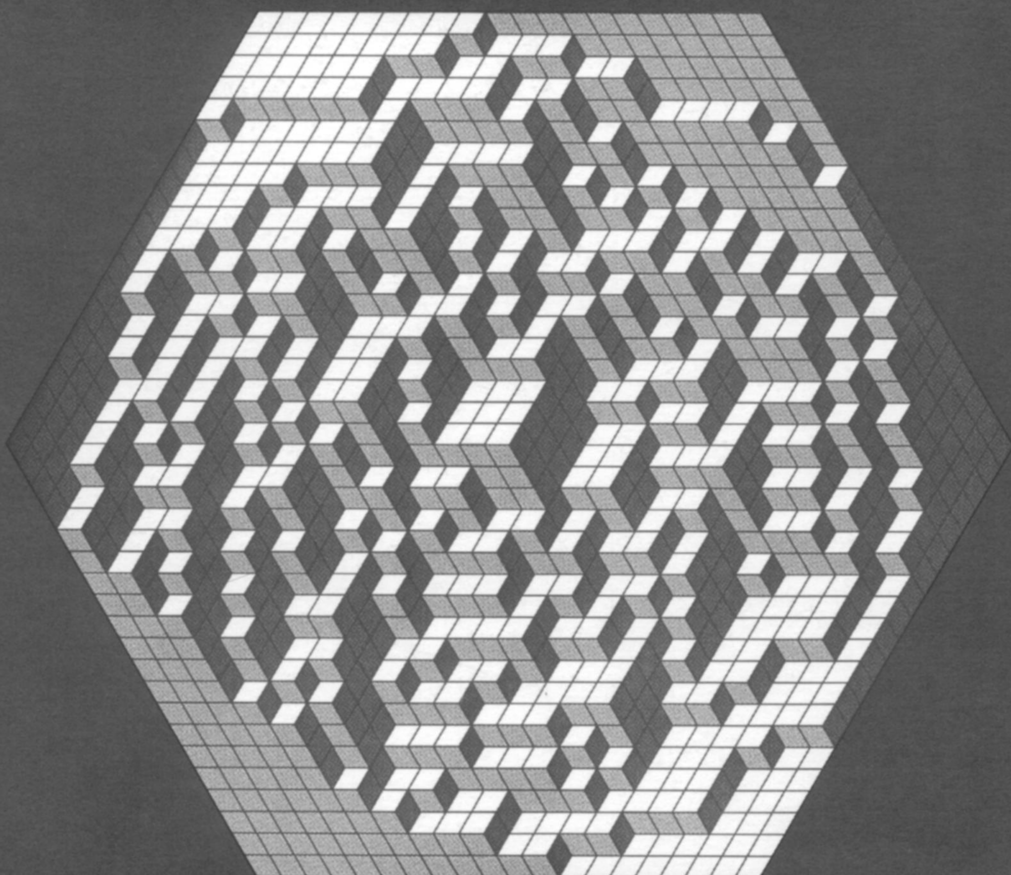
Vol. 71, No. 2 April 1998

MATHEMATICS MAGAZINE



- Beholding A Rotating Beacon
- Abstract Algebra: A Historical Focus
- Defining Chaos

An Official Publication of The MATHEMATICAL ASSOCIATION OF AMERICA

EDITORIAL POLICY

Mathematics Magazine aims to provide lively and appealing mathematical exposition. This is not a research journal and, in general, the terse style appropriate for such a journal (lemma-theorem-proof-corollary) is not appropriate for an article for the *Magazine*. Articles should include examples, applications, historical background, and illustrations, where appropriate. They should be attractive and accessible to undergraduates and would, ideally, be helpful in supplementing undergraduate courses or in stimulating student investigations. Manuscripts on history are especially welcome, as are those showing relationships between various branches of mathematics and between mathematics and other disciplines.

A more detailed statement of author guidelines appears in this *Magazine*, Vol. 71, pp. 76–78, and is available from the Editor. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, or published by another journal or publisher.

Send new manuscripts to Paul Zorn, Editor, Department of Mathematics, St. Olaf College, 1520 St. Olaf Avenue, Northfield, MN 55057-1098. Manuscripts should be laser-printed, with wide line-spacing, and prepared in a style consistent with the format of *Mathematics Magazine*. Authors should submit three copies and keep one copy. In addition, authors should supply the full five-symbol Mathematics Subject Classification number, as described in *Mathematical Reviews*, 1980 and later. Copies of figures should be supplied on separate sheets, both with and without lettering added.

Cover Illustration: The figure shows a random tiling of a regular hexagon of side length $n = 20$ by rhombuses of side length 1. The algorithm that gave rise to it, called coupling from the past, samples from the uniform distribution on the set of all tilings. In a random tiling, the tiles in the six corners tend to line up with each other, while the tiles in the middle tend to have interspersed orientations. The boundary between the two regimes becomes increasingly circular as n gets large. Produced by the MIT Tilings Research Group, under the supervision of Jim Propp; for more information (and pictures), see `http://web.mit.edu/tiling/www` and `http://www-math.mit.edu/~propp/trg.html`.

AUTHORS

Irl C. Bivens, a professor of mathematics at Davidson College, received his A.B. degree from Pfeiffer College and his Ph.D. from the University of North Carolina–Chapel Hill. Before coming to Davidson in 1982 he taught at Pfeiffer College and was a G.C. Evans Instructor of Mathematics at Rice University. He has long been interested in applications of mathematics to physics and to the exploring of connections between geometry and analysis. These interests have been enjoyably shared over the last couple of years with his coauthor, Andrew Simoson.

Israel Kleiner is professor in the Department of Mathematics and Statistics at York University in Toronto. He received his Ph.D. in ring theory from McGill University. His current research interests are in the history of mathematics, in mathematics education, and in their interface. He was for many years coordinator of an in-service master's program for teachers of mathematics. Recently he served as vice-president of the Canadian Society for History and Philosophy of Mathematics, and is currently on the advisory board of the International Study Group for the Relations between the History and Pedagogy of Mathematics.

Mario Martelli did his graduate work at the University of Florence, Italy where his thesis advisor was Roberto Conti. He was promoted to full professor at the University of Florence in 1976, and came to the USA for family reasons in 1978. He taught at Bryn Mawr College in Pennsylvania and, since 1987, at Cal State-Fullerton. His research interests include differential equations, bifurcation theory, and dynamical systems. **Tanya Seph** and **Mai Dang** did their undergraduate work at Cal State-Fullerton, and are now doing graduate work at UC Davis and the University of Arizona, Tucson, respectively. This paper started as a class project of Tanya and Mai while they were students of Martelli in a course on dynamical systems.

Andrew Simoson received his Ph.D. in functional analysis under Len Asimow at the University of Wyoming in 1979. Since that time he has been chairman of the mathematics department at King College, in eastern Tennessee, with two Fulbright professorship excursions to Africa, one to Botswana ('90–'91) and now in Tanzania ('97–'98). Most of the results in his paper with Irl Bivens were the outcome of a two year e-mail conversation about the rotating beacon problem.

Vol. 71, No. 2, April 1998

MATHEMATICS MAGAZINE

The *MATHEMATICS MAGAZINE* (ISSN 0025-570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, D.C. 20036 and Montpelier, VT, bimonthly except July/August.

The annual subscription price for the MATHEMATICS MAGAZINE to an individual member of the Association is $16 included as part of the annual dues. (Annual dues for regular members, exclusive of annual subscription prices for MAA journals, are $64. Student and unemployed members receive a 66% dues discount; emeritus members receive a 50% discount; and new members receive a 40% dues discount for the first two years of membership.) The nonmember/library subscription price is $68 per year.

Subscription correspondence and notice of change of address should be sent to the Membership/Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036. Microfilmed issues may be obtained from University Microfilms International, Serials Bid Coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

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

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

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

PRINTED IN THE UNITED STATES OF AMERICA

ARTICLES

Beholding a Rotating Beacon

IRL BIVENS
Davidson College
Davidson, NC 28036-1719

ANDREW SIMOSON
King College
Bristol, TN 37620

1. Introduction

Imagine a powerful beacon positioned on an island, its beam illuminating the (convex) shoreline of a lake as it rotates counterclockwise with constant angular velocity ω. Is there any place on the lake where an observer could sit in a rowboat so that the illuminated spot on the beach always appears to move about the shoreline in a counterclockwise direction? The reader might be inclined to think that nothing to the contrary could occur, that any place on the lake would be equally satisfactory. However, if ω is large enough, and if we take into account the finite speed of light, then some unexpected behavior results.

One purpose of this paper is to characterize the set of "ordinary" vantage points, from which the beacon's light show is always counterclockwise. We prove that at moderate rotation rates the set of ordinary points is a proper, open, convex subset of the region bounded by the shoreline. Furthermore, in all cases save one, the set of ordinary points will be empty at high rotation rates. The single exception is the case of an elliptical shoreline with the beacon at one focus. In this case the set of ordinary points always contains the second focus of the ellipse. As the rotation rate of the beacon increases, the set of ordinary points shrinks to the second focus at a rate which (to first order) is inversely proportional to the rotation rate of the beacon.

An investigation into the structure of the set of ordinary points leads us into mathematics that is interesting in its own right. For example, in order to study the "shape" of the set of ordinary points we construct an explicit parametrization for the envelope of a family of lines that make specified angles with some fixed curve. This parametrization should be of general interest apart from its specific application in our paper. (In a number of cases it is much easier to use our parametrization than to carry out the classical envelope procedure.) Another result of some general interest is our "elliptical" generalization of unit normalization: given an ellipse, pick a focus and scale each point on the ellipse "away" from that focus by the reciprocal of its distance to the second focus. In the case of a circle the result is of course simply a concentric unit circle. More generally, in the case of an ellipse the result is always a second ellipse whose congruence class depends only upon the *similarity* class of the original ellipse.

Our most surprising result (Theorem 6) has to do with the *shape* of the ordinary set at high rotation rates in the case of an elliptical shoreline with the beacon at one focus. We prove that this shape is described by a (classical) curve known as an *antiorthotomic of* an ellipse. (See FIGURE 14 for an example of an antiorthotomic.) However, the ellipse in question is not our shoreline, but its "elliptical" normalization. The manner in which the kinematics of the rotating beacon and these other seemingly unrelated elements come together is, to us, most pleasing.

But first, let's review the problem as stated in the related rates section of the typical calculus text: "A beacon rotating counterclockwise at ω radians per second is one mile from shore. How quickly does the illuminated spot on the shoreline move along the beach?" Assume the beacon is located at a point Q. Since the assumption in this problem is that the beach is a straight line, let x be a coordinate along the beach such that the point R on the beach closest to the beacon corresponds to $x = 0$. (See FIGURE 1.) Let θ denote the angle between the direction of the beacon and ray QR at time t. The (usually unstated) assumption that the speed of light is infinite implies that at any given time there will be a (unique) spot of light on the beach if and only if the beacon is pointing towards the shoreline at that moment. In this case, $x = \tan\theta$ and by the chain rule

$$\frac{dx}{dt} = \frac{dx}{d\theta}\frac{d\theta}{dt} = \omega\sec^2\theta = \omega(1 + x^2). \tag{1}$$

Note that according to this solution the position x of the spot is a strictly increasing function of t and its velocity $\frac{dx}{dt}$ becomes infinite as $|x|$ approaches infinity. Likewise, the velocity of the spot becomes infinite as ω approaches infinity.

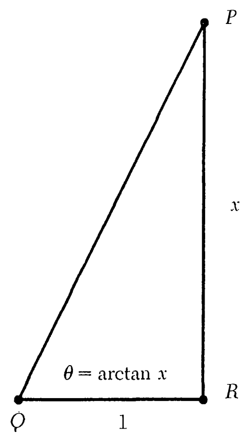


FIGURE 1
The beacon, Q, and illuminated spot P.

One problem with this solution is that it ignores the fact the speed of light c is actually finite. Of course, for all practical terrestrial problems this objection is rather academic. Nonetheless, we can still ask for the correct model under the assumption of finite light speed. To compute the velocity of the spot under this assumption, we must differentiate position x with respect to the time t at which the light from the beacon actually arrives at x. It follows from the analysis in **[1]** that, in this case,

$$\frac{dx}{dt} = \frac{c\omega(1 + x^2)}{c + \omega x\sqrt{1 + x^2}}. \tag{2}$$

A little algebra reveals that the denominator of (2) vanishes at $x_0 = -\sqrt{\frac{\sqrt{\omega^2 + 4c^2} - \omega}{2\omega}}$, so the velocity of the spot is undefined at x_0. (For example, if the beacon is rotating at one revolution per minute, then $x_0 \approx -1333$ miles.) Geometrically, x_0 is the point at which the spiral wavefront of light from the beacon initially "splashes" onto the beach. (See FIGURE 2.) The velocity of the spot is negative for $x < x_0$ and is positive for $x > x_0$. Thus, contrary to the infinite light speed solution, the spot on the shoreline is actually moving in the *negative* x direction for $x < x_0$. (A similar phenomenon sometimes appears in old war movies: a machine gunner swings his machine gun in an arc from a position parallel to a building toward the building while firing the gun; however, the bullet holes strike the wall in the reverse direction, with the track of bullet holes traveling away from the gun. A safer demonstration of this phenomenon can be performed with a rotating lawn sprinkler.)

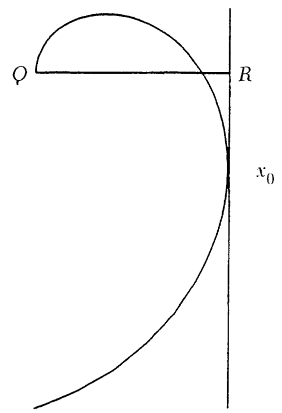


FIGURE 2
A wave rolls onto the beach.

If we allow c to approach infinity in equation (2) then we recover the infinite light speed solution of equation (1). Furthermore, note that as $|x|$ approaches infinity the speed of the spot does not become infinite but instead approaches c. On the other hand, near the point x_0 the speed of the spot *does* become arbitrarily large. (See **[3]** for further discussions of such phenomena.) As ω approaches infinity the initial contact point x_0 approaches 0 and the velocity of the spot at $x \neq 0$ approaches $\frac{c\sqrt{1+x^2}}{x}$. Although this limiting velocity has magnitude greater than c, it is still finite. If we assume the beacon has been rotating for all time, then at any given moment there will be infinitely many spots moving along the shoreline in both directions. Note that these conclusions are in dramatic opposition to those of the infinite light speed model.

As is suggested in **[1]**, let us now imagine that the "beach" is actually a smooth convex closed curve. In fact, to "reflect" the function of the beach more accurately, we will henceforth refer to it as a "screen." We will choose a coordinate system such that the beacon is at the origin and the screen is described by a polar graph $r = f(\theta) > 0$. To simplify our formulas we will choose our units such that the speed of light c is equal to 1. Assume that at time $t = 0$ the beacon points in the direction $\theta = 0$. The time at which light illuminates the spot at $r = f(\theta)$ is given by $t = t(\theta) = \frac{\theta}{\omega} + f(\theta)$. By the familiar arclength formula, $\frac{ds}{d\theta} = \sqrt{[f(\theta)]^2 + [f'(\theta)]^2}$, where $s = s(\theta)$ is the distance measured counterclockwise along the screen from the point $r = f(0)$ to the point $r = f(\theta)$. (This notation and these assumptions will remain in effect throughout the remainder of this paper.) Then, $\frac{dt}{d\theta} = \frac{1}{\omega} + f'(\theta)$ so that on intervals of θ for which $f'(\theta) \neq -\frac{1}{\omega}$, we can express θ as a smooth function of t

with implicit derivative $\frac{d\theta}{dt} = \frac{\omega}{1+\omega f'(\theta)}$. Using the chain rule, the velocity $v(\theta)$ of the spot on the screen at point $r = f(\theta)$ is given by

$$v(\theta) = \frac{ds}{dt} = \frac{ds}{d\theta}\frac{d\theta}{dt} = \frac{\omega\sqrt{[f(\theta)]^2 + [f'(\theta)]^2}}{1+\omega f'(\theta)}. \tag{3}$$

Since the sign of $v(\theta)$ is equal to that of $\frac{d\theta}{dt}$ we see that the spot is moving counterclockwise around the screen when $v(\theta) > 0$ and is moving clockwise when $v(\theta) < 0$. As in the case of a straight beach, there may be more than one spot on the screen at a time. To better understand this phenomenon, consider first FIGURE 3, where the beacon is rotating at a slow rate. At any time, only one spot on the screen is illuminated, and the "light show" on the screen is always moving counterclockwise. However, FIGURE 4 illustrates that as the rotation rate increases, a qualitative change in

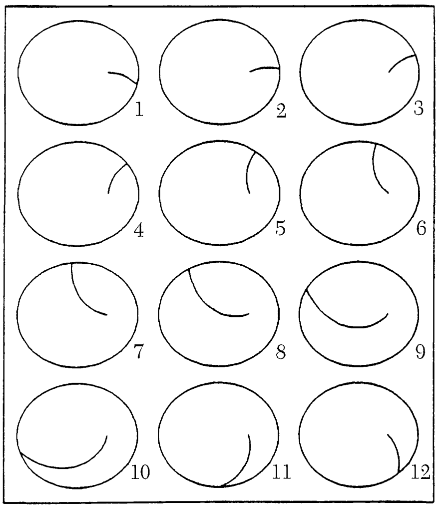


FIGURE 3
Slower rotation.

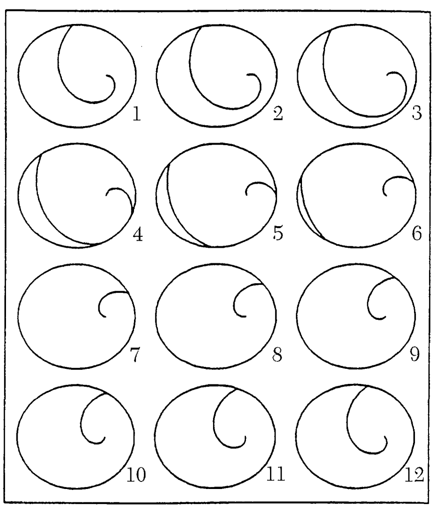


FIGURE 4
Faster rotation.

the behavior of the spot takes place. Up to around $t = 3$ there is a single spot on the screen. Then, at about $t = 3$, a "splash" occurs and three points on the screen are illuminated; two of these move counterclockwise and the other moves clockwise. Shortly after $t = 6$, two of these spots collide (at infinite speed) in a "crash" and disappear at one end of the screen while the third continues moving counterclockwise at the other end.

As the rotation rate is increased, more and more points along the screen will be illuminated concurrently, so that as $\omega \to \infty$ the entire screen becomes ablaze with light continually moving in both directions. Even more complications can arise. For example, if $f'(\theta) = -\frac{1}{\omega}$ on some interval then light from the beacon arrives at all the corresponding points $r = f(\theta)$ *simultaneously*. (Geometrically, this means that a portion of the screen actually coincides with the wavefront of the beacon.) In this case, it becomes difficult even to *define* the "position" of the spot on the screen. Such a light show is in a stark contrast to what one might "naively" expect; namely, a single spot of light moving counterclockwise around the screen. However, with this naive expectation in mind, we define a vantage point within the region bounded by the screen to be *ordinary* for a particular rotation rate, if the view of the screen from that point shows a single spot of light moving with finite speed counterclockwise around the screen. A vantage point that is not ordinary will be called *extraordinary*.

Given the possible complexity of the light show on the screen, the determination of the set of ordinary points might appear to be a difficult problem. However, as we will see in the next section, its solution becomes relatively straightforward if we *ignore* what is actually occurring, and focus instead upon what *appears* to be happening.

2. Ordinary vantage points and separation lines

In assigning space and time coordinates to physical events it is important to distinguish between *observing* an event and *seeing* the event occur. In effect, an "observer" is assumed to be omniscient and omnipresent, knowing at every "instant" what is going on anywhere within the observer's frame of reference. On the other hand, for someone to "see" an event occur, light must travel from the location of the event to the eyes of the person viewing it. Because of this optical backlog, what is actually happening and what appears to be occurring can be quite different. Henceforth, when we use the words "see," "view," and "appears" we will mean "seeing," not "observing."

Our first goal is to separate the ordinary from the extraordinary points. Let $g(\theta) = (f(\theta)\cos\theta, f(\theta)\sin\theta)$ denote a parametrization of the screen in terms of θ and let $\mathbf{T} = \mathbf{T}(\theta) = \frac{g'(\theta)}{\|g'(\theta)\|}$ denote the unit tangent vector field to g. Let $\rho = 1/\omega$ denote the reciprocal of the rotation rate ω and note that the expression $\frac{\rho + f'(\theta)}{\|g'(\theta)\|} = \frac{\rho + f'(\theta)}{\sqrt{[f(\theta)]^2 + [f'(\theta)]^2}}$ is always greater than -1. For all values of θ such that $-1 < \frac{\rho + f'(\theta)}{\|g'(\theta)\|} < 1$, define $\alpha_\rho(\theta) = \arccos\left(\frac{\rho + f'(\theta)}{\|g'(\theta)\|}\right)$. Then, for each value of θ such that $\alpha_\rho(\theta)$ is defined, let $L(\theta)$ denote the line obtained by rotating the tangent line to the screen at $g(\theta)$ counterclockwise through an angle of $\alpha_\rho(\theta)$. We will refer to the lines $L(\theta)$ as *separation lines*.

The next result shows that a separation line does, in fact, separate ordinary points from extraordinary points.

THEOREM 1. *Let Q denote any fixed point within the region bounded by the screen and assume the beacon is rotating at some fixed rotation rate ω.*

(a) *The point Q is ordinary if and only if for each separation line $L(\theta)$, Q lies on the side of $L(\theta)$ opposite the direction of the screen at $g(\theta)$. (That is, Q and the point $g(\theta)+\mathbf{T}(\theta)$ lie on opposite sides of $L(\theta)$.)*

(b) *The point Q is extraordinary if and only if there exists a separation line containing Q.*

Proof. (a) If $Q=(x,y)$, let $h_Q(\theta)=\sqrt{(f(\theta)\cos\theta-x)^2+(f(\theta)\sin\theta-y)^2}$ denote the distance from Q to the point $g(\theta)$ on the screen. Light will leave the beacon heading towards $g(\theta)$ at time $\theta/\omega=\theta\rho$, will reflect from point $g(\theta)$ at time $\theta\rho+f(\theta)$, and will arrive at point Q at time $t=t_Q(\theta)=\rho\theta+f(\theta)+h_Q(\theta)$. If Q is an ordinary vantage point then $t_Q(\theta)$ must be a strictly increasing function of θ. Therefore, $t'_Q(\theta)\geq 0$. Because the spot appears to have finite speed at all times, $\frac{ds}{dt}$ is always defined and finite. It follows from the chain rule that

$$\frac{ds}{dt}t'_Q(\theta)=\frac{ds}{dt}\frac{dt}{d\theta}=\frac{ds}{d\theta}=\sqrt{[f(\theta)]^2+[f'(\theta)]^2}=\|g'(\theta)\|\neq 0,$$

since the screen is assumed to be a regular curve. Consequently, if Q is ordinary then $t'_Q(\theta)>0$ for all values of θ. Since this reasoning can be reversed when $t'_Q(\theta)>0$, it follows that Q is ordinary if and only if

$$t'_Q(\theta)=\rho+f'(\theta)+h'_Q(\theta)>0. \tag{4}$$

Let $\phi_Q(\theta)$ denote the angle between $\mathbf{T}(\theta)$ and the displacement vector from $g(\theta)$ to Q. A little vector calculus shows that $h'_Q(\theta)=-\|g'(\theta)\|\cos\phi_Q(\theta)$ and inequality (4) then becomes

$$t'_Q(\theta)=\rho+f'(\theta)+h'_Q(\theta)=\rho+f'(\theta)-\|g'(\theta)\|\cos\phi_Q(\theta)>0.$$

Equivalently, Q is ordinary if and only if, for all θ,

$$\cos\phi_Q(\theta)<\frac{\rho+f'(\theta)}{\|g'(\theta)\|}. \tag{5}$$

This inequality is automatically satisfied if $\frac{\rho+f'(\theta)}{\|g'(\theta)\|}\geq 1$, since Q lies in the region bounded by the screen. If $-1<\frac{\rho+f'(\theta)}{\|g'(\theta)\|}<1$ then this inequality is satisfied if and only if $\alpha_\rho(\theta)<\phi_Q(\theta)$, since the cosine is a decreasing function on the range of the arccosine. Geometrically this means that Q is ordinary if and only if for each separation line $L(\theta)$, Q lies on the side of $L(\theta)$ opposite the direction of the screen at $g(\theta)$.

(b) It follows from inequality (4) that Q is extraordinary if and only if $t'_Q(\theta)\leq 0$ for some value of θ. Since $t_Q(\theta)>\rho\theta$, $t'_Q(\theta)$ cannot be negative for all values of θ. Because $t'_Q(\theta)$ is a continuous function of θ, Q is thus extraordinary if and only if the equation $t'_Q(\theta)=\rho+f'(\theta)-\|g'(\theta)\|\cos\phi_Q(\theta)=0$ has a solution θ. This equation may be written in the form $\cos\phi_Q(\theta)=\frac{\rho+f'(\theta)}{\|g'(\theta)\|}$. Since $-1<\cos\phi_Q(\theta)<1$, this equation has a solution if and only if $\alpha_\rho(\theta)=\phi_Q(\theta)$ for some value of θ. Geometrically, this means that Q is extraordinary if and only if Q lies on some separation line $L(\theta)$.

It follows from equation (3) that when the spot has a well-defined position and speed on the screen, the velocity of the spot is given by $v(\theta) = \frac{\|g'(\theta)\|}{\rho + f'(\theta)}$. If $v(\theta) > 0$ then a point Q is ordinary if and only if $v(\theta)\cos\phi_Q(\theta) < 1$. The reader can show that this condition is a consequence of the Doppler shift phenomenon.

Theorem 1 can be used in a couple of ways to display the set of ordinary points. For example, we can sample points in the region bounded by the screen and plot those for which inequality (4) is violated. The unshaded portion of the region will then approximate the set of ordinary points. FIGURE 5 depicts these approximations, at various rotation rates, for the ellipse $r = \frac{1}{2 + \cos\theta}$. A more efficient method is to plot a representative sample of separation lines. The set of points within the region belonging to no separation line is then the ordinary set. FIGURE 6 illustrates this procedure for the ellipse and rotation rates of FIGURE 5.

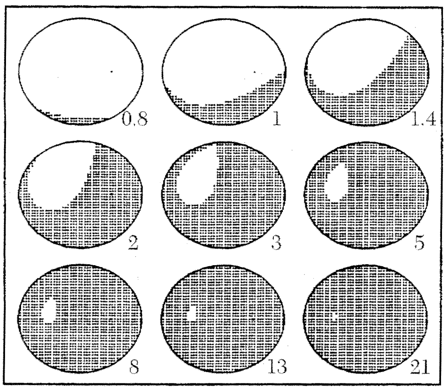


FIGURE 5
The vanishing ellipse.

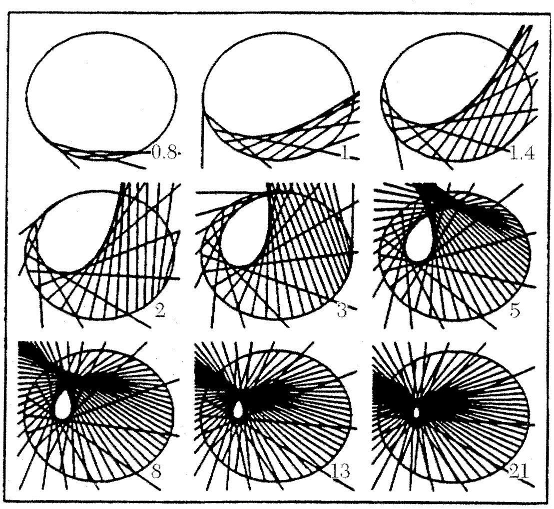


FIGURE 6
The vanishing ellipse (separation lines version).

An immediate consequence of Theorem 1 gives us some information about the structure of the ordinary set.

COROLLARY 2. *For every rotation rate the set of ordinary points is an open, convex subset of the region bounded by the screen.*

Proof. It follows from Theorem 1 (a) that the ordinary set may be obtained as the intersection of the convex region bounded by the screen with open half-planes bounded by separation lines. Since the intersection of convex sets is convex, the set of ordinary points must be convex.

Define the function $\beta = \beta(\theta)$ to be $\alpha_p(\theta)$ when $\alpha_p(\theta)$ is defined and to be 0 otherwise. It is easy to see that β is a continuous function on $[0, 2\pi]$. Let $M(\theta)$ denote the line obtained by rotating the tangent to the screen at $g(\theta)$ by angle $\beta(\theta)$ counterclockwise. As θ varies from 0 to 2π the set of points on $M(\theta)$ whose distance to $g(\theta)$ is no more than the diameter of the screen sweeps out a compact (and thus closed) subset of the plane that contains all extraordinary points and no ordinary points. The intersection of the (open) complement of this set with the region bounded by the screen is the set of ordinary points. Therefore, the set of ordinary points is open.

Using inequality (4) it is easily shown that a decrease in the rotation rate of the beacon can never result in an ordinary point becoming extraordinary, nor can an increase in the rotation rate cause an extraordinary point to become ordinary. Furthermore, FIGURES 5 and 6 suggest that at low rotation rates most vantage points will be ordinary, while at high rotation rates the view becomes extraordinary. The next result gives further details on the relationship between rotation rates and the ordinary set.

PROPOSITION 3. (*a*) *The only screens that have vantage points that are ordinary for every rotation rate are ellipses, with the beacon positioned at one focus. For such a configuration, the only always-ordinary vantage point is the other focus. In every other case, for every vantage point Q, there is a critical rotation rate ω_Q such that Q is ordinary for rotation rates less than ω_Q, and extraordinary otherwise.*

(*b*) *For every screen and for every position of the beacon, there exists a rotation rate ω_0 such that the set of ordinary points is the entire region bounded by the screen precisely for those rotation rates no greater than ω_0.*

(*c*) *For every nonelliptical screen or for every elliptical screen for which the beacon is not located at a focus, there exists a rotation rate ω_1 such that the set of ordinary points is the empty set precisely for those rotation rates no less than ω_1.*

Proof. We assume the notation used in the proof of Theorem 1.

(a) Let Q denote some fixed point within the region bounded by a particular screen. We first argue that if the function $H(\theta) = f(\theta) + h_Q(\theta)$ is *not* identically constant then there exists a rotation rate ω_Q such that Q is ordinary for rotation rates less than ω_Q, and extraordinary otherwise. If H is not constant then its periodicity implies that the minimum value of $H'(\theta)$ is some *negative* number m. Define $\omega_Q = 1/|m|$. Then $t'_Q(\theta) = \rho + H'(\theta) = 1/\omega + H'(\theta)$ is positive precisely for rotation rates $\omega < \omega_Q$. In other words, it follows from condition (4) that Q is ordinary if $\omega < \omega_Q$ and extraordinary otherwise. On the other hand, the function H *is* identically constant if and only if the screen is an ellipse with foci the beacon and Q. Furthermore, in this case $t'_Q(\theta) = \rho$ is a positive constant and we see that the focus Q is ordinary for every rotation rate.

(b) The set of ordinary points is equal to the region bounded by the screen if and only if there are no separation lines. This occurs if and only if $\frac{\rho+f'(\theta)}{\|g'(\theta)\|} \geq 1$ for all θ. Equivalently, $\rho \geq \|g'(\theta)\| - f'(\theta)$ for all θ. But this inequality is satisfied if and only if ρ is equal to or greater than the maximum value of $\|g'(\theta)\| - f'(\theta)$, for θ in $[0, 2\pi]$. Equivalently, the rotation rate of the beacon must be less than or equal to the reciprocal ω_0 of this maximum value in order for every point to be ordinary.

(c) Assume that the screen is either not an ellipse or is an ellips for which the beacon is not located at a focus. First we argue that there exists a rotation rate for which the set of ordinary points is empty. By choosing ω large enough, we can ensure that a separation line is defined for each value of θ. Then, for each separation line $L(\theta)$, we let $H(\theta)$ denote the closed half-space of points either on $L(\theta)$ or on the opposite side of $L(\theta)$ from the direction of the screen at $g(\theta)$. The intersection of the compact set bounded by the screen and all closed half-spaces $H(\theta)$ is then a compact subset F that contains the set of ordinary points corresponding to rotation rate ω. If F is empty then no points are ordinary for rotation rate ω and we are done. Suppose then that F is not empty. Since the screen is a smooth curve, it is straightforward to show that F is contained in the interior of the region bounded by the screen. For any point Q in F, if the beacon has rotation rate ω_Q then Q is extraordinary and must lie on some separation line $L(\theta)$. Equivalently, for some value of θ, $\alpha_\rho(\theta) = \phi_Q(\theta)$. It follows that if we increase the rotation rate to $\omega_Q + 1$ then Q will belong to the open half-space U_Q of points on the same side of $L(\theta)$ as the direction of the screen at $g(\theta)$. If Q is allowed to vary over all points in F, the collection of open sets $\{U_Q\}$ will cover F. Since F is compact, some finite subcollection $\{U_{Q_1}, U_{Q_2}, \ldots, U_{Q_n}\}$ of these open sets will also cover F. The maximum of $\{\omega, \omega_{Q_1} + 1, \omega_{Q_2} + 1, \ldots, \omega_{Q_n} + 1\}$ will then be a rotation rate for which the set of ordinary points is empty.

