either a *yes* answer or a *no* answer. (A deterministic algorithm may also be viewed as an algorithm that follows the same sequence of operations each time it is executed with the same input. This is in contrast to *randomized algorithms* that make random decisions at certain points in the execution, so that the execution paths may differ each time the algorithm is invoked with the same input. See [9] for a discussion of some randomized algorithms, which we will not discuss here.)

Fibonacci also discussed the well-known class of *Fibonacci numbers*, $\{F_n\}$, defined by the sequence

$$F_1 = F_2 = 1, \quad F_n = F_{n-1} + F_{n-2} \quad (n \geq 3).$$

In addition to being one of Fibonacci's memorable accomplishments, this sequence later played a surprising role in primality testing, as we shall see.

Perfect numbers

Another distinguished set of numbers that had a deep influence on the development of primality testing was the set of perfect numbers. A *perfect number* is an integer $n \in \mathbb{N}$ equal to the sum of its *proper divisors* (those $m \in \mathbb{N}$ where $m \mid n$ but $m \neq n$). For example, 6 is a perfect number, since $6 = 3 + 2 + 1$. The Pythagoreans probably knew about perfect numbers; the idea is founded in mysticism, which was their venue. Perfect numbers appear in Euclid's *Elements*, so we know the concept had been around for some time. The number $2^{n-1}(2^n - 1)$ is perfect for $n = 2, 3, 5, 7$, and these are the first four perfect numbers: 6, 28, 496, and 8128.

The ancient Greeks attributed mystical properties to perfect numbers. St. Augustine (354–430 CE) is purported to have said that God created the earth in six days since the perfection of the work is signified by the perfect number 6. Also, the moon orbits the earth every twenty-eight days, and 28 is the second perfect number.

Pietro Antonio Cataldi (1548–1626) developed an algorithmic approach to primality testing, but is probably best known for his work on continued fractions. In particular, his work *Trattato del modo brevissimo di trovar la radice quadra delli numeri* published in 1613, represents a significant contribution to the development of continued fractions. His work on perfect numbers was also considerable. Among his thirty

books, he wrote on military applications of algebra, and even published an edition of Euclid's *Elements*. Cataldi proved that the fifth, sixth, and seventh perfect numbers are:

$$\begin{aligned} 33550336 &= 2^{12}(2^{13} - 1), \\ 8589869056 &= 2^{16}(2^{17} - 1), \end{aligned}$$

and

$$137438691328 = 2^{18}(2^{19} - 1).$$

It is uncertain whether Cataldi was the first to discover these perfect numbers, but his are the first known proofs of these facts. Cataldi was also the first to observe that if $2^n - 1$ is prime then n must be prime. In fact, the following result was known to Cataldi, though proved by Fermat.

THEOREM 1. (PERFECT NUMBERS) *If $2^n - 1$ is prime, then n is prime and $2^{n-1}(2^n - 1)$ is perfect.*

Proof. Since $(2^m - 1) \mid (2^n - 1)$ whenever $m \mid n$, then n must be prime whenever $2^n - 1$ is prime. (Note that, in general, if $n = \ell m$, then for any $b \in \mathbb{N}$, $b^n - 1 = (b^m - 1) \sum_{j=1}^{\ell} b^{m(\ell-j)}$.)

Let S_1 be the sum of all divisors of 2^{n-1} and let S_2 be the sum of all the divisors of the prime $2^n - 1$. Then the sum S of all divisors of $2^{n-1}(2^n - 1)$ is given by:

$$S = \sum_{\ell \mid 2^{n-1}(2^n-1)} \ell = \sum_{\ell \mid 2^{n-1}, \ell' \mid (2^n-1)} \ell \ell' = \sum_{\ell \mid 2^{n-1}} \ell \sum_{\ell' \mid (2^n-1)} \ell' = S_1 S_2.$$

Also, $S_1 = \sum_{j=0}^{n-1} 2^j$, so as a geometric series, we know that

$$S_1 = 2^n - 1.$$

Finally, since $2^n - 1$ is prime, then $S_2 = 2^n$. Hence,

$$S = 2^n(2^n - 1),$$

so $2^{n-1}(2^n - 1)$ is perfect. ■

Long after Cataldi, Euler showed that every even perfect number has the form given in Theorem 1. It is unknown whether there are any odd perfect numbers and the search for them has exceeded the bound 10^{300} . Moreover, if such a beast exists, then it is known that it must have at least twenty-nine (not necessarily distinct) prime factors (see Guy [6, B1, p. 44]).

The French enter the fray

Theorem 1 tells us that the search for even perfect numbers is essentially the search for primes of the form

$$M_p = 2^p - 1, \text{ where } p \text{ is prime.}$$

Such primes are called *Mersenne primes*, the largest known of which is given above (see: <http://www.utm.edu/research/primes/largest.html>). These are named after the mendicant monk, Marin Mersenne (1588–1648). Although Mersenne was not a for-

mally trained mathematician, he had great enthusiasm for number theory. Among his contributions were his multifarious communications with many of the outstanding scholars of the day, including Descartes, Fermat, Frénicle de Bessy, and Pascal. He also published *Cognitata Physica-Mathematica* in 1644 in which he claimed that of all the primes $p \leq 257$, the only Mersenne primes M_p that occur are when

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

It was not until the twentieth century that Mersenne's claims were completely checked. We now know that Mersenne made five mistakes. For example, M_p is *not* prime for $p = 67$ and $p = 257$, but M_p is prime for $p = 61$, $p = 89$, and $p = 107$. It is for this list, and the impact which it had, that these primes were named after him.

Pierre de Fermat (1607–1665) kept Mersenne informed of the progress that he, too, was making in number theory. In particular, Fermat informed him that he had proved

$$223 \mid (2^{37} - 1) = M_{37}.$$

Fermat was able to do this by using a series of results, that began with his well-known “little theorem.”

THEOREM 2. (FERMAT'S LITTLE THEOREM) *If q is a prime not dividing $b \in \mathbb{N}$, then $q \mid (b^{q-1} - 1)$.*

Proof. The result is obvious if $q = 2$, so we assume that $q > 2$. We now use the Binomial Theorem. First, we establish that $q \mid \binom{q}{j}$ for any natural number $j < q$. Since $q > 2$ is prime, then neither j nor $q - j$ divides q for any j with $1 \leq j \leq q - 1$. Therefore, the integer

$$\binom{q}{j} = \frac{q!}{(q-j)! j!}$$

is a multiple of q . Now, the Binomial Theorem in conjunction with this fact tells us that

$$b^q = (b - 1 + 1)^q = \sum_{j=0}^q \binom{q}{j} (b - 1)^{q-j} 1^j = (b - 1)^q + 1 + qa_1$$

for some $a_1 \in \mathbb{N}$. Applying this same argument to $(b - 1)^q$, we get

$$(b - 1)^q = (b - 2)^q + 1 + qa_2$$

for some $a_2 \in \mathbb{N}$. Continuing in this fashion, for each $(b - i)^q$ with $1 \leq i < b$, we ultimately get that

$$b^q = b + q \sum_{j=1}^b a_j.$$

Hence, $q \mid (b^q - b) = b(b^{q-1} - 1)$, but $q \nmid b$ so $q \mid (b^{q-1} - 1)$. ■

Fermat was actually interested in a result slightly different from the “little theorem” stated above. It is trivial that the little theorem implies the following theorem:

THEOREM 3. *Let $b \in \mathbb{N}$ and q a prime such that q does not divide b . Then there exists an $n \in \mathbb{N}$ such that $n \mid (q - 1)$ and $q \mid (b^{(q-1)/n} - 1)$.*

This is trivially implied by the little theorem by setting $n = 1$. However, cases where larger values of n occur were of special interest to Fermat, as we shall see. The following result shows that in some cases we may actually find them:

COROLLARY 1. *If $p > 2$ is prime, then any prime divisor q of $2^p - 1$ must be of the form $q = 2mp + 1$ for some $m \in \mathbb{N}$. Also, if m is the smallest natural number for which $q \mid (b^m - 1)$, then $q \mid (b^t - 1)$ whenever $m \mid t$.*

Here, the number “ $2m$ ” takes the role of n in the statement of Theorem 2. In particular, not only may we assume that $n > 1$, but that it is even.

Proof. First we prove the second assertion, which follows from the fact that if $t = ms$ for some $s \in \mathbb{N}$, then $(b^t - 1) = (b^m - 1) \sum_{j=1}^s b^{m(s-j)}$.

Now we establish the first assertion. Let q be a prime dividing $2^p - 1$. Then by the “little theorem,” $q \mid (2^{q-1} - 1)$.

$$\text{CLAIM. } \gcd(2^p - 1, 2^{q-1} - 1) = 2^{\gcd(p, q-1)} - 1.$$

Let $g = \gcd(p, q - 1)$ and $g_1 = \gcd(2^p - 1, 2^{q-1} - 1)$. Thus, by the second assertion $(2^g - 1) \mid g_1$. It remains to show that $g_1 \mid (2^g - 1)$. By the Euclidean Algorithm there exist $x, y \in \mathbb{N}$ such that $g = xp - y(q - 1)$. Since $g_1 \mid (2^p - 1)$, then $g_1 \mid (2^{px} - 1)$ by the second assertion, and similarly $g_1 \mid 2^{(q-1)y} - 1$. Thus, g_1 divides

$$2^{px} - 2^{(q-1)y} = 2^{(q-1)y} (2^{px-(q-1)y} - 1) = 2^{(q-1)y} (2^g - 1).$$

However, since g_1 is odd, then $g_1 \mid (2^g - 1)$. This proves the Claim.

Since $q \mid (2^{q-1} - 1)$ and $q \mid (2^p - 1)$, then $g > 1$. However, since p is prime, then we must have that $g = p$, so $p \mid (q - 1)$. In other words, there exists an $n \in \mathbb{N}$ such that $q - 1 = np$. Since $p, q > 2$, then $n = 2m$ for some $m \in \mathbb{N}$. This completes the proof. ■

From these results Fermat sought a number $n > 1$ as in Corollary 1 to use in trial divisions to test Mersenne numbers for primality. He saw that Corollary 1 could be useful to detect possible primes q such that $q \mid (2^{37} - 1)$. For example, $q = 37n + 1$ may be tested for low, even values of n until we find, when $n = 6$, that 223 divides $(2^{37} - 1) = (2^{(q-1)/n} - 1)$. Fermat also discovered that

$$q = 47 \text{ divides } (2^{23} - 1) = (2^{(q-1)/2} - 1)$$

using this method. We note that it takes only two trial divisions using this method to prove that

$$q = 233 \text{ divides } (2^{29} - 1) = (2^{(233-1)/8} - 1).$$

The reason is that by Corollary 1 any prime divisor of $2^{29} - 1$ must be of the form $58m + 1$ so by testing for $m = 1, 2, 3, 4$ of which only two are prime, 59 and 233, we get the nontrivial prime divisor $q = 233$.

Some of Fermat's most famous results were found in his correspondence with an excellent amateur mathematician, Bernard Frénicle de Bessy (1605–1675). In Fermat's letter dated October 8, 1640, Fermat's Little Theorem, in certain special cases, makes its first recorded appearance. Frénicle de Bessy also corresponded with Descartes, Huygens, and Mersenne. He actually solved several problems posed by Fermat, and posed further problems himself.

After Fermat's earlier success with Mersenne primes, he suggested to Frénicle de Bessy that numbers of the form

$$2^{2^n} + 1$$

should be prime. Today such numbers are called *Fermat numbers*, denoted by \mathfrak{F}_n . Fermat knew that \mathfrak{F}_n for $n = 0, 1, 2, 3, 4$ were prime, called *Fermat primes*, but could not prove primality for $n = 5$. Today we know that \mathfrak{F}_n is composite for $5 \leq n \leq 24$, and it is suspected that \mathfrak{F}_n is composite for all $n > 24$ as well. (On July 25, 1999, F_{382447} , which has over 10^{105} decimal digits, was shown to be composite by John Cosgrave (see <http://www.spd.dcu.ie/johnbcos/fermat.htm>).)

Fermat's work also had consequences for factoring. We define a *factorization algorithm* as one that solves the problem of determining the complete factorization of an integer $n > 1$, as guaranteed by the Fundamental Theorem of Arithmetic. In other words, the algorithm should find distinct primes p_j and $a_j \in \mathbb{N}$ such that $n = \prod_{j=1}^k p_j^{a_j}$. We observe that it suffices for such algorithms to merely find $r, s \in \mathbb{N}$ such that $1 < r \leq s < n$ with $n = rs$ (called *splitting* n), since we can then apply the algorithm to r and to s , thereby recursively splitting each composite number until a complete factorization is found. Furthermore, since *deciding* whether a given $n > 1$ is composite or prime is easier, in general, than factoring, one should always check first whether n is composite (primality test) before applying a factorization algorithm.

In 1643, Fermat developed a method for factoring that was based on a simple observation. If $n = rs$ is an odd natural number with $r < \sqrt{n}$, then

$$n = a^2 - b^2 \text{ where } a = (s + r)/2 \text{ and } b = (s - r)/2.$$

Hence, in order to find a factor of n , we look through the various quantities $a^2 - n$ as a ranges among the values $a = \lfloor \sqrt{n} \rfloor + 1, \lfloor \sqrt{n} \rfloor + 2, \dots, (n - 1)/2$ until we find a perfect square, which will play the role of b^2 . (Here $\lfloor z \rfloor$ is the *greatest integer function* or *floor*, namely the greatest integer less than or equal to z .) Once the appropriate values of a and b have been determined, we may solve for the factors r and s . This is called the *difference of squares method* of factoring, and it has been rediscovered numerous times.

From Euler to Gauss

The Swiss mathematician, Leonhard Euler (1707–1783), became interested in Fermat's work in 1730. He found that

$$641 \mid \mathfrak{F}_5,$$

thereby refuting Fermat's conjecture. Euler's method was to generalize a result of Fermat:

THEOREM 4. (EULER'S RESULT ON FERMAT NUMBERS) *If $\mathfrak{F}_n = 2^{2^n} + 1$, then every prime divisor of \mathfrak{F}_n is of the form $2^{n+1}r + 1$ for some $r \in \mathbb{N}$.*

Proof. Let p be a prime divisor of \mathfrak{F}_n . Suppose that $m \in \mathbb{N}$ is the smallest value such that $p \mid (2^m - 1)$, and set $2^m = pw + 1$ for some integer w . Then since $p \mid (2^{2^n} + 1)$ and $p \mid (2^{2^{n+1}} - 1)$, we must have $2^{n+1} \geq m > 2^n$. By the Division Algorithm, there must exist $k \in \mathbb{N}$ and a nonnegative integer $\ell < m$, such that $2^{n+1} = mk + \ell$. Since $m > 2^n$, then $k = 1$ must be true. Also, p divides

$$(2^{2^{n+1}} - 1) = 2^{m+\ell} - 1 = (2^m)2^\ell - 1 = (pw + 1)2^\ell - 1,$$

so we have shown that $p \mid (2^\ell - 1)$. By the minimality of m , we must have $\ell = 0$. Hence, $m = 2^{n+1}$.

Now, by Theorem 2, $p \mid (2^{p-1} - 1)$, so $p - 1 \geq 2^{n+1}$. Again, by the Division Algorithm, there must exist $r \in \mathbb{N}$ and a nonnegative integer $\ell_1 < 2^{n+1}$ such that $p - 1 = 2^{n+1}r + \ell_1$. Since p divides

$$(2^{p-1} - 1) = 2^{2^{n+1}r + \ell_1} - 1 = (2^{2^{n+1}})^r 2^{\ell_1} - 1 = (pw + 1)^r 2^{\ell_1} - 1,$$

a quick application of the Binomial Theorem shows that this equals $(pv_1 + 1)2^{\ell_1} - 1$ for some integer v_1 . This means that $p \mid (2^{\ell_1} - 1)$, forcing $\ell_1 = 0$ by the minimality of 2^{n+1} . Hence, $p = 2^{n+1}r + 1$. ■

In particular, we know from Theorem 4 that all divisors of \mathfrak{F}_5 must be of the form $64k + 1$. Thus, Euler only needed five trial divisions to find the factor 641, namely for $k = 3, 4, 7, 9, 10$, since the values $64k + 1$ for $k = 2, 5, 8$ are divisible by 3, and those for $k = 1, 6$ are divisible by 5.

Euler also knew of the seven perfect numbers

$$2^{n-1}(2^n - 1) \text{ for } n = 2, 3, 5, 7, 13, 17, 19.$$

By 1771, he had determined that M_{31} is also prime (using a methodology we outline below), the largest known prime to that date, a record that held until 1851.

In 1830, a valuable technique for factoring any odd integer n was discovered by Adrien-Marie Legendre (1752–1833) using the theory of *quadratic residues*. This theory, studied since the time of Euler and greatly advanced by Gauss was applied by Legendre to develop a new sieve method. An integer c is called a *quadratic residue* modulo $n \in \mathbb{N}$ if there is an integer x such that

$$c \equiv x^2 \pmod{n}$$

(meaning that $n \mid (c - x^2)$).

Suppose we wish to find prime divisors of an integer n . For different primes p , Legendre studied congruences of the form

$$x^2 \equiv \pm p \pmod{n}.$$

Suppose a solution to this congruence could be found. This would imply that $\pm p$ is a quadratic residue modulo all prime factors of n . This fact can be used to greatly reduce the search for prime divisors of n by only considering those primes q for which p is also a quadratic residue \pmod{q} . For instance, suppose 2 is a quadratic residue \pmod{n} . A result that follows from Fermat's Little Theorem states that 2 is a quadratic residue modulo a prime q if and only if $q \equiv \pm 1 \pmod{8}$. Thus, already we have halved the search for factors of n (by eliminating odd divisors whose remainders are $\pm 3 \pmod{8}$).

Legendre applied this method repeatedly for various primes p . This can be viewed as constructing a (quadratic) sieve by computing lots of residues modulo n , thereby eliminating potential prime divisors of n that sit in various linear sequences. He found that if you computed enough of them, then one could eliminate primes up to \sqrt{n} as prime divisors and thus show n was prime.

Some results of Euler had actually anticipated Legendre's work. He considered two representations of n :

$$n = x^2 + ay^2 = z^2 + aw^2,$$

so

$$(xw)^2 \equiv (n - ay^2)w^2 \equiv nw^2 - ay^2w^2 \equiv -ay^2w^2 \equiv (z^2 - n)y^2 \equiv (zy)^2 \pmod{n},$$

and we are back to a potential factor for n . The basic idea in the above, for a given $n \in \mathbb{N}$, is simply that if we can find integers x, y such that

$$x^2 \equiv y^2 \pmod{n}, \quad (1)$$

and $x \not\equiv \pm y \pmod{n}$, then $\gcd(x - y, n)$ is a nontrivial factor of n . This idea is still exploited by numerous algorithms in current use: *Pollard's $p - 1$ algorithm*, *the continued fraction algorithm*, *the quadratic sieve*, and the powerful *number field sieve*. For a complete description of these methods and their applications to cryptography, see [9].

Legendre was only concerned with building the sieve on the prime factors of n , and so he was unable to *predict*, for a given prime p , a second residue to yield a square. In other words, if he found a solution to $x^2 \equiv py^2 \pmod{n}$, he could not predict a different solution $w^2 \equiv pz^2 \pmod{n}$. If he had been able to do this, then he would have been able to combine the two as

$$(xw)^2 \equiv (pzy)^2 \pmod{n},$$

so if $xw \not\equiv \pm pzy \pmod{n}$, then $\gcd(xw - pzy, n)$ would be a nontrivial factor of n , thereby putting us back in the situation given in (1).

The idea of trying to match the primes to create a square can be attributed to Maurice Borisovich Kraitchik (1882–1957). Kraitchik, in the early 1920s, reasoned that it might suffice to find a *multiple* of $n \in \mathbb{N}$ as a difference of squares. He chose a quadratic polynomial of the form $kn = ax^2 \pm by^2$ for some $k \in \mathbb{N}$. In its simplest form with $k = a = b = 1$, he would sieve over $x^2 - n$ for $x \geq \lfloor \sqrt{n} \rfloor$. This is the basic idea behind the quadratic sieve method mentioned above. Thus, what Kraitchik had done was to opt for “fast” generation of quadratic residues, and in so doing abandoned Legendre’s Method (meaning that, generally, he did not have residues less than $2\sqrt{n}$), but gained control over finding of two distinct residues at a given prime to form a square (as described above), which Legendre was unable to do. Thus, Kraitchik could start at values bigger than \sqrt{n} and sieve until “large” residues were found.

A version of Legendre’s method for factoring was developed by one of the greatest mathematicians who ever lived, Carl Friederich Gauss (1777–1855), in his influential masterpiece *Disquisitiones Arithmeticae* [5]. Gauss recognized the importance of factoring [5, Art. 329, p. 396]: “The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.” Gauss also discussed another factoring method in [5], which may be described as follows.

Suppose that we want to factor $n \in \mathbb{N}$. We choose some $m \in \mathbb{N}$ such that $\gcd(m, n) = 1$. Suppose that $x = r, s \in \mathbb{N}$ are two solutions of

$$n \mid (x^2 - m). \quad (2)$$

Then, if $n \nmid (r \pm s)$, then $\gcd(r - s, n)$ must be a nontrivial divisor of n because $n \mid (r - s)(r + s)$, while $n \nmid (r - s)$ and $n \nmid (r + s)$.

Landry, Lucas, and Lehmer

Once we enter the nineteenth century, the work of several individuals stands out in the development of factoring and primality testing. Among these is C. G. Reuschle (1813–1875). Tables compiled by Reuschle included all known prime factors of $b^n - 1$ for

$$b = 2, 3, 5, 7, 11, \text{ and } n \leq 42.$$

He also included partial factorizations of $2^n - 1$ for some values of $n \leq 156$, and as we have already seen, this information is useful for primality testing. In 1925, Cunningham and Woodall [3] published tables of factorizations of $b^n \pm 1$ for a small number of values $b \leq 12$, and some high powers of n . As a consequence, work on extending these tables has come to be known as the *Cunningham Project*. (Relatively recent work on the Cunningham Project and related problems is available [1].)

In the late 1860s a Parisian named Fortuné Landry worked on finding factors of M_n . He began by looking closely at Euler's proof of the primality of M_{31} , and tried to improve it. Euler had observed that any prime p dividing M_{31} must be of the form $p \equiv 1 \pmod{62}$. Since primes dividing forms of the type $x^2 - 2y^2$ must satisfy $p \equiv \pm 1 \pmod{8}$, Euler knew that if $p \mid M_{31}$, then $p \equiv 1, 63 \pmod{248}$, given that $p \mid ((2^{16})^2 - 2)$. Since $\lfloor \sqrt{M_{31}} \rfloor = 46340$, Euler had to trial divide M_{31} by primes of the form $p = 248k + 1$ or $p = 248k + 63$, where $p \leq 46340$. Finding no such primes, he concluded that M_{31} must be prime. Landry extended Euler's ideas as follows: If a given $n \in \mathbb{N}$ is known to have only factors of the form $ax + b$ for some (known) integers a, b , and if $n = (ax_1 + b)(ax_2 + b)$ for some (unknown) integers x_1, x_2 , he deduced that there exist integers q, h, r such that

$$x_1 x_2 = q - bh, \quad (3)$$

$$x_1 + x_2 = r + ah, \quad (4)$$

and

$$h = \frac{q - x_1(r - x_1)}{ax_1 + b}. \quad (5)$$

Landry also showed that if $h = gh' + k$ for some integers g, h' , then there exists a bound B such that if $x_1 > B$, then $h' = 0$. Hence, his algorithm involved testing all possible values of $k = h$ to see whether Equations (3)–(4) have solutions when $x_1 > B$. If they do, then we have a factor of n . If they do not, then we test all possible values of $x_1 \leq B$ to see if Equation (5) has a solution. We either get a factor of n or show that n is prime. (Dickson [4, p. 371] mentions Landry's efforts in the case where $a = 6$ and $b = \pm 1$, for instance.)

