Vol. 84, No. 2, April 2011

MAA

MATHEMATICS MAGAZINE

Ready to construct a hyperbola

- "With This String I Thee Wed . . ."
- An Indian Approximation to the Sine Function
- Integrals, Matchings, and Rook Polynomials

An Official Publication of the **Mathematical Association of America**

EDITORIAL POLICY

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

A more detailed statement of author guidelines appears in this *Magazine*, Vol. 83, at pages 73–74, and is available at the *Magazine*'s website www.maa.org/pubs/mathmag.html. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, or published by another journal or publisher.

Please submit new manuscripts by email directly to the editor at mathmag@maa.org. A brief message containing contact information and with an attached PDF file is preferred. Word-processor and DVI files can also be considered. Alternatively, manuscripts may be mailed to Mathematics Magazine, 132 Bodine Rd., Berwyn, PA 19312-1027. If possible, please include an email address for further correspondence.

Cover image by Annie Stromquist

MATHEMATICS MAGAZINE (ISSN 0025-570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, D.C. 20036 and Lancaster, PA, bimonthly except July/August.
The annual subscription price for *MATHEMATICS MAGAZINE* to an individual member of the Association is $131. Student and unemployed members receive a 66% dues discount; emeritus members receive a 50% discount; and new members receive a 20% dues discount for the first two years of membership.)

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

Advertising correspondence should be addressed to

MAA Advertising
1529 Eighteenth St. NW
Washington DC 20036

Phone: (866) 821-1221
Fax: (202) 387-1208
E-mail: advertising@maa.org

Further advertising information can be found online at www.maa.org

Change of address, missing issue inquiries, and other subscription correspondence:

MAA Service Center, *maahq@maa.org*

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036

Copyright © by the Mathematical Association of America (Incorporated), 2011, including rights to this journal issue as a whole and, except where otherwise noted, rights to each individual contribution. Permission to make copies of individual articles, in paper or electronic form, including posting on personal and class web pages, for educational and scientific use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear the following copyright notice:

Copyright the Mathematical Association of America 2011. All rights reserved.

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

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

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

Printed in the United States of America

Vol. 84, No. 2, April 2011

MAA

MATHEMATICS MAGAZINE

EDITOR
Walter Stromquist

ASSOCIATE EDITORS

Bernardo M. Ábrego
California State University, Northridge

Paul J. Campbell
Beloit College

Annalisa Crannell
Franklin & Marshall College

Deanna B. Haunsperger
Carleton College

Warren P. Johnson
Connecticut College

Victor J. Katz
University of District of Columbia, retired

Keith M. Kendig
Cleveland State University

Roger B. Nelsen
Lewis & Clark College

Kenneth A. Ross
University of Oregon, retired

David R. Scott
University of Puget Sound

Paul K. Stockmeyer
College of William & Mary, retired

Harry Waldman
MAA, Washington, DC

LETTER FROM THE EDITOR

Again we celebrate the arrival of Spring with a few pages of color. In our first article, Tom Apostol and Mamikon Mnatsakanian use colorful figures to illustrate a construction of a hyperbola using pencil, string, and a common drinking straw. The construction follows the well known pencil-and-string construction for an ellipse, and uses the straw to turn an addition operation into a subtraction operation. The authors show how this construction helps to unify the treatment of families of conic sections.

Next is Shailesh Shirali's appreciation of the Indian mathematician Bhāskarā I, who gave a rational approximation to the sine function during India's golden age. We have better techniques now, but it's not clear that we could find a better result.

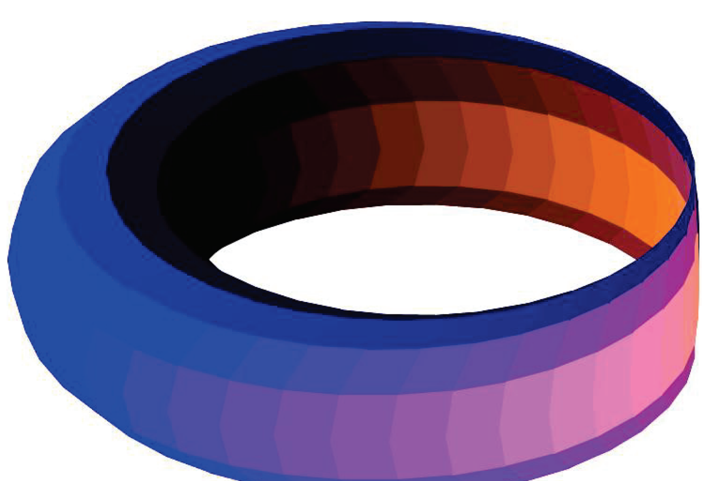
The third article is Mark Kayll's exploration of the interplay between discrete and continuous mathematics. He starts with a simple integral and finishes with a value of the Gamma function, but along the way he finds matchings in graphs, derangements, and rook polynomials.

In the Notes, two teams of authors begin from a common point in group theory ("Pr(G)") and develop it in very different directions. Andrew Bremner finds some large integers lurking in elliptic curves. Rafael Jakimczuk presents a new approach to deciding when 2 is congruent to a square mod p, and Matt Duchnowski reveals a new counting formula for crossword puzzles. Authors Brown, Knight, and Wolfe bring us a checkerboard counting problem, and solve it using—among other tools—linear algebra over a finite field.

Are you looking for the usual April feature on the USAMO? It was in the October, 2010 issue.

Finally—I can show a color graphic on this page, and so I must! The picture below is a Klein bottle, drawn in five dimensions and then projected into two. Two of the original dimensions influence the colors. Alas, the "square" tiles are not really square, or even flat. Is it possible to construct a Klein bottle in $\mathbf{R}^5$ using only square tiles?

Walter Stromquist, Editor



ARTICLES

Ellipse to Hyperbola: "With This String I Thee Wed"

TOM M. APOSTOL
Project MATHEMATICS!
California Institute of Technology
Pasadena, CA 91125
apostol@caltech.edu

MAMIKON A. MNATSAKANIAN
Project MATHEMATICS!
California Institute of Technology
Pasadena, CA 91125
mamikon@caltech.edu

String construction for both ellipse and hyperbola The title was inspired by our modification of the well-known string construction for the ellipse. In FIGURE 1a a piece of string joins two fixed points (the foci of the ellipse), and the string is kept taut by a moving pencil that traces the ellipse. The bifocal property of the ellipse states that the sum of distances from pencil to foci is the constant length of the string.

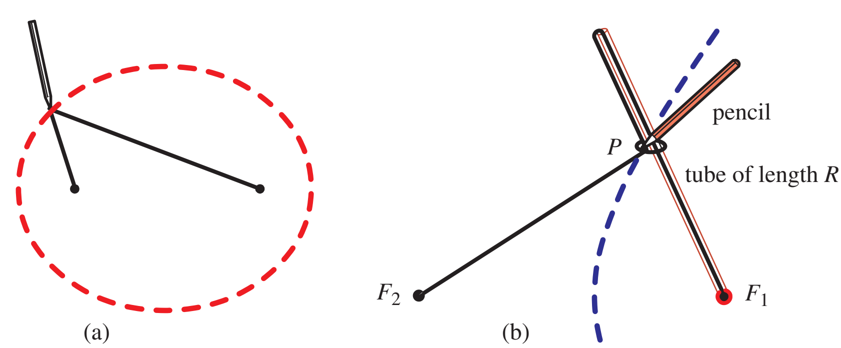


Figure 1 (a) String construction for the ellipse. (b) New mechanism for tracing a hyperbola. The pencil pushes inward along the outer edge of the tube.

The same string fastened to the same points can also be used to trace a hyperbolic arc with the same foci. How is this possible? The bifocal property of the hyperbola states that the *difference* of distances (longer minus shorter) from any point on the hyperbola to the foci is constant. Nevertheless, a slight modification of the string construction for the ellipse shows how to do it.

The points of intersection of an ellipse with the line through its foci are called its vertices. Take a thin rigid tube shorter than the string but longer than the distance from a focus to the nearest vertex. Pass part of the string through the tube and fasten the ends

Math. Mag. **84** (2011) 83–97. doi:10.4169/math.mag.84.2.083. © Mathematical Association of America

of the string to the foci as before. One end of the tube pivots at a focus, like one hand of a clock. The free end traces a circle that plays a crucial role in this paper. A pencil keeps the string taut by pushing it inward along the outer edge of the tube, as indicated in FIGURE 1b. If it pushes outward in the radial direction, the tube plays no role and the pencil traces part of the ellipse as in FIGURE 1a. But if it pushes inward as in FIGURE 1b, it traces a portion of a hyperbola lying inside the ellipse with the same foci, as in FIGURE 2a. This is easily verified by noting that the constant length c of the string is the sum of three distances in FIGURE 1b, the tube length R, plus $R - PF_1$ (the portion along the outside edge), plus focal distance PF_2. Therefore $PF_2 - PF_1 = c - 2R$, a constant.

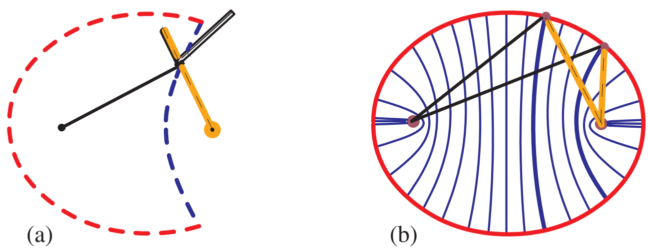


Figure 2 (a) The hyperbolic arc is inside the ellipse with the same foci. (b) If the length of the tube is varied, the pencil traces arcs of all confocal hyperbolas.

By varying the length of the tube you can draw an entire family of confocal hyperbolic arcs (FIGURE 2b). Because these arcs are confocal with the ellipse, they intersect it orthogonally. One of the arcs so constructed is the perpendicular bisector of the segment joining the foci.

Contents of this paper The string mechanism that weds the ellipse and hyperbola leads in a natural way to a generalization of the classical bifocal property, in which each focus is replaced by a circle, called a *focal circle*, centered at that focus. Focal circles extend the string construction by using two tubes, each pivoted at a focus; each free end traces a focal circle. Theorem 1 reveals that each of the sum and difference of distances to the focal circles can be constant on both the ellipse and hyperbola. Special pairs of focal circles, called *circular directrices*, are then introduced. Those familiar with paper-folding activities for constructing an ellipse or hyperbola using a circle as a guide, will be pleased to learn that the guiding circle is, in fact, a circular directrix. This is followed by an extended bifocal property for the ellipse and hyperbola, a converse to Theorem 1.

Although a parabola has only one focus, the extended bifocal properties of the ellipse and hyperbola can be transferred to a parabola by moving one focus to ∞. In the limit, a circular directrix centered at the moving focus becomes the classical directrix of the parabola. An application is also given to a pursuit problem involving conics.

Focal circles for ellipse and hyperbola

FIGURE 3 shows a string mechanism generalizing that in FIGURE 1b for tracing both elliptic and hyperbolic arcs with the same foci. This involves two tubes, each pivoting around a focus. The free end of each tube traces a circle that we call a *focal circle*. The focal circles may or may not intersect, and one of them might lie inside the other. The example in FIGURE 3 shows them intersecting. Join the foci with a string of constant length which passes through the two tubes. A new feature, not needed in FIGURE 1b, is the introduction of a ring to insure that the pencil keeps the string taut at the intersection of the radial directions. The four diagrams in FIGURE 3 show how the mechanism works in different parts of the plane determined by the intersecting focal circles.

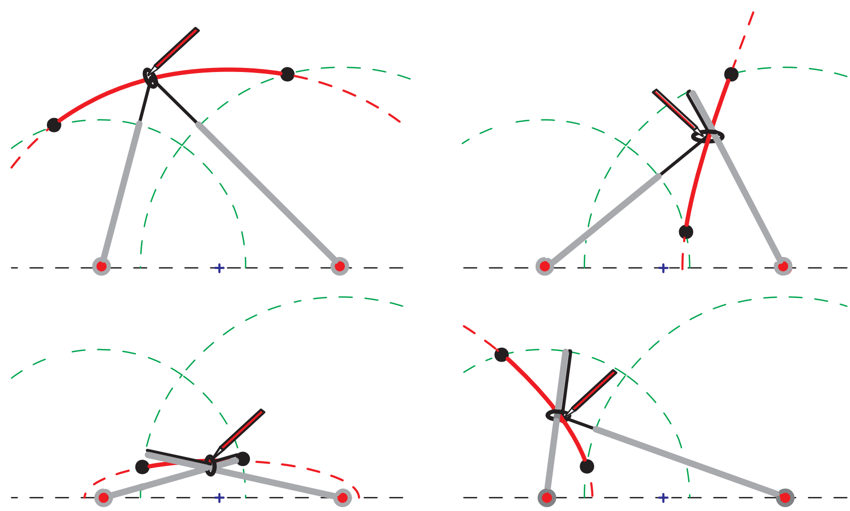


Figure 3 String mechanism involving two tubes. A wedding ring keeps the string taut at the intersection of the radial directions.

What is the locus traced by continuous motion of this string mechanism?

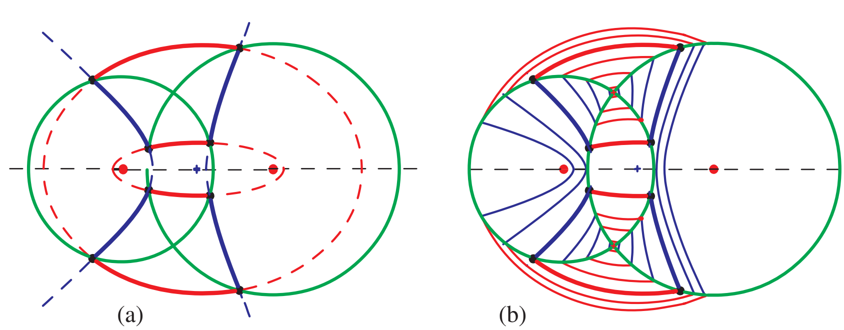


Figure 4 (a) A curvilinear trapezoid and its mirror image, each traced by one continuous motion of the two-tube string mechanism. (b) A family of trapezoids obtained by varying the length of the portion of the string outside the tubes.

The result, which may seem surprising, is a curvilinear 'trapezoid' bounded by elliptic and hyperbolic arcs, as shown in FIGURE 4a. FIGURE 4b shows a family of curvilinear trapezoids obtained by varying the length of the portion of the string outside the tubes.

To analyze the situation more precisely, refer to FIGURE 5 which shows two distinct points F_1 and F_2 that will serve as foci for an ellipse or a hyperbola. Draw two coplanar circles C_1 and C_2, which are the focal circles, centered at the foci with respective radii $R_1 \geq 0$ and $R_2 \geq 0$.

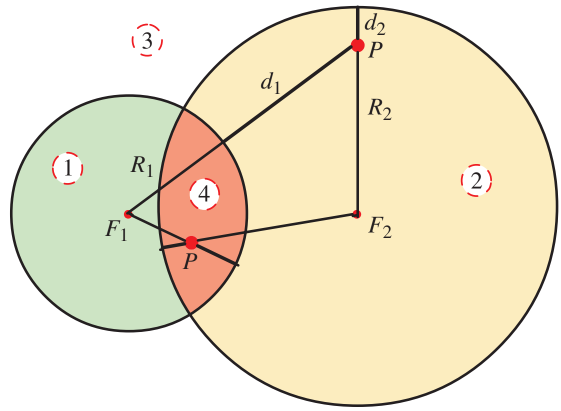


Figure 5 Two focal circles that divide the plane into four regions.

The example in FIGURE 5 shows two intersecting focal circles that divide the plane into four regions: region 1 inside C_1 and outside C_2, region 2 inside C_2 and outside C_1, region 3 outside both C_1 and C_2, and region 4 inside both C_1 and C_2. In some cases, one of regions 1, 2 or 4 may be empty.

FIGURE 4a shows a curvilinear trapezoid and its mirror image, each of which can be traced by the string mechanism in one continuous motion through all four regions in FIGURE 5. The upper trapezoid has two lower vertices on the boundary of region 4, and two upper vertices on the boundary of region 3. Place the pencil at the lower right vertex on circle C_1, moving it through region 4 to the lower left vertex on circle C_2. As we show later, this traces an arc of an ellipse (the lower edge of the trapezoid). Now continue the motion in region 1 to trace a hyperbolic arc (the left edge of the trapezoid), and then in region 3 to trace another elliptical arc (the upper edge of the trapezoid). Finally, return to the starting point by tracing another hyperbolic arc in region 2 (the right edge of the trapezoid). Theorem 1a will show that the length d of the portion of the string outside the tubes is the same constant on each edge of the trapezoid. By changing the value of d we obtain an entire family of trapezoids, as depicted in FIGURE 4b. As d shrinks to 0 the trapezoid becomes a point of intersection of the focal circles.

Two locus properties relating the ellipse and hyperbola

This section introduces two new and surprising locus properties relating the ellipse and hyperbola. Refer to the focal circles in FIGURE 5. Choose any point P in the plane of the circles, and let f_1 be the distance from P to focus F_1, and f_2 the distance from P to focus F_2. Also, let d_1, d_2 be the respective shortest distances from P to focal circles C_1 and C_2, each measured radially, so that $d = d_1 + d_2$ is the length of the portion of the string outside the tubes in the string mechanism. FIGURE 5 shows two choices of P, one in region 2, the other in region 4. We note that the following relations hold in FIGURE 5:

$$\text{In region 1, } d_1 = R_1 - f_1 \text{ and } d_2 = f_2 - R_2. \tag{1}$$

$$\text{In region 2, } d_1 = f_1 - R_1 \text{ and } d_2 = R_2 - f_2. \tag{2}$$

$$\text{In region 3, } d_1 = f_1 - R_1 \text{ and } d_2 = f_2 - R_2. \tag{3}$$

$$\text{In region 4, } d_1 = R_1 - f_1 \text{ and } d_2 = R_2 - f_2. \tag{4}$$

By adding d_1 and d_2 in each region we obtain:

LEMMA 1.

(1) *If P is in region* 1, *then* $d_1 + d_2 = (f_2 - f_1) - (R_2 - R_1)$.
(2) *If P is in region* 2, *then* $d_1 + d_2 = (f_1 - f_2) - (R_1 - R_2)$.
(3) *If P is in region* 3, *then* $d_1 + d_2 = (f_1 + f_2) - (R_1 + R_2)$.
(4) *If P is in region* 4, *then* $d_1 + d_2 = (R_1 + R_2) - (f_1 + f_2)$.

When $d_1 + d_2$ is constant, Lemma 1 reveals the following information about the curves traced by the string mechanism:

In region 1, $f_2 - f_1$ is constant and P traces part of a hyperbola with foci F_1 and F_2. In FIGURE 4a, this part is shown as two solid arcs on the left branch of this hyperbola.

In region 2, $f_1 - f_2$ is a different constant and P traces part of a different hyperbola with the same foci. In FIGURE 4a, this part is shown as two solid arcs on the right branch of the second hyperbola.

In region 3, $f_1 + f_2 = R_1 + R_2 + d_1 + d_2 = c$, the length of the string, and P traces part of an ellipse, shown in FIGURE 4a as two solid elliptical arcs.

In region 4, the constant focal sum $f_1 + f_2$ differs from that in region 3, and P traces two solid arcs of the smaller ellipse shown in FIGURE 4a.

By subtracting distances d_1 and d_2 in each region, we obtain:

LEMMA 2.

(1) *If P is in region* 1, *then* $d_2 - d_1 = (f_1 + f_2) - (R_1 + R_2)$.
(2) *If P is in region* 2, *then* $d_1 - d_2 = (f_1 + f_2) - (R_1 + R_2)$.
(3) *If P is in region* 3, *then* $d_1 - d_2 = (f_1 - f_2) - (R_1 - R_2)$.
(4) *If P is in region* 4, *then* $d_2 - d_1 = (f_1 - f_2) - (R_1 - R_2)$.

When $|d_1 - d_2|$ is constant, Lemma 2 reveals the following information about the curves traced by the string mechanism:

In regions 1 and 2, the focal sum $f_1 + f_2 = R_1 + R_2 + |d_1 - d_2|$ is constant, so P traces an elliptical arc. Each of these arcs, shown dashed in FIGURE 4a, is a continuation of a corresponding solid elliptical arc in FIGURE 4a, because their focal sums agree at those points where the arcs intersect the focal circles.

A similar analysis shows that each dashed hyperbolic arc in regions 3 and 4 of FIGURE 4a is a continuation of a corresponding solid hyperbolic arc in regions 1 and 2.

Thus, from Lemmas 1 and 2 we deduce:

THEOREM 1.

(a) *The locus of points P such that $d_1 + d_2$ is constant is part of an ellipse or a hyperbola.*
(b) *The locus of points P such that $|d_1 - d_2|$ is constant is part of an ellipse or a hyperbola.*

Proof. Part (a) follows from Lemma 1, and part (b) from Lemma 2. ■

Theorem 1 uncovers the surprising fact that use of focal circles allows each of $d_1 + d_2$ and $|d_1 - d_2|$ to be constant on both the ellipse and hyperbola.

Circular directrices for the ellipse and hyperbola Unlike central conics (ellipse and hyperbola), which have two foci, a parabola has only one focus F. It can be described as the locus of a point P that moves in a plane with its focal distance PF always equal to its distance PD from a fixed line D, called its directrix. Now we introduce an analogous equidistant property for central conics, using two special focal circles with the property that *from each point of the central conic, the shortest distances to the two focal circles are equal.* If such focal circles exist, we call them *circular directrices*. Now we will show that Lemma 2 implies that they *do* exist and tells us how to determine them.

A point P is equidistant (equal shortest distances) from the two focal circles if, and only if, $d_1 = d_2$. According to Lemma 2, this happens in regions 1 and 2 of FIGURE 5 when $R_1 + R_2 = f_1 + f_2$, and the same occurs in regions 3 and 4 when $R_1 - R_2 = f_1 - f_2$.

On an ellipse, the constant sum $f_1 + f_2$ represents the length of the major axis of the ellipse, while on a hyperbola the constant difference $|f_1 - f_2|$ represents the length of the transverse axis. This gives us the following:

DESCRIPTION OF CIRCULAR DIRECTRICES. *Any two focal circles with sum of radii $R_1 + R_2 = f_1 + f_2$ serve as a pair of circular directrices for the ellipse; any two focal circles with $|R_1 - R_2| = |f_1 - f_2|$ serve as a pair of circular directrices for the hyperbola.*

Each central conic has *infinitely many pairs* of circular directrices. FIGURE 6 shows three pairs of circular directrices for a given ellipse. In (a), $R_1 = 0$, C_1 becomes focus F_1, and $R_2 = f_1 + f_2$, so the entire ellipse lies inside focal circle C_2, hence in region 2. Each point on the ellipse is equidistant from focus F_1 and from this particular focal circle C_2, as depicted in FIGURE 6a. This circular directrix C_2 is used in standard paper-folding constructions for the ellipse. It was also used by Feynman [**2**, p. 152] in his geometric treatment of Kepler's laws of planetary motion.

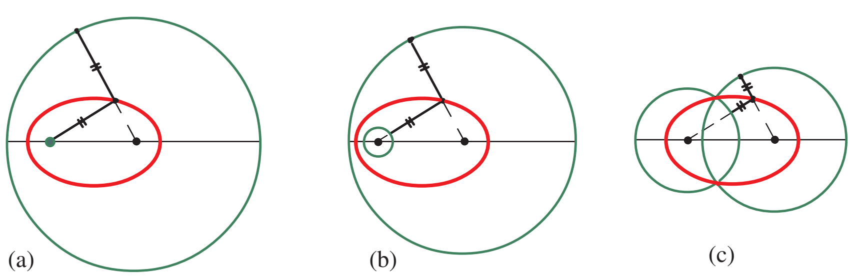


Figure 6 An ellipse and three pairs of its circular directrices. In (a), $R_1 = 0$ and $R_2 = f_1 + f_2$. In (b) and (c), $R_1 > 0$ and $R_2 = f_1 + f_2 - R_1$. For each P on the ellipse, the shortest distances d_1 and d_2 to the focal circles are equal.

In FIGURES 6b and 6c, both circular directrices have positive radii, but the sum of the radii is constant, so an increase in R_1 results in a corresponding decrease in R_2. In FIGURE 6b, the entire ellipse is in region 2, but in FIGURE 6c part of the ellipse is in region 2 and the remaining part in region 1.

FIGURE 7 shows three pairs of circular directrices for one given branch of a hyperbola. In FIGURE 7a, $R_1 = 0$ and $R_2 = f_2 - f_1$. This circular directrix is used in standard paper-folding constructions for the hyperbola. In FIGURES 7b and 7c, $R_1 > 0$ and $R_2 = f_2 - f_1 + R_1$, so an increase in R_1 results in a corresponding increase in R_2.

One may very well ask *"What about the other branch of the hyperbola?"*

FIGURE 8 shows both branches and reveals something new. From any point P there are *two* distances to each focal circle, the *shortest* distances, which we have denoted by d_1 and d_2, and the *longest* distances, which we denote by D_1 and D_2. The difference $D_i - d_i$ is $2R_i$, the diameter of focal circle C_i. The longest distance D_2 plays a role on the second branch. FIGURE 8a shows both branches of the hyperbola in FIGURE

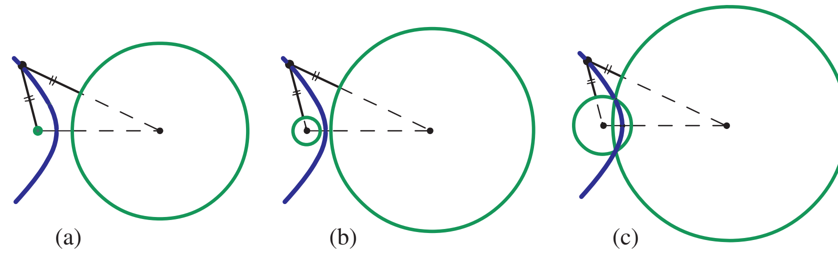


Figure 7 One branch of a hyperbola and three pairs of its circular directrices. In (a), $R_1 = 0$, $R_2 = f_2 - f_1$. In (b) and (c), $R_1 > 0$, $R_2 = f_2 - f_1 + R_1$. For each P on the hyperbola, the shortest distances d_1 and d_2 to the focal circles are equal.