For any Q in the region bounded by the screen, ω_Q will be a lower bound for the collection of rotation rates with empty set of ordinary points. Let ω_1 denote the greatest lower bound for this set. Then for all points Q, $\omega_Q \leq \omega_1$, so that for any rotation rate equal to or greater than ω_1, the set of ordinary points is empty. On the other hand, by definition of the greatest lower bound, the set of ordinary points must be nonempty for any rotation rate less than ω_1.

Example 1. Consider the case of a circular screen of radius 1 with the beacon at the center. Then it follows from Corollary 2 and Proposition 3 (a) that for any rotation rate the set of ordinary points will be a nonempty open convex set containing the beacon. Symmetry then implies the ordinary set will be an open disk concentric with the screen. Since $r = f(\theta) = 1$, $f'(\theta) = 0$ and $\|g'(\theta)\| = 1$, it follows from the proof of Proposition 3 (b) that $\omega_0 = 1$. Therefore, if $\omega \leq 1$ the ordinary set is then the entire unit disk. If $\omega > 1$ then simple geometry (see FIGURE 7) shows that the distance of each separation line to the beacon is $\rho = 1/\omega$. Consequently, in this case the ordinary set is an open disk of radius ρ centered at the beacon.

FIGURE 8 illustrates Proposition 3 (c) in the case of a convex limaçon $r = 2 + \cos(\theta)$.

3. Enveloping the set of ordinary points

We have seen that the set of ordinary points is always an open convex subset of the region bounded by the screen. In order to describe the shape of this set more

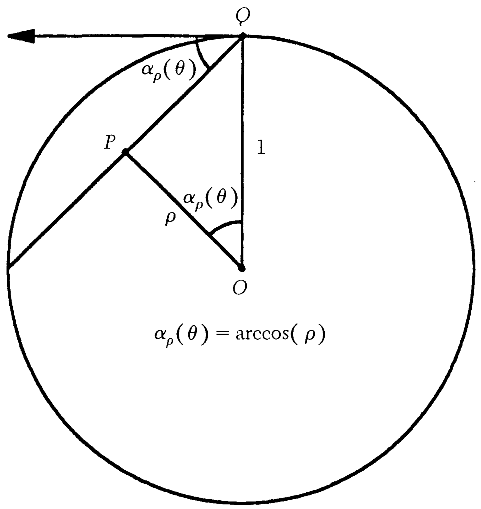


FIGURE 7
A circular screen.

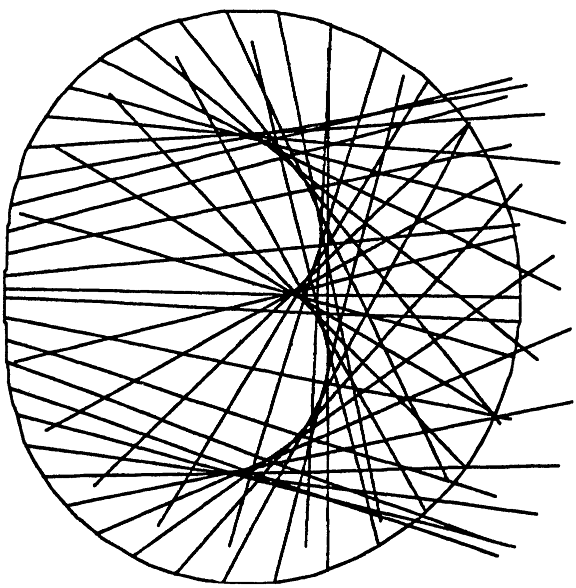


FIGURE 8
An empty set of normal points.

precisely, we need to determine the boundary of the ordinary region. In general the boundary of a convex region in the plane will be a continuous curve that is differentiable almost everywhere. Any point S within the region bounded by the screen that is on the boundary of the set of ordinary points must be extraordinary and thus must lie on some separation line L. Since points on the "extraordinary" side of L will be isolated from the ordinary set, if the boundary of the ordinary set has a tangent line at S, then this tangent line must be L. Consequently, within the region bounded by the screen the boundary of the ordinary set will be almost everywhere tangent to the collection of separation lines. This *suggests* that the boundary of the ordinary set will either be on the screen itself or will be part of the envelope of the family of separation lines. While FIGURE 6 seems to lend credence to this conclusion, a careful proof turns out to be rather delicate.

We will sketch a proof of this result after first constructing an explicit parametrization of an envelope for a one-parameter family of lines $\mathscr{F}$ whose angles with some specified curve g are known. Let $g = g(s)$ denote a unit-speed curve with Frenet frame $\mathbf{T} = \mathbf{T}(s)$ and $\mathbf{N} = \mathbf{N}(s)$, where $\mathbf{N}$ is obtained from $\mathbf{T}$ by a counterclockwise rotation of 90 degrees. Assume that through each point $g(s)$ there is a line $M(s)$ parallel to $\mathbf{W}_1(s) = \cos\alpha(s)\mathbf{T}(s) + \sin\alpha(s)\mathbf{N}(s)$, where $\alpha = \alpha(s)$ is a smooth function of s. Let $\mathscr{F} = \{M(s)\}$ denote the resulting one-parameter family of lines. Let $\mathbf{W}_2 = -\sin\alpha\mathbf{T} + \cos\alpha\mathbf{N}$ denote the rotation of $\mathbf{W}_1$ 90 degrees counterclockwise and observe that $\mathbf{W}_1' = (\kappa + \alpha')\mathbf{W}_2$ and $\mathbf{W}_2' = -(\kappa + \alpha')\mathbf{W}_1$, where $\kappa = \kappa(s)$ is the curvature of g. Also note that $\mathbf{T} = \cos\alpha\mathbf{W}_1 - \sin\alpha\mathbf{W}_2$. By an *envelope* for $\mathscr{F}$ we will mean a smooth curve $P = P(s)$, parametrized by the arclength of g, such that at any regular point $P(s)$ the tangent line to P is $M(s)$. Then, P may be written in the form $P(s) = g(s) + Q(s)\mathbf{W}_1(s)$, for some smooth function $Q(s)$ such that $P'(s)$ is always a multiple of $\mathbf{W}_1(s)$. Since

$$\begin{aligned} P'(s) &= \mathbf{T} + Q'(s)\mathbf{W}_1(s) + (\kappa(s) + \alpha'(s))Q(s)\mathbf{W}_2(s) \\ &= (Q'(s) + \cos\alpha(s))\mathbf{W}_1(s) + [(\kappa(s) + \alpha'(s))Q(s) - \sin\alpha(s)]\mathbf{W}_2(s), \end{aligned}$$

we must have

$$(\kappa(s) + \alpha'(s))Q(s) - \sin\alpha(s) = 0. \tag{6}$$

On intervals for which $\kappa(s) + \alpha'(s) \neq 0$ we can solve equation (6) for Q, getting $Q(s) = \frac{\sin\alpha(s)}{\kappa(s) + \alpha'(s)}$, and our envelope takes the form

$$P(s) = g(s) + Q(s)\mathbf{W}_1(s), \quad Q(s) = \frac{\sin\alpha(s)}{\kappa(s) + \alpha'(s)}. \tag{7}$$

Conversely, if $\kappa(s) + \alpha'(s) \neq 0$ and P is defined by (7) then P is an envelope for $\mathscr{F}$. (The existence of an envelope for $\mathscr{F}$ when $\kappa(s) + \alpha'(s) = 0$ is a much more subtle question whose investigation would take us too far afield.)

A few examples will illustrate the usefulness of parametrization (7).

Example 2. Recall that the general solution $y = mx + f(m)$ to Clairaut's differential equation, $y = xy' + f(y')$ may be interpreted as a one-parameter family of lines in which the parameter is the *slope* of each line. The singular solution of Clairaut's equation is the envelope of this family of lines and can be parametrized by the pair of equations $x = -f'(t)$ and $y = -tf'(t) + f(t)$. On the other hand, we could consider a one-parameter family $\mathscr{F}$ of lines $y = f(b)x + b$ in which the parameter is the *y-intercept* of each line. The corresponding variant of Clairaut's equation is then given by

$$y' = f(y - xy'). \tag{8}$$

Using the parametrization (7) we can obtain the envelope of $\mathscr{F}$. In this case the curve $g(s) = (0, s)$ has curvature identically 0, $\mathbf{T} = \mathbf{j}, \mathbf{N} = -\mathbf{i}$. We assume without loss of generality that our spanning vector $\mathbf{W}_1$ always has negative $\mathbf{i}$ component. Then our angle function $\alpha(s)$ satisfies the equations $\sin\alpha = \frac{1}{\sqrt{1+f^2}}$, $\cos\alpha = -\frac{f}{\sqrt{1+f^2}}$, and $\cot\alpha(s) = -f(s)$. Since $\alpha' = \frac{f'}{1+f^2}$ and $\kappa + \alpha' = \alpha' = \frac{f'}{1+f^2}$, we will restrict attention to intervals over which $f'(s) \neq 0$. Then $Q = \frac{\sqrt{1+f^2}}{f'}$ and $\mathbf{W}_1 = -\left(\frac{1}{\sqrt{1+f^2}}\mathbf{i} + \frac{f}{\sqrt{1+f^2}}\mathbf{j}\right)$. Substitution into our expression (7) for $P(s)$ yields $P(s) = \left(-\frac{1}{f'(s)}, s - \frac{f(s)}{f'(s)}\right)$. It can be checked directly that the equations $x = -\frac{1}{f'(s)}$ and $y = s - \frac{f(s)}{f'(s)}$ parametrize a singular solution to (8). (The reader is invited to solve (8) in the manner of Clairaut's equation by making the change of variables $s = y - xy'$.)

Example 3. Fix a pair of positive integers $q < p$ and take $g(s) = (\cos s, \sin s)$ to be the unit-circular immersion of the s-axis into the plane. Define $\mathscr{F}$ to be the family of chords between $g(s)$ and $g(\frac{ps}{q})$. FIGURE 9 displays $\mathscr{F}$ for $(p, q) = (2, 1)$ and $(p, q) = (9, 4)$. The central angle of each chord has measure $\frac{ps}{q} - s = \frac{(p-q)}{q}s$ from which it immediately follows that the angle $\alpha(s)$ between the chord and the unit tangent $\mathbf{T}$ at $g(s)$ has measure $\alpha(s) = \frac{(p-q)}{2q}s$. Since the unit tangent $\mathbf{T}$ makes an angle of $s + \pi/2$ with the horizontal, our spanning vector $\mathbf{W}_1(s)$ makes an angle of $s + \pi/2 + \frac{(p-q)}{2q}s = \pi/2 + \frac{(p+q)}{2q}s$ with the horizontal. Therefore,

$$\begin{aligned}\mathbf{W}_1(s) &= \cos\left(\pi/2 + \frac{(p+q)}{2q}s\right)\mathbf{i} + \sin\left(\pi/2 + \frac{(p+q)}{2q}s\right)\mathbf{j}\\ &= -\sin\left(\frac{(p+q)}{2q}s\right)\mathbf{i} + \cos\left(\frac{(p+q)}{2q}s\right)\mathbf{j}.\end{aligned}$$

Since $\alpha'(s) = \frac{(p-q)}{2q}$ and $\kappa = 1$, we compute that

$$Q(s) = \frac{\sin\left(\frac{p-q}{2q}s\right)}{1 + \frac{p-q}{2q}} = \frac{2q\sin\left(\frac{p-q}{2q}s\right)}{p+q}.$$

Equation (7) for the envelope then becomes (after using the identities $\sin A \sin B = \frac{1}{2}\cos(A-B) - \frac{1}{2}\cos(A+B)$ and $\sin A \cos B = \frac{1}{2}\sin(A+B) + \frac{1}{2}\sin(A-B)$)

$$P(s) = g(s) + Q(s)\mathbf{W}_1(s) = \left(\frac{p\cos s + q\cos\left(\frac{p}{q}s\right)}{p+q}, \frac{p\sin s + q\sin\left(\frac{p}{q}s\right)}{p+q}\right).$$

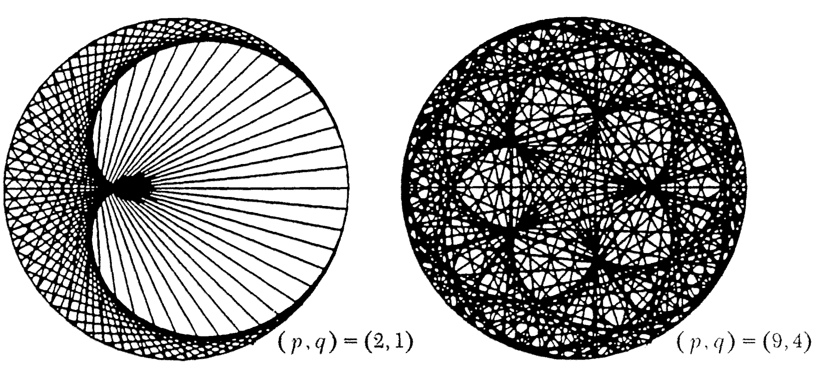


FIGURE 9
Families of chords in a circle.

Since $P'(s) = (Q'(s) + \cos\alpha(s))\mathbf{W}_1(s)$, to find the cusps of this envelope we must find the solutions to

$$Q'(s) + \cos\alpha(s) = \frac{p-q}{p+q}\cos\alpha(s) + \cos\alpha(s) = \frac{2p}{p+q}\cos\alpha(s) = 0.$$

It follows that cusps occur for $s = \frac{(2n-1)q\pi}{p-q} = \frac{(2n-1)q'\pi}{p'-q'}$, $n = 1, \dots, p'-q'$, where p' and q' are the quotients of p and q by the g.c.d. of p and q. This fact has an interesting interpretation in terms of a spirograph **[4]**.

Example 4. Suppose g is the ellipse $r = f(\theta) = \frac{A}{1 + e\cos\theta}$ of eccentricity e, with left focus F_1 and right focus the origin F_2, oriented counterclockwise. Let s denote arclength along g and express θ as the function $\theta = \theta(s)$. Define $\mathscr{F}$ to be the one-parameter family of lines through F_1 and $g(\theta) = (f(\theta)\cos\theta, f(\theta)\sin\theta)$ parametrized by s. A spanning vector field $\mathbf{W}_1(s)$ for $\mathscr{F}$ is obtained by rotating the oriented unit tangent $\mathbf{T}$ to g at $g(\theta)$ counterclockwise through an angle $\alpha = \alpha(s)$ such that $\cos\alpha(s) = \frac{f'(\theta)}{\sqrt{f'(\theta)^2 + f(\theta)^2}}$. The point curve $P(s) = F_1$ may be written in the form $F_1 = P(s) = g(\theta) + Q(s)\mathbf{W}_1(s)$ where $Q(s)$ is the distance from $g(\theta)$ to F_1. It is clear that P is an everywhere singular envelope of $\mathscr{F}$ and it then follows from equation (6) that (i) $(\kappa(s) + \alpha'(s))Q - \sin\alpha(s) = 0$ for all values of s. Since $\sin\alpha(s) = \frac{f(\theta)}{\sqrt{f'(\theta)^2 + f(\theta)^2}} \neq 0$, (i) implies $\kappa(s) + \alpha'(s) \neq 0$. (We will need this result later.) Because $\mathbf{0} = P'(s) = (Q'(s) + \cos\alpha(s))\mathbf{W}_1(s)$ it follows that (ii) $Q'(s) + \cos\alpha(s) = Q'(s) + \frac{f'(\theta)}{\sqrt{f'(\theta)^2 + f(\theta)^2}} = 0$. Both (i) and (ii) correspond to geometrical properties of an ellipse, the second well-known and the first less-known. Since $Q(s)$ is the distance from $g(s)$ to F_1 and $Q'(s) = \frac{Q'(\theta)}{\sqrt{f'(\theta)^2 + f(\theta)^2}}$, equation (ii) is equivalent to the defining property that the sum of the distances from any point on the ellipse to the two foci is a constant. Equation (i) also has an interesting geometrical interpretation. Let $\beta = \beta(s)$ denote the angle $\mathbf{T}$ makes with the horizontal and let $\gamma(\theta)$ denote the angle that the ray from F_1 through the point $r = f(\theta)$ makes with the horizontal (i.e., γ is the angle of elevation of points on the ellipse with respect to the left-hand focus F_1). Then, in terms of the notation above, $\alpha + \beta = \gamma + \pi$. Differentiating both sides of this equation with respect to s and using equation (i) together with the fact that $\kappa(s) = \beta'(s)$ yields $\gamma'(s) = \frac{\sin\alpha(s)}{Q(s)}$. Since $\sin\alpha(s) = \frac{f(\theta)}{\sqrt{f'(\theta)^2 + f(\theta)^2}}$ and $\gamma'(s) = \frac{\gamma'(\theta)}{\sqrt{f'(\theta)^2 + f(\theta)^2}}$ we have $\gamma'(\theta) = \frac{f}{Q}$. In other words, the rate at which γ is changing with respect to θ is equal to the ratio of the distances to the two foci of the corresponding point on the ellipse.

We now return to the family of separation lines associated to our rotating beacon problem. Since α_p is a smooth function defined on open θ intervals, we may use (7) to parametrize the envelope of this family.

Example 5. Consider again Example 1 and assume the rotation rate ω is greater than 1. We argued previously that the set of ordinary points is then the open disk centered at the origin of radius $\rho = 1/\omega$. Furthermore, it is clear that in this case the boundary of this disk is also an envelope for the family $\mathscr{F}$ of separation lines. We see from FIGURE 7 that this disk has a parametrization $P(\theta) = \rho(\cos(\theta + \alpha_\rho(\theta)), \sin(\theta + \alpha_\rho(\theta))$. We can confirm this observation using our parametrization (7). We have, $r = f(\theta) = 1$, $\kappa = 1$, $\cos\alpha(s) = \rho$, $Q(s) = \sin\alpha(s) = \sqrt{1-\rho^2}$, and $\mathbf{W}_1(s) = \rho\mathbf{T} + \sqrt{1-\rho^2}\,\mathbf{N}$ where $\mathbf{T} = -\sin\theta\mathbf{i} + \cos\theta\mathbf{j}$ and $\mathbf{N} = -\cos\theta\mathbf{i} - \sin\theta\mathbf{j}$. Substitution into equation (7) yields

$$P(\theta) = \left(\rho^2\cos\theta - \rho\sqrt{1-\rho^2}\sin\theta,\ \ \rho^2\sin\theta + \rho\sqrt{1-\rho^2}\cos\theta\right).$$

We showed in Example 1 that $\alpha_\rho(\theta)$ is the constant $\arccos\rho$. It immediately follows from the addition formulas for sine and cosine that $P(\theta) = \rho(\cos(\theta + \alpha_\rho(\theta)), \sin(\theta + \alpha_\rho(\theta))$.

Next we wish to show that the boundary of the set of ordinary points is a subset of the union of the screen with the envelope for the family of separation lines.

THEOREM 4. *Let S denote a boundary point of the ordinary set. Then S is either on the screen or on the envelope of the family of separation lines.*

Proof. Because a complete proof of this result is rather lengthy, we will merely sketch the argument. Suppose S is a boundary point of the set of ordinary points that does not belong to the screen. Then there is a separation line $L(s)$ through some $g(s)$ that contains S. Assume without loss of generality that $s = 0$ and consider the separation line $L = L(s)$ through $g(s)$ for a *negative* value of s very close to 0. Since $g(0)$ will then belong to the extraordinary side of $L(s)$, $L(s)$ must intersect $L(0)$ either at the point S or at a point between S and $g(0)$ in order that S not be on the extraordinary side of $L(s)$ and thus isolated from the set of ordinary points. We let $A(s)$ denote the intersection of $L(s)$ and $L(0)$ for s a negative number close to 0. Likewise, for s a very small *positive* number, the intersection $B(s)$ of the separation line $L(s)$ with $L(0)$ must either be at S or S must lie between $B(s)$ and $g(0)$. (See FIGURE 10 for a typical picture.) It can be shown that the existence of boundary point S implies $\kappa(0) + \alpha_\rho'(0) > 0$ so that an envelope $P = P(s)$ for the family of separation lines is defined for values of s near 0. An envelope for a family of curves is sometimes referred to as the *locus of intersections*. What this means for our family $\mathscr{F}$ of separation lines, is that as s approaches 0, both $A(s)$ and $B(s)$ approach the point $P(0)$ on the envelope of $\mathscr{F}$. Since S is always "between" $A(s)$ and $B(s)$, the squeeze theorem implies $S = P(0)$ and S is on the envelope.

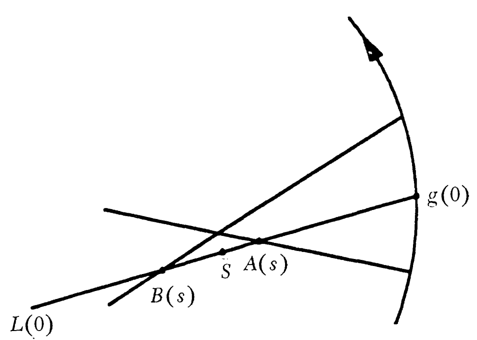


FIGURE 10
Intersecting separation lines near a boundary point S.

It follows from Theorem 4 that to understand the "shape" of the set of ordinary points, it suffices to understand the shape of the envelope. In the next section we will discover a surprising interpretation of this shape in the case of an elliptical screen.

4. Interpreting a fishy-looking envelope

We saw in PROPOSITION 3(a) that the only scenario for which there is a nonempty set of ordinary points at arbitrarily high rotation rates is an elliptical screen with the beacon located at a focus of the ellipse. In other words, for no other case will the set of ordinary points display interesting "asymptotic" behavior at high rotation rates of the beacon.

FIGURE 11 illustrates the effects of an increasing rotation rate ω on the envelope of separation lines for the ellipse $r = \frac{1}{2+\cos\theta}$. We see that one effect of the rotation rate is upon the *size* of the envelope. As the rate increases the envelope appears to shrink to the second (non-beacon) focus of the ellipse. In fact, a straightforward continuity argument using equations (7) shows this to be the case whenever the beacon is at a focus of an elliptical screen.

A more subtle effect of the rotation rate is upon the *shape* of the envelope. Note that in FIGURE 11 as the rotation rate ω increases, the envelope becomes more symmetric and appears to rotate towards a vertical axis of symmetry. It also appears that the influence of the rotation rate upon the shape of the envelope becomes less pronounced as ω increases. In this regard, it is instructive to plot the envelopes corresponding to relatively large rotation rates. FIGURE 12 displays *Mathematica* plots of the envelopes for $\omega = 100$ and $\omega = 1000$. At first glance the two envelopes appear to be the same curve. However, by inspecting the scale of the two plots we see that the envelope that corresponds to $\omega = 1000$ is actually 10 times smaller than the envelope for $\omega = 100$. Consequently, it appears that for large values of ω the *shape* of the envelope stabilizes while the *size* of the envelope becomes a linear function of $\rho = 1/\omega$. Such (approximate) linear behavior suggests that we are viewing some kind of derivative.

Let us fix an elliptical screen E with foci F_1 and F_2 and assume the beacon is located at F_2. Let $P(\theta, \rho)$ denote the envelope for the family of separation lines

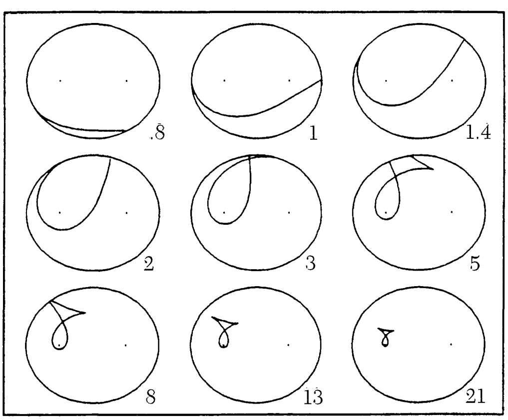


FIGURE 11
The vanishing ellipse (envelope version).

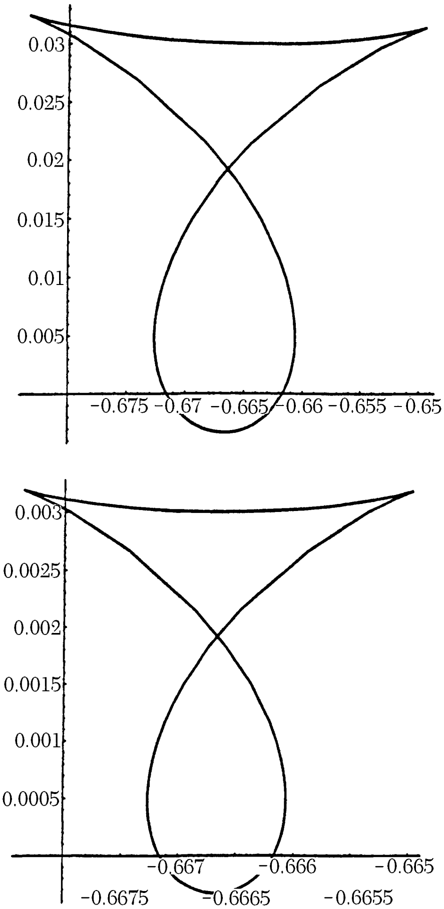


FIGURE 12
Same or different?

through E corresponding to a rotation rate of $\omega = 1/\rho$. When $\rho = 0$ the family of separation lines becomes the family $\mathscr{F}$ of Example 4 which has the everywhere singular envelope $P(\theta, 0) = F_1$. The argument in Example 4 shows that $\kappa(s) + \frac{\partial \alpha}{\partial s}(s, 0) \neq 0$, from which it follows that for values of ρ near 0 a separation line is defined for each value of θ and we have $\kappa(s) + \frac{\partial \alpha}{\partial s}(s, \rho) \neq 0$. We will restrict attention to such values of ρ throughout the remainder of this paper. We then expect $P(\theta, \rho) \approx F_1 + \rho \frac{\partial P}{\partial \rho}(\theta, 0)$ for values of ρ close to 0. This suggests that for large rotation rates, the *shape* of the envelope will be approximately that of the curve $\theta \to \frac{\partial P}{\partial \rho}(\theta, 0)$. FIGURE 13 shows that a *Mathematica* plot of this curve is in agreement with the expected shape.

Next, we wish to determine *why* the curve $\theta \to \frac{\partial P}{\partial \rho}(\theta, 0)$ has the shape of an inverted, stylized "fish." An important clue is provided in FIGURE 14, which is taken from page 133 of *Curves and Singularities*, by J. W. Bruce and P. J. Giblin **[2]**. The family of lines in the figure consists of the perpendicular bisectors of segments joining the left focus of the ellipse (the "eye" of the fish) to points of the ellipse. The envelope of this family of lines is called an *antiorthotomic* of the ellipse. (The locus of

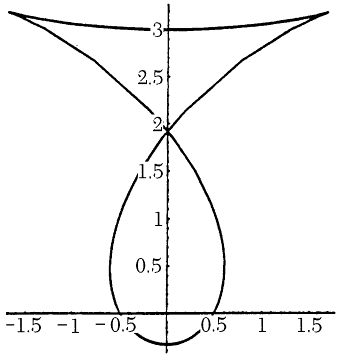


FIGURE 13

The partial derivative curve $\frac{\partial P}{\partial p}(\theta, 0)$.

reflections of a fixed point in the tangent lines of some curve is known as an *orthotomic* of the curve. By construction, the orthotomic of the "fish" curve with respect to the left focus of the ellipse is the ellipse itself. Hence, this fish-shaped curve is known as an antiorthotomic of the ellipse.) The similarity in shapes suggests that the curve $\theta \to \frac{\partial P}{\partial p}(\theta, 0)$ is an antiorthotomic of some ellipse. While our elliptical screen is an obvious candidate, some experimentation with *Mathematica* shows that, in general, the curve $\theta \to \frac{\partial P}{\partial p}(\theta, 0)$ has neither the size nor the shape nor the orientation of an antiorthotomic for our screen. Nonetheless, the similarity in shapes between our partial derivative curve and the antiorthotomic of an ellipse is so close that it would be a mistake to dismiss some sort of connection between the two. In order to make this connection, we need first to present a natural transformation of any ellipse into a second ellipse.

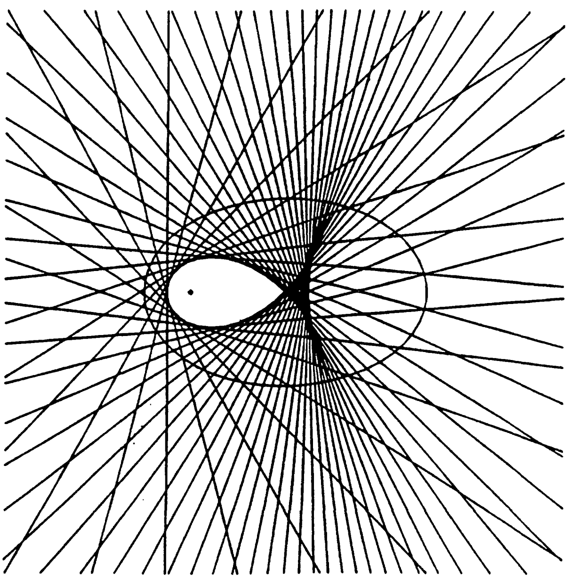


FIGURE 14

The antiorthotomic of an ellipse (p. 133 of *Curves and Singularities*, by J. W. Bruce and P. J. Giblin).

Suppose F_1 and F_2 denote the foci of an ellipse E in the plane. We let $F_1(E)$ denote the set of points that results if each point on E is scaled "away" from F_1 by the reciprocal of its distance to F_2. More precisely, a point Q is in $F_1(E)$ if and only if there exists a point P on E such that Q is the image of P under the dilation with center F_1 and ratio $1/\text{dist}(F_2, P)$. Note that when E is a circle then $F_1(E)$ is simply the unit circle concentric with E. Furthermore, it is easy to see that if E and E' are *similar* ellipses with F_1 a focus of E and F_1' a focus of E', then $F_1(E)$ is *congruent* to $F_1'(E')$. We can therefore think of the transformation $E \to F_1(E)$ as an "elliptical" or "two-point" generalization of unit normalization. Of particular significance is the fact that the elliptical transform of an ellipse is again an ellipse.

PROPOSITION 5. *If F_1 is a focus of an ellipse E of eccentricity e, then $F_1(E)$ is an ellipse with one focus at F_1 and eccentricity $\frac{2e}{1+e^2}$.*

Proof. Let F_1 and F_2 denote the foci of E and choose a system of polar coordinates with pole at F_1 and initial ray F_1F_2. Without loss of generality it may be assumed that E has a polar equation of the form $r = f(\theta) = \frac{A}{1 - e\cos\theta}$ for some positive constant A. Suppose P is the point $r = f(\theta)$ on E. Then $f(\theta) = \text{dist}(F_1, P)$ and $\text{dist}(F_1, P) + \text{dist}(F_2, P) = \frac{2A}{1-e^2}$. Consequently,

$$\text{dist}(F_2, P) = \frac{2A}{1-e^2} - f(\theta) = \frac{2A(1 - e\cos\theta) - A(1-e^2)}{(1-e^2)(1 - e\cos\theta)},$$

and a little algebra shows that the image of P under the dilation with center F_1 and ratio $1/\text{dist}(F_2, P)$ is a point whose distance to F_1 is

$$r = \frac{(1-e^2)/(1+e^2)}{1 - 2e\cos\theta/(1+e^2)}.$$

This is the polar equation of an ellipse with a focus at F_1 and with eccentricity $\frac{2e}{1+e^2}$.

We have already observed that the *similarity* class of E determines the *congruence* class of $F_1(E)$. In fact, it is straightforward to show that $F_1(E)$ is the unique ellipse with eccentricity $\frac{2e}{1+e^2}$, a focus at F_1, center on ray F_1F_2, and semiminor axis 1. FIGURE 15 illustrates the effects of this transformation on several choices of E. Our next goal is to relate the partial derivative curve $\theta \to \frac{\partial P}{\partial \rho}(\theta, 0)$ with the elliptical transformation of our screen.