Using these methods, Landry completely factored $2^n \pm 1$ for all $n \leq 64$ with four exceptions. He even found the largest known prime of the time, namely

$$(2^{53} + 1)/321 = 2805980762433.$$

Perhaps the most influential nineteenth-century individual in the area of primality testing was François Édouard Anatole Lucas (1842–1891). Lucas had interests in recreational mathematics, such as his invention of the well-known *Tower of Hanoi* problem. However, his serious interest was in number theory, especially Diophantine analysis. Although he spent only the years 1875–1878 on the problems of factoring and primality testing, his contribution was impressive. Some of the ideas developed by Lucas may be interpreted today as the beginnings of computer design. He studied Fibonacci numbers and by 1877 had completely factored the first sixty of them. This led him to develop results on the divisibility of Fibonacci numbers, and ultimately to a proof that M_{127} is prime (modulo a corrected proof of the theorem below). The significance of this feat is revealed by the fact that this number held the distinction of being the largest known prime for three-quarters of a century. A larger prime was not found until 1951 by Miller and Wheeler [8].

The influence that Lucas had on modern-day primality testing is well described in a recent book by Hugh Williams [10], devoted to a discussion of the work of Lucas and his influence on the history of primality testing.

To see how Lucas determined that M_{127} is prime, we state the following result that was known to Lucas, although it was not given a *valid* proof until 1913 by R. D. Carmichael [2].

THEOREM 5. *Suppose that F_k denotes the k^{th} Fibonacci number and $n \in \mathbb{N}$ is given. If $n \equiv \pm 3 \pmod{10}$ and $n \mid F_{n+1}$ but $n \nmid F_m$ for all divisors m of n with $1 \leq m \leq n$, then n is prime. Also, if $n \equiv \pm 1 \pmod{10}$ and $n \mid F_{n-1}$ but $n \nmid F_m$ for all divisors m of n with $1 \leq m \leq n-2$, then n is prime.*

Based upon this result, all Lucas had to establish was that $M_{127} \mid F_{2^{127}}$ but $M_{127} \nmid F_{2^n}$ for all natural numbers $n < 127$. He did this in 1876, using methods that led to a primality test, the last we include in our historical discussion.

In the 1930s a pioneering giant in the world of primality testing, Derrick Henry Lehmer (1905–1991), extended the ideas of Lucas to provide the following primality test. (A look at his collected works [7] is highly recommended.)

Lucas-Lehmer true primality test for Mersenne numbers The algorithm consists of the following steps performed on a Mersenne number $M_n = 2^n - 1$ with $n \geq 3$.

- (1) Set $s_1 = 4$ and compute $s_j \equiv s_{j-1}^2 - 2 \pmod{M_n}$ for $j = 1, 2, \dots, n-1$.
- (2) If $s_{n-1} \equiv 0 \pmod{M_n}$, then conclude that M_n is prime. Otherwise, conclude that M_n is composite.

Lucas knew only that the test was sufficient for primality, and this only for certain restricted types of values of n . In 1930, Lehmer proved both that the condition is necessary and that the test holds for any $n \in \mathbb{N}$.

EXAMPLE 2. *Input $M_7 = 127$. Then we compute \overline{s}_j , the least nonnegative residue of s_j modulo M_7 as follows. $\overline{s}_2 = 14$, $\overline{s}_3 = 67$, $\overline{s}_4 = 42$, $\overline{s}_5 = 111$, and $\overline{s}_6 = 0$. Thus, M_7 is prime by the Lucas-Lehmer Test.*

This celebrated test is a fine example of the efforts of the pioneers such as Lehmer whose work, it may reasonably be said, had a deep and lasting influence upon the development of *computational number theory*, an experimental science with its feet in both the mathematical and computer science camps. One aspect of computational number theory that has given it high profile is *cryptography*, the study of methods for sending messages in secret.

Our age is dominated by information, and the need for secrecy is paramount in industry, academe, and the military, not to mention our personal lives. As we send email messages and financial data, we hope they remain private. Factoring and primality testing play a dominant role in the development of modern cryptographic techniques. Though the ideas of the pioneers are ubiquitous in modern algorithms, credit for their work is often overlooked. We hope to have increased the readers interest, understanding, and appreciation for these ideas.

Acknowledgments. The author's research is supported by NSERC Canada grant # A8484. Thanks go to the two anonymous referees whose comments inspired a complete rewriting of the first draft of this article in order to make the article more accessible and focused. Also, thanks to Glenn Appleby for help with the final edition.

REFERENCES

1. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff Jr., Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers, *Contemporary Math.* **22**, Amer. Math. Soc., Providence, R.I., Second Edition (1988).
2. R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Annals of Math.*, **15** (1913), 30–70.

3. A. J. C. Cunningham and H. J. Woodall, *Factorization of $y^n \mp 1$* , $y = 2, 3, 5, 6, 7, 10, 11, 12$ *Up to High Powers* (n), Hodgson, London, 1925.
4. L. Dickson, *Theory of Numbers*, Vol. I, Chelsea, New York, 1992.
5. C. F. Gauss, *Disquisitiones Arithmeticae* (English edition), Springer-Verlag, Berlin, 1985.
6. R. K. Guy, *Unsolved Problems in Number Theory*, Vol. 1, Second Edition, Springer-Verlag, Berlin, 1994.
7. D. H. Lehmer, *Selected Papers of D. H. Lehmer*, Vol. I–III, D. McCarthy (Ed.), The Charles Babbage Research Centre, St. Pierre, Canada, 1981.
8. J. C. P. Miller, Large primes, *Eureka* **14** (1951), 10–11.
9. R. A. Mollin, *An Introduction to Cryptography*, Chapman and Hall/CRC Press, New York, 2001.
10. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 22, Wiley-Interscience, New York, Toronto, 1998.

Doing Math

DONNA DAVIS

P.O. Box 23392
Billings, MT 59104

Au contraire, Three Dog Night, one
is not the loneliest number. Two,
however, is indeed the loneliest number
since the number one—is out of the running.
In a three-legged race, it helps to become one
with the two you're tied-to.

The Foursquare Gospel Church has truth
cornered. Five in the hive and before
you know it, honey, we're done for.
Six times six times six gets
you 200+ years
to plant apricots and pots of petunias.

Two calls me again—it's that double
helix, the doublecross, the double we
all are said to have somewhere in the world.
Mine was on a TV show once, *Jeopardy*, but
then again aren't we all in danger?

Seven's so lucky, we should prime the pump
with her before every bath and baptism. Eight
won't wait—ask any cat with only one more life left.
Nine is fine—faceted like a sparkle.
And ten lets you start again where

your number system's bass'ed
and cello'ed and violin'ed and viola'ed
and the way to heaven is charted for you.

NOTES

The Perfect Shape for a Rotating Rigid Body

FRANK MORGAN

Department of Mathematics and Statistics
Williams College
Williamstown, MA 01267
Frank.Morgan@williams.edu

What is the perfect, energy-minimizing shape for a rotating rigid body? When my friend Michael Hutchings first asked me this question, I thought that the answer would be a rotationally symmetric, flattened ball or oblate spheroid, something like the earth, exaggerated in FIGURE 1.

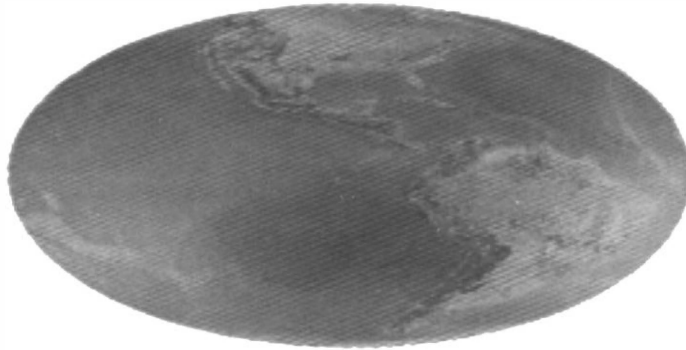


Figure 1 If the earth rotated once an hour, would it look like this very oblate spheroid?

For relatively small angular momentum, such shapes are indeed stable, relative although not absolute minima of energy. Motivated by understanding the shape of the earth and stars, historically mathematicians and scientists have studied many such surfaces of revolution, spheroids and tori, stable and unstable. Chandrasekhar [1] gives a fascinating survey, featuring Newton, Maclaurin, Jacobi, Liouville, Dirichlet, Dedekind, Riemann, Poincaré, and Cartan. Poincaré suggested that the instabilities in a rapidly rotating star could cause it to break up into a planetary system.

We will consider two kinds of energy, gravitational potential energy U and rotational kinetic energy K . The gravitational energy between two masses m_1, m_2 at distance r equals $-Gm_1m_2/r$, where G is the gravitational constant. In addition, each body has its own negative gravitational energy due to the interaction between each pair of particles. For a single body, the gravitational potential energy U is smallest (most negative) for a round ball, as you might guess. Happily, we won't need to know any more than that about gravitational potential energy to answer our question. (The surprisingly tricky proof [2, 3] uses the fact that so-called Steiner symmetrization, centering each vertical segment on the x - y plane, reduces U .)

A rigid body's rotational kinetic energy about an axis depends on its mass distribution or *moment of inertia*, I , and its angular velocity, ω (perhaps measured in revolutions per hour). For a single particle of mass m at radius r , the moment of inertia $I = mr^2$. (The r^2 will take into account the fact that parts farther from the axis move faster; indeed, velocity $v = r\omega$.) In general, you can compute I by an integral, $\int r^2 dm$, but we won't need to do that.

For a rigid body, the angular velocity ω must be the same at all points. The kinetic energy is given by $K = \frac{1}{2}I\omega^2$. For a single particle this is just the familiar

$$\frac{1}{2}mv^2 = \frac{1}{2}mr^2\omega^2 = \frac{1}{2}I\omega^2.$$

What is conserved in physics, in addition to the mass (with, say, unit density), is the angular momentum $L = I\omega$. It is to conserve angular momentum L that the skater who pulls in his arms, reducing I , must spin faster, increasing ω , to keep $L = I\omega$ constant.

For angular momentum 0 (no rotation, no kinetic energy), the perfect shape, with the most negative gravitational potential energy U , is a round ball, as mentioned earlier. But what if the body is rotating with some given angular momentum and consequential kinetic energy K ?

Question Find the shape of a rotating body of given mass, unit density, and given angular momentum to minimize gravitational potential energy U plus kinetic energy K .

What are some good candidates? A round ball has smallest possible gravitational potential energy, but fairly large rotational kinetic energy. Moving mass closer to the axis of revolution, as for a thin cylinder, actually increases kinetic energy, because like an ice skater pulling in his arms, with a smaller moment of inertia, it must spin faster to preserve angular momentum. Indeed, for fixed angular momentum $L = I\omega$, if I is small, the angular velocity ω must be large, and hence the kinetic energy

$$K = \frac{1}{2}I\omega^2 = \frac{1}{2}(I\omega)\omega = \frac{1}{2}L\omega$$

must be large. Conversely, allowing the body to follow its natural tendency to bulge outward, like the earth of FIGURE 1, reduces kinetic energy, though increasing gravitational potential energy. The right amount of bulging, striking a balance between the savings in kinetic energy and the cost in gravitational potential energy, is indeed a stable relative minimum of energy, but it is not the absolute minimum.

Answer The answer is that there is no minimum of energy, but the infimum value may be approached by a round ball circled by a small, very distant planet (connected by a negligibly thin rod if you insist). The infimum energy value is the best you could hope for: the same as for a round ball of angular momentum zero.

Remark: It is interesting to note that these approximate minima are not rotationally symmetric surfaces of revolution. They could be, however, by replacing the small planet with a toroidal ring.

Proof of answer: A ball with a planet of small mass m at very large radius r has large moment of inertia (at least mr^2) and hence small kinetic energy $K = I\omega^2/2 = L^2/(2I)$ (since L is fixed). Because most of the mass is in the central ball, the gravitational potential energy is almost as negative as if all the mass were in the central ball. Therefore, the total energy approaches that of a single, round, stationary ball, the best you could hope for.

Post-Mortem Does our answer mean that as the solar system runs down, the planets will drift farther away? No, because there is no mechanism for transferring mass to the sun, to make the planets smaller. But isn't the moon drifting farther from the earth? Yes, but that is because its energy is increasing, as energy is transferred from the earth's rotation, which is slowing down.

Acknowledgments. I would like to thank Michael Hutchings, Ira Wasserman, Bill Wootters, and a referee for help and inspiration. This work is partially supported by a National Science Foundation grant.

REFERENCES

1. S. Chandrasekhar, Ellipsoidal figures of equilibrium: an historical account, *Comm. Pure. Appl. Math.* **20** (1967), 251–265.
2. T. Carleman, Über eine isoperimetrische Eigenschaft des Kreises, *Math. Z.* **3** (1919), 1–7.
3. Frank Morgan, A round ball uniquely minimizes gravitational potential energy, preprint (2001).

One Sequence, Many Interesting Ideas in Analysis

RUSSELL A. GORDON

Whitman College
Walla Walla, WA 99362

CHARLES KICEY

SUDHIR GOEL
Valdosta State University
Valdosta, GA 31698

Consider the sequence $\{x_n\}$, where x_n is defined by

$$x_n = \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}$$

for each positive integer n . This sequence nicely illustrates the theorem that guarantees the convergence of bounded monotone sequences: it is elementary to prove that our sequence is increasing and bounded above by 1, and so it has a limit. However, for the novice at least, it is not at all clear what the limit of the sequence is. Hence, the existence of the limit is established without knowing its value. Somewhat surprisingly, it turns out that this sequence also illustrates Riemann sums and rearrangements of conditionally convergent series. Furthermore, as we will show, the sequence can be generalized without losing any of its interesting features.

We begin by summarizing five properties of the sequence $\{x_n\}$, and advise the reader to work through the elementary justifications of these facts before reading further.

1. The sequence $\{x_n\}$ is increasing and all of its terms are in the interval $[0.5, 1]$.
2. For each positive integer n , x_n is equal to the right-endpoint approximation to $\int_1^2 x^{-1} dx$ using n subintervals of equal length. It follows that the sequence $\{x_n\}$ converges to $\ln 2$.
3. Let $\{h_n\}$ be the sequence of partial sums for the alternating harmonic series $\sum_{k=1}^{\infty} (-1)^{k+1}/k$. Then $x_n = h_{2n}$ for each positive integer n , so this series converges to $\ln 2$.

4. It is easy to verify that the series

$$1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{3} - \frac{1}{3} + \frac{1}{4} - \frac{1}{4} + \cdots$$

is conditionally convergent. Consider the rearrangement of this series that consists of two positive terms followed by one negative term, where the positive and negative terms remain in the same order as in the original series:

$$1 + \frac{1}{2} - 1 + \frac{1}{3} + \frac{1}{4} - \frac{1}{2} + \frac{1}{5} + \frac{1}{6} - \frac{1}{3} + \frac{1}{7} + \frac{1}{8} - \frac{1}{4} + \cdots$$

If $\{t_n\}$ is the sequence of partial sums for this series, then $x_n = t_{3n}$ for each positive integer n . Hence (with a little more work, see the lemma below), the rearranged series converges to $\ln 2$, a value different from the sum of the original series.

5. The following theorem is not quite as well known (see Rudin [4, p. 70]). If the series $\sum_{i=1}^{\infty} a_i$ has bounded partial sums and the sequence $\{b_i\}$ decreases to 0, then the series $\sum_{i=1}^{\infty} a_i b_i$ converges. Apply this by letting $a_i = (-1)^{i+1}$ and $b_i = 1/i$ for each positive integer i . Let $\{y_n\}$ be the sequence of partial sums for the series $\sum_{i=1}^{\infty} a_i b_i$, which then is guaranteed to converge. Computation shows that $x_n = y_{2n}$ for each positive integer n . (Of course, this is no surprise since $\{y_n\}$ is the same as $\{h_n\}$ from (3); when we generalize our sequence, the results are more interesting.)

We referred to a lemma in item (4), which will also be useful in our generalization. It provides conditions to guarantee that a sequence of partial sums converges if one of its arithmetic subsequences converges.

LEMMA. Let $\sum_{i=1}^{\infty} d_i$ be a series for which $\lim_{i \rightarrow \infty} d_i = 0$, let $\{t_n\}$ be the sequence of partial sums for this series, and let j be a fixed positive integer. If the sequence $\{t_{jn}\}$ converges to t , then $\{t_n\}$ converges to t .

Proof. Let $\epsilon > 0$. Since $\lim_{i \rightarrow \infty} d_i = 0$, there exists a positive integer N_1 such that $|d_i| < \epsilon/j$ for all $i \geq N_1$. Since $\{t_{jn}\}$ converges to t , there exists an integer $N > N_1$ such that $|t_{jn} - t| < \epsilon$ for all $n \geq N$. Suppose that $n \geq jN$. Then there exists an integer $m \geq N$ such that $mj \leq n < (m+1)j$ and it follows that

$$|t_n - t| \leq |t_n - t_{jm}| + |t_{jm} - t| \leq \sum_{i=mj+1}^{(m+1)j} |d_i| + |t_{jm} - t| < j \cdot \frac{\epsilon}{j} + \epsilon = 2\epsilon.$$

This shows that $|t_n - t| < 2\epsilon$ for all $n \geq jN$. Therefore, the sequence $\{t_n\}$ converges to t . ■

Generalizing the example The term x_n of the sequence $\{x_n\}$ represents the sum of the reciprocals of the consecutive integers from $n+1$ to $2n$. In order to generalize this sequence, we will add the reciprocals of consecutive integers over a different range. Let p and q be positive integers with $p > q$. Consider the sequence $\{X_n^{pq}\}$, where X_n^{pq} is defined by

$$X_n^{pq} = \frac{1}{qn+1} + \frac{1}{qn+2} + \cdots + \frac{1}{pn}$$

for each positive integer n . Of course, $X_n^{21} = x_n$. We will obtain analogs of the results (1) through (5) for this sequence.

We will begin with the simplest observation concerning the sequence $\{X_n^{pq}\}$. For each positive integer n ,

$$\frac{p-q}{p} = \sum_{i=qn+1}^{pn} \frac{1}{pn} \leq \sum_{i=qn+1}^{pn} \frac{1}{i} \leq \sum_{i=qn+1}^{pn} \frac{1}{qn} = \frac{p-q}{q}.$$

This shows that the terms of the sequence $\{X_n^{pq}\}$ lie in the interval $[(p-q)/p, (p-q)/q]$. However, except for the case in which $q = 1$, it is not at all apparent how to go about proving that the sequence is increasing. It turns out that proving this fact is easily accomplished by connecting the sequence to Riemann sums, as follows:

For each positive integer n , let R_n^{pq} be the right-endpoint approximation to $\int_q^p x^{-1} dx$ using n subintervals of equal length. Note that

$$R_{(p-q)n}^{pq} = \sum_{i=1}^{(p-q)n} \frac{1}{q + i/n} \cdot \frac{1}{n} = \sum_{i=qn+1}^{pn} \frac{1}{i} = X_n^{pq}.$$

Hence, the terms of the sequence $\{X_n^{pq}\}$ are Riemann sums and the sequence converges to $\ln(p/q)$.

But is the convergence monotone? In an article in this MAGAZINE, Stein [5, Theorem 3.1] set out conditions to ensure that the sequence of right-endpoint approximations to an integral is monotone. A sufficient condition is that the integrand should be decreasing and convex. (If the term *convex* is unfamiliar, just interpret it as *concave up*.) Since the function $1/x$ has these properties on the interval $[q, p]$, the sequence $\{R_n^{pq}\}$ is increasing; thus, the sequence $\{X_n^{pq}\}$ is increasing as well.

To pursue an analog of item (4), consider the rearrangement of the series

$$1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{3} - \frac{1}{3} + \frac{1}{4} - \frac{1}{4} + \cdots$$

that consists of p positive terms followed by q negative terms and so on indefinitely, where the positive terms remain in the same order as in the original series as do the negative terms. For example, if $p = 3$ and $q = 2$, then the series is

$$1 + \frac{1}{2} + \frac{1}{3} - 1 - \frac{1}{2} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} - \frac{1}{3} - \frac{1}{4} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} - \frac{1}{5} - \frac{1}{6} + \cdots$$

Let $\{T_n^{pq}\}$ be the sequence of partial sums for the rearranged series and note that

$$X_n^{pq} = \sum_{i=1}^{pn} \frac{1}{i} - \sum_{i=1}^{qn} \frac{1}{i} = T_{(p+q)n}^{pq}.$$

Thus, the sequence $\{T_{(p+q)n}^{pq}\}$ converges to $\ln(p/q)$. The lemma guarantees that $\{T_n^{pq}\}$ converges to $\ln(p/q)$, that is, the sum of the rearranged series is $\ln(p/q)$.

The same rearrangement scheme can be applied to the alternating harmonic series. Let $\{H_n^{pq}\}$ be the sequence of partial sums for the resulting rearranged series and note that

$$H_{(p+q)n}^{pq} = \sum_{i=1}^{pn} \frac{1}{2i-1} - \sum_{i=1}^{qn} \frac{1}{2i} = \sum_{i=1}^{2pn} \frac{(-1)^{i+1}}{i} + \sum_{i=qn+1}^{pn} \frac{1}{2i} = h_{2pn} + \frac{1}{2} X_n^{pq},$$

where $\{h_n\}$ is the sequence of partial sums for the alternating harmonic series. Hence, the sequence $\{H_{(p+q)n}^{pq}\}$ converges to $\ln 2 + (1/2) \ln(p/q)$. By the lemma, this particular rearrangement of the alternating harmonic series converges to this same value.

Now suppose that q has the value 1. Let $\{a_i\}$ be the sequence defined by $a_i = 1$ if i is not a multiple of p and $a_i = 1 - p$ if i is a multiple of p . Since the series $\sum_{i=1}^{\infty} a_i$ has bounded partial sums, the series $\sum_{i=1}^{\infty} a_i/i$ converges by the theorem quoted in item (5). Let $\{Y_n^{p1}\}$ be the sequence of partial sums for this series and compute

$$Y_{pn}^{p1} = \sum_{i=1}^{pn} \frac{a_i}{i} = \sum_{i=1}^{pn} \frac{1}{i} - \sum_{i=1}^n \frac{1}{i} = X_n^{p1}.$$

Therefore, the sum of the series is $\ln p$.

More on rearrangements As we have shown, the sequence $\{X_n^{pq}\}$ generalizes all of the properties of the sequence $\{x_n\}$. We now change focus and consider the rearrangements of the series

$$1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{3} - \frac{1}{3} + \frac{1}{4} - \frac{1}{4} + \cdots$$

for the case in which $q = 1$.