7a, labeled as H_1. Here we have $d_1 = D_2$ on the second branch. In other words, the shortest distance to C_1 is equal to the longest distance to C_2. In this case, $C_1 = F_1$ because $R_1 = 0$.

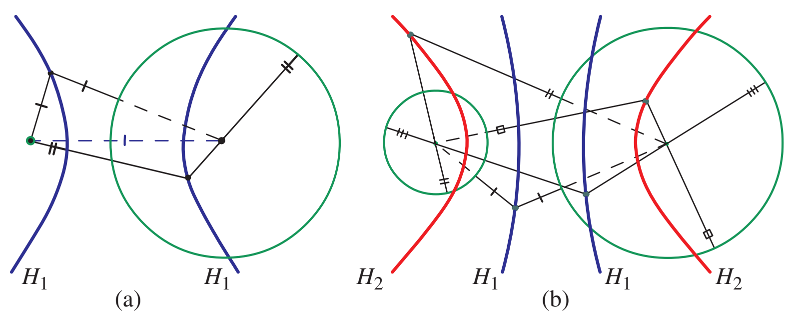


Figure 8 (a) Both branches of hyperbola in FIGURE 7a. For each P on the right branch the shortest distance d_1 is equal to the longest distance D_2. (b) Two confocal hyperbolas H_1 and H_2 with transverse axes of different lengths.

But when $R_1 > 0$ and $R_2 = f_2 - f_1 + R_1$, a new phenomenon occurs. A second hyperbola comes into play with the same foci but with a different transverse axis, as shown in FIGURE 8b. Let H_1 denote the hyperbola with the shorter transverse axis, and H_2 the one with the longer. Each point on the left branch of H_1 has $d_1 = d_2$, as in FIGURE 7, but each point on the right branch of H_1 has $D_1 = D_2$. On the left branch of H_2 we have $D_1 = d_2$, and on the right branch of H_2 we have $d_1 = D_2$, as indicated by tick marks in FIGURE 8b. Circular directrices play a deeper role than indicated in FIGURE 6.

This is illustrated further in FIGURE 9a, which can be thought of as a continuation of FIGURE 8b. As radius R_2 increases, the asymptotes of hyperbola H_2 become more and more horizontal until R_2 reaches a critical value for which H_2 degenerates to a pair of rays emanating from the foci. For points on the degenerate hyperbola, $|f_2 - f_1|$ is the distance between the foci, which is also $f_1 + f_2$, the sum of focal distances from points on the line segment joining the foci. This segment is a degenerate ellipse. As R_2 increases beyond the critical value and the circular directrices C_1 and C_2 intersect as shown in FIGURE 9a, hyperbola H_2 in FIGURE 8b is replaced by a confocal ellipse E_2 on which $d_1 = d_2$. On the left branch of H_1 we have $d_1 = d_2$, and on its right branch we have $D_1 = D_2$, as in FIGURE 8b. As radius R_2 increases further, so that C_2 contains C_1 in its interior, as in FIGURE 9b, hyperbola H_1 also degenerates and is replaced by a second confocal ellipse E_1 on which $d_1 = d_2$.

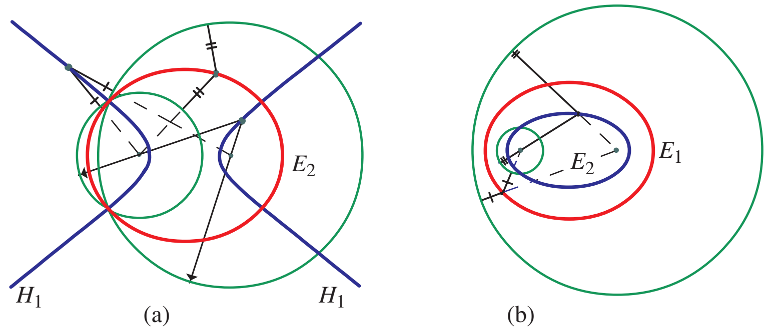


Figure 9 (a) Hyperbola H_2 in FIGURE 8b is replaced by ellipse E_2. (b) Hyperbolas H_1 and H_2 in FIGURE 8b are replaced by ellipses E_1 and E_2, respectively.

Extended bifocal property of the ellipse and hyperbola

The next theorem provides an extended bifocal property which has the same form for the ellipse and for the hyperbola. It is stated in terms of the shortest distances d_1, d_2 to the focal circles. Recall that the sum of focal distances $f_1 + f_2$ from any point on a ellipse to its foci is a constant equal to the length of the major axis, which we denote by A. On a hyperbola, the difference $|f_1 - f_2|$ of focal distances is another constant equal to the length of the transverse axis, which we denote by B. On the left branch (enclosing focus F_1) we have $f_2 - f_1 = B$, and on the other branch we have $f_1 - f_2 = B$.

THEOREM 2.

(a) *Given an ellipse with major axis of length A, and given two focal circles C_1, C_2 of radii R_1, R_2. Let $d = R_1 + R_2 - A$. Then each point on the ellipse satisfies*

$$d_1 + d_2 = |d| \tag{5}$$

or

$$|d_1 - d_2| = |d|. \tag{6}$$

(b) *Given a hyperbola with transverse axis of length B, and given the same focal circles as in (a). Let $d' = B - (R_1 + R_2)$. Then each point on the left branch of the hyperbola satisfies*

$$d_1 + d_2 = |d'| + 2R_1 \tag{7}$$

or

$$|d_1 - d_2| = |d'| + 2R_1. \tag{8}$$

Each point on the right branch satisfies

$$d_1 + d_2 = |d'| + 2R_2 \tag{9}$$

or

$$|d_1 - d_2| = |d'| + 2R_2. \tag{10}$$

If $R_1 = R_2$, then on both branches we have $d_1 + d_2 = B$ or $|d_1 - d_2| = B$.

Proof of (a). We consider two cases, depending on the algebraic sign of d.

Case 1. $d \le 0$, so $R_1 + R_2 \le A$. If both focal circles lie inside the ellipse, then $d_1 = f_1 - R_1$ and $d_2 = f_2 - R_2$, hence $d_1 + d_2 = f_1 + f_2 - (R_1 + R_2) = A - (R_1 + R_2) = -d = |d|$, so (5) holds on the entire ellipse.

If the ellipse intersects a focal circle, say C_1, then at the point of intersection we have $d_1 = 0$, $f_1 = R_1, d_2 = f_2 - R_2 = A - f_1 - R_2 = A - (R_1 + R_2) = -d = |d|$, hence both (5) and (6) are satisfied at this point. But Lemma 2 shows that for this value of d, (6) holds for every point of the ellipse in regions 1 or 2. A similar argument works if the ellipse intersects focal circle C_2. This proves (a) in Case 1.

Case 2. $d > 0$, so $R_1 + R_2 > A$. Now the focal circles intersect each other and also intersect the ellipse. At a point where C_1 intersects the ellipse we have $d_1 = 0$, $f_1 = R_1, d_2 = f_2 - R_2 = A - f_1 - R_2 = A - (R_1 + R_2) = -d$, hence $d_1 - d_2 = d = |d|$ at the point of intersection. But Lemma 2(1) shows that $d_1 - d_2 = d$ for every point of the ellipse in region 1, and that $d_2 - d_1 = d$ in region 2. Also, Lemma 1(4) shows that $d_1 + d_2 = d$ for every point of the ellipse in region 4. This proves (a) in Case 2. ■

Proof of (b). On a hyperbola $|f_1 - f_2|$ is constant, so $B = |f_1 - f_2|$. Again we consider two cases, depending on the relation between B and $R_1 + R_2$.

Case 1. $B \geq R_1 + R_2$. In this case the focal circles do not intersect, and at most one of them can intersect the hyperbola. If neither focal circle intersects the hyperbola, then $f_1 = R_1 + d_1$ and $f_2 = R_2 + d_2$, hence $d_1 - d_2 = f_1 - f_2 + R_2 - R_1$, which is the same as $d_2 - d_1 = f_2 - f_1 + R_1 - R_2$. On the left branch, $f_1 < f_2$, so $f_2 - f_1 = B$ and $d_2 - d_1 = B + R_1 - R_2 = B - (R_1 + R_2) + 2R_1$, so (8) is satisfied everywhere on this branch.

On the right branch, $f_2 < f_1$, so $f_1 - f_2 = B$ and $d_1 - d_2 = B + R_2 - R_1 = B - (R_1 + R_2) + 2R_2$, so (10) is satisfied everywhere on this branch.

Now suppose that one focal circle, say C_1, intersects the hyperbola. At a point of intersection we have $d_1 = 0$, $R_1 = f_1$ so $d_2 - d_1 = f_2 - R_2 = f_2 - f_1 + R_1 - R_2 = B + R_1 - R_2 = B - (R_1 + R_2) + 2R_1$. By Lemma 2(3), $d_2 - d_1$ has the same value everywhere in region 3, hence (8) holds everywhere in region 3. Now by Lemma 1(1), in region 1 we have $d_1 + d_2 = f_2 - f_1 - R_2 + R_1 = B - (R_1 + R_2) + 2R_1$, so (7) holds everywhere in region 1. Therefore either (7) or (8) holds on the left branch, whereas (10) holds everywhere on the right branch. If, however, focal circle C_2 intersects the hyperbola, then the same type of argument shows that either (9) or (10) holds on the right branch, and (8) holds everywhere on the left branch. This proves (b) in Case 1.

Case 2. $B < R_1 + R_2$. In this case the focal circles overlap and each intersects the hyperbola. The same type of argument used for Case 1 shows that, on the left branch, (7) holds in regions 3 and 4, and (8) holds in region 1. Similarly, on the right branch, (9) holds in regions 3 and 4, and (10) holds in region 2. ■

Bifocal properties transferred to the parabola

The extended bifocal properties of the central conics were obtained by replacing each focus by a focal circle. Although the parabola has only one focus, we can transfer the extended bifocal properties to the parabola by keeping one focal circle fixed and moving the second focus to ∞, allowing the radius of the second focal circle to increase without bound. The second focal circle now becomes a line perpendicular to the focal axis, which we call a *floating focal line*. The central conic becomes a parabola whose focus is the center of the fixed focal circle, and whose directrix is parallel to the floating focal line. As expected, the bifocal properties of the central conics can be transferred to the focal circle and the floating focal line.

This process is consistent with the geometric definition of conics as sections of a cone. Recall that a plane cutting one nappe of a right circular cone produces an ellipse.

As the plane is tilted to become nearly parallel to a generator of the cone, the ellipse becomes more elongated, and when the cutting plane is parallel to a generator the intersection becomes a parabola. Tilt the plane even further so it cuts both nappes, and the intersection is a hyperbola. Thus, as a section of a cone, the parabola is a transition between the ellipse and hyperbola, so it's not surprising that properties of the parabola can be obtained as limiting cases of those of a central conic.

First we introduce the parabolic version of circular directrices. For central conics, circular directrices occur in pairs, each a special focal circle. In the parabolic version, one of the circular directrices is replaced by a limiting line called a floating directrix.

Pairs of circular and floating directrices for the parabola Recall that a parabola has only one focus F, and is the locus of a point P that moves in a plane with its focal distance PF always equal to its distance PD from a fixed line D, called its directrix (FIGURE 10a). We call D the *linear directrix* of the parabola, to distinguish it from *circular directrices*, which we define as follows. Any line L parallel to directrix D we call a *floating focal line*. In FIGUREs 10b and 10c, L is between F and D. Let R denote the distance between L and D. Then the focal circle $C(R)$ of radius R and center F is called a *circular directrix* for the parabola, *relative to* L. In this context, line L is also called a *floating directrix* corresponding to the circular directrix. This terminology was chosen because for every point P on the parabola we have $d_C = d_L$, where d_C is the shortest distance from P to focal circle $C(R)$, and d_L is the distance from P to L. This common distance is $PF - R$, as shown in FIGURES 10b and 10c. *When the radius of C is zero, circular directrix C becomes the focus of the parabola, and floating directrix L becomes its classical directrix D,* as in FIGURE 10a.

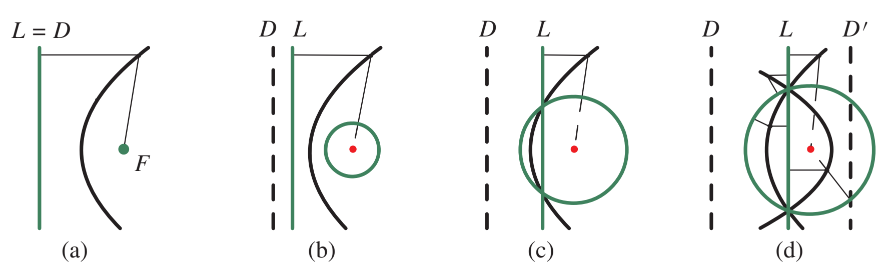


Figure 10 (a) Focus and directrix of a parabola. In (b)–(d), circular directrix and floating directrix. In (d), two intersecting confocal parabolas with linear directrices D and D', but with the same circular directrix and floating directrix.

As expected, each circular directrix of a parabola can be obtained as the limiting case of a circular directrix of a central conic by sending one of the foci to ∞. To illustrate, begin with an ellipse and two circular directrices C_1, C_2, as in FIGURE 6b or 6c, where $d_1 = d_2$ for each point on the ellipse. Let Q be the point where circle C_2 intersects the focal axis. Keep F_1, R_1 and Q fixed, and move focus F_2 along the focal axis arbitrarily far away, so that $R_2 \to \infty$. Then, the limiting circle C_2 becomes a line L through Q perpendicular to the focal axis. The radial distance d_2 becomes d_L, the distance from P to L, and the ellipse becomes a limit curve with the property that $d_1 = d_L$ at each of its points. This limit curve is, in fact, a parabola with focus F_1 and linear directrix D, whose distance from L is R_1, because each of its points is equidistant from F_1 and D. The circular directrix C_1 for the ellipse is now a circular directrix for the parabola with L as its floating directrix. The parabola opens to the right, as in FIGURES 10b and 10c. The initial choice of Q determines the position of the floating directrix L.

We can arrive at the same circular directrix and the same floating directrix L by starting with the left branch of the hyperbola shown in FIGURE 7, keeping F_1, R_1 and Q fixed as before, and letting $R_2 \to \infty$. If Q is between F_1 and the vertex of the left branch, as in FIGURE 7c, the limit curve is a parabola that opens to the left and intersects the first parabola, as shown by the example in FIGURE 10d, with its linear directrix D' parallel to L. Both parabolas intersect the floating directrix L and the circular directrix at the same points.

Parabolic version of the extended bifocal properties The extended bifocal properties of central conics in Theorems 1 and 2 have counterparts for the parabola. They can be obtained by starting with two focal circles C_1 and C_2 of a central conic, and letting the radius of one of them, say R_2, go to ∞, keeping F_1, R_1, and Q fixed, as was done earlier. The limiting C_2 becomes a floating focal line L through Q perpendicular to the focal axis, and the limiting central conic becomes a parabola with focus F_1 and focal circle C_1. The new properties relate C_1 and L.

FIGURE 11a shows what happens to FIGURE 5 in this limiting case, and FIGURE 11b shows how the four central conics in FIGURE 4a become four parabolas. On the solid portions of the parabolas, the sum of distances $d_1 + d_L$ to the focal circle and the floating focal line is constant, just as on the corresponding ellipses and hyperbolas in FIGURE 4a. On the dashed portions, the absolute difference $|d_1 - d_L|$ is constant, just as on the corresponding central conics in FIGURE 4a. FIGURE 11b also illustrates the following parabolic counterparts of Theorems 1 and 2, whose proofs are omitted.

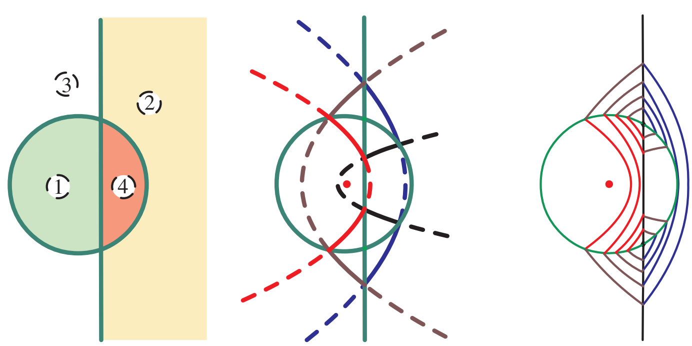


Figure 11 (a) Four regions formed by a focal circle and a coplanar line. (b) Limiting case of FIGURE 4a when the ellipses and hyperbolas become four parabolas. (c) Family of parabolic trapezoids obtained as limiting case of FIGURE 4b.

THEOREM 3. *Given a circle C with center at F, and a coplanar line L. If P is in the plane of C and L, let d_C and d_L denote the shortest distances from P to C and L, respectively. Then the locus of points P such that either the sum $d_C + d_L$ or the absolute difference $|d_C - d_L|$ is constant is part of a parabola with focus F and directrix parallel to L.*

THEOREM 4. *Given a parabola with a focal circle C, and given any line L parallel to its directrix D, whose distance from D is the radius of C. Then either the sum $d_C + d_L$ or the absolute difference $|d_C - d_L|$ is constant.*

String construction for the parabola When focal circle C has radius 0, the property that $d_C + d_L$ is constant reduces to $d_F + d_L$ is constant, and leads to a string construction for the parabola, illustrated in FIGURE 12a. One endpoint of a string of constant length is fastened to a fixed point, but the other end is attached to a small ring that slides freely along a rigid rod (a fixed line) that may or may not pass through the fixed point. Again, the string is kept taut by a pencil that moves so that the sum of distances from the pencil to the fixed point and to the fixed line is the constant length of the string. The pencil traces a portion of a parabola with the fixed point as its focus. A second parabola with the same focus can be drawn by placing the pencil on the other side of the fixed line, as indicated in FIGURE 12a. Kepler [**3**, p. 110] devised a similar string construction for the parabola that does not use a ring and produces only one of the two parabolas. Our construction for two confocal parabolas is justified by the diagram in FIGURE 12b, which shows the common circular directrix of the two parabolas with the fixed line as floating directrix.

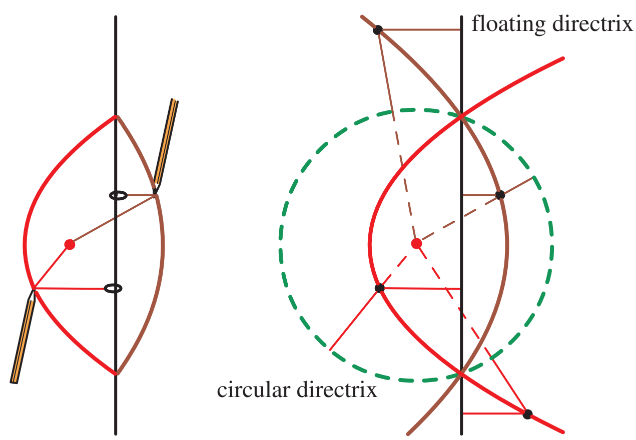


Figure 12 (a) String construction that gives two confocal parabolas, one on either side of the fixed line. (b) Justification of construction, using the common circular directrix of the two parabolas, with the corresponding floating directrix.

FIGURE 13a shows an equivalent form of the string construction in FIGURE 12a with a focal circle C of radius $R > 0$ centered at F. Then $d_C = d_F - R$, and the constant sum $d_F + d_L$ is replaced by $d_C + d_L = d_F + d_L - R$, another constant. The small ring that moves freely around the rigid boundary of the focal circle allows the pencil to trace the parabolas in FIGURE 12. Similarly, the two tubes and the single ring in the string mechanism of FIGURE 3 could be replaced by two small rings (illustrated by two examples in FIGURE 13b) that move freely around the two focal circles, with

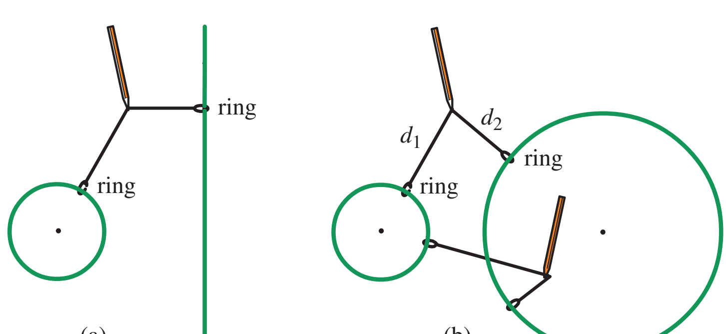


Figure 13 Alternative string construction (a) for parabolas, using a focal circle, and (b) for central conics, using two focal circles.

one end of the string attached to each ring. The pencil keeps the string taut so that the two portions of the string are in the appropriate radial directions.

Application of Theorem 3 to a pursuit problem A classical pursuit problem involves an aircraft flying at constant speed $v > 0$ from a given point A toward a fixed base F (FIGURE 14a). Because visibility is limited, an automatic pilot always aims the aircraft toward F. Ordinarily, the path would be along a straight line from A to F. However, a steady north wind with constant speed w forces the aircraft off course, so its trajectory is along a curved path which depends on the ratio of the speeds v and w. The problem is to determine this path.

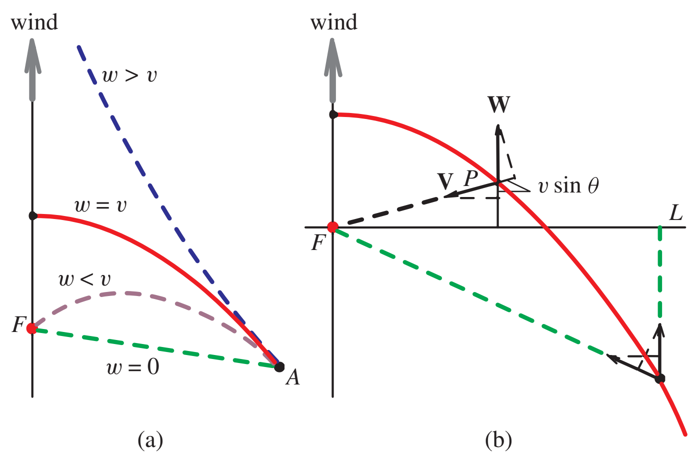


Figure 14 (a) Qualitative shape of trajectory depends on speeds v and w. (b) When $v = w$, the sum $d_F + d_L$ is constant above L, whereas $d_F - d_L$ is constant below L, hence the trajectory is a parabola with focus F.

If $w > v$, the craft cannot overcome the influence of the wind and moves further away from the base, approaching asymptotically the line due north from F. But if $v > w$, the aircraft overcomes the influence of the wind and returns to F along a curved path. These two solutions, which seem intuitively reasonable, can also be verified analytically by solving a suitable differential equation. The dashed curves in FIGURE 14a indicate the qualitative nature of the solutions. The line segment from A to F shows the path when $w = 0$.

The case of interest for us is when $w = v$. In this case the solution of the differential equation is part of a parabola, shown as the solid curve in FIGURE 14a. Point F is the focus of this parabola. The aircraft moves along the parabola until it is due north of F at which point it remains stationary because the effect of its speed and that of the wind cancel each other. We shall obtain this solution by applying Theorem 3.

Choose a line L through F perpendicular to the wind direction, as in FIGURE 14b. We regard L as a focal line, and let F serve as a focal point. Let P denote a general point on the path of the aircraft, and let d_F and d_L denote its distances from F and L, respectively, as indicated in FIGURE 14b. Line L divides the trajectory into two parts, one above L and one below. We will show that the sum $d_F + d_L$ is constant when P is above L, and that the difference $d_F - d_L$ is the same constant when P is below L. By Theorem 3 with $C = F$, this will prove that the path is a parabola with focus F.

Suppose P is above L. Let θ denote the angle between L and the line joining F to P. In general, point P moves along a tangent vector to the path with velocity $\mathbf{V} + \mathbf{W}$, the resultant of two vectors $\mathbf{V}$ and $\mathbf{W}$ of lengths $v = |\mathbf{V}|$ and $w = |\mathbf{W}|$. We are considering the case in which $w = v$. Vector $\mathbf{W}$, in the direction of the wind, acts to increase d_L at the time rate v. But $\mathbf{V}$ acts to decrease d_L by a component of magnitude $v \sin\theta$ opposite to $\mathbf{W}$. Hence the resultant $\mathbf{V} + \mathbf{W}$ has a component in the direction of $\mathbf{W}$ equal to $v - v\sin\theta$, which represents the time rate of change of d_L. Similarly, the component of the resultant in the direction of $\mathbf{V}$ is $v\sin\theta - v$, which represents the time rate of change of d_F. Therefore the time rate of change of the sum $d_F + d_L$ is zero, hence $d_F + d_L$ is constant. This constant is d_F when $d_L = 0$, and is the distance from F to the point where L intersects the trajectory.

When P is below L the analysis is similar, except that both $\mathbf{V}$ and $\mathbf{W}$ act to decrease d_L so the resultant $\mathbf{V} + \mathbf{W}$ has a component in the direction of $\mathbf{W}$ with magnitude $v + v\sin\theta$, whose negative is the time rate of change of d_L, and a component in the direction of $\mathbf{V}$ of the same magnitude, whose negative is the time rate of change of d_F. Therefore the time rate of change of the difference $d_F - d_L$ is zero, hence $d_F - d_L$ is constant, the same constant obtained when P is above L. This shows that the trajectory satisfies Theorem 3, so it is a parabola with focus at F.

Modified pursuit problem The problem can be modified so that the parabola is replaced by other conics. Specifically, suppose a wind of constant speed v blows radially outward from a given point F_0 different from F. This particular application may not conform to reality, but other more realistic physical situations can be imagined that involve the same ideas. In this case one can verify, with analysis similar to that given above, that the aircraft moves along a portion of an ellipse. If the wind blows radially inward toward F_0, then the aircraft moves along a portion of a hyperbola. In both cases the foci are at F_0 and F.