THEOREM 6. *Let $P(\theta, \rho)$ denote the envelope of the family of separation lines associated to a rotating beacon problem within an elliptical screen of eccentricity e, beacon at a fixed focus of the screen, and rotation rate $\omega = 1/\rho$. The curve $\frac{\partial P}{\partial \rho}(\theta, 0)$ is then an antiorthotomic of an ellipse of eccentricity $\frac{2e}{1+e^2}$ and semiminor axis 2. Furthermore, this antiorthotomic has an axis of symmetry orthogonal to the major axis of the elliptical screen.*

Proof. Assume that $g(s)$ is a unit speed parametrization of an elliptical screen with the beacon at the right-hand focus F_2, Frenet frame $\mathbf{T}$ and $\mathbf{N}$, and curvature κ. Let $\alpha(s, \rho) = \alpha_\rho(s)$ denote the angle between $\mathbf{T}$ and the separation line through $g(s)$ that corresponds to a rotation rate of $\omega = \frac{1}{\rho}$. The vector field $\mathbf{W}_1 = \mathbf{W}_1(s, \rho) = \cos\alpha\mathbf{T} + \sin\alpha\mathbf{N}$ is then a spanning vector field for the family of separation lines

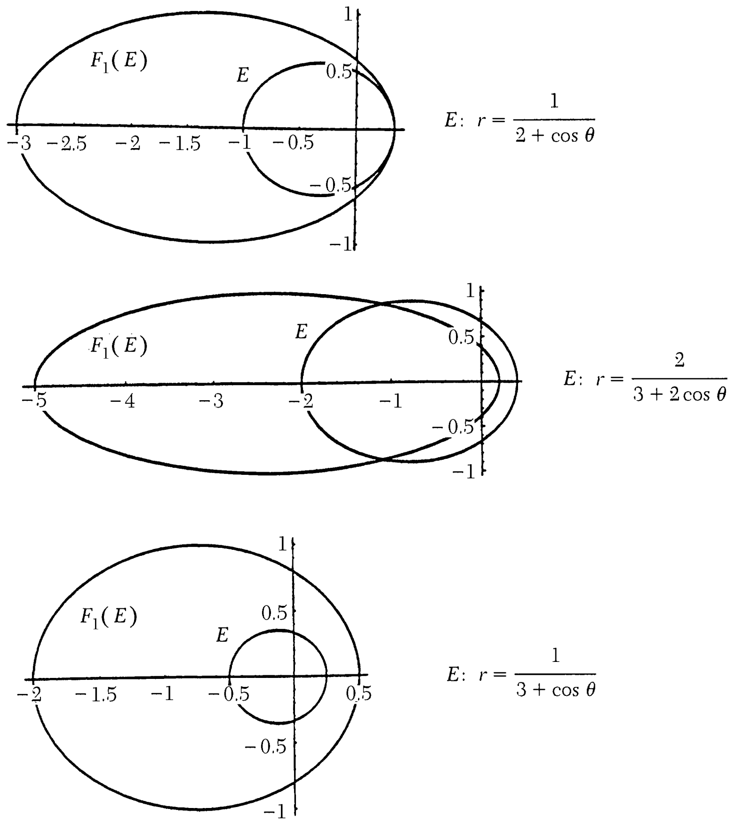


FIGURE 15
Transforming an ellipse E into a second ellipse $F_1(E)$.

corresponding to rotation rate ω. Define $\mathbf{W}_2 = \mathbf{W}_2(s, \rho) = -\sin\alpha\mathbf{T} + \cos\alpha\mathbf{N}$. Then

$$\frac{\partial \mathbf{W}_1}{\partial \rho} = \frac{\partial \alpha}{\partial \rho}\mathbf{W}_2 \quad \text{and} \quad \frac{\partial \mathbf{W}_1}{\partial s} = \left(\kappa + \frac{\partial \alpha}{\partial s}\right)\mathbf{W}_2. \tag{9}$$

Likewise,

$$\frac{\partial \mathbf{W}_2}{\partial \rho} = -\frac{\partial \alpha}{\partial \rho}\mathbf{W}_1 \quad \text{and} \quad \frac{\partial \mathbf{W}_2}{\partial s} = -\left(\kappa + \frac{\partial \alpha}{\partial s}\right)\mathbf{W}_1. \tag{10}$$

It follows from (7) that for fixed ρ,

$$P(s, \rho) = g(s) + Q(s, \rho)\mathbf{W}_1(s, \rho), \quad Q(s, \rho) = \frac{\sin\alpha}{\kappa + \dfrac{\partial \alpha}{\partial s}},$$

is an envelope of the corresponding family of separation lines. We wish to show that $\frac{\partial P}{\partial \rho}(s, 0)$ is an antiorthotomic of an ellipse. Using the equations above, we have

$$\frac{\partial P}{\partial \rho} = \frac{\partial Q}{\partial \rho}\mathbf{W}_1 + Q\frac{\partial \alpha}{\partial \rho}\mathbf{W}_2. \tag{11}$$

We will first show that the tangent vector $\frac{\partial^2 P}{\partial s \partial \rho}(s,0)$ to $\frac{\partial P}{\partial \rho}(s,0)$ is a multiple of $\mathbf{W}_1(s,0)$. Differentiating both sides of equation (11) with respect to s and using equations (9) and (10), we have

$$\frac{\partial^2 P}{\partial s \partial \rho} = \left(\frac{\partial^2 Q}{\partial s \partial \rho} - Q\frac{\partial \alpha}{\partial \rho}\left(\kappa + \frac{\partial \alpha}{\partial s}\right)\right)\mathbf{W}_1 + \left(\frac{\partial Q}{\partial \rho}\left(\kappa + \frac{\partial \alpha}{\partial s}\right) + \frac{\partial Q}{\partial s}\frac{\partial \alpha}{\partial \rho} + Q\frac{\partial^2 \alpha}{\partial s \partial \rho}\right)\mathbf{W}_2.$$

It suffices to show that the coefficient of $\mathbf{W}_2$ vanishes when $\rho = 0$. By definition, $(\kappa + \frac{\partial \alpha}{\partial s})Q - \sin\alpha = 0$, identically. Differentiating both sides of this equation with respect to ρ yields $(\kappa + \frac{\partial \alpha}{\partial s})\frac{\partial Q}{\partial \rho} + \frac{\partial^2 \alpha}{\partial \rho \partial s}Q - (\cos\alpha)\frac{\partial \alpha}{\partial \rho} = 0$. Equation (ii) of Example 4 implies $\frac{\partial Q}{\partial s}(s,0) = -\cos\alpha(s,0)$. Replacing $-\cos\alpha$ by $\frac{\partial Q}{\partial s}(s,0)$ we see that the coefficient of $\mathbf{W}_2(s,0)$ is indeed 0. As a result, we have shown that at nonsingular points, the tangent line to the curve $\frac{\partial P}{\partial \rho}(s,0)$ is parallel to the line through $g(s)$ and the non-beacon focus F_1 of the ellipse. (Recall that all the "separation lines" pass through F_1 when $\rho = 0$.)

It follows that the translate $F_1 + \frac{\partial P}{\partial \rho}(s,0)$ is an envelope for the family of lines $\mathscr{F} = \{M(s)\}$ where $M(s)$ is the line through $F_1 + \frac{\partial P}{\partial \rho}(s,0)$ parallel to the line through F_1 and $g(s)$. On the other hand, we are endeavoring to also show that this curve is the antiorthotomic of some ellipse. Consider the locus of reflections of the non-beacon focus F_1 through every line in $\mathscr{F}$. Since $\mathbf{W}_1(s,0)$ is parallel to $M(s)$ and since $\frac{\partial P}{\partial \rho} = \frac{\partial Q}{\partial \rho}\mathbf{W}_1 + Q\frac{\partial \alpha}{\partial \rho}\mathbf{W}_2$, $M(s)$ will be located a distance of $|Q(s,0)\frac{\partial \alpha}{\partial \rho}(s,0)|$ from F_1. We saw in Example 4 that $Q(s,0)$ is the distance from $g(s)$ to F_1. From the definition of a separation line we know that

$$\cos\alpha = \frac{\rho}{\sqrt{f'^2 + f^2}} + \frac{f'}{\sqrt{f'^2 + f^2}} \tag{12}$$

where $r = f(\theta)$ is the polar equation of the ellipse. It follows that $\cos\alpha(s,0) = \frac{f'(\theta)}{\sqrt{f'^2(\theta) + f^2(\theta)}}$; we then also have $\sin\alpha(s,0) = \frac{f(\theta)}{\sqrt{f'^2(\theta) + f^2(\theta)}}$. Differentiating both sides of equation (12) with respect to ρ yields the equation $(-\sin\alpha)\frac{\partial \alpha}{\partial \rho} = \frac{1}{\sqrt{f'^2 + f^2}}$. Solving, we find that

$$\frac{\partial \alpha}{\partial \rho}(s,0) = \frac{-1}{\sin\alpha(s,0)\sqrt{f'^2 + f^2}} = \frac{-1}{f}.$$

Therefore, the distance from F_1 to the line $M(s)$ is the ratio $\frac{Q(s,0)}{f(s)}$ of the distance from $g(s)$ to F_1 to the distance from $g(s)$ to the beacon F_2. Furthermore, we know that $M(s)$ is parallel to the line through $g(s)$ and F_1 and is on the side of this line opposite the direction of $\mathbf{W}_2(s,0)$ (since $Q(s,0)\frac{\partial \alpha}{\partial \rho}(s,0) = \frac{-Q(s,0)}{f(s)}$ is *negative*). Consequently, the operation of reflection of F_1 through $M(s)$ yields the same point as the operation of first scaling $g(s)$ "away" from F_1 by twice the reciprocal of the distance from $g(s)$ to F_2, then rotating this scaled point 90 degrees counterclockwise about F_1. If this operation is applied to each point $g(s)$ on the elliptical screen, the resulting collection of points is the orthotomic (with respect to F_1) of the (translated) partial derivative curve $F_1 + \frac{\partial P}{\partial \rho}(s,0)$. Scaling by twice the reciprocal simply makes the orthotomic twice as big as scaling by the reciprocal, and the only effect of rotating 90 degrees about F_1 is to change the orientation of the orthotomic. Thus, it immediately follows from Proposition 5 that this orthotomic is an ellipse and the translate $F_1 + \frac{\partial P}{\partial \rho}(s, 0)$ is an antiorthotomic of this ellipse. Therefore, $\frac{\partial P}{\partial \rho}(s, 0)$ is an antiorthotomic for a translate of this ellipse.

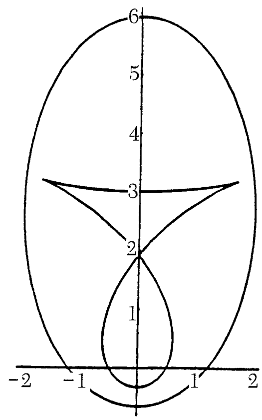


FIGURE 16

The curve $\dfrac{\partial P}{\partial p}(\theta, 0)$ is the antiorthotomic of an ellipse.

FIGURE 16 illustrates Theorem 6 in the case of the elliptical screen $r = \frac{1}{2 + \cos\theta}$.

5. Further questions and conclusions

Theorem 6 answers our question about the "shape" of the partial derivative curve $\frac{\partial P}{\partial \rho}(s, 0)$. Perhaps the next natural problem would be to determine the shape of the higher order partial derivative curves $\frac{\partial^n P}{\partial \rho^n}(s, 0)$. For example, FIGURE 17 shows the partial derivative curves corresponding to $n = 1, 2, 3$ and 4 for the ellipse $r = \frac{1}{2 + \cos\theta}$. Inspecting FIGURE 17 one might suspect that the odd order partial derivative curves have an axis of symmetry orthogonal to the major axis of the elliptical screen, while for the even order partial derivative curves the (extended) major axis of the screen is an axis of symmetry. A careful bookkeeping of the even and odd functions that appear in the expressions for the partial derivative curves shows that this is indeed the case. Unfortunately, the authors have had no success in interpreting the shape of these higher order partial derivative curves. Do there exist geometrical interpretations analogous to that in Theorem 6?

The *global* behavior of the envelope for a family of separation lines is worthy of further study. For example, it can be shown that if the envelope has self-intersections then some type of singular behavior (cusps, running off to infinity, etc.) must occur. What other results of this type are there? (In this regard, we intentionally avoided the consideration of singularities in our parametrization. What can be said if singularities are allowed?)

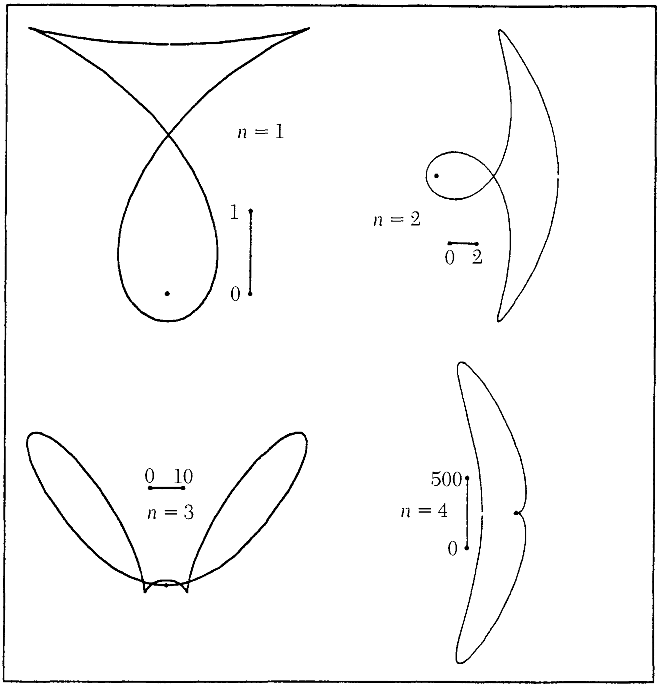


FIGURE 17

The curves $\frac{\partial^n P}{\partial p^n}(\theta, 0)$, for $n = 1$, 2, 3, and 4.

To conclude, we hope to have shown the reader that the rotating beacon problem is not simply an "old chestnut" located somewhere in the related rates section of his or her calculus textbook. Indeed, the authors have found the study of this problem to be a source of surprising connections between calculus and geometry. We hope that some reader will be inspired to continue the study of these connections.

REFERENCES

1. S. C. Althoen and J. F. Weidner, Related rates and the speed of light, *College Math. J.* 16 (1995), 186–189.
2. J. W. Bruce and P. J. Giblin, *Curves and Singularities*, Cambridge University Press, Cambridge, UK, 1984.
3. M. A. Rothman, Things that go faster than light, *Scientific American* 203 (1960), 142–152.
4. Andrew Simoson, An envelope for a spirograph, *College Math. J.* 28 (1997), 134–139.

A Historically Focused Course in Abstract Algebra

ISRAEL KLEINER
York University
Toronto, Ontario M3J 1P3
Canada

Introduction

I propose to describe a course in abstract algebra which I taught in an In-Service Master's Programme for Teachers of Mathematics at our university. Students do not follow this course with another in abstract algebra, so I was fortunate in not having to worry whether I had covered this or that material for the next algebra course. This presented an opportunity and a challenge: What are some of the major ideas of abstract algebra that I would want to impart? What algebraic legacy would I want to leave the students with? Since the students were high school teachers of mathematics, I wanted the course also to have at least broad relevance to their concerns as teachers.

All this suggested to me that the history of mathematics should play an important role in the course. History points to the sources of abstract algebra, hence to some of its central ideas; it provides motivation; and it makes the subject come to life.

To set the context for the course, here is a history of abstract algebra—in 100 words or less.

Prior to the 19th century algebra meant essentially the study of polynomial equations. In the 20th century algebra became the study of abstract, axiomatic systems such as groups, rings, and fields. The transition from the so-called classical algebra of polynomial equations to the so-called modern algebra of axiom systems occurred in the 19th century. Modern algebra came into existence principally because mathematicians were unable to solve classical problems by classical (pre-19th century) means. They invented the concepts of group, ring, and field to help them solve such problems [**2**], [**4**], [**14**], [**16**], [**17**], [**27**], [**28**].

This mini-history of algebra suggests the major theme of the course, namely showing how abstract algebra originated in, and sheds light on, the solution of "concrete" problems. It is a confirmation of Whitehead's paradoxical dictum that "the utmost abstractions are the true weapons with which to control our thought of concrete fact" [**18**, p. 466]. What I do in the course can be represented schematically as follows:

Problems ⟶ Abstractions ⟶ Solutions of original problems
Abstractions ⟶ Solutions of other problems

The item "Solutions of other problems" is intended to convey an important idea, namely that the abstract concepts whose introduction was motivated by concrete problems often superseded in importance the original problems which inspired them. In particular, the emerging new concepts and results were employed in the solution of other problems, often unrelated to, and sometimes more important than, the original problems which gave them birth. I will call the solutions of such problems "payoffs."

PROBLEM I. *Why is* $(-1)(-1) = 1$?

This problem is an instance of the issue of justification of the laws of arithmetic. It deals with relations between arithmetic and abstract algebra, and it leads the students to the concepts of ring, integral domain, ordered structure, and axiomatics.

The above problem became pressing for English mathematicians of the 19th century, who wanted to set algebra—to them this meant the laws of operation with numbers—on an equal footing with geometry by providing it with logical justification. The task was tackled by members of the Analytical Society at Cambridge [**21**]. We will focus on Peacock's work, *Treatise of Algebra* (1830), which proved the most influential.

Peacock's major idea was to distinguish between "arithmetical algebra" and "symbolical algebra." The former referred to operations involving only *positive* numbers, and hence in Peacock's view required no justification. For example, $a-(b-c) = a+c-b$ is a law of arithmetical algebra when $b > c$ and $a > (b-c)$. It becomes a law of symbolical algebra if no restrictions are placed on a, b, and c. In fact, *no interpretation of the symbols is called for*. Thus *symbolical algebra* is the subject—newly founded by Peacock—of operations with symbols which need not refer to specific objects but which obey the laws of arithmetical algebra. Peacock's justification for identifying the laws of symbolical algebra with those of arithmetical algebra is his *Principle of Permanence of Equivalent Forms* (a type of Principle of Continuity going back at least to Leibniz):

> *Whatever algebraic forms are equivalent when the symbols are general in form but specific in value, will be equivalent when the symbols are general in value as well as in form.*

Thus Peacock *decrees* that the laws of arithmetic shall also be the laws of (symbolical) algebra—an idea not at all unlike the axiomatic approach to arithmetic. For example, we can use Peacock's *Principle* to prove that $(-x)(-y) = xy$, as follows.

Since $(a-b)(c-d) = ac+bd-ad-bc$ whenever $a > b$ and $c > d$, this being a law of arithmetic and hence requiring no justification, it also becomes a law of symbolical algebra—that is, without restrictions on a, b, c, d. Letting $a = 0$ and $c = 0$ yields $(-b)(-d) = bd$, and completes the proof.

The significance of Peacock's work was that symbols took on a life of their own, becoming objects of study in their own right rather than a language to represent relationships among numbers. Some have said that these developments signalled the birth of abstract algebra [**2**].

We now make a seventy-year leap forward and take a modern, Hilbertian approach to the above topic. The idea is to define (characterize) the integers axiomatically as an ordered integral domain in which the positive elements are well ordered ([**19**], [**24**]), just as Hilbert (in 1900) characterized the reals axiomatically as the maximal archimedean ordered field [**3**], [**11**]. Of course, in the process we must define the various algebraic concepts that enter into the above characterization of the integers. We can then readily prove such laws as $(-a)(-b) = ab$ and $a \times 0 = 0$. This was done in the more general context of rings by Fraenkel in 1914 [**4**], [**7**].

Payoffs: The following issues arise from the account above:

(a) How can we establish (prove) a law such as $(-1)(-1) = 1$? This question leads to axioms. We cannot prove everything.

(b) What axioms should we set down to give a description of the integers? This question enables us to introduce the concepts of ring, integral domain, ordered ring, and well ordering (induction).

(c) How do we know when we have enough axioms? Here we introduce the idea of completeness of a set of axioms.

(d) What does it mean to characterize the integers? This sets the stage for the introduction of the notion of isomorphism.

(e) Could we have used fewer axioms to characterize the integers? For example, $a+b=b+a$ is not needed. Here we come face to face with the concept of independence of a set of axioms.

(f) Are we at liberty to pick and choose axioms as we please? This question permits us to introduce the notion of consistency, and more broadly, the issue of freedom of choice in mathematics.

The innocent-looking problem $(-1)(-1)=1$ can be a rich source of ideas!

PROBLEM II. *What are the integer solutions of* $x^2+2=y^3$?

This diophantine equation is an example of the famous Bachet equation $x^2+k=y^3$, introduced in the 17th century and solved only recently for arbitrary k. The problem deals with relations between number theory and abstract algebra, and it gives rise to the concepts of unique factorization domain and euclidean domain—important examples of commutative rings.

We begin with a simpler problem, namely to solve the diophantine equation $x^2+y^2=z^2$, with $(x, y)=1$, that is, to find all primitive Pythagorean triples. Although the solution was known in ancient Greece over 2000 years ago, if not earlier, we are interested in an "algebraic" solution—a legacy of the 19th century.

The key idea is to factor the left side of $x^2+y^2=z^2$ and thus obtain the equation $(x+yi)(x-yi)=z^2$ in the domain $G=\{a+bi\colon a,b\in\mathbb{Z}\}$ of Gaussian integers. This domain shares with the integers the property of unique factorization. In particular, since $x+yi$ and $x-yi$ are relatively prime in G (this follows because x and y are relatively prime in $\mathbb{Z}$) and their product is a square, each is a square (in G). Thus $x+yi=(a+bi)^2=(a^2-b^2)+2abi$. Comparing real and imaginary parts yields $x=a^2-b^2$, $y=2ab$, and since $x^2+y^2=z^2$, $z=a^2+b^2$. Conversely, it is easily shown that for any $a,b\in\mathbb{Z}$, $(a^2-b^2, 2ab, a^2+b^2)$ is a solution of $x^2+y^2=z^2$. We thus get all pythagorean triples. It is easy to single out the primitive ones among them.

Coming back to $x^2+2=y^3$, we proceed analogously by factoring the left side and get $(x+\sqrt{2}\,i)(x-\sqrt{2}\,i)=y^3$, an equation in the domain $D=\{a+b\sqrt{2}\,i\colon a,b\in\mathbb{Z}\}$. Here, too, we can show that $(x+\sqrt{2}\,i,\ x-\sqrt{2}\,i)=1$, hence $x+\sqrt{2}\,i$ and $x-\sqrt{2}\,i$ are cubes in D. In particular, $x+\sqrt{2}\,i=(a+b\sqrt{2}\,i)^3$. Simple algebra yields $x=\pm 5$, $y=3$. Of course it is easy to see that these are solutions of $x^2+2=y^3$. What the argument above shows is that they are the *only* solutions.

The Fermat equation $x^3+y^3=z^3$ can be dealt with similarly: $z^3=x^3+y^3=(x+y)(x+y\omega)(x+y\omega^2)$—an equation in the domain $E=\{a+b\omega\colon a,b\in\mathbb{Z},\ \omega$ a primitive cube root of $1\}$. The technical details are more complex here **[1]**, **[9]**.

Justifying the "details" in the solutions of the three diophantine equations above involves considerable work. In particular, we need to introduce the notions of unique factorization domain (UFD) and euclidean domain and to discuss some of their arithmetic properties. The three diophantine equations can be solved in the indicated manner *because* the respective domains G, D, and E in which they were embedded are UFDs.

Payoffs:

(a) We can solve Fermat's problem about the representability of integers as sums of two squares by a careful scrutiny of the primes in the domain G of Gaussian integers **[9]**, **[20]**.

(b) In arithmetic domains in which unique factorization fails we introduce, following Dedekind, ideals. We can thereby obtain a proof of Fermat's Last Theorem —the unsolvability in integers of $x^p + y^p = z^p$—for all $p < 100$ **[20]**. Here appear the elements of a rich subject—algebraic number theory. The subject originated to a large extent in attempts to solve such diophantine equations as we have considered above, in particular the Fermat equation **[14]**.

PROBLEM III. *Can we trisect a* 60^o *angle using only straightedge and compass?*

This is an instance of one of the three famous classical construction problems going back to Greek antiquity. It deals with relations between geometry and abstract algebra, and it leads the students to the concepts of field and vector space. This is a standard problem, usually given following the presentation of Galois theory. I put it centre-stage as a means of providing a "gentle" introduction to fields.

The problem of trisection was posed about 2500 years ago but solved only in 1837, by Wantzel, following the introduction of the requisite algebraic machinery. One must persevere!

The initial key idea was the translation of the geometric problem into the language of classical algebra—numbers and equations. This occurred in the 17th century. Thus the basic goal became the construction of *real numbers*, often as roots of equations. ("Construction" will henceforth mean "construction with straightedge and compass.") How do fields and vector spaces enter the picture?

If a and b are constructible, so are $a+b$, $a-b$, ab, and a/b (if $b \neq 0$)—all this is easy to show. Thus the constructible numbers form a field. But what *are* they?

Given a unit length 1, the above implies that we can construct all rational numbers $\mathbb{Q}$. We can also construct, for example, $\sqrt{2}$, as the diagonal of a unit square. More generally, if a is constructible, so is $\sqrt{a}$. We can therefore construct the field $\mathbb{Q}(\sqrt{a}) = \{p + q\sqrt{a} : p, q \in \mathbb{Q}\}$. This introduces the important notion of *field adjunction*. The objective is to show that all constructible numbers can be obtained by an iteration of the adjunction of square roots.

To proceed we need a numerical measure of how far $\mathbb{Q}(\sqrt{a})$ is removed from $\mathbb{Q}$. This leads to the concept of *degree* of a field extension, here the dimension of $\mathbb{Q}(\sqrt{a})$ as a vector space over $\mathbb{Q}$. The problem of trisection is next phrased in terms of fields. This is now late-19th-century abstract algebra. Enough machinery of field extensions is introduced—and not much more than that—to solve the trisection problem **[12]**.

A word about history versus genesis. Wantzel solved the trisection problem in 1837, essentially as we do: he reduced the problem to the solution of polynomial equations; introduced irreducible polynomials and rational functions of a given number of elements; and he derived conditions for constructibility in terms of the iteration of solutions of polynomial equations **[30]**. Although Wantzel's approach is similar in spirit to the modern one, he used neither fields nor vector spaces. We use both. Our approach in this course is genetic rather than strictly historical when this serves our purpose.

Payoffs:

(a) A characterization of the real numbers as a complete ordered field **[3]**.

(b) A discussion of algebraic and transcendental numbers **[8]**, **[20]**.

(c) A characterization of finite fields [**10**], [**19**].

(d) Proof of a special case of Dirichlet's theorem on primes in arithmetic progression, namely that $1, 1+b, 1+2b, 1+3b, \ldots$ contains infinitely many primes. For this we need cyclotomic field extensions [**8**].

PROBLEM IV. *Can we solve* $x^5 - 6x + 3 = 0$ *by radicals?*

Problems such as this, dealing with the solution of equations by radicals, gave rise to Galois theory. They touch on the relations between classical and abstract algebra.

Galois theory, in its modern incarnation, is a grand symphony on two major themes —groups and fields, and two minor themes—rings and vector spaces. Galois theory is thus a highlight of any course in abstract algebra. But to do it in detail would take almost an entire term. Moreover, the proofs of theorems are often long and sometimes tedious, and the payoff is long in coming. The intent in this course, then, is to get across some of the central ideas of Galois theory (such as the correspondence between groups and fields and what it is good for) often with examples rather than proofs.

We begin where the history of the subject begins: with Lagrange. Lagrange analyzed past solutions of the cubic and quartic to see if he could find in them a common method extendible to the quintic. Although he did not resolve the problem of solvability of the quintic by radicals, he did light upon a key idea, namely that the permutations of the roots of a polynomial equation are the "metaphysics" of its solvability by radicals [**17**], [**27**].

I try to give students a sense of Lagrange's ideas by showing how permutations of the roots of cubic and quartic equations help solve them by radicals [**5**], [**6**], [**27**]. Implicit in this is the notion of a group.

Although the Fundamental Theorem of Galois Theory is not needed to resolve the problem of solvability of the quintic, we do discuss the theorem, illustrating it with examples. It is a beautiful and important result, and it has nice applications—payoffs —aside from solvability by radicals.

Payoffs:

(a) Proofs of several important number-theoretic results: Fermat's "little" theorem, Euler's theorem, Wilson's theorem. The proofs use only very elementary group theory [**23**].

(b) Classification of the regular polygons constructible with straightedge and compass. Although Galois theory yields a rather quick solution [**25**], the problem can be resolved using some field theory (cyclotomic extensions) and very elementary group theory [**23**].

(c) An essentially algebraic proof of the Fundamental Theorem of Algebra [**25**].

(d) Proof of the irrationality of expressions such as $\sqrt[4]{3} + \sqrt[5]{4} + \sqrt[6]{72}$ [**22**].

PROBLEM V. *"Papa, can you multiply triples?"*

This problem deals with extensions of the complex numbers to hypercomplex numbers, for example, the quaternions. The question in the title was asked by Hamilton's sons of their father to inquire whether he had succeeded, after years of effort, in obtaining an algebra of triples of reals analogous to the complex numbers. The problem bears on relations between arithmetic/classical algebra and abstract algebra, and it gives rise to the concepts of an algebra (not necessarily associative) and a division ring (a skew field).

To set the scene, I give the students a brief history of complex numbers. An important point to keep in mind here is that complex numbers arose in connection with the solution of the *cubic* rather than the quadratic [**15**].

Hamilton's quaternions—a noncommutative "number system"—was conceptually a most important development, for it liberated algebra from the canons of arithmetic [**16**]. The history of their invention in 1843 is well documented and gives a rare glimpse of the creative process at work in mathematics [**29**].

Are there "numbers" beyond the quaternions? (What *is* a number, anyway?) Cayley's and, independently, Graves' octonions (8-tuples of reals) gave an affirmative answer, and raised the obvious question whether there are numbers beyond the octonions. This time the answer was negative; it was given by Frobenius and C. S. Peirce, again independently [**13**]. Implicit in these ideas are the notions of division ring and algebra.

Payoffs:

(a) Ideas on quaternions can be used to prove Lagrange's four-squares theorem: Every positive integer is a sum of four squares [**9**], [**10**].

(b) Are complex numbers unavoidable in the solution of the so-called irreducible cubic? Yes. There is a proof using the considerable power of Galois theory [**3**], but the result can also be established by means of elementary field-extension theory [**26**].

General remarks on the course

(a) The first and last problems, and probably also the second, are atypical in an abstract algebra course, but I have found them to be pedagogically enlightening and rich in algebraic ideas. Historically, they signalled the transition from classical to modern (abstract) algebra.

(b) The first problem begins with a "simple" numerical question. The idea is to ease students gently into the abstractions.

(c) While the sequence of topics in algebra books, and therefore in algebra courses, is usually: groups, rings, and fields, our problems introduce students first to rings, then fields, and finally groups. I have found this order to be more effective. It leaves to the end the conceptually most difficult notion, that of a group, which is "unnatural" to students.

(d) I have listed only five problems. It might be argued that this does not appear to be sufficient for an entire course. However, the problems are wide-ranging and rich in ideas, and are extendible in various directions, some of which are indicated in the various "payoff" sections.

(e) No textbook is used in the course. However, many references are given, both technical and historical, and students are expected to *read* some of them!

(f) The historical material used in the course comes mainly from secondary sources. Asking students (and instructors!) to read and assimilate primary sources would make the course unreasonably difficult. The course is quite challenging as it is. And its objectives can be met using secondary sources.

(g) The course tries to deal with wider mathematical *ideas* in addition to the standard algebraic fare: the "why" and "what for" in addition to the "how." This is reflected in the assignments. Thus, aside from being asked to do the usual types of problems, for example, to show that the additive inverse in a ring is unique, students are expected to write "mini-essays" involving both historical and technical matters, for example, to discuss De Morgan's contribution to algebra and how it advanced abstract algebraic thinking.

To read independently in the mathematical literature, and to *write* about what they have read, are tasks which mathematics students are not—but should become—accustomed to.