When we asked students to explore the partial sums of the rearranged series numerically, they observed that some arithmetic subsequences of the sequence of partial sums converged faster than others. When writing out the terms of the rearranged series, there are two “reasonable” ways to group the terms of the series. To illustrate with a specific case, let $p = 5$. The rearranged series is

$$\begin{aligned} &1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} - 1 + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} - \frac{1}{2} \\ &+ \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} - \frac{1}{3} + \cdots \end{aligned}$$

and the two groupings are

$$\begin{aligned} &\left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} - \frac{4}{5}\right) + \left(\frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} - \frac{4}{10}\right) \\ &+ \left(\frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} - \frac{4}{15}\right) + \cdots; \\ &1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4} - \frac{4}{5} + \frac{1}{6} + \frac{1}{7}\right) + \left(\frac{1}{8} + \frac{1}{9} - \frac{4}{10} + \frac{1}{11} + \frac{1}{12}\right) \\ &+ \left(\frac{1}{13} + \frac{1}{14} - \frac{4}{15} + \frac{1}{16} + \frac{1}{17}\right) + \cdots. \end{aligned}$$

It is not difficult to show that the n^{th} term in the first grouping is proportional to $1/n^2$, while the n^{th} term of the second grouping is proportional to $1/n^3$. In other words, the sequence of partial sums for the second grouping converges more quickly than those of the first grouping.

When we work this out for more general values of p , we find similar behavior. As shown below, the first grouping has terms proportional to $1/n^2$ for any integer $p > 1$, while the second grouping has terms proportional to $1/n^3$ for any odd integer $p > 1$; an odd integer is required for the second grouping to be symmetrical.

We first consider the case where $p > 1$ is an odd integer. Fix such an integer p and let $p = 2m + 1$, where m is a positive integer. As above, let $\{a_i\}$ be the sequence

defined by $a_i = 1$ if i is not a multiple of p and $a_i = 1 - p$ if i is a multiple of p . Then the series $\sum_{i=1}^{\infty} a_i/i$ can be written in a form like that in the second grouping:

$$\sum_{i=1}^m \frac{1}{i} + \sum_{n=1}^{\infty} C_n^{p1}, \quad \text{where} \quad C_n^{p1} = \sum_{i=1}^m \frac{1}{pn-i} - \frac{2m}{pn} + \sum_{i=1}^m \frac{1}{pn+i}.$$

Noting that

$$C_n^{p1} = \sum_{i=1}^m \left(\frac{2pn}{p^2n^2 - i^2} - \frac{2}{pn} \right) = \sum_{i=1}^m \frac{2i^2}{pn(p^2n^2 - i^2)},$$

under and over estimates reveal that

$$\frac{2}{pn(p^2n^2 - 1)} \sum_{i=1}^m i^2 < C_n^{p1} < \frac{2}{pn(p^2n^2 - m^2)} \sum_{i=1}^m i^2.$$

It then follows that

$$\lim_{n \rightarrow \infty} n^3 C_n^{p1} = \frac{2}{p^3} \sum_{i=1}^m i^2 = \frac{m(m+1)}{3(2m+1)^2}.$$

However, a more enlightening way to establish this result involves an interesting consequence of Taylor's Theorem. We will show that for each positive integer n , there exists a number w_n in the interval $(pn - m, pn + m)$ such that

$$C_n^{p1} = \frac{m(m+1)(2m+1)}{6} \cdot \frac{2}{w_n^3}.$$

The term $2/w_n^3$ represents the second derivative of the function $1/x$ evaluated at w_n . The following two results will be needed to establish this result.

THEOREM 1. Let f be defined on $[a, b]$ and let $c = (a + b)/2$. If f is twice differentiable on $[a, b]$, then there exists a point $z \in (a, b)$ such that

$$f(a) - 2f(c) + f(b) = \frac{1}{4} (b - a)^2 f''(z).$$

Proof. By Taylor's Theorem, there exist points $u \in (a, c)$ and $v \in (c, b)$ such that

$$f(a) = f(c) + f'(c)(a - c) + \frac{f''(u)}{2} (a - c)^2;$$

$$f(b) = f(c) + f'(c)(b - c) + \frac{f''(v)}{2} (b - c)^2.$$

Since c is the midpoint of $[a, b]$,

$$f(a) - 2f(c) + f(b) = \left(\frac{b - a}{2} \right)^2 \cdot \frac{f''(u) + f''(v)}{2}.$$

Finally, since f'' has the intermediate value property (see [1, p. 174]), there exists a point z between u and v such that $f''(z) = (f''(u) + f''(v))/2$. This completes the proof. ■

THEOREM 2. Let m be a positive integer and let a be a real number. If f is twice differentiable on $[a, a + 2m]$, then there exists a point $w \in (a, a + 2m)$ such that

$$\sum_{i=0}^{m-1} f(a+i) - 2m f(a+m) + \sum_{i=m+1}^{2m} f(a+i) = \frac{m(m+1)(2m+1)}{6} f''(w).$$

Proof. By Theorem 1, for each integer i between 0 and $m-1$, there exists $z_i \in (a+i, a+2m-i)$ such that

$$f(a+i) - 2f(a+m) + f(a+2m-i) = \frac{1}{4} (2m-2i)^2 f''(z_i).$$

Let $s = \sum_{i=1}^m i^2$ and compute

$$\begin{aligned} & \sum_{i=0}^{m-1} f(a+i) - 2m f(a+m) + \sum_{i=m+1}^{2m} f(a+i) \\ &= \sum_{i=0}^{m-1} (f(a+i) - 2f(a+m) + f(a+2m-i)) \\ &= \sum_{i=0}^{m-1} (m-i)^2 f''(z_i) \\ &= s \sum_{i=1}^m \frac{i^2}{s} f''(z_{m-i}). \end{aligned}$$

The last sum represents a weighted average of the numbers $f''(z_0), \dots, f''(z_{m-1})$. Since f'' has the intermediate value property, there exists $w \in (a, a + 2m)$ such that

$$s \sum_{i=1}^m \frac{i^2}{s} f''(z_{m-i}) = s f''(w).$$

Since $s = m(m+1)(2m+1)/6$, the proof is complete. ■

The result quoted prior to Theorem 1 concerning the form of C_n^{p1} follows by applying Theorem 2 to the function $f(x) = 1/x$ on the interval $[pn-m, pn+m]$. Consequently, the number C_n^{p1} is of the same order of magnitude as $1/n^3$.

To study the other grouping, the first of the two above, we let $p > 1$ be an arbitrary integer. Then the series $\sum_{i=1}^{\infty} a_i/i$ can be written as $\sum_{n=1}^{\infty} L_n^{p1}$, where

$$L_n^{p1} = \sum_{i=1}^{p-1} \frac{1}{pn-i} - \frac{p-1}{pn}.$$

Using an argument similar to, but easier than, the one for C_n^{p1} , it can be shown that for each positive integer n , there exists a number v_n in the interval $(p(n-1)+1, pn)$ such that

$$L_n^{p1} = \frac{p(p-1)}{2} \cdot \frac{1}{v_n^2}.$$

It then follows that the number L_n^{p1} is of the same order of magnitude as $1/n^2$. As with C_n^{p1} , it is possible to obtain this result without calculus.

Our original sequence illustrated a number of properties in elementary analysis, and generalizing it preserved the interesting features. Discovering the connections discussed here would make a good project for students in real analysis. Using them to enrich a discussion of infinite series in a calculus course would be appropriate, with further guidance from the instructor. We conclude with two comments.

- i) Riemann's rearrangement theorem, which states that the terms of a conditionally convergent series can be rearranged to sum to any number, is a well-known result. The examples presented here provide concrete illustrations of that theorem. The results obtained in this paper for the alternating harmonic series can also be found in [3] and are generalized somewhat in [2].
- ii) It is not necessary that the subsequence considered in the lemma be arithmetic. The conclusion is valid (and the proof does not change very much) if the subsequence $\{t_{n_j}\}$ converges and the set of integers $\{n_{j+1} - n_j : j \in \mathbb{Z}^+\}$ has an upper bound. However, the following example shows that this last condition is essential. Define a sequence $\{d_i\}$ by $d_i = (-2)^{1-n}$ when $2^{n-1} \leq i < 2^n$. Let $\{V_n\}$ be the sequence of partial sums for the series $\sum_{i=1}^{\infty} d_i$. It is not difficult to verify that

$$V_{2^n-1} = \frac{1 + (-1)^{n+1}}{2}.$$

Hence, the sequence $\{V_n\}$ has several convergent subsequences, but the series does not converge.

REFERENCES

1. R. Bartle and D. Sherbert, *Introduction to Real Analysis*, 3rd ed., John Wiley & Sons, 2000.
 2. C. C. Cowen, K. R. Davidson, and R. P. Kaufman, Rearranging the alternating harmonic series, *Amer. Math. Monthly*, **87** (1980), 817–819.
 3. G. Klambauer, *Problems and Propositions in Analysis*, Marcel Dekker, New York, 1979.
 4. W. Rudin, *Principles of Mathematical Analysis*, 3rd ed., McGraw-Hill, New York, 1976.
 5. S. Stein, Do estimates of an integral really improve as n increases?, this MAGAZINE, **68** (1995), 16–26.
-

Proof Without Words: The Pigeonhole Principle

RAN LIBESKIND-HADAS

Harvey Mudd College
Claremont, CA 91711

Seven pigeons in six boxes

Letter to the Editor

Dear Editor:

The article by Dresden in the October 2001 issue presents a solution to the problem of the periodicity of the sequence of rightmost nonzero digits of $n!$. This problem has appeared in several places. I first learned about it from *Crux Mathematicorum* **19** (1993), 260–261 and **20** (1994) 45, where it was presented as an unused Olympiad problem. A discussion of the problem that focuses on the issue of a fast algorithm to get, say, the rightmost nonzero digit of the factorial of a googol appears as Problem 90 in my book *Which Way Did the Bicycle Go?* (with D. Velleman and J. Konhauser, MAA, 1996). And in Exercise 4.40 of *Concrete Mathematics* by Graham, Knuth, and Patashnik (Addison-Wesley, 1989) one finds a formula (see also Problem 90.2 of my book) for this digit in base p , when p is prime.

Stan Wagon
Macalester College
St. Paul, MN 55105
wagon@macalester.edu

Proof Without Words: A Sum and Product of Three Tangents

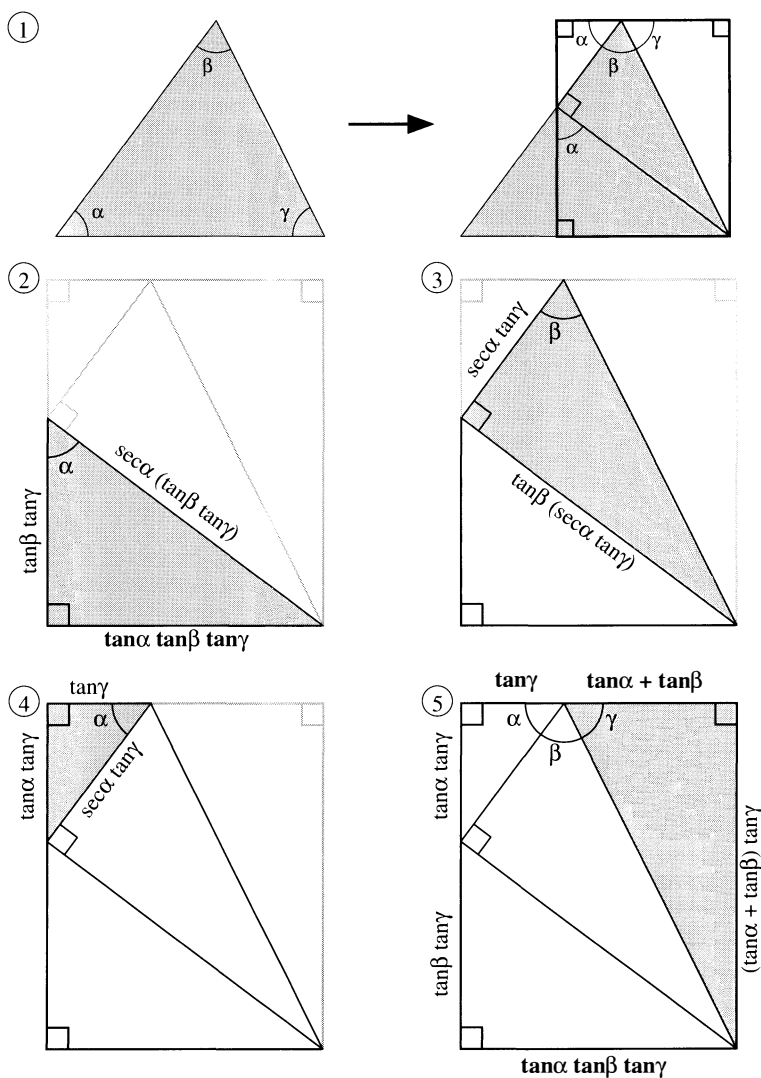
ROGER B. NELSEN

Lewis & Clark College
Portland, OR 97219

THEOREM. *If α , β , and γ denote angles in an acute triangle, then*

$$\tan \alpha + \tan \beta + \tan \gamma = \tan \alpha \tan \beta \tan \gamma.$$

Proof.



Note: The theorem holds for any angles α , β , γ (none an odd multiple of $\pi/2$) whose sum is π .

When Does a Sum of Positive Integers Equal Their Product?

MICHAEL W. ECKER

Pennsylvania State University, Wilkes-Barre
Lehman, PA 18627

The coordinates of the simple triple $(1, 2, 3)$ have the marvelous property that their sum equals their product. Can we come up with, say, 11 positive integers whose sum and product coincide? How about 100 such numbers?

More generally, given any integer $n > 1$, can we always find n positive integers whose sum and product are equal? We will see that we can, and the interesting question turns out to be identifying the integers for which this can be done in only one way.

Trigonometric origins Our journey begins with elementary trigonometry. Let's start with this identity, which seems not so well known:

For any triangle ABC , the sum of the tangents equals the product of the tangents:

$$\tan A + \tan B + \tan C = \tan A \tan B \tan C$$

The proof can be easily derived from simple trigonometric identities, or seen visually in a Proof Without Words on page 40.

Seeing this, one might wonder: Is it possible for all three of $\tan A$, $\tan B$, and $\tan C$ to be integers? If so, how many such triangles are there?

Let's approach this question algebraically rather than geometrically. We'll write $x = \tan A$, $y = \tan B$, $z = \tan C$, and then solve $x + y + z = xyz$ for solutions (x, y, z) in positive integers only. (The answer appears later in this Note.) But why stop here?

The general question and basic solutions We now divorce ourselves from any geometric context and examine the more general Diophantine equation

$$x_1 + x_2 + \cdots + x_n = x_1 x_2 \cdots x_n \quad (*)$$

That is, for each positive integer n , we seek solutions (x_1, x_2, \dots, x_n) in positive integers. Once a solution is found, there will be needless repetition in all its permutations of the coordinates. Thus, we consider only ordered sequences, stipulating that solutions to $(*)$ are positive integers that satisfy $x_1 \leq x_2 \leq \cdots \leq x_n$.

The $n = 1$ case is trivial, as any one number is a solution to $(*)$. For each integer $n \geq 2$, this equation always has at least one solution: $(1, 1, \dots, 1, 2, n)$, where there are $n - 2$ 1s, followed by a 2 and an n . Let's call this the *basic solution*. The first two nontrivial basic solutions are $(2, 2)$ and $(1, 2, 3)$.

Thus, for each n , one can always find n positive integers whose sum and product coincide. However, there may also be nonbasic solutions. For instance, for $n = 5$, we have the basic solution $(1, 1, 1, 2, 5)$ and two nonbasic solutions: $(1, 1, 2, 2, 2)$ and $(1, 1, 1, 3, 3)$. TABLE 1 shows all solutions with twelve or fewer terms.

Verifying that one has solutions to $(*)$ is trivial, but proving there are no others is more demanding. To verify that $(2, 2)$ is the unique solution for $n = 2$, suppose

TABLE 1: Table of solutions for $2 \leq n \leq 12$.

n	n -tuple solution	solution type	sum = product
2	(2, 2)	basic	4
3	(1, 2, 3)	basic	6
4	(1, 1, 2, 4)	basic	8
5	(1, 1, 1, 2, 5)	basic	10
5	(1, 1, 1, 3, 3)	nonbasic	9
5	(1, 1, 2, 2, 2)	nonbasic	8
6	(1, 1, 1, 1, 2, 6)	basic	12
7	(1, 1, 1, 1, 1, 2, 7)	basic	14
7	(1, 1, 1, 1, 1, 3, 4)	nonbasic	12
8	(1, 1, 1, 1, 1, 1, 2, 8)	basic	16
8	(1, 1, 1, 1, 1, 2, 2, 3)	nonbasic	12
9	(1, 1, 1, 1, 1, 1, 1, 2, 9)	basic	18
9	(1, 1, 1, 1, 1, 1, 1, 3, 5)	nonbasic	15
10	(1, 1, 1, 1, 1, 1, 1, 1, 2, 10)	basic	20
10	(1, 1, 1, 1, 1, 1, 1, 1, 4, 4)	nonbasic	16
11	(1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 11)	basic	22
11	(1, 1, 1, 1, 1, 1, 1, 1, 1, 3, 6)	nonbasic	18
11	(1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 4)	nonbasic	16
12	(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 12)	basic	24
12	(1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2)	nonbasic	16

$x + y = xy$ with $x \leq y$. If either x or y is 1, then we have a contradiction. Therefore, $x, y \geq 2$, implying $x + y \leq y + y = 2y \leq xy$. If the first and last expressions are equal, then we must have only equalities, so $y = x$ and $x = 2$. Thus, the basic solution (2, 2) is the only solution for $n = 2$.

As we will soon need it, let’s note this last result for $n = 2$ more explicitly here: For positive integers x and y , we have $x + y \leq xy$, with equality if and only if $x = y = 2$.

Now, an unsurprising result: Suppose $m \geq 3$ and $2 \leq x_1 \leq x_2 \leq x_3 \leq \dots \leq x_m$ for an arbitrary m -tuple (x_1, x_2, \dots, x_m) of positive integers. Then

$$x_1 + x_2 + \dots + x_m < x_1 x_2 \dots x_m.$$

Proof. We use induction on $m \geq 3$. If $m = 3$, then $x + y + z \leq xy + z \leq xyz$, using the above $n = 2$ case results twice. However, since $xy > 2$, we have strict inequality in the second instance; hence $x + y + z < xyz$.

Suppose now that $m > 3$ and the result is true for $m - 1$. Then

$$(x_1 + x_2 + \dots + x_{m-1} + x_m) < x_1 x_2 \dots x_{m-1} + x_m \leq x_1 x_2 \dots x_{m-1} x_m.$$

This completes the proof, showing what seems obvious—that if we have three or more positive integers all greater than 1, then their sum is always less than the product. In any solution to the “sum equals product” problem (*) for $n > 2$, there must be at least one 1, and lots of them for larger n . ■

Viewing and generating solutions; padding Throughout this paper, let k denote the number of 1s in any n -tuple solution, and m the number of non-1s. (We call m the *index* of the solution.) In this notation, $n = k + m$.

We've already seen that $n > 2$ implies $k > 0$ for a solution to (*). Note also that $m \geq 2$; otherwise, $m = 1$, leading to

$$\prod_{i=1}^n x_i = x_n < \sum_{i=1}^n x_i.$$

Interestingly, we can always generate solutions from nonsolutions. Regard n as not yet fixed. Consider an m -tuple of positive integers (x_1, x_2, \dots, x_m) with $m \geq 3$ and no 1s. Since the product of the coordinates must exceed their sum, we "pad" the existing ordered sequence (x_1, x_2, \dots, x_m) with

$$k = x_1 x_2 \dots x_m - (x_1 + x_2 + \dots + x_m)$$

initial 1s. This padding has no effect on the product $x_1 x_2 \dots x_m$ but increases the original sum $x_1 + x_2 + \dots + x_m$ by $k = x_1 x_2 \dots x_m - (x_1 + x_2 + \dots + x_m)$ to $x_1 x_2 \dots x_m$. Relabel by adding k to each index. The resulting ordered sequence of $n = k + m$ numbers, $(1, 1, \dots, 1, x_{k+1}, x_{k+2}, \dots, x_n)$, is a solution to (*).

In fact, we need not even insist on all non-1s initially. For instance, the 4-tuple $(1, 2, 2, 4)$ is not a solution, having sum = 9 < product = 16, so we pad the 4-tuple with $16 - 9 = 7$ copies of 1, resulting in the 11-tuple solution $(1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 4)$ of index 3.

Index 2 We consider the case of precisely two non-1 components.

PROPOSITION 0. *Let $n \geq 2$ with $m = 2$. The equation (*) has a nonbasic solution of the form $(1, 1, \dots, 1, a, b)$ with $2 \leq a \leq b$ in the n -tuple if and only if $n - 1$ is composite. Moreover, for such a nonbasic solution, $b < n$ (the largest coordinate is less than the number of coordinates), and $ab < 2n$ (the common value of sum and product is less than twice the number of coordinates).*

Proof. Since the sum of the coordinates equals the product, we have $n - 2 + a + b = ab$ if and only if $n - 1 = ab - a - b + 1 = (a - 1)(b - 1)$. Thus, because $2 \leq a \leq b$, $n - 1$ is prime if and only if $a = 2$ and $b = n$. If $n > 2$, then we obtain the basic solution $(1, 1, \dots, 1, 2, n)$. If $n = 2$, then we obtain the basic solution $(2, 2)$.

It follows that the only values of n for which there exist nonbasic solutions of the form $(1, 1, 1, \dots, 1, a, b)$ are those for which $n - 1$ is composite. Choose a factorization $n - 1 = (a - 1)(b - 1)$, with $a - 1 > 1$ and $b - 1 < n - 1$.

For this nonbasic solution, $a - 1 \geq 2$ and $b - 1 = (n - 1)/(a - 1) \leq (n - 1)/2$, so $b \leq (n + 1)/2 < n$. Thus,

$$ab = (n - 2) + a + b \leq n - 2 + 2b \leq n - 2 + n + 1 = 2n - 1 < 2n. \quad \blacksquare$$

Compare these results with the case of a basic solution, for which the largest coordinate is n and the common value of sum and product is $2n$.

Boundedness properties of solutions Bounds, which may be interesting in their own right, can help us be sure of having found all solutions to (*) for a given value of n . These are extremely useful for computer programs, which can narrow the search dramatically.

BOUNDEDNESS PROPOSITION 1. *If*

$$v = x_1 + x_2 + \dots + x_n = x_1 x_2 \dots x_n$$

for positive integers $n > 1$ and $x_1 \leq x_2 \leq x_3 \leq \cdots \leq x_n$, then the common value of sum and product for any solution n -tuple is at most $2n$:

$$v \leq 2n.$$

In view of the basic solution, this bound is sharp: if the index $m > 2$, then $v < 2n$.

BOUNDEDNESS PROPOSITION 2. *If $x_1 + x_2 + \cdots + x_n = x_1 x_2 \cdots x_n$ for positive integers $n > 1$ and $x_1 \leq x_2 \leq x_3 \leq \cdots \leq x_n$, then $x_n \leq n$. That is, the largest coordinate of any solution is bounded from above by the number of coordinates.*

In view of the basic solution, this bound is sharp. If the index m is greater than 2, then $x_n < n$.