Concluding remarks

Replacing a focus of a conic by a focal circle is a very simple idea that has profound consequences. It allows us to obtain new characteristic properties of central conics and to extend them to a parabola, and *vice versa*.

The classical characterization of an ellipse as the locus of points whose sum of focal distances $f_1 + f_2$ is constant, and the hyperbola as the locus of points whose absolute distance $|f_1 - f_2|$ is constant, has been generalized to a common bifocal property $|d_1 \pm d_2|$ is constant, where d_1 and d_2 are the shortest distances from a point to the focal circles. By allowing the radius of one of the focal circles to become infinite, we obtained corresponding properties for the parabola. We also introduced special pairs of focal circles, called circular directrices, which provide equidistant properties for central conics analogous to the classical focus-directrix equidistant property for the parabola.

It should be mentioned that in an earlier paper [**1**] we replaced the foci of a central conic by circular *disks*, called focal disks, whose centers are not necessarily at the foci, and found a new set of properties that characterize the conics in terms of the sums and differences of tangent lengths to the focal disks. This characterization occurs naturally when the conics are regarded as sections of a twisted cylinder, of which the circular cone is a special case.

REFERENCES

1. Tom M. Apostol and Mamikon A. Mnatsakanian, New descriptions of conics via twisted cylinders, focal disks, and directors. *Amer. Math. Monthly* **115** (2008) 795–812.

2. David L. Goodstein and Judith R. Goodstein, *Feynman's lost lecture: the motion of planets around the sun*, Norton, New York, 1996.
3. Johannes Kepler, *New Astronomy*, translated by William H. Donahue, Green Lion Press, Santa Fe, NM, 2004.

Summary We introduce a string mechanism that traces both elliptic and hyperbolic arcs having the same foci. This suggests replacing each focus by a focal circle centered at that focus, a simple step that leads to new characteristic properties of central conics that also extend to the parabola.

The classical description of an ellipse and hyperbola as the locus of a point whose sum or absolute difference of focal distances is constant, is generalized to a common bifocal property, in which the sum or absolute difference of the distances to the focal circles is constant. Surprisingly, each of the sum or difference can be constant on both the ellipse and hyperbola. When the radius of one focal circle is infinite, the bifocal property becomes a new property of the parabola.

We also introduce special focal circles, called circular directrices, which provide equidistance properties for central conics analogous to the classical focus-directrix property of the parabola. Those familiar with paper-folding activities for constructing an ellipse or hyperbola using a circle as a guide, will be pleased to learn that the guiding circle is, in fact, a circular directrix.

TOM M. APOSTOL joined the Caltech faculty in 1950 and became professor emeritus in 1992. He is director of Project MATHEMATICS! (http://www.projectmathematics.com) an award-winning series of videos he initiated in 1987. His long career in mathematics is described in the September 1997 issue of the *College Mathematics Journal*. He is currently working with colleague Mamikon Mnatsakanian to produce materials demonstrating Mamikon's innovative and exciting approach to mathematics.

MAMIKON A. MNATSAKANIAN received a Ph.D. in physics in 1969 from Yerevan University, where he became professor of astrophysics. As an undergraduate he began developing innovative geometric methods for solving many calculus problems by a dynamic and visual approach that makes no use of formulas. He is currently working with Tom Apostol under the auspices of Project MATHEMATICS! to present his methods in a multimedia format.

The Bhaskara-Aryabhata Approximation to the Sine Function

SHAILESH A. SHIRALI
Community Mathematics Center, Rishi Valley School (KFI)
Rishi Valley 517 352, Andhra Pradesh, India
shailesh.shirali@gmail.com

Is it possible that well over a thousand years back, mathematicians knew of an approximation to the sine function that yields close to 99% accuracy, using a function that is simply a ratio of two quadratic functions? Such is the case, and the formula in question was found by the Indian mathematician Bhāskarā I: if $0 \leq x \leq 180$, then

$$\sin x^\circ \approx \frac{4x(180-x)}{40500 - x(180-x)}. \tag{1}$$

This article is about how one may find such a formula, and what makes it "tick."

Bhāskarā I (600–680) belonged to the school of mathematics established by the great Indian mathematician Āryabhaṭa (476–550). Āryabhaṭa lived in what has been called the golden age in India, when great advances were being made in fields as diverse as science, art, mathematics, astronomy, technology, and philosophy. The decimal numeration system and use of zero were developed during this period. Āryabhaṭa established a flourishing school of mathematics in northern India, but only one of his works has survived to modern times: the *Āryabhatīyā*, a terse compendium of results in arithmetic, algebra, areas of plane figures, volumes of solids, and astronomy—all set in Sanskrit verse. References to another work, the *Arya Siddhantha*, have been found in the works of later Indian mathematicians such as Varahamihira (500–587), Bhāskarā I himself, and Brahmagupta (598–670); but this work appears to be lost; see Plofker [**7**].

Bhāskarā I wrote valuable commentaries on Āryabhaṭa's work in mathematics and astronomy, and the lasting influence of Āryabhaṭa's work owes in no small measure to these expository works. (Historians have given him the designation "Bhāskarā I" in order to distinguish him from the later and much more famous Bhāskarā of Indian mathematics—Bhāskarā II, the twelfth century mathematician who wrote the lyrical work *Līlavati*.)

The *Āryabhatīyā* has a table of sine values, stated in a rather unfamiliar form. It is actually a table of first differences of chord lengths corresponding to different central angles, and stated in an alphabetic code invented by Āryabhaṭa himself. It also gives a recursive rule for computing these differences. The story of how the word used in that text for chord length, *jyā*, eventually morphed into the term used today, *sin*, over the course of a journey spanning six centuries and three continents, has been beautifully told by Eves; see [**2**, page 105].

Bhāskarā's formula (1) first appears in his book *Mahābhāskarīya*; he attributes it to Āryabhaṭa, but as there is no mention of the formula anywhere in the *Āryabhatīyā*, we shall refer to it as Bhāskarā's formula (though in the title of this article we do call it the Bhāskarā-Āryabhaṭa formula). As per the custom of the time, he stated the formula in stylized verse. Here is how it has been translated by Plofker in [**7**, p. 81]:

> The degree of the arc, subtracted from the total degrees of half a circle, multiplied by the remainder from that [subtraction], are put down twice. [In one place] they

Math. Mag. **84** (2011) 98–107. doi:10.4169/math.mag.84.2.98. © Mathematical Association of America

are subtracted from sky-cloud-arrow-sky-ocean [40500]; [in] the second place, [divided] by one-fourth of [that] remainder [and] multiplied by the final result [i.e., the trigonometric radius].

This prescription may be cast in a form more familiar to us. Let $f(x)$ be defined for real numbers x lying between 0 and 180, thus:

$$f(x) = \frac{4x(180-x)}{40500 - x(180-x)}.$$

(We ignore the bit about multiplication by the radius; this serves to give the chord length rather than the sine value. To be precise, if a chord has central angle θ in a circle of radius R, then its length is $2R\sin(\theta/2)$.) The approximation given by Bhāskarā I states that if $0 \le x \le 180$, then $\sin x^\circ \approx f(x)$.

From the form of f it is clear that $f(x) = f(180-x)$, so the formula captures the symmetry of the sine function about the 90° point. Here is a comparison of the values of $\sin x^\circ$ and $f(x)$, given to three significant figures, for some x-values:

x	0	15	30	45	60	75	90
$\sin x^\circ$	0	0.259	0.5	0.707	0.866	0.966	1
$f(x)$	0	0.260	0.5	0.706	0.865	0.965	1

We see a striking closeness between the two sets of values. It is clear that $f(x)$ yields a very good approximation to the sine function over the interval [0°, 180°]. See [**3**] for another such comparison of values.

As part of our study of this approximation, we give a heuristic derivation of the above function, and use various criteria to measure the degree of closeness of the intended approximation.

A simpler formulation

A change of origin and scale allows us to cast the problem in a more appealing way. We first note that

$$f(90-x) = \frac{4(90-x)(90+x)}{32400+x^2}, \qquad f(90-90x) = \frac{4(1-x^2)}{4+x^2}.$$

Since $\cos x^\circ = \sin(90-x)^\circ$, Bhāskarā's approximation (1) may be stated in an equivalent form as follows:

$$\text{For } -1 \le x \le 1,\ \cos 90x^\circ \approx \frac{4(1-x^2)}{4+x^2}.$$

For our purposes, a still more convenient form is obtained by switching to radian measure:

$$\text{For } -1 \le x \le 1,\ \cos\frac{\pi x}{2} \approx \frac{4(1-x^2)}{4+x^2}.$$

For convenience we shall refer to the function $B(x) := 4(1-x^2)/(4+x^2)$ as the *Bhāskarā function*. It is no good presenting the graphs of $C(x) := \cos \pi x/2$ and $B(x)$ on the same pair of axes, because the two graphs cannot be distinguished by the eye. We present them, instead, side by side (see FIGURE 1); their closeness is evident.

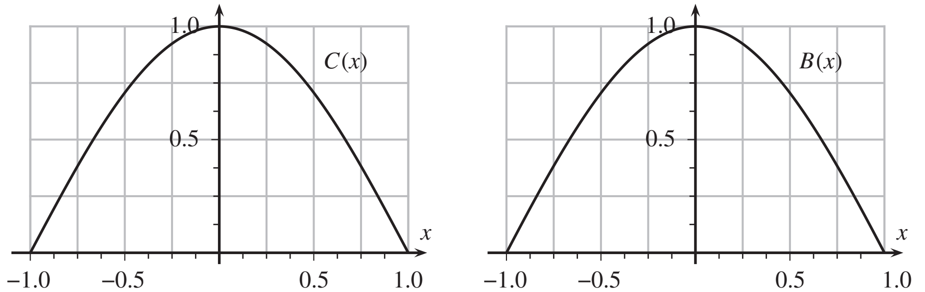


Figure 1 Graphs of $C(x) = \cos(\pi x/2)$ and $B(x) = 4(1 - x^2)/(4 + x^2)$

How good an approximation is it?

Various criteria may be used to assess how close two given functions are to each other. We make the following observations with regard to the two functions $C(x) = \cos \pi x/2$ and $B(x) = 4(1 - x^2)/(4 + x^2)$ defined on the interval $[-1, 1]$.

1. Both functions are even, and both are concave over $-1 \leq x \leq 1$. Their points of intersection with the two axes match exactly.
2. Other than $x = \pm 1$ and $x = 0$, the curves also intersect at $x = \pm 2/3$. (Indeed, these five values of x give all the points of intersection of the two curves.)
3. *Comparison of area.* The areas of the regions enclosed by the curves and the x-axis may be compared:

$$\int_{-1}^{+1} \cos \frac{\pi x}{2}\, dx = \frac{4}{\pi} \approx 1.27324,$$

$$\int_{-1}^{+1} \frac{4(1 - x^2)}{4 + x^2}\, dx = 20 \tan^{-1} \frac{1}{2} - 8 \approx 1.27295.$$

   The values compare favourably.
4. The slopes at the left endpoint are $C'(-1) = \pi/2 \approx 1.571$ and $B'(-1) = 1.6$.
5. FIGURE 2 shows the graph of $C(x) - B(x)$ over $-1 \leq x \leq 1$. We see that the maximum value of $|C(x) - B(x)|$ over this interval is roughly 0.0016. The plot has been made using *Mathematica*; use of its `FindRoot` function reveals that the maximum is achieved at $x \approx \pm 0.872$.

   FIGURE 3 shows the graph of the percentage error, $100(1 - B(x)/C(x))$, made in using $B(x)$ to estimate $C(x)$. Observe that the percentage error is largest for x close to ± 1. The use of L'Hôpital's rule shows that the percentage error tends to $|1 - 16/5\pi| \approx 1.9\%$ as $x \to \pm 1$. However, for $|x| < 0.9$, the error does not exceed 1%.
6. Using some of the known irrational values of the cosine function, we get moderately good rational approximations to these numbers, thus:

   - For $x = 1/2$ we get $C(x) = 1/\sqrt{2}$, $B(x) = 12/17$, hence $\sqrt{2} \approx 17/12$. The error is about 0.17%.
   - For $x = 1/3$ we get $C(x) = \sqrt{3}/2$, $B(x) = 32/37$, hence $\sqrt{3} \approx 64/37$. The error is about 0.13%.
   - For $x = 4/5$ we get $C(x) = (\sqrt{5} - 1)/4$, $B(x) = 9/29$, hence $\sqrt{5} \approx 65/29$. The error is about 0.24%.

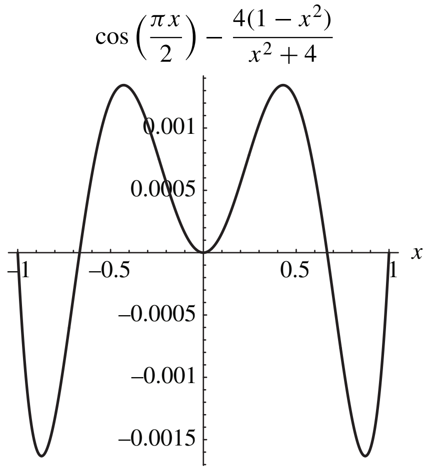


Figure 2 Graph of $C(x) - B(x)$ over $-1 \le x \le 1$

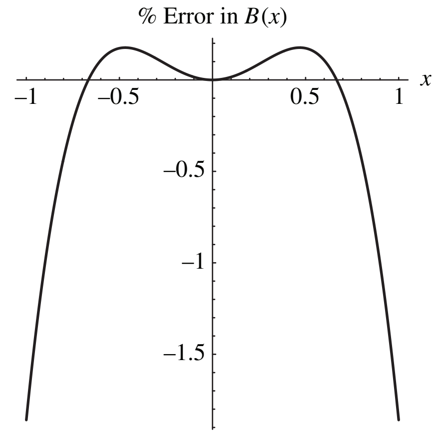


Figure 3 Graph of $100(1 - B(x)/C(x))$ over $-1 \le x \le 1$

The Padé approximant

To understand the relationship between the functions C and B a bit better, it helps to recall the basic facts about Padé approximants. Given a function f and integers $m, n \ge 0$, the *Padé approximant* of order (m, n) to f is that rational function

$$r(x) = \frac{p_0 + p_1 x + p_2 x^2 + \cdots + p_m x^m}{1 + q_1 x + q_2 x^2 + \cdots + q_n x^n}$$

for which $f(x)$ and $r(x)$ agree at $x = 0$ up to the $(m+n)$-th derivative; the $m + n + 1$ coefficients are found using these $m + n + 1$ conditions. (See [**1**] for details.) Padé approximants are very useful in numerical work, as they provide an efficient tool for computing the values of otherwise intractable functions. For example, over the interval $-0.5 \le x \le 0.5$, the exponential function e^x is extremely well approximated by its Padé approximant of order (3, 3),

$$\frac{120 + 60x + 12x^2 + x^3}{120 - 60x + 12x^2 - x^3},$$

the error never being more than 1 part in 10^7.

Let us now find the Padé approximant of order $(2, 2)$ for the function $C(x) = \cos \pi x/2$. As the function is even, we need to include only the even powers of x in the approximant. Hence $r(x)$ has the form

$$r(x) = \frac{a + bx^2}{1 + cx^2},$$

where the constants a, b, c are to be found. The zeroth, second and fourth derivatives of $C(x)$ evaluated at $x = 0$ are

$$1, \qquad -\frac{\pi^2}{4}, \qquad \frac{\pi^4}{16}.$$

(The odd order derivatives of $C(x)$ and $r(x)$, evaluated at $x = 0$, are all 0, so we do not need to worry about them.) The zeroth, second, and fourth derivatives of $r(x)$

evaluated at $x = 0$ are

$$a, \qquad 2(b - ac), \qquad 24c(ac - b).$$

So we want

$$a = 1, \qquad 2(b - ac) = -\frac{\pi^2}{4}, \qquad 24c(ac - b) = \frac{\pi^4}{16}.$$

Solving these equations for a, b, c we get:

$$a = 1, \qquad b = -\frac{5\pi^2}{48}, \qquad c = \frac{\pi^2}{48}.$$

Thus the desired function is

$$r(x) = \frac{48 - 5\pi^2 x^2}{48 + \pi^2 x^2}.$$

We see that Bhāskarā's function $B(x)$ is close to being a Padé approximant to $\cos \pi x/2$; but its coefficients are slightly different. It is therefore reasonable to ask how these two rational approximants compare with each other.

By design, $r(x)$ agrees with $\cos \pi x/2$ at $x = 0$ for derivatives up to order 4. However it does not do so well on other fronts. The intersections of the graph of $r(x)$ with the x-axis occur at $x = \pm c$ where $c = \sqrt{48/5\pi^2}$, i.e., at $x \approx \pm 0.9862$, which falls a bit short of ± 1. The area enclosed by the curve and the x-axis is

$$\int_{-c}^{+c} \frac{48 - 5\pi^2 x^2}{48 + \pi^2 x} \, dx \approx 1.2664.$$

The discrepancy between this and the true value (1.27324) is larger than for Bhāskarā's function $B(x)$.

FIGURE 4 shows the graph of $C(x) - r(x)$ over $-1 \le x \le 1$. We see that the curve lies above the x-axis (i.e., $C(x) - r(x) \ge 0$ for $-1 \le x \le 1$) and has a very flat portion around $x = 0$; this is clearly a consequence of the equality of the first four derivatives of $C(x)$ and $r(x)$ at $x = 0$. But outside this region the curve rises more steeply, and the maximum value of $|C(x) - r(x)|$ over $-1 \le x \le 1$, achieved at $x = \pm 1$, is

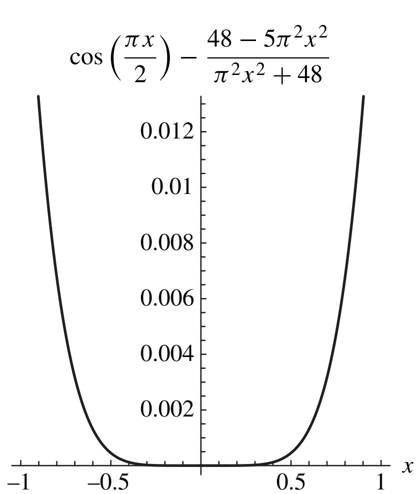


Figure 4 Graph of $\cos \pi x/2 - (48 - 5\pi^2 x^2)/(48 + \pi^2 x^2)$ over $-1 \le x \le 1$

much larger than the maximum value of $|C(x) - B(x)|$ over $-1 \leq x \leq 1$. (Indeed, $\max_{-1\leq x\leq 1} |C(x) - r(x)|$ is roughly 0.023, as compared to a maximum value of about 0.0016 for $|C(x) - B(x)|$.)

It is curious that Bhāskarā's function $B(x)$ out-performs the Padé approximant $r(x)$ on many counts.

Heuristic derivation of Bhaskara's function

We now show a heuristic way of arriving at Bhāskarā's function $B(x)$ as a rational approximation for $C(x) = \cos \pi x/2$ over the interval $-1 \leq x \leq 1$.

Since the graph of $C(x)$ over $-1 \leq x \leq 1$ is a concave arch passing through the points $(\pm 1, 0)$ and $(0, 1)$, a simple minded first approximation to $C(x)$ over the same interval is the function $1 - x^2$, whose graph shows the same features. But this function consistently yields an overestimate (except, of course, at $x = 0, \pm 1$); see FIGURE 5.

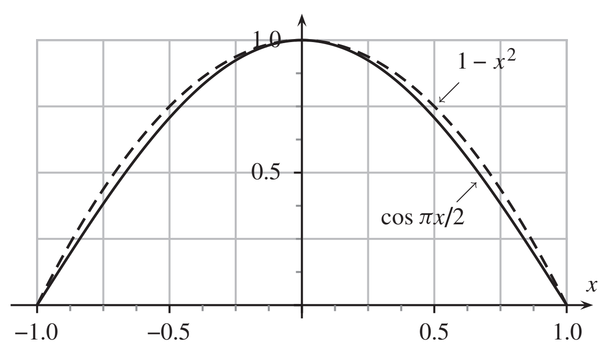


Figure 5 Graphs of $\cos(\pi x/2)$ and $1 - x^2$ over $-1 \leq x \leq 1$

In order to "fix" the overestimate, we examine the quotient

$$p(x) = \frac{1 - x^2}{\cos \pi x/2}$$

a little more closely. FIGURE 6 shows the graph of $p(x)$ for $-1 \leq x \leq 1$. Note that at $x = \pm 1$ the indeterminate form $0/0$ is encountered, but if we require p to be continuous at $x = \pm 1$ and use L'Hôpital's rule, then we get $p(\pm 1) = 4/\pi \approx 1.27$.

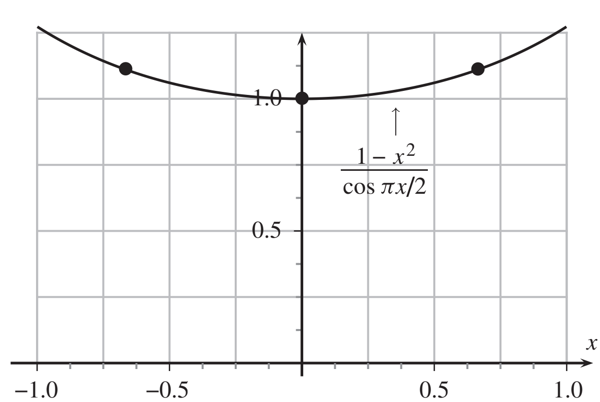


Figure 6 Graph of $(1 - x^2)/\cos(\pi x/2)$ over $-1 \leq x \leq 1$

(For fixing the overestimate, we could also study the reciprocal of $p(x)$, namely, the function $\cos(\pi x/2)/(1-x^2)$, rather than $p(x)$; but we opt for $p(x)$ as its graph has a more familiar shape and proves easier to approximate.)

The shape is strongly suggestive of a parabolic function, so let us look for such a function to fit the data. To this end we mark three points on the graph: (0, 1) and $(\pm 2/3, 10/9)$; conveniently for us, points with rational coordinates are available. For the parabola $y = d + ex^2$ to pass through them we must have $d = 1$ and $d + 4e/9 = 10/9$, giving $e = 1/4$. So the desired parabolic function is $y = 1 + x^2/4$, which means that we have the approximate relation

$$\frac{1-x^2}{\cos \pi x/2} \approx 1 + \frac{x^2}{4} \qquad (-1 \leq x \leq 1).$$

This leads right away to Bhāskarā's approximation, in which all the coefficients are rational numbers:

$$\cos \frac{\pi x}{2} \approx \frac{1-x^2}{1+x^2/4} = \frac{4(1-x^2)}{4+x^2}.$$

Adjustments using the Maclaurin series

Since the Maclaurin series for $C(x) = \cos \pi x/2$ about $x = 0$ is $1 - \pi^2 x^2/8 + \cdots$, while that of $B(x) = 4(1-x^2)/(4+x^2)$ about $x = 0$ is $1 - 5x^2/4 + \cdots$, the closeness of the two functions $C(x)$ and $B(x)$ for $-1 \leq x \leq 1$ may also be attributed to the approximate relation $\pi^2/8 \approx 5/4$ (which is equivalent to $\pi^2 \approx 10$).

Now the approximation $\pi^2 \approx 9.9$ is clearly better than $\pi^2 \approx 10$ (naturally, we prefer to use a rational approximation for π^2). Can we exploit this fact and improve on Bhāskarā's approximation, by replacing the '4' in that approximation by some suitable number a? The Maclaurin series for $a(1-x^2)/(a+x^2)$ about $x = 0$ is $1 - (1 + 1/a)x^2 + \cdots$, so we must solve the equation $1 + 1/a = 9.9/8$ for a; we get $a = 80/19$. This yields a new approximation:

$$B_1(x) := \frac{80(1-x^2)}{80+19x^2}.$$

Does this do better than Bhāskarā's approximation, $B(x)$? Contrary to expectation, it does not. It *does* do better on the interval $-0.5 \leq x \leq 0.5$; for example, for $x = 0.4$ we have:

$$\cos 0.2\pi \approx 0.8090, \qquad B(0.4) \approx 0.8077, \qquad B_1(0.4) \approx 0.8092.$$

But outside this interval, Bhāskarā's function continues to do better; for example, for $x = 0.8$ we have:

$$\cos 0.4\pi \approx 0.3090, \qquad B(0.8) \approx 0.3103, \qquad B_1(0.8) \approx 0.3125.$$

Approaches using the functional equation

Another approach, quite different in motivation, comes from the basic functional equation satisfied by the cosine function: $\cos 2x = 2\cos^2 x - 1$. This suggests that a possible criterion for closeness between a candidate function $g(x)$ and the cosine function $C(x)$, on the interval $[-1, 1]$, is the closeness between $g(x)$ and $2\,(g(x/2))^2 - 1$, on the same interval. Invoking the least-squares philosophy, we could look for a function g, within some well-defined class, which minimizes the quantity

$$\int_{-1}^{+1} \left(g(x) - 2(g(x/2))^2 + 1\right)^2 \, dx.$$

We shall stick to functions $g(x)$ of the type $(a + bx^2)/(c + x^2)$ which satisfy the boundary conditions $g(0) = 1$, $g(\pm 1) = 0$; these imply that $a = c$, $b = -a$. So our class consists of all the functions $g(x, a)$ of the type

$$g(x, a) := \frac{a(1 - x^2)}{a + x^2},$$

where a is a real number.

Analytically attempting to find the value of a that minimizes the function

$$k(a) := \int_{-1}^{+1} \left(g(x, a) - 2(g(x/2, a))^2 + 1\right)^2 \, dx$$

leads to decidedly unpleasant expressions, so we opt instead to do it numerically, using *Mathematica*. (We can use *Mathematica*'s `FullSimplify` command to get $k(a)$ in closed form, but the form is so forbidding that our aspirations for a closed form minimization quickly cool down.) FIGURES 7 and 8 display plots of $k(a)$ for $1 \le a \le 6$ and $3.8 \le a \le 4.8$, respectively, obtained using this CAS. We see that a minimum value of $k(a)$ occurs near $a = 4.3$. Use of the `FindRoot` function of *Mathematica* allows us to get this value more precisely; it is roughly 4.294.