REFERENCES

1. W. W. Adams and L. J. Goldstein, *Introduction to Number Theory*, Prentice-Hall, Englewood Cliffs, NJ, 1976.
2. G. Birkhoff, Current trends in algebra, *Amer. Math. Monthly* 80 (1973), 760–782.
3. G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, 5th ed., A. K. Peters, New York, NY, 1996.
4. D. M. Burton and D. H. Van Osdol, Toward the definition of an abstract ring, in: *Learn from the Masters*, ed. by F. Swetz *et al*, Math. Assoc. of America, Washington, DC, 1995, 241–251.
5. A. Clark, *Elements of Abstract Algebra*, Dover, New York, NY, 1984.
6. R. A. Dean, *Classical Abstract Algebra*, Harper and Row, New York, NY, 1990.
7. A. Fraenkel, Über die Teiler der Null und die Zerlegung von Ringen, *Jour. für die Reine und Angew. Math.* 145 (1914), 139–176.
8. L. J. Goldstein, *Abstract Algebra: A First Course*, Prentice-Hall, Englewood Cliffs, NJ, 1973.
9. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Pr., Oxford, UK, 1978.
10. I. N. Herstein, *Topics in Algebra*, 2nd ed., Wiley, New York, NY, 1975.
11. D. Hilbert, Über den Zahlbegriff, *Jahresb. der Deut. Math. Verein.* 8 (1900), 180–184.
12. A. Jones, S. A. Morris, and K. R. Pearson, *Abstract Algebra and Famous Impossibilities*, Springer-Verlag, New York, NY, 1991.
13. I. L. Kantor and A. S. Solodovnikov, *Hypercomplex Numbers*, tr. by A. Shenitzer, Springer-Verlag, New York, NY, 1989.
14. I. Kleiner, The roots of commutative algebra in algebraic number theory, this MAGAZINE 68 (1995), 3–15.
15. ______, Thinking the unthinkable: the story of complex numbers (with a moral), *Math. Teacher* 81 (1988), 583–592.
16. ______, A sketch of the evolution of (noncommutative) ring theory, *L'Enseign. Math.* 33 (1987), 227–267.
17. ______, The evolution of group theory: a brief survey, this MAGAZINE 56 (1986), 195–215.
18. M. Kline, *Mathematics in Western Culture*, Oxford Univ. Pr., Oxford, UK, 1964.
19. N. H. McCoy and G. J. Janusz, *Introduction to Modern Algebra*, Wm. C. Brown, Dubuque, IA, 1992.
20. H. Pollard and H. G. Diamond, *The Theory of Algebraic Numbers*, Math. Assoc. of America, Washington, DC, 1975.
21. H. Pycior, George Peacock and the British origins of symbolical algebra, *Hist. Math.* 8 (1981), 23–45.
22. I. Richards, An application of Galois theory to elementary arithmetic, *Advances in Math.* 13 (1974), 268–273.
23. F. Richman, *Number Theory: An Introduction to Algebra*, Brooks/Cole, Belmont, CA, 1971.
24. I. Stewart, *Concepts of Modern Algebra*, Penguin, Harmondsworth, UK, 1975.
25. ______, *Galois Theory*, Chapman & Hall, London, UK, 1973.
26. J. M. Thomas, *Theory of Equations*, McGraw-Hill, New York, NY, 1938.
27. J. P. Tignol, *Galois Theory of Algebraic Equations*, Wiley, New York, NY, 1988.
28. B. L. van der Waerden, *A History of Algebra*, Springer-Verlag, New York, NY, 1985.
29. ______, Hamilton's discovery of quaternions, this MAGAZINE 49 (1976), 227–234.
30. P. L. Wantzel, Recherches sur les moyens de reconnaitre si un Problème de Géométrie peut se résoudre avec la règle et le compas, *Journ. de Math. Pures et Appl.* 2 (1837), 366–372.

Defining Chaos

MARIO MARTELLI
MAI DANG
TANYA SEPH
California State University
Fullerton, CA 92634-9480

I. Introduction

In the last thirty years scientists have found that unusual and unexpected evolution patterns arise frequently in important deterministic processes of interest to many different fields, including Chemistry, Physics, Biology, Medicine, Engineering, and Economics. Examples of such processes include chemical reactions, pulsation in gas lasers, atmospheric changes, blood cell oscillations, and neural networks. The most peculiar aspect of these patterns is their random-like behavior. The systems are deterministic. Consequently they are, at least in theory, perfectly predictable. Hence, it may seem contradictory to talk about random-like behavior. However, more often than not their evolution appears as a random sequence of events, at least to superficial analysis.

The name "chaotic systems" has been proposed to collect them loosely under a common roof. Biologists, chemists, mathematicians, philosophers, physicists, and others have tried to capture in a formal definition the distinctive and essential features characterizing these systems among all dynamical processes. The success has been limited. On the one hand, everyone recognizes that certain systems cannot be considered chaotic; on the other hand we could say, with a bit of exaggeration, that there are as many definitions of chaos as experts in this new area of knowledge (see, for example **[5]**, **[3]**, **[8]**, **[4]**, **[7]**). Moreover, and this is certainly not a desirable situation, the various definitions are not equivalent to each other.

Many reasons can be given for this state of affairs, and the fact that chaotic behavior is of great interest to many disciplines is certainly one of them. It is difficult to find a common ground that meets the needs and the standards of different fields. For example, an experimental scientist is inclined to adopt a definition that can be tested in a laboratory setting and is less concerned with exceptions. A theoretician, however, is interested in characterizing chaotic behavior uniquely, and does not feel the urgency to provide a definition which can be easily verified by means of numerical or experimental techniques.

The main purpose of this paper is to bring a contribution to the efforts aimed at capturing the distinctive features of chaotic systems in a way that is easily accessible to undergraduates. This purpose is achieved in two ways. The first is by introducing the reader to those definitions of chaotic systems that are more frequently encountered in the literature and do not use advanced mathematical concepts and tools. We illustrate the key components of each definition. We also include a comparison table (Table 3.1) to provide the reader with an "at a glance" overview of the common traits and differences among the various definitions. The second is by analyzing in more detail two simple definitions proposed in recent years, one by S. Wiggins **[8]** and the other by M. Martelli **[6]**. Although formulated in different manner, the two definitions are practically equivalent. Moreover, they seem to embody the essential features which all other definitions are trying to capture. Finally, the characterizing traits of these two definitions are suitable for easy and reliable numerical verification. Therefore, they appear to represent the most effective way to introduce chaotic behavior at an undergraduate level.

The paper is organized as follows. In section 2 we introduce terminology and notation frequently used throughout. In section 3 we present some of the most common definitions of chaos; and we analyze briefly their key components. In section 4 we establish the basic equivalence of the definitions of Wiggins and Martelli. We conclude the paper (section 5) with an analysis of the baker's transformation and with short remarks on numerical tests of chaotic behavior.

Before embarking on the plan we have outlined, we illustrate a simple dynamical system, which is chaotic according to *all* definitions presented later. The purpose of this discussion, conducted mainly by means of graphs, is to make the reader familiar with the characteristic features that each definition of chaos tries to capture.

Example 1.1. Let $f(x) = 4x(1-x)$. Notice that f maps the interval $[0,1]$ onto itself. Consider the dynamical system $x_{n+1} = f(x_n)$ governed by the function f in $[0,1]$. Select the point $x_0 = 0.3$ and study the sequence of iterates of f: $x_1 = f(0.3)$, $x_2 = f(x_1), \dots, x_{n+1} = f(x_n), \dots$. To see how this sequence behaves, plot the points (x_n, x_{n+1}) for $n = 500, 501, \dots, 1000$ and for $n = 1500, 1501, \dots, 2000$ in two side-by-side plots. (See FIGURE 1.1.) The points belong to the graph $G(f)$ of f since $x_{n+1} = f(x_n)$. It appears that they fill up $G(f)$ entirely in both cases. This graphical evidence suggests that no matter how small an interval $[a,b]$ is selected in $[0,1]$, the sequence $x_1 = f(0.3)$, $x_2 = f(x_1), \dots, x_{n+1} = f(x_n), \dots$ visits $[a,b]$ infinitely often. This is one feature of chaotic systems which all definitions try to capture: the presence of a sequence of iterates (orbit) that passes "as close as we like to any possible state of the system." We shall make this idea more precise in section 2 with the definition of topological transitivity.

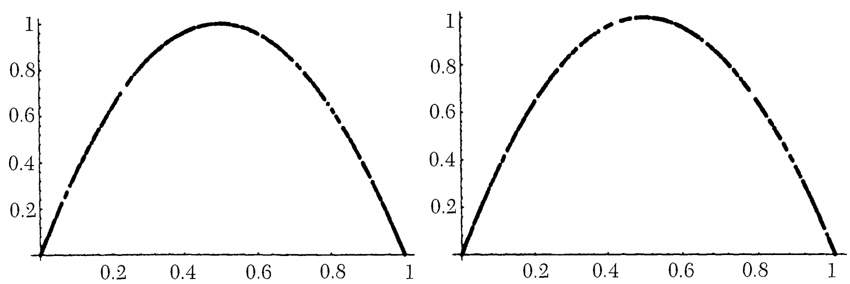


FIGURE 1.1

On the left graph we have plotted (x_n, x_{n+1}) for $n = 500, \dots, 1000$ and on the right for $n = 1500, \dots, 2000$ from the same sequence of iterates of f starting at $x_0 = 0.3$. It appears that in both cases the sequence is "reconstructing" the entire graph of f.

To illustrate another important property of the system $x_{n+1} = f(x_n)$, consider two sequences of iterates, one starting (as before) at $x_0 = 0.3$ and the other starting at a point very close to 0.3. Choose, for example, $y_0 = 0.300001$. Plot the points $(n, |x_n - y_n|)$, i.e., the iteration number on the horizontal axis and the distance between corresponding iterates of f on the vertical axis. At the beginning (for small values of n) the two sequences are close to each other. Later, they become separated, and the distance $|x_n - y_n|$ oscillates between 0 and 1 in an unpredictable fashion. (See FIGURE 1.2.)

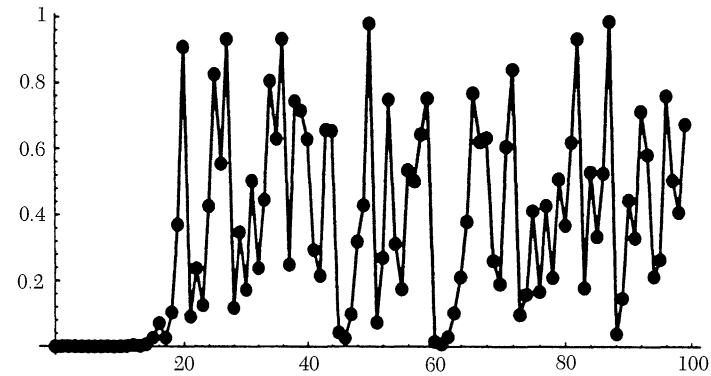


FIGURE 1.2

The distance $|x_n - y_n|$ is plotted versus the iteration number n. Notice that the two sequences of iterates are very close for $n = 0, 1, \dots, 15$. After that, separation takes over. Sometimes the two sequences are very close (around $n = 45$ and $n = 60$), and sometimes they are as far as they can be.

The graphical evidence suggests that the evolution of the system is very sensitive to small changes. Thus, if this system were a model of a real process, we would be tempted to conclude that its evolution, although governed by a known function, is nevertheless "unpredictable," since it is practically impossible to know the initial state exactly. This is a second feature of chaotic systems which every definition tries to capture, namely the sensitivity to small changes, and the unpredictability that comes with it. We shall make this idea more precise with the definition of unstable orbits and of sensitive dependence on initial conditions.

II. Notations and definitions

Let $F : \operatorname{Dom} F \subseteq \mathbb{R}^q \to \mathbb{R}^q$. A set $X \subseteq \operatorname{Dom} F$ is said to be *invariant* under the action of F if $F(X) \subseteq X$. In the case when $F(X)$ is bounded and F is continuous we can assume that the closure of X is contained in the domain of F. Then the invariance of X implies the invariance of its closure. In this paper we shall always assume, unless otherwise stated, that F is continuous and its invariant sets are closed and bounded.

Let $X \subseteq \operatorname{Dom} F \subseteq \mathbb{R}^q$ and assume that X is invariant. The discrete dynamical system defined by F in X takes the form

$$x_{n+1} = F(x_n). \tag{2.1}$$

Equation (2.1) provides the state x_{n+1} of the system at time $n + 1$ once its state x_n at time n is known. Given an initial state $x_0 \in \mathbb{R}^q$, the sequence of iterates of F:

$$x_0,\ x_1 = F(x_0),\ x_2 = F(x_1) = F(F(x_0)) = F^2(x_0), \dots, x_n = F^n(x_0), \dots \tag{2.2}$$

is the *orbit* of x_0, denoted by $O(x_0, F)$ or simply $O(x_0)$ when the function F is clearly specified. An orbit $O(x_0)$ is periodic if for some $p \geq 1$

$$x_p = x_0. \tag{2.3}$$

The smallest integer p for which (2.3) holds is called the *period* of the orbit. When $p = 1$ the orbit $O(x_0)$ is *stationary*, and the point x_0, now denoted by x_s, is an *equilibrium point* of the system. An orbit $O(y_0)$ is *asymptotically periodic* if there is a periodic orbit $O(x_0)$ such that

$$\lim_{n \to \infty} \| x_n - y_n \| = 0. \tag{2.4}$$

If, in addition, $y_k = x_k$ for some $k \geq 1$, then $O(y_0)$ is *eventually periodic*.

A point y is a *limit point* of $O(x_0)$ if a subsequence of $O(x_0)$ converges to y. The set of limit points of $O(x_0)$ is denoted by $L(x_0)$. Under our standard assumptions on X and F we have that $L(x_0)$ is closed and bounded and it satisfies the important equality

$$F(L(x_0)) = L(x_0). \tag{2.5}$$

The set $L(x_0)$ is finite if and only if $O(x_0)$ is asymptotically periodic. When $L(x_0)$ is infinite we say that $O(x_0)$ is *aperiodic*.

$O(x_0)$ is said to be *unstable* if there exists $r(x_0) > 0$ such that for every $d > 0$ we can find $y_0 \in \operatorname{Dom} F$ and $n \geq 1$ satisfying the two inequalities $\| y_0 - x_0 \| \leq d$ and $\| y_n - x_n \| > r(x_0)$. An orbit which is not unstable is said to be *stable*. When $O(x_0)$ is contained in an invariant set $X \subset \operatorname{Dom} F$, we say that $O(x_0)$ is unstable with *respect to* X if $y_0 \in X$. Notice that, in this case, the set X has to be infinite.

Let $X \subseteq \operatorname{Dom} F \subseteq \mathbb{R}^q$. F has in X *sensitive dependence on initial conditions* if there exists $r_0 > 0$ such that for every $x_0 \in X$ and $d > 0$ we can find $y_0 \in \operatorname{Dom} F$ and $n \geq 1$ with the property that $\|x_0 - y_0\| \leq d$ and $\|x_n - y_n\| > r_0$. Therefore, every orbit $O(x)$ with $x \in X$ is unstable with the same constant r_0. Consequently, sensitive dependence on initial conditions is stronger than instability. When $X \subset \operatorname{Dom} F$ is an invariant set and we require that $y_0 \in X$, we say that F has in X sensitive dependence on initial conditions *with respect to* X. In this case no point of X is isolated, i.e., for every $x \in X$ and every $c > 0$ we can find $y \in X$, $y \neq x$, such that $\|x - y\| \leq c$.

A set $U \subset X \subseteq \mathbb{R}^q$ is said to be *open in* X if $U = X \cap O$ where O is an open subset of $\mathbb{R}^q$. The function F is *topologically transitive* on an invariant set X if for every pair of sets $U, V \subset X$ which are open in X, there exists an integer $k \geq 1$ such that $F^k(U) \cap V \neq \varnothing$. This property, as we shall see in section 4, guarantees the presence of an orbit "that passes as close as we like to any state of the system."

III. Some common definitions of chaos

In this section we present some definitions of chaos that can be found in the current literature and are accessible to undergraduates.

1. Li–Yorke chaos Let I be an interval and $f: I \to I$ be a continuous function. Assume that f has a periodic orbit of period 3. In a well-known paper Li and Yorke **[5]** proved that

(i) f has periodic orbits of every period;
(ii) there is an uncountable set $S \subset I$ such that $O(x)$ is aperiodic and unstable for every $x \in S$.

Maps of this type have been called *chaotic in the Li–Yorke sense*, without specifying if the chaotic behavior should be considered in the entire interval I or simply in the closure of S.

One of the clear advantages of this definition is that it can be easily verified, by means of graphical techniques, whether a continuous map has a periodic orbit of period 3. Moreover, property (ii) addresses, at least in part, the question of unpredictability of the system, since the orbits starting at points of S are unstable. The following simple example shows that the assumption of continuity is critical in the Li–Yorke approach.

Example 3.1. Let $f : [0,1] \to [0,1]$ be defined by

$$f(x) = \begin{cases} x + .5 & 0 \le x \le .5 \\ 0 & .5 < x \le 1. \end{cases}$$

Notice that f is discontinuous at $x = 0.5$. Every orbit of f in $[0,1]$ is eventually periodic of period 3. For example, for $x_0 = 0.2$ we have $x_1 = 0.7$, $x_2 = 0$, $x_3 = 0.5$, $x_4 = 1$, $x_5 = 0, \ldots$.

We can also find examples of maps for which the set S is negligible, in the sense that for every $r > 0$, S can be covered with a countable family of intervals of total length not exceeding r. Consequently, the probability that an orbit $O(x_0)$ is not asymptotically periodic is zero, and the chaotic behavior is not experimentally observable. The following example illustrates the situation.

Example 3.2. Let

$$f(x) = \begin{cases} 0 & 0 \le x < .25 \\ 4x - 1 & .25 \le x < .5 \\ -4x + 3 & .5 \le x < .75 \\ 0 & .75 \le x \le 1. \end{cases}$$

It can be easily verified that $O(23/65)$ is a periodic orbit of period 3 and $f^2(x) \to 0$ whenever $x < 1/3$ or $x > 2/3$. Moreover, $f^2(x) = 0$ if $x \in \mathrm{I}_1 = [5/12, 7/12]$, whose length is $1/6$. The inverse image of this interval is made of those points x such that $f^3(x) = 0$ and is the union of the two intervals $I_{21} = [17/48, 19/48]$ and $I_{22} = [29/48, 31/48]$. The total length of the two intervals is $1/12$. The inverse image of $I_{21} \cup I_{22}$ is the union of four intervals $I_{31} = [65/192, 67/192]$, $I_{32} = [77/192, 79/192]$, $I_{33} = [113/192, 115/192]$, $I_{34} = [125/192, 127/192]$. Their total length is $1/24$. Every point x of these four intervals has the property $f^4(x) = 0$. Proceeding in this way we find a family of disjoint intervals contained in the interval $[1/3, 2/3]$ and whose total length is $1/6 + 1/12 + 1/24 + \cdots = 1/6(1 + 1/2 + 1/4 + 1/8 + \cdots) = 1/3$. Every point x that belongs to one of these intervals satisfies $f^n(x) = 0$ for some $n \ge 1$. Hence the set of points S_0 whose orbit does not go to zero is negligible. Since $S \subset S_0$ we see that the orbit of a point x selected at random in $[0,1]$ converges to 0.

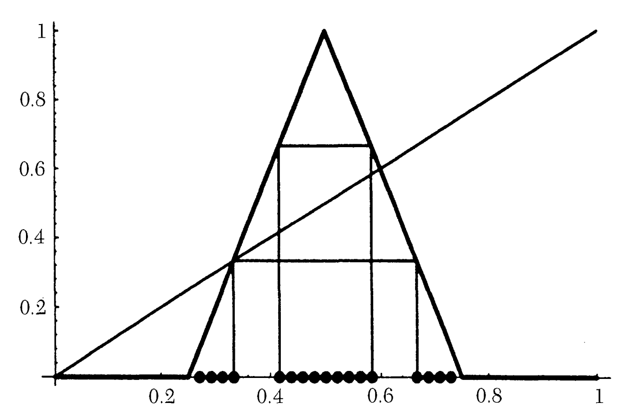


FIGURE 3.1
Shown are the points x such that $f^n(x) = 0$ for $n = 1, 2$.

The result of Li–Yorke does not hold in dimension higher than one. For example, a rotation in $\mathbb{R}^2$ of 120° around the origin has a periodic orbit of period three (all non-stationary orbits are periodic of period 3), but fails to satisfy both (i) and (ii). The orbits of such a system have neither of the two properties we indicated (see Example 1.1) as relevant to chaotic behavior. Table 3.1 compares the definition of chaos according to Li–Yorke to the other definitions listed below.

TABLE 3.1 Comparison among different definitions of chaos

Definition	map	domain	requirements	advantages	weak points
Li–Yorke	continuous	bounded interval	periodic orbit of period 3	easy to check	can be used only in $\mathbb{R}$
Experimentalists'	continuous	$X \subset \mathbb{R}^q$ bounded, closed, invariant	sensitivity on initial conditions	easy to check	defines as chaotic systems which are not
Devaney	continuous	$X \subset \mathbb{R}^q$ bounded, closed, invariant	sensitivity, transitivity, dense periodic orbits	goes to the roots of chaotic behavior	redundancy
Wiggins	continuous	$X \subset \mathbb{R}^q$ bounded, closed, invariant	sensitivity, transitivity	goes to the roots of chaotic behavior	admits degenerate chaos
Martelli	continuous	$X \subset \mathbb{R}^q$ bounded, closed, invariant	dense orbit in X which is unstable	"equivalence" with Wiggins, easy to check numerically	none of the above

2. Experimentalists' definition of chaos (sensitive dependence on initial conditions) According to many non-mathematicians, particularly physical scientists, a dynamical system $x_{n+1} = F(x_n)$ is chaotic in an invariant set X if F has in X sensitive dependence on initial conditions. Therefore, we may obtain very different orbits from two almost identical starting points (see Example 1.1). It follows that the evolution of the system is unpredictable, since it is practically impossible to know the initial conditions exactly (mainly due to unavoidable measurement errors). This is obviously an important feature of the experimentalists' definition of chaos. An additional merit is that sensitive dependence on initial conditions can be checked numerically. However, despite the advantages, this definition of chaos is not satisfactory. The following example illustrates some of the problems which may arise.

Example 3.3. Let $D = \{x \in \mathbb{R}^2 : \|x\| \leq 2\}$. Using polar coordinates define F: $D \to D$ by

$$F(x) = F(\rho, \theta) = (\rho, \theta + \rho). \tag{3.1}$$

Notice that for every $\rho \in (0, 2]$ the set $C_\rho = \{x \in \mathbb{R}^2 : \|x\| = \rho\}$ is invariant and the dynamical system defined by F is a rotation in C_ρ. Consequently, it does not seem appropriate to label the system as chaotic in the invariant set C_ρ. However, the system has in C_ρ sensitive dependence on initial conditions with $r_0 = \rho$. In fact, let $x_0 = (\rho_0, \theta_0)$ and $d > 0$. Choose n so large that $\frac{\pi}{n} < d$ and $\rho_0 - \frac{2\pi}{n} > 0$. Let $y_0 =$

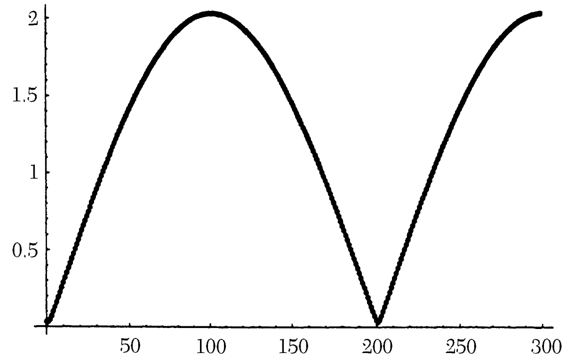


FIGURE 3.2
Plot of $(n, \|x_n - y_n\|)$, with $x_0 = (1,0)$ and $y_0 = (1 - 0.01\pi, 0)$. We see that the distance can be as large as the diameter of the smaller circle.

$(\rho_0 - \frac{\pi}{n}, \theta_0)$. Then $\|x_0 - y_0\| < d$ and

$$x_n = (\rho_0, \theta_0 + n\rho_0), \quad y_n = \left(\rho_0 - \tfrac{\pi}{n}, \theta + n\rho_0 - \pi\right). \tag{3.2}$$

Consequently $\|x_n - y_n\| > r_0$ and the system is chaotic in C_ρ for every $\rho \in (0,2]$. However, the system is non-chaotic in the disk D. We do not seem to have a satisfactory situation (see Table 3.1).

3. Wiggins' definition of chaos According to Wiggins **[8]** a map F is chaotic in an invariant set X provided that

(i) F is topologically transitive in X;
(ii) F has in X sensitive dependence on initial conditions.

We shall see in section 4 that topological transitivity implies the existence of an orbit "passing as close as we like to any state" of the system in X. Therefore the definition of Wiggins embodies both properties mentioned in Example 1.1 as fundamental to chaotic behavior. However, Wiggins' approach presents some problems. For example, the map $F(\rho, \theta)$ of Example 3.3 is chaotic in the sense of Wiggins in every circle C_ρ such that ρ/π is irrational. In fact, F has sensitive dependence on initial conditions in C_ρ. Moreover, the orbit $O(x_0)$, $x_0 = (\rho, 0)$ visits every arc of C_ρ, no matter how small. Hence F is topologically transitive in C_ρ. Notice that F is non-chaotic in any annulus $R[a,b] = \{x \in D\colon a \le \|x\| \le b, 0 \le a < b < 2\}$ since F fails to be topologically transitive. An additional problem with Wiggins' definition arises from the so-called "degenerate chaos" (see **[1]**), which is chaotic behavior in a finite set of points. In fact, according to Wiggins a dynamical system can be chaotic in a singleton $X = \{x_0\}$. For example the system governed by the function

$$f(x) = -2|x| + 1 \tag{3.3}$$

is chaotic in the set $X = \{1/3\}$. FIGURE 3.3 illustrates that orbits starting close to $1/3$ move away from the equilibrium point (see Table 3.1 for a summary).

4. Martelli's definition of chaos According to Martelli **[6]**, F is chaotic in an invariant set X provided that there exists $x_0 \in X$ such that

(i) $L(x_0) = X$;
(ii) $O(x_0)$ is unstable with respect to X.

Since $F(L(x_0)) = L(x_0)$ (see Equation 2.5) we obtain that $F(X) = X$, i.e., F is onto.

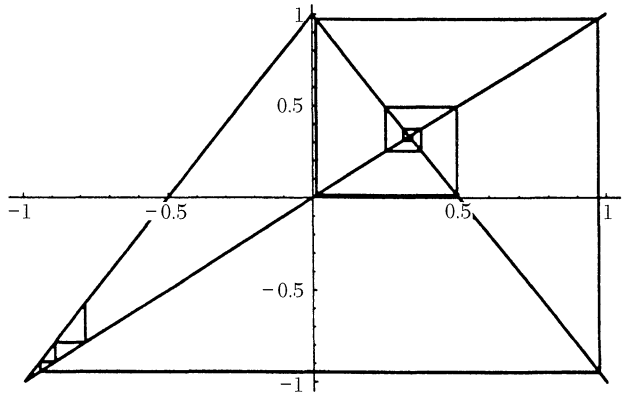


FIGURE 3.3
The orbits of points close to 1/3 more away from the equilibrium point.

The map $F(\rho, \theta)$ of Example 3.3 is non-chaotic in the sense of Martelli in any circle C_ρ or in any annulus $R[a, b]$. In a circle C_ρ the map fails to satisfy (ii), and in an annulus $R[a, b]$ fails to satisfy (i). Moreover, according to Martelli, no map can be chaotic on a finite set, since instability of $O(x_0)$ with respect to X implies that X is infinite.

5. Devaney's definition of chaos A map F is chaotic in the sense of Devaney **[3]** in an invariant set X if

(i) F is topologically transitive in X;
(ii) F has in X sensitive dependence on initial conditions;
(iii) the set P of periodic orbits of F is dense in X.

Devaney adds the density of P in X to the two conditions required by Wiggins, thus bringing back, at least to some extent, a feature of Li–Yorke chaos. Moreover, as Crannell **[2]** points out, the "requirement that periodic orbits be dense appeals to those who look for patterns within a seemingly random system."

It has been shown **[1]** that conditions (i) and (iii) imply (ii). In this sense, Devaney's definition of chaos is redundant. Moreover, as the following example shows, there are systems that seem to deserve the label "chaotic" and do not satisfy the third requirement of Devaney's definition (see Table 3.1 for a summary).

Example 3.4. Let F be given in polar coordinates by $F(\rho, \theta) = (4\rho(1-\rho), \theta + 1)$ and let $D(0, 1)$ be the invariant disk centered at the origin, with radius 1. The origin is the only fixed point for F, and F does not have any periodic orbit of period $p > 1$. In fact, F stretches or shrinks the distance of every point of $D(0, 1)$ from the origin, while rotating the point by an angle of 1 radian. Since $1/\pi$ is irrational, no point $x_n \in O(x_0)$ can come back to the same ray which contains x_0. At the end of this paper we will show that the dynamical system governed by F in $D(0, 1)$ is "unpredictable" and has orbits that pass as close as we like to every point of $D(0, 1)$. Thus this system has exactly the two fundamental properties of chaotic behavior mentioned in Example 1.1.

IV. Defining Chaos

Recall that, according to Wiggins **[8]**, F is chaotic in an invariant set X if

(i) F is topologically transitive in X;
(ii) F has in X sensitive dependence on initial conditions.

According to Martelli [**6**], F is chaotic in X provided that there exists $x_0 \in X$ such that

(i) $L(x_0) = X$;

(ii) $O(x_0)$ is unstable with respect to X.

These two definitions can be considered equivalent. In fact, (see Theorem 4.1) F is topologically transitive in X if and only if there exists $x_0 \in X$ such that $L(x_0) = X$. In addition, F has in X sensitive dependence on initial conditions *with respect to* X if and only if $O(x_0)$ is unstable *with respect to* X (see Theorem 4.2).

There remains an important difference between the two approaches. Wiggins does not require sensitivity *with respect to* X, while Martelli requires instability *with respect to* X. Theorems 4.1 and 4.2 contain the theoretical results that establish the practical equivalence between these two definitions of chaos. For both theorems we provide a brief sketch of the proof, leaving details to the reader.

THEOREM 4.1. *Let $X \subset \mathbb{R}^q$ be closed and bounded and $F: X \to X$ be continuous. Then F is topologically transitive in X if and only if there exists $x_0 \in X$ such that $L(x_0) = X$.*

Proof. The "if" part is easy. The presence of an orbit $O(x_0)$ such that $L(x_0) = X$ clearly implies topological transitivity.

The "only if" part is a bit more difficult. The basic idea is that given any positive integer m we can cover X with finitely many balls of radius $1/m$ and find a point x_m whose orbit visits each ball of the covering. Moreover, the choice of x_m can be made so that the sequence $\{x_m,\ m = 1, 2, \dots\}$ converges. Let x_0 be its limit. It is easy to verify that $L(x_0) = X$.

THEOREM 4.2. *Let $x_0 \in X$ be such that $L(x_0) = X$. Then F has in X sensitive dependence on initial conditions with respect to X if and only if $O(x_0)$ is unstable with respect to X.*

Proof. This time the "only if" part is immediate. In fact, sensitivity to initial conditions with respect to X clearly implies that $O(x_0)$ is unstable with respect to X.

The "if" part is a bit longer. Given $y_0 \in X$ and $d > 0$, determine an iterate x_n of x_0 such that $\|x_n - y_0\| \leq d/2$. This can be done since $L(x_0) = X$. Next, one shows that for every $n > 1$ the orbit $O(x_n)$ has the same instability constant of $O(x_0)$, i.e., $r(x_n) = r(x_0)$. It follows that either some iterate y_p of y_0 is at least as far as $r(x_0)/3$ from x_{n+p}, or this separation happens for some iterate z_p of a point z_0 which is closer than d to both y_0 and x_n. In either case, we obtain that $r(y_0) \geq r(x_0/3)$.

A second look at Example 3.4. With Theorem 4.1 and 4.2 we can establish that the dynamical system of Example 3.4 is chaotic in $D(0,1)$ according to Wiggins and Martelli. We use the fact, well-established in the literature, that the map $f(x) = 4x(1-x)$ of Example 1.1 not only is topologically transitive in $[0,1]$ but has the additional property that given any interval $[a,b] \subset [0,1]$, $a < b$, there is an integer p such that $f^p[a,b] = [0,1]$. Consequently, after finitely many iterations, the F-image of a small open disk in $D(0,1)$ will contain an open set $U \subset D(0,1)$ with a full radius. The rotation of 1 radian spreads U entirely over $D(0,1)$ in finitely many additional iterations. Hence F is topologically transitive in $D(0,1)$. From Theorem 4.1 there is $x_0 \in D(0,1)$ such that $L(x_0) = D(0,1)$. Consequently, using once more the statement from Example 1.1, the orbit passes as close as we like to any point of $D(0,1)$. It is also well known that the map f has sensitive dependence on initial conditions in $[0,1]$. Hence, $O(x_0)$ is unstable in $D(0,1)$ and F is chaotic in $D(0,1)$ according to Wiggins and Martelli. In FIGURE 4.1 we plot $\|x_n - y_n\|$ versus the iteration number n, with $x_0 = (.3, 0)$ and $y_0 = (.300001, 0)$. (The reader should compare the graph with Fig.

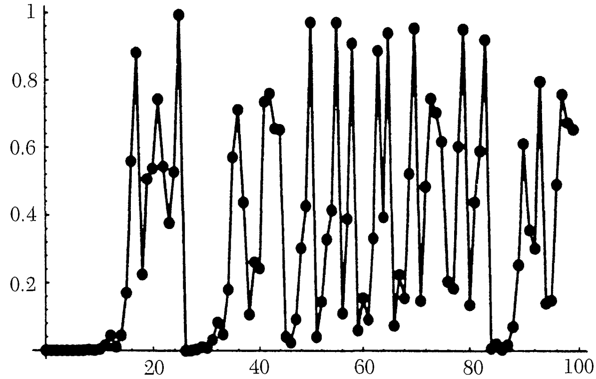


FIGURE 4.1
Plot of $(n, \|x_n - y_n\|)$. The behavior of the distances repeats the situation of Example 1.1.