To simplify the proofs, which are otherwise very messy, it is convenient to begin with this

LEMMA. *Let $m \geq 2$ with $a_j \geq 1$ for all j . Then*

$$(a_1 + 1)(a_2 + 1) \cdots (a_m + 1) \geq 2(a_1 + a_2 + \cdots + a_m).$$

Proof. Use induction on m . If $m = 2$, then

$$(a_1 + 1)(a_2 + 1) - 2(a_1 + a_2) = (a_1 - 1)(a_2 - 1) \geq 0.$$

[Note that equality is possible, but only if some $a_j = 1$.] Now suppose we know that

$$(a_1 + 1)(a_2 + 1) \cdots (a_m + 1) \geq 2(a_1 + a_2 + \cdots + a_m)$$

for a given $m \geq 2$. Multiply each side by $(a_{m+1} + 1)$ to obtain

$$\begin{aligned} (a_1 + 1)(a_2 + 1) \cdots (a_m + 1)(a_{m+1} + 1) \\ \geq 2(a_1 + a_2 + \cdots + a_m) + 2a_{m+1}(a_1 + a_2 + \cdots + a_m) \\ > 2(a_1 + \cdots + a_m + a_{m+1}) \quad (\text{since } a_1 + a_2 + \cdots + a_m > 1). \end{aligned}$$

Note that equality is not possible for $m \geq 3$. ■

Proof of Boundedness Proposition 1. Let $n = k + m$, with k = number of 1s and m = number of non-1s. The common value of the sum and product is v .

First, $x_1 = x_2 = \cdots = x_k = 1$, so

$$\prod_{i=1}^n x_i = \prod_{i=k+1}^n x_i = \prod_{i=k+1}^n [(x_i - 1) + 1] = \prod_{j=1}^m [(x_{k+j} - 1) + 1],$$

where we've used $k + m = n$ and reindexed with $i = k + j$. For $j = 1, 2, \dots, m$, put $a_j = x_{k+j} - 1 \geq 1$. By the lemma,

$$\prod_{j=1}^m [(x_{k+j} - 1) + 1] \geq 2 \sum_{j=1}^m (x_{k+j} - 1).$$

Applying this to the common value v gives

$$\begin{aligned} v &\geq 2 \sum_{j=1}^m (x_{k+j} - 1) \\ &= 2 \sum_{i=1}^n x_i - 2k - 2m = 2v - 2n. \end{aligned}$$

Rearranging this inequality gives $v \leq 2n$. ■

We have proved the first proposition. However, note that, by the lemma, this last inequality is strict for $m > 2$. From this and Proposition 0, we conclude that only the basic solutions have

$$v = \sum_{i=1}^n x_i = \prod_{i=1}^n x_i = 2n.$$

Thus we have:

COROLLARY. *For solutions (*) of index $m > 2$, we have $2^{m-1} < n$.*

Proof.

$$2^m \leq \prod_{i=1}^n x_i < 2n. \quad \blacksquare$$

COMMENT. The average coordinate in any solution to (*) is at most 2, with equality only for the basic solution. (Given the large number of 1s in solutions, this makes sense.)

Proof of Boundedness Proposition 2. Since $m > 2$, there are at least two components different from 1, namely x_{k+1} and x_n , which must be at least 2. Then

$$2x_n \leq \prod_{i=1}^n x_i = v \leq 2n$$

by Boundedness Proposition 1, so $x_n \leq n$. Note that this last inequality is strict for $m \geq 3$. From this and Proposition 0 of the previous section we conclude that only the basic solutions have $x_n = n$, and all nonbasic solutions have $x_n < n$. \blacksquare

Incidentally, Dickson [1] cites Murent [2] as showing

$$2^m - m \leq n,$$

with equality only when the solution consists exclusively of 1s and 2s.

Application to Triangles: $n = 3$ We now handle by algebraic means the unanswered opening question: Are there triangles whose tangents are all integral?

Again, write $x = \tan A$, $y = \tan B$, and $z = \tan C$, and look for solutions to $x + y + z = xyz$, with $x \leq y \leq z$. Proposition 2 and our preliminary considerations show that $z \leq 3$ and $x = 1$. We note that $y > 1$. (Otherwise, $z = z + 2$.) So, $m = 2$. By Proposition 0 of section 4, since $n - 1 = 3 - 1 = 2$ is prime, the only solution is the basic one, $(1, 2, 3)$.

(Alternatively, once we know $z \leq 3$ and $x = 1$, we can simply enumerate the few remaining possibilities, each of the form $(1, y, z)$ with $y \leq z \leq 3$. Of the resulting few candidates, we eliminate all but $(1, 2, 3)$. This foreshadows the computer search we will carry out in a later section.)

It now follows that, up to similarity, there is precisely one triangle whose tangents are all integral. This triangle ABC has angles with tangents 1, 2, and 3; i.e., $\tan A = 1$, $\tan B = 2$, $\tan C = 3$. This subsumes the well-known result that $\arctan 1 + \arctan 2 + \arctan 3 = \pi$.

The search for exceptional values The solutions for the $n = 2, 3$ cases are each unique; their basic solutions are the only solutions. However, for most values of n ,

there are other solutions—nonbasic solutions. For which values of n is the basic solution the only one? Let's call a value of n *exceptional* if the corresponding basic solution is the only one.

Recall this conclusion for $m = 2$: The only values of n for which there are no nonbasic solutions of the form $(1, 1, \dots, 1, a, b)$ are those for which $n - 1$ is prime.

Hence, our search for exceptional values need only investigate those values of n for which $n - 1$ is prime and $m > 2$. So, consider such a solution $(1, 1, \dots, 1, x_{k+1}, x_{k+2}, \dots, x_n)$, which is nonbasic since it contains at least three coordinates greater than 1. The corollary above shows $n > 2^{3-1} = 4$, so $n = 2, 3$, and 4 are exceptional values.

Let's look back at the $m = 3$ case more closely. Now $n - 1$ is an odd prime. In order that $n - 1 = x_1 x_2 x_3 - (x_1 + x_2 + x_3) + 2$ be odd, precisely one of the x_i must be odd. So, consider $(1, 1, \dots, 1, 2, 2, 2j + 1)$, for which $n - 1 = 2 \times 2 \times (2j + 1) - (2 + 2 + 2j + 1) + 2 = 6j + 1$.

It follows that whenever $n - 1$ is a prime of the form $6j + 1$, there is at least one nonbasic solution, namely the $m = 3$ solution $(1, 1, \dots, 1, 2, 2, 2j + 1)$. The common value of sum and product is $v = 8j + 4$, and the number of 1s is $k = 6j - 1$.

Since all primes above 5 are of the form $6j + 1$ or $6j + 5$, we have reduced the problem to seeking nonbasic solutions when $n - 1$ is a prime of the form $6j + 5$. In other words, the only possible exceptional values still to be found must be hiding out among the integer multiples of 6, and specifically among those multiples that are 1 more than a prime.

Note that the smallest possible odd value for $n - 1$ in the displayed equation above is $n - 1 = 2 \cdot 2 \cdot 3 - (2 + 2 + 3) + 2 = 7$ (using $j = 1$). It follows that there is no nonbasic solution for $n - 1 = 5$, thus adding 6 to our list of exceptional values.

Let E denote the set of exceptional values. We can analyze more cases as we have above, or we can write a computer program, aided by the boundedness results. Thus:

CONJECTURE. *The set of exceptional values is finite: $E = \{2, 3, 4, 6, 24, 114, 174, 444\}$.*

As of mid-2000, I had tested up to $n = 316,200,000$, using improved computer programs by Harry J. Smith and Alan Zimmermann. In turn, they tested further, going past 10,000,000,000. We've found no other solutions.

Readers may wish to analyze more cases by hand, in searching for a proof of the conjecture. For example, is it coincidence that all the exceptional values listed here, beyond a certain point, have $n - 1$ a prime congruent to 23 mod 30?

Further exploration

- Easy Question 1) What is the set of the achieved common values $v = \sum_{i=1}^n x_i = \prod_{i=1}^n x_i$ as we vary n with $n > 1$? The answer is precisely the set of composite numbers. Given any composite number v , factor it nontrivially as ab . Then $(1, 1, \dots, 1, a, b)$, with k 1s, is a solution with $v = k + a + b = ab$, if $k = ab - a - b > 0$. On the other hand, if v is a prime p , then the only possibility to consider would be of the form $(1, 1, \dots, 1, p)$, but this is not a solution.
- Not-So-Easy Question 2) For $n > 1$, define

$$f(n) = \text{the number of different solutions to } \sum_{i=1}^n x_i = \prod_{i=1}^n x_i.$$

What can we say about the function f and its behavior? What is its range? Does f have a maximum? Are there infinitely many values of n for which $f(n) = 2$? If so, assuming it exists, what is the natural density of this set of values of n ?

Acknowledgments. I thank Herb Conn for pointing out the trigonometric identity of the sum and product of the tangents, which led me to think about all this. I also thank Harry J. Smith and Alan Zimmermann for programming support in search of exceptional values. I also thank an anonymous referee, who suggested the reference in Dickson.

REFERENCES

1. Leonard Eugene Dickson, *History of the Theory of Numbers*, Carnegie Institution of Washington publication, no. 256, Vol. II, 1934, p. 694.
2. J. Murent, *Nouv. Ann. Math.* (2), **4** (1865), 116–120.

The Scarcity of Regular Polygons on the Integer Lattice

DANIEL J. O'LOUGHLIN

Macalester College
St. Paul, Minnesota 55105
oloughlin@macalester.edu

While devising a lab about Green's Theorem for a calculus class, I happened on an amusing fact. The ideas needed to prove it span many areas of undergraduate mathematics; Green's Theorem itself is probably the most complicated, although some simple divisibility arguments and facts about rational roots of polynomials are needed for a fully rigorous proof. Consider:

THE THEOREM. *The only regular polygons in the plane whose coordinates are all integers are squares.*

I came upon this theorem more or less by accident. I wanted to find a good application of Green's Theorem for a lab exercise, and it occurred to me to ask students to show that no equilateral triangle has its vertices on the integer lattice in the plane, that is, with all vertex coordinates integers. Naturally, I wondered which regular polygons were possible: of course squares are trivially possible, and, with just a little thought, I was easily able to see that regular hexagons and octagons are not possible.

After I had proved this theorem in general, and shown it to a few colleagues, I was directed by Stan Wagon to a paper by Beeson [2], which contains many results along these lines. It addresses questions about triangles with their vertices on the integer lattice in n dimensions (which he calls *embeddable*). Beeson references two proofs of the theorem above, one by Schoenberg [4] and also a very elegant geometric proof attributed to Scherrer [3] in 1946. The advantage of the approach offered here is that it uses many areas of mathematics, all at a relatively elementary level, and can be used as part of an undergraduate course.

In my multivariable calculus classes, I have the students discover facts about polygonal areas and regular polygons using a simple program I wrote using *Matlab*. The program is interactive: the user enters the number of vertices in a polygon and the

coordinates of these vertices (in the plane). The computer then plots the polygon and gives its area. In the lab, the students discover that there cannot be an equilateral triangle whose vertices lie on the integer lattice in the plane by using fact **A** below.

Then the students show, using the same reasoning, that there cannot be any regular hexagons or octagons on the integer lattice. In a class with more advanced students—say, an abstract algebra class—the proof for all regular n -gons would be a nice addition.

Proving the Theorem The proof is straightforward once we establish three elementary facts:

- A.** If A is the area of any polygon all of whose vertices lie on the integer lattice in the plane, then $2A$ is an integer.
- B.** A formula for the area of a regular polygon with n sides in terms of its side length s is

$$A(P_n) = \frac{ns^2}{4 \tan\left(\frac{\pi}{n}\right)}.$$

- C.** When $n \geq 3$ the quantity $\tan(\pi/n)$ is rational only for $n = 4$.

The proof of the theorem now follows easily since any polygon whose vertices lie on the integer lattice must be one for which s^2 is an integer (apply the Pythagorean Theorem to any one of the sides). So in the formula for the area of a regular polygon with n sides we see that the area is rational only when $\tan(\pi/n)$ is rational, and this is only true when $n = 4$, that is, when the polygons are squares.

Proving the elementary facts

A. Let $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ be the n corners of a polygon P in the plane. Assume that the boundary of the polygon is oriented counterclockwise, then the area of the polygon is given by the following formula which can be found in many multivariable calculus texts [1, pp. 423–425]:

$$A(P) = \frac{1}{2} \left\{ \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} + \det \begin{pmatrix} x_2 & x_3 \\ y_2 & y_3 \end{pmatrix} + \cdots + \det \begin{pmatrix} x_n & x_1 \\ y_n & y_1 \end{pmatrix} \right\}. \quad (1)$$

This formula follows easily from Green's Theorem in the plane, by simply parametrizing each of the edges of the polygon, and applying Green's Theorem in the form:

$$A(P) = \oint_{\partial P} x \, dy.$$

Clearly this formula shows that any polygon whose vertices lie on the integer lattice in the plane must satisfy the simple condition that twice its area is an integer, since all of the entries in the 2×2 determinants are integers, and so each of the determinants is an integer, and the sum of all the determinants is an integer.

We should note that Green's Theorem, although it gave the impetus for this investigation, is not essential in the proof. As one of the referees pointed out, a bright student in a vector calculus course might say, "I can prove that with cross-products," and give reasoning as follows: by a suitable translation any lattice triangle can be assumed to have coordinates at $(0, 0)$, (m, n) , and (j, k) , where m, n, j , and k are integers. Then twice the area of the triangle is given by the length of the cross-product of the vectors, thought of as vectors in \mathbb{R}^3 , i.e., $\text{Area} = |(m, n, 0) \times (j, k, 0)| = |mk - jn|$, an integer. By partitioning the polygon into lattice triangles we get formula (1).

If you showed Fact A to students as an application of Green's Theorem, it would be interesting to see whether one of them comes up with the shorter proof.

B. This formula is very simple to derive using elementary trigonometry.

Let s be the length of each side of the regular polygon P_n with n sides. Inscribe P_n in a circle and subdivide it into n isosceles triangles. We will find the area of each of these triangles in terms of s and multiply by n . Each triangle has two sides of length r , which is the radius of the circle, and one side of length s . The central angle between the two sides of length r has measure $2\pi/n$. We find the height of the triangle using simple trigonometry:

$$h = \frac{s}{2 \tan\left(\frac{\pi}{n}\right)}.$$

So the area of the regular polygon is

$$A = n \left(\frac{1}{2} sh \right) = \frac{ns^2}{4 \tan\left(\frac{\pi}{n}\right)}.$$

C. The third fact may be the hardest to prove. No one part of the proof is difficult, but there are many parts.

The main idea here is to show that $\tan(\pi/k)$ is irrational whenever k is an odd prime. Then the proof for general k follows from the identity

$$\tan(\alpha + \beta) = \frac{\tan \alpha + \tan \beta}{1 - \tan \alpha \tan \beta}.$$

Clearly the left-hand side of this identity will be rational whenever the right-hand side is rational. Using this identity repeatedly we can show that if $\tan(\theta)$ is rational, then $\tan(m\theta)$ is rational. For example, since $\tan(\pi/3) = \sqrt{3}$ is irrational we can show that whenever k is a multiple of 3 then $\tan(\pi/k)$ is irrational, since otherwise we could use the identity to show that $\tan(\pi/3)$ is rational, which is not true. Similarly since $\tan(\pi/8) = \frac{1}{\sqrt{2}+1}$ is irrational then $\tan(\pi/k)$ is irrational if k is any multiple of 8, in particular if k is any power of 2 greater than 8.

Thus, the tangent identity lets us boil the proof down to the case when k has an odd prime factor greater than 3. Indeed, without loss of generality we can assume that k is an odd prime greater than 3. We also assume $\tan(\pi/k) = p/q$, where the greatest common divisor of p and q is 1, that is, the rational number is in lowest terms. Then we have

$$\sin\left(\frac{\pi}{k}\right) = \frac{p}{\sqrt{q^2 + p^2}} \quad \text{and} \quad \cos\left(\frac{\pi}{k}\right) = \frac{q}{\sqrt{q^2 + p^2}}.$$

In particular, we know that the following are rational numbers:

$$\sin\left(\frac{2\pi}{k}\right) = \frac{2pq}{q^2 + p^2} \quad \text{and} \quad \cos\left(\frac{2\pi}{k}\right) = \frac{q^2 - p^2}{q^2 + p^2}.$$

The terms $\sin(2\pi/k)$ and $\cos(2\pi/k)$ are the real and imaginary parts of one of the k th roots of unity, that is,

$$\left(\cos\left(\frac{2\pi}{k}\right) + i \sin\left(\frac{2\pi}{k}\right) \right)^k = 1$$

which, as $\tan(\pi/k) = p/q$, is equivalent to

$$(q^2 - p^2 + 2pqi)^k = (q^2 + p^2)^k.$$

Let k be any odd prime greater than or equal to 5; in this case we are guaranteed that $q > p$ since $\tan(\pi/5) < \tan(\pi/4) = 1$. Set $y = 2pq$ and consider

$$(q^2 - p^2 + yi)^k = (q^2 + p^2)^k.$$

Now equate the real and imaginary parts of the two sides of this equation. Looking at the imaginary parts we get the polynomial equation

$$y^k - \binom{k}{k-2}(q^2 - p^2)^2 y^{k-2} + \cdots \pm \binom{k}{3}(q^2 - p^2)^{k-3} y^3 \mp \binom{k}{1}(q^2 - p^2)^{k-1} y = 0.$$

Dividing by y we can rewrite this polynomial equation as:

$$y^{k-1} - \binom{k}{k-2}(q^2 - p^2)^2 y^{k-3} + \cdots \pm \binom{k}{3}(q^2 - p^2)^{k-3} y^2 \mp \binom{k}{1}(q^2 - p^2)^{k-1} = 0.$$

By the rational roots test, any rational root of this equation must be an integer and must divide the constant term, $k(q^2 - p^2)^{k-1}$. So if $2pq$ is such a root, then $2pq$ must divide $k(q^2 - p^2)^{k-1}$. We will show that this cannot happen.

Note that we cannot have both $p = 1$ and $q = k$, since for $k > 2$

$$\tan\left(\frac{\pi}{k}\right) > \frac{\pi}{k} > \frac{1}{k}.$$

This follows directly from the Maclaurin series for the tangent (see, for example, Stewart, [5, p. 618]), which is

$$\tan x = x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + \cdots.$$

So if $p = 1$, then $q < k$, since we have shown that $p/q > 1/k$. This implies that q must divide $k(q^2 - p^2)^{k-1}$, but since q cannot divide the prime k and since we are assuming that $p = 1$, this means that q divides $(q^2 - 1)^{k-1} = (q - 1)^{k-1}(q + 1)^{k-1}$. But this is impossible since q is relatively prime to both $q - 1$ and $q + 1$. So we cannot have $p = 1$ at all.

Therefore $q > p > 1$. So if $2pq$ is to divide $k(q^2 - p^2)^{k-1}$, then any prime factor of p or q must divide $k(q^2 - p^2)^{k-1}$, but cannot divide $(q^2 - p^2)^{k-1}$, for on expanding the binomial, we see that it already divides all but at most one of the terms; hence it would also have to divide the remaining term, contradicting our assumption that $\gcd(p, q) = 1$. Therefore all prime factors of p and q —and there must be more than one of these—must divide k . But k is itself prime, which is a contradiction.

Thus we have shown that $\tan(\pi/k)$ is irrational whenever k is an odd prime, and the proof is finished. ■

Although the original question which prompted this paper concerned regular polygons on the integer lattice, one of my colleagues correctly noticed—after a seminar I gave on this subject—that this theorem says more: *there can be no regular polygons (except squares) such that the vertices all have rational coordinates*. In other words there is an inherent irrationality to all non-square regular polygons. So the proof, as constructed here, goes beyond the proofs of Schoenberg [4] and Scherrer [3] mentioned earlier. Consult the paper by Beeson [2] for more similar results.

For more information on the lab which prompted this paper and which was first used in the spring of 1998 at the University of Minnesota, see <http://www.macalester.edu/~oloughlin/math37/>.

Acknowledgments. I would like to thank Mike Lawler, Paul Campbell, Stan Wagon, David Bressoud, and the referees for conversations and suggestions regarding this paper. I would also like to thank the diligent students in the Calculus Initiative at the University of Minnesota. They were very patient and helpful during the preparation of lab materials including some of the material in this paper.

REFERENCES

1. Thomas Barr, *Vector Calculus*, Prentice-Hall, 1997.
2. Michael J. Beeson, Triangles with vertices on lattice points, *Amer. Math. Monthly*, **99**:3 (1992), 243–252.
3. W. Scherrer, Die einlagerung eines regulären vielecks in ein gitter, *Elemente der Mathematik* **1**, (1946), 97–98.
4. I. J. Schoenberg, Regular simplices and quadratic forms, *Journal of the London Mathematical Society* **12**, (1937), 48–55.
5. James Stewart, *Multivariable Calculus: Concepts and Contexts*, Brooks-Cole, 1998.

Medical Tests and Convergence

STEPHEN FRIEDBERG

Illinois State University
Normal, IL 61790

In the syndicated column by Marilyn Vos Savant, a reader writes that she wants to be tested for a certain disease. However, she only wants to hear from her doctor if the news is good. Of course, having the doctor call her if and only if the result is good reveals bad news if the doctor does not call.

Marilyn suggests the following plan:

Take the test, and have the laboratory send the results to the doctor in a sealed envelope. The doctor flips a coin. If a head appears, then he looks at the result. If she does not have the disease, he calls her. If she does have the disease, he does not call her. If a tail appears, then he does not look at the result, and he does not call her.

This way, she only hears good news. If she hears nothing, she cannot conclude that the test result is bad.

Let us examine Marilyn's plan, using some basic real analysis and some results about difference equations. Two questions naturally come to mind.

- Q1. Is the patient really more comfortable with hearing nothing than she was before she took the test?
- Q2. Assuming that the patient is not called, what happens to the probability that she has the disease if the test result is sent to other doctors and a similar plan is used by each doctor?

The sample space may be described as consisting of the four outcomes, HD , HD' , TD , and TD' , where, for example, HD represents the outcome that the doctor obtains a head on the coin toss and the patient has the disease. The letter D' denotes the case that the patient does not have the disease. Let $p = \Pr(D)$ be the probability that she has

the disease. Suppose C is the event she is called and C' the event that she is not called. We are interested in comparing $\Pr(D|C')$, the probability that she has the disease when she is not called, with p . Note that by Marilyn's plan, $\Pr(C'|H)$, the probability that she is not called given that the doctor flipped heads, is simply p . Using the fact that $D \subset C'$, we have

$$\Pr(D|C') = \frac{\Pr(D \cap C')}{\Pr(C')} = \frac{\Pr(D)}{\Pr(C')}.$$

Also

$$\Pr(C') = \Pr(C'|H) \Pr(H) + \Pr(C'|T) \Pr(T) = p(1/2) + (1)(1/2).$$

From the previous two equations, we conclude that

$$\Pr(D|C') = \frac{p}{\frac{1}{2}p + \frac{1}{2}} = \frac{2p}{p+1} > p,$$

because $0 < p < 1$.

What does this mean? If she is not called, then she should be more worried under this plan than she was before she took the test. Therefore, the answer to our first question is "No," and for relatively rare diseases the "No" is even more resounding: the probability that she has the disease given that she is not called is about twice the probability that she has the disease at all.