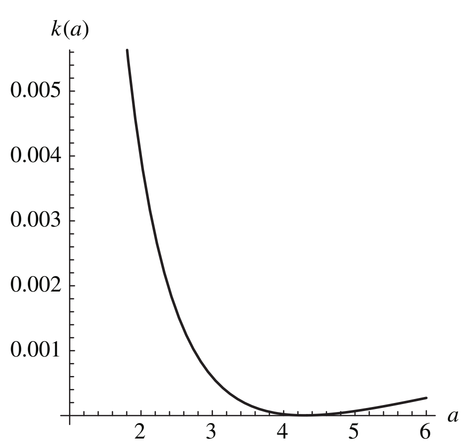


Figure 7 Plot of $k(a)$ for $1.0 \le a \le 6.0$

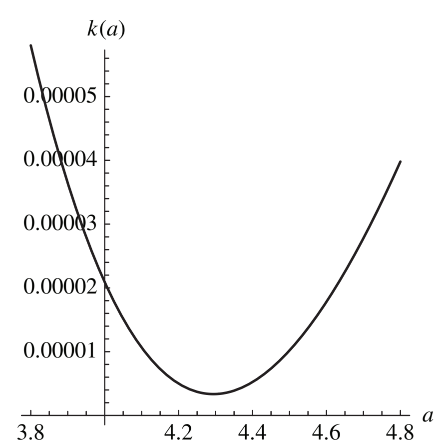


Figure 8 Plot of $k(a)$ for $3.8 \le a \le 4.8$

This idea can be extended by recalling another functional equation satisfied by the cosine function: $\cos 3x = 4\cos^3 x - 3\cos x$. Now we seek the value of a that minimizes the following function $j(a)$:

$$j(a) := \int_{-1}^{+1} \left(g(x, a) - 4(g(x/3, a))^3 + 3g(x/3, a)\right)^2 \, dx.$$

A plot of $j(a)$ for $4.0 \le a \le 4.8$ is shown in FIGURE 9. Once again, we use the `FindRoot` function to find more precisely the minimizing value of a; it is found to be roughly 4.366.

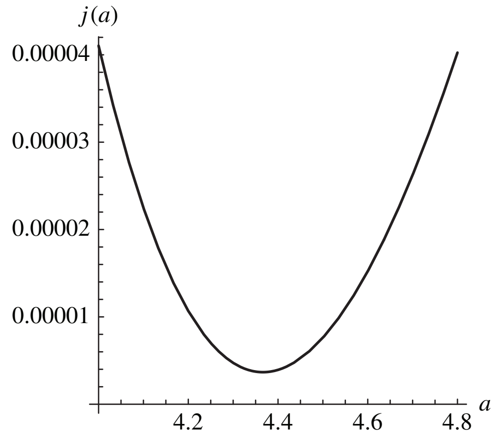


Figure 9 Plot of $j(a)$ for $4.0 \leq a \leq 4.8$

It is striking that the values of a that minimize $k(a)$ and $j(a)$ respectively are both close to 4; this means that the functions they yield are numerically not very far from Bhāskarā's function $B(x)$.

Remarks on the origin of the approximation

It is remarkable that Bhāskarā's approximation has fielded all the challenges we have thrown at it, and has walked away with credit!

There remains now the crucial question of the origin of the approximation. How did Bhāskarā I hit upon his formula? Unfortunately, we draw a blank here. Despite much thought having gone into this question, the origins remain obscure. Possible explanations have been offered, for example, in [**9**, p. 105], [**4**, pp. 121–136], [**5**, pp. 39–41], [**6**, pp. 39–41]; but these are essentially derivations from a modern viewpoint, much like the one in this article. In that respect none of them seems really satisfactory.

A feature common to early Indian mathematical writing is that justifications are rarely (if ever) given. (An exception is provided by the Kerala school of mathematics which flourished between the 14th and 16th centuries; see [**7**] and [**8**, pp. 291–306].) In the absence of definitive data, we may never know just how Bhāskarā I came upon this truly remarkable approximation; whether actually it is Āryabhaṭa's work and not Bhāskarā's; or how so non-intuitive a notion as one function approximating another might have arisen in that distant era. It is not the kind of relation that one would hit upon by chance, and one can only speculate about the depth of mathematical insight needed to find it.

REFERENCES

1. G. A. Baker, Jr. and P. Graves-Morris, *Padé Approximants*, 2nd ed., Cambridge University Press, Cambridge, UK, 2010.
2. Howard Eves, *Great Moments in Mathematics Before 1650*, Mathematical Association of America, Washington, DC, 1983.
3. http://www.gap-system.org/~history/Biographies/Bhaskara_I.html
4. R. C. Gupta, Bhāskarā I's approximation to sine, *Indian J. History Sci.* **2** (1967) 121–136.
5. ———, On derivation of Bhāskarā I's formula for the sine, *Ganita Bharati* **8**(1–4) (1986) 39–41.
6. T. Hayashi, A note on Bhāskarā I's rational approximation to sine, *Historia Sci.* **42** (1991) 45–48.
7. Kim Plofker, *Mathematics in India*, Princeton University Press, Princeton, NJ, 2008.

8. Ranjan Roy, Discovery of the Series Formula for π by Leibniz, Gregory, and Nilakantha, *Mathematics Magazine* **63**(5) (1990) 291–306.
9. Glen Van Brummelen, *The Mathematics of the Heavens and the Earth: The Early History of Trigonometry*, Princeton University Press, Princeton, NJ, 2009.

Summary In the seventh century AD the Indian mathematician Bhāskarā I gave a curious rational approximation to the sine function; he stated that if $0 \le x \le 180$ then $\sin x$ deg is approximately equal to $4x(180 - x)/(40500 - x(180 - x))$. He stated this in verse form, in the style of the day, and attributed it to his illustrious predecessor Āryabhaṭa (fifth century AD); however there is no trace of such a formula in Āryabhaṭa's known works. Considering the simplicity of the formula it turns out to be astonishingly accurate. Bhāskarā did not give any justification for the formula, nor did he qualify it in any way. In this paper we examine the formula from an empirical point of view, measuring its goodness of fit against various criteria. We find that the formula measures well, and indeed that these different criteria yield formulas that are very close to the one given by Bhāskarā.

SHAILESH A. SHIRALI holds a Ph.D. from the University of Texas at Dallas. He is the Head of the Community Mathematics Center in Rishi Valley School (India). He has been involved in the Indian Mathematics Olympiad movement since the 1980s. He is the author of many books for high school students, including *Adventures in Iteration*, *A Primer on Number Sequences* and *First Steps in Number Theory* (published by Universities Press, India), and serves as an editor for the undergraduate science magazine, "Resonance." He is currently engaged in outreach work in mathematics education. He loves teaching children, looking after kittens, star gazing, trekking, and the music of Bob Dylan and Sant Kabir in roughly equal measure.

Integrals Don't Have Anything to Do with Discrete Math, Do They?

P. MARK KAYLL
University of Montana
Missoula, MT 59812-0864
mark.kayll@umontana.edu

To students just beginning their study of mathematics, the subject appears to come in two distinct flavours: continuous and discrete. The former is embodied by the calculus, into which many math majors delve extensively, while the latter has its own introductory course (often entitled Discrete Mathematics) whose overlap with calculus is slight. The distinction persists as we learn more mathematics, since most advanced undergraduate math courses have their focus on one side or the other of this apparent divide.

This article attempts to bridge the divide by describing one surprising connection between continuous and discrete mathematics. Its goal is to convince readers that the two worlds are not so very far apart. Though they may frequently feel like polar opposites, there are also times when they join to become one, like antipodal points in projective space. Therefore, any serious study of discrete math ought to include a healthy dose of the continuous, and vice versa.

Before we are done, various players from both worlds will make their appearance: rook polynomials, derangements, the gamma function, and the Gaussian density (just to name the headliners).

Teaser To whet the reader's appetite, we begin with a challenge.

PROBLEM 1. Give a *combinatorial proof* that

$$\int_0^\infty (t^3 - 6t^2 + 9t - 2)e^{-t}\,dt = 1; \tag{1}$$

i.e., count something that, on one hand, is easily seen to number the left side of (1) and on the other, the right.

For a delightful treatment of combinatorial proofs in general, see [**4**].

At first blush, Problem 1 may appear to be out of reach—a *combinatorial* proof of an integral identity—what in heavens should we count? The answer provides part of the fun of writing (and hopefully reading) this article.

Entities: continuous and discrete

After introducing our objects of study, we reveal some of their connections in the next few sections, and also present a solution to Problem 1. In an attempt to make the article self-contained, we include an appendix containing some basic facts and other curiosities about these objects.

Math. Mag. **84** (2011) 108–119. doi:10.4169/math.mag.84.2.108. © Mathematical Association of America

Integrals The integral on the left side of (1) belongs to a family of integrals enjoying discrete connections. The family's matriarch is Euler's *gamma function*, which can be defined, for $0 < x < \infty$, by

$$\Gamma(x) := \int_0^\infty t^{x-1}e^{-t}\,dt. \tag{2}$$

One can check that this improper integral converges for such x; see, e.g., [**2**, pp. 11–12]. (In fact, Γ need not be confined to the positive real numbers—it is possible to extend its definition so that Γ becomes a meromorphic function on the complex plane, with poles at the origin and each negative integer; see, e.g., [**1**, p. 199] or [**11**, p. 54]—but we'll restrict our attention to positive real x.)

Some close cousins of the gamma function are certain 'probability moments.' For integers $n \geq 0$, the *nth moment* (of a Gaussian random variable with mean 0 and variance 1, i.e., a standard normal random variable) is defined by

$$\mathcal{M}_n := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} t^n e^{-t^2/2}\,dt.$$

These integrals also converge (see, e.g., [**8**, p. 148]), and though probability language enters in their naming, we won't be making much use of this connection. Since we do need the fact that $\mathcal{M}_0 = 1$ (see Theorem 4), we present a standard proof of this identity in the Appendix (Lemma 6).

Graphs The right side of (1)—i.e., the number 1—counts the 'perfect matchings' in a certain graph. While we shall assume that the reader is familiar with graphs, we nevertheless introduce the few required elementary notions. Any standard graph theory text should suffice to close our expositional gaps; see, e.g., [**5**].

Recall that a *graph* $G = (V, E)$ consists of a finite set V (of *vertices*), together with a set E of unordered pairs $\{x, y\}$ (*edges*) with $x \neq y$ and both of $x, y \in V$. (Such graphs are called *simple graphs* in [**5**, p. 3].) A graph is *complete* if, for each pair x, y of distinct vertices, the edge $\{x, y\}$ appears in E. FIGURE 1 depicts the complete graphs with $1 \leq |V| \leq 6$ and introduces the standard notation K_n for the complete graph on $n \geq 1$ vertices.

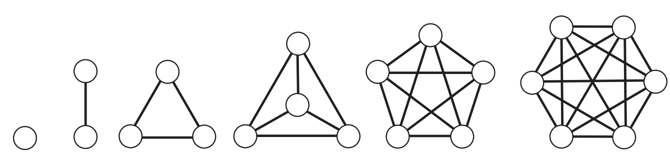
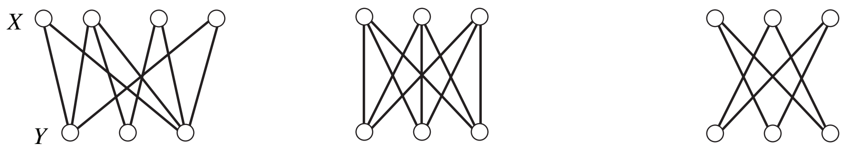


Figure 1 Complete graphs on up to six vertices

The second graph family of primary interest in this article is the collection of *bipartite graphs* G, i.e., those for which the vertex set admits a partition $V = X \oplus Y$ into nonempty sets X, Y such that each edge of G is of the form $\{x, y\}$, with $x \in X$ and $y \in Y$. One often forms a mental picture of a bipartite graph by imagining two rows of dots—a row for X and a row for Y—together with a collection of line segments xy joining an $x \in X$ to a $y \in Y$ whenever $\{x, y\} \in E$. In the next definition, we fix two positive integers n, m. The bipartite graph $(X \oplus Y, E)$ for which $|X| = n$, $|Y| = m$, and E consists of all nm possible edges between X and Y is called a *complete bipartite graph* and denoted by $K_{n,m}$. The bipartite graphs arising in this article are the complete bipartite ones for which $n = m$ (for $n \geq 1$) and their *spanning subgraphs*, i.e., those bipartite graphs $(X \oplus Y, E)$ with $|X| = |Y| = n$. It's worth noting that a subgraph H of G is a spanning subgraph exactly when they share a common vertex set; the edge set of H may form any subset of the edge set of G, including the empty set. FIGURE 2 depicts a few small bipartite graphs.



(a) a bipartite graph (b) the complete bipartite graph $K_{3,3}$ (c) a spanning subgraph of $K_{3,3}$

Figure 2 Bipartite and complete bipartite graphs

A first brush between continuous and discrete For the gamma function (2), it is easy to check that $\Gamma(1) = 1$, and integration by parts yields the recurrence

$$\Gamma(x + 1) = x\Gamma(x), \tag{3}$$

valid for positive real numbers x. It follows by mathematical induction that each nonnegative integer n satisfies $\Gamma(n + 1) = n!$; i.e., the gamma function generalizes the factorial function to the real numbers.

Given this generalization, a natural question to ponder might be: What values does Γ take on at half-integers? The reader might enjoy showing that

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi} \tag{4}$$

and then using (3) to prove that

$$\Gamma\left(n + \frac{1}{2}\right) = \frac{(2n)!\,\sqrt{\pi}}{4^n n!}$$

whenever n is a nonnegative integer. (Corollary 7 in the Appendix provides a key step in this exercise.) The ease in determining Γ at half-integers belies the dearth of known exact values; for example, no simple expression is known for $\Gamma(1/3)$ or $\Gamma(1/4)$—see [**11**, p. 55], or, for a more recent and specific discussion, [**15**].

What good, we might ask, is a continuous version of the factorial function? One answer is that a careful study of Γ can be used to establish Stirling's approximation for $n!$:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n, \tag{5}$$

published by James Stirling [**18**, p. 137] in 1730. (Here and below, the symbol $\sim$ means that the ratio of the left to the right side tends to 1 as $n \to \infty$.) See, e.g., [**14**] for an elementary proof of (5) starting from the definition (2) of Γ. A complex-analytic proof, based on the extension of Γ to $\mathbb{C} \setminus \{0, -1, -2, \ldots\}$ to which we alluded earlier, appears in [**1**, pp. 201–204]. However it's reached, the estimate (5), involving two of the most famous mathematical constants and invoking only basic algebraic operations, is no doubt beautiful. Moreover, it is useful any time one wants to gain insight into the growth rate of functions involving factorials. For example, using (5), one easily shows that

$$\binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{\pi n}},$$

and so learns something about the asymptotics of the *Catalan numbers* $\binom{2n}{n}/(n+1)$ (see, e.g., [**17**, pp. 219–229] for more on this pervasive sequence).

Our purpose is to refute the first part of this article's title, and as we move in that direction, we can't resist sharing a couple more fun facts about Γ that enhance the stature of Γ in the gallery of basic mathematical functions. First, as long as x is not an integer, we have

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin(\pi x)},$$

which generalizes (4). This 'complement formula' was first proved by Leonhard Euler; see, e.g., [**1**, pp. 198–199] or [**11**, p. 59] for modern proofs. Second, if

$$\zeta(x) := \sum_{k=1}^{\infty} \frac{1}{k^x}$$

denotes the Riemann zeta function, then whenever $\Gamma(x)$ is finite, we have

$$\zeta(x)\Gamma(x) = \int_0^\infty \frac{t^{x-1}}{e^t - 1}\, dt, \tag{6}$$

which bears a striking resemblance to (2); again, see [**1**, p. 214] or [**11**, pp. 59–60] for proofs. Because of ζ's central role in connecting number theory to complex analysis, the relation (6) opens deeper connections of Γ to number theory (beyond those stemming from the factorial function). Viewing number theory as falling within the discrete realm, we see in (6) a further refutation of this article's title.

Counting perfect matchings in $K_{n,n}$

A *matching* M in a bipartite graph $G = (X \oplus Y, E)$ is a subset $M \subseteq E$ such that the edges in M are pairwise disjoint. We think of M as 'matching up' some members of X with some members of Y. If every $x \in X$ appears in some $e \in M$, and likewise for Y, then we call M a *perfect matching*. It is a simple exercise to show that if G contains a perfect matching, then $|X| = |Y|$, so that G is a spanning subgraph of some $K_{n,n}$. FIGURE 3 highlights one matching within each of the graphs in FIGURE 2.

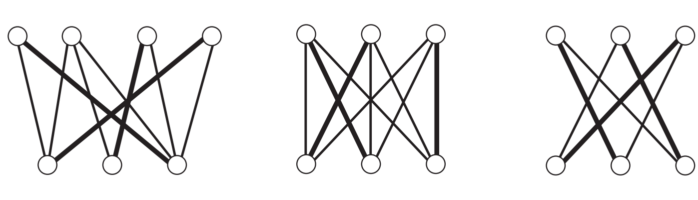


Figure 3 Matchings in the graphs of FIGURE 2 indicated by bold edges; those in (b) and (c) are perfect.

Given a bipartite graph G, we might be interested to know how many perfect matchings it contains; we use $\Xi(G)$ to denote this number.[1] Let's warm up by asking for the value of $\Xi(K_{n,n})$; a moment's reflection shows that for each integer $n \geq 1$, the answer is $n!$. (To see this, continue to denote the 'bipartition' by (X, Y), and notice that the perfect matchings of $K_{n,n}$ are in one-to-one correspondence with the bijections between X and Y.) Since $n! = \Gamma(n+1)$, we have proven our first result.

PROPOSITION 2. $\Xi(K_{n,n}) = \int_0^\infty t^n e^{-t}\, dt.$

If we replace $K_{n,n}$ by a different bipartite graph, how must we modify the formula in Proposition 2? It turns out that a so-called 'rook polynomial' should replace the polynomial t^n.

Rook polynomials Given a graph G and an integer r, we denote by $\mu_G(r)$ the number of matchings in G containing exactly r edges.

EXAMPLE 1. (THE GRAPH $G = K_{3,3} - \{\{x_1, y_1\}, \{x_2, y_2\}, \{x_3, y_3\}\}$) This is the graph in FIGURE 2(c). Since the empty matching contains no edges, we have $\mu_G(0) = 1$; since each singleton edge forms a matching, we have $\mu_G(1) = 6$, and since G contains two perfect matchings, we have $\mu_G(3) = 2$. Fixing a vertex x, we see that there are three matchings of size two using either of the edges incident with x and three more two-edge matchings not meeting x; thus $\mu_G(2) = 9$.

Now suppose that G is a spanning subgraph of $K_{n,n}$. The *rook polynomial* of G is defined by

$$R_G(t) := \sum_{r=0}^{n} (-1)^r \mu_G(r) t^{n-r}.$$

See [**10**, p. 8] or [**16**, pp. 164–166] for the etymology of this term.

EXAMPLE 1. (CONTINUED) Based on our observations in the first part of this example, we see that

$$R_G(t) = t^3 - 6t^2 + 9t - 2;$$

we're getting a little ahead of ourselves, but this is the polynomial appearing in the integrand in Problem 1.

EXAMPLE 2. (EMPTY GRAPHS) If G is the empty graph on $2n$ vertices (i.e., $|V| = 2n$ and $E = \varnothing$), then

$$\mu_G(r) = \begin{cases} 0 & \text{if } r > 0 \\ 1 & \text{if } r = 0, \end{cases}$$

so that $R_G(t) = t^n$; keeping ahead of ourselves, notice that this polynomial appears in the integrand in Proposition 2.

EXAMPLE 3. (PERFECT MATCHINGS) If G consists of n pairwise disjoint edges (i.e., G is induced by a perfect matching), then one can easily see that $\mu_G(r) = \binom{n}{r}$ for $0 \leq r \leq n$. Thus, the binomial theorem shows that $R_G(t) = (t-1)^n$.

[1]We chose this notation because (whether we write it in English or Greek!) the letter XI (Ξ) resembles a perfect matching in a graph of order six, and, conveniently enough, six is a perfect number.

Continuing to let G denote a spanning subgraph of $K_{n,n}$, we now define its *bipartite complement* $\widetilde{G}$; this graph shares the vertex set of G and has for edges all the edges of $K_{n,n}$ that are not in G. We're ready to state a generalization of Proposition 2. To avoid possible confusion as to which graph is being complemented, we use next H instead of G to denote a generic graph.

THEOREM 3. (GODSIL [**9**, THEOREM 3.2]; JONI AND ROTA [**12**, COROLLARY 2.1]) *If H is a spanning subgraph of $K_{n,n}$, then*

$$\Xi(H) = \int_0^\infty R_{\widetilde{H}}(t)e^{-t}\,dt.$$

The proof of Theorem 3 is beyond our scope, but we'll present two applications in the following sections; [**7**] presents a recent proof. Theorem 3 generalizes Proposition 2 because the bipartite complement of $K_{n,n}$ is the empty graph on $2n$ vertices; see Example 2. Further generalizations of Theorem 3 are discussed in [**10**, pp. 9–10].

Solution to Problem 1. As noted in Example 1, the integral in Problem 1 is

$$\int_0^\infty (t^3 - 6t^2 + 9t - 2)e^{-t}\,dt = \int_0^\infty R_G(t)e^{-t}\,dt, \tag{7}$$

where, recall, G is the graph depicted in FIGURE 2(c) and defined at the start of Example 1. Thus, to bring Theorem 3 to bear, it will suffice to determine a spanning subgraph H of $K_{3,3}$ such that $\widetilde{H} = G$. The graph H in FIGURE 4 does the trick. Now ask: how many perfect matchings are contained in H? The answer is obviously $\Xi(H) = 1$ because H is induced by the edges of a perfect matching. On the other hand, Theorem 3 tells us that $\Xi(H)$ coincides with (7) because $\widetilde{H} = G$. ■

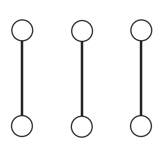


Figure 4 A graph H with $\widetilde{H} = G$ from FIGURE 2(c)

The fruit borne by the instantiation of Theorem 3 to the graphs in Examples 1 and 2 (respectively, a solution to Problem 1 and a proof of Proposition 2) might provide inspiration to consider this theorem in yet another instance, this time with $\widetilde{H}$ being the graph(s) in Example 3. This application of Theorem 3 takes us down an atypical path to a commonly studied class of combinatorial objects.

Derangements A *derangement* σ of a set S is a permutation of S with no fixed points; i.e., $\sigma\colon S \to S$ is a bijection such that $\sigma(x) \neq x$ for each $x \in S$. Counting the number of derangements of a finite set is a standard problem in introductory combinatorics and probability texts. We'll let $\mathcal{D}_n$ denote the set of derangements of $\{1, 2, \ldots, n\}$ and $d_n = |\mathcal{D}_n|$. We can easily determine these parameters for the smallest few values of n; TABLE 1 displays the results. We leave it as an exercise to show that $d_5 = 44$ and (for the punishment gluttons) $d_6 = 265$. But what is the pattern? Perhaps surprisingly, one way to obtain a general expression for d_n is to invoke Theorem 3.

Consider the bipartite graph G obtained from $K_{n,n}$ by removing the edges of a perfect matching; say, $G = K_{n,n} - \{\{x_1, y_1\}, \{x_2, y_2\}, \ldots, \{x_n, y_n\}\}$. Notice that each perfect matching in G corresponds to exactly one derangement of $\{1, 2, \ldots, n\}$ and vice

TABLE 1: Derangement numbers and their corresponding derangements for $1 \leq n \leq 4$

n	d_n	$\mathcal{D}_n$
1	0	$\varnothing$
2	1	$\{21\}$
3	2	$\{231, 312\}$
4	9	$\{2143, 2341, 2413, 3142, 3412, 3421, 4123, 4312, 4321\}$

versa. Thus, $d_n = \Xi(G)$. Since the bipartite complement of G is the graph considered in Example 3, Theorem 3 implies that

$$d_n = \int_0^\infty (t-1)^n e^{-t}\, dt. \tag{8}$$

If we separate the integral and change variables on the first subinterval, an evaluation of Γ presents itself:

$$\begin{aligned} d_n &= \int_1^\infty (t-1)^n e^{-t}\, dt + \int_0^1 (t-1)^n e^{-t}\, dt \\ &= \int_0^\infty x^n e^{-(x+1)}\, dx \;\; + \int_0^1 (t-1)^n e^{-t}\, dt \\ &= e^{-1}\Gamma(n+1) \qquad + E_n, \end{aligned} \tag{9}$$

where we now view the second integral as an error term E_n. It turns out that E_n doesn't contribute much to d_n; since $e^{-t} < 1$ on the interval (0, 1), we obtain

$$|E_n| \leq \int_0^1 \left|(t-1)^n e^{-t}\right| dt < \int_0^1 (1-t)^n\, dt = \frac{1}{n+1}.$$

This shows that for each $n \geq 1$, the error satisfies $|E_n| < 1/2$, and it follows from (9) that d_n is the integer closest to $e^{-1}\Gamma(n+1)$, i.e., to $n!/e$.