1.2.) The map F is non-chaotic in $D(0,1)$ according to Devaney. This example seems to suggest that the density of periodic orbits may not be necessary in defining chaos.

V. Conclusion

The definitions of chaos of Wiggins and Martelli, together with the one of Devaney and with the experimentalists' definition, can be applied to a certain class of maps with "admissible" discontinuities. The class is denoted by QC, which stands for "quasi-continuous." It can be shown (the result will appear in a forthcoming paper by A. Crannell and M. Martelli), that the definitions of Wiggins and Martelli remain equivalent in QC. In the following example we present the so-called baker's transformation, which defines a well-known chaotic system in [0, 1], and which belongs to QC.

Example 5.1. Let $B(x) = 2x - [2x]$, where $[2x]$ denotes the greatest integer less than or equal to $2x$. Notice that B maps $[0,1]$ into itself and it is discontinuous at $x = .5$ and $x = 1$. The action of B and its iterates on the elements of $[0,1]$ is better understood if we write them with their binary expansion. Then, for $x \in [0, 0.5)$ we have $x = 0.0a_2a_3\dots$, while for $x \in [0.5, 1)$ we have $x = 0.1a_2a_3\dots$ where a_i, $i = 2, 3, \dots,$ are either 0 or 1. In both cases we obtain $B(x) = 0.a_2a_3\dots$. Now we can easily see that the orbit of $x_0 = 0.\ 0\ 1\ 00\ 01\ 10\ 11\ 000\ 001\ 010\ 100\ \dots$ has the property $L(x_0) = [0,1]$. Moreover, $O(x_0)$ is unstable, since $B'(x) = 2$ for $x \neq 0, 1$.

Hence B is chaotic in $[0,1]$ according to Martelli's definition (applied to QC). Under the action of B the length of every interval $[a,b] \subset [0,1]$, $a < b$ is doubled until, after finitely many iterations, we have $B^k[a,b] = [0,1]$. Thus B is topologically transitive in $[0,1]$. Sensitivity is ensured by $B'(x) = 2$ for $x \neq 0.5$, 1. Hence, B is chaotic in $[0,1]$ according to Wiggins and to the experimentalists' definition (applied to QC). It can be shown that the periodic orbits of B are dense in $[0,1]$. Thus B is chaotic in $[0,1]$ according to the definition of Devaney (applied to QC). B has a periodic orbit of period 3 in $[0,1]$, but the Li–Yorke definition of chaos cannot be applied to B, since we have seen that continuity is critical in the Li–Yorke case.

We close this survey with a remark regarding the possibility of numerically investigating the chaotic behavior of a map. We feel that Martelli's definition is possibly most suitable for this purpose. The property $L(x_0) = X$ can be tested by covering the set X with small boxes (segments in $\mathbb{R}$, squares in $\mathbb{R}^2$, cubes in $\mathbb{R}^3\ldots$) and by verifying that the orbit "visits" all of them. The instability of the orbit can be tested with the method we used in Example 1.2 and in our second look at Example 3.4. As mentioned in the introduction, chaotic behavior is of great interest to many disciplines. Proving it theoretically, however, is never an easy task, if at all possible. Numerical tests are frequently the only ones available in practical applications and we feel that the simpler they are, the greater their reliability will be.

Acknowledgment. We are much indebted to the referees for their useful comments and particularly for the suggestion to incorporate the comparison table.

REFERENCES

1. J. Banks, J. Brooks, G. Cairns, G. Davis, P. Stacey, On Devaney's definition of chaos, *Amer. Math. Monthly* 99, (1992), 332–334.
2. A. Crannell, The role of transitivity in Devaney's definition of chaos, *Amer. Math. Monthly* 102 (1995), 788–793.
3. R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd Edition, Addison-Wesley, Redwood City, CA, 1989.
4. J. Ford, What is chaos, that we should be mindful of it? in *The New Physics*, ed. P. Davies, Cambridge University Press (1989), 348–371.
5. T. Y. Li and J. A. Yorke, Period three implies chaos, *Amer. Math. Monthly* 82 (1975), 985–992.
6. M. Martelli: *An Introduction to Discrete Dynamical Systems and Chaos*, Gordon and Breach, to appear Fall 1998.
7. M. A. Stone, Chaos, prediction and Laplacean determinism, *American Philosophical Quarterly*, 26, 2 (1989), 123–132.
8. S. Wiggins, *Chaotic Transport in Dynamical Systems*, Springer-Verlag, New York, NY, 1991.

A Lambda Slaughter

Mary had a little lamb-
Da curled and curved for show.
And everywhere that lambda went,
The math came out just so.

It followed her to calculus
With multiplier rules,
Which show the way to meet constraints
As in Lagrange's school.

In matrix class it proved itself
To be a trusty pal, whose
Assistance could be counted on
For writing eigenvalues.

So keep an eye on Mary's friend—
Its uses transcend measure.
Beyond a doubt her lambda is
A character to treasure.

—Dan Kalman
American University
Washington, DC 20016

covering the set X with small boxes (segments in $\mathbb{R}$, squares in $\mathbb{R}^2$, cubes in $\mathbb{R}^3 \ldots$) and by verifying that the orbit "visits" all of them. The instability of the orbit can be tested with the method we used in Example 1.2 and in our second look at Example 3.4. As mentioned in the introduction, chaotic behavior is of great interest to many disciplines. Proving it theoretically, however, is never an easy task, if at all possible. Numerical tests are frequently the only ones available in practical applications and we feel that the simpler they are, the greater their reliability will be.

Acknowledgment. We are much indebted to the referees for their useful comments and particularly for the suggestion to incorporate the comparison table.

REFERENCES

1. J. Banks, J. Brooks, G. Cairns, G. Davis, P. Stacey, On Devaney's definition of chaos, *Amer. Math. Monthly* 99, (1992), 332–334.
2. A. Crannell, The role of transitivity in Devaney's definition of chaos, *Amer. Math. Monthly* 102 (1995), 788–793.
3. R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd Edition, Addison-Wesley, Redwood City, CA, 1989.
4. J. Ford, What is chaos, that we should be mindful of it? in *The New Physics*, ed. P. Davies, Cambridge University Press (1989), 348–371.
5. T. Y. Li and J. A. Yorke, Period three implies chaos, *Amer. Math. Monthly* 82 (1975), 985–992.
6. M. Martelli: *An Introduction to Discrete Dynamical Systems and Chaos*, Gordon and Breach, to appear Fall 1998.
7. M. A. Stone, Chaos, prediction and Laplacean determinism, *American Philosophical Quarterly*, 26, 2 (1989), 123–132.
8. S. Wiggins, *Chaotic Transport in Dynamical Systems*, Springer-Verlag, New York, NY, 1991.

A Lambda Slaughter

Mary had a little lamb-
Da curled and curved for show.
And everywhere that lambda went,
The math came out just so.

It followed her to calculus
With multiplier rules,
Which show the way to meet constraints
As in Lagrange's school.

In matrix class it proved itself
To be a trusty pal, whose
Assistance could be counted on
For writing eigenvalues.

So keep an eye on Mary's friend—
Its uses transcend measure.
Beyond a doubt her lambda is
A character to treasure.

—Dan Kalman
American University
Washington, DC 20016

NOTES

Archimedes' *Quadrature of the Parabola* Revisited

GORDON SWAIN
THOMAS DENCE
Ashland University
Ashland, OH 44805

Introduction In a letter (later titled *Quadrature of the Parabola*) to his friend Dositheus, Archimedes wrote, "...it is shown here that every segment bounded by a straight line and a section of a right-angled cone [a parabola] is four-thirds of the triangle with the same base and equal height with the segment ..." [**3**, p. 233]. Thus the area of a segment of a parabola cut by a chord can be determined from the area of a certain inscribed triangle (FIGURE 1). In this note we will extend the result of Archimedes to a formula for the area of a parabolic segment from the area of *any* inscribed triangle having the chord as one side. We will also give an algebraic (coordinatized) proof of the result, which has the additional bonus of showing that the area of the segment can be expressed as a geometric series. Finally, we will address the question of whether geometric series appear in calculating the areas of segments of other curves.

Archimedes' result In *Quadrature of the Parabola*, Archimedes presents two proofs of his result. In the first the segment is divided into wedges with a common vertex at one end of the chord, and the formula is found through center of mass

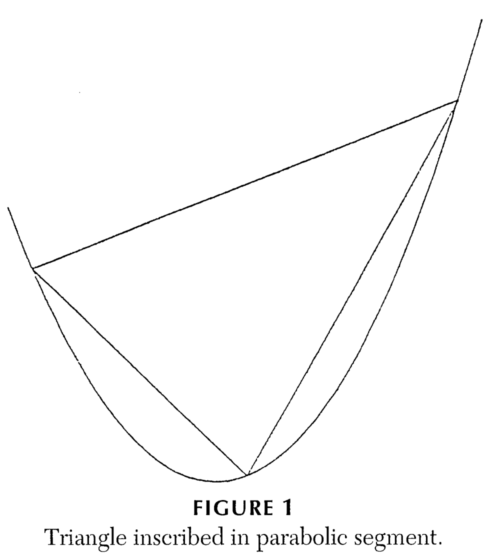


FIGURE 1
Triangle inscribed in parabolic segment.

arguments and increasing the number of wedges (see [**1**, p. 336–342][1]. The second, which is of interest here, is purely geometric (see [**1**, p. 243–245][2]. The proof we present here, while using somewhat modern notation, gives the flavor of his original work. For example, AB refers both to the line segment and its length, and $\triangle ABC$ is both the triangle and its area.

THEOREM 1. (*Archimedes*) *The area of a segment of a parabola is four-thirds the area of the triangle which has the chord as one side and as the opposite vertex the point on the parabola in the direction parallel to the axis from the midpoint of the chord.*

In FIGURE 2, let M be the midpoint of the chord AB, and MC be parallel to the axis of the parabola. A property of parabolas in general is that, if DE is parallel to AM, then

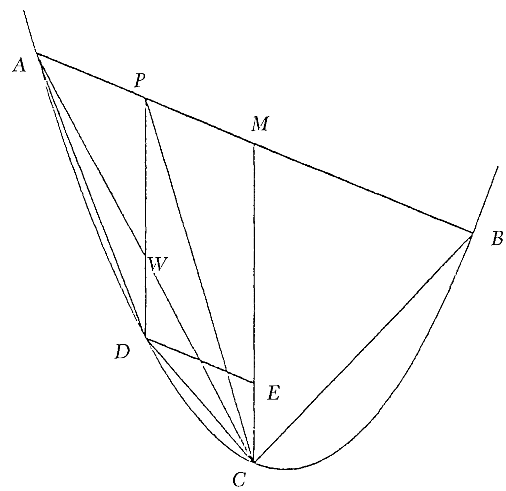


FIGURE 2
Segment formed by chord AB.

$$\frac{AM^2}{DE^2} = \frac{MC}{EC}.$$

Archimedes refers the reader to the classic works on conics by Euclid and Aristaeus for a derivation of this property [**3**, p. 235]. We note that AB and MC need not be perpendicular.

Now, in FIGURE 2, suppose further that P is the midpoint of AM, and PD is parallel to the axis of the parabola.

$$\frac{MC}{EC} = \frac{AM^2}{DE^2} = \frac{(2\cdot DE)^2}{DE^2},$$

so $MC = 4\cdot EC$ and $ME = 3\cdot EC$. Thus $MC = \frac{4}{3}\cdot ME = \frac{4}{3}\cdot PD$.

[1] The Arab mathematician Thābit ibn Qurra (836–901 AD, Harrān and Baghdad, [**2**]) gave a proof which, while similar to Archimedes', divided the segment into slices parallel to the chord, giving a Riemann integral style derivation of the area (see [**4**]).

[2] Thābit's grandson Ibrāhīm ibn Sinān (908–946 AD, Baghdad, [**2**]) provided a proof which was also geometric in nature, but depended on the invariance of ratios of areas of plane figures under affine transformations (see [**4**]).

By similarity of triangles, $MC = 2 \cdot PW$. Thus $PW = \frac{2}{3} \cdot PD$ and $PW = 2 \cdot WD$. Then $\triangle ACP = 2 \cdot \triangle ADC$, $\triangle ACM = 4 \cdot \triangle ADC$, and $\triangle ACB = 8 \cdot \triangle ADC$. The triangle similarly inscribed in the segment determined by the chord CB also has an eighth of the area $\triangle ACB$. In each of the four remaining parabolic segments we can inscribe a triangle that has again an eighth of the area of the larger triangle with which it shares a side. This process can be continued indefinitely, and in the limit fills the segment.

At this point Archimedes applied an indirect limiting process to approximate the area of the original segment, showing that it can be neither greater than nor less than $\frac{4}{3} \cdot \triangle ACB$. We arrive at the same conclusion by noting that the area of the segment is the sum of the infinite sequence of the areas of all the inscribed triangles. Namely,

$$\sum_{n=0}^{\infty} 2^n \cdot \frac{1}{8^n} \cdot \triangle ACB = \triangle ACB \cdot \sum_{n=0}^{\infty} \frac{1}{4^n} = \frac{4}{3} \cdot \triangle ACB.$$

Example. To gain a little more insight into the process described in the proof above, consider the segment of the parabola $y = x^2$ cut by the chord from $(-3, 9)$ to $(5, 25)$. We first inscribe a triangle such that the vertex opposite the chord lies at $(1, 1)$, directly below the midpoint, $(1, 17)$, of the chord (FIGURE 3). The area of this triangle will be $\frac{1}{2} \cdot (5 - (-3)) \cdot (17 - 1) = 64$, thus, by Theorem 1, the area of the segment should be $\frac{4}{3} \cdot 64 = \frac{256}{3}$. We could show this using a simple integration, but let us continue inscribing triangles instead. We next inscribe triangles in the two parabolic regions that remain, again with the opposite vertex below the midpoint of the chord which defines each segment. The area of each of these is $\frac{1}{2} \cdot 4 \cdot 4 = 8$. At the next stage, each of the four triangles will have area 1. We continue inscribing triangles (2^{n-1} triangles at the n^{th} stage) to fill the parabolic segment, yielding a total area of

$$64 + 2 \cdot 8 + 4 \cdot 1 + 8 \cdot .25 + \cdots = 64\left(1 + \frac{1}{4} + \left(\frac{1}{4}\right)^2 + \left(\frac{1}{4}\right)^3 + \cdots\right) = 64 \cdot \frac{1}{1 - \frac{1}{4}} = \frac{256}{3}$$

as we had expected.

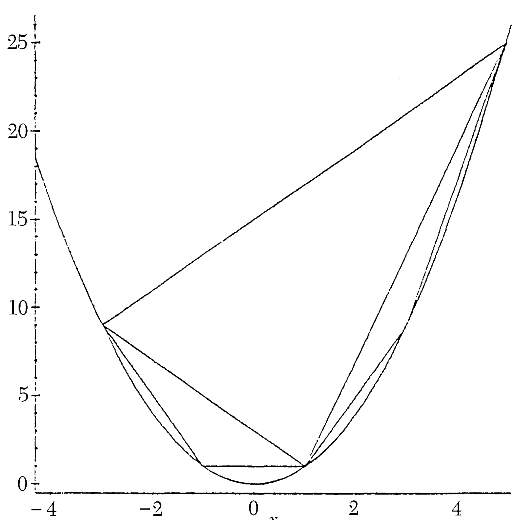


FIGURE 3
Sequence of inscribed triangles.

A generalization What happens if we take the parabolic segment in the example above, but inscribe a triangle which has the opposite vertex at a different point on the parabola? Archimedes' formula does not apply but perhaps something similar occurs.

Example. Let us start with a triangle where the vertex is at $(-1,1)$, directly below the point $(-1,13)$ on the chord (FIGURE 4). We note that the point $(-1,13)$ divides the chord into two parts according to the proportion $\frac{1}{4}:\frac{3}{4}$. The area of this triangle will be $\frac{1}{2}\cdot(5-(-3))\cdot(13-1)=48$. We inscribe triangles in the remaining two segments, again choosing the vertex to lie below the point on the corresponding chord that divides it in the same proportions as before. Thus the new vertices are $(-2.5, 6.25)$ and $(.5, .25)$ respectively. The areas of these triangles will be $\frac{3}{4}$ and $\frac{81}{4}$ respectively. The areas of the four triangles at the next stage are $\frac{3}{256}$, $\frac{81}{256}$, $\frac{81}{256}$, and $\frac{2187}{256}$ respectively, left to right. Continuing to inscribe triangles, the area of the original segment will be

$$\text{Area} = 48 + \left(\frac{3}{4}+\frac{81}{4}\right) + \left(\frac{3}{256}+\frac{81}{256}+\frac{81}{256}+\frac{2187}{256}\right) + \cdots$$

$$= 48 + 21 + \frac{147}{16} + \cdots = 48\left(1 + \frac{7}{16} + \left(\frac{7}{16}\right)^2 + \cdots\right).$$

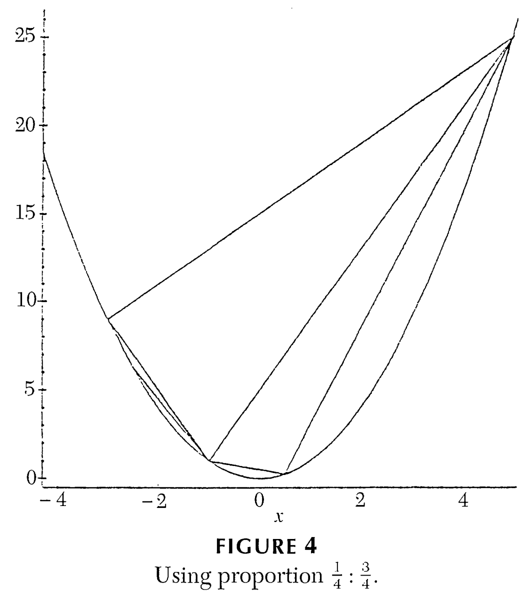


FIGURE 4
Using proportion $\frac{1}{4}:\frac{3}{4}$.

If we assume the series is geometric, then the sum is

$$48\cdot\frac{1}{1-\frac{7}{16}} = 48\cdot\frac{16}{9} = \frac{256}{3}$$

as before. We will see later that this is indeed a geometric series. The above example motivates a generalization of Theorem 1.

THEOREM 2. *If in a parabolic segment a triangle is inscribed which has the chord as one side and the opposite vertex below the point on the chord which divides it according to the proportion* $r{:}1-r$, *then the area of the parabolic segment is* $\frac{1}{3r-3r^2}$ *times the area of the inscribed triangle.*

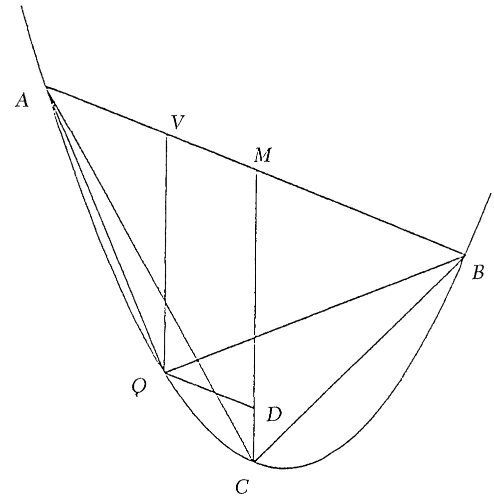


FIGURE 5
General case.

In FIGURE 5, let V be the point which divides the chord AB according to the proportion $r{:}1-r$, and Q the point on the parabola directly below. We assume $r<\frac{1}{2}$; the proof is similar for $r>\frac{1}{2}$ while Theorem 1 is when $r=\frac{1}{2}$. Let M be the midpoint of AB, MC parallel to VQ and the axis of the parabola, and QD parallel to AB. Then, by the property of parabolas, $MC/DC = AM^2/QD^2 = AM^2/VM^2$ or $DC/MC = VM^2/AM^2$. By assumption, $r = AV/AB = AV/2\cdot AM$. So $2r = AV/AM$ and $1-2r = VM/AM$. Thus $DC/MC = (1-2r)^2$ and $MD/MC = 1-(1-2r)^2 = 4r-4r^2$. Now

$$\frac{\triangle AQB}{\triangle ACB} = \frac{VQ}{MC} = \frac{MD}{MC} = 4r - 4r^2.$$

Using Theorem 1, the area of the segment is

$$\frac{4}{3}\cdot\triangle ACB = \frac{4}{3}\cdot\frac{1}{4r-4r^2}\cdot\triangle AQB = \frac{1}{3r-3r^2}\cdot\triangle AQB.$$

Theorem 2 gives us a formula for the area of the segment in terms of the area of any inscribed triangle which has the chord as a side.

An algebraic proof The following is a coordinatized version of Theorem 2. Though the mathematics is not as clean as in Theorems 1 and 2, we have the surprise of seeing the appearance of geometric series descriptions for the area of the parabolic segment. By the *width* of a segment we mean the difference between the x-coordinates of the endpoints of the chord which determines the segment.

THEOREM 3. *Let $f(x) = Ax^2 + Bx + C$ be any quadratic function, $w>0$ and $0<r<1$ any real numbers. Then the area of a parabolic segment of f with width w is $A_1(1+R+R^2+R^3+\cdots)$ where $A_1 = \frac{|A|}{2}r(1-r)w^3$ and $R = 3r^2-3r+1$.*

Let $a<b$ be any real numbers and let $c = a + r(b-a)$ be the number between them determined by the proportion $r{:}1-r$. We calculate the area of the triangle T (see FIGURE 6) using the difference of the areas of the trapezoids below the sides of the

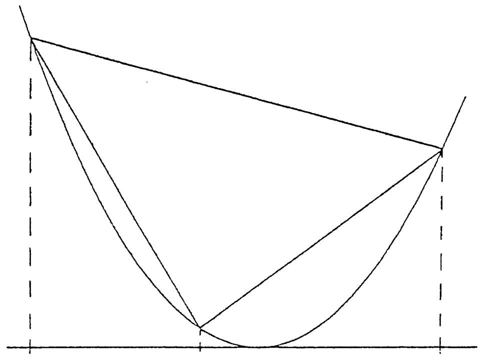


FIGURE 6
Triangle and trapezoids.

triangle:

$$T=\left|\frac{f(a)+f(b)}{2}(b-a)-\frac{f(a)+f(c)}{2}(c-a)-\frac{f(c)+f(b)}{2}(b-c)\right|$$
$$=\left|\frac{f(a)+f(b)}{2}(b-a)-\frac{f(a)+f(c)}{2}r(b-a)-\frac{f(c)+f(b)}{2}(1-r)(b-a)\right|$$
$$=\left|\frac{1}{2}(b-a)[(1-r)f(a)+rf(b)-f(c)]\right|.$$

Substituting for f and simplifying,

$$T=\left|\frac{A}{2}r(1-r)(b-a)^3\right|=\frac{|A|}{2}r(1-r)(b-a)^3. \qquad (1)$$

In the two remaining segments we inscribe triangles with total area, using equation (1),

$$T'=\frac{|A|}{2}r(1-r)(c-a)^3+\frac{|A|}{2}r(1-r)(b-c)^3$$
$$=\frac{|A|}{2}r(1-r)[r(b-a)]^3+\frac{|A|}{2}r(1-r)[(1-r)(b-a)]^3$$
$$=\frac{|A|}{2}r(1-r)(b-a)^3(3r^2-3r+1).$$

If we define $R=3r^2-3r+1$, then $T'=T\cdot R$. Writing $A_1=\frac{|A|}{2}r(1-r)w^3$ for the area of the first triangle inscribed in the original parabolic segment of width w and A_n for the total area of the triangles added at the n stage, then clearly $A_{n+1}=A_n\cdot R$. Adding up the areas of all the triangles gives us the area of the parabolic segment as the geometric series

$$\text{Area}=A_1+A_2+A_3+A_4+\cdots = A_1(1+R+R^2+R^3+\cdots)$$

as stated in the theorem.

We name the formula $R=3r^2-3r+1$ the *Cummins function* in honor of Professor Emeritus Kenneth Cummins of Kent State University, whose presentation of the first example above at an Ohio Section MAA meeting inspired the authors' further interest in this problem.

TABLE 1 Values of A_{i+1}/A_i for $f(x)=x^3$

i	$r=$	.1	.25	.5	.6
1		.7955	.5130	.25	.2475
2		.7840	.4847	.25	.2596
3		.7752	.4687	.25	.2678
5		.7627	.4524	.25	.2760
10		.7462	.4403	.25	.2798
15		.7387	.4381	.25	.2800
	$R=$	.7300	.4375	.25	.2800

COROLLARY 1. *The area of any parabolic segment is* $\frac{T}{1-R}$.

Since any value of r in $(0,1)$ will yield a value of R in $[.25,1)$, the geometric series in Theorem 3 will converge to the value given. With $R=3r^2-3r+1$, this is the same result as Theorem 2.

In the proof of Theorem 3, equation (1) does not depend on the intersection points of the chord with the parabola, but only on the width of the segment. This observation leads to the following property:

COROLLARY 2. *For a given parabola, any two segments of the same width will have the same area.*

We note that Archimedes was aware of this property, though in stating it, he characterized the segments by their height at the midpoint of the chord [**1**, p. 79].

Other curves The curious reader might wonder if the methods used in this note apply to finding areas of segments of other plane curves. The area of any convex segment could be estimated by inscribing many triangles, but this would be practical only if we encountered series whose sums we knew (ideally, geometric series). Sadly, this method does not yield geometric series in general. It seems that this phenomenon is unique to quadratic functions. For the segment of the cubic $f(x)=x^3$ over the interval $[1,4]$, Table 1 gives values of the ratio A_{i+1}/A_i (using notation from the proof of Theorem 3) for various values of r, along with the values of the Cummins function. The exact values when $r=.5$ is an exceptional case, though it does occur for any cubic over any interval (the proof is similar to that of Theorem 3). It appears that for other values of r the ratios converge to the value of the Cummins function as i increases. Data for higher degree polynomials also appear to exhibit this trend.

We sketch an argument for why this convergence occurs. Consider a convex segment of the graph of a polynomial $f(x)$ of degree n. Suppose we are at the i stage of inscribing triangles into the segment, and focus on one of the triangles, say one that falls over the interval $[a,b]$. Expanding f as a Taylor series about a, and using the notation of Section 4, the area of this triangle is

$$T=\frac{1}{2}r(1-r)(b-a)^3\frac{f''(a)}{2}+\frac{1}{2}(b-a)^4\sum_{k=3}^{n}\frac{f^{(k)}(a)}{k!}(r-r^k)(b-a)^{k-3}$$

The area of the two triangles that are inscribed adjacent to it at the $i+1$ stage is

$$T'=\frac{1}{2}r(1-r)(3r^2-3r+1)(b-a)^3\frac{f''(a)}{2}$$
$$+\frac{1}{2}(b-a)^4\sum_{k=3}^{n}\frac{f^{(k)}(a)}{k!}g_k(r)(b-a)^{k-3}$$

where $g_k(r)$ are polynomial functions of r only. The ratio of these areas is

$$\frac{T'}{T}=\frac{f''(a)r(1-r)(3r^2-3r+1)+(b-a)M}{f''(a)r(1-r)+(b-a)N}$$

where M and N are bounded terms (involving derivatives of f, polynomials in r, and powers of $(b-a)$). As long as f'' is not zero anywhere on the segment, we can see that the ratio converges to $R=3r^2-3r+1$ as $b-a$ goes to zero. As we go from stage to stage, the width of the triangles does go to zero at least as fast as a geometric series with ratio $\max\{r,1-r\}$. The same will be true when we look at the ratio A_{n+1}/A_n of the total areas at each stage. The curious reader may want to show that convergence will also occur in classes of functions other than polynomials.

Acknowledgment. The authors would like to thank Glen Van Brummelen for the idea of using Taylor series that made the convergence argument possible, and for many other helpful comments on this paper.

REFERENCES

1. E. J. Dijksterhuis, *Archimedes*, Princeton Univ. Pr., Princeton, NJ, 1987.
2. C. C. Gillispie, editor, *Dictionary of Scientific Biography*, Scribners, New York, NY, 1970.
3. T. L. Heath, editor, *The Works of Archimedes*, Dover, New York, NY, 1912.
4. R. Rashed, *Les mathématiques infinitésmales du IX^e au XI^e siècle, vol* 1, Al-Furqān Islamic Foundation, London, UK, 1996.

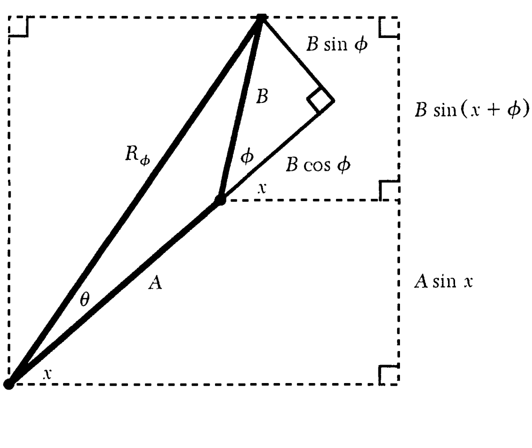
Proof Without Words: Adding Like Sines

$$R_\phi=\sqrt{A^2+B^2+2\;AB\cos\phi}\qquad \tan\theta=\frac{B\sin\phi}{A+B\cos\phi}$$

$$A\sin x+B\sin(x+\phi)=R_\phi\sin(x+\theta)$$

$$\phi=\pi/2\Rightarrow\tan\theta=\frac{B}{A}$$

$$A\sin x+B\cos x=\sqrt{A^2+B^2}\,\sin(x+\theta)$$



—Rick Mabry
Paul Deiermann
Louisiana State University
Shreveport, LA 71115

where $g_k(r)$ are polynomial functions of r only. The ratio of these areas is

$$\frac{T'}{T} = \frac{f''(a)r(1-r)(3r^2-3r+1)+(b-a)M}{f''(a)r(1-r)+(b-a)N}$$

where M and N are bounded terms (involving derivatives of f, polynomials in r, and powers of $(b-a)$). As long as f'' is not zero anywhere on the segment, we can see that the ratio converges to $R = 3r^2 - 3r + 1$ as $b-a$ goes to zero. As we go from stage to stage, the width of the triangles does go to zero at least as fast as a geometric series with ratio $\max\{r, 1-r\}$. The same will be true when we look at the ratio A_{n+1}/A_n of the total areas at each stage. The curious reader may want to show that convergence will also occur in classes of functions other than polynomials.

Acknowledgment. The authors would like to thank Glen Van Brummelen for the idea of using Taylor series that made the convergence argument possible, and for many other helpful comments on this paper.

REFERENCES

1. E. J. Dijksterhuis, *Archimedes*, Princeton Univ. Pr., Princeton, NJ, 1987.
2. C. C. Gillispie, editor, *Dictionary of Scientific Biography*, Scribners, New York, NY, 1970.
3. T. L. Heath, editor, *The Works of Archimedes*, Dover, New York, NY, 1912.
4. R. Rashed, *Les mathématiques infinitésmales du IX^e au XI^e siècle*, *vol* 1, Al-Furqān Islamic Foundation, London, UK, 1996.

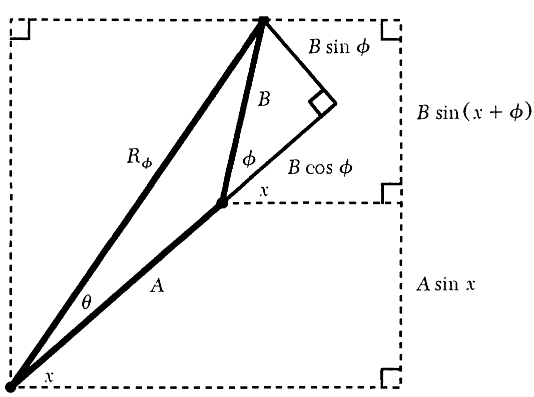
Proof Without Words: Adding Like Sines

$$R_\phi = \sqrt{A^2 + B^2 + 2\ AB\cos\phi} \qquad \tan\theta = \frac{B\sin\phi}{A + B\cos\phi}$$

$$A\sin x + B\sin(x+\phi) = R_\phi \sin(x+\theta)$$

$$\phi = \pi/2 \Rightarrow \tan\theta = \frac{B}{A}$$

$$A\sin x + B\cos x = \sqrt{A^2+B^2}\sin(x+\theta)$$



—Rick Mabry
Paul Deiermann
Louisiana State University
Shreveport, LA 71115

Perfectly Odd Cubes

STEVEN KAHAN
Queens College
Flushing, NY 11367-1597

A *perfect number* is one that is equal to the sum of its proper divisors, with 6 and 28 being the two smallest examples. More than two thousand years ago, Euclid stated and proved, as Proposition 36 of Book IX of the *Elements*:

If $M_p = 2^p - 1$ is prime, then $E_p = 2^{p-1}(2^p - 1)$ is perfect.