Now suppose she is not called, and decides to seek the opinion of a second doctor, who will carry out the same scheme. For the second doctor, the probability that she has the disease is now $p_1 = 2p/(p+1)$. So, if she is not called a second time, the probability that she has the disease is $p_2 = 2p_1/(p_1+1)$. If her result is sent to n doctors, and she is not called by the n^{th} doctor, then the probability that she has the disease is

$$p_{n+1} = \frac{2p_n}{p_n + 1}. \quad (*)$$

We use two very different methods for evaluating the limit of the sequence p_n .

Analysis Note from (*) that $\{p_n\}$ is an increasing sequence that is bounded above (by 2); hence it converges to some number c . Clearly, $c > 0$. Let $n \rightarrow \infty$ in (*), and obtain

$$c = 2c/(c+1).$$

It follows that $c = 1$. So we have $p_n \rightarrow 1$ as $n \rightarrow \infty$.

Difference equations We recognize that (*) is a first order nonlinear nonhomogeneous difference equation with initial condition $p_0 = p$. Solving this would be a good exercise for students. Elementary techniques (see Goldberg [2]) yield the solution:

$$p_{n+1} = \frac{2^{n+1}p}{p(2^{n+1}-1)+1} = \frac{p}{p(1-2^{1-n})+2^{1-n}} \rightarrow 1$$

as $n \rightarrow \infty$.

What does this mean for our patient hoping to avoid bad news? If she requests that this process be repeated many times because she has not heard any news, then the probability that she has the disease approaches 1 no matter how small the initial

probability p is. This result not only conforms to our intuition, but our explicit formula for p_{n+1} allows us to check how quickly p_{n+1} converges to 1 for various values of p .

REFERENCES

1. R. Hogg and E. Tanis, *Probability and Statistical Inference*, Prentice Hall, Upper Saddle River, NJ, 1997.
2. S. Goldberg, *Introduction to Difference Equations*, Dover Publications, New York, NY, 1986.

Uniquely Determined Unknowns in Systems of Linear Equations

KENNETH HARDY

KENNETH S. WILLIAMS

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
khardy@math.carleton.ca
williams@math.carleton.ca

BLAIR K. SPEARMAN

Department of Mathematics and Statistics
Okanagan University College
Kelowna, British Columbia, Canada V1V 1V7
bkspearm@okuc02.okanagan.bc.ca

Perhaps the reader has noticed that when solving a consistent system of linear equations (linear system) it can happen that some unknowns are uniquely determined, while others are not?

EXAMPLE. Consider the linear system

$$\begin{cases} 6x_1 + 12x_2 + x_3 + 6x_4 + x_5 = 7, \\ 5x_1 + 10x_2 + x_3 + 5x_4 + x_5 = 6, \\ 13x_1 + 26x_2 + 2x_3 + 13x_4 + 3x_5 = 18, \end{cases}$$

over the field \mathbb{R} of real numbers. The solution set is

$$x_1 = 1 - 2s - t, \quad x_2 = s, \quad x_3 = -2, \quad x_4 = t, \quad x_5 = 3, \quad \text{where } s, t \in \mathbb{R},$$

and in this case x_3, x_5 are uniquely determined while x_1, x_2, x_4 can take infinitely many values.

This example suggests the following three questions.

QUESTION 1. *What is a necessary and sufficient condition for an unknown to be uniquely determined by a consistent linear system?*

QUESTION 2. *How many of the unknowns are uniquely determined by a linear system?*

QUESTION 3. *If an unknown is uniquely determined by a linear system, is there an explicit formula for it?*

In this paper we answer these questions for linear systems defined over an arbitrary field \mathbb{F} .

We will write a linear system in its matrix form

$$AX = B, \quad (1)$$

where the coefficient matrix is

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \in M_{m,n}(\mathbb{F}),$$

the column vectors of unknowns and constant terms are respectively

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in M_{n,1}(\mathbb{F}) \quad \text{and} \quad B = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \in M_{m,1}(\mathbb{F}),$$

and the augmented matrix is

$$[A \mid B] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{bmatrix} \in M_{m,n+1}(\mathbb{F}).$$

The linear system defined by (1) is consistent if and only if

$$\text{rank } A = \text{rank}[A \mid B]. \quad (2)$$

From this point on, we assume that (2) holds and so (1) has at least one solution $X \in M_{n,1}(\mathbb{F})$.

Let $A^{(j)}$ denote the $m \times (n - 1)$ matrix obtained by removing the j th column of A . Clearly, removing the j th column of A from A decreases the rank of A by at most 1. We can therefore classify the columns of the matrix A as either “rank-preserving” or “rank-decreasing.”

DEFINITION 1. *The j th column of A is said to be “rank-preserving” if $\text{rank } A^{(j)} = \text{rank } A$ and to be “rank-decreasing” if $\text{rank } A^{(j)} = \text{rank } A - 1$.*

For example the matrix

$$A = \begin{bmatrix} 1 & 2 & 4 & i \\ 1 & 2 + i & 4 + i & 2i \\ 1 + i & 3 & 5 + 2i & 1 - 3i \end{bmatrix} \in M_{3,4}(\mathbb{C}),$$

where \mathbb{C} denotes the field of complex numbers, has three rank-preserving columns and one rank-decreasing column because

$$\text{rank } A = \text{rank } A^{(1)} = \text{rank } A^{(2)} = \text{rank } A^{(3)} = 3, \quad \text{rank } A^{(4)} = 2.$$

We are now ready to answer Question 1.

THEOREM 1. *Suppose that the linear system defined by (1) is consistent. Then the unknown x_j ($j = 1, 2, \dots, n$) is uniquely determined if and only if the j th column of A is rank-decreasing.*

Proof. We denote the columns of A by C_1, C_2, \dots, C_n . Suppose that the j th column of A is rank-decreasing. Then $\text{rank } A^{(j)} = \text{rank } A - 1$. Hence C_j is not a linear combination of the other columns. Thus every solution of

$$AX = x_1 C_1 + \dots + x_j C_j + \dots + x_n C_n = 0$$

has $x_j = 0$, and so every solution of $AX = B$ has the same value for x_j . Hence x_j is uniquely determined.

Now suppose that the j th column of A is rank-preserving. Then $\text{rank } A^{(j)} = \text{rank } A$. Hence C_j is a linear combination of the other columns in A and so there are solutions of

$$AX = x_1 C_1 + \dots + x_j C_j + \dots + x_n C_n = 0$$

with $x_j \neq 0$. Hence $AX = B$ has solutions with different values of x_j . Thus x_j is not uniquely determined. ■

The linear system in the example has coefficient matrix

$$A = \begin{bmatrix} 6 & 12 & 1 & 6 & 1 \\ 5 & 10 & 1 & 5 & 1 \\ 13 & 26 & 2 & 13 & 3 \end{bmatrix},$$

and it is routine to check that $\text{rank } A = \text{rank } A^{(1)} = \text{rank } A^{(2)} = \text{rank } A^{(4)} = 3$ and that $\text{rank } A^{(3)} = \text{rank } A^{(5)} = 2$ so that only the third and fifth columns of A are rank-decreasing. Theorem 1 confirms that only x_3 and x_5 are uniquely determined.

Theorem 1 can now be applied to answer Question 2.

THEOREM 2. *Suppose that the linear system defined by (1) is consistent and that $r = \text{rank } A$. Then the number of unknowns that are uniquely determined by the system is*

$$nr - \sum_{j=1}^n \text{rank } A^{(j)}.$$

Proof. By Theorem 1, the number N of the x_j uniquely determined by (1) is precisely the number of rank-decreasing columns of A , and because

$$r - \text{rank } A^{(j)} = \begin{cases} 1, & \text{if the } j\text{th column of } A \text{ is rank-decreasing,} \\ 0, & \text{if the } j\text{th column of } A \text{ is rank-preserving,} \end{cases}$$

we have

$$N = \sum_{j=1}^n (r - \text{rank } A^{(j)}) = nr - \sum_{j=1}^n \text{rank } A^{(j)}. \quad \blacksquare$$

Applying Theorem 2 to the system in the example, we have

$$N = 5 \times 3 - (3 + 3 + 2 + 3 + 2) = 15 - 13 = 2.$$

DEFINITION 2. *For $i = 1, 2, \dots, n$ the matrix $E_i \in M_{1,n}(\mathbb{F})$ is defined by*

$$E_i = [0 \quad \dots \quad 0 \quad 1 \quad 0 \quad \dots \quad 0],$$

where 1 occurs in the i th place and 0 elsewhere.

We are now ready to answer Question 3. By eliminating any equations from the system (1) that are linear combinations of other equations, we may suppose without loss of generality that $m = r = \text{rank } A$.

THEOREM 3. Suppose that the linear system defined by (1) is consistent, and that $m = r$ ($= \text{rank } A$). Let A_i ($i = 1, 2, \dots, m$) denote the i th row of A . Integers k_1, \dots, k_{n-r} with $1 \leq k_1 < k_2 < \dots < k_{n-r} \leq n$ may be chosen so that

$$\text{span}(A_1, \dots, A_r, E_{k_1}, \dots, E_{k_{n-r}}) = \mathbb{F}^n.$$

Let $A^{(k_1, \dots, k_{n-r})} \in M_{r,r}(\mathbb{F})$ be formed from A by deleting columns k_1, \dots, k_{n-r} . Let $j \in \{1, 2, \dots, n\}$ be such that x_j is a uniquely determined unknown in (1). Let $A^{(k_1, \dots, k_{n-r})}(j, B) \in M_{r,r}(\mathbb{F})$ be formed from A by replacing the j th column by B and deleting columns k_1, \dots, k_{n-r} . Then

$$x_j = \frac{\det(A^{(k_1, \dots, k_{n-r})}(j, B)})}{\det(A^{(k_1, \dots, k_{n-r})})}.$$

Proof. As $\{E_1, \dots, E_n\}$ span \mathbb{F}^n and $\{A_1, \dots, A_r\}$ are linearly independent over \mathbb{F} , by the Steinitz Exchange Theorem [2, p. 276], r of $\{E_1, \dots, E_n\}$ can be replaced by $\{A_1, \dots, A_r\}$ so that

$$\text{span}(A_1, \dots, A_r, E_{k_1}, \dots, E_{k_{n-r}}) = \mathbb{F}^n,$$

where $1 \leq k_1 < k_2 < \dots < k_{n-r} \leq n$.

We note that as x_j is uniquely determined, E_j belongs to the row space of A so that $j \neq k_1, \dots, k_{n-r}$. Let $A^* \in M_{n,n}(\mathbb{F})$ be formed from A by adjoining $E_{k_1}, \dots, E_{k_{n-r}}$ as rows $r+1, \dots, n$. Clearly the set $\{A_1, \dots, A_r, E_{k_1}, \dots, E_{k_{n-r}}\}$ is a basis for \mathbb{F}^n and so $\det A^* \neq 0$. Moreover, using the Laplace expansion theorem (see, for example, [1, p. 21]) to expand $\det A^*$ by its last $n-r$ rows, we obtain

$$\det A^* = (-1)^{(r+1)+\dots+n+k_1+\dots+k_{n-r}} \det A^{(k_1, \dots, k_{n-r})}.$$

Hence

$$\det A^{(k_1, \dots, k_{n-r})} \neq 0. \quad (3)$$

Let $X^* \in M_{r,1}(\mathbb{F})$ be the column matrix formed from X by removing $x_{k_1}, \dots, x_{k_{n-r}}$. Set

$$B^* = B - x_{k_1} A^{(k_1)} - \dots - x_{k_{n-r}} A^{(k_{n-r})}.$$

Then the linear system defined by (1) can be rewritten as

$$A^{(k_1, \dots, k_{n-r})} X^* = B^*. \quad (4)$$

From (3) and (4) we see that all the x_v with $v \neq k_1, \dots, k_{n-r}$ are uniquely determined in terms of the $n-r$ free variables $x_{k_1}, \dots, x_{k_{n-r}}$. Thus x_j is independent of the choice of $x_{k_1}, \dots, x_{k_{n-r}}$ and so we may choose $x_{k_1} = \dots = x_{k_{n-r}} = 0$ in (4) to determine x_j . The matrix form of the linear system becomes

$$A^{(k_1, \dots, k_{n-r})} X^* = B$$

and Cramer's rule gives

$$x_j = \frac{\det(A^{(k_1, \dots, k_{n-r})}(j, B)})}{\det(A^{(k_1, \dots, k_{n-r})})}. \quad \blacksquare$$

We close by revisiting the example to compute the uniquely determined unknowns x_3 and x_5 . We have $m = 3$, $n = 5$, $r = 3 = \text{rank } A$ and $n-r = 2$ in this case. It is easy to check that

$$\text{span}(A_1, A_2, A_3, E_1, E_2) = \mathbb{R}^5$$

so that we can take $k_1 = 1, k_2 = 2$ here. By Theorem 3, we obtain

$$x_3 = \frac{\det(A^{(1,2)}(3, B))}{\det(A^{(1,2)})} = \frac{\begin{vmatrix} 7 & 6 & 1 \\ 6 & 5 & 1 \\ 18 & 13 & 3 \end{vmatrix}}{\begin{vmatrix} 1 & 6 & 1 \\ 1 & 5 & 1 \\ 2 & 13 & 3 \end{vmatrix}} = \frac{2}{-1} = -2$$

and

$$x_5 = \frac{\det(A^{(1,2)}(5, B))}{\det(A^{(1,2)})} = \frac{\begin{vmatrix} 1 & 6 & 7 \\ 1 & 5 & 6 \\ 2 & 13 & 18 \end{vmatrix}}{\begin{vmatrix} 1 & 6 & 1 \\ 1 & 5 & 1 \\ 2 & 13 & 3 \end{vmatrix}} = \frac{-3}{-1} = 3.$$

Acknowledgments. The authors would like to express their thanks to two unknown referees for suggestions for improvements to an earlier draft of this paper.

REFERENCES

1. L. Mirsky, *An Introduction to Linear Algebra*, Oxford, 1972.
2. W. K. Nicholson, *Elementary Linear Algebra*, McGraw-Hill Ryerson, 2001.

Counterintuitive Aspects of Plane Curvature

RUSSELL A. GORDON
COLIN FERGUSON

Whitman College
Walla Walla, WA 99362

A study of the curvature of a plane curve of the form $y = f(x)$ leads to some counterintuitive results. For instance, the curvature of a function whose graph is concave up may not approach 0 as x approaches ∞ , and the curvature of a function with a vertical asymptote at $x = c$ may not approach 0 as x approaches c . In addition, scaling a function affects its curvature qualitatively as well as quantitatively. A discussion of the limit properties of curvature involves ideas from elementary real analysis, while the impact of scaling can be used to create some exploratory exercises for calculus students using a computer algebra system.

Let f be a real-valued twice differentiable function defined on an interval I . The curvature κ of f , which is a measure of the rate at which the graph of $y = f(x)$ is turning, is given by

$$\kappa(x) = \frac{f''(x)}{(1 + (f'(x))^2)^{3/2}}$$

for each x in I . There are various ways to derive this formula; see most any calculus textbook. An elementary approach that illustrates some nice ideas from differential calculus (namely, using derivatives to find approximations of a function and implicit differentiation) is to determine the circle that “best” approximates the function f at $(c, f(c))$. This circle must go through the point $(c, f(c))$ and match the slope and concavity of the graph of f at c . The curvature of f at c is the reciprocal of the radius of this circle. (Some comments on the history of curvature and how Newton viewed this concept can be found in [2].)

We begin by considering the curvature of a function as x tends to infinity. For polynomials, a simple computation of the degrees of the terms that appear in the numerator and denominator of the formula for curvature make it clear that the curvature tends to zero, while it is obvious that the curvature of the sine function does not have a limit as x tends to infinity. In fact, for most of the functions that are found in calculus books, it can be shown easily that the curvature either tends to zero or does not have a limit as x tends to infinity. A look at over 80 calculus and advanced calculus books written in the past 100 years as well as a literature search revealed only two general comments on this topic. Loomis [5] and Grossman [4] both make the following claim:

- If f'' has constant sign for all $x > M$, then $\lim_{x \rightarrow \infty} \kappa(x) = 0$.

Loomis states only that the proof is too sophisticated for students at this level, while Grossman leaves the proof as a guided exercise. The result seems plausible geometrically, but it turns out to be false; an example will be given in a moment.

The problem with this statement is not the value of the limit but the existence of the limit. We will show that the curvature must tend to zero if it has a limit. Intuitively, if the curvature remains larger than some positive value (or smaller than some negative value), the graph will eventually curl back over itself like a circle and this, of course, is impossible for the graph of a function. The proof uses the fact that the curvature function has an elementary antiderivative.

As a reminder, the limit inferior of a function g is defined by

$$\begin{aligned}\liminf_{x \rightarrow \infty} g(x) &= \lim_{r \rightarrow \infty} \inf\{g(x) : x > r\} \quad \text{and} \\ \liminf_{x \rightarrow c^+} g(x) &= \lim_{r \rightarrow 0^+} \inf\{g(x) : c < x < c + r\}.\end{aligned}$$

THEOREM 1. If f is twice differentiable on an infinite interval (c, ∞) and κ represents the curvature of f , then $\liminf_{x \rightarrow \infty} |\kappa(x)| = 0$.

Proof. If the set $\{x \in (c, \infty) : \kappa(x) = 0\}$ is unbounded, then the result is trivial, so suppose that $\kappa(x) \neq 0$ for all $x > c_1 \geq c$. Since f'' has the intermediate value property (all derivatives have this property, see [1, p. 174]), it follows that f'' has constant sign on (c_1, ∞) . Without loss of generality, we may assume that f'' is positive on (c_1, ∞) . The proof proceeds by contradiction. Suppose that $\liminf_{x \rightarrow \infty} \kappa(x) = L > 0$ and let r be a number that satisfies $0 < r < L$. By the definition of limit inferior, there exists $d > c_1$ such that $\kappa(x) > r$ for all $x \geq d$. For each $x \geq d$,

$$\frac{d}{dx} \left(\frac{f'(x)}{\sqrt{1 + (f'(x))^2}} - rx \right) = \kappa(x) - r > 0,$$

which indicates that the function in parentheses is increasing. In particular, for each $x > d$,

$$\frac{f'(x)}{\sqrt{1 + (f'(x))^2}} > r(x - d) + \frac{f'(d)}{\sqrt{1 + (f'(d))^2}}.$$

This is a contradiction since the left side of the inequality is bounded by 1 and the right side is unbounded on the interval (d, ∞) . This completes the proof. ■

COROLLARY 2. Suppose that f is twice differentiable on an infinite interval (c, ∞) and let κ be the curvature of f . If κ has a limit as x tends to infinity, then $\lim_{x \rightarrow \infty} \kappa(x) = 0$. In particular, if the curvature of f is eventually monotone, then the curvature goes to zero as x tends to infinity.

In order to discuss the behavior of the curvature function at a vertical asymptote, we first consider the relationship between the curvature of a function and its inverse. Suppose that f is a twice differentiable function and that f' is nonzero on some interval I . Then f has an inverse on I . Let f_i denote the inverse of f , let $J = f(I)$ be the domain of f_i , and let κ_i be the curvature of f_i . Since the graph of $y = f_i(x)$ is simply the reflection of the graph of $y = f(x)$ through the line $y = x$, it should be clear that $|\kappa_i(x)| = |\kappa(f_i(x))|$ for all $x \in J$ or $|\kappa(x)| = |\kappa_i(f(x))|$ for all $x \in I$. If this geometric argument is not convincing, the reader can start with $f'_i(x) = 1/f'(f_i(x))$ and actually compute $\kappa_i(x)$ to obtain the same result.

THEOREM 3. Suppose that f is twice differentiable on an interval (v, w) and let κ represent the curvature of f . If $\lim_{x \rightarrow v^+} f(x) = \infty$, then $\liminf_{x \rightarrow v^+} |\kappa(x)| = 0$.

Proof. There are two cases. If f' oscillates between negative and positive values as $x \rightarrow v^+$, then (by the intermediate value property) f' equals 0 arbitrarily close to v and consequently (by Rolle's Theorem) f'' equals 0 arbitrarily close to v . The result then follows immediately. For the other case, we may assume that f' is positive on an interval (v, w_1) . Then f has an inverse on (v, w_1) . Let f_i be the inverse of f , let κ_i be the curvature of f_i , and note that f_i is twice differentiable on the interval $(f(w_1), \infty)$. By the remarks preceding the theorem and Theorem 1,

$$\liminf_{x \rightarrow v^+} |\kappa(x)| = \liminf_{x \rightarrow v^+} |\kappa_i(f(x))| = \liminf_{x \rightarrow \infty} |\kappa_i(x)| = 0.$$

This completes the proof. ■

We will now construct a function f that has the following two properties:

- i) f'' is positive on $(0, \infty)$, but the curvature of f does not have a limit as x tends to infinity;
- ii) the inverse of f has a vertical asymptote, but its curvature does not tend to 0 at the asymptote.

The motivating idea that lies behind the construction of this function is the following fact: if $\lim_{x \rightarrow \infty} h(x) = L$, then it does not follow that $\lim_{x \rightarrow \infty} h'(x) = 0$. This is the error in the outline of the proof given by Grossman, see [4, p. 737]. For each positive integer k , define a function g_k on \mathbb{R} by

$$g_k(x) = \begin{cases} 0, & \text{if } x < k - 2^{-k-1}; \\ 1 + \sin(2^k \pi(x - k)), & \text{if } k - 2^{-k-1} \leq x \leq k + 2^{-k-1}; \\ 2, & \text{if } x > k + 2^{-k-1}. \end{cases}$$

The function g_k is continuous and differentiable on \mathbb{R} and

$$g'_k(x) = \begin{cases} 0, & \text{if } x < k - 2^{-k-1}; \\ 2^k \pi \cos(2^k \pi(x - k)), & \text{if } k - 2^{-k-1} \leq x \leq k + 2^{-k-1}; \\ 0, & \text{if } x > k + 2^{-k-1}. \end{cases}$$

Note that $g'_k(x) \geq 0$ for all x and that $g'_k(k) = 2^k \pi$. Consider the function g that is defined by $g(x) = \sum_{k=1}^{\infty} g_k(x)/2^k$ for each real number x . The function g is nondecreasing since each of the terms of the series is nondecreasing and g is bounded since

$\lim_{x \rightarrow \infty} g(x) = \sum_{k=1}^{\infty} 2/2^k = 2$. For each positive integer n , $g(x) = \sum_{k=1}^n g_k(x)/2^k$ for x in the interval $[0, n]$. It follows that g is continuous and differentiable on \mathbb{R} and (since the remaining terms of the series are all 0) that $g'(x) = \sum_{k=1}^{\infty} g'_k(x)/2^k$ for all x . Note that g' is a nonnegative function and that $g'(n) = \pi$ for each positive integer n .

Now let f be the function defined by

$$f(x) = \int_0^x (g(t) - 2) dt + e^{-x}.$$

Then $f'(x) = g(x) - 2 - e^{-x} < 0$ for all $x > 0$ and $f''(x) = g'(x) + e^{-x} > 0$ for all $x > 0$. Hence, the function f is decreasing and concave up on the interval $(0, \infty)$. Since $\lim_{x \rightarrow \infty} f'(x) = 0$ and $f''(n) = \pi + e^{-n} > \pi$ for all n , the curvature of the function f cannot have a limit of 0 as x goes to infinity.