Remarks The nonstandard derivation of d_n presented above is due to Godsil [**10**, pp. 8–9]. More typical approaches (e.g., [**6**, pp. 77–78] or [**13**, pp. 71, 109–110])—that apply either the principle of inclusion-exclusion or generating functions—lead to a perhaps more familiar expression

$$d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \tag{10}$$

for the derangement numbers. Starting from (8), this 'standard' expression (10) for d_n requires even less effort to derive than the former. We first apply the binomial theorem, obtaining

$$\begin{aligned} d_n &= \int_0^\infty \left(\sum_{k=0}^{n} \binom{n}{k} (-1)^k t^{n-k} \right) e^{-t}\, dt \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!\,(n-k)!} \int_0^\infty t^{n-k} e^{-t}\, dt, \end{aligned} \tag{11}$$

and then invoke the definition (2) of Γ to replace each integral by $(n-k)!$, after which (11) becomes (10). Alternately, via the MacLaurin series for $1/e$, (10) is easily seen to be equivalent to the 'integer closest to $n!/e$' description obtained via Godsil's derivation.

Counting perfect matchings in K_n

Since matching enumeration is not confined to the realm of bipartite graphs, it is natural to seek analogues of Proposition 2 and Theorem 3 for determining $\Xi(K_n)$ and, more generally, $\Xi(G)$ for a spanning subgraph G of K_n. Here again, we will expose the speciousness of this article's title.

A *matching* M in a graph $G = (V, E)$ is defined as it is in a bipartite graph, and, as before, if each $v \in V$ is an end of some $e \in M$, then M is called *perfect*. FIGURE 5 displays all of the perfect matchings admitted by K_4 and some of those admitted by K_6. The bracketed numbers in FIGURE 5(b) indicate how many different perfect matchings result under the action of successive rotation by 60°; in this way, all $15 = 2+3+6+3+1$ perfect matchings of K_6 are obtained.

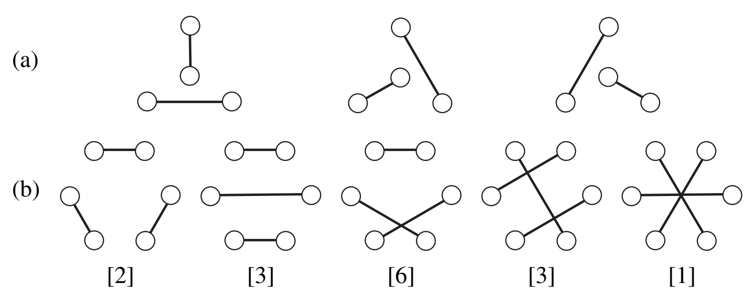


Figure 5 (a) All three perfect matchings in K_4; (b) five of fifteen perfect matchings in K_6

Following our earlier line of inquiry, we ask how many perfect matchings are contained in K_n. Since matchings pair off vertices, the question is interesting only when n is even; say $n = 2m$ for an integer $m \geq 1$. Let $V := V(K_{2m}) = \{1, 2, \ldots, 2m\}$. To determine a matching M, it is enough to decide, for each vertex $i \in V$, with which vertex i is paired under M. There are $(2m-1)$ choices for pairing with vertex 1. Having formed this pair, say $\{1, j\}$, it remains to decide how to pair the remaining $(2m-2)$ vertices. Selecting one of these, say k, there are $(2m-3)$ choices for pairing with vertex k, namely, any member of $V \setminus \{1, j, k\}$. Continuing in this fashion and applying the multiplication rule of counting, we find that

$$\Xi(K_n) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ (2m-1)(2m-3)\cdots 5\cdot 3\cdot 1 & \text{if } n = 2m \text{ for an integer } m \geq 1. \end{cases} \tag{12}$$

The last expression, reminiscent of a factorial, is sometimes called a *double factorial* which is defined, for a positive integer n, by $n!! := n(n-2)(n-4)\cdots(2 \text{ or } 1)$—see, e.g., [**20**]. This notation shortens (12) to

$$\Xi(K_n) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ (n-1)!! & \text{if } n \text{ is even.} \end{cases} \tag{13}$$

When n is even ($n = 2m$), we have

$$\Xi(K_{2m}) = (2m-1)!! = \frac{(2m)!}{2^m m!}, \tag{14}$$

which leads to an alternate way to count $\Xi(K_{2m})$: think of determining a matching by permuting the elements of V in a horizontal line (in $(2m)!$ ways) and then simply grouping the vertices into pairs from left to right. Of course, this over-counts $\Xi(K_{2m})$—by a factor of $m!$ since the resulting m matching edges are ordered, and by a factor of 2^m since each edge itself imposes one of two orders on its ends. After correcting for the over-counting, we arrive at (14) and thus have a second verification of (12).

As a final refutation of our title, we'll show that $\Xi(K_n)$ can also be expressed as an integral.

THEOREM 4. (GODSIL [**9**, THEOREM 1.2]; AZOR ET AL. [**3**, THEOREM 1])

$$\Xi(K_n) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} t^n e^{-t^2/2}\, dt.$$

Proof. The right side of the identity is the moment $\mathcal{M}_n$. Since the integrand of each $\mathcal{M}_n$, for odd n, is an odd function, we have

$$\mathcal{M}_n = 0 \quad \text{whenever } n \text{ is odd.} \tag{15}$$

For even n, say $n = 2m$, we apply induction. Since $\mathcal{M}_0$ is the area under the curve for the probability density function of a standard normal random variable, we have

$$\mathcal{M}_0 = 1; \tag{16}$$

the proof of Lemma 6 below verifies this directly.

Fix an integer $m \geq 1$; starting with $\mathcal{M}_{2m-2}$ and integrating by parts yields the recurrence

$$\mathcal{M}_{2m} = (2m-1)\mathcal{M}_{2m-2} \quad \text{for } m \geq 1. \tag{17}$$

Now

$$\mathcal{M}_{2m} = (2m-1)!! \quad \text{for } m \geq 1 \tag{18}$$

follows easily from (16) and (17) by induction. Comparing (15) and (18) with (13) shows that Theorem 4 is proved. ∎

Just as Proposition 2 generalizes to Theorem 3, so too does Theorem 4 generalize. For a given (not necessarily bipartite) graph G (now with n vertices instead of the earlier $2n$ in the bipartite setting), the *matchings polynomial* is defined by $P_G(t) := \sum_{r=0}^{\lfloor n/2 \rfloor} (-1)^r \mu_G(r) t^{n-2r}$. To determine $\Xi(G)$, we need to replace the factor t^n in the integrand of Theorem 4 by the matchings polynomial of the complementary graph $\overline{G}$ of G. We close this section by stating this analogue of Theorem 3 precisely.

THEOREM 5. (GODSIL [**9**, THEOREM 1.2]) *If G is a spanning subgraph of K_n, then*

$$\Xi(G) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} P_{\overline{G}}(t) e^{-t^2/2}\, dt.$$

A proof of Theorem 5 may be found in [**10**, p. 6].

Appendix

After establishing that the 0th moment $\mathcal{M}_0 = 1$ (which was needed in the proof of Theorem 4), we indicate how to obtain (4). Evaluating the integral in the definition of $\mathcal{M}_0$ is an enjoyable polar coordinates exercise.

LEMMA 6. $\displaystyle\int_{-\infty}^{\infty} e^{-u^2/2}\,du = \sqrt{2\pi}.$

Proof. Denoting the integral by $\mathcal{J}$, we have

$$\mathcal{J}^2 = \left(\int_{-\infty}^{\infty} e^{-u^2/2}\,du\right)\left(\int_{-\infty}^{\infty} e^{-v^2/2}\,dv\right)$$

$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-(u^2+v^2)/2}\,du\,dv \tag{19}$$

$$= \int_{0}^{2\pi}\int_{0}^{\infty} r\,e^{-r^2/2}\,dr\,d\vartheta, \tag{20}$$

where we used Tonelli's Theorem to obtain (19) (see, e.g., [**21**, Theorem 6.10]) and a switch to polar coordinates to reach (20). Since the inner integral here is unity, the result follows. ■

Perhaps the simplicity of the preceding proof coloured the views of Lord Kelvin (1824–1907), as hinted in the following anecdote from [**19**, p. 1139]:

> Once when lecturing he used the word "mathematician," and then interrupting himself asked his class: "Do you know what a mathematician is?" Stepping to the blackboard he wrote upon it:—
>
> $$\int_{-\infty}^{\infty} e^{-x^2}\,dx = \sqrt{\pi}.$$
>
> Then, putting his finger on what he had written, he turned to his class and said: "A mathematician is one to whom *that* is as obvious as that twice two makes four is to you. Liouville was a mathematician." Then he resumed his lecture.

At any rate, now the relation (4) is almost immediate:

COROLLARY 7. $\Gamma(1/2) = \sqrt{\pi}.$

Proof. By definition, $\Gamma(1/2) = \int_0^\infty t^{-1/2}e^{-t}\,dt$. On putting $t = u^2/2$, we find that $\Gamma(1/2) = \sqrt{2}\int_0^\infty e^{-u^2/2}\,du$, or, since the last integrand is an even function, $\Gamma(1/2) = \sqrt{2}\int_{-\infty}^{\infty} e^{-u^2/2}\,du/2$. Now Lemma 6 gives the value of this integral to confirm the assertion. ■

Concluding remarks

Proposition 2 and Theorem 4 present just two examples of combinatorially interesting sequences that can be expressed in the form $\int_\Omega t^n\,d\nu$ for some measure ν and space Ω. This topic is considered in detail in [**10**, Chapter 9].

What is one to make of these connections between integrals and enumeration? We don't claim that integrals provide the preferred lens for viewing these counting problems. For example, nobody would make the case that the integral in Theorem 4 is the 'right way' to determine $\Xi(K_n)$ because the explicit formula (12) provides a direct route. However, perhaps surprisingly, integrals do offer *one* lens. And this connection between the continuous and the discrete reveals just one of the myriad ways in which mathematics intimately links to itself. These links can benefit the mathematical branches at either of their ends. The application to counting derangements illustrates how continuous methods can shed light on a discrete problem, while Problem 1 and its solution indicate how a discrete viewpoint might yield a fresh approach to an essentially continuous question. This symbiotic relationship between the different branches of mathematics should inspire students (and their teachers) not to overly specialize. As in life, it's better to keep one's mind as open as possible.

Acknowledgments The author drafted this article during a sabbatical at Université de Montréal. *Merci à mon hôte généreux, Geňa Hahn, et au Département d'informatique et de recherche opérationnelle. Un merci particulier à André Lauzon, qui a apprivoisé mon ordinateur.* Thanks also to Karel Stroethoff who pointed me to the Lord Kelvin connection and whose post-colloquium observation led to an improvement of the derangements discussion.

REFERENCES

1. L. V. Ahlfors, *Complex Analysis*, 3rd ed., McGraw-Hill, New York, 1979.
2. E. Artin, *The Gamma Function*, trans. Michael Butler, Holt, Rinehart and Winston, New York, 1964.
3. R. Azor, J. Gillis, and J. D. Victor, Combinatorial applications of Hermite polynomials, *SIAM J. Math. Anal.* **13** (1982) 879–890. doi:10.1137/0513062
4. A. Benjamin and J. Quinn, *Proofs that Really Count: The Art of Combinatorial Proof*, Mathematical Association of America, Washington, DC, 2003.
5. J. A. Bondy and U. S. R. Murty, *Graph Theory*, Springer, New York, 2008.
6. P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge, UK, 1994.
7. E. E. Emerson and P. M. Kayll, Another short proof of the Joni-Rota-Godsil integral formula for counting bipartite matchings, *Contrib. Discrete Math.* **4** (2009) 89–93.
8. M. Fisz, *Probability Theory and Mathematical Statistics*, 3rd ed., trans. R. Bartoszynski, John Wiley, New York, 1963.
9. C. D. Godsil, Hermite polynomials and a duality relation for matching polynomials, *Combinatorica* **1** (1981) 257–262. doi:10.1007/BF02579331
10. C. D. Godsil, *Algebraic Combinatorics*, Chapman & Hall, New York, 1993.
11. J. Havil, *Gamma. Exploring Euler's Constant*, Princeton University Press, Princeton, NJ, 2003.
12. S. A. Joni and G.-C. Rota, A vector space analog of permutations with restricted position, *J. Combin. Theory Ser. A* **29** (1980) 59–73. doi:10.1016/0097-3165(80)90047-3
13. J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, UK, 1992.
14. R. Michel, On Stirling's formula, *Amer. Math. Monthly* **109** (2002) 388–390. doi:10.2307/2695504
15. A. Nijenhuis, Short gamma products with simple values, *Amer. Math. Monthly* **117** (2010) 733–737. doi:10.4169/000298910X515802
16. J. Riordan, *An Introduction to Combinatorial Analysis*, John Wiley, New York, 1958.
17. R. P. Stanley, *Enumerative Combinatorics*, Vol. 2, Cambridge University Press, Cambridge, UK, 1999.
18. J. Stirling, *Methodus Differentialis: sive Tractatus de Summatione et Interpolatione Serierum Infinitarum*, William Bowyer (printer), G. Strahan, London, 1730.
19. S. P. Thompson, *The Life of William Thomson, Baron Kelvin of Largs*, Macmillan, London, 1910.
20. E. W. Weisstein, *Double factorial*, from MathWorld—A Wolfram Web Resource, available at http://mathworld.wolfram.com/DoubleFactorial.html, 1999–2010.
21. R. L. Wheeden and A. Zygmund, *Measure and Integral: An Introduction to Real Analysis*, Marcel Dekker, New York, 1977.

Summary To students just beginning their study of mathematics, the discipline appears to come in two distinct flavours: continuous and discrete. This article attempts to bridge the apparent divide by describing a surprising connection between these ostensible opposites. Various inhabitants from both worlds make appearances: rook

polynomials, Euler's gamma function, derangements, and the Gaussian density. Uncloaking combinatorial proof of an integral identity serves as a thread tying these notions together.

MARK KAYLL earned mathematics degrees from Simon Fraser University (B.Sc. 1987) and Rutgers University (Ph.D. 1994), then joined the faculty at the University of Montana in Missoula. To date, he has enjoyed sabbaticals at University of Ljubljana, Slovenia (2001–2002) and Université de Montréal, Canada (2008–2009). In high school, while playing with a calculator, he noticed that 1.0000001 raised to the ten millionth power is awfully close to the mysterious number e and the following year learned that this theorem is already taken. Three decades down the road, he still thinks about e occasionally, as exemplified by his contribution here.

Letter to the Editor

The sequence discussed in G. Minton's Note, "Three approaches to a sequence problem," in the February issue [**4**] is known as Perrin's sequence and has a long history. (Perrin's sequence is defined by $x_1 = 0$, $x_2 = 2$, $x_3 = 3$, and $x_n = x_{n-2} + x_{n-3}$ for $n \geq 4$.) An important question is: Is an integer prime if and only if it satisfies the Perrin condition, n divides x_n? This question was raised by R. Perrin in 1899. A counterexample, now known as a *Perrin pseudoprime,* was not discovered until 1982: the smallest one is 271441. This is quite remarkable compared to, say, Fermat pseudoprimes with base 2, for which 341 is the smallest example. Recent work by J. Grantham [**3**] shows that there are infinitely many Perrin pseudoprimes. One can run the Perrin recurrence backward and verify that if p is prime then x_{-p} is divisible by p. When the Perrin condition is enhanced by this additional condition, then the first composite that satisfies both congruences, called a symmetric Perrin pseudoprime, is 27664033. For more information, see the references listed below.

STAN WAGON
Macalester College, St. Paul, MN 55105
wagon@macalester.edu

REFERENCES

1. W. Adams and D. Shanks, Strong primality tests that are not sufficient, *Math. Comp.* **39** (1982) 255–300. doi:10.1090/S0025-5718-1982-0658231-9
2. D. Bressoud and S. Wagon, *A Course in Computational Number Theory,* New York, Wiley, 2000, exercise 8.18.
3. J. Grantham, There are infinitely many Perrin pseudoprimes, *J. Number Th.* **130** (2010) 1117–1128. doi:10.1016/j.jnt.2009.11.008
4. G. Minton, Three approaches to a sequence problem, *Math. Mag.* **84** (2011) 33–37. doi:10.4169/math.mag.84.1.033
5. Online Encyclopedia of Integer Sequences, sequence A013998, Unrestricted Perrin pseudoprimes, http://oeis.org/A013998
6. Weisstein, Eric W., Perrin pseudoprime, from MathWorld—A Wolfram Web Resource, http://mathworld.wolfram.com/PerrinPseudoprime.html
7. Wikipedia entry on "Perrin number," http://en.wikipedia.org/wiki/Perrin_number

Math. Mag. **84** (2011) 119. doi:10.4169/math.mag.84.2.119. © Mathematical Association of America

NOTES

Positively Prodigious Powers or How Dudeney Done It?

ANDREW BREMNER
Arizona State University
Tempe, AZ 85287
bremner@asu.edu

Henry Ernest Dudeney was a foremost constructor of puzzles during the early part of the twentieth century. His puzzles covered an extraordinary range, from geometric dissections to river crossing problems to puzzles in logic and in combinatorics. Among his books are: *The Canterbury Puzzles and Other Curious Problems* [**2**], *Amusements in Mathematics* [**3**], *The World's Best Word Puzzles* [**4**], *Modern Puzzles* [**5**], *536 Puzzles and Curious Problems* [**6**], and *More Puzzles and Curious Problems* [**7**].

Of his mathematical puzzles, the most intriguing relate to writing an integer as the sum of two rational cubes. For example, *The Canterbury Puzzles and Other Curious Problems* [**2**] lists the puzzle of the "Silver Cubes," which asks for the dimensions in rational numbers of two cubes of silver that contain precisely 17 cubic inches. This requires finding a pair of (positive) rational numbers x, y satisfying $x^3 + y^3 = 17$. The "Puzzle of the Doctor of Physic" requires finding the diameters of two spheres (in rational numbers) whose combined volume equals that of two spheres of diameters one foot and two feet (and, of course, different from one foot and two feet). This in turn resolves easily into finding positive rational numbers x, y, not equal to 1, 2, with $x^3 + y^3 = 1^3 + 2^3$.

The solutions given must have startled his readership, who likely were more accustomed to solving simple problems in logic: for the first problem, the solution given is $(x, y) = \left(\frac{104940}{40831}, \frac{11663}{40831}\right)$, and for the second, $(x, y) = \left(\frac{415280564497}{348671682660}, \frac{676702467503}{348671682660}\right)$. How on earth did Dudeney find these solutions with their big numbers? There were no calculators or other aids at that time, and he could only have used paper and pencil computations. He had little formal education, starting work as a clerk in the English civil service at the age of 13. The solutions astonished me as a young teenager when first coming across these puzzles in the books. It took several years for me to realize just how Dudeney must have done it!

The key is to think geometrically. The Doctor of Physic for instance asks us to find rational numbers x, y satisfying $x^3 + y^3 = 9$, in other words to find a rational *point* (x, y) on the *curve* with equation $x^3 + y^3 = 9$. The graph of this curve is shown in FIGURE 1. We certainly know one point on the curve, namely $P = (2, 1)$. Suppose we construct the tangent line l to the curve at the point P. It has an equation of type $y = mx + b$, so has exactly three points of intersection with the cubic curve $x^3 + y^3 = 9$, that is, precisely where $x^3 + (mx + b)^3 - 9 = 0$. Since P is a point of tangency, the cubic will have a double root at the x-coordinate ($= 2$) of P; and the third root will correspond to the point Q in FIGURE 1. Now if a cubic with integer coefficients has

Math. Mag. **84** (2011) 120–125. doi:10.4169/math.mag.84.2.120. © Mathematical Association of America

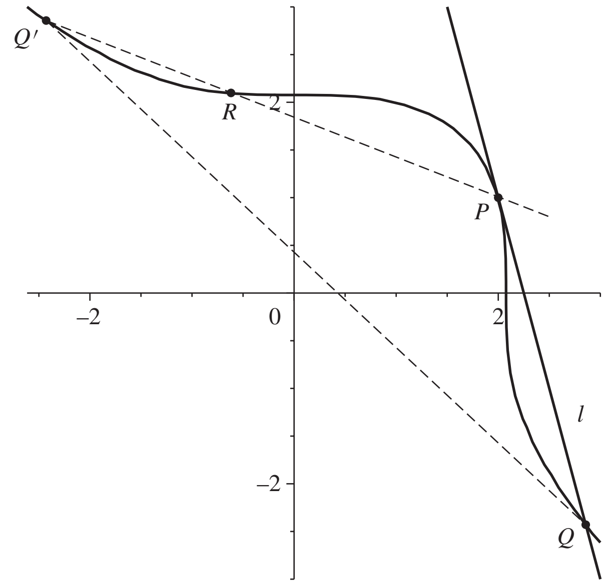


Figure 1 $x^3 + y^3 = 9$

two rational roots, then necessarily the third root will be rational. Let's actually do this, and find the coordinates of Q.

To compute the equation of l, we need to know the value of $\frac{dy}{dx}$ at P. But $x^3 + y^3 = 9$, and using implicit differentiation, $3x^2 + 3y^2\frac{dy}{dx} = 0$, so that $\frac{dy}{dx} = -\frac{x^2}{y^2}$. Thus at $P = (2, 1)$, $\frac{dy}{dx} = -\frac{2^2}{1^2} = -4$. The equation of the tangent line l is therefore $y - 1 = -4(x - 2)$, that is, $y = -4x + 9$. Where does this line meet the curve? It will do so where $x^3 + (-4x + 9)^3 = 9$, namely, where $9(-7x^3 + 48x^2 - 108x + 80) = 0$. Because of the tangency, we know there is a double root at $x = 2$, and sure enough, the cubic factors to give $9(x - 2)^2(20 - 7x) = 0$. Accordingly, the line meets the curve again at the third point Q with x-coordinate equal to $\frac{20}{7}$. Since Q lies on the tangent line $y = -4x + 9$, it is easy to compute the y-coordinate, namely $y = -\frac{80}{7} + 9 = -\frac{17}{7}$. Thus $Q = \left(\frac{20}{7}, -\frac{17}{7}\right)$.

We have now found a new solution to $x^3 + y^3 = 9$ in rational numbers, specifically $\left(\frac{20}{7}\right)^3 + \left(-\frac{17}{7}\right)^3 = 9$. The only problem is that one of the numbers is negative, and spheres of negative diameter pose an existential problem for the Doctor of Physic! Well, one suggestion is simply to repeat the previous process, but start with the point Q rather than P; this will in turn deliver a new point. However, by the following trick, we can keep the numbers smaller in size. The curve obviously has symmetry about the line $y = x$: that is, if (x, y) is a point on the curve, then so is (y, x). If we now join the flipped point $Q' = \left(-\frac{17}{7}, \frac{20}{7}\right)$ to the point $P = (2, 1)$, we have a line which as before meets the cubic in three points, of which we know two: so again we should find a new point R. Here goes. The line joining $\left(-\frac{17}{7}, \frac{20}{7}\right)$ to P has equation $\left(y - \frac{20}{7}\right)/\left(\frac{20}{7} - 1\right) = \left(x + \frac{17}{7}\right)/\left(-\frac{17}{7} - 2\right)$, that is, $y = -\frac{13}{31}x + \frac{57}{31}$. This line meets the curve where $x^3 + \left(-\frac{13}{31}x + \frac{57}{31}\right)^3 = 9$, and so, expanding the parenthesis, where $3066x^3 + 3211x^2 - 14079x - 9214 = 0$. We know the cubic must contain the factors $x + \frac{17}{7}$ and $x - 2$: and sure enough, we get $(x - 2)(7x + 17)(438x + 271) = 0$, giving the x-coordinate of the new point R as $x = -\frac{271}{438}$. The y-coordinate of R is now given by $y = -\frac{13}{31}x + \frac{57}{31} = \frac{919}{438}$. Sure thing, $\left(-\frac{271}{438}\right)^3 + \left(\frac{919}{438}\right)^3 = 9$. But the sphere still has negative diameter!

Of course, what we seek is a rational point on the curve which lies in the *first* quadrant, where $x > 0$, $y > 0$. It appears plausible from FIGURE 1 that the tangent line at R meets the curve again in the first quadrant. As a check, the tangent line at R has equation $y = -\frac{844561}{73441}x + \frac{1726596}{73441}$, which meets the curve twice at R, and at the new point $\left(\frac{415280564497}{348671682660}, \frac{676702467503}{348671682660}\right)$ which does indeed lie in the first quadrant, and provides Dudeney's solution to the problem.

For the silver cubes, Dudeney had likely noticed that $18^3 - 1^3 = 17 \cdot 7^3$, so that the curve $x^3 + y^3 = 17$ contains the point $P = \left(\frac{18}{7}, -\frac{1}{7}\right)$. (This is presumably the reason why he chose the number 17 in this problem.) The reader can try the above technique, and will find that just one line needs to be drawn. The tangent line at P, namely $y = -324x + 833$, meets the curve twice at P, and at the new point $(x, y) = \left(\frac{104940}{40831}, \frac{11663}{40831}\right)$.

We have here a powerful technique for constructing new points from old. Given one point on the curve, we can compute the tangent line and find the third point of intersection of the line and the curve. Given two points on the curve, we can compute the chord joining them, and again determine the third point of intersection with the curve. For obvious reasons, this procedure is usually called the chord-and-tangent method. It turns out that the set of rational points on the curve is actually a *group*, and what we are doing is *adding* two points in this group. For technical reasons, there's a slight subtlety to mention. To add the points P, Q, we construct the chord joining P to Q, and find the third point of intersection (u, v) of this line and the curve. Then the sum $P + Q$ of P and Q is defined to be the *flipped* point (v, u). (The reason for this is to ensure *associativity*, that $P + (Q + R) = (P + Q) + R$ for any three points P, Q, R). To add a point P to itself, in other words to compute $P + P$, usually denoted by $2P$, we use the tangent line at P (think of Q getting closer and closer to P in the previous description of $P + Q$), and proceed as above. (Remark: a group needs a *zero* element which here involves talking about *projective space* and *points at infinity*, and the interested reader can find full details in, for example, the undergraduate text by Silverman and Tate [**8**]). As an example, for the curve $x^3 + y^3 = 9$ with $P = (2, 1)$, we obtain $2P = Q' = \left(-\frac{17}{7}, \frac{20}{7}\right)$. The second computation we did above was to add $2P$ to P, and the result is therefore $3P = 2P + P = R' = \left(\frac{919}{438}, -\frac{271}{438}\right)$ (remember to flip the coordinates). We can now successively compute mP, $m = 4, 5, 6, \ldots$ by repeatedly adding P. We get the following:

$$P = (2, 1), \qquad 2P = \left(-\frac{17}{7}, \frac{20}{7}\right),$$

$$3P = \left(\frac{919}{438}, -\frac{271}{438}\right), \qquad 4P = \left(-\frac{36520}{90391}, \frac{188479}{90391}\right),$$

$$5P = \left(\frac{169748279}{53023559}, -\frac{152542262}{53023559}\right),$$

$$6P = \left(\frac{415280564497}{348671682660}, \frac{676702467503}{348671682660}\right).$$

So the first proper multiple of P to lie in the first quadrant is $6P$.