Primes of the form M_p are known as *Mersenne primes*, to honor the French priest who conjectured their primality in 1644. Mersenne primes occur only when p itself is prime, although not every prime p leads to a Mersenne prime. At present, there are 36 known Mersenne primes; the largest, discovered in August 1997, has 895,932 digits.

In the eighteenth century, the prolific Swiss mathematician Leonhard Euler proved that every even perfect number *must* be generated by a Mersenne prime, as described in Euclid's Proposition 36. The following result describes a somewhat surprising characteristic of all even perfect numbers greater than 6:

THEOREM. *Let p be an odd prime that generates the even perfect number $E_p = 2^{p-1}(2^p - 1)$. Then E_p is expressible as the sum of the cubes of the first n consecutive odd integers, where $n = 2^{(p-1)/2}$.*

For example, if $p = 7$, then $E_7 = 8128$, and we can write $8128 = 1^3 + 3^3 + 5^3 + 7^3 + 9^3 + 11^3 + 13^3 + 15^3$. More remarkable is the fact that the largest perfect number now known, which has 1,791,864 digits, is the sum of the cubes of the first $2^{1488110}$ consecutive odd integers. (Skeptical readers are invited to verify this audacious claim.)

Proof. Standard summation formulas verify that

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

With $n = 2^{(p-1)/2}$, the right-hand side of this equation becomes

$$\left(2^{(p-1)/2}\right)^2\left(2\left(2^{(p-1)/2}\right)^2 - 1\right) = 2^{p-1}\left(2(2^{p-1}) - 1\right) = 2^{p-1}(2^p - 1)$$

or E_p, as claimed.

The Square Root of Two is Irrational: Proof by Poem

Double a square is never a square, and here is the reason why:
If m-squared were equal to two n-squared, then to their prime factors we'd fly.
But the decomposition that lies on the left has all of its exponents even,
But the power of two on the right must be odd: so one of the twos is "bereaven."

—MAURICE MACHOVER
ST. JOHN'S UNIVERSITY
JAMAICA, NY 11439

Small Denominators: No Small Problem

SCOTT J. BESLIN
DOUGLAS J. BANEY
VALERIO DE ANGELIS
Nicholls State University
Thibodaux, LA 70310

I. Introduction This article is primarily concerned with the following problem.

(*P*) Let a and b be real numbers in the unit interval, with $a < b$. Define $F(a,b)$ to be the reduced fraction with smallest denominator in the open interval (a,b). Find a formula or algorithm for computing $F(a,b)$.

It is always assumed that when either a or b is a fraction, it is in reduced form. The special case $a = \frac{19}{94}$ and $b = \frac{17}{76}$ appeared as a problem in **[2]**. As often happens in mathematics, the simplicity with which the problem is stated belies the complexity of solving it.

We will observe interesting connections among the solution of (P), Farey sequences, and continued fractions. Many of these connections lead to good classroom problems in elementary number theory and computer science. Diligent readers will uncover some unanswered problems of their own.

Is $F(a,b)$ a function? The *existence* of a minimal denominator is ensured by the Well-Ordering Property of the natural numbers. We establish *uniqueness* of $F(a,b)$ in the following proposition.

PROPOSITION 1. *Suppose n is the minimal denominator occurring in the interval (a,b), and suppose $\frac{m}{n}$ is in (a,b). Then $\frac{m}{n}$ is the only such fraction.*

Proof. Suppose the conclusion fails. Then, without loss of generality, $\frac{m+1}{n}$ is also in (a,b). Now $(m+1) < n$ so that $-(m+1) > -n$ and hence $-(m+1)+(m+1)n > -n+(m+1)n$, or $(m+1)(n-1) > nm$. Thus $\frac{m+1}{n} > \frac{m}{n-1}$. So $\frac{m+1}{n} > \frac{m}{n-1} > \frac{m}{n}$, and $\frac{m}{n-1}$ is in (a,b), which contradicts the minimality of n. □

(There is of course no fraction with *maximum* denominator in (a,b).)

We observe by inspection that

$$F(0,1) = \frac{1}{2},\ F\left(0,\frac{1}{2}\right) = \frac{1}{3},\ F\left(0,\frac{1}{3}\right) = \frac{1}{4},\ldots,\ F\left(0,\frac{1}{n}\right) = \frac{1}{n+1}.$$

These examples are special cases of the following more general result. The notation $\lfloor y \rfloor$ denotes the greatest integer less than or equal to y.

PROPOSITION 2. *If* $0 < b \le 1$, *then*

$$F(0,b) = \frac{1}{\left\lfloor \frac{1}{b} \right\rfloor + 1}$$

For example,

$$F(0,0.2191) = \frac{1}{\left\lfloor \frac{1}{0.2191} \right\rfloor + 1} = \frac{1}{5} \quad \text{and} \quad F\left(0, \frac{1}{\pi}\right) = \frac{1}{\lfloor \pi \rfloor + 1} = \frac{1}{4}$$

Proposition 2 can be proved directly. We will obtain it as a corollary to a more general theorem at the end of this article.

One method of computing $F(a, b)$ is through an exhaustive search, which "tries" $\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}$, etc., until $F(a, b)$ is found. Such an algorithm becomes computationally impractical as the denominator of $F(a, b)$ gets larger.

II. Farey sequences and continued fractions Many sources, including **[1]** and **[3]**, treat Farey sequences and continued fractions. We summarize the main results below.

Farey Sequences. The *Farey sequence of order n*, F_n, is the list of reduced fractions in the interval [0, 1], arranged in ascending order, whose denominators are less than or equal to n. For example, the Farey sequence of order 4 is

$$F_4 = \tfrac{0}{1}, \tfrac{1}{4}, \tfrac{1}{3}, \tfrac{1}{2}, \tfrac{2}{3}, \tfrac{3}{4}, \tfrac{1}{1}.$$

Reduced fractions $\frac{a}{b}$ and $\frac{c}{d}$ in the unit interval, with $\frac{a}{b} < \frac{c}{d}$, are *adjacent Farey fractions* if they occur in consecutive order in some Farey sequence. The interval $\left[\frac{a}{b}, \frac{c}{d}\right]$ is then called a *Farey interval.*

For example, $\frac{1}{2}$ and $\frac{1}{3}$ are adjacent Farey fractions in F_3, and $\left[\frac{1}{3}, \frac{1}{2}\right]$ is a Farey interval—even though they are no longer adjacent in F_5.

It can be shown (usually by induction) that $\frac{a}{b}$ and $\frac{c}{d}$ are adjacent if and only if $|ad - bc| = 1$; that is, if the matrix $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ is a unimodular transformation on $\mathbb{R}^2$. The *mediant* of a Farey pair $\frac{a}{b} < \frac{c}{d}$ is defined to be the fraction $\frac{a+c}{b+d}$. We write $\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$ to indicate Farey addition as opposed to ordinary real-number addition. The following statements about the mediant of a Farey pair are true. Items (1), (2), (3) are routine exercises; item (4) requires some effort.

(1) The mediant is in reduced form;

(2) $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$;

(3) $\left[\frac{a}{b}, \frac{a+c}{b+d}\right]$ and $\left[\frac{a+c}{b+d}, \frac{c}{d}\right]$ are Farey intervals;

(4) Among all fractions $\frac{x}{y}$ with $\frac{a}{b} < \frac{x}{y} < \frac{c}{d}$, the mediant is the unique one with smallest denominator.

These facts yield a recursive procedure for generating F_{n+1} from F_n: insert the mediant into F_{n+1} if its denominator is less than or equal to $n + 1$. For example, F_5 is obtained from F_4 as follows.

(i) The first Farey pair in F_4 is $\frac{0}{1}, \frac{1}{4}$. Farey add: $\frac{0}{1} \oplus \frac{1}{4} = \frac{1}{5}$. Because $\frac{1}{5}$ has denominator ≤ 5, $\frac{1}{5}$ is in F_5.

(ii) The next Farey pair is $\frac{1}{4}, \frac{1}{3}$. Farey add: $\frac{1}{4} \oplus \frac{1}{3} = \frac{2}{7}$. Because $\frac{2}{7}$ has denominator > 5, $\frac{2}{7}$ is not in F_5.

(iii) Repeat this procedure for each successive pair in F_4 to obtain F_5:

$$F_5 = \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}.$$

(In [**5**], the author discusses the sequences derived by including *all* mediants in the generating process, and obtains what he calls *modified Farey sequences*.)

Statement (4) above is a partial answer to problem (P). For example, the fact that $\det\begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} = -1$, implies that $\frac{2}{5}$ and $\frac{3}{7}$ are a Farey pair. Hence $F(\frac{2}{5}, \frac{3}{7}) = \frac{2}{5} \oplus \frac{3}{7} = \frac{5}{12}$.

Two questions remain:

1. What if the endpoints of the interval are not a Farey pair?
2. What if either endpoint is irrational?

One computational solution to both questions is to use a "Farey process" to trap the given interval between two adjacent Farey fractions. The recursion resembles the bisection method; it proceeds as follows. Given $0 \le a < b \le 1$:

(i) Start with $\frac{0}{1}, \frac{1}{1}$.
(ii) Farey add to obtain the mediant.
(iii) If the mediant is in the interval, then $F(a, b) =$ mediant; otherwise, repeat (ii) and (iii) for a new Farey pair which includes the mediant.

Example. Find $F\left(\frac{\sqrt{2}}{2}, \frac{71}{100}\right)$. The following sequence of Farey additions yields the result.

$$\frac{0}{1} \oplus \frac{1}{1} = \frac{1}{2} < \frac{\sqrt{2}}{2} \qquad \frac{1}{2} \oplus \frac{1}{1} = \frac{2}{3} < \frac{\sqrt{2}}{2}$$

$$\frac{2}{3} \oplus \frac{1}{1} = \frac{3}{4} > \frac{71}{100} \qquad \frac{2}{3} \oplus \frac{3}{4} = \frac{5}{7} > \frac{71}{100}$$

$$\frac{2}{3} \oplus \frac{5}{7} = \frac{7}{10} < \frac{\sqrt{2}}{2} \qquad \frac{7}{10} \oplus \frac{5}{7} = \frac{12}{17} < \frac{\sqrt{2}}{2}$$

Since $\frac{12}{17} \oplus \frac{5}{7} = \frac{17}{24} \in \left(\frac{\sqrt{2}}{2}, \frac{71}{100}\right)$, we have $F\left(\frac{\sqrt{2}}{2}, \frac{71}{100}\right) = \frac{17}{24}$.

It is plausible, but not entirely obvious, that the process described above must terminate. See [**4**] for details.

In Section III we will give a method for obtaining the last, "critical" Farey interval —$(\frac{12}{17}, \frac{5}{7})$ in the above example—without using the recursive Farey process.

Continued Fractions. (See [**1**], [**3**], and [**4**] for further details on continued fractions.)

A *simple continued fraction* $[a_0, a_1, a_2, \dots]$ is an expression of the form

$$a_0 \frac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots}}},$$

where a_0 is an integer and a_i is a positive integer for $i > 0$. If the expression terminates, the continued fraction is said to be *finite* and represents a rational number. Otherwise, the continued fraction is *infinite*, and converges to an irrational number.

The successive rational numbers $[a_0] = a_0$, $[a_0, a_1] = a_0 + \frac{1}{a_1}$, $[a_0, a_1, a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$, etc., are called the *convergents* to (or of) the continued fraction. We denote the convergent $[a_0, a_1, \dots, a_n]$ by $\frac{p_n}{q_n}$.

Every rational number can be expressed as a continued fraction in two ways, for $[a_0, a_1, \dots, a_{m-1}, a_m] = [a_0, a_1, a_2, \dots, a_{m-1}, a_m - 1, 1]$ if $a_m > 1$. For example,

$$\frac{11}{4} = 2 + \cfrac{1}{1 + \cfrac{1}{3}} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}}.$$

Observe that $0 \le [a_0, a_1, a_2, \dots, a_n] < 1$ if and only if $a_0 = 0$.

The successive convergents $\frac{p_k}{q_k}$ can be generated recursively by the following scheme:

$$p_0 = a_0;\ q_0 = 1;$$
$$p_1 = a_1 a_0 + 1;\ q_1 = a_1.$$

For $k \ge 2$, $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$.

If we begin with a real number r_0, its continued fraction expansion may be obtained by the following scheme.

(i) Let $a_0 = \lfloor r_0 \rfloor$.

(ii) Let $r_1 = \frac{1}{r_0 - a_0}$ and set $a_1 = \lfloor r_1 \rfloor$.

(iii) Repeat inductively, so that $a_k = \lfloor r_k \rfloor$ and $r_{k+1} = \frac{1}{r_k - a_k}$.

(iv) If r_0 is rational, then r_k is an integer for some k, and the process terminates.

Example. Let $r_0 = \frac{4}{11}$. Then

$$a_0 = \left\lfloor \frac{4}{11} \right\rfloor = 0;\ r_1 = \frac{1}{\frac{4}{11} - 0} = \frac{11}{4};$$

$$a_1 = \left\lfloor \frac{11}{4} \right\rfloor = 2;\ r_2 = \frac{1}{\frac{11}{4} - 2} = \frac{4}{3};$$

$$a_2 = \left\lfloor \frac{4}{3} \right\rfloor = 1;\ r_3 = \frac{1}{\frac{4}{3} - 1} = 3;$$

$$a_3 = \lfloor 3 \rfloor = 3.$$

Hence $\frac{4}{11} = [0, 2, 1, 3]$, and the convergents to $\frac{4}{11}$ are $[0] = 0$; $[0, 2] = \frac{1}{2}$; $[0, 2, 1] = \frac{1}{3}$; and $\frac{4}{11}$.

We will use the following two standard theorems (see **[3]**).

THEOREM 1. $[a_0, a_1, \dots, a_n] < [a_0, a_1, \dots, a_n, a_{n+1}]$ *if and only if* n *is even.*

THEOREM 2. *The convergents* $c_k = \frac{p_k}{q_k}$ *to* r_0 *satisfy* $c_0 < c_2 < c_4 < \cdots \le r_0 \le \cdots < c_5 < c_3 < c_1$. *In other words,* $\{c_{2k}\}$ *is increasing,* $\{c_{2k+1}\}$ *is decreasing, and* $c_{2k} < c_{2j+1}$ *for all* j, k.

Theorem 2 implies the well-known result that when r_0 is irrational, its convergents form two monotone sequences of rational numbers, each converging to r_0.

The following two theorems link Farey fractions with continued fractions.

THEOREM 3. (*See, for example,* **[1]** *and* **[2]**.) *Two successive convergents* $[a_0, a_1, \dots, a_{n-1}]$ *and* $[a_0, a_1, \dots, a_{n-1}, a_n]$ *are adjacent Farey fractions.*

Proof. $[a_0, a_1, \dots, a_n] = \frac{p_n}{q_n}$, where $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$. Thus $D(n) = \begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = p_n q_{n-1} - p_{n-1} q_n = (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) = p_{n-2} q_{n-1} - p_{n-1} q_{n-2} = -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = -D(n-1)$. Since $D(1) = \begin{vmatrix} a_1 a_0 + 1 & a_0 \\ a_1 & 1 \end{vmatrix} = +1$, an inductive argument shows that $D(n) = +1$ if n is odd and $D(n) = -1$ if n is even. □

The following result is now readily proved. Details are left to the reader.

THEOREM 4. *The mediant of two successive convergents* $[a_0, a_1, \dots, a_{n-1}]$ *and* $[a_0, a_1, \dots, a_{n-1}, a_n]$ *is* $[a_0, a_1, \dots, a_{n-1}, a_n, 1]$.

The proof follows from the identity

$$\frac{p_n + p_{n-1}}{q_n + q_{n-1}} = \frac{(1 + a_n) p_{n-1} + p_{n-2}}{(1 + a_n) q_{n-1} + q_{n-2}}.$$

III. Solution to problem (P) We begin by establishing a result about continued fractions.

PROPOSITION 3. *If n is even, $[a_0, a_1, \dots, a_{n-1}, a_n] < [a_0, a_1, \dots, a_{n-1}, b_n]$ if and only if $a_n < b_n$; if n is odd, $[a_0, a_1, \dots, a_{n-1}, a_n] < [a_0, a_1, \dots, a_{n-1}, b_n]$ if and only if $a_n > b_n$.*

The proposition (and Theorem 1 as well) may be proved inductively by observing the following: Consider the expression $a_0 + \frac{1}{a_1}$. Increasing the denominator, either by adding $\frac{1}{a_2}$ to a_1 or by replacing a_1 with a larger integer b_1, makes the last term smaller, and hence the original expression smaller. Thus $[a_0, a_1] > [a_0, a_1, a_2]$ and $[a_0, a_1] > [a_0, b_1]$ if $a_1 < b_1$. Likewise,

$$[a_0, a_1, a_2] = a_0 + \frac{1}{[a_1, a_2]} < a_0 + \frac{1}{[a_1, a_2, a_3]} = [a_0, a_1, a_2, a_3] \quad \text{and}$$

$$[a_0, a_1, a_2] = a_0 + \frac{1}{[a_1, a_2]} < a_0 + \frac{1}{[a_1, b_2]} = [a_0, a_1, b_2] \text{ if } a_2 < b_2. \qquad \square$$

We are now ready to state our main result.

Let $0 \le a < b \le 1$. Suppose the continued fraction convergents of a and b are listed up to the terms where they first differ. Suppose the convergents of a first differ from the convergents of b at the kth entry. If k is even, let f_1 be the last listed convergent of a, and let f_2 be the next-to-last convergent to a. If k is odd, let f_2 be the last listed convergent of b, and let f_1 be the next-to-last listed convergent of b. Recall from Theorem 2 that $f_1 < a$ and $b < f_2$. Theorem 3 ensures that f_1 and f_2 are adjacent Farey fractions. Thus the interval (a, b) is "trapped" by the Farey interval (f_1, f_2).

THEOREM 5. *$F(a, b)$ is the mediant $f_1 \oplus f_2$ of f_1 and f_2 if $f_1 \oplus f_2$ is not equal to a or b. Otherwise, an additional Farey addition is needed to obtain $F(a, b)$.*

Proof. The proof uses Theorem 1, Theorem 2, Theorem 4, and Proposition 3. For example, suppose the lists of convergents first differ at entry $n + 1$, an even number. Then $f_2 = [a_0, a_1, \dots, a_n]$ and $f_1 = [a_0, a_1, \dots, a_n, s]$, where f_1 is a common convergent to the endpoints a and b, and f_2 is a convergent to a. Suppose the convergent to b following f_2 is $[a_0, a_1, \ldots, a_n, k]$. By Theorem 2, $f_1 < f_2$, so that $s < k$ from Theorem 1. Now $f_1 \oplus f_2 = [a_0, a_1, \ldots, a_n, s, 1]$ from Theorem 4. Observe that $f_1 \oplus f_2$ can also be written $[a_0, a_1, \ldots, a_n, s+1]$. Using Theorem 2 again we obtain

$$b > [a_0, a_1, \ldots, a_n, k] \geq [a_0, a_1, \ldots, a_n, s+1] = f_1 \oplus f_2.$$

Let $[a_0, a_1, \ldots a_n, s, d]$ be the convergent to a following f_1. Since n is odd and $d \geq 1$, Proposition 3 implies that

$$a \leq [a_0, a_1, \ldots, a_n, s, d] \leq [a_0, a_1, \ldots, a_, s, 1] = f_1 \oplus f_2.$$

Thus $a \leq f_1 \oplus f_2 \leq b$. Now $f_1 \oplus f_2$ is in the closed interval $[a, b]$; moreover, $[a, b] \subseteq (f_1, f_2)$, and $F(f_1, f_2) = f_1 \oplus f_2$, so $F(a, b) = f_1 \oplus f_2$ unless $f_1 \oplus f_2 = a$ or b. In this case, at least one more Farey addition is necessary. (If this happens, at least one of a and b must be rational.) □

Example. Let $a = 0.56 = \frac{14}{25}$ and $b = 0.62 = \frac{31}{50}$. Find $F(a, b)$.

(i) Write the continued fraction convergents of a and b up to the point where they first differ.

Level 0	a: $[0] = 0$	b: $[0] = 0$
1	$[0, 1] = 1$	$[0, 1] = 1$
2	$[0, 1, 1] = \frac{1}{2}$	$[0, 1, 1] = \frac{1}{2}$
3	$[0, 1, 1, 3] = \frac{4}{7}$	$[0, 1, 1, 1] = \frac{2}{3}$

(ii) The convergents first differ on level 3, so $f_1 = \frac{1}{2}$ and $f_2 = \frac{2}{3}$.
(iii) Compute $f_1 \oplus f_2$: $\frac{1}{2} \oplus \frac{2}{3} = \frac{3}{5}$.
(iv) Since $f_1 \oplus f_2$ is not an endpoint, $F(a, b) = f_1 \oplus f_2$.
We conclude that $F(0.56, 0.62) = \frac{3}{5}$.

Example. $a = \frac{1}{4}$; $b = \frac{5}{17}$. Find $F(a, b)$.

Level 0	a: $[0] = \frac{0}{1}$	b: $[0] = \frac{0}{1}$
1	$[0, 4] = \frac{1}{4}$	$[0, 3] = \frac{1}{3}$

Thus $f_1 = \frac{0}{1}$, $f_2 = \frac{1}{3}$, and $f_1 \oplus f_2 = \frac{1}{4} = a$. So another Farey addition gives $\frac{1}{4} \oplus \frac{1}{3} = \frac{2}{7} = F(a, b)$.

COROLLARY 1. [*See Proposition* 2, *Section I.*] *If* $0 < b \leq 1$, *then* $F(0, b) = \dfrac{1}{\left\lfloor \frac{1}{b} \right\rfloor + 1}$.

Proof. $0 = [0]$ and $b = \left[0, \left\lfloor \frac{1}{b} \right\rfloor, \ldots\right]$ so $f_1 = \frac{0}{1}$ and $f_2 = \left[0, \left\lfloor \frac{1}{b} \right\rfloor\right] = \dfrac{1}{\left\lfloor \frac{1}{b} \right\rfloor}$. The conclusion follows after Farey adding. □

We observe that if a and b are reduced fractions and $F(a, b) = a \oplus b$, then a and b need not be adjacent Farey fractions. The example $a = \frac{14}{25}$ and $b = \frac{31}{50}$ computed above shows that $F(a, b) = \frac{3}{5} = \frac{14}{25} \oplus \frac{31}{50}$, but $\begin{vmatrix} 14 & 31 \\ 25 & 50 \end{vmatrix} = -75$.

The reader is now invited to solve the case at the beginning of this article: What is $F(\frac{19}{94}, \frac{17}{76})$?

Acknowledgment The authors would like to thank Todd Morales (graduate student) for his help with the computer programming in this project. The authors also acknowledge the referee for helpful comments. Research funded by N.S.U. Research Council.

REFERENCES

1. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th Ed., Oxford University Press, Oxford, UK, 1993.
2. *Math Horizons*, Mathematical Association of America, Winter 1993, Problem 5, p. 34.
3. I. Niven and H. S. Zuckerman, *In Introduction to the Theory of Numbers*, 4th Ed., John Wiley & Sons, New York, NY, 1980.
4. I. Richards, Continued fractions without tears, this MAGAZINE 54 (1981), pp. 163–171.
5. M. Shrader-Frechette, Modified Farey sequences and continued fractions, this MAGAZINE 54 (1981), pp. 60–63.

Math Bite: On $n^{1/n} > (n+1)^{1/(n+1)}$, $n \geq 3$

Let $a_n = n^{1/n}$, $n = 1, 2, \ldots$. The familiar fact

$$I_n:\ a_n > a_{n+1},\ n \geq 3$$

is usually proved by proving more (see, e.g., **[1]**):

$$(1 + 1/n)^n < 3.$$

But I_n is immediate from the inequality

$$J_n:\ b_n = \left(\frac{a_n}{a_{n+1}}\right)^{n(n+1)} > \left(\frac{a_{n-1}}{a_n}\right)^{n(n-1)} = b_{n-1},\ n \geq 2,$$

which simply asserts that

$$n^2 = a_n^{2n} > a_{n+1}^{n+1} a_{n-1}^{n-1} = n^2 - 1.$$

That $b_n > 1$ ($n \geq 3$), as required, follows from J_n and

$$b_2 < 1 < b_3,$$

which, thanks to $a_4 = a_2$, is implicit in J_3: $0 < b_2 < b_3 (= b_2^{-2})$.

REFERENCE

1. G. H. Hardy, *A Course of Pure Mathematics*, 10th Ed., Cambridge, Cambridge, UK 1952, pp. 141–143.

—T. S. NANJUNDIAH
"PRASHANTHI"
180, I CROSS
GANGOTRI LAYOUT-I STAGE
MYSORE-570 009
INDIA

Acknowledgment The authors would like to thank Todd Morales (graduate student) for his help with the computer programming in this project. The authors also acknowledge the referee for helpful comments. Research funded by N.S.U. Research Council.

REFERENCES

1. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th Ed., Oxford University Press, Oxford, UK, 1993.
2. *Math Horizons*, Mathematical Association of America, Winter 1993, Problem 5, p. 34.
3. I. Niven and H. S. Zuckerman, *In Introduction to the Theory of Numbers*, 4th Ed., John Wiley & Sons, New York, NY, 1980.
4. I. Richards, Continued fractions without tears, this MAGAZINE 54 (1981), pp. 163–171.
5. M. Shrader-Frechette, Modified Farey sequences and continued fractions, this MAGAZINE 54 (1981), pp. 60–63.

Math Bite: On $n^{1/n} > (n+1)^{1/(n+1)}$, $n \geq 3$

Let $a_n = n^{1/n}$, $n = 1, 2, \ldots$. The familiar fact

$$I_n:\ a_n > a_{n+1},\ n \geq 3$$

is usually proved by proving more (see, e.g., **[1]**):

$$(1 + 1/n)^n < 3.$$

But I_n is immediate from the inequality

$$J_n:\ b_n = \left(\frac{a_n}{a_{n+1}}\right)^{n(n+1)} > \left(\frac{a_{n-1}}{a_n}\right)^{n(n-1)} = b_{n-1},\ n \geq 2,$$

which simply asserts that

$$n^2 = a_n^{2n} > a_{n+1}^{n+1} a_{n-1}^{n-1} = n^2 - 1.$$

That $b_n > 1$ $(n \geq 3)$, as required, follows from J_n and

$$b_2 < 1 < b_3,$$

which, thanks to $a_4 = a_2$, is implicit in J_3: $0 < b_2 < b_3 (= b_2^{-2})$.

REFERENCE

1. G. H. Hardy, *A Course of Pure Mathematics*, 10th Ed., Cambridge, Cambridge, UK 1952, pp. 141–143.

—T. S. NANJUNDIAH
"PRASHANTHI"
180, I CROSS
GANGOTRI LAYOUT-I STAGE
MYSORE-570 009
INDIA

The Randomness of Remainders

D. A. MORAN
B. M. STEWART[1]
Michigan State University
East Lansing, MI 48824

The Monte Carlo simulation technique, used for statistical predictions of numerical data in complex models of scientific situations, depends on a constant supply of a long stream of random numbers. Highly sophisticated computer programs have been devised to generate such a supply and (sometimes after long usage) the numbers generated by the program often prove to be not so random after all. For example, in an article in *Physics Review Letters* a few years ago (December 7, 1992), it was reported that five of the most widely-used random number generators produced errors when applied to a model of the behavior of atoms in a magnetic crystal.

Some random number generators contain a process wherein a stream of digits is added together, then divided into some large number, and the remainder used to compute further digits in the next step of the process. A little experimentation might well convince the casual observer of the unpredictability (and hence, presumably, the randomness) of this sort of calculation. For example, if 1,000,001 is divided by the integers 1234, 1235, ..., 1250, the following remainders result: 461, 886, 77, 505, 935, 128, 561, 996, 191, 629, 1069, 266, 709, 1159, 353, 801 and 1. These numbers appear to be spread quite uniformly over the interval $[0, 1250]$, even though the divisors are so regular. A few computations such as this might lead the experimenter astray.

Bad guess. A pretty good way to find k random integers in the interval $[0, n]$ might be to divide some large number by the integers $n-k,\ n-k+1,\ n-k+2, \dots, n$ and look at the remainders.

In fact this guess can be *spectacularly* bad, as illustrated in the following table, which gives the remainder when 2^{101} is divided by $2^{34}+k$:

k	Remainder	k	Remainder
1	$8{,}589{,}934{,}592 = 2^{33}$	5	8,589,934,532
2	$17{,}179{,}896{,}182 = 2^{34} - 2$		...
3	8,589,934,580	99	8,589,886,082
4	17,179,869,156	100	17,179,369,286

Indeed, the table could be carried more than a thousand entries further before the remainders lost their "look-alike" quality. Hardly a random set of numbers!

The unexpected regularity of these data is hinted at by the entries in the first two rows of the table; the dividend, divisors, and remainders are all near a power of 2. As it turns out, the number 2 is not important in this regard; any larger integer M will play the same role, if the exponents are chosen properly.

General result. Let M be an integer greater than 1. When M^{3a-b} is divided by integers in the vicinity of M^a $(a \gg b)$, the remainders in the division are grouped together in clusters near numbers whose locations are calculable in advance. The

[1]Professor Stewart died on April 15, 1994.

number of clusters is exactly the number of quadratic residues mod M^b (except in a few singular cases).

(The nonnegative number t ($t < n$) is said to be a *quadratic residue mod n* if the congruence $x^2 \equiv t$ mod n has a solution. For example $0, 1, 4, 5, 6, 9$ are the quadratic residues mod 10.) In the above example, $a = 34$, $b = 1$ and $3a - b = 101$; there are only two quadratic residues mod 2^1, so the remainders are clustered about two numbers (2^{33} and 2^{34}). If we were to examine the division of 2^{101} by integers in the vicinity of 2^{35} (so that now $a = 35$, $b = 4$), we would obtain four classes of look-alike remainders corresponding to the four distinct quadratic residues modulo 2^4 (i.e., mod 16).

The result can be derived by carefully scrutinizing the size of the remainder R that results when M^{3a-b} is divided by a number of the form $M^a + k$, where $0 < k^3 < M^a$. By long division, we find that:

$$M^{3a} = (M^a + k)(M^{2a} - kM^a + k^2) - k^3. \tag{1}$$

Now suppose that $k^2 \equiv t \pmod{M^b}$, where $0 < t < M^b$, so that t is a quadratic residue mod M^b. (We'll consider the case $t = 0$ later.) Then $k^2 - t = uM^b$ for some u, $0 < u < M^b$. Now rewrite (1) in the form

$$M^{3a} = (M^a + k)(M^{2a} - kM^a + k^2 - t) - k^3 + (M^a + k)t.$$

Multiplying each side by M^{-b} yields

$$M^{3a-b} = (M^a + k)(M^{2a-b} - kM^{a-b} + u) + R,$$

where $R = (M^a + k)tM^{-b} - k^3M^{-b}$. We wish to show that $0 < R < M^a + k$. First, $t < M^b$, so $tM^{-b} < 1$, and $R < M^a + k$. Now $k^3 < M^a$, so $k^3M^{-b} < M^{a-b}$. Since $t > 0$, i.e., $t \geq 1$, we have

$$(M^a + k)tM^{-b} > (M^a + k)M^{-b} > M^aM^b = M^{a-b}.$$

Thus

$$(M^a + k)tM^{-b} - k^3M^{-b} > M^{a-b} - M^{a-b} = 0.$$

The dominant term in the remainder R is $(M^a + k)tM^{-b}$, because $a \gg b$ and $k^3 < M^a$. If the values of k are very small compared to M^a, the clustering of the resulting remainders is very dramatic, as in the example.

If we examine the dominant term $(M^a + k)tM^{-b}$ found above, we note that different values of t (i.e., different quadratic residues mod M^b) will give different clusterings of remainders, again because $a \gg b$. The clusters will be in the vicinity of the numbers tM^{a-b}, one cluster for each quadratic residue t (mod M^b), $t > 0$.

It remains to examine what happens if $k^2 = 0 \pmod{M^b}$. In this case, $k^2 = uM^b$ for some u, $0 < u < M^b$, and we now rewrite (1) in the form

$$M^{3a} = (M^a + k)(M^{2a} - kM^a + k^2 - M^b) - k^3 + (M^a + k)M^b.$$

Now, multiplying each side by M^{-b} yields

$$M^{3a-b} = (M^a + k)\big(M^{2a-b} - kM^{a-b} + (u - 1)\big) + R,$$

where $R = (M^a + k) - k^3$.

In this case, it is clear that $R < M^a + k$ and $R > 0$ because $k^3 < M^a$, so the remainders cluster around M^a.