Since f is strictly decreasing on $(0, \infty)$, it has an inverse on $(0, \infty)$. To show that the inverse of f has a vertical asymptote, we must show that $\lim_{x \rightarrow \infty} f(x)$ exists. Since f is decreasing, it is sufficient to prove that the sequence $\{\int_0^n (g(x) - 2) dx\}$ converges. If n and k are positive integers with $k < n$, an elementary computation yields $\int_0^n g_k = 2(n - k)$. It follows that

$$\begin{aligned} \int_0^n (g(x) - 2) dx &= \sum_{k=1}^{n-1} \frac{1}{2^k} \int_0^n g_k + \frac{1}{2^n} \int_0^n g_n - 2n \\ &= \frac{1}{2^n} \int_0^n g_n + \sum_{k=1}^{n-1} \frac{n-k}{2^{k-1}} - \sum_{k=1}^{\infty} \frac{n}{2^{k-1}} \\ &= \frac{1}{2^n} \int_0^n g_n - \sum_{k=n}^{\infty} \frac{n}{2^{k-1}} - \sum_{k=1}^{n-1} \frac{k}{2^{k-1}} \\ &= \frac{1}{2^n} \int_0^n g_n - \frac{4n}{2^n} - 2 \sum_{k=1}^{n-1} \frac{k}{2^k}. \end{aligned}$$

The sequence in question converges to $-2 \sum_{k=1}^{\infty} k/2^k = -4$, so $\lim_{x \rightarrow \infty} f(x) = -4$.

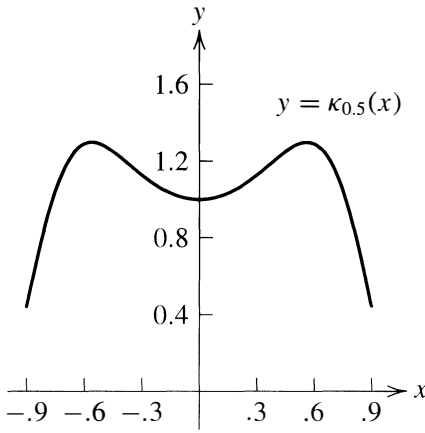
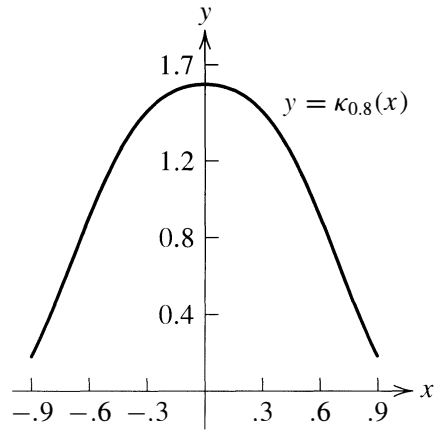
Thus, the function $f : [0, \infty) \rightarrow (-4, 1]$ is a bijection, and the graph of the inverse function of f has a vertical asymptote at -4 . By the remarks prior to Theorem 3, the curvature of this graph does not tend to zero as $x \rightarrow -4^+$.

Scaling The third aspect of curvature mentioned in the introduction involves the effect of scaling on the curvature of a function. Let f be a twice differentiable function, let a be a positive constant, and consider the graph of the function af . The parameter a represents a scaling of the y -axis. Since the curvature measures the rate at which a graph turns, it is no surprise that a stretching of the graph affects its curvature. The curvature κ_a of the function af at the point x is given by

$$\kappa_a(x) = \frac{af''(x)}{(1 + a^2(f'(x))^2)^{3/2}},$$

and this expression clearly depends on a in a nonlinear way. A somewhat surprising aspect of scaling is the fact that scaling changes curvature qualitatively as well as quantitatively.

To get a sense for the impact of scaling on the curvature function, consider the following pair of curvature graphs for two scalings of the function $y = -\ln(1 - x^2)$.

curvature for $y = -0.5 \ln(1 - x^2)$ curvature for $y = -0.8 \ln(1 - x^2)$

Clearly, the number of extreme points on the curvature graph depends on the parameter a or, to say it another way, the parameter a determines whether the curvature graph has a relative minimum or a relative maximum at 0. We will call the value of the scaling factor a at which the nature of the critical point at 0 on the curvature graph changes a **transition value** and denote it by a_t .

In order to generalize the problem, we will extrapolate the relevant properties of the function $-\ln(1 - x^2)$. The curvature of a sufficiently differentiable function f behaves in this way if $f'(0) = 0$, $f''(0) > 0$, and $\kappa'_a(0) = 0$ for all values of a . This last condition is satisfied if $f'''(0) = 0$. One way to determine the transition value is to examine the sign of $\kappa''_a(0)$ since κ_a has a relative minimum (maximum) at 0 if $\kappa''_a(0)$ is positive (negative). Using the properties of f , the reader can verify (with straightforward but tedious computations) that

$$\kappa''_a(0) = a(f^{(4)}(0) - 3a^2(f''(0))^3).$$

If $f^{(4)}(0) \leq 0$, then there is no transition value; the function κ_a has a relative maximum at 0 for all positive values of a . If $f^{(4)}(0) > 0$, then there is a transition value a_t given by

$$a_t = \sqrt{\frac{f^{(4)}(0)}{3(f''(0))^3}}.$$

If $0 < a < a_t$, then κ_a has a relative minimum at 0, and if $a_t < a < \infty$, then κ_a has a relative maximum at 0. Carrying out this computation for the function $f(x) = -\ln(1 - x^2)$ yields a transition value of $1/\sqrt{2}$, a value consistent with the graphs displayed previously.

Writing these results formally generates the following theorem.

THEOREM 4. Suppose that f has a continuous fourth derivative on an interval (v, w) containing 0, that $f'(0) = 0 = f'''(0)$, and that f'' is positive on (v, w) . Then f has a transition value if and only if $f^{(4)}(0)$ is positive and the transition value satisfies $a_t^2 = f^{(4)}(0)/3(f''(0))^3$.

One particularly simple class of functions with these properties are even functions that have a Maclaurin series expansion. Functions of this type can be expressed in the form $c_0 + c_2x^2 + c_4x^4 + c_6x^6 + \dots$. If c_2 and c_4 are positive, then the transition value satisfies $a_t^2 = c_4/c_2^3$.

It is important to clear up a possible misconception that could develop from the foregoing discussion. For the function $f(x) = -\ln(1 - x^2)$, the number of extreme points on the scaled curvature graphs drops from 3 to 1 as the scaling factor increases through the transition value. This is not always the case. For an example, consider the function $f(x) = 2x^2 + 3x^4 + 2x^5$ on the interval $(-1, \infty)$. The transition value for this function is $\sqrt{3/8} \approx 0.61237$ and careful examination of the curvature graphs and/or solving the equation $\kappa'_a(x) = 0$ shows that the number of extreme points of κ_a in $(-1, \infty)$ is three if $0 < a < \sqrt{3/8}$, three if $\sqrt{3/8} < a < 0.6250$, and one if $0.6251 < a < \infty$. The nature of the critical point at 0 does change at the transition value, but the number of extreme points does not decrease at that value. For the record, when $a = \sqrt{3/8}$, the curvature function has an inflection point at 0. After looking at the curvature graphs for various values of a , it is clear what happens and we leave it for the reader to view some of these graphs. As a second example, the function $g(x) = x^2 + x^4 + 4x^6$ on the interval $(-\infty, \infty)$ has a transition value of 1 and it can be shown that the number of extreme points of κ_a is three if $0 < a \leq 1$, five if $1 < a < 1.065$, and one if $1.066 < a < \infty$. For this function, the number of extreme points of the curvature function increases at the transition value.

Each of these last two functions has a second *transition value*, a value of the scaling factor for which the curvature function has a qualitative change. These values (approximately 0.6250 and 1.065, respectively) were determined using a computer algebra system. There appears to be no analytic formula for transition values of this type. It is this aspect of curvature that can be used to generate exploratory exercises for students who have access to a computer algebra system.

As a final comment, it is possible to look at scaling from a different point of view: fix a point u in the domain of f and see how the curvature of af at the point u varies with the parameter a . This problem was considered by Whittemore [6] as an aid to searching for empirical laws in experimental data before the days of computers. The interested reader can find some further results in [6].

REFERENCES

1. R. Bartle and D. Sherbert, *Introduction to Real Analysis*, 3rd ed., John Wiley & Sons, 2000.
2. J. L. Coolidge, The unsatisfactory story of curvature, *Amer. Math. Monthly*, **59** (1952) 375–379.
3. D. Gans, Angle of inclination and curvature, this MAGAZINE, **31** (1957) 31–32.
4. S. Grossman, *Calculus*, 2nd ed., Academic Press, New York, 1981.
5. L. Loomis, *Calculus*, Addison-Wesley, Reading, MA, 1974.
6. J. Whittemore, The effect of change of scale on curvature, *Amer. Math. Monthly*, **30** (1923) 22–26.

PROBLEMS

ELGIN H. JOHNSTON, *Editor*

Iowa State University

Assistant Editors: RĂZVAN GELCA, Texas Tech University; ROBERT GREGORAC, Iowa State University; GERALD HEUER, Concordia College; VANIA MASCIONI, Western Washington University; PAUL ZEITZ, The University of San Francisco

Proposals

To be considered for publication, solutions should be received by July 1, 2002.

1638. *Proposed by Jody M. Lockhart and William P. Wardlaw, U. S. Naval Academy, Annapolis, MD.*

Let m be a positive integer. Show that there are infinitely many positive integers k such that m is a divisor of f_k and $f_{k+1} - 1$, where f_n denotes the n -th Fibonacci number.

1639. *Proposed by José Luis Díaz-Barrero and Juan José Egozcue, Universitat Politècnica de Catalunya, Barcelona, Spain.*

Let $n \geq 3$ be a positive integer and let z_1, z_2, \dots, z_n be distinct, nonzero, complex numbers. Prove that

$$\sum_{k=1}^n \frac{1}{z_k} \left(-1 + (1 + z_k^{n-1}) \prod_{\substack{j=1 \\ j \neq k}}^n \frac{z_j}{z_j - z_k} \right) = 0.$$

1640. *Proposed by Péter Ivády, Budapest, Hungary.*

Show that for $0 < x, y < \pi/2$,

$$\frac{x \csc x + y \csc y}{2} < \sec \left(\frac{x+y}{2} \right).$$

1641. *Proposed by Murray S. Klamkin, University of Alberta, Edmonton, Alberta, Canada.*

We invite readers to submit problems believed to be new and appealing to students and teachers of advanced undergraduate mathematics. Proposals must, in general, be accompanied by solutions and by any bibliographical information that will assist the editors and referees. A problem submitted as a Quickie should have an unexpected, succinct solution.

Solutions should be written in a style appropriate for this MAGAZINE. Each solution should begin on a separate sheet.

Solutions and new proposals should be mailed to Elgin Johnston, Problems Editor, Department of Mathematics, Iowa State University, Ames, IA 50011, or mailed electronically (ideally as a \LaTeX file) to ehjohnst@iastate.edu. All communications should include the readers name, full address, and an e-mail address and/or FAX number.

Show that if the midpoints of the six edges of a tetrahedron lie on a sphere, then the tetrahedron has an orthocenter.

1642. *Proposed by Erwin Just (Emeritus) and Norman Schaumberger (Emeritus), Bronx Community College, New York, NY.*

Prove that for any positive integer k there is a positive integer n such that there exists a set of n consecutive odd integers that includes more than $k\lfloor\sqrt{n}\rfloor$ primes.

Quickies

Answers to the Quickies are on page 69.

Q917. *Proposed by Norman Schaumberger (Emeritus), Bronx Community College, New York, NY.*

Prove that if $b > a > 0$, then $(\frac{a}{b})^a > \frac{e^a}{e^b} > (\frac{a}{b})^b$.

Q918. *Proposed by Jayavel Sounderpandian, University of Wisconsin–Parkside, Kenosha, WI.*

On a horizontal plane, n boys B_1, B_2, \dots, B_n of equal weight are standing at points P_1, P_2, \dots, P_n , respectively. Initially, B_1 is facing B_2 , B_2 is facing B_3 , \dots , B_n is facing B_1 . Every boy turns through angle θ_0 to his left. Then B_1 moves forward a distance equal to $a(P_1P_2)$; B_2 moves forward a distance equal to $a(P_2P_3)$; \dots ; B_n moves forward a distance equal to $a(P_nP_1)$, where a is a nonnegative real number. Prove that after all boys have moved, the center of gravity of the boys is at the same point it was before any of the boys moved.

Solutions

A Recursion in Four Parts

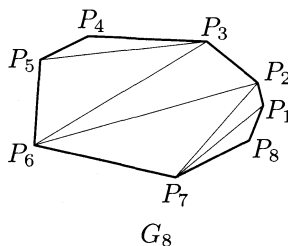
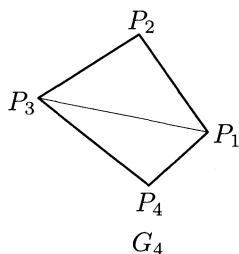
February 2001

1613. *Proposed by Emeric Deutsch, Polytechnic University, Brooklyn, NY.*

Given a convex n -gon $P_1P_2\cdots P_n$, let G_n be the graph obtained as a result of tracing the zig-zag polygonal path

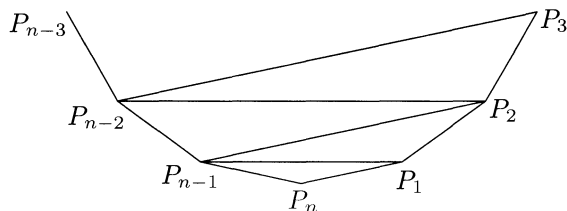
$$P_1P_{n-1}P_2P_{n-2}P_3P_{n-3}\cdots P_m,$$

where $m = (n-1)/2$ if n is odd and $m = (n+2)/2$ if n is even. (In the figure below we show G_4 and G_8 .) For $n \geq 3$, let a_n be the number of sets of nonadjacent edges from G_n . Find a recurrence relation satisfied by the a_n s. (As an example, $a_4 = 8$ because in addition to the empty set, G_4 has 5 sets consisting of one edge each and 2 sets consisting of two nonadjacent edges.)



All of the solvers listed below submitted a solution along the following lines.

Let $n \geq 7$. The portion of the graph G_n that includes vertices P_1, P_2, P_{n-1} , and P_n is shown below.



If S is any set of nonadjacent vertices from G_n , then exactly one of the following is true:

- S contains neither edge $P_1 P_n$ nor edge $P_{n-1} P_n$.
- S contains $P_1 P_n$.
- S contains $P_{n-1} P_n$ but does not contain $P_1 P_2$.
- S contains $P_{n-1} P_n$ and $P_1 P_2$.

If a) is true, then S is a set of disjoint edges from a graph that is isomorphic to G_{n-1} . There are a_{n-1} such sets.

If b) is true, then S contains none of the edges $P_1 P_2, P_1 P_{n-1}, P_{n-1} P_n$. Thus when $P_1 P_n$ is deleted from S the remaining edges are a set of disjoint edges from a graph isomorphic to G_{n-2} . There are a_{n-2} such sets.

By similar reasoning, there are a_{n-3} sets satisfying c), and a_{n-4} sets satisfying d). Thus, for $n \geq 7$,

$$a_n = a_{n-1} + a_{n-2} + a_{n-3} + a_{n-4}.$$

Solved by Roy Barbara (Lebanon), Daniele Donini (Italy), Robert L. Doucette, Reiner Martin, Skidmore College Problem Group, Joel Schlosberg, Alexey Vorobyov, Li Zhou, and the proposer. There was one incorrect submission.

Simultaneous Minima

February 2001

1614. Proposed by Achilleas Sinefakopoulos, student, University of Athens, Athens, Greece.

Determine the minimum values of each of $x + y - xy$ and $x + y + xy$, where x and y are positive real numbers such that $(x + y - xy)(x + y + xy) = xy$.

I. Solution by Heinz-Jürgen Seiffert, Berlin, Germany.

The condition $(x + y - xy)(x + y + xy) = xy$ is equivalent to $(x + y)^2 = xy(xy + 1)$. Because $(x + y)^2 \geq 4xy$ and x and y are positive, it follows that $xy \geq 3$. Hence

$$x + y - xy = \sqrt{xy(xy + 1)} - xy = \frac{1}{\sqrt{1 + \frac{1}{xy}} + 1} \geq \frac{1}{\sqrt{\frac{4}{3} + 1}} = 2\sqrt{3} - 3,$$

with equality when $x = y = \sqrt{3}$. In addition

$$x + y + xy \geq 2\sqrt{xy} + xy \geq 2\sqrt{3} + 3,$$

again with equality when $x = y = \sqrt{3}$.

II. *Solution by Daniele Donini, Bertinoro, Italy.*

The positive real numbers x and y satisfy $(x + y - xy)(x + y + xy) = xy$ if and only if $u = 1/x$ and $v = 1/y$ satisfy

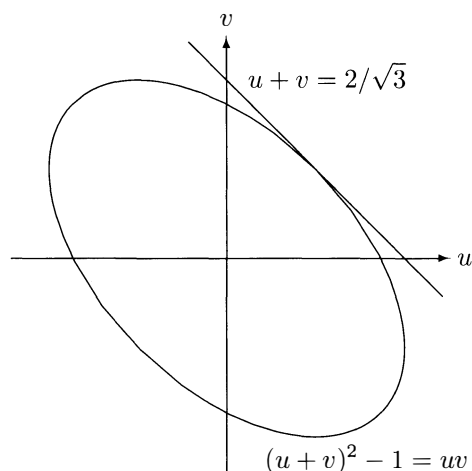
$$(u + v)^2 - 1 = uv. \quad (1)$$

Equation (1) is the equation of an ellipse in the (u, v) -plane. This ellipse can be obtained by rotating through an angle of 45° about the origin an ellipse with axes parallel to the u - and v -axes. See the accompanying figure. Next observe that if u and v are positive and satisfy (1), then

$$x + y - xy = \frac{1}{u + v + 1} \quad \text{and} \quad x + y + xy = \frac{1}{u + v - 1}. \quad (2)$$

The line $u + v = c$ is tangent to the ellipse when $c = 2/\sqrt{3}$; this is the maximum value of $u + v$ for (u, v) on the ellipse. It follows from (2) that the minimum values of $x + y - xy$ and $x + y + xy$ are, respectively,

$$\frac{1}{\frac{2}{\sqrt{3}} + 1} = 2\sqrt{3} - 3 \quad \text{and} \quad \frac{1}{\frac{2}{\sqrt{3}} - 1} = 2\sqrt{3} + 3.$$



Also solved by Reza Akhlaghi, Herb Bailey, Roy Barbara (Lebanon), Michel Bataille (France), Robert Betts, Jean Bogaert (Belgium), Brian Bradie, Len Brin, Marc A. Brodie, Minh Can, John Christopher, Jeffrey Clark, Con Amore Problem Group (Denmark), Robert L. Doucette, Petar Drianov (Canada), Andrew Iannaccone, Stephen Kaczowski, Victor Y. Kutsenok, George B. Marketos, Daniel R. Patten, Shiva K. Saksena, Volkhard Schindler (Germany), Joel Schlosberg, Ajaj A. Tarabay and Bassem B. Ghalayini (Lebanon), Tracy Wang, Dean Witter III, Michael Woltermann, Li Zhou, and the proposer. There were also five incorrect submissions and one solution with no name.

A Drawn Out Process

February 2001

1615. *Proposed by M. N. Deshpande, Nagpur, India.*

An urn contains 3 white balls and $2n - 3$ black balls, with $n \geq 2$. Balls are drawn from the urn two at a time, at random and without replacement. At each stage, the two balls drawn are inspected. If they are of the same color, they are set aside and two more balls are drawn. This process continues until a drawn pair consists of two balls of different color, after which the process stops. Let E_n denote the expected number of balls drawn before the process is stopped. Prove that $(2n - 1)E_n$ is a perfect square.

Solution by JPV Abad, San Francisco, CA.

Imagine that the $2n$ balls are drawn one at a time from the urn. There are then $\binom{2n}{3}$ possible sequences of the 3 white and $2n - 3$ black balls. Each of these sequences is equally likely. Now consider the first two balls drawn to be the first pair, the third and fourth drawn to be the second pair, and so forth. The number of sequences in which balls of different color first occur in the k th pair can be counted by considering two cases:

Case 1: one of the previous $k - 1$ pairs was white-white.

Case 2: no white ball was drawn among the earlier $k - 1$ pairs.

There are $2(k - 1)$ possible sequences described by Case 1, and $2\binom{2n-2k}{2}$ sequences described by Case 2. It follows that

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

Also solved by Robert A. Agnew, Michael Andreoli, Herb Bailey, Roy Barbara (Lebanon), Michel Bataille (France), David M. Bloom, Jean Bogaert (Belgium), Brian Bradie, Marc A. Brodie, Con Amore Problem Group (Denmark), Daniele Donini (Italy), Robert L. Doucette, Jerrold W. Grossman, James C. Hickman, Mike Hitchman, Stephen Kaczowski, N. J. Kuenzi, Kathleen E. Lewis, Reiner Martin, Robert Patenaude, Rob Pratt, Dave Trautman, Shiva K. Saksena, Joel Schlosberg, Skidmore College Problem Group, Alexey Vorobyov, Michael Vrabie, Dean Witter III, Michael Woltermann, Li Zhou, Harald Ziehms (Germany), Paul J. Zwier, and the proposer. There were also two incorrect submissions.

Sharp Bounds on Sums

February 2001

1616. *Proposed by Erwin Just (Emeritus) and Norman Schaumberger (Emeritus), Bronx Community College, NY.*

Let $k \geq 2$ be a positive integer, and let S_k be the set of all numbers of the form $\sum_{j=1}^k \frac{a_j}{a_j + b_j}$, where $a_j, b_j > 0$ for $1 \leq j \leq k$ and $\sum_{j=1}^k a_j = \sum_{j=1}^k b_j$. Determine the greatest lower bound and the least upper bound of S_k .

Solution by Bill Stone, New Mexico Institute of Mining and Technology, Socorro, NM.

We show that the greatest lower bound of S_k is $\frac{1}{2}$ and the least upper bound is $k - \frac{1}{2}$.

Because $\sum_{j=1}^k a_j = \sum_{j=1}^k b_j$, there is a j_0 with $a_{j_0} \geq b_{j_0}$. Because $k \geq 2$ and all terms are positive,

$$\sum_{j=1}^k \frac{a_j}{a_j + b_j} > \frac{a_{j_0}}{a_{j_0} + b_{j_0}} \geq \frac{1}{2}.$$

Hence $\frac{1}{2}$ is a lower bound for S_k . Next, for $0 < \epsilon < \frac{1}{k}$, let $a_1 = a_2 = \dots = a_{k-1} = \epsilon^2$ and $a_k = 1 - (k-1)\epsilon^2$, and let $b_1 = b_2 = \dots = b_{k-1} = \epsilon$ and $b_k = 1 - (k-1)\epsilon$. We then have

$$\sum_{j=1}^k \frac{a_j}{a_j + b_j} = (k-1) \frac{\epsilon}{1+\epsilon} + \frac{1 - (k-1)\epsilon^2}{2 - (k-1)\epsilon - (k-1)\epsilon^2}.$$

As $\epsilon \rightarrow 0^+$, this expression approaches $\frac{1}{2}$. Thus $\frac{1}{2}$ is the greatest lower bound of S_k .