One of the deep mathematical properties of the curve $x^3 + y^3 = 9$ (a particular example of an *elliptic curve*) is that if (u, v) is *any* rational point on the curve, then one of (u, v), (v, u), must be of the form mP, $m \geq 1$. So rational solutions can only be those delivered by $P, 2P, 3P, 4P, \ldots$. Since the multiples of P have coordinates that are getting increasingly large, the solution in smallest rationals sought by the Doctor of Physic is indeed that provided by $6P$.

Let's consider more generally a curve of the form $x^3 + y^3 = n$ for an arbitrary positive integer n. There may in fact be no rational points on the curve at all, as happens for example when $n = 3, 4, 5, 10, \ldots$. It is conjectured that roughly half of all such curves fall into this category, and that in almost all the other cases, there exists a single point P on the curve such that *all* the rational points on the curve are constructed by the multiples mP of P. There are certainly exceptions. If we take $n = 65$, which is in fact the smallest exception, then we can determine points $(4, 1)$ and $\left(\frac{197}{86}, \frac{323}{86}\right)$ on the curve $x^3 + y^3 = 65$. But it can be shown, with a certain amount of difficulty, that there is *no* point P on the curve such that $(4, 1) = m_1 P$ and $\left(\frac{197}{86}, \frac{323}{86}\right) = m_2 P$. We will not go further here with this interesting topic, involving the *rank* of an elliptic curve, but Silverman and Tate [**8**] can provide further information. We shall look only at curves where there is the single point P generating all the rational points.

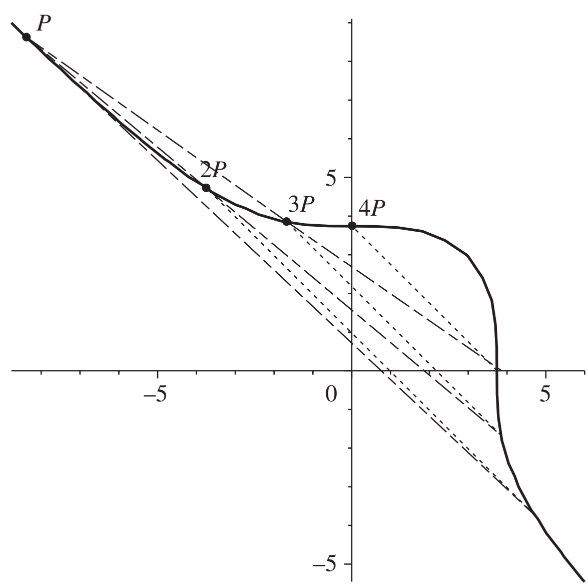


Figure 2 $x^3 + y^3 = 53$

If P lies in the second quadrant quite a long way out along the curve, then the multiples of P display a progression that we illustrate in FIGURE 2 for the case $n = 53$. Here, the dashed lines represent the tangent line at P, the line joining P to $2P$, the line joining P to $3P$, etc. The dotted lines represent the flip, or interchange of coordinates (equivalently, reflection in the line $y = x$). So, for example, the dashed line through P and $3P$ meets the curve again at a point which when flipped, gives $4P$.

Here, for $n = 53$, P is the point $\left(-\frac{1819}{217}, \frac{1872}{217}\right)$, with x-coordinate approximately -8.38. The first multiple of P to lie in the positive quadrant (just barely, the x-coordinate is approximately 0.00005737) is $4P$, so that the smallest solution of $x^3 + y^3 = 53$ in positive rationals is given by

$$(x, y) = \left(\frac{50639315258668885605233901479122847978994584928 1}{8826496053992240180747889267060920081280019625992613}, \frac{3315484138729951843398423832639234683056970305467296 0}{8826496053992240180747889267060920081280019625992613}\right).$$

Fair warning: Actually finding the generator P in any numerical example can be very difficult, and the algorithms involved are beyond the scope of this article (all the more reason to sign up for courses in number theory and elliptic curves; Silverman [**9**] is a useful but more advanced reference here). Fortunately, the algorithms have been programmed into various computer algebra systems (Magma [**1**] was used for the computations of this article), and for a given value of n there is good chance of being able to find the generator.

In general, we can see from the chord-and-tangent construction that the multiples $2P, 3P, 4P, \ldots$ will slowly move down the second quadrant branch in the direction of the first quadrant. General theory tells us that eventually we *will* hit a multiple that indeed lies in the first quadrant; but the further out the generator P, the higher that multiple will be. Talking about Dudeney and his problem to our undergraduate Math Club, I decided to try and find an example where the smallest solution to $x^3 + y^3 = n$ in positive rationals was *really* big. Of course, unlike Dudeney, I'm privileged to have access to modern computers, and it wasn't too difficult to come up with the case of $n = 94$. This is a curve where all the rational points are constructed from a single generator P; but P itself has very large coefficients, specifically $P = \left(-\frac{15616184186396177}{590736058375050}, \frac{15642626656646177}{590736058375050}\right)$. The x-coordinate of P is roughly equal to -26.435, so lies quite far out on the branch of the curve in the second quadrant. If we compute the multiples of P, we find that they lie on the graph as shown in FIGURE 3. It is not until $11P$ that we get a point in the first quadrant, and $11P$ has coordinates given by rational fractions with about 1960 digits in each numerator and denominator! Displaying them on a laptop can take a couple of screens.

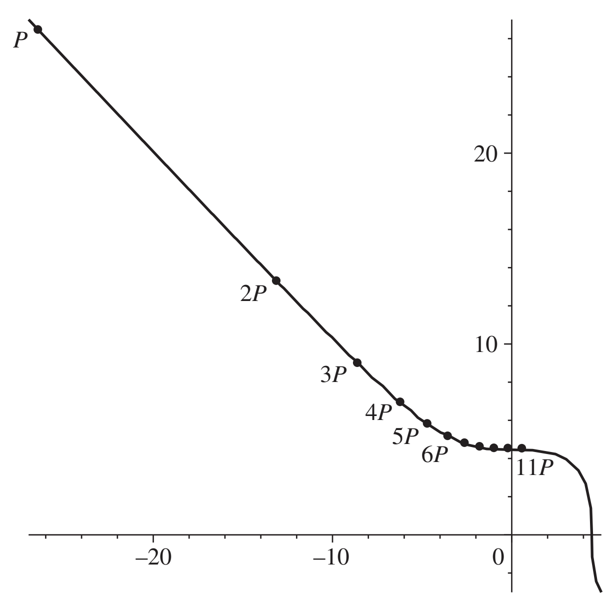


Figure 3 $x^3 + y^3 = 94$

Appetite whetted, the search was on for a really BIG smallest solution, and all curves $x^3 + y^3 = n$ for $n < 5000$ were investigated. That turned out to be a lucky choice of upper bound, with $n = 4981$ providing an excellent example. Here again, there is a single generator P such that all rational points on $x^3 + y^3 = 4981$ are constructed from the multiples mP, $m = 1, 2, 3, 4, \ldots$. This time, we have P the truly enormous

$$
\begin{aligned}
P = \Bigg(-&\frac{2579396069252461884476214386914906799758012129009229089 40}{8446297640205982464443847198386318723591730999406540406 20} \\
&\frac{5450955747647839037708393781319249995298580890184488194 44}{6337658894679192590937691512946325320013924853635685343 46} \\
&\frac{20715555962964819660153619536333953216972422389552271 03}{45443762063529213083752106248760127183243053777256 6}, \\
&\frac{2579396219621471354767591593533092593856365012686378583 15}{8446297640205982464443847198386318723591730999406540406 20} \\
&\frac{6647749359159264232102397417828422723715367938812311441 45}{6337658894679192590937691512946325320013924853635685343 46} \\
&\frac{48147777582476405201716392912380652947279493932113244 87}{45443762063529213083752106248760127183243053777256 6}\Bigg).
\end{aligned}
$$

In addition, the x-coordinate of P is roughly -3053.887, a *long* way out on the second quadrant branch. The multiples of P slowly progress down the second quadrant branch until at $316P$ they finally enter the first quadrant. The point $316P$ is truly BIG. Its coordinates are rational fractions with about 16816898 digits in each numerator and denominator. If Dudeney had asked his readers to find two rational sided silver cubes with volume 4981 cubic inches, he would have needed the space of approximately 80 paperback novels to write out the two fractions giving the smallest solution, with their 67 million digits!

REFERENCES

1. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**(3–4) (1997) 235–265. doi:10.1006/jsco.1996.0125
2. H. E. Dudeney, *The Canterbury Puzzles and Other Curious Problems*, Nelson, London, 1907; reprinted Dover, New York, 1972.
3. ———, *Amusements in Mathematics*, Dover, New York, 1917; reprinted Dover, 1958.
4. ———, *The World's Best Word Puzzles*, *Daily News*, London, 1925.
5. ———, *Modern Puzzles and How to Solve Them*, C. Arthur Pearson, London, 1926.
6. ———, *536 Puzzles and Curious Problems*, Scribner, New York, 1967.
7. ———, *More Puzzles and Curious Problems*, Fontana, London 1970.
8. J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer, New York, 2010.
9. J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, Springer, New York, 2009.

Summary Dudeney's puzzles of a hundred years ago included writing integers (specifically 9 and 17) as sums of two cubes of positive rational numbers (where in the former case, a solution other than 1, 2 is required). We study the corresponding equations $x^3 + y^3 = 9$ and $x^3 + y^3 = 17$ as examples of specific elliptic curves. The group structure is introduced, and the smallest solutions found for Dudeney's puzzles. Generalization to $x^3 + y^3 = n$ reveals that sometimes the smallest rational solution can be very large, for example when $n = 94$ and $n = 4981$: the latter solution involves fractions with numerator and denominator having almost 17 million digits.

The Quadratic Character of 2

RAFAEL JAKIMCZUK
Universidad Nacional de Luján
Buenos Aires, Argentina
jakimczu@mail.unlu.edu.ar

There are many proofs of the quadratic character of 2. The text by Ireland and Rosen contains a non-elementary proof [**1**, p. 69] and an elementary proof using Gauss's Lemma [**1**, p. 53], and there are also combinatorial proofs [**3, 2**]. Euler, in an early paper, proved that 2 is a quadratic residue of primes of the form $8k+1$ [**1**, p. 70], assuming the existence of a primitive root modulo p. Later, Gauss was the first to give a rigorous proof that primitive roots exist. In this short note we give a complete, elementary proof of the quadratic character of 2 assuming the existence of a primitive root mod p.

THEOREM. *The number* 2 *is a quadratic residue of primes of the form* $p = 8k+1$ *and* $p = 8k+7$. *The number* 2 *is not a quadratic residue of primes of the form* $p = 8k+3$ *and* $p = 8k+5$.

Proof. Let p be an odd prime and let g be a primitive root modulo p. The set $\{1, 2, \dots, p-1\}$ can be written in the form $\{g^1 = g, g^2, g^3, \dots, g^{p-1} = 1\}$.

Note that $g^{\frac{p-1}{2}} = p-1$ since $(g^{\frac{p-1}{2}})^2 = 1$. Also, g^n is a quadratic residue if and only if n is even.

Consider the following system of $\frac{p-1}{2} - 1$ congruences, all mod p.

$$\begin{aligned} g^1(1 + g^{(p-1)-1}) &= (1 + g^1) \\ g^2(1 + g^{(p-1)-2}) &= (1 + g^2) \\ g^3(1 + g^{(p-1)-3}) &= (1 + g^3) \\ &\vdots \\ g^{\frac{p-1}{2}-1}(1 + g^{\frac{p-1}{2}+1}) &= (1 + g^{\frac{p-1}{2}-1}) \end{aligned}$$

Consider the sums $(1+g^k)$ that that appear either on the right side, or as the second factor on the left side. Every residue appears exactly once in one of these positions except for the values $0 = (1 + g^{\frac{p-1}{2}})$, $1 = (1+0)$, and $2 = (1 + g^{p-1})$.

In each congruence, if the first factor is a quadratic residue then the second factor and the product have the same character—that is, both are quadratic residues or neither is a quadratic residue. On the other hand, if the first factor is a quadratic nonresidue then the second factor and the product have opposite character. Consequently each congruence contains an odd number of quadratic residues.

The rest of the proof is a simple counting argument. We may think of the system of congruences as a table with three columns. In the first column are the powers of g from g^1 to $g^{(p-1)/2-1}$, and in the second and third columns are the various sums $(1+g^k)$.

Suppose $p = 8k+1$.

(a) The table contains an odd number of congruences, each containing an odd number of quadratic residues, so the number of quadratic residues in the table is odd. The

Math. Mag. **84** (2011) 126–127. doi:10.4169/math.mag.84.2.126. © Mathematical Association of America

number of quadratic residues in the first column is $2k - 1$ (count the even powers of g), which is also odd. So the number of quadratic residues in the second and third columns must be even. But those columns contain every number in Z/pZ exactly once, except for 0, 1, and 2. So the number of quadratic residues in Z/pZ, other than 0, 1, and 2, is even.

(b) But the number of quadratic residues in Z/pZ, other than 0 and 1, is $(p-1)/2 - 1 = 4k - 1$, which is odd.

(c) Since (a) and (b) differ, 2 must be a quadratic residue.

Suppose $p = 8k + 3$.

(a) The table contains an even number of congruences, each containing an odd number of quadratic residues, so the number of quadratic residues in the table is even. The number of quadratic residues in the first column is $2k$, which is also even. So the number of quadratic residues in the second and third columns must be even. But those columns contain every number in Z/pZ exactly once, except for 0, 1, and 2. So the number of quadratic residues in Z/pZ, other than 0, 1, and 2, is even.

(b) But the number of quadratic residues in Z/pZ, other than 0 and 1, is $4k$, which is even.

(c) Since (a) and (b) coincide, 2 cannot be a quadratic residue.

The other cases ($p = 8k + 5$ and $p = 8k + 7$) work the same way. The theorem is thus proved. ■

Acknowledgment The author is very grateful to Universidad Nacional de Luján.

Dedication In memory of my sister Fedra Marina Jakimczuk, 1970–2010.

REFERENCES

1. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, New York, 1998.
2. R. Jakimczuk, The quadratic equation in F_p and the quadratic reciprocity law, *International Journal of Contemporary Mathematical Sciences* **4** (2009) 419–431.
3. K. S. Williams, The quadratic character of 2 (mod p), *Mathematics Magazine* **49** (1976) 89–90. doi:10.2307/2689440

Summary The number 2 is a quadratic residue mod p if $p = 8k + 1$ or $p = 8k + 7$, but not if $p = 8k + 3$ or $p = 8k + 5$. This is proved by a simple counting argument, assuming the existence of a primitive root mod p.

Two Generalizations of the 5/8 Bound on Commutativity in Nonabelian Finite Groups

THOMAS LANGLEY
Rose-Hulman Institute of Technology
Terre Haute, IN 47803
langley@rose-hulman.edu

DAVID LEVITT
Carnegie Mellon University
Pittsburgh, PA 15213

JOSEPH ROWER
California Lutheran University
Thousand Oaks, CA 91360

How close to abelian can a nonabelian finite group be? Consider the dihedral group of the square, D_4. We'll denote the counterclockwise rotations of the square in multiples of 90 degrees by r_0, r_{90}, r_{180}, and r_{270}, and the reflections of the square around its horizontal axis, vertical axis, and the two diagonals by h, v, d, and u, respectively. The following chart lends insight into the commutativity of D_4, where a 1 indicates that the corresponding pair of elements commute [**7**]:

	r_0	r_{90}	r_{180}	r_{270}	h	v	d	u
r_0	1	1	1	1	1	1	1	1
r_{90}	1	1	1	1	0	0	0	0
r_{180}	1	1	1	1	1	1	1	1
r_{270}	1	1	1	1	0	0	0	0
h	1	0	1	0	1	1	0	0
v	1	0	1	0	1	1	0	0
d	1	0	1	0	0	0	1	1
u	1	0	1	0	0	0	1	1

A similar chart for an abelian group would contain all 1s, and so a natural measure of the *abelianness* of a finite group is the number of 1s in the chart divided by the number of entries. That is, let

$$\mathrm{Comm}(G) = |\{(a, b) \in G \times G \mid ab = ba\}|,$$

where for any set A, $|A|$ denotes the number of elements in the set, and define

$$\Pr(G) = \frac{\mathrm{Comm}(G)}{|G|^2}.$$

The quantity $\Pr(G)$ is often interpreted as the probability that two elements in G commute [**4, 6, 7**], viewing the set of all ordered pairs of group elements as the sample space and the set counted by $\mathrm{Comm}(G)$ as the event that a randomly selected pair commutes. There are forty 1s in the above chart, so the probability that two elements of D_4 commute is $\Pr(D_4) = 40/64 = 5/8$. (A discussion of $\Pr(G)$ for other dihedral groups and their direct products also appears in this MAGAZINE [**1**].)

Math. Mag. **84** (2011) 128–136. doi:10.4169/math.mag.84.2.128. © Mathematical Association of America

It turns out that $5/8$ is the maximum value of $\Pr(G)$ for any nonabelian finite group [**3, 4, 6, 7**]. A closer examination of the chart reveals that the key to understanding this result lies, as is so often the case in group theory, in understanding the role of certain subgroups. The 1s in a given row (or column) indicate the elements in the *centralizer* of the corresponding element of D_4. For example, the centralizer of h, denoted $C(h)$, is the set $\{r_0, r_{180}, h, v\}$, as indicated by the 1s in the 1st, 3rd, 5th, and 6th columns of the chart in the row indexed by h. Two elements, r_0 and r_{180}, are distinguished by the fact that their centralizers are all of D_4, indicated by a row of 1s in the chart. These two elements form the *center* of D_4, denoted $Z(D_4)$.

We would expect highly commutative groups to have a large center and large centralizers. How large? By Lagrange's Theorem the sizes of the center and centralizers in a finite group G must divide $|G|$. But if $g \in G$ is not in $Z(G)$, then $Z(G) \subsetneq C(g) \subsetneq G$. So $|C(g)| \le |G|/2$ and $|Z(G)| \le |C(g)|/2 \le |G|/4$. In particular, if $|Z(G)| = |G|/4$, then $|C(g)| = |G|/2$ for all $g \notin Z(G)$. Therefore the sizes of the center and centralizers in D_4, relative to the size of D_4, are as large as possible for any nonabelian finite group. With $|Z(G)| = |G|/4$, then, we have

$$\begin{aligned}\mathrm{Comm}(G) &= \sum_{g\in G} |C(g)| \\ &= \sum_{g\in Z(G)} |C(g)| + \sum_{g\notin Z(G)} |C(g)| \\ &= \sum_{g\in Z(G)} |G| + \sum_{g\notin Z(G)} \frac{1}{2}|G| \\ &= \frac{1}{4}|G|\cdot|G| + \frac{3}{4}|G|\cdot\frac{1}{2}|G| \\ &= \frac{5}{8}|G|^2,\end{aligned}$$

and therefore $\Pr(G) = 5/8$.

An elegant result to be sure, but not the end of the story. We will show that this bound is in fact a special case of two more general results that involve products of several group elements. We obtain the first such result by generalizing the equation $ab = ba$ to $a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$ and defining

$$\mathrm{Comm}_n(G) = |\{(a_1, a_2, \ldots, a_n) \in G^n \mid a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1\}|$$

and

$$P_n(G) = \frac{\mathrm{Comm}_n(G)}{|G|^n}$$

for $n \ge 2$. Then $P_n(G)$ is the probability that a product of n group elements is equal to its reverse, and $P_2(G) = \Pr(G)$. It is still true that $P_n(G) = 1$ if and only if G is abelian since, for example, if $P_n(G) = 1$, then for any $a, b \in G$,

$$ab = abe^{n-2} = e^{n-2}ba = ba$$

where e is the identity element of G. For nonabelian groups, bounds on $P_n(G)$ naturally extend the $5/8$ bound. The first few values are

$$\begin{aligned} &P_2(G) \le 5/8 \qquad P_4(G) \le 17/32 \qquad P_6(G) \le 65/128 \\ &P_3(G) \le 5/8 \qquad P_5(G) \le 17/32 \qquad P_7(G) \le 65/128, \end{aligned}$$

and in general, we'll prove the following theorem.

THEOREM 1. *For a nonabelian finite group G and n even, the probability that a product of n group elements is equal to its reverse, $P_n(G)$, satisfies*

1. $P_n(G) \leq \frac{1}{2} + \frac{1}{2^{n+1}}$ *and*
2. $P_{n+1}(G) = P_n(G)$.

Not surprisingly, the bounds are again realized when $|Z| = |G|/4$. We'll also discuss a conjecture that Theorem 1 is actually a special case of a broader result dealing with the number of transpositions in the rearrangement of the product $a_1a_2\cdots a_n$. Questions for undergraduate research arise.

For the second generalization, let a permutation σ in the symmetric group S_n act on a product of n group elements by scrambling it so that the ith element in the product ends up in the $\sigma(i)$th position. For example, if $\sigma \in S_4$ is the four-cycle $(1, 2, 3, 4)$, then

$$(a_1a_2a_3a_4)^{\sigma} = a_4a_1a_2a_3.$$

If $\sigma = (1, 2, \ldots, n)^j$ for some j, $1 \leq j \leq n-1$, we'll call $(a_1a_2\cdots a_n)^{\sigma}$ a *cyclic rearrangement* of the product $a_1a_2\cdots a_n$. For example, the three cyclic rearrangements of $a_1a_2a_3a_4$ are $a_4a_1a_2a_3$, $a_3a_4a_1a_2$, and $a_2a_3a_4a_1$.

We can then view the equation $ab = ba$ as $ab = (ab)^{(1,2)}$ and ask the more general question: What is the probability that a product $a_1a_2\cdots a_n$ is equal to at least one cyclic rearrangement of itself? Specifically, define

$$\text{Comm}_n^{\text{cyc}}(G) = |\{(a_1, a_2, \ldots, a_n) \in G^n \mid a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^{(1,2,\ldots,n)^j} \text{ for some } j, 1 \leq j \leq n-1\}|$$

and set

$$P_n^{\text{cyc}}(G) = \frac{\text{Comm}_n^{\text{cyc}}(G)}{|G|^n}.$$

Then once again, $P_2^{\text{cyc}}(G) = \Pr(G)$ and $P_n^{\text{cyc}}(G) = 1$ if and only if G is abelian. For nonabelian groups,

$$P_2^{\text{cyc}}(G) \leq 5/8 \qquad P_4^{\text{cyc}}(G) \leq 29/32$$
$$P_3^{\text{cyc}}(G) \leq 13/16 \qquad P_5^{\text{cyc}}(G) \leq 61/64,$$

and in general, the following theorem.

THEOREM 2. *For a nonabelian finite group G and $n \geq 2$, the probability that a product of n group elements is equal to a cyclic rearrangement of itself, $P_n^{cyc}(G)$, satisfies*

$$P_n^{\text{cyc}}(G) \leq 1 - \frac{3}{2^{n+1}}.$$

It's interesting to note that while both $P_n(G)$ and $P_n^{\text{cyc}}(G)$ generalize the probability that two elements commute, $P_n(G)$ tends to $1/2$ as n approaches infinity while $P_n^{\text{cyc}}(G)$ tends to 1.

The probability that a product is equal to its reverse To approach Theorem 1, we'll start with the following stronger version of the second part of the theorem with $n = 2$, which is interesting in its own right. First, fix x in a finite group G and set

$$\text{Comm}_x(G) = |\{(a, b) \in G \times G \mid axb = bxa\}|$$

and

$$P_x(G) = \frac{\mathrm{Comm}_x(G)}{|G|^2},$$

so that $P_x(G)$ is the probability that two group elements "commute" around a fixed middle element.

PROPOSITION 1. *For any x in a finite group G, we have $P_x(G) = \Pr(G)$.*

Note that if $x \notin Z(G)$, Proposition 1 does not imply that the pairs (a, b) that satisfy $axb = bxa$ are the same pairs that satisfy $ab = ba$, only that the same number of pairs satisfy each equation.

The following elementary facts will facilitate the proof of Proposition 1, and later Theorem 1. All are good exercises for students.

LEMMA 1. *Let G be a finite group with center $Z(G)$.*

1. *Suppose a and b are conjugate in G, that is, the equation $x^{-1}ax = b$ has at least one solution for x in G. Then the number of such solutions is $|C(a)|$.*
2. *The products ab and ba are conjugate for all $a, b \in G$.*
3. *For any $a, b \in G$, if ab is in $Z(G)$ then $ab = ba$.*

Proof of Proposition 1. Rewrite $axb = bxa$ as $b^{-1}(ax)b = xa$. By Lemma 1, ax and xa are conjugate, and the number of choices for b is $|C(ax)|$. So

$$\mathrm{Comm}_x(G) = \sum_{a\in G} |C(ax)| = \sum_{g\in G} |C(g)| = \mathrm{Comm}(G).$$

Dividing both sides by $|G|^2$ completes the proof. ■

Since x is arbitrary, a direct consequence of Proposition 1 is that

$$P_3(G) = \frac{\sum_{x\in G} \mathrm{Comm}_x(G)}{|G|^3} = \frac{\sum_{x\in G} \mathrm{Comm}(G)}{|G|^3} = \frac{|G| \cdot \mathrm{Comm}(G)}{|G|^3}$$
$$= \frac{\mathrm{Comm}(G)}{|G|^2} = \Pr(G),$$

which proves Theorem 1 with $n = 3$. This provides the basis for an inductive proof.