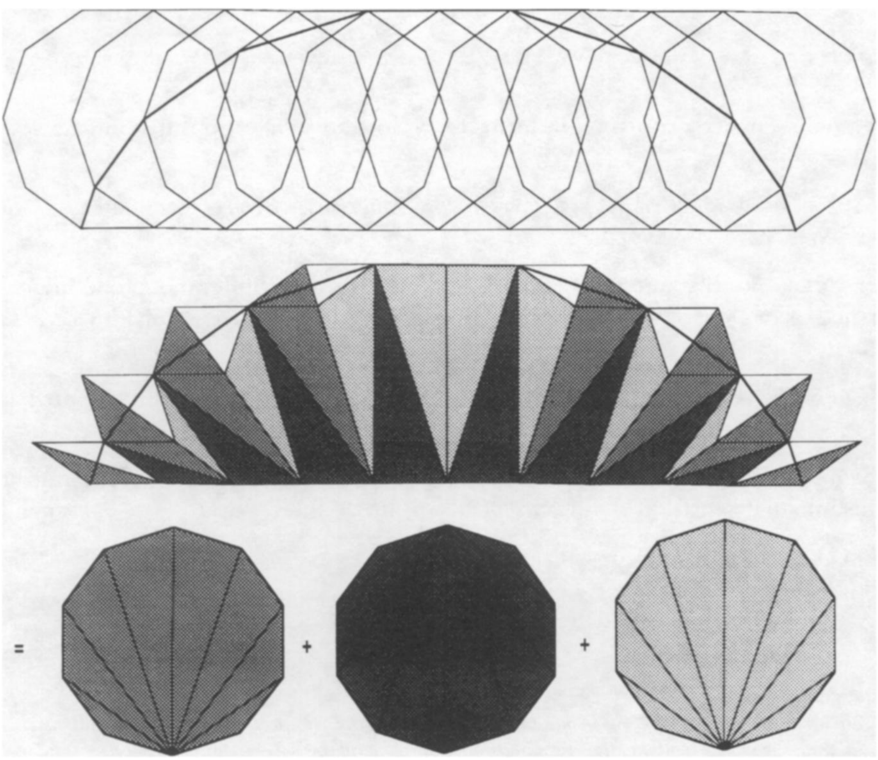
This completes the proof that the remainder R is dominated by one of the numbers M^a or tM^{a-b}, resulting in "look-alike" remainders. It should be noted that the clusters of remainders about M^a (for $t=0$) and M^{a-b} (for $t=1$) are distinct because $a>b$, and that $k \ll M^b$, for otherwise it might happen that $tM^{a-b} \approx M^a$, and the clusters for $t=0$ and $t=1$ would coalesce.

The above analysis shows that small perturbations in a divisor can sometimes cause quite predictable changes in the remainder, so it is not always a good idea to depend on long division to try to produce randomness. Incidentally, this idea might be of some use in identifying intervals of integers that contain no divisors of Mersenne numbers, Fermat numbers, and other numbers near large powers of small integers.

Acknowledgment. I thank the referee for helpful suggestions.

Proof Without Words: Area Under a Polygonal Arch

The area under the polygonal arch generated by a regular polygon rolling along a straight line is three times the area of the polygon.



COROLLARY. *The area under one arch of a cycloid is three times the area of the generating circle.*

—PHILIP R. MALLINSON
PHILLIPS EXETER ACADEMY
EXETER, NH 03833-2460

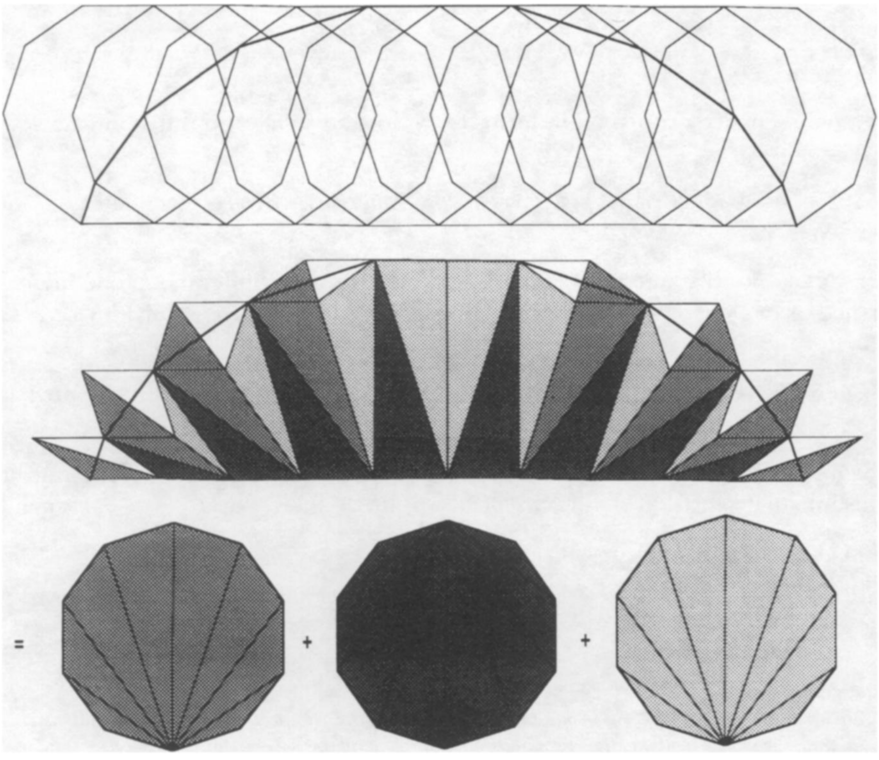
This completes the proof that the remainder R is dominated by one of the numbers M^a or tM^{a-b}, resulting in "look-alike" remainders. It should be noted that the clusters of remainders about M^a (for $t=0$) and M^{a-b} (for $t=1$) are distinct because $a > b$, and that $k \ll M^b$, for otherwise it might happen that $tM^{a-b} \approx M^a$, and the clusters for $t=0$ and $t=1$ would coalesce.

The above analysis shows that small perturbations in a divisor can sometimes cause quite predictable changes in the remainder, so it is not always a good idea to depend on long division to try to produce randomness. Incidentally, this idea might be of some use in identifying intervals of integers that contain no divisors of Mersenne numbers, Fermat numbers, and other numbers near large powers of small integers.

Acknowledgment. I thank the referee for helpful suggestions.

Proof Without Words: Area Under a Polygonal Arch

The area under the polygonal arch generated by a regular polygon rolling along a straight line is three times the area of the polygon.



COROLLARY. *The area under one arch of a cycloid is three times the area of the generating circle.*

—PHILIP R. MALLINSON
PHILLIPS EXETER ACADEMY
EXETER, NH 03833-2460

PROBLEMS

GEORGE T. GILBERT, *Editor*
Texas Christian University

ZE-LI DOU, KEN RICHARDSON, and SUSAN G. STAPLES, *Assistant Editors*
Texas Christian University

Proposals

To be considered for publication, solutions should be received by September 1, 1998.

1544. *Proposed by* 1996 *MathCamp Students, University of Washington.*

Let a_0 be a positive integer and let

$$a_{k+1} = \begin{cases} a_k + 1 & \text{if } a_k \text{ is odd,} \\ a_k/2 & \text{if } a_k \text{ is even.} \end{cases}$$

Find a nonrecursive expression in terms of a_0 for the smallest positive integer k such that $a_k = 1$.

1545. *Proposed by Erwin Just, Professor Emeritus, Bronx Community College, Bronx, New York.*

Let k be a positive integer. Prove that there exists an infinite, monotone increasing sequence of integers (a_n) such that a_n divides $a_{n+1}^2 + k$ and a_{n+1} divides $a_n^2 + k$ for all $n \geq 1$.

1546. *Proposed by Benjamin G. Klein, Davidson College, Davidson, North Carolina, and Arthur L. Holshouser, Charlotte, North Carolina.*

Given $y > 1$, let P be the set of all real polynomials $p(x)$ with nonnegative coefficients that satisfy $p(1) = 1$ and $p(3) = y$. Prove there exists $p_0(x) \in P$ such that

(i) $\{p(2)\colon p(x) \in P\} = (1, p_0(2)]$;
(ii) if $p(x) \in P$ and $p(2) = p_0(2)$, then $p(x) = p_0(x)$.

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 containing the solver's name and full address.*

Solutions and new proposals should be mailed to George T. Gilbert, Problems Editor, Department of Mathematics, Box 298900, Texas Christian University, Fort Worth, TX 76129, or mailed electronically (ideally as a LATEX file) to g.gilbert@tcu.edu. *Readers who use e-mail should also provide an e-mail address.*

1547. *Proposed by Homer White, Georgetown College, Georgetown, Kentucky, and Robert Bailey, Lexington, Kentucky.*

Consider the function

$$f(n)=\begin{cases}\dfrac{3n}{2} & \text{if } n \text{ is even,}\\[2mm] \dfrac{3n+1}{2} & \text{if } n \text{ is odd.}\end{cases}$$

Let $N>1$ be a positive integer, and define $a_n(i)$ to be the remainder when the ith iterate of f, $f^{(i)}(n)$, is divided by N. Prove that, for any $n\geq 1$, the sequence $(a_n(i))_{i\geq 0}$ is not periodic.

1548. *Proposed by Ken Richardson, Texas Christian University, Fort Worth, Texas.*

Let D be a convex domain in the plane, and suppose that its boundary curve α is piecewise C^2. Imagine that a fence is built along the boundary, and that a rope of length L is attached to the outside of the fence at a point along the boundary. By pulling on the rope so that it is taut but constrained to remain outside D, a new curve β is traced out by the end of the rope. Assuming that L is at least half of the length of the curve α, is it true that the curve β determines the curve α?

Quickies

Answers to the Quickies are on page 150.

Q877. *Proposed by Eugene W. Sard, Huntington, New York.*

An American League baseball player noticed that after he got his 50th career hit against the Yankees, his career batting average rose by exactly .0005. What was his most likely batting average before this last hit?

(Batting average is the number of hits divided by the number of official at bats, which include hits.)

Q878. *Proposed by Charles Vanden Eynden, Illinois State University, Normal, Illinois.*

Let $c(n)$ be the number of ways of tiling a $2^n\times 2^n$ checkerboard with 1×2 tiles. Evaluate

$$\lim_{n\to\infty}\frac{\ln\ln c(n)}{n}.$$

Q879. *Proposed by Jan Mycielski, University of Colorado at Boulder, Boulder, Colorado.*

A sphere S (in $\mathbb{R}^3$) intersects a sphere B of radius 1. Furthermore, S passes through the center of B. Show that the surface area of that part of S lying inside B is independent of the radius of S.

Solutions

Symmetry of a Doubly-Indexed Sequence **April 1997**

1519. *Proposed by Sam Northshield, SUNY, Plattsburgh, New York.*

Given a sequence $(a_n)_{n\geq 1}$, let $A_{0j}=1$ and

$$A_{ij}=\prod_{1\leq k\leq i}(1+ja_k)$$

for positive i and nonnegative j. What sequences (a_n) satisfy $A_{ij}=A_{ji}$ for all nonnegative i and j?

Solution by Howard Morris, Germantown, Tennessee.

The sequence may start with any a_1 that is not the reciprocal of a negative integer. The other terms are given by

$$a_n=\frac{a_1}{1+(n-1)a_1}.$$

From

$$1+na_1=A_{1n}=A_{n1}=A_{n-1,1}(1+a_n)=A_{1,n-1}(1+a_n)=(1+(n-1)a_1)(1+a_n),$$

it follows that a_1 is not the reciprocal of a negative integer and that

$$a_n=\frac{a_1}{1+(n-1)a_1}.$$

To prove that such a sequence implies $A_{ij}=A_{ji}$, there is no loss of generality in assuming $i>j$. Then

$$A_{ij}=\prod_{k=1}^{i}\frac{1+(j+k-1)a_1}{1+(k-1)a_1}=\frac{\prod_{k=1-i+j}^{j}1+(i+k-1)a_1}{\prod_{k=1}^{i}1+(k-1)a_1}$$

$$=\frac{\prod_{k=1}^{j}1+(i+k-1)a_1}{\prod_{k=1}^{j}1+(k-1)a_1}\,\frac{\prod_{k=1-i+j}^{0}1+(i+k-1)a_1}{\prod_{k=j+1}^{i}1+(k-1)a_1}$$

$$=\prod_{k=1}^{j}\frac{1+(i+k-1)a_1}{1+(k-1)a_1}=A_{ji},$$

as required.

Also solved by Vic Abad, Cai Bo (Australia), Sabin Cautis (Canada), John Christopher, Daniele Donini (Italy), Thomas Jager, Ioana Mihaila, Can A. Minh (graduate student), R. P. Sealy (Canada), Yongzhi Yang, and the proposer. There were two incomplete solutions.

Loci for Symmetric Conditions in a Triangle **April 1997**

1520. *Proposed by Victor Kutsenok, St. Francis College, Fort Wayne, Indiana.*

(a) Given points A and B in the plane, describe the set of points C in the plane such that A, B, and C form a triangle satisfying $am_a = bm_b$, where $a = BC$, $b = AC$, and m_a and m_b are the lengths of the medians from A and B respectively;

(b) Given points A and B in the plane, describe the set of points C in the plane such that A, B, and C form a triangle satisfying $al_a = bl_b$, where l_a and l_b are the lengths of the angle bisectors from A and B respectively.

I. *Solution by Paul Yiu, Florida Atlantic University, Boca Raton, Florida.*

Clearly, in both cases, the point C can be chosen on the perpendicular bisector of the segment AB. Thus, we shall henceforth assume $a \neq b$ and let $c = AB$.

(a) The medians m_a and m_b satisfy

$$m_a^2 = \frac{1}{4}(2b^2 + 2c^2 - a^2) \quad \text{and} \quad m_b^2 = \frac{1}{4}(2a^2 + 2c^2 - b^2).$$

From the relation $am_a = bm_b$, we obtain

$$(a^2 - b^2)(a^2 + b^2 - 2c^2) = 0.$$

Since $a \neq b$, we must have $a^2 + b^2 = 2c^2$. From this, $m_c^2 = 3c^2/4$, and C lies on the circle with center at the midpoint of AB and radius $AB \cdot \sqrt{3}/2$.

(b) Let α, β, and γ denote the measures of the angles A, B, and C, respectively. The angle bisectors have lengths given by

$$l_a = \frac{2bc}{b+c}\cos\frac{\alpha}{2} \quad \text{and} \quad l_b = \frac{2ac}{a+c}\cos\frac{\beta}{2}.$$

Now, $al_a = bl_b$ if and only if

$$\frac{\cos\frac{\alpha}{2}}{b+c} = \frac{\cos\frac{\beta}{2}}{c+a}.$$

By the law of sines, this equation is equivalent to

$$\frac{\cos\frac{\alpha}{2}}{\sin\beta + \sin\gamma} = \frac{\cos\frac{\beta}{2}}{\sin\gamma + \sin\alpha}.$$

We obtain

$$\frac{\cos\frac{\alpha}{2}}{\sin\beta + \sin\gamma} = \frac{\cos\frac{\alpha}{2}}{2\sin\frac{\beta+\gamma}{2}\cos\frac{\beta-\gamma}{2}} = \frac{1}{2\cos\frac{\beta-\gamma}{2}},$$

for the left-hand side, and similarly $1/(2\cos\frac{\gamma-\alpha}{2})$ on the right-hand side. It follows that

$$\cos\frac{\beta-\gamma}{2} = \cos\frac{\gamma-\alpha}{2},$$

and $\beta - \gamma = \pm(\gamma - \alpha)$. Since $a \neq b$, we must choose the positive sign, and obtain $\alpha + \beta = 2\gamma$. This means $\gamma = 60°$, and C lies on the major arc of the circumcircle of one of the two equilateral triangles on AB.

II. *Solution by David Zhu, Jet Propulsion Laboratory, Pasadena, California.*

(a) Choose a coordinate system so that $A = (-c/2, 0)$ and $B = (c/2, 0)$. If $C = (x, y)$,

$$a^2 = \left(x - \frac{c}{2}\right)^2 + y^2,$$

$$b^2 = \left(x + \frac{c}{2}\right)^2 + y^2,$$

$$m_a^2 = \left(\frac{x + c/2}{2} + \frac{c}{2}\right)^2 + \left(\frac{y}{2}\right)^2,$$

$$m_b^2 = \left(\frac{x - c/2}{2} - \frac{c}{2}\right)^2 + \left(\frac{y}{2}\right)^2.$$

Then $a^2 m_a^2 = b^2 m_b^2$ can be simplified to

$$x\left((x^2 + y^2) - \frac{3}{4}c^2\right) = 0.$$

Thus the set of points C is on the perpendicular bisector of AB and the circle centered at the midpoint of AB with radius $\sqrt{3}/2$ times the length of AB.

(b) Let $\angle A = \alpha$, $\angle B = \beta$, and $AB = c$. Using the law of sines,

$$a = \frac{c \sin \alpha}{\sin(\alpha + \beta)},$$

$$b = \frac{c \sin \beta}{\sin(\alpha + \beta)},$$

$$l_a = \frac{c \sin \beta}{\sin(\alpha/2 + \beta)},$$

$$l_b = \frac{c \sin \alpha}{\sin(\alpha + \beta/2)}.$$

Then $al_a = bl_b$ is reduced to

$$\sin\left(\alpha + \frac{\beta}{2}\right) = \sin\left(\frac{\alpha}{2} + \beta\right),$$

hence

$$\alpha = \beta \text{ or } \alpha + \beta = \frac{2\pi}{3}.$$

Thus, the set of points C is on the perpendicular bisector of AB and the 60° arcs about chord AB.

Also solved by Sabin Cautis (Canada), Daniele Donini (Italy), Ragnar Dybvik (Norway), Milton P. Eisner (part (a)), H. Guggenheimer, Howard Cary Morris, Volkhard Schindler (Germany), Michael Vowe (Switzerland), and the proposer. There was one incorrect solution.

A Difference of Powers Functional Equation **April 1997**

1521. *Proposed by Wu Wei Chao, He Nan Normal University, Xin Xiang City, He Nan Province, China.*

Let a function $f: \mathbb{R} \to \mathbb{R}$ satisfy

$$f(x^n - y^n) = (x - y)\left[f(x)^{n-1} + f(x)^{n-2}f(y) + \cdots + f(x)f(y)^{n-2} + f(y)^{n-1}\right].$$

Prove that $f(rx) = rf(x)$ for all rational r and all real x.

Solution by John Baker and John Lawrence, University of Waterloo, Waterloo, Ontario, Canada.

We will show that the only functions satisfying the given functional equation are $f(x) = x$, $f(x) = 0$ for $n \geq 2$, $f(x) = -x$ for n even, and $f(x) = cx$ for $n = 2$. It is easy to verify that such functions satisfy the given.

To show there are no other functions, begin by setting $x = y$ to see that $f(0) = 0$. Next, set $y = 0$ to obtain $f(x^n) = xf(x)^{n-1}$ and $x = 0$ to obtain $f(-y^n) = -yf(y)^{n-1}$. These combine to yield that $f(-x) = -f(x)$ for all $x \in \mathbb{R}$.

Assume first that n is even. Then

$$\begin{aligned} 0 &= f(x^n - y^n) - f(x^n - (-y)^n) \\ &= 2(xf(y) - yf(x))\left[f(x)^{n-2} + f(x)^{n-4}f(y)^2 + \cdots + f(y)^{n-2}\right]. \end{aligned}$$

Note that each term in the square brackets is an even power. If there exists a such that $f(a) \neq 0$, it follows that $xf(a) - af(x) = 0$, or $f(x) = (f(a)/a)x$. From $f(1^n) = 1 \cdot f(1)^{n-1}$, we see that $f(x) = x$ or $f(x) = -x$, unless $n = 2$, in which case there is no restriction on $f(a)/a$.

Now assume that n is odd. Let $F = \{\alpha \in \mathbb{R}\colon f(\alpha x) = \alpha f(x) \text{ for all } x \in \mathbb{R}\}$. We want to show that $\mathbb{Q} \subset F$ and ultimately that $F = \mathbb{R}$. Clearly, $0, \pm 1 \in F$ and F is closed under multiplication and reciprocation. It remains to show that F is closed under addition. We show first that F is closed under taking nth roots. For $\alpha \in F$,

$$\alpha x f(x)^{n-1} = \alpha f(x^n) = f(\alpha x^n) = f\left((\alpha^{1/n}x)^n\right) = \alpha^{1/n}xf(\alpha^{1/n}x)^{n-1}.$$

Noting that $f(x^n) = xf(x)^{n-1}$ also implies $f(x) \geq 0$ for $x > 0$ and $f(x) \leq 0$ for $x < 0$, it follows that $f(\alpha^{1/n}x) = \alpha^{1/n}f(x)$. Setting $a = \alpha^{1/n}$ and $b = \beta^{1/n}$, the closure of F under addition now follows from

$$\begin{aligned} &f((\alpha + \beta)x^n) \\ &\quad = f\left((ax)^n - (-bx)^n\right) \\ &\quad = (ax + bx)\left[f(ax)^{n-1} - f(ax)^{n-2}f(bx) + \cdots - f(ax)f(bx)^{n-2} + f(bx)^{n-1}\right] \\ &\quad = (a + b)x(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1})f(x)^{n-1} \\ &\quad = (\alpha + \beta)xf(x)^{n-1} = (\alpha + \beta)f(x^n). \end{aligned}$$

Having shown that $\mathbb{Q} \subset F$, we now show that F is continuous on $\mathbb{R}$. We begin by showing continuity at 0. If $x > y > 0$, then

$$\begin{aligned} &\frac{f(x^n - y^n)}{x - y} - \frac{f(x^n + y^n)}{x + y} \\ &\quad = 2\left[f(x)^{n-2}f(y) + f(x)^{n-4}f(y)^3 + \cdots + f(x)f(y)^{n-2}\right] \geq 0, \end{aligned}$$

so that

$$0 \leq f(x^n + y^n) \leq \frac{x + y}{x - y}f(x^n - y^n).$$

Replace x and y with $(1+x)^{1/n}$ and $x^{1/n}$ respectively, $x \geq 0$, to obtain

$$0 \leq f(1+2x) \leq \frac{(1+x)^{1/n} + x^{1/n}}{(1+x)^{1/n} - x^{1/n}} f(1).$$

The right-hand side of this last inequality is bounded on any finite interval, hence $f(x)$ is bounded above by some constant M on the interval $[1,2]$. Now for $1/2^k \leq x < 1/2^{k-1}$, k a positive integer, $f(x) = f(2^k x)/2^k \leq M/2^k$. Because f is odd, we conclude that $\lim_{x \to 0} f(x) = 0$. From the given functional equation,

$$\begin{aligned}
&\lim_{y \to 0} f(x^n - y^n) \\
&= \lim_{y \to 0} (x-y)\left[f(x)^{n-1} + f(x)^{n-2} f(y) + \cdots + f(x) f(y)^{n-2} + f(y)^{n-1}\right] \\
&= x f(x)^{n-1} = f(x^n).
\end{aligned}$$

Therefore, f is continuous on $\mathbb{R}$. Because $f(x) = xf(1)$ for $x \in F$ and F is dense in $\mathbb{R}$, it follows that $f(x) = xf(1)$ for $x \in \mathbb{R}$. Finally, again from $f(1^n) = 1 \cdot f(1)^{n-1}$, we conclude that $f(x) = x$ or, if $n > 1$, $f(x) = 0$.

Also solved by Cai Bo (Australia), Sabin Cautis (Canada), Daniele Donini (Italy), Thomas Jager, and the proposer.

A Constrained Trigonometric Inequality **April 1997**

1522. *Proposed by Bogdan Kotkowski, Kent State University, Tuscarawas Campus, New Philadelphia, Ohio.*

Prove that if

$$\cos^2 \alpha + \cos^2 \beta + \cos^2 \gamma + 2\cos\alpha\cos\beta\cos\gamma = 1$$

and two of the expressions

$$\cos\alpha\cos\beta + \cos\gamma, \qquad \cos\beta\cos\gamma + \cos\alpha, \qquad \cos\gamma\cos\alpha + \cos\beta$$

are positive, then the third expression is also. Moreover, if α, β, and γ are positive numbers less than π, then $\alpha + \beta + \gamma = \pi$.

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

Without loss of generality, suppose the first two expressions are positive. Then,

$$\begin{aligned}
0 &< (\cos\alpha\cos\beta + \cos\gamma)(\cos\beta\cos\gamma + \cos\alpha) \\
&= (\cos^2\beta + 1)\cos\alpha\cos\gamma + \cos\beta(\cos^2\alpha + \cos^2\gamma) \\
&= (\cos^2\beta + 1)\cos\alpha\cos\gamma + \cos\beta(1 - \cos^2\beta - 2\cos\alpha\cos\beta\cos\gamma) \\
&= (1 - \cos^2\beta)(\cos\alpha\cos\gamma + \cos\beta).
\end{aligned}$$

Because $1 - \cos^2\beta \geq 0$, it follows that $\cos\alpha\cos\gamma + \cos\beta$ is positive.

Suppose, in addition, that $0 < \alpha, \beta, \gamma < \pi$. Applying the quadratic formula to the equation produces

$$\cos\gamma = -\cos\alpha\cos\beta + \sqrt{(1-\cos^2\alpha)(1-\cos^2\beta)} = -\cos\alpha\cos\beta \pm \sin\alpha\sin\beta.$$

Since $\cos\alpha\cos\beta+\cos\gamma$ is positive,

$$\cos\gamma = -\cos\alpha\cos\beta + \sin\alpha\sin\beta = \cos(\pi-(\alpha+\beta)).$$

Suppose $\pi<\alpha+\beta<2\pi$. Then, $-\pi<\pi-(\alpha+\beta)<0$, so $\gamma=(\alpha+\beta)-\pi$. Hence, $\cos\gamma\cos\beta+\cos\alpha=\cos\gamma\cos\beta-\cos(\gamma-\beta)=-\sin\gamma\sin\beta<0$, which is false. Thus, $0<\alpha+\beta\le\pi$, so that $0\le\pi-(\alpha+\beta)<\pi$ and $\gamma=\pi-(\alpha+\beta)$.

Also solved by Cai Bo (Australia), Sabin Cautis (Canada), Daniele Donini (Italy), S. A. Greenspan, Robert Heller, Murray S. Klamkin (Canada), Victor Y. Kutsenok, Kee-Wai Lau (Hong Kong), Ioana Mihaila, Can A. Minh (graduate student), P. E. Nüesch (Switzerland), Allan Pedersen (Denmark), Michael Vowe (Switzerland), David Zhu, and the proposer. There was one incorrect solution.

A Maclaurin Series with Integral Coefficients **April 1997**

1523. *Proposed by Emeric Deutsch, Polytechnic University, Brooklyn, New York.*

Let m and n be positive integers. Show that the Maclaurin series expansion of

$$f(x)=\frac{2}{\sqrt{3}}\sqrt{\frac{1-mx}{nx^3}}\sin\left(\frac{1}{3}\arcsin\left(\frac{3\sqrt{3}}{2}\sqrt{\frac{nx^3}{(1-mx)^3}}\right)\right)$$

has integer coefficients.

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

The domain of $f(x)$, as it is defined, is an interval $I=(0,\delta]$, with $\delta>0$ depending on m and n. Let $x\in I$. Applying the formula $\sin 3\alpha=3\sin\alpha-4\sin^3\alpha$, one may verify that $f(x)$ satisfies

$$nx^3f(x)^3-(1-mx)f(x)+1=0, \qquad (1)$$

so that $g(x,f(x))=0$, where $g(x,y)=nx^3y^3-(1-mx)y+1$. Since $g(0,1)=0$ and $\partial g/\partial y(0,1)=-1\neq 0$, the implicit function theorem assures that $f(x)$ may be extended to a real analytic function in a neighborhood of $x=0$. Let $f(x)=\sum_{k=0}^{\infty}a_kx^k$ be the Maclaurin series expansion of $f(x)$. Substituting into (1), we have

$$(1-a_0)+(ma_0-a_1)x+(ma_1-a_2)x^2 + \sum_{k=3}^{\infty}\left(ma_{k-1}-a_k+n\sum_{i+j+l=k-3}a_ia_ja_l\right)x^k=0,$$

or, equivalently,

$$a_0=1,\ a_1=m,\ a_2=m^2,\ a_k=ma_{k-1}+n\sum_{i+j+l=k-3}a_ia_ja_l, \text{ for } k\ge 3.$$

Thus, a_k is a positive integer for every k.

II. *Solution by Paul Bracken, Centre de Recherches Mathématiques, Montreal, Québec, Canada.*

We show, more generally, that the Maclaurin series expansion of

$$f(x)=\frac{2}{\sqrt{3}}\sqrt{\frac{1-mx}{nx^3}}\sin\left(\frac{1}{3}\arcsin\left(\frac{3\sqrt{3}}{2}\sqrt{\frac{nx^3}{(1-mx)^{2p+1}}}\right)\right)$$

has integer coefficients for all nonnegative integers p.

Set

$$\theta=\arcsin\left(\frac{3\sqrt{3}}{2}\sqrt{\frac{nx^3}{(1-mx)^{2p+1}}}\right).$$

Then the identity $\sin\theta = 3\sin(\theta/3) - 4\sin^3(\theta/3)$ leads to the equation

$$\frac{nx^3}{1-mx}f(x)^3 - f(x) + \frac{1}{(1-mx)^p} = 0.$$

For v, w, and y satisfying

$$wy^q - y + v = 0, \text{ or } w = \frac{y-v}{y^q},$$

we wish to find the power series expansion of y in terms of w (and v) about the point $w=0$, $y=v$. The general Lagrange series expansion of $w - w_0 = (y-y_0)/g(y)$, $g(w_0) \neq 0$, about $w = w_0$, $y = y_0$, is given by

$$y = y_0 + \sum_{k=1}^{\infty} \frac{1}{k!}\left(\left.\frac{d^{k-1}}{dy^{k-1}}\right|_{y=y_0} g(y)^k\right)(w-w_0)^k$$

(see T. J. I. Bromwich, *An Introduction to the Theory of Infinite Series*, 1947, p. 159, or M. Abramowitz and C. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th printing, 1972, p. 14). Applied to our situation, this yields

$$y = v + \sum_{k=1}^{\infty} \frac{1}{k!}\left(\left.\frac{d^{k-1}}{dy^{k-1}}\right|_{y=v} y^{kq}\right)w^k$$
$$= v + \sum_{k=1}^{\infty} \frac{1}{k}\binom{kq}{k-1} v^{k(q-1)+1} w^k.$$

Now, the identity

$$\frac{1}{k}\binom{kq}{k-1} = \binom{kq+1}{k} - q\binom{kq}{k-1}$$

shows that $\binom{kq}{k-1}/k$ is an integer. Because the Maclaurin series expansions of $nx^3/(1-mx)$ and $(1-mx)^{-p}$ have integral coefficients, the former with no constant term, substituting for v and w and expanding shows that the Maclaurin series of f in terms of x has integral coefficients.

Also solved by Thomas Jager, Hans Kappus (Switzerland), Peter W. Lindstrom, Howard Cary Morris, Michael Vowe (Switzerland), and the proposer.

Answers

Solutions to the Quickies on page 143.

A877. Letting h and a denote the number of hits and official at bats before the last hit. Then

$$\frac{h+1}{a+1} = \frac{h}{a} + \frac{1}{2000}.$$

Solving for h yields $h = a(1999-a)/2000$. Since $h > 0$, it follows that 16 divides one of the positive integers a and $1999 - a$, and that 125 divides the other. Thus, we may write a and $1999 - a$ as $16m$ and $125n$, in some order. Since $16m + 125n = 1999$, we have $0 < n < 16$ and $-3n \equiv 15 \pmod{16}$, hence $n \equiv -5 \pmod{16}$. Therefore, $n = 11$ and $m = 39$. There are two possibilities: $a = 1375$ and $h = 429$, a batting average of

.312, or $a = 624$ and $h = 429$, a batting average of .6875. No major league batter has approached the latter average over even half as many at bats (the modern major league record for one season is .424, set by Rogers Hornsby in 1924 in 536 at bats); thus, the second answer is highly improbable.

A878. We show that

$$\lim_{n \to \infty} \frac{\ln \ln c(n)}{n} = \ln 4.$$

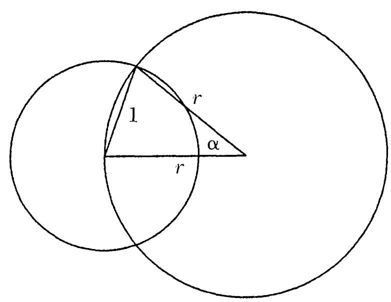
There are two ways to tile a 2×2 square. Dividing a $2^n \times 2^n$ checkerboard into $4^{n-1} 2 \times 2$ squares, we see that $2^{4^{n-1}} \le c(n)$. On the other hand, there are at most 4 ways a 1×2 tile can cover a square of the checkerboard in such a tiling. Thus, $c(n) \le 4^{4^n}$. Taking logarithms twice yields

$$(n-1)\ln 4 + \ln \ln 2 \le \ln \ln c(n) \le n \ln 4 + \ln \ln 4.$$

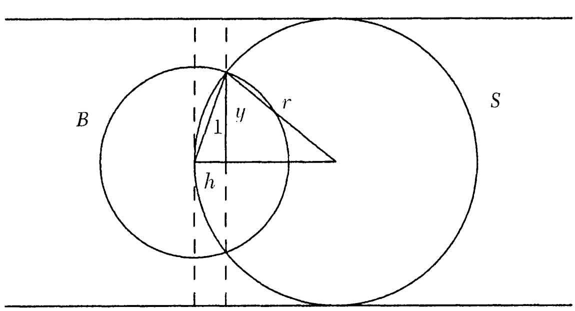
The desired limit follows from dividing by n and letting n approach ∞.