Next observe that both $\sum_{j=1}^k \frac{a_j}{a_j+b_j}$ and $\sum_{j=1}^k \frac{b_j}{a_j+b_j}$ are in S_k , and that

$$\sum_{j=1}^k \frac{a_j}{a_j+b_j} + \sum_{j=1}^k \frac{b_j}{a_j+b_j} = k.$$

It follows that $\text{lub } S_k = k - \text{glb } S_k = k - \frac{1}{2}$.

Also solved by Roy Barbara (Lebanon), Michel Bataille (France), Jean Bogaert (Belgium), Knut Dale (Norway), Daniele Donini (Italy), Robert L. Doucette, Andrew Iannaccone, Reiner Martin, Markus Neher (Germany), Joel Schlosberg, Aja A. Tarabay and Bassem B. Ghalayini (Lebanon), Alexey Vorobyov, Li Zhou, and the proposer. There were also four incorrect submissions and one solution with no name.

A Four Square Inequality

February 2001

1617. *Proposed by Zhang Yun, First Middle School of Jin Chang City, Gan Su Province, China.*

Let $A_1A_2A_3A_4$ be a cyclic quadrilateral that also has an inscribed circle. Let B_1, B_2, B_3 , and B_4 , respectively, be the points on sides A_1A_2, A_2A_3, A_3A_4 , and A_4A_1 at which the inscribed circle is tangent to the quadrilateral. Prove that

$$\left(\frac{A_1A_2}{B_1B_2}\right)^2 + \left(\frac{A_2A_3}{B_2B_3}\right)^2 + \left(\frac{A_3A_4}{B_3B_4}\right)^2 + \left(\frac{A_4A_1}{B_4B_1}\right)^2 \geq 8.$$

Solution by Achilleas Sinefakopoulos, University of Athens, Athens, Greece.

Set $a_i = A_iA_{i+1}$ and $b_i = B_iB_{i+1}$, $i = 1, 2, 3, 4$, where the subscripts are taken modulo 4. We assume only that $A_1A_2A_3A_4$ has an inscribed circle of center O and radius r , and prove more generally that

$$\left(\frac{a_1}{b_1}\right)^2 + \left(\frac{a_2}{b_2}\right)^2 + \left(\frac{a_3}{b_3}\right)^2 + \left(\frac{a_4}{b_4}\right)^2 \geq \frac{8}{\sin^2\left(\frac{A_2 + A_4}{2}\right)}. \quad (*)$$

Because the right hand side of $(*)$ is greater than or equal to 8, this proves the inequality in the problem statement for all quadrilaterals that have an inscribed circle.

By the arithmetic-geometric mean inequality, the left side of $(*)$ is greater than or equal to $4\sqrt{\frac{a_1a_2a_3a_4}{b_1b_2b_3b_4}}$. Thus, it suffices to show that

$$a_1a_2a_3a_4 \sin^4\left(\frac{A_2 + A_4}{2}\right) \geq 4b_1b_2b_3b_4.$$

Because line OA_{i+1} is the perpendicular bisector of segment B_iB_{i+1} and bisects $\angle B_iOB_{i+1} = \theta_i$ we have $b_i = 2r \sin(\theta_i/2)$, $i = 1, 2, 3, 4$. Moreover, by Jensen's inequality,

$$\sin \frac{\theta_1}{2} \sin \frac{\theta_2}{2} \sin \frac{\theta_3}{2} \sin \frac{\theta_4}{2} \leq \sin^4\left(\frac{\theta_1 + \theta_2 + \theta_3 + \theta_4}{8}\right) = \sin^4\left(\frac{\pi}{4}\right) = \frac{1}{4}.$$

Thus, we need only prove that

$$a_1a_2a_3a_4 \sin^4\left(\frac{A_2 + A_4}{2}\right) \geq 16r^4.$$

Let K and s be, respectively, the area and semiperimeter of $A_1A_2A_3A_4$. Because $A_1A_2A_3A_4$ has an inscribed circle, $s = a_1 + a_3 = a_2 + a_4$. Hence, using the area formula for a general quadrilateral,

$$\begin{aligned}
 K^2 &= (s - a_1)(s - a_2)(s - a_3)(s - a_4) - a_1 a_2 a_3 a_4 \cos^2 \left(\frac{A_2 + A_4}{2} \right) \\
 &= a_1 a_2 a_3 a_4 \sin^2 \left(\frac{A_2 + A_4}{2} \right).
 \end{aligned}$$

Because $A_1 A_2 A_3 A_4$ has an inscribed circle we also have $K = (a_1 + a_3)r = (a_2 + a_4)r$. Hence,

$$\begin{aligned}
 a_1 a_2 a_3 a_4 \sin^4 \left(\frac{A_2 + A_4}{2} \right) &= \frac{K^4}{a_1 a_2 a_3 a_4} = \frac{(a_1 + a_3)^2}{a_1 a_3} r^2 \frac{(a_2 + a_4)^2}{a_2 a_4} r^2 \\
 &\geq 4r^2 \cdot 4r^2 = 16r^4.
 \end{aligned}$$

Also solved by Roy Barbara (Lebanon), Michel Bataille (France), Jean Bogaert (Belgium), Minh Can, Con Amore Problem Group (Denmark), Daniele Donini (Italy), Robert L. Doucette, Ovidiu Furdui, Victor Y. Kutsenok, Joel Schlosberg, Ajaj A. Tarabay and Bassem B. Ghalayini (Lebanon), Alexey Vorobyov, Robert L. Young, Li Zhou, Paul J. Zwier, and the proposer. There was also one incorrect submission.

Answers

Solutions to the Quickies from page 64.

A917. Solution I. Applying the Mean Value Theorem to the function defined by $x \ln x - x$, we find

$$\ln b > \frac{(b \ln b - b) - (a \ln a - a)}{b - a} > \ln a.$$

Hence

$$\ln b^{b-a} > \ln \left(\frac{b^b}{a^a} e^{a-b} \right) > \ln a^{b-a}.$$

The desired result follows after exponentiating, then multiplying by $\frac{a^a}{b^b}$.

Solution II. It is well known that for real r , the strictly monotone sequence $a_n = (1 + \frac{r}{n})^n$ increases to e^r . Taking $n = 1$ and $r = \frac{b-a}{a}$ we find

$$\frac{b}{a} = \left(1 + \frac{b-a}{a} \right) < e^{(b-a)/a} \quad \text{from which} \quad \frac{e^a}{e^b} < \left(\frac{a}{b} \right)^a.$$

Similarly,

$$\frac{a}{b} = \left(1 + \frac{a-b}{b} \right) < e^{(a-b)/b} \quad \text{leads to} \quad \left(\frac{a}{b} \right)^b < \frac{e^a}{e^b}.$$

A918. Assume that the boys are in the complex plane, and that P_k is the complex number associated with the position of B_k . Without loss of generality we may assume that the center of gravity is at the origin, so $\sum_{k=1}^n P_k = 0$. After moving as described in the problem statement, B_k will be at position $P_k + ae^{i\theta_0}(P_{k+1} - P_k)$, where subscripts are taken modulo n . Because

$$\sum_{k=1}^n (P_k + ae^{i\theta_0}(P_{k+1} - P_k)) = \sum_{k=1}^n P_k + ae^{i\theta_0} \sum_{k=1}^n (P_{k+1} - P_k) = 0,$$

the position of the center of gravity is unchanged.

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 mathematics literature. Readers are invited to suggest items for review to the editors.

A Beautiful Mind. Film from Universal Pictures (PG-13, 129 min). Directed by Ron Howard, written by Akiva Goldsman, based on the book by Sylvia Nasar. With Russell Crowe and Jennifer Connelly.

Taylor, Charles, "A Beautiful Mind," *Salon* (21 December 2001), http://salon.com/ent/movies/review/2001/12/21/beautiful_mind/index.html.

Scott, A.O., From math to madness and back, *New York Times* (21 December 2001), E1, E37; <http://www.nytimes.com/2001/12/21/movies/21MIND.html>.

Carr, Jay, 'Beautiful Mind' brilliantly probes a genius's agony, *Boston Globe* (21 December 2001), F1; http://www.boston.com/dailyglobe2/355/living/_Beautiful_Mind_brilliantly_probes_a_genius_s_agony.html.

Turan, Kenneth, A perplexing equation, *Los Angeles Times* (21 December 2001), <http://www.latimes.com/entertainment/printedition/calendar/la-000100941dec21.story>.

Whitty, Stephen, Traversing mental fault lines of a genius, (Newark, NJ) *Star-Ledger* (21 December 2001), Ticket section, 28; <http://www.njo.com/entertainment/ledger/index.ssf%3Fmovies/ledger/155f268.html>.

Hunter, Stephen, Fragile genius of "A Beautiful Mind," *Washington Post* (21 December 2001), C1; <http://www.washingtonpost.com/wp-dyn/articles/A9998-2001Dec20.html>.

Clark, John, So smart it hurts, *Los Angeles Times* (16 December 2001); <http://www.latimes.com/entertainment/printedition/calendar/la-000099609dec16.story>.

Thompson, Nicholas, The math in 'A Beautiful Mind,' *Boston Globe* (1 January 2002), E1; http://www.boston.com/dailyglobe2/001/science/The_math_in_A_Beautiful_mind+.html.

Nasar, Sylvia, and Harold W. Kuhn (eds.), *The Essential John Nash*, Princeton University Press, 2002; \$29.95. ISBN 0-691-09527-2. Chapter 1: Press Release—The Royal Swedish Academy of Sciences and Chapter 2: Autobiography are available at http://pup.princeton.edu/chapters/s1_7238.html or at http://pup.princeton.edu/chapters/s1_7238.pdf.

Warsh, David, The Nash program, *Boston Globe* (30 December 2001), E2; http://www.boston.com/dailyglobe2/364/business/The_Nash_program+.html. Meyerson, Roger B., Nash equilibrium and the history of economic theory, *Journal of Economic Literature* **37** (3) (September 1999) 1067–1082.

Johnson, Paul B., and Zwillinger, Daniel, News and letters: Simpler, simpler, ... [proofs of first-player win in Hex], this *MAGAZINE* **49** (3) (May 1976) 156. Brown, Cameron, *Hex Strategy: Making the Right Connections*, A K Peters, 2000; xi + 242 pp, \$38.50 (P). ISBN 1-56881-117-9. By the time you read this, *A Beautiful Mind* will have come and gone from your area theater. The distributor's strategy of releasing it first only in a few major markets kept it 50 miles away from me before this issue's deadline, yet I could read the opinions of those big-city critics who did get to see it. So, I can't review the film; the best I can do is review the reviews and pass on some perspective.

Any film based on actual people or events has the compelling advantage that audience interest is enhanced by the basis in reality but also the unavoidable drawback that it cannot be a completely faithful mirror of that original reality. Even a documentary is fictionalized in part by the choice of materials to include and to exclude. This film was not intended to be a documentary but may be perceived as one by audiences, who may regard it as comparable in that regard to the competing film *Ali* and similar docudramas. *A Beautiful Mind* leaves out facts about John Nash that would diminish audience sympathy ("we aren't told that ..."), and some critics condemn the simplifications in the film: "this isn't some concoction. It's the story of a man's life. ... It's John Nash's life,

being turned into an Oscar machine and an easy way to jerk tears" (Charles Taylor in *Salon*). A. O. Scott of the *New York Times* raises the crucial question, "How much fidelity do movies owe to the historical figures they purport to be about?", and goes on to suggest that here the divergence is great enough that "the movie character should be thought of as 'Nash prime' or Nash *i* (referring to an imaginary number). The story of this Nash is not without its beauty." Director Howard says that "the idea was to use the architecture of this life to surprise people and offer real insight into . . . mental illness." Kenneth Turan of the *Los Angeles Times* notes that "Screenwriter Akiva Goldsman and director Howard are candid about the way their film is what biographer Nasar describes as 'a highly stylized dramatization rather than a literal retelling' of those events, in which everything from the nature of Nash's incapacitating delusions to the shape of his marriage has been changed for dramatic effect." All of this is to say that the film tells a story based on Nash's life, but it is a different story from Nash's. How different? And how much does that matter? Those are certainly interesting questions; but what is important in the end is whether the story that the film tells inspired you and your nonmathematical friends and neighbors. Richard Roeper and Roger Ebert of TV's "Ebert and Roeper at the Movies" thought it should—it was one of only three films they both agreed on as being in the year's top 10.

But, as John Clark suggests, is that story mainly the familiar anti-intellectual one of the genius as miserable "tortured artist"—about genius humbled to our level, so we can feel good?

As mathematicians, we could hope that the film educates about what Nash did in mathematics, but reviewers complain that they get little inkling. Mathematicians can turn to the new collection of his papers edited by Sylvia Nasar and Harold Kuhn. Nonmathematicians may find understandable—but hyperbolic—the brief summary by David Warsh of economist Roger Meyerson's assessment of Nash as more central to 20th century mathematics than Keynes, Samuelson, or Friedman and his work "as fundamental and pervasive" to the social sciences as the discovery of the double helix structure of DNA to the biological sciences . . . because it unlocks the hidden structure of social interaction."

After you describe Nash's work for friends and they reach a high level of admiration (if not understanding), bring them back to earth: Teach them the game of Hex (which Nash invented independently of Piet Hein) and show them the clever nonconstructive topological proof that the first player can win, even though we don't know how. You could then discuss the equivalence of this result to the Brouwer fixed-point theorem (and do the crumpled paper demonstration of that result), plus the fact that Hex is PSPACE-hard (so finding a winning strategy in effect demands constructing the entire enormous tree of the game). Don't pass up letting the film occasion a lesson in mathematics.

Holden, Constance, For mathematics, Abel = Nobel, *Science* **293** (7 September 2001) 1761.

If you have always felt that you and John Nash were deprived because there is no Nobel Prize in mathematics, then this news is for you: The Norwegian government has established an annual "Abel Prize" in mathematics, in honor of the 200th birthday of Niels Henrik Abel (1802–1829). Worth about \$500,000, it will be awarded for the first time in 2003 by the Norwegian Academy of Science and Letters. (The Nobel Prizes are worth about \$1 million each but usually are shared.)

Lapointe, Joe, Disputed selection is revenge of the nerds, *New York Times* (10 December 2001) D1, D8. Sandomir, Richard, What computers choose to ignore, *New York Times*, (15 October 2001); <http://www.nytimes.com/2001/10/15/sports/ncaafootball/15RANK.html>. Dufresne, Chris, Background computer stories of BCS, *Los Angeles Times* (18 October 2001); <http://www.latimes.com/sports/la-000083115oct18.story>. Dufresne, Chris, Now seen . . . but not nerd, *Los Angeles Times* (18 October 2001), <http://www.latimes.com/sports/la-000083118oct18.story>. Bowl winners, sinners, *USA Today* (31 December 2001) 10A; <http://www.usatoday.com/news/comment/2001-12-31-edtwof2.htm>.

I write on January 1 amid contention about whether the Rose Bowl invited the two best teams. That pairing is determined by the Bowl Championship Series (B.C.S.) formula, based on eight ranking systems plus polls (full details are in the sidebar "It's Miami and Nebraska," *New York Times* (10 December 2001) D8). Strangely, only one of the eight ranking systems was devised by a statistician; and the *New York Times* ranking was eliminated from the formula for this season because the *Times* would not alter its system to conform to B.C.S. demands on how it should be slanted differently. The *USA Today* editorial details how invitations to other bowls are based on ticket sales, TV ratings, and payments from the universities. "Bowls were invented . . . as meaningless exhibitions to promote holiday tourism in Sunbelt cities. . . . That's still their primary reason for existence."

NEWS AND LETTERS

62nd Annual William Lowell Putnam Mathematical Competition

Editor's Note: The *American Mathematical Monthly* will print additional Putnam solutions later in the year. The solutions here were chosen to be among the most elementary.

PROBLEMS

A1 Consider a set S and a binary operation $*$ on S (that is, for each a, b in S , $a * b$ is in S). Assume that $(a * b) * a = b$ for all a, b in S . Prove that $a * (b * a) = b$ for all a, b in S .

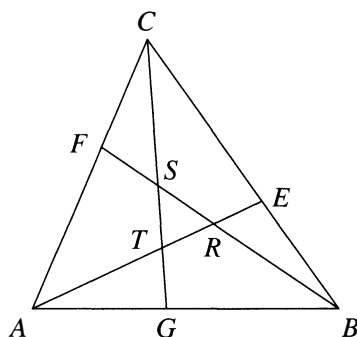
A2 You have coins C_1, C_2, \dots, C_n . For each k , coin C_k is biased so that, when tossed, it has probability $1/(2k + 1)$ of falling heads. If the n coins are tossed, what is the probability that the number of heads is odd? Express the answer as a rational function of n .

A3 For each integer m , consider the polynomial

$$P_m(x) = x^4 - (2m + 4)x^2 + (m - 2)^2.$$

For what values of m is $P_m(x)$ the product of two nonconstant polynomials with integer coefficients?

A4 Triangle ABC has area 1. Points E, F, G lie, respectively, on sides BC, CA, AB such that AE bisects BF at point R , BF bisects CG at point S , and CG bisects AE at point T . Find the area of triangle RST .



A5 Prove that there are unique positive integers a, n such that

$$a^{n+1} - (a + 1)^n = 2001.$$

A6 Can an arc of a parabola inside a circle of radius 1 have length greater than 4?

B1 Let n be an even positive integer. Write the numbers $1, 2, \dots, n^2$ in the squares of an $n \times n$ grid so that the k th row, from left to right, is

$$(k-1)n+1, (k-1)n+2, \dots, (k-1)n+n.$$

Color the squares of the grid so that half of the squares in each row and in each column are red and the other half are black (a checkerboard coloring is one possibility). Prove that for each such coloring, the sum of the numbers on the red squares is equal to the sum of the numbers on the black squares.

B2 Find all pairs of real numbers (x, y) satisfying the system of equations

$$\begin{aligned}\frac{1}{x} + \frac{1}{2y} &= (x^2 + 3y^2)(3x^2 + y^2) \\ \frac{1}{x} - \frac{1}{2y} &= 2(y^4 - x^4).\end{aligned}$$

B3 For any positive integer n let $\langle n \rangle$ denote the closest integer to \sqrt{n} . Evaluate

$$\sum_{n=1}^{\infty} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n}.$$

B4 Let S denote the set of rational numbers different from $-1, 0$ and 1 . Define $f : S \rightarrow S$ by $f(x) = x - \frac{1}{x}$. Prove or disprove:

$$\bigcap_{n=1}^{\infty} f^{(n)}(S) = \emptyset,$$

where $f^{(n)} = \underbrace{f \circ f \circ \dots \circ f}_{n \text{ times}}$.

(Note: $f(S)$ denotes the set of all values $f(s)$ for $s \in S$.)

B5 Let a and b be real numbers in the interval $(0, \frac{1}{2})$ and let g be a continuous real-valued function such that $g(g(x)) = ag(x) + bx$ for all real x . Prove that $g(x) = cx$ for some constant c .

B6 Assume that $(a_n)_{n \geq 1}$ is an increasing sequence of positive real numbers such that $\lim_{n \rightarrow \infty} \frac{a_n}{n} = 0$. Must there exist infinitely many positive integers n such that

$$a_{n-i} + a_{n+i} < 2a_n \quad \text{for } i = 1, 2, \dots, n-1?$$

SOLUTIONS

Solution to A1 For a, b in S , $a * (b * a) = [(b * a) * b] * (b * a) = b$.

Solution to A2 Let P_n denote the desired probability. We will use induction to show that $P_n = n/(2n+1)$. The result is true for $n=1$ because the first coin is biased in this way by assumption. Assume the result is true when n such biased coins are tossed, and now toss the $n+1$ coins, biased as indicated. There are two independent ways of obtaining an odd number of heads: there are an odd number of heads

among C_1, C_2, \dots, C_n and C_{n+1} falls tails, or there are an even number of heads among C_1, C_2, \dots, C_n and C_{n+1} falls heads. This translates into the recurrence,

$$\begin{aligned} P_{n+1} &= P_n \left(1 - \frac{1}{2n+3} \right) + (1 - P_n) \left(\frac{1}{2n+3} \right) \\ &= \left(\frac{2n+1}{2n+3} \right) P_n + \frac{1}{2n+3}. \end{aligned}$$

Therefore, by the induction assumption,

$$P_{n+1} = \left(\frac{2n+1}{2n+3} \right) \frac{n}{2n+1} + \frac{1}{2n+3} = \frac{n+1}{2n+3},$$

which is the desired form, so the induction is complete.

Solution to A3 $P_m(x)$ factors if and only if m or $2m$ is a perfect square.

- (i) $P_m(x)$ has a factor $x^2 + a$ (a an integer)
 \iff the quadratic $y^2 - (2m+4)y + (m-2)^2$ has a factor of the form $y + a$
 \iff the discriminant $(2m+4)^2 - 4(m-2)^2 = 32m$ is a perfect square
 $\iff 2m$ is a perfect square.
- (ii) $P_m(x)$ has a factor $x^2 + ax + b$ (with a, b integers, $a \neq 0$)
 $\iff P_m(x) = (x^2 + ax + b)(x^2 - ax + b)$ (since coefficients of x, x^3 in P_m are 0)
 $\iff 2b - a^2 = -2m - 4$ and $b^2 = (m-2)^2$.
 The choice $b = -(m-2)$ leads to $a^2 = 8$, which is impossible. The choice $b = m-2$ leads to $a^2 = 4m$, which is solvable if and only if m is a perfect square.

Finally, note that if $P_m(x)$ has a linear factor $x + a$, then $x - a$ would also be a factor (a is a root if and only if $-a$ is a root), so $x^2 - a^2$ would be a factor, hence this case is subsumed in (i).