Proof of Theorem 1. We'll give an inductive argument for n even. Since $P_2(G) = P_3(G)$, the case with n odd follows similarly. So suppose

$$P_n(G) \le \frac{1}{2} + \frac{1}{2^{n+1}}$$

for a positive even integer n. We need to show

$$P_{n+2}(G) \le \frac{1}{2} + \frac{1}{2^{n+3}}.$$

So we're interested in when $a_1a_2\cdots a_{n+1}a_{n+2} = a_{n+2}a_{n+1}\cdots a_2a_1$. Fix $a_2\cdots a_{n+1}$ and consider two cases.

1. $a_1a_2\cdots a_{n+1} \in Z(G)$. This occurs for $|Z(G)|$ choices of a_1, namely $a_1 = z(a_2\cdots a_{n+1})^{-1}$ for $z \in Z(G)$. Since $a_1a_2\cdots a_{n+1}$ is in $Z(G)$ and therefore by Lemma 1 a_1 and $a_2\cdots a_{n+1}$ commute, the equation

$$a_1a_2\cdots a_{n+1}a_{n+2} = a_{n+2}a_{n+1}\cdots a_2a_1$$

reduces to

$$a_2 \cdots a_{n+1} = a_{n+1} \cdots a_2.$$

By the inductive assumption, this equation is satisfied by at most

$$\left(\frac{1}{2} + \frac{1}{2^{n+1}}\right)|G|^n$$

n-tuples $(a_2, \ldots, a_{n+1})$. Since we have $|Z(G)|$ choices for a_1 and $|G|$ choices for a_{n+2} to fill out an $(n+2)$-tuple $(a_1, a_2, \ldots, a_{n+1}, a_{n+2})$ satisfying $a_1 a_2 \cdots a_{n+1} a_{n+2} = a_{n+2} a_{n+1} \cdots a_2 a_1$, we obtain a bound of

$$|Z(G)| \left(\frac{1}{2} + \frac{1}{2^{n+1}}\right)|G|^{n+1}$$

on the number of such $(n+2)$-tuples.

2. $a_1 \cdots a_{n+1} \notin Z(G)$. This occurs for $|G| - |Z(G)|$ choices for a_1. Viewing the reverse equation in terms of conjugation, we need to find a_{n+2} so that

$$a_{n+2}^{-1}(a_1 a_2 \cdots a_{n+1}) a_{n+2} = a_{n+1} \cdots a_2 a_1.$$

This is only possible if $a_1 a_2 \cdots a_{n+1}$ and $a_{n+1} \cdots a_2 a_1$ are conjugate. In the event that they are, the number of choices for a_{n+2} is $|C(a_1 a_2 \cdots a_{n+1})|$. Since the choice of a_2 through a_{n+1} is arbitrary, by assuming all products $a_1 a_2 \cdots a_{n+1}$ and $a_{n+1} \cdots a_2 a_1$ not in $Z(G)$ are conjugate we can bound the number of $(n+2)$-tuples in this case by

$$|G|^n \sum_{g \in G - Z(G)} |C(g)| \leq |G|^n (|G| - |Z(G)|) \cdot \frac{1}{2}|G| = \frac{1}{2}|G|^{n+1}(|G| - |Z(G)|).$$

Combining cases 1 and 2, and recalling that $|Z(G)| \leq |G|/4$, we have

$$\begin{aligned}
\mathrm{Comm}_{n+2}(G) &\leq |Z(G)| \left(\frac{1}{2} + \frac{1}{2^{n+1}}\right)|G|^{n+1} + \frac{1}{2}|G|^{n+1}(|G| - |Z(G)|) \\
&= \frac{1}{2^{n+1}}|Z(G)||G|^{n+1} + \frac{1}{2}|G|^{n+2} \\
&\leq \frac{1}{2^{n+1}} \cdot \frac{1}{4}|G| \cdot |G|^{n+1} + \frac{1}{2}|G|^{n+2} \\
&= \left(\frac{1}{2} + \frac{1}{2^{n+3}}\right)|G|^{n+2}.
\end{aligned}$$

Dividing by $|G|^{n+2}$ completes the induction. ∎

If $|Z(G)| = |G|/4$, all products $a_1 a_2 \cdots a_{n+1}$ and $a_{n+1} \cdots a_2 a_1$ not in $Z(G)$ are conjugate (and therefore the bound in Theorem 1 is realized). The proof is not trivial, but it relies on the interesting fact that in such groups the product

$$a_1 a_2 \cdots a_n a_1^{-1} a_2^{-1} \cdots a_n^{-1}$$

is a commutator, that is,

$$a_1 a_2 \cdots a_n a_1^{-1} a_2^{-1} \cdots a_n^{-1} = xyx^{-1}y^{-1}$$

for some x and y.

Restating the problem in terms of transpositions In an attempt to generalize Theorem 1 (and looking ahead to Theorem 2) we'll now view the reverse of a product of group elements in terms of a permutation acting on the product. For example,

$$\begin{aligned}(a_1a_2)^{(1,2)} &= a_2a_1\\ (a_1a_2a_3)^{(1,3)} &= a_3a_2a_1\\ (a_1a_2a_3a_4)^{(1,4)(2,3)} &= a_4a_3a_2a_1\\ (a_1a_2a_3a_4a_5)^{(1,5)(2,4)} &= a_5a_4a_3a_2a_1,\end{aligned}$$

and so on. So we can reformulate the reversal equation

$$a_1a_2\cdots a_n = a_n\cdots a_2a_1 \quad \text{as} \quad a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^{\sigma}$$

where $\sigma = (1,n)(2,n-1)\cdots$. Since the number of transpositions in the disjoint cycle notation for σ is $\lfloor n/2 \rfloor$, we can rephrase Theorem 1 as

$$P_n(G) \le \frac{1}{2} + \frac{1}{2^{2k+1}}$$

where k is the number of transpositions in the disjoint cycle notation of $\sigma = (1,n)(2,n-1)\cdots$.

This leads naturally to the following question. For any $\sigma \in S_n$, let $P_n^{\sigma}(G)$ be the probability that $a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^{\sigma}$. Is there a nice bound for $P_n^{\sigma}(G)$, and does it depend on transpositions? Well, it appears so, and almost. Let $n = 4$ and $\sigma = (1,3)(2,4)$. Consider the equation

$$a_1a_2a_3a_4 = (a_1a_2a_3a_4)^{(1,3)(2,4)} = a_3a_4a_1a_2.$$

Although σ factors into two transpositions, we can show that $P_4^{\sigma}(G) \le \frac{5}{8}$, the bound for one transposition. The reason? We can view the preceding equation as

$$(a_1a_2)(a_3a_4) = (a_3a_4)(a_1a_2),$$

the action of transposing two blocks of consecutive elements. This leads to the following definition.

DEFINITION 1. A *block transposition* is a permutation that transposes two disjoint blocks of consecutive elements.

In our example, σ transposes the blocks $[1,2]$ and $[3,4]$, so we'll write $\sigma = (1,3)(2,4) = ([1,2],[3,4])$. We allow the blocks to have size 1, so a regular transposition is a block transposition. The blocks also may have different sizes. For example,

$$(a_1a_2a_3a_4a_5)^{(1,3,5,2,4)} = (a_4a_5)(a_1a_2a_3),$$

so $(1,3,5,2,4) = ([1,2,3],[4,5])$.

Much experimental evidence, obtained with the computational algebra package GAP, suggests the following conjecture, generalizing Theorem 1.

CONJECTURE 1. *For a nonabelian finite group G, $n \ge 2$, and $\sigma \in S_n$,*

$$P_n^{\sigma}(G) \le \frac{1}{2} + \frac{1}{2^{2k+1}}$$

where k is the fewest number of block transpositions in a factorization of σ.

This presents two interesting problems. One, to prove (or disprove, but hopefully not) the conjecture. Two, to determine a fast way to factor a given permutation σ into block transpositions. Consider $\sigma = (1, 2, 3, 5, 4)$ in S_5 and the equation

$$a_1a_2a_3a_4a_5 = (a_1a_2a_3a_4a_5)^{\sigma} = a_4a_1a_2a_5a_3.$$

How many block transpositions are lurking? We can turn $a_1a_2a_3a_4a_5$ into $a_4a_1a_2a_5a_3$ in the following two steps:

$$a_1a_2(a_3)a_4(a_5) \to a_1a_2(a_5)a_4(a_3) = (a_1a_2a_3a_4a_5)^{(3,5)}$$

and

$$(a_1a_2a_5)(a_4)a_3 \to (a_4)(a_1a_2a_5)a_3 = (a_1a_2a_5a_4a_3)^{([1,2,3],4)}.$$

So $(1, 2, 3, 5, 4) = ([1, 2, 3], 4)(3, 5)$ where we multiply from right to left, and therefore we conjecture that

$$P_n^{(1,2,3,5,4)}(G) \le 17/32.$$

In the case where the block transpositions in the factorization of σ are disjoint, we can reduce to the case where all blocks have size 1, and where there are no consecutive fixed points. For example, consider

$$(a_1a_2a_3a_4a_5a_6a_7a_8)^{([1,2],[7,8])(3,6)} = (a_7a_8)a_6(a_4a_5)a_3(a_1a_2).$$

By viewing the products in parentheses as single elements, it's not hard to show that

$$P_8^{([1,2],[7,8])(3,6)}(G) = P_5^{(1,5)(2,4)}(G).$$

Cyclic rearrangements We now return to Theorem 2 and the idea of a cyclic rearrangement. We wish to bound the probability that $a_1a_2\cdots a_n$ is equal to at least one of the following:

$$\begin{aligned}
(a_1a_2\cdots a_n)^{(1,2,\dots,n)} &= a_na_1a_2\dots a_{n-1}\\
(a_1a_2\cdots a_n)^{(1,2,\dots,n)^2} &= a_{n-1}a_na_1a_2\dots a_{n-2}\\
&\vdots\\
(a_1a_2\cdots a_n)^{(1,2,\dots,n)^{n-1}} &= a_2\cdots a_{n-1}a_na_1.
\end{aligned}$$

It's interesting to note that each cyclic rearrangement of $a_1a_2\cdots a_n$ results from a single block transposition of the form

$$([a_1\cdots a_i], [a_{i+1}\cdots a_n]).$$

So the probability that $a_1a_2\cdots a_n$ is equal to one particular cyclic rearrangement of itself is at most 5/8.

Proof of Theorem 2. We would like to count all n-tuples $(a_1, a_2, \dots, a_n)$ that satisfy at least one of the conditions

$$a_1a_2\cdots a_n = (a_1a_2\cdots a_n)^{(1,2,\dots,n)^j}, \quad 1 \le j \le n-1.$$

Instead we'll count the complement, that is, the number of $(a_1, a_2, \dots, a_n)$ for which

$$a_1a_2\cdots a_n \ne (a_1a_2\cdots a_n)^{(1,2,\dots,n)^j}$$

for all j, $1 \le j \le n-1$. These conditions imply that $g = a_1 a_2 \cdots a_n \notin Z(G)$, since by Lemma 1, $a_1 a_2 \cdots a_n \in Z(G)$ implies

$$a_1 a_2 \cdots a_n = (a_{n-j+1} \cdots a_n)(a_1 \cdots a_{n-j}) = (a_1 a_2 \cdots a_n)^{(1,2,\ldots,n)^j}$$

for *all* j. Now let $g = a_1 a_2 \cdots a_n$ and $h_i = a_{i+1} \cdots a_n$ for $1 \le i \le n-1$. Then $h_i \notin C(g)$ for all i since

$$g = (a_1 \cdots a_i)(a_{i+1} \cdots a_n) \neq (a_{i+1} \cdots a_n)(a_1 \cdots a_i) = h_i(g h_i^{-1})$$

if and only if $g h_i \neq h_i g$.

So for each $g \notin Z(G)$, and h_1 through h_{n-1} (not necessarily distinct) not in $C(g)$, we can write

$$g = (g h_1^{-1})(h_1 h_2^{-1})(h_2 h_3^{-1}) \cdots (h_{n-2} h_{n-1}^{-1}) h_{n-1}$$

and set

$$a_1 = g h_1^{-1}, \quad a_2 = h_1 h_2^{-1}, \quad a_3 = h_2 h_3^{-1}, \quad \ldots, \quad a_n = h_{n-1}.$$

Then for each i, $1 \le i \le n-1$, we have $h_i = a_{i+1} \cdots a_n$ with $h_i \notin C(g)$, and therefore

$$(a_1 \cdots a_i)(a_{i+1} \cdots a_n) \neq (a_{i+1} \cdots a_n)(a_1 \cdots a_i),$$

as required.

So in general, the number of n tuples $(a_1, a_2, \ldots, a_n)$ that we seek is equal to

$$\sum_{g \notin Z(G)} (|G| - |C(g)|)^{n-1}.$$

Since $|C(g)| \le |G|/2$ and $|Z(G)| \le |G|/4$, this is at least $\frac{3}{4}|G| \left(\frac{1}{2}|G|\right)^{n-1} = \frac{3}{2^{n+1}}|G|^n$ (with equality exactly when $|Z(G)| = |G|/4$), so

$$P_n^{\text{cyc}}(G) \le \frac{|G|^n - \frac{3}{2^{n+1}}|G|^n}{|G|^n} = 1 - \frac{3}{2^{n+1}}. \qquad \blacksquare$$

For further consideration We'll conclude with a generalization of Theorem 2 that suggests avenues of further investigation. Let A be a fixed subset of $\{(1, 2, \ldots, n)^i \mid 1 \le i \le n-1\}$. Then what is the probability that $a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma$ for at least one $\sigma \in A$? If $|A| = 1$ the answer is at most $5/8$, and Theorem 2 gives an upper bound when $|A| = n-1$. A slight modification of the proof will show that this probability is at most $1 - \frac{3}{2^{k+2}}$ where $|A| = k$. Now, instead of restricting to cyclic rearrangements, let A be any set of k permutations, each of which factors into a single block transposition. When does this bound still hold? What about permutations that factor into two block transpositions? We believe that the bound for a particular rearrangement due to one permutation that factors into two block transpositions is 17/32 (Conjecture 1). What about a set of permutations, each of which factors into two block transpositions? Is there a generalization along the lines of Theorem 2 for the right set of permutations?

Theorem 2 can also be viewed as addressing a special case of the following question: What is the probability that $a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_n)^\sigma$ for at least one $\sigma \in A$ where A consists of the nonidentity elements of a subgroup of S_n? In Theorem 2 the subgroup is the cyclic subgroup generated by $(1, 2, \ldots, n)$. What about other cyclic subgroups? Other subgroups? In particular, this question has been studied when the subgroup in question is all of S_n [**5**]. A group in which every product $a_1 a_2 \cdots a_n$ is equal to at least one non-identity permutation of itself is called n-rewriteable. The groups that realize the $5/8$ bound are 3-rewriteable [**5**], and it has been shown that the probability that a product $a_1 a_2 a_3$ is equal to at least one non-identity permutation of itself is either 1 or at most $17/18$ [**2**].

Finally, there is another useful characterization of $\Pr(G)$ that turns the problem of determining the probability that two elements commute into an exercise in counting conjugacy classes:

$$\Pr(G) = \frac{\text{the number of conjugacy classes in } G}{|G|}$$

[**3, 7**]. Are there analogous statements for the other probabilities that we've discussed?

Acknowledgment The authors thank Gary Sherman for introducing them to the topic, and the referees for many helpful suggestions.

REFERENCES

1. C. Clifton, D. Guichard, and P. Keef, How commutative are direct products of dihedral groups? *Math. Mag.* **84** (2011) 137–140.
2. J. S. Ellenberg, An upper bound for 3-rewriteability in finite groups, Rose-Hulman Institute of Technology MS TR 91-02, 1991.
3. Joseph Gallian, *Contemporary Abstract Algebra*, 7th ed., Brooks Cole, Belmont, CA, 2009.
4. W. H. Gustafson, What is the probability that two group elements commute?, *Amer. Math. Monthly* **80** (1973) 1031–1034. doi:10.2307/2318778
5. J. L. Leavitt, G. J. Sherman, and M. E. Walker, Rewriteability in finite groups, *Amer. Math. Monthly* **99** (1992) 446–452. doi:10.2307/2325089
6. David J. Rusin, What is the probability that two elements of a finite group commute? *Pacific J. Math.* **82** (1979) 237–247.
7. Gary J. Sherman, Trying to do group theory with undergraduates and computers, *J. Symb. Comp.* **23** (1997) 577–587. doi:10.1006/jsco.1996.0108

Summary The probability that two elements in a nonabelian finite group commute is at most $5/8$, and this bound is realized exactly when the center of the group is one fourth of the group. We generalize this result by finding similar bounds on the probability that a product of several group elements is equal to its reverse, and the probability that a product is equal to at least one cyclic rearrangement of itself. Both of these naturally extend the $5/8$ bound.

How Commutative Are Direct Products of Dihedral Groups?

CODY CLIFTON
University of Kansas
Lawrence, KS 66045
cclifton@math.ku.edu

DAVID GUICHARD
Whitman College
Walla Walla, WA, 99362
guichard@whitman.edu

PATRICK KEEF
Whitman College
Walla Walla, WA, 99362
keef@whitman.edu

In his popular text on abstract algebra, Gallian describes a way to measure the commutativity of a finite group G [**3**, pp. 397–398]. An ordered pair $(a, b) \in G \times G$ is said to be *commuting* if $ab = ba$. If $\mathrm{Comm}(G)$ is the number of commuting pairs, then let

$$\Pr(G) = \mathrm{Comm}(G)/|G|^2$$

(where $|S|$ is the cardinality of the set S). In other words, $\Pr(G)$ is the probability that two randomly selected elements of the group actually commute.

A great deal is known about the set of fractions that can occur as $\Pr(G)$ for some group G [**2, 4, 6, 7**]. For example, if $1/2 < x \le 1$, then there is a group G with $x = \Pr(G)$ if and only if $x = (1 + 4^k)/(2 \cdot 4^k)$ for some non-negative integer k (see the chart on p. 246 of [**7**]). For example, if $k = 0$, then $\Pr(G) = 1$ and G is abelian. And if $k = 1$, then $x = 5/8$ is the largest value of $P(G)$ for a non-abelian group. In addition, the only other possible values of $P(G)$ greater than $11/32$ are $3/8$, $25/64$, $2/5$, $11/27$, $7/16$, and $1/2$. (This upper bound for Pr(G) is generalized in [**5**].)

This note, which is based on [**1**], addresses the following question: Given a positive integer m, is there an easily constructed group G such that $\Pr(G) = 1/m$? For example, if $m = 100$, then we are asking if there is a straightforward way to find a group such that two randomly selected elements of the group commute precisely one percent of the time. Our main result (Theorem 2) produces such a group G that is a direct product of dihedral groups.

We also show (Theorem 3) that for any positive integer m there is a direct product of dihedral groups G such that $\Pr(G) = m/m'$, where m, m' are relatively prime; in fact, such a G can be found that is itself a dihedral group. We close by showing that there is a finite group H such that $\Pr(H)$ is not a member of the set $\{\Pr(G) : G$ is a direct product of dihedral groups$\}$.

Recall that if n is a positive integer, then the dihedral group D_n is generated by two elements, ρ (for "rotation") and ϕ (for "flip"), subject to the relations

$$\rho^n = \phi^2 = e \quad \text{and} \quad \phi\rho = \rho^{-1}\phi. \tag{1}$$

It follows that the elements of D_n can be written as

$$e, \rho, \ldots, \rho^{n-1}, \phi, \rho\phi, \ldots, \rho^{n-1}\phi,$$

Math. Mag. **84** (2011) 137–140. doi:10.4169/math.mag.84.2.137. © Mathematical Association of America

so that $|D_n| = 2n$ is even. If $n \geq 3$, then D_n is usually interpreted as the symmetries of a regular n-gon in the plane.

Our main computational tool will be the following result.

THEOREM 1. *If n is a positive integer, then*

$$\Pr(D_n) = \begin{cases} \dfrac{n+3}{4n} & \text{if } n \text{ is odd;} \\ \dfrac{n+6}{4n} & \text{if } n \text{ is even.} \end{cases}$$

Proof. An easy computation using the relations (1) shows that, whether n is odd or even, we have commuting pairs (ρ^i, ρ^j) for all $0 \leq i, j < n$, as well as $(\rho^i \phi, e)$, $(e, \rho^i \phi)$ and $(\rho^i \phi, \rho^i \phi)$ for all $0 \leq i < n$.

If n is odd, this is actually a complete list, so that there are $n^2 + 3n$ commuting pairs. On the other hand, if n is even, then we have the additional commuting pairs $(\rho^i \phi, \rho^{i+(n/2)})$, $(\rho^{i+(n/2)}, \rho^i \phi)$, and $(\rho^i \phi, \rho^{i+(n/2)} \phi)$ for all $0 \leq i < n$. Therefore, when n is even there are $n^2 + 6n$ commuting pairs. Since $|D_n|^2 = 4n^2$, the result follows. ■

If n is a positive integer, we let $d_n = \Pr(D_n)$. If n is odd, it follows that

$$d_n = \frac{n+3}{4n} = \frac{2n+6}{4(2n)} = d_{2n},$$

so that $\{d_n : n \text{ is a positive integer}\} = \{d_n : n \text{ is an even positive integer}\} = \{1, 5/8, 1/2, 7/16, 2/5, 3/8, 5/14, \dots\}$.

We denote the direct product of the groups G and H by $G \oplus H$, which is the cartesian product $G \times H$ with the usual coordinate-wise operation. It is easy to verify that $\text{Comm}(G \oplus H) = \text{Comm}(G) \cdot \text{Comm}(H)$, so

$$\Pr(G \oplus H) = \frac{\text{Comm}(G \oplus H)}{|G \oplus H|^2} = \frac{\text{Comm}(G)}{|G|^2} \cdot \frac{\text{Comm}(H)}{|H|^2} = \Pr(G) \cdot \Pr(H).$$

This gives the following well-known result (see, for example, p. 1033 of [**4**]).

LEMMA 1. *If G and H are finite groups, then* $\Pr(G \oplus H) = \Pr(G) \cdot \Pr(H)$.

Let $\mathcal{D}$ be the set of all possible fractions that can appear as $\Pr(G)$, where G is isomorphic to a direct product of dihedral groups. By the lemma, $\mathcal{D}$ is the set of all possible products of the form $d_{n_1} \cdots d_{n_k}$, where $n_1, \dots, n_k$ are positive integers. Clearly, $\mathcal{D}$ is closed under multiplication.

Building denominators

This brings us to our main result.

THEOREM 2. *For every positive integer m, there is a collection of dihedral groups, $D_{n_1}, \dots, D_{n_k}$, such that*

$$\Pr(D_{n_1} \oplus \cdots \oplus D_{n_k}) = \frac{1}{m}.$$

Proof. We want to show for all m, that $1/m \in \mathcal{D}$. Note that

$$\frac{1}{1} = d_1 \in \mathcal{D}, \ \frac{1}{2} = d_3 \in \mathcal{D}, \ \frac{1}{3} = d_9 \in \mathcal{D},$$

so assume $m \geq 4$ and the result holds for all positive integers $m' < m$.

If m is even, then $m = 2m'$ for some positive integer $m' < m$. It follows that $1/m' \in \mathcal{D}$, so that

$$\frac{1}{m} = \frac{1}{2} \cdot \frac{1}{m'} = d_3 \cdot \frac{1}{m'} \in \mathcal{D}.$$

If m is odd, then it is of the form either $4j + 1$ or $4j + 3$ for some positive integer j. If $m = 4j + 1$, then let $n = 8j + 2 = 2m$ and $m' = j + 1 < m$. We then have

$$d_n = \frac{n+6}{4n} = \frac{8j+8}{32j+8} = \frac{j+1}{4j+1} = \frac{m'}{m}.$$

On the other hand, if $m = 4j + 3$, let $n = 24j + 18 = 6m$ and $m' = j + 1 < m$. Now,

$$d_n = \frac{n+6}{4n} = \frac{24j+24}{96j+72} = \frac{j+1}{4j+3} = \frac{m'}{m}.$$

In either case, by induction, $1/m' \in \mathcal{D}$, so that

$$\frac{1}{m} = \frac{m'}{m} \cdot \frac{1}{m'} = d_n \cdot \frac{1}{m'} \in \mathcal{D},$$

which completes the proof. ■

The above argument is actually an algorithm for expressing $1/m$ as $\Pr(G)$, where G is a direct product of dihedral groups. For example, if we consider the question mentioned at the beginning of constructing a group such that the probability of two elements commuting is exactly one percent, it yields

$$\begin{aligned}\frac{1}{100} = d_3 \cdot \frac{1}{50} = d_3 \cdot d_3 \cdot \frac{1}{25} &= d_3 \cdot d_3 \cdot d_{50} \cdot \frac{1}{7} \\ &= d_3 \cdot d_3 \cdot d_{50} \cdot d_{42} \cdot \frac{1}{2} = d_3 \cdot d_3 \cdot d_{50} \cdot d_{42} \cdot d_3.\end{aligned}$$

So $1/100 = \Pr(G)$ where G is a group of order $6^3 \cdot 100 \cdot 84 = 1{,}814{,}400$. Clearly, though the method is easy to apply, it can produce groups that are exceptionally large.

Every fraction $1/m$ is a product of fractions of the form d_n, but this expression is not unique. For example,

$$d_4 \cdot d_5 = \frac{5}{8} \cdot \frac{2}{5} = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = d_3 \cdot d_3.$$

Building numerators

We now show that every positive integer also appears as the numerator of an element of $\mathcal{D}$ written in lowest terms.

THEOREM 3. *If m is a positive integer, then there is a dihedral group D_n such that*

$$\Pr(D_n) = \frac{m}{m'},$$

where m' is an integer relatively prime to m.