A879. I. Let r be the radius of S and let α be the angle formed by the line segment between the centers of the two spheres and any radius from the center of S to a point on the intersection of S and B. Then, by the law of cosines, $1 = 2r^2 - 2r^2 \cos \alpha = 2r^2(1 - \cos \alpha)$. The area of S inside B equals

$$\int_0^{\alpha} (2\pi r \sin \theta) r \, d\theta = 2\pi r^2 (1 - \cos \alpha) = \pi.$$



II. We will use the theorem of Archimedes that the projection of S to the surface of a circumscribed cylinder preserves areas. Let r be the radius of S, and let y be the radius of the intersection of S and B. Let h be the height of the projection of the part of S lying inside B to the circumscribed cylinder parallel to the segment between the centers of S and B, as in the diagram. We have $y^2 + h^2 = 1$ and $y^2 + (r-h)^2 = r^2$. Solving these equations for h, we get $h = 1/(2r)$. The area of that part of S lying inside B equals that of the projection, which is $2\pi r h = \pi$.



REVIEWS

PAUL J. CAMPBELL, *editor*
Beloit College
1997–98: Universität Augsburg,
Germany

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.

GIMPS discovers 37th known Mersenne prime, $2^{3,021,377}-1$ is now the largest known prime, `http://www.mersenne.org/3021377.htm` . Rae-Dupree, Janet, Student hits math jackpot, *San Jose Mercury News* (2 February 1998) `http://www.sjmercury.com/scitech/center/prime020398.htm` . Caldwell, Chris K., The art of giant slaying is refined: GIMPS finds $2^{3,021,377}-1$ is prime, `http://www.utm.edu/research/primes/notes/3021377/` .

Another year, another Mersenne prime, found by an even larger team of computers (4,000). This time, the newsworthy aspect was that the winning candidate turned out to be tested on the computer of a college student. Can we say that he discovered it? Or did he just win a kind of lottery? For the 38th Mersenne prime, it really will be like a lottery: The person on whose computer it is found will win max{ \$1000, \$1 × (number of digits)/1000 }, thanks to Scott Kurowski, author of the software used. If there are infinitely many Mersenne primes, eventually every participant should win!

Forbes, Tony, Ten primes: A search for ten consecutive primes in arithmetic progression, `http://www.ltkz.demon.co.uk/ar2/10primes.htm` .

Recently, it has been hard to keep up with progress in *consecutive* primes in arithmetic progression. Only in 1995 was the first sequence of seven discovered; in late 1997, a sequence of eight was found; and early in 1998, a set of nine was discovered (along with 27 new sets of eight and hundreds of sets of seven, thereby greatly cheapening sets of seven or eight). We refrain from printing the 92-digit starting prime (the common difference is only 210), especially since the hunt is already on for a set of ten. Leader Forbes expects to have to try about 3×10^{15} candidates, which would take about 250,000 years on a typical PC. But, like the search for the set of nine, this will be a distributed effort running in the spare time of collaborators' computers. If this search had as many collaborators as GIMPS (fat chance!—no prize money here), it would take only about 6 years. So, the next several times that somebody on the street asks you what the record is for consecutive primes in progression, you can be confident of probably being right if you say "9."

Corry, Leo, Jürgen Renn, and John Stackel, Belated decision in the Hilbert-Einstein priority dispute, *Science* 278 (14 November 1997) 1270–1273.

Perhaps forgotten by many mathematicians is Hilbert's great interest in physics. At almost the same time as Einstein, he published the theory of general relativity. Examination of the proofs of Hilbert's paper, however, reveals that he added crucial elements in proof, perhaps after seeing Einstein's results; they had consulted frequently on the problem.

Hayes, Brian, The invention of the genetic code, *American Scientist* (January–February 1998). Also available at `http://www.amsci.org/amsci/issues/Comsci98/compsci9801/html` .

This article recounts the code-breaking attempts that followed Watson and Crick's discovery of the double helix of DNA. The question was, how did the sequence of bases in DNA code for amino acids? There are 4 kinds of bases and 20 kinds of amino acids. A code whose codewords (*codons*) consist of three consecutive bases provides $2^3 = 64$ different codewords, far more than the 20 needed. Physicists George Gamow, Edward Teller, and Richard Feynman all proposed such codes that were overlapping, meaning that each base was a part of three consecutive codeword of three bases each. In most of these ingenious attempts, the 64 codons sorted themselves into exactly 20 families. All of these codes were ruled out by experimental evidence. In 1957, Crick proposed a *comma-free* code, in which, of the three codons that each base belongs to, only one holds biochemical meaning and the other two must be nonsense. The codons AAA, CCC, GGG, and UUU would have to be nonsense; the remaining 60 codons are factored by cyclic permutation into 20 groups, but only one in each group could be meaningful. Another beautiful theory! But in 1961 it was discovered that UUU does code for an amino acid. By 1965, the genetic code was mostly solved, by laboratory work. It turned out to be fairly redundant (hence tolerant of mutations): Some amino acids are coded for by as many as six codons. This is a fascinating tale of "intellectual elegance" vs. reality; the proposed mathematical models were not the solution to the original problem but did lead to fruitful mathematical research into codes.

Bogomolny, Alex, Cut the knot! An interactive column using Java applets, `http://www.maa.org/editorial/knot/` . Interactive Mathematics Miscellany and Puzzles, `http://www.cut-the-not.com/` .

MAA Online, the presence of the MAA on the Worldwide Web, features several regular columns, most of which have been reviewed here earlier. Here we look at a relatively new column, intended mainly for teachers, students, and parents. Each monthly edition contains a puzzle or problem simulation in the form of a Java applet (a program, downloaded automatically, that makes the screen of your Web browser change dynamically with your input). Recent topics include breaking a chocolate bar into component squares (how many breaks does it take? try on the screen and see) and properties of addition and multiplication tables (pick a base to view them in). Author Bogomolny also maintains a Web site with far more material of the same sort, plus other resources, which should be interesting to puzzle-lovers everywhere.

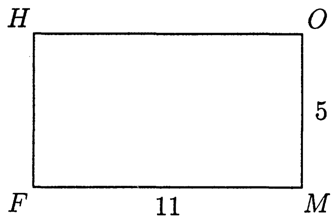
West, Beverly, Steven Strogatz, Jean Marie McDill, John Cantwell, and Hubert Hohn, *Interactive Differential Equations*, Addison Wesley Longman, 1997; xvi + 357 pp + CD-ROM (Macintosh/Windows) + User's Guides for Macintosh and Windows. ISBN 0–201–57132–3.

Here is a fun and useful collection of "tools" to supplement a course in differential equations with productive labs. Its 90 groups of activities, in 31 units, are keyed to appropriate chapters of major textbooks. The activities are grouped into first-order differential equations, second-order equations, linear algebra, systems of differential equations, chaos and bifurcation, and series solutions and boundary value problems. Students' favorite labs are likely to be Golf (why does the theory mispredict the optimal angle for the longest drive?) and Romeo and Juliet (in which students can explore the consequences of various emotional responses of the two), while I particularly enjoyed exploring graphically the differences between exact solution curves and ones computed numerically.

NEWS AND LETTERS

58th Annual William Lowell Putnam Mathematical Competition

A-1 A rectangle, $HOMF$, has sides $HO = 11$ and $OM = 5$. A triangle ABC has H as the intersection of the altitudes, O the center of the circumscribed circle, M the midpoint of BC, and F the foot of the altitude from A. What is the length of BC?



Solution. The length of BC is 28.

Place coordinates on the rectangle so that $F = (0,0)$, $M = (11,0)$, $O = (11,5)$, $H = (0,5)$, and because B and C are on the x-axis, suppose that $B = (-b, 0)$. Then, because M is the midpoint of BC, $C = (22+b, 0)$. The equation of line AC is $5y = -b(x-(22+b))$, and it follows that $A = (0, (b^2 + 22b)/5)$, and D, the midpoint of AC has coordinates $((22+b)/2, (b^2+22b)/10)$. In addition OD has slope $5/b$, so

$$\frac{(b^2 + 22b)/10 - 5}{(22+b)/2 - 11} = \frac{5}{b}.$$

This equation has three solutions: $b = 0$, which corresponds to an infinite triangle, $b = -25$ and $b = 3$, which give the same triangle (except for labeling) and give the answer.

A-2 Players $1, 2, 3, \ldots, n$ are seated around a table and each has a single penny. Player 1 passes a penny to Player 2, who then passes two pennies to Player 3. Player 3 then passes one penny to Player 4, who passes two pennies to Player 5, and so on, players alternately passing one penny or two to the next player who still has some pennies. A player who runs out of pennies drops out of the game and leaves the table. Find an infinite set of numbers n for which some player ends up with all n pennies.

Solution. If $n = 2^s + 2$, $(s = 1, 2, 3, \ldots)$, Player 3 ends with $2^s + 2$ coins.

LEMMA 1. Suppose there are $2N + 2$ players at the beginning of the game. After one round (that is, after each player has passed once), exactly N players remain in the game. Player 3 will have just received 2 coins from Player $2N+2$ and will have 4 coins. All other remaining players will have 2 coins.

Proof. Players 1 and 2 will drop out after their first pass. Odd-numbered players greater than 3 receive 2 pennies and give 1 away, for a net gain of 1, leaving those players with 2 coins. Even-numbered players greater than 2 receive 1 penny but give away 2, so must drop out of the game. Player 3 receives 2 pennies from Player $2N + 2$, so ends this round with 4 pennies, and will continue in the next round by passing 1 coin.

LEMMA 2. Suppose there are $2N$ players at the beginning of the game, and suppose that Player 1 has $a + 2$ pennies, that the even-numbered players have b pennies, $b \leq a$, and that the odd-numbered players larger than 1 have a pennies. Then after one round, the odd-numbered players will each have one more penny, and the even-numbered players will have one fewer penny. Also, Player 1 will have just received 2 pennies from Player $2N$. Consequently, after b rounds, only N players will remain in the game; Player 1 will have $a + b + 2$ coins, and all other remaining players will have $a + b$ coins.

Proof. Odd-numbered players receive 2 coins and give away 1, for a net gain of 1; even-numbered players receive 1 penny but give away 2, for a net loss of 1.

So now, suppose we begin with $2^s + 2$ players. After one round 2^{s-1} players remain in the game; one of them, Player 3, has 4 pennies and all other remaining players have 2 (from Lemma 1). After 2 more rounds, Player 3 has 6 coins, and the remaining 2^{s-2} players have 4 coins apiece (from Lemma 2). At the next stage (4 more rounds), Player 3 has 10 coins and the remaining 2^{s-3} players have 8. At each stage the number of players is cut in half, and in the end, Player 3 will have all the pennies.

A-3 Evaluate

$$\int_0^\infty \left(x - \frac{x^3}{2} + \frac{x^5}{2 \cdot 4} - \frac{x^7}{2 \cdot 4 \cdot 6} + \cdots\right) \left(1 + \frac{x^2}{2^2} + \frac{x^4}{2^2 \cdot 4^2} + \frac{x^6}{2^2 \cdot 4^2 \cdot 6^2} + \cdots\right) dx\,.$$

Solution 1. The first multiplicand is $xe^{-x^2/2} \geq 0$ for $x \geq 0$, so by the monotone convergence theorem, the integral in question is equal to

$$\lim_{n \to \infty} \int_0^\infty xe^{-x^2/2} \sum_{k=0}^{n} \frac{x^{2k}}{2^{2k}k!^2}\, dx = \sum_{k=0}^{\infty} \int_0^\infty \frac{x^{2k+1}e^{-x^2/2}}{2^{2k}k!^2}\, dx\,.$$

Integrating by parts gives

$$\int_0^\infty x^{2k+1}e^{-x^2/2}\, dx = 2k \int_0^\infty x^{2k-1}e^{-x^2/2}\, dx\,.$$

By induction on k,

$$\int_0^\infty x^{2k+1}e^{-x^2/2}\, dx = 2^k k! \int_0^\infty xe^{-x^2/2}\, dx = 2^k k!\,.$$

Therefore the value of the integral is $\displaystyle\sum_{k=0}^{\infty} \frac{1}{2^k k!} = \sqrt{e}\,.$

Solution 2. Let $u = x^2/2$ and $du = x\,dx$. Under this substitution, our integral becomes

$$\int_0^\infty \left(1 - u + \frac{u^2}{2!} - \frac{u^3}{3!} + \cdots\right)\left(1 + \frac{u/2}{(1!)^2} + \frac{(u/2)^2}{(2!)^2} + \cdots\right) du$$
$$= \int_0^\infty e^{-u} \sum_{n=0}^\infty \frac{u^n}{2^n (n!)^2}\, du = \sum_{n=0}^\infty \frac{1}{2^n (n!)^2} \int_0^\infty u^n e^{-u}\, du = \sum_{n=0}^\infty \frac{1}{2^n (n!)^2}\, n!$$

where the interchange of the integral and summation is justified because the power series in the integrand is uniformly convergent on the interval $[0, \infty]$, and where we have used the the formula $\Gamma(n+1) = \int_0^\infty u^n e^{-u}\, du = n!$. So our integral is

$$\sum_{n=0}^\infty \frac{(1/2)^n}{n!} = \sqrt{e}\,.$$

A-4 Let G be a group with identity e and $\phi : G \longrightarrow G$ a function such that

$$\phi(g_1)\phi(g_2)\phi(g_3) = \phi(h_1)\phi(h_2)\phi(h_3)$$

whenever $g_1 g_2 g_3 = e = h_1 h_2 h_3$. Prove that there exists an element a in G such that $\psi(x) = a\phi(x)$ is a homomorphism (that is, $\psi(xy) = \psi(x)\psi(y)$ for all x and y in G).

Solution. Because a group homomorphism takes the identity to the identity, $e = \psi(e) = a\phi(e)$, so if ψ is a homomorphism, a must be $\left(\phi(e)\right)^{-1}$. So define $\psi(x) = a\phi(x)$, where $a^{-1} = \phi(e)$.

From $exx^{-1} = e = xex^{-1} = eee$, our condition implies that

$$a^{-1}\phi(x)\phi(x^{-1}) = \phi(x)a^{-1}\phi(x^{-1}) = a^{-3}.$$

The first equality (after cancellation) shows that a^{-1} (and a) commutes with $\phi(x)$ for all x. This fact, together with the second equality, shows that $\phi(x^{-1}) = \left(\phi(x)\right)^{-1} a^{-2}$. Using this and $eee = e = xy(y^{-1}x^{-1})$, we see that

$$a^{-3} = \phi(x)\phi(y)\phi((xy)^{-1}) = \phi(x)\phi(y)\left(\phi(xy)\right)^{-1} a^{-2},$$

so $\phi(xy) = a\,\phi(x)\phi(y)$. Thus,

$$\psi(xy) = a\phi(xy) = a^2\phi(x)\phi(y) = \left(a\phi(x)\right)\left(a\phi(y)\right) = \psi(x)\psi(y).$$

A-5 Let N_n denote the number of ordered n-tuples of positive integers $(a_1, a_2, \ldots, a_n)$ such that $1/a_1 + 1/a_2 + \cdots + 1/a_n = 1$. Determine whether N_{10} is even or odd.

Solution. The number of different ordered 10-tuples for each multiset $\{a_1, a_2, \ldots, a_{10}\}$ is $M = \dfrac{10!}{m_1! \cdots m_k!}$, where the m_i are the multiplicities. For any given multiplicities, an unordered multiset A contributes to $N_{10} \pmod 2$ if and only if M is odd. As 10 has two nonzero binary digits, this can happen in exactly two ways: $m_1 = 10$, or $\{m_1, m_2\} = \{2, 8\}$. The first case corresponds to the single solution $(10, 10, \ldots, 10)$, the second to solutions $\{a, a, b, \ldots, b\}$, where $2/a + 8/b = 1$, and $a \neq b$. This last equation can be rewritten $ab = 2b + 8a$ or $(a-2)(b-8) = 16$. The solutions (a, b) are $(3, 24)$, $(4, 16)$, $(6, 12)$, $(18, 9)$. Therefore N_{10} is odd.

A-6 For a positive integer n and any real number c, define x_k recursively by $x_0 = 0$, $x_1 = 1$, and for $k \geq 0$,

$$x_{k+2} = \frac{cx_{k+1} - (n-k)x_k}{k+1}.$$

Fix n and then take c to be the largest value for which $x_{n+1} = 0$. Find x_k in terms of n and k, $1 \leq k \leq n$.

Solution. For $n = 1$, $x_2 = c$. Thus, the only value that works for $n = 1$ is $c = 0$, in which case $x_0 = 0$, $x_1 = 1$, and $x_2 = 0$. In general, x_k is a polynomial in c of degree at most $k-1$. Thus, $x_{n+1} = 0$ has at most n solutions for c. We claim these solutions are $\left\{-(n-1), -(n-3), \ldots, n-5, n-3, n-1\right\}$, and that for $c = n-1$ the sequence is $x_k = \binom{n-1}{k-1}$ for $1 \leq k \leq n$.

We prove this claim by induction on n. We have already verified the claim for $n = 1$. Assume now that the claim is proved for $n \geq 1$. Choose c from among the members of $\{-(n-1), \ldots, n-3, n-1\}$ and let y_k be the corresponding sequence. Define $x_k = y_k + y_{k-1}$ for $k \geq 1$, and set $x_0 = 0$. We are given $(k+1)y_{k+2} + (n-k)y_k = cy_{k+1}$ for $k \geq 0$. Then

$$\begin{aligned}(k+1)x_{k+2} + (n+1-k)x_k &= (k+1)\left(y_{k+2} + y_{k+1}\right) + (n+1-k)\left(y_k + y_{k-1}\right)\\ &= cy_{k+1} + y_k + cy_k + y_{k+1} = (c+1)(y_{k+1} + y_k) = (c+1)x_{k+1}.\end{aligned}$$

Thus, x_k satisfies the required recurrence for $n+1$ and $c+1$. Also, $x_{n+2} = y_{n+2} + y_{n+1} = 0$, since $y_{n+1} = 0$ implies $y_{n+2} = 0$ by the recurrence. This proves that for $n+1$ the solutions to $x_{n+2} = 0$ include $\{-(n-2), \ldots, n-2, n\}$.

Also, the sequence

$$x_k = y_k + y_{k-1} = \binom{n-1}{k-1} + \binom{n-1}{k-2} = \binom{n}{k-1}$$

for $c = n$. To prove $c = n$ is the largest solution for $n+1$, we must produce the missing value. If x_k is the sequence for $c = n$, it is easy to see that $y_k = (-1)^{k-1}x_k$ is the sequence for $c = -n$. Thus, $c = -n$ is the $(n+1)$-st distinct solution to x_{n+2}, which proves our claim entirely.

B-1 Let $\{x\}$ denote the distance between the real number x and the nearest integer. For each positive integer n, evaluate

$$S_n = \sum_{m=1}^{6n-1} \min\left(\left\{\frac{m}{6n}\right\}, \left\{\frac{m}{3n}\right\}\right).$$

(Here, $\min(a, b)$ denotes the minimum of a and b.)

Solution. Using the properties $\{-x\} = \{x\} = \{1+x\}$, we see that

$$\min\left(\left\{\frac{6n-m}{6n}\right\}, \left\{\frac{6n-m}{3n}\right\}\right) = \min\left(\left\{\frac{m}{6n}\right\}, \left\{\frac{m}{3n}\right\}\right).$$

Thus, by symmetry, $S_n = 2 \sum_{m=1}^{3n-1} \min\left(\left\{\frac{m}{6n}\right\}, \left\{\frac{m}{3n}\right\}\right)$. Note that

$$\left\{\frac{m}{3n}\right\} = \begin{cases} \dfrac{m}{3n}, & \text{if } 1 \le m \le 3n/2, \\ 1 - \dfrac{m}{3n}, & \text{if } 3n/2 \le m \le 3n-1. \end{cases}$$

Also, $1 - \frac{m}{3n} \ge \frac{m}{6n}$ if and only if $m \le 2n$. Thus,

$$\frac{1}{2} S_n = \sum_{m=1}^{2n} \frac{m}{6n} + \sum_{m=2n+1}^{3n} \left(1 - \frac{m}{3n}\right) = \frac{(2n)(2n+1)}{12n} + \sum_{k=1}^{n-1} \frac{k}{3n} = \frac{2n+1}{6} + \frac{(n-1)n}{6n} =$$

This proves $S_n = n$.

B-2 Let f be a twice-differentiable real-valued function satisfying

$$f(x) + f''(x) = -xg(x)f'(x),$$

where $g(x) \ge 0$ for all real x. Prove that $|f(x)|$ is bounded.

Solution. For $x > 0$,

$$f'(x)\Big(f(x) + f''(x)\Big) = -x\Big(f'(x)\Big)^2 g(x) \le 0.$$

Setting $F(x) = \Big(f(x)\Big)^2 + \Big(f'(x)\Big)^2$, we conclude that $F'(x) \le 0$, or by integration,

$$F(x) = F(0) + \int_0^x F'(t)\,dt \le F(0).$$

Therefore $F(x)$, and hence $|f(x)|$, is bounded above as $x \to \infty$.

Setting $h(x) = f(-x)$, we have $h(x) + h''(x) = -xg(-x)h'(x)$, so $|h(x)| = |f(-x)|$ is bounded above as $x \to \infty$ as well.

B-3 For each positive integer n write the sum $\sum_{m=1}^{n} \frac{1}{m}$ in the form $\frac{p_n}{q_n}$ where p_n and q_n are relatively prime positive integers. Determine all n such that 5 does not divide q_n.

Solution. Such n must lie in one of the ranges 1 to 4, 20 to 24, 100 to 104, or 120 to 124, inclusive.

Let S be the set of n such that 5 does not divide q_n. Define $\rho(n) = \lfloor n/5 \rfloor$ and

$$t_n = \sum_{\substack{m=1 \\ 5 \nmid m}}^{n} \frac{1}{m},$$

the sum extending over only those m not divisible by 5. Then $s_n = t_n + s_{\rho(n)}/5$. The denominator of t_n is clearly prime to 5. Since $s_n = t_n$ for $1 \le n \le 4$, these values $1, 2, 3, 4$ belong to S. For $n \ge 5$, s_n has denominator prime to 5 if and only if $s_{\rho(n)}$ has denominator prime to 5 *and* numerator divisible by 5.

The next smallest member n of S must satisfy $\rho(n) = 1, 2, 3$, or 4. Of $1, 2, 3, 4$, only $s_4 = 25/12$ has numerator divisible by 5. Thus the next smallest members of S are 20 to 24 (all the n with $\rho(n) = 4$).

Note that $\sum_{l=1}^{4} \frac{1}{5k+l}$ has numerator divisible by 25, while $\sum_{l=1}^{j} \frac{1}{5k+l}$ has numerator relatively prime to 5 for $j = 1, 2, 3$. Thus, among 20 to 24, only s_{20} and s_{24} have numerator divisible by 5, since $s_5/5 = 5/12$ and t_{20} and t_{24} have numerator divisible by 25.

Thus, 100 to 104 and 120 to 124, inclusive, all belong to S. For these n,

$$s_n = t_n + \frac{s_{\rho(n)}}{5} = t_n + \frac{t_{\rho(n)}}{5} + \frac{s_{\rho(\rho(n))}}{25} = t_n + \frac{t_{\rho(n)}}{5} + \frac{1}{12},$$

since $\rho(\rho(n)) = 4$. Since $\rho(n) = 20$ or 24, $t_{\rho(n)}$ has numerator divisible by 25. Observing that $\frac{1}{5k+l} + \frac{1}{5k+5-l}$ has numerator divisible by 5 for $1 \le l \le 4$, we are left to consider which of

$$\frac{1}{101} + \frac{1}{12}, \quad \frac{1}{101} + \frac{1}{102} + \frac{1}{12}, \quad \frac{1}{121} + \frac{1}{12}, \quad \frac{1}{121} + \frac{1}{122} + \frac{1}{12}$$

has numerator divisible by 5. Working modulo 5, it is easy to see that none of these sums does. Hence, none of $n = 100$ to 104 or 120 to 124 yields a sum s_n with numerator divisible by 5. The tree stops here.

B-4 Let $a_{m,n}$ denote the coefficient of x^n in the expansion of $(1 + x + x^2)^m$. Prove that for all $k \ge 0$,

$$0 \le \sum_{i=0}^{\lfloor 2k/3 \rfloor} (-1)^i a_{k-i,i} \le 1.$$

Solution. The x^n coefficient of $(1 - x + x^2)^m$ is $(-1)^n a_{m,n}$. Therefore, the sum in question is the x^k coefficient of

$$x^0(1 - x + x^2)^0 + x(1 - x + x^2) + x^2(1 - x + x^2)^2 + \cdots + x^k(1 - x + x^2)^k + \cdots$$
$$= \frac{1}{1 - x(1 - x + x^2)} = \frac{1}{2}\left(\frac{1}{1-x} + \frac{1+x}{1+x^2}\right) = \sum_{n=0}^{\infty}(x^{4n} + x^{4n+1}).$$

B-5 Prove that for $n \ge 2$, $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\Big\}n \equiv 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\Big\}n-1 \pmod{n}$.

Solution. Every integer $n > 0$ can be written uniquely as $n = 2^t m$, where m is odd.

LEMMA. If ϕ denotes the Euler ϕ-function and a and b are integers such that $a \ge b \ge t$ and $a \equiv b \pmod{\phi(m)}$, then $2^a \equiv 2^b \pmod{n}$.

Proof. As $t \le a, b$, $2^a - 2^b$ is divisible by 2^t. By Euler's theorem, $2^a \equiv 2^b \pmod{m}$. Since 2^t and m are relatively prime, n divides $2^a - 2^b$.

Now let $a_1 = 2$, $a_{k+1} = 2^{a_k}$ for $k \ge 1$. As $2^{a_k} > a_k + 1$, by induction on k, $a_{k-1} \ge k$. For $k \ge 2$ and $n = 2^t m \le k$, we have $a_{k-1} \ge a_{k-2} \ge k - 1 \ge 2^t - 1 \ge t$. Therefore,

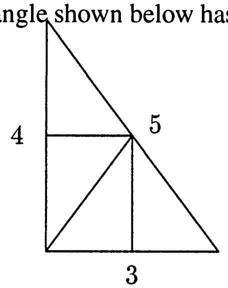
$$a_{k-2} \equiv a_{k-1} \pmod{\phi(m)} \implies a_{k-1} \equiv a_k \pmod{n}.$$

As $\phi(m) \leq m - 1 \leq n - 1$, the statement

$$a_{k-1} \equiv a_k \pmod{n} \qquad \text{for all } n \leq k,$$

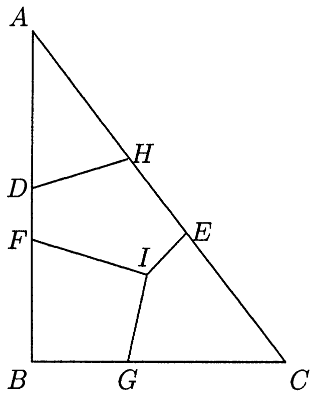
follows by induction on k.

B-6 The dissection of the 3-4-5 triangle shown below has diameter $5/2$.

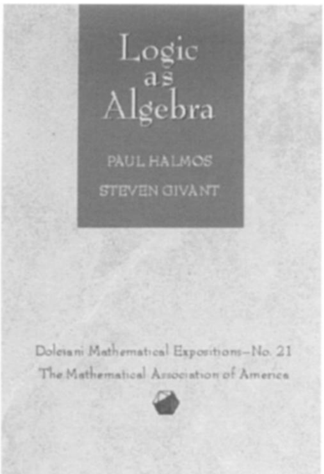


Find the least diameter of a dissection of this triangle into four parts. (The diameter of a dissection is the least upper bound of the distances between pairs of points belonging to the same part.)

Solution. $d = 25/13$.



Take points D, E on AB, AC so that $AD = DE = EC$ (i.e., = 25/13). By the pigeonhole principle, two of A, B, C, D, E must lie in the same set. So some set must have a diameter at least 25/13, the minimum distance between any two of A, B, C, D, E. On the other hand, one can find points F, G, H, I, (for example, with $BF = 20/13$, $CG = 25/13 = AH$ and I the midpoint of CD) so that the diameters of ADH, $BFIG$, $CEIG$, $DFIEH$ are each $\leq 25/13$. $FG = \sqrt{596}/13$, $BI = CI = DI = \sqrt{562.5}/13$, $EG = \sqrt{500}/13$, $FE = 24/13$, $IH = \sqrt{362.5}/13$, $FH = \sqrt{369}/13$.



THE MATHEMATICAL ASSOCIATION OF AMERICA

Logic as Algebra

Paul Halmos and Steven Givant

Series: Dolciani Mathematical Expositions

This book is based on the notes of a course in logic given by Paul Halmos. This book retains the spirit and purpose of those notes, which was to show that logic can (and perhaps should) be viewed from an algebraic perspective. When so viewed, many of its principal notions are seen to be old friends, familiar algebraic notions that were "disguised" in logical clothing. Moreover, the connection between the principal theorems of the subject and well-known theorems in algebra becomes clearer. Even the proofs often gain in simplicity.

Propositional logic and monadic predicate calculus—predicate logic with a single quantifier— are the principal topics treated. The connections between logic and algebra are carefully explained. The key notions and the fundamental theorems are elucidated from both a logical and algebraic perspective. The final section gives a unique and illuminating algebraic treatment of the theory of syllogisms—perhaps the oldest branch of logic, and a subject that is neglected in most modern logic texts.

The presentation is aimed at a broad audience—mathematics amateurs, students, teachers, philosophers, linguists, computer scientists, engineers, and professional mathematicians. Whether the reader's goal is a quick glimpse of modern logic or a more serious study of the subject, the book's fresh approach will bring novel and illuminating insights to beginners and professionals alike. All that is required of the reader is an acquaintance with some of the basic notions encountered in a first course in modern algebra. In particular, no prior knowledge of logic is assumed. The book could serve equally well as a fireside companion and as a course text.

Contents: **What is Logic?:** To count or to think; A small alphabet; A small grammar; A small logic; What is truth?; Motivation of the small language; All mathematics. **Propositional Calculus:** Propositional symbols; Propositional abbreviations; Polish notation; Language as an algebra; Concatenation; Theorem schemata; Formal proofs; Entailment; Logical equivalence; Conjunction; Algebraic identities. **Boolean Algebra:** Equivalence classes; Interpretations; Consistency and Boolean algebra; Duality and commutativity; Properties of Boolean algebras; Subtraction; Examples of Boolean algebras. **Boolean Universal Algebra:** Subalgebras; Homomorphisms; Examples of homomorphisms; Free algebras; Kernels and ideals; Maximal ideals; Homomorphism theorem; Consequences; The representation theorem. **Logic via Algebra:** Pre-Boolean algebras; Substitution rule; Boolean logics; Algebra of the propositional calculus; Algebra of proof and consequence. **Lattices and Infinite Operations:** Lattices; Non-distributive lattices; Infinite operations. **Monadic Predicate Calculus:** Propositional functions; Finite functions; Functional monadic algebras; Functional quantifiers; Properties of quantifiers; Monadic algebras; Free monadic algebras; Modal logics; Monadic logics; Syllogisms.

Catalog Code: DOL-21/JR98
152 pp., Paperbound, 1998, ISBN 0-88385-327-2
List: $27.00 MAA Member: $21.95

Phone in Your Order Now! ☎ 1-800-331-1622

Monday – Friday 8:30 am – 5:00 pm FAX (301) 206-9789

or mail to: The Mathematical Association of America, PO Box 91112, Washington, DC 20090-1112

Shipping and Handling: Postage and handling are charged as follows: **USA orders (shipped via UPS):** $2.95 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 10 days 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:** $3.50 per item ordered for books sent surface mail. Airmail service is available at a rate of $7.00 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.

Name ______________________

Address ______________________

City ______________ State _____ Zip ________

Phone ______________________

QTY.	CATALOG CODE	PRICE	AMOUNT
______	DOL-21/JR98	______	______

All orders must be prepaid with the exception of books purchased for resale by bookstores and wholesalers.

Shipping & handling ______

TOTAL ______

Payment ☐ Check ☐ VISA ☐ MasterCard

Credit Card No. ______________ Expires ___/___

Signature ______________________

CONTENTS

ARTICLES

NOTES

PROBLEMS

REVIEWS

NEWS AND LETTERS

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, NW
Washington, D.C. 20036