Solution to A4 The area of triangle RST is $(7 - 3\sqrt{5})/4$:

Let K_{XYZ} denote the area of triangle XYZ . Let $x = \overline{BE}/\overline{BC}$, $y = \overline{CF}/\overline{CA}$, and $z = \overline{AG}/\overline{AB}$. Then $K_{ABE} = K_{ABE}/K_{ABC} = x$. Because

$$\frac{K_{AGT}}{K_{ABE}} = \frac{\overline{AG} \cdot \overline{AT}}{\overline{AB} \cdot \overline{AE}} = \frac{\overline{AG}}{\overline{AB}} \cdot \frac{\overline{AT}}{\overline{AE}} = \frac{z}{2},$$

$K_{AGT} = xz/2$. By symmetry, $K_{BCF} = y$, $K_{CAG} = z$, $K_{BER} = yx/2$, $K_{CFS} = zy/2$. Because $AT = TE$, $K_{ACT} = K_{ACE}/2$, or

$$K_{ACT} = K_{CAG} - K_{AGT} = \frac{K_{ABC} - K_{ABE}}{2},$$

and so

$$z - \frac{xz}{2} = \frac{1-x}{2}.$$

By symmetry,

$$x - \frac{yx}{2} = \frac{1-y}{2}, \quad y - \frac{zy}{2} = \frac{1-z}{2}.$$

Solving this system, we find

$$x = y = z = \frac{3 - \sqrt{5}}{2}$$

(the root $(3 + \sqrt{5})/2$ is > 1 and therefore extraneous). Then

$$\begin{aligned} K_{RST} &= K_{ABC} - K_{ACT} - K_{BAR} - K_{CBS} \\ &= 1 - 3K_{ACT} = 1 - 3\left(\frac{1-x}{2}\right) = \frac{7 - 3\sqrt{5}}{4}. \end{aligned}$$

Solution to A5 Suppose that a, n are positive integers and

$$a^{n+1} - (a+1)^n = 2001.$$

Looking at this equation modulo a , we see that a divides 2002. Looking at the equation modulo 3, we see that $a \equiv 1 \pmod{3}$ and that n is even. Looking at the equation modulo $a+1$, we see that $a+1$ divides 2002. Thus, in any solution, a and $a+1$ must be divisors of 2002. Because $2002 = 2 \times 7 \times 11 \times 13$, we see that the only possibilities for a are 1 and 13. The case $a = 1$ is quickly discarded. Because n is even and $13^2 \equiv 1 \pmod{8}$, $13^{n+1} \equiv 5 \pmod{8}$, so that $14^n \equiv 5 - 2001 \equiv 4 \pmod{8}$. Thus, $n = 2$, and the choice $a = 13, n = 2$ does work; that is,

$$13^3 - 14^2 = 2001.$$

Solution to A6 The answer is yes. Let b be any number with $0 < b < 1$, and consider the parabola with vertex at $(0, -1)$ and which passes through $(\pm\sqrt{1-b^2}, b)$. This parabola is $y = cx^2 - 1$, with $c = 1/(1-b)$. Solving for the nonnegative x branch, we get $x = \sqrt{(y+1)(1-b)}$ and so the arc length from $y = -1$ to $y = b$ is

$$L(b) = \int_{-1}^b \sqrt{1 + \frac{1-b}{4(y+1)}} dy.$$

Then the arc length of the parabolic arc is $2L(b)$. Note that $L(1) = 2$ corresponds to a degenerate parabola. We will show that $L(b)$ is decreasing as $b \rightarrow 1^-$, so there is some nondegenerate parabola with $L(b) > 2$, and so with arc length > 4 . Taking the derivative of $L(b)$ with respect to b , we get

$$L'(b) = \sqrt{1 + \frac{1-b}{4(y+1)}} - \frac{1}{8} \int_{-1}^b \frac{dy}{(y+1)\sqrt{1 + \frac{1-b}{4(y+1)}}}.$$

We have

$$\int_{-1}^b \frac{dy}{(y+1)\sqrt{1 + \frac{1-b}{4(y+1)}}} = \int_0^{1+b} \frac{dt}{t\sqrt{1 + \frac{1-b}{4t}}} > \int_{1-b}^{1+b} \frac{dt}{t\sqrt{1 + \frac{1-b}{4t}}}.$$

For t in the range $1-b \leq t \leq 1+b$, we have

$$1 + \frac{1-b}{4t} \leq \frac{5}{4},$$

so that

$$\int_{1-b}^{1+b} \frac{dt}{t\sqrt{1+\frac{1-b}{4t}}} > \frac{1}{2} \int_{1-b}^{1+b} \frac{dt}{t} = \frac{1}{2} \log \frac{1+b}{1-b}.$$

We conclude that $L'(b) \rightarrow -\infty$ as $b \rightarrow 1^-$, so that there is some $\beta < 1$ with $L'(b) < 0$ for $\beta < b < 1$. This shows there is some choice for b with $L(b) > 2$.

Solution to B1 The grid G can be separated into two parts, G_1 and G_2 .

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ n+1 & n+2 & \cdots & n+n \\ 2n+1 & 2n+2 & \cdots & 2n+n \\ 3n+1 & 3n+2 & \cdots & 3n+n \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ n & n & \cdots & n \\ 2n & 2n & \cdots & 2n \\ 3n & 3n & \cdots & 3n \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} + \begin{bmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}$$

Let S, S_1, S_2 denote the sum of the numbers on the red squares of G, G_1, G_2 , respectively. Then, $S = S_1 + S_2$. Regardless of how the coloring is done, subject to the stipulations, half of the numbers in each row of G_1 are red, so the sum of the red numbers in the k th row of G_1 is $((k-1)n) \cdot (n/2)$, and therefore $S_1 = \sum_{k=1}^n \frac{(k-1)n^2}{2}$. Similarly, half of the numbers in each column of G_2 are red, so the sum of the red numbers in the k th column of G_2 is $k \cdot (n/2)$; thus $S_2 = \sum_{k=1}^n (kn)/2$. It follows that

$$S = \sum_{k=1}^n \frac{(k-1)n^2}{2} + \sum_{k=1}^n \frac{kn}{2} = \frac{n^2}{2} \sum_{k=1}^n (k-1) + \frac{n}{2} \sum_{k=1}^n k = \frac{n^2(n^2+1)}{4}.$$

This number (equal to one-half the sum of all the numbers in G) is independent of the coloring, as long as each row and column contains exactly half red squares. More succinctly,

$$\begin{aligned} \text{Red sum} &= \sum_{(i,j) \text{ Red}} ((i-1)n + j) \\ &= \sum_{(i,j) \text{ Red}} (i-1)n + \sum_{(i,j) \text{ Red}} j \\ &= \sum_{i=1}^n (i-1)n \cdot (\#\{j : (i,j) \text{ Red}\}) + \sum_{j=1}^n j \cdot (\#\{i : (i,j) \text{ Red}\}) \\ &= \frac{n^2}{2} \sum_{i=1}^n (i-1) + \frac{n}{2} \sum_{i=1}^n i \end{aligned}$$

Solution to B2 Add and subtract, multiply the results by x and y respectively, to obtain the equivalent system

$$\begin{aligned} x^5 + 10x^3y^2 + 5xy^4 &= 2 \\ 5x^4y + 10x^2y^3 + y^5 &= 1. \end{aligned}$$

Add and subtract these to get

$$(x+y)^5 = 3 \quad \text{and} \quad (x-y)^5 = 1,$$

from which it follows that

$$x = \frac{3^{1/5} + 1}{2} \quad \text{and} \quad y = \frac{3^{1/5} - 1}{2}.$$

(The other complex fifth roots don't give real solutions for x and y .)

Solution to B3 Note that

$$\sum_{n=1}^{\infty} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n} = \sum_{n=1}^{\infty} \frac{1}{2^{n-\langle n \rangle}} + \sum_{n=1}^{\infty} \frac{1}{2^{n+\langle n \rangle}}.$$

We claim that the multiset $A = \{n - \langle n \rangle : n \geq 1\} = \{0, 1, 1, 2, 3, 4, 4, 5, 6, \dots\}$ consists of the natural numbers with the positive squares repeated, while $B = \{n + \langle n \rangle : n \geq 1\} = \{2, 3, 5, 5, 6, 7, \dots\}$ consists of the positive integers with the positive squares omitted. It follows that every positive integer appears exactly twice in the multiset $A \cup B$, so that

$$\sum_{n=1}^{\infty} \frac{2^{\langle n \rangle} + 2^{-\langle n \rangle}}{2^n} = 1 + 2 \sum_{k=1}^{\infty} \frac{1}{2^k} = 3.$$

To establish the claims, we use

$$\begin{aligned} \langle n \rangle = k &\iff k - \frac{1}{2} < \sqrt{n} < k + \frac{1}{2} \\ &\iff k^2 - k + \frac{1}{4} < n < k^2 + k + \frac{1}{4} \\ &\iff (k-1)k < n \leq k(k+1). \end{aligned}$$

In particular,

$$\langle n+1 \rangle = \langle n \rangle + 1 \iff n = k(k+1) \quad \text{for some } k.$$

Now $n - \langle n \rangle = n + 1 - \langle n + 1 \rangle \iff \langle n + 1 \rangle = \langle n \rangle + 1$, so that integers repeated in A are of the form $n - \langle n \rangle = k(k+1) - k = k^2$.

But we also have $n + 1 + \langle n + 1 \rangle > n + \langle n \rangle + 1 \iff \langle n + 1 \rangle = \langle n \rangle + 1$, so that integers skipped in B are of the form $n + \langle n \rangle + 1 = k(k+1) + k + 1 = (k+1)^2$.

Solution to B4 We will show that the intersection is empty.

It suffices to show that if $p/q \in f^{(n)}(S)$, where p, q are integers, then $|pq| > 2^n$.

The result holds (vacuously) for $n = 0$.

Suppose the result holds for $n = k$ and that $p/q \in f^{(k+1)}(S)$. Then $p/q = (r^2 - s^2)/rs$ where $r/s \in f^{(k)}(S)$. We may assume that $\gcd(r, s) = 1$, in which case $\gcd(r^2 - s^2, rs) = 1$. Then $|pq| \geq |r - s| \cdot |r + s| \cdot |r| \cdot |s| > 2 \cdot 2^k = 2^{k+1}$, so the claim follows by induction.

Solution to B5 We show that there are exactly two such functions, namely, $g_1(x) = \rho_1 x$ and $g_2(x) = \rho_2 x$, where ρ_1, ρ_2 are the roots of $x^2 - ax - b$. Say

$$\rho_1 = \frac{a + \sqrt{a^2 + 4b}}{2}, \quad \rho_2 = \frac{a - \sqrt{a^2 + 4b}}{2}.$$

Then

$$\rho_2 < 0 < \rho_1 \quad \text{and} \quad |\rho_2| < |\rho_1| < 1.$$

The given condition implies that g is one-to-one; indeed, if $g(x) = g(y)$ then $g(g(x)) = g(g(y))$, so $bx = by$, which implies $x = y$. Because g is continuous and one-to-one, g is monotonic. The condition also implies that g is unbounded (above and below), for otherwise there is a sequence (s_n) with $\lim_{n \rightarrow \infty} s_n = \pm\infty$ and $\lim_{n \rightarrow \infty} g(s_n) = B \neq \pm\infty$ leading to the contradiction $g(g(B) - ag(B)) = \lim_{n \rightarrow \infty} g(g(s_n)) - ag(s_n) = \lim_{n \rightarrow \infty} bs_n = \pm\infty$. Hence, g is invertible.

For all t and all integers n , we have

$$g^n(t) = \left(\frac{g(t) - \rho_2 t}{\rho_1 - \rho_2} \right) \rho_1^n + \left(\frac{\rho_1 t - g(t)}{\rho_1 - \rho_2} \right) \rho_2^n. \quad (1)$$

This is shown via two inductions, one for positive n and one for negative n using $g(x) = ax + bg^{-1}(x)$ (obtained by substituting $g^{-1}(x)$ for x in the functional equation).

In particular, $\lim_{n \rightarrow \infty} g^n(0) = 0$ and so, by continuity, $g(0) = g(\lim_{n \rightarrow \infty} g^n(0)) = \lim_{n \rightarrow \infty} g^{n+1}(0) = 0$.

Case 1: g is increasing. Since $g(0) = 0$, $\text{sign}(g(x)) = \text{sign}(x)$ for all x . It follows that $g(t) = \rho_1 t$, for all t , otherwise $\text{sign}(g^n(t))$ alternates for negative n of large absolute value since $g^n(t)$ is then dominated by the second term in (1).

Case 2: g is decreasing. Since $g(0) = 0$, $\text{sign}(g(x)) = -\text{sign}(x)$ for all x . It follows that $g(t) = \rho_2 t$, otherwise $\text{sign}(g^n(t))$ is stable for large positive n since $g^n(t)$ is then dominated by the first term in (1).

Solution to B6 Consider the convex hull of the set of points (n, a_n) in the plane. For each real number $x \geq 1$, let $f(x)$ be the largest number such that $(x, f(x))$ is in the convex hull. Then, f is continuous, piecewise linear, increasing, and concave down. Further, there are infinitely many vertices on the graph of f ; that is, points where f is not differentiable. Such points must occur at original points (n, a_n) from which the process was started, and such numbers n satisfy the condition of the problem.

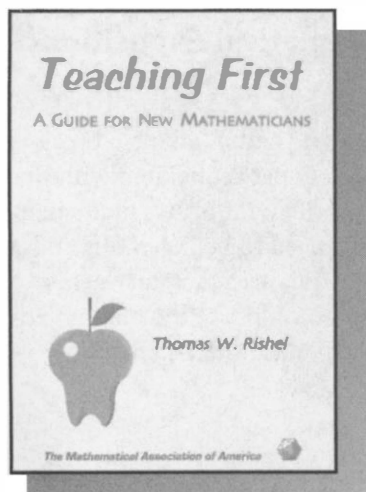


The Mathematical Association of America

Teaching First: A Guide for New Mathematicians

Thomas W. Rishel

Series: MAA Notes



In this volume Thomas Rishel draws on his nearly forty years of teaching experience to address the “nuts and bolts” issues of teaching college mathematics. This book is written for the mathematics TA or young faculty member who may be wondering just where and how to start. Rishel opens the readers’ eyes to pitfalls they may never have considered, and offers advice for balancing an obligation “to the student” with an obligation “to mathematics.”

Throughout, he provides answers to seemingly daunting questions shared by most new TAs, such as how to keep a classroom active and lively; how to prepare writing assignments, tests, and quizzes; how exactly to write a letter of recommendation; and how to pace, minute by minute, the “mathematical talks” one will be called upon to give.

This book is Rishel’s answer to those who may suggest that good teaching is innate and cannot be taught. This he emphatically denies, and he insists that solid teaching starts with often overlooked “seeming trivialities” that one needs to master before exploring theories of learning. Along the way he also covers the general issues that teachers of all subjects eventually experience: fairness in grading, professionalism among students and colleagues, identifying and understanding student “types”, technology in the classroom. All of the subjects in this book are considered within the context of Rishel’s experience as a mathematics teacher. All are illustrated with anecdotes and suggestions specific to the teaching of mathematics.

Teaching First is a comprehensive guide for a mathematics TA, from the first semester preparations through the unforeseen challenges of accepting a faculty position. Its aim is to prepare the new TA with clear suggestions for rapidly improving their teaching abilities.

Catalog Code: NTE-54/JR 150 pp., Paperbound, 2000 ISBN 088385-165-2 List: \$19.00 MAA Member: \$15.00

Name _____	Credit Card No. _____
Address _____	Signature _____ Exp. Date ____/____/____
City _____	Qty _____ Price \$ _____ Amount \$ _____
State _____ Zip _____	Shipping and Handling \$ _____
Phone _____	Catalog Code: NTE-54/JR Total \$ _____

Shipping and Handling: USA orders (shipped via UPS): \$3.00 for the first book, and \$1.00 for each additional book. Canadian orders: \$4.50 for the first book and \$1.50 for each additional book. Canadian orders will be shipped within 2-3 weeks of receipt of order via the fastest available route. We do not ship via UPS into Canada unless the customer specially requests this service. Canadian customers who request UPS shipment will be billed an additional 7% of their total order. Overseas Orders: \$4.50 per item ordered for books sent surface mail. Airmail service is available at a rate of \$10.00 per book. Foreign orders must be paid in US dollars through a US bank or through a New York clearinghouse. Credit card orders are accepted for all customers. All orders must be prepaid with the exception of books purchased for resale by bookstores and wholesalers.

Phone: 1 (800) 331.1622

Fax: (301) 206.9789

Mail: Mathematical Association of America

PO Box 91112

Washington, DC 20090-1112

Web: www.maa.org

Order Via:

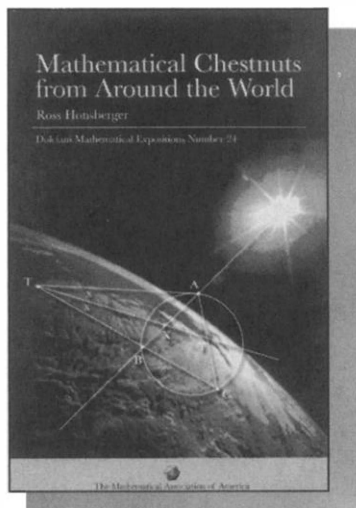


The Mathematical Association of America

Mathematical Chestnuts from Around the World

Ross Honsberger

Series: Dolciani Mathematical Expositions



From time to time great pleasure is to be had in taking a break from our own mathematical activities to get acquainted with the engaging work of others; and how gratifying it is that mathematics doesn't have to be difficult or advanced to be ingenious and beautiful. In this miscellaneous collection of elementary gems you will encounter brilliant insights from many fine mathematical minds. It is remarkable how much exciting mathematics exists at the elementary level.

These essays are presented solely for your pleasure. No attempt is made to give formal instruction; in the few places where preliminaries are presented, it is done so only in preparation for a gem to follow. While a certain degree of concentration is required for the appreciation of some of these delights, this book aims to provide the reader with relaxing enjoyment; it's meant to be mathematical entertainment, not a collection of exacting studies.

The more than 150 problems in this volume come mainly from Euclidean geometry, combinatorics and combinatorial geometry, algebra and number theory, and most of the dissuasions can be followed comfortably by a college freshman.

The problems are not grouped according to subject or arranged in a particular order. Squeeze this book anywhere and an intriguing problem, a striking result, or an ingenious solution is sure to pop out.

Catalog Code: DOL-24/JR 320 pp., Paperbound, 2001 ISBN 088385-330-2 List: \$32.95 MAA Member: \$25.95

Name _____	Credit Card No. _____
Address _____	Signature _____ Exp. Date ____/____/____
City _____	Qty _____ Price \$ _____ Amount \$ _____
State _____ Zip _____	Shipping and Handling \$ _____
Phone _____	Catalog Code: DOL-24/JR Total \$ _____

Shipping and Handling: USA orders (shipped via UPS): \$3.00 for the first book, and \$1.00 for each additional book. Canadian orders: \$4.50 for the first book, and \$1.50 for each additional book. Canadian orders will be shipped within 2-3 weeks of receipt of order via the fastest available route. We do not ship via UPS into Canada unless the customer specially requests this service. Canadian customers who request UPS shipment will be billed an additional 7% of their total order. Overseas Orders: \$4.50 per item ordered for books sent surface mail. Airmail service is available at a rate of \$10.00 per book. Foreign orders must be paid in US dollars through a US bank or through a New York clearinghouse. Credit card orders are accepted for all customers. All orders must be prepaid with the exception of books purchased for resale by bookstores and wholesalers.

Phone: 1 (800) 331.1622

Fax: (301) 206.9789

Mail: Mathematical Association of America

PO Box 91112

Washington, DC 20090-1112

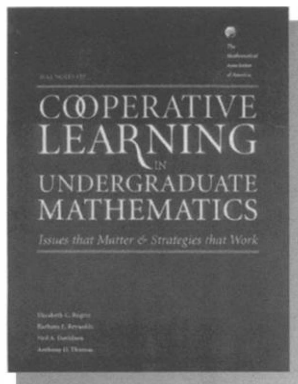
Web: www.maa.org

Order Via:



The Mathematical Association of America

Cooperative Learning in Undergraduate Mathematics: Issues that Matter and Strategies that Work



Elizabeth C. Rogers, Barbara E. Reynolds,
Neil A. Davidson, and Anthony D. Thomas, Editors

Series: MAA Notes

This volume offers practical suggestions and strategies both for instructors who are already using cooperative learning in their classes, and for those who are thinking about implementing it. The authors are widely experienced with bringing cooperative learning into the undergraduate mathematics classroom. In addition they draw on the experiences of colleagues who responded to a survey about cooperative learning which was conducted in 1996-97 for Project CLUME (Cooperative Learning in Undergraduate Mathematics Education).

The volume discusses many of the practical implementation issues involved in creating a cooperative learning environment:

- how to develop a positive social climate, form groups and prevent or resolve difficulties within and among the groups.
- what are some of the cooperative strategies (with specific examples for a variety of courses) that can be used in courses ranging from lower-division, to calculus, to upper division mathematics courses.
- what are some of the critical and sensitive issues of assessing individual learning in the context of a cooperative learning environment.
- how do theories about the nature of mathematics content relate to the views of the instructor in helping students learn that content.

The authors present powerful applications of learning theory that illustrate how readers might construct cooperative learning activities to harmonize with their own beliefs about the nature of mathematics and how mathematics is learned.

In writing this volume the authors analyzed and compared the distinctive approaches they were using at their various institutions. Fundamental differences in their approaches to cooperative learning emerged. For example, choosing Davidson's guided-discovery model over a constructivist model based on Dubinsky's action-process-object-schema (APOS) theory affects one's choice of activities. These and related distinctions are explored.

A selected bibliography provides a number of the major references available in the field of cooperative learning in mathematics education. To make this bibliography easier to use, it has been arranged in two sections. The first section includes references cited in the text and some sources for further reading. The second section lists a selection (far from complete) of textbooks and course materials that work well in a cooperative classroom for undergraduate mathematics students.

Catalog Code: NTE-55/JR 250 pp., Paperbound, 2001 ISBN 088385-166-0 List: \$ 31.95 MAA Member: \$25.95

Name _____	Credit Card No. _____
Address _____	Signature _____ Exp. Date ____/____
City _____	Qty _____ Price \$ _____ Amount \$ _____
State _____ Zip _____	Shipping and Handling \$ _____
Phone _____	Catalog Code: NTE-55/JR Total \$ _____

Shipping and Handling: USA orders (shipped via UPS): \$3.00 for the first book, and \$1.00 for each additional book. Canadian orders: \$4.50 for the first book and \$1.50 for each additional book. Canadian orders will be shipped within 2-3 weeks of receipt of order via the fastest available route. We do not ship via UPS into Canada unless the customer specially requests this service. Canadian customers who request UPS shipment will be billed an additional 7% of their total order. Overseas Orders: \$4.50 per item ordered for books sent surface mail. Airmail service is available at a rate of \$10.00 per book. Foreign orders must be paid in US dollars through a US bank or through a New York clearinghouse. Credit card orders are accepted for all customers. All orders must be prepaid with the exception of books purchased for resale by bookstores and wholesalers.

Phone: 1 (800) 331.1622

Fax: (301) 206.9789

Mail: Mathematical Association of America

PO Box 91112

Washington, DC 20090-1112

Web: www.maa.org

Order Via:

CONTENTS

ARTICLES

- 3 Znam's Problem, *by Lawrence Brenton and Ana Vasiliu*
- 12 The Josephus Problem: Once More Around,
by Peter Schumer
- 18 A Brief History of Factoring and Primality Testing B. C.
(Before Computers), *by Richard A. Mollin*
- 29 Poem: Doing Math, *by Donna Davis*

NOTES

- 30 The Perfect Shape for a Rotating Rigid Body,
by Frank Morgan
- 32 One Sequence, Many Interesting Ideas in Analysis,
by Sudhir Goel, Russell A. Gordon, and Charles Kicey
- 39 Proof Without Words: The Pigeonhole Principle,
by Ran Libeskind-Hadas
- 40 Proof Without Words: A Sum and Product of Three Tangents,
by Roger B. Nelsen
- 41 When Does a Sum of Positive Integers Equal Their Product?,
by Michael W. Ecker
- 47 The Scarcity of Regular Polygons on the Integer Lattice,
by Daniel J. O'Loughlin
- 51 Medical Tests and Convergence, *by Stephen Friedberg*
- 53 Uniquely Determined Unknowns in Systems of Linear
Equations, *by Kenneth Hardy, Blair K. Spearman,
and Kenneth S. Williams*
- 57 Counterintuitive Aspects of Plane Curvature,
by Russell A. Gordon and Colin Ferguson

PROBLEMS

- 63 Proposals 1638–1642
- 64 Quickies 917–918
- 64 Solutions 1613–1617
- 69 Answers 917–918

REVIEWS

70

NEWS AND LETTERS

- 72 62nd Annual William Lowell Putnam Mathematical
Competition

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, NW
Washington, DC 20036