Proof. Let $n = 24m - 6$, which is an even positive integer, and $m' = 4m - 1$. It follows that

$$\Pr(D_n) = \frac{24m - 6 + 6}{96m - 24} = \frac{m}{m'},$$

and since $1 = 4m - m'$, we can conclude that m and m' are relatively prime. ■

For example, if we want $m = 10$ as a numerator, we need only set $n = 234$, so that $d_{234} = 240/(4 \cdot 234) = 10/39$. Again, in Theorem 2 we might have to take the product of many dihedral groups to show that $1/m \in \mathcal{D}$, but in Theorem 3 it was only necessary to use a single dihedral group to show $m/m' \in \mathcal{D}$.

It is natural to ask if there are groups H for which $\Pr(H)$ is not in $\mathcal{D}$. To construct such an example, by [**7**] there is a group H such that $\Pr(H) = (1 + 16)/2 \cdot 16 = 17/32$. If n is an even positive integer with

$$\frac{17}{32} = d_n = \frac{n + 6}{4n},$$

then we could conclude that $68n = 32n + 192$, i.e., $n = 16/3$, which is not an integer. On the other hand, any element of $\mathcal{D}$ which is the product of at least two $d_n < 1$ can be no larger than

$$\left(\frac{5}{8}\right)^2 = \frac{25}{64} < \frac{17}{32}.$$

Therefore, $\Pr(H)$ is not in $\mathcal{D}$.

REFERENCES

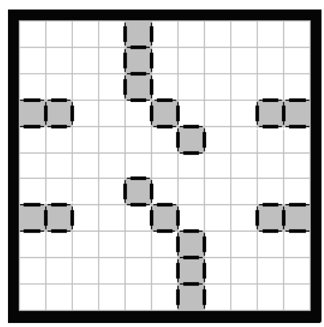
1. C. Clifton, Commutativity in non-abelian groups, Senior Project Report, Whitman College, 2010.
2. P. Gallagher, The number of conjugacy classes in a finite group, *Math. Z.* **118** (1970) 175–179. doi:10.1007/BF01113339
3. J. Gallian, *Contemporary Abstract Algebra*, 7th ed., Brooks Cole, Belmont, CA, 2010.
4. W. H. Gustafson, What is the probability that two group elements commute? *Amer. Math. Monthly* **80** (1973) 1031–1034. doi:10.2307/2318778
5. T. Langley, D. Levitt, and J. Rower, Two generalizations of the 5/8 bound on commutativity in nonabelian finite groups, *Math. Mag.* **84** (2011) 128–136. doi:10.4169/math.mag.84.2.128
6. D. MacHale, How commutative can a non-commutative group be? *Math. Gaz.* **58** (1974) 199–202. doi:10.2307/3615961
7. D. Rusin, What is the probability that two elements of a finite group commute? *Pacific J. Math.* **82** (1979) 237–247.

Summary If G is a finite group, then $\Pr(G)$ is the probability that two randomly selected elements of G commute. So G is abelian iff $\Pr(G) = 1$. For any positive integer m, we show that there is a group G which is a direct product of dihedral groups such that $\Pr(G) = 1/m$. We also show that there is a dihedral group G such that $\Pr(G) = m/m'$, where m' is relatively prime to m.

Crossword Word Count

MATTHEW DUCHNOWSKI
Newtown, PA
mattduchnowski@yahoo.com

The number of black squares in a crossword puzzle cannot alone determine the number of words that the puzzle contains. Interestingly though, the number of marks needed to bound these black squares provides additional information sufficient for making the calculation. As illustrated below, marks are used to outline all of the puzzle's black squares, but are not required at the puzzle's perimeter.



THEOREM 1. *The number of words in an $M \times N$ crossword puzzle is given by*

$$M + N + n - 2b$$

where b black squares have been bound using n marks.

Proof. Let $G = (V, E)$ be a rectangular $M \times N$ grid graph with $V = V_W \cup V_B$ where the sets V_B and V_W represent our black and white squares, respectively. We let $|V_B| = b$ and note that $|V_W| = MN - b$.

Let G' be an induced subgraph on V_W with edge set E'. Clearly G' is the union of paths which represent our puzzle's k words. These paths have order p_i and size $p_i - 1$ for $1 \le i \le k$. While most crosswords don't contain words shorter than 3 letters, we put no restrictions on the order or size of these paths.

Now, because each letter in a puzzle appears in exactly two words, $\sum p_i = 2(MN - b)$ and, because each edge $e \in E'$ lies in a unique path,

$$|E'| = \sum_{i=1}^{k}(p_i - 1) = 2(MN - b) - k. \tag{1}$$

We also see that our n marks intersect all edges in E that are not in E'. Using the number of edges in an $M \times N$ grid graph, we obtain a second expression for $|E'|$.

$$|E'| = |E| - n = 2MN - M - N - n. \tag{2}$$

Our result can now be obtained by setting (1) and (2) equal and solving for k. ∎

Summary This short paper uses grid graphs and other concepts from elementary graph theory to enumerate the number of words contained in a crossword puzzle.

Math. Mag. **84** (2011) 141. doi:10.4169/math.mag.84.2.141. © Mathematical Association of America

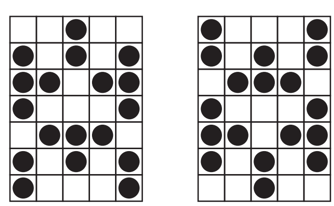
Parity Party with Picture Proofs: An Odd Checkerboard Problem

JASON I. BROWN
Dalhousie University
Halifax, Nova Scotia, Canada B3H 3J5
brown@mathstat.dal.ca

ERICK KNIGHT
Princeton University
Princeton, New Jersey 08544
rp2knight@gmail.com

DAVID WOLFE
Dalhousie University
Halifax, Nova Scotia, Canada B3H 3J5
davidgameswolfe@gmail.com

How many ways can checkers be placed on an $m \times n$ board so that each square (whether or not it is occupied) is orthogonally adjacent to an odd number of checkers? For example, on a 7×5 grid there are exactly two ways:



There is a natural even variant of the problem, where each square is adjacent to an even number of checkers. We will call a solution to the odd (respectively, even) variant of the problem an *odd* (respectively, *even*) *solution.* For an $m \times n$ board, define the quantities

$$\mathbf{O}(m, n) = \text{the number of odd solutions, and}$$

$$\mathbf{E}(m, n) = \text{the number of even solutions.}$$

In this paper, we determine $\mathbf{O}(m, n)$ and $\mathbf{E}(m, n)$ exactly, using a delightful hodgepodge of parity arguments.

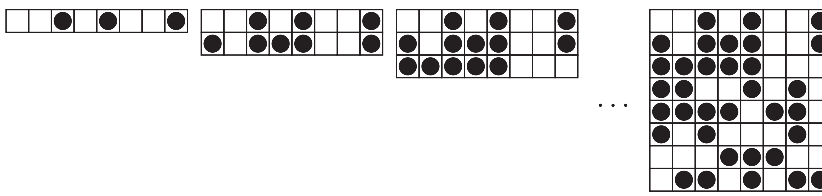
The authors came upon the 8×8 version of this problem on a Turkish puzzle website [**1**, problem 05 from 2006], and later in a book [**2**, problem 192]. In the latter, the solutions are counted up to 6×6 (but two solutions are deemed equal if they are symmetric). They also describe the otherwise unpublished work of Barry Cipra who attempts to identify conditions on m and n under which a solution exists. When proving a solution does not exist, Cipra uses techniques similar to ours here.

The upper bound

In both the even or the odd variant of the problem, once the placement of checkers in the first row is fixed, the remaining rows are completely determined because, when

Math. Mag. **84** (2011) 142–149. doi:10.4169/math.mag.84.2.142. © Mathematical Association of America

$k \geq 3$, rows $k-2$ and $k-1$ determine row k, for there is only one way to place checkers on row k so that the parity of the neighbors of checkers adjacent to each square of row $k-1$ is correct. (This is also true when $k=2$, if we interpret row $k-2=0$ as being off the board and having no checkers.) Once several rows are fixed, we call the process of naturally filling in rows or columns thereafter *completing* a (potential) solution. (We call it a *potential* solution because the completion, while uniquely defined, may fail to produce a legal configuration. It yields an actual solution only if the last row satisfies the requirements.) An example of *completing* an 8×8 odd solution appears below:



The reader is encouraged to confirm that the first row determines each of the following rows. For instance, in the single row on the left, the leftmost square is initially adjacent to no checkers, so there must be a checker in the leftmost square in the second row so that the top left square is adjacent to an odd number. In this example, the 8×8 completion is an actual solution.

Since there are exactly 2^n ways of placing checkers in the first row, we obtain the upper bounds on the number of solutions for the $m \times n$ board:

$$\textit{If } m \geq n, \textit{ then } \mathbf{O}(m,n) \leq 2^n \textit{ and } \mathbf{E}(m,n) \leq 2^n.$$

(When $m < n$, we can exchange the roles of m and n and obtain a bound of 2^m.)

Graph theory and vector space connections

In fact, provided there is at least one solution, the number of solutions on *any* $m \times n$ board must be a power of 2. Before returning to our parity proofs, we will first see this via vector spaces. We associate a graph $G_{m,n}$ whose vertices are the mn squares of the board, with two such vertices adjacent if and only if they are horizontally or vertically adjacent. Given an ordering of the vertices of the graph, we can form the 0–1 *adjacency* matrix $A_{m,n}$, which is an $mn \times mn$ square matrix whose (i, j)th entry is 0 if ith and jth vertices are adjacent in the graph, and 0 otherwise.

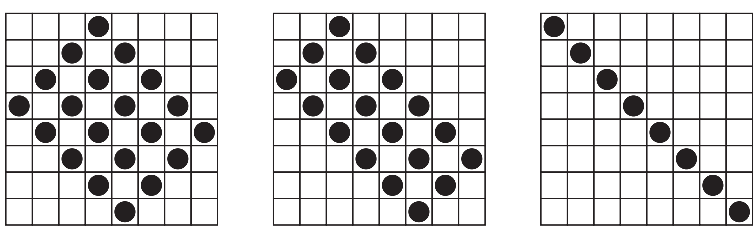
We note that if $\mathbf{x}$ is any vector of length mn with all entries being 0 or 1 (that is, a vector in the vector space $\mathbb{Z}_2^{mn}$ over $\mathbb{Z}_2$), then the kth component of $A\mathbf{x}$ is the sum of all components of $\mathbf{x}$ corresponding to neighbors of vertex k in the graph $G_{m,n}$. If we represent a configuration of checkers on an $m \times n$ board by the vector of length mn whose component corresponding to a square is 1 if there is a checker present and 0 otherwise, then we see that the vectors corresponding to the even solutions are precisely the kernel of the adjacency matrix over $\mathbb{Z}_2$ (the kernel of a matrix M is the set of all vectors $\mathbf{x}$ such that such that $M\mathbf{x} = \mathbf{0}$. Since the kernel is a subspace, it follows that the vectors corresponding to the even solutions form a subspace $E_{m,n}$ of $\mathbb{Z}_2^{mn}$ over $\mathbb{Z}_2$. Moreover, if the dimension of this subspace is d, then the size of the subspace (which is $\mathbf{E}(m,n)$, the number of even solutions) is 2^d, a power of 2.

Finally, what about the *odd* solutions? It is easy to check that the sum of two vectors corresponding to any odd solutions is a vector corresponding to an even solution, and the sum of a vector corresponding to an odd solution and a vector corresponding to an even solution is a vector corresponding to an odd solution. We conclude that the set of vectors corresponding to the odd solutions is either empty, or the affine subspace $S + E_{m,n}$, where S is the vector corresponding to *any* odd solution. An immediate consequence is that either $\mathbf{O}(m, n)$ is 0, or it is equal to $\mathbf{E}(m, n)$ (and hence also a power of 2).

Throughout the remainder of the paper, we will identify the checker configurations on a board with their corresponding 0–1 vectors, and hence talk about adding solutions, the *space* of even solutions, a basis, and so on. But back now to the boards and solutions....

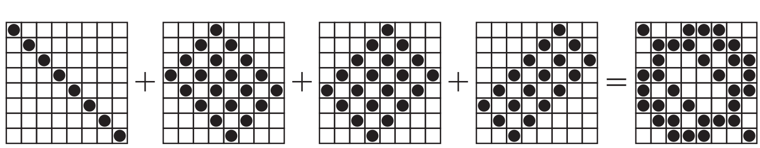
Even solutions

Consider the even variant on square boards. Each of the n starting rows that have exactly one checker in the top row leads to a solution on an $n \times n$ board, as evidenced by the examples below:



In particular, if the kth square of the top row has a checker, draw a rectangle with corners $(k, 1)$, $(1, k)$, $(n, n - k + 1)$, $(n - k + 1, k)$, and place checkers along the rectangle's boundary and on every other square inside it. Each square is easily seen to be adjacent to an even number of checkers. These solutions form a basis for all 2^n even solutions on the $n \times n$ board. For example, to find a solution having the fixed top row,

we add four basis solutions, one for each checker in the top row:

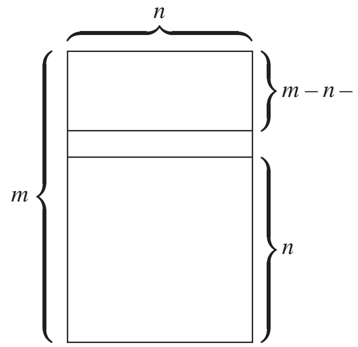


Since any top row yields a solution, we have proved that every choice for the first row of an $n \times n$ square completes uniquely to an even solution for the $n \times n$ board, so

$$\mathbf{E}(n, n) = 2^n.$$

Furthermore, as noted earlier, $\mathbf{O}(n, n)$ is either 0 or 2^n.

We next consider non-square $m \times n$ boards, taking $m > n$ for convenience. Such a board can be broken up into three components adjoined one atop the next: (1) an $n \times n$ square, (2) a $1 \times n$ strip, and (3) an $(m-n-1) \times n$ rectangle. (The last rectangle could be trivial with height 0.)



We now show that if $m > n$, then

$$\mathbf{E}(m, n) = \mathbf{E}(m-n-1, n).$$

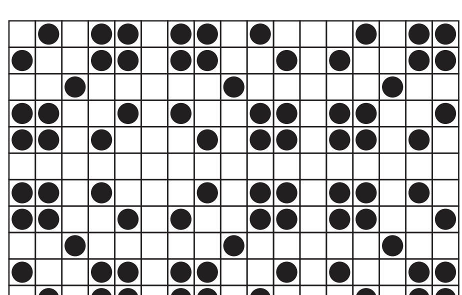
by drawing a one-to-one correspondence of solutions to the $m \times n$ board with solutions to the $(m-n-1) \times n$ board.

We begin by fixing a solution to an $(m-n-1) \times n$ board; we will argue this solution can be *completed* to the $m \times n$ board. Since we started with a solution to the $(m-n-1) \times n$ board, the next row (that is, row $m - n$) must be blank. Setting the following row equal to the row just above the blank row, we can complete the remaining square portion uniquely to a solution to the $m \times n$ board, and we are done.

We can repeatedly apply the previous reduction to any rectangular board—exchanging m and n when necessary—until it becomes square, say of side length d. Recall that a basic step in Euclid's gcd algorithm computes $\gcd(m, n) = \gcd(m-n, n)$. Here we are reducing $\mathbf{E}(m, n) = \mathbf{E}(m-n-1, n)$. Since we are subtracting $n + 1$ rather than n at each step (where n is the smaller of the two numbers), this minor augmentation of Euclid's algorithm ends with $\mathbf{E}(d, d)$ where $d = \gcd(m + 1, n + 1) - 1$. Hence, the reduction, when combined with our previous determination of $\mathbf{E}(m, n)$, implies:

$$\mathbf{E}(m, n) = 2^{\gcd(m+1,n+1)-1}.$$

In particular, the structure of any solution consists of reflected copies of a solution to a $d \times d$ block, separated by blank rows and columns of width 1. Here is an example with $d = 5$:



Back to the odd problem

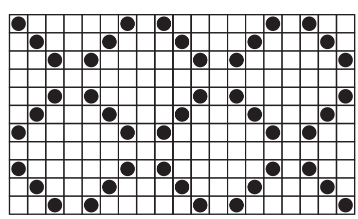
Fix m and n and suppose there exists an odd solution, say S, to the $m \times n$ board. As we have seen, adding S to any odd solution yields an even solution, and adding

S to any even solution yields an odd solution. Hence, when there exists an odd solution, $\mathbf{E}(m, n) = \mathbf{O}(m, n)$. That is, $\mathbf{O}(m, n)$ is either 0 or $2^{\gcd(m+1,n+1)-1}$, and we have reduced the counting problem of odd solutions to an existence problem.

Also note that any solution to the odd problem must have an even number of checkers. To see why, fix such a solution S, and consider the subgraph of $G_{m,n}$ induced by the vertices corresponding to squares with checkers in S. Since S was an odd solution, each vertex of the subgraph has odd degree. But a graph must have an even number of odd-degree vertices, and so S has an even number of checkers.

It follows that if the $m \times n$ problem has an even solution E with an odd number of checkers, then there are no odd solutions, as if there were an odd solution S, then either S or $S + E$ would have an odd number of checkers, contradicting our observation about any solution to the odd problem having an even number of checkers.

Fix m and n and define $d = 2^k - 1$, where 2^k is the largest power of 2 dividing both $m + 1$ and $n + 1$. If d, $(m + 1)/(d + 1)$, and $(n + 1)/(d + 1)$ are all odd, then there is an even solution to the $m \times n$ problem with an odd number of checkers obtained by constructing an $(m + 1)/(d + 1) \times (n + 1)/(d + 1)$ quilt made up of $d \times d$ blocks, separated by strips one square wide. Each block has checkers down one of its diagonals; adjacent blocks are reflections of each other. Here is an example with $m = 11$, $n = 19$, and so $d = 3$, $(m + 1)/(d + 1) = 3$, and $(n + 1)/(d + 1) = 5$:



The condition that d, $(m + 1)/(d + 1)$, and $(n + 1)/(d + 1)$ all be odd is equivalent to m and n being odd and ending in an equal number of ones when written in binary. So we define,

$$\Theta(n) = \text{the number of trailing 1s when } n \text{ is written in binary}$$

Equivalently, if 2^k is the largest power of 2 dividing $n + 1$, then $\Theta(n) = k$. This leads us to suspect that

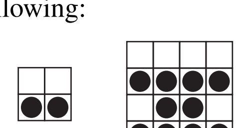
$$\mathbf{O}(m, n) = \begin{cases} 0 & \text{if } m \text{ and } n \text{ are odd with } \Theta(m) = \Theta(n) \text{, and} \\ 2^{\gcd(m+1,n+1)-1} & \text{otherwise.} \end{cases}$$

We have already proved the case corresponding to $\mathbf{O}(m, n) = 0$. To prove the remaining case it suffices to construct a solution, which we do in the next section.

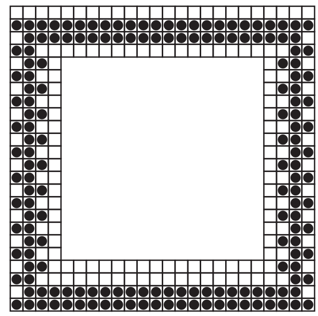
Constructing a solution to the odd problem

It remains to construct a solution to the odd problem in the case when m or n is even, or both are odd but with $\Theta(m) \neq \Theta(n)$. Alas, the parity party is over, and the next constructions are by induction.

Case: $m = n$ even. We first focus on $m = n$ even. For the 2×2 and 4×4 cases, the solutions we take are the following:



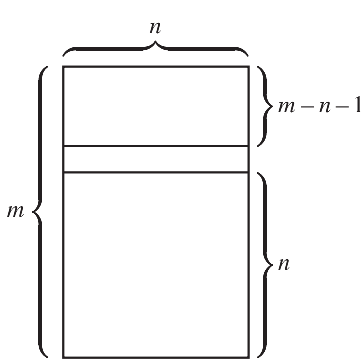
For $n = m \geq 6$, we start with the following 4-ring (meaning 4 rows on each side) frame:



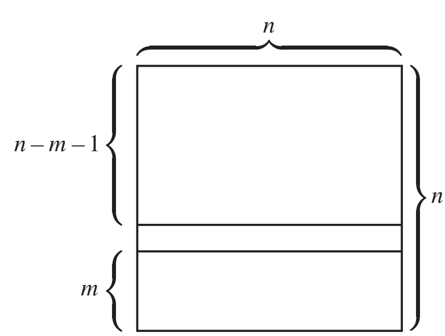
It is easy to check that this can be the outer frame of a solution if and only if there is a $(n-4) \times (n-4)$ solution with an outer 1-ring of the same form as the outer 1-ring of this 4-ring (the top row blank, the second row full, the bottom row full, the second from the bottom full except the two ends, and the left and right sides alternating nonchecker/checker). We can continue filling the interior with this type of 4-ring until we arrive at an inner 2×2 or 4×4 square. We finally complete the solution with one of the base solutions, which both have the appropriate outer 1-ring.

Note that cutting off the top, blank row of the above $n \times n$ solution yields an odd solution to the $(n-1) \times n$ problem for even n.

Case: $m \neq n$ with m or n even. We next consider non-square boards which have at least one even dimension. In this case, swap m and n if needed so that n is even, and either m is odd or $m \geq n$. We already constructed solutions when $m = n$ or $m = n - 1$ and are left with two cases summarized by the diagram below:



$m > n$, n even



$m < n - 1$ with m odd, n even

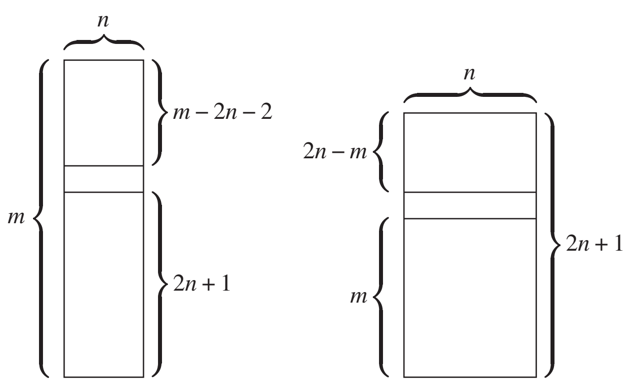
In the first case inductively compose an odd solution to the $(m-n-1) \times n$ board and complete it to the $m \times n$ board. If $m < n - 1$ is odd, inductively compose an $(n-m-1) \times n$ solution. (The induction is on the smaller even dimension, n.) Now, complete that solution to an $n \times n$ board working as diagrammed. Observe that:

- from the $n \times n$ case, the solution must complete to an $n \times n$ solution; and
- since we started with a solution to the $(m-n-1) \times n$ board, the $(n+1)$th row must be blank; and so,
- the bottom m rows constitute a solution to the $m \times n$ board.

A similar inductive frame argument for square boards can be used to construct an odd solution for a $2n \times n$ board for n odd, with the top and bottom rows having a complete row of checkers (see http://www.mathstat.dal.ca/~brown/research/checkerboard/appendix.pdf for details).

Case: m and n both odd (with $\Theta(m) \neq \Theta(n)$). We can now complete the construction for our last case, where both m and n are odd and $\Theta(m) \neq \Theta(n)$. As in our construction of the $2n \times n$ solution, the top and bottom rows have a complete row of checkers, tacking one blank row onto the bottom yields a $(2n+1) \times n$ solution. Once there is one such solution, there must be 2^n odd solutions (since there are that many even solutions.) That is, *every* possible top row can be completed to a solution to the $(2n+1) \times n$ board.

Using the above observations, we are now ready to complete the construction of an odd solution when m and n are both odd and $\Theta(m) \neq \Theta(n)$. Without loss of generality, let $m > n$. The case $m = 2n + 1$ was handled above, and we have two cases as diagrammed below:



$m > 2n+1$ $\qquad\qquad$ $n < m < 2n+1$

Since we can inductively assume cases only where $\Theta(m') \neq \Theta(n')$, the following result is required to complete the induction argument: If m and n are odd with $\Theta(m) \neq \Theta(n)$, then

$$\Theta(n) \neq \Theta(m - 2n - 2) \quad \text{and} \quad \Theta(n) \neq \Theta(2n - m).$$

To convince ourselves of this, it's easier to show that if $\Theta(n) = \Theta(m - 2n - 2)$ (or if $\Theta(n) = \Theta(2n - m)$), then $\Theta(m) = \Theta(n)$. Fix n odd and write it in binary. Suppose that n ends in k 1s. Now, $2(n + 1)$ ends in exactly $k + 1$ 0s, and $2n$ ends in k 1s followed by a 0. Here is an example with $k = 3$:

n ends 0111
$2n$ ends 01110
$2n + 2$ ends 10000

m	$\cdots ????$
$-2n - 2$	$- \cdots 10000$
	$\cdots 0111$

$2n$	$\cdots 01110$
$-m$	$- \cdots ????$
	$\cdots 0111$

It is not hard to see that the ???? must be 0111 in either case and m ends in k 1s.

Returning to the inductive construction, if $m > 2n + 1$, then a solution to the $(m - 2n - 2) \times n$ board can be completed to a solution to the $m \times n$ board. If, on the other hand, $n < m < 2n + 1$, then inductively begin with a solution to the $(2n - m) \times (2n+1)$ board. When completing this solution to a $(2n+1) \times n$ board, the first additional row will be blank. Consequently, the remainder of the board constitutes a solution to the $m \times n$ board.

Where to go from here?

We have determined the exact number of solutions to both variants of the $m \times n$ problem. In particular, the even problem has exactly $2^{\gcd(m+1,n+1)-1}$ solutions, while the odd problem has

$$\begin{cases} 0 \text{ solutions} & \text{if } m \text{ and } n \text{ are odd with } \Theta(m) = \Theta(n), \text{ and} \\ 2^{\gcd(m+1,n+1)-1} & \text{otherwise} \end{cases}$$

The vector space connection via graph theory raises some interesting questions. Suppose we stack 0, 1 or 2 checkers on each square of an $m \times n$ board, and insist that the sum of the number of checkers be a multiple of 3; how many legal configurations are there? We are now looking for the size of a subspace of $\mathbb{Z}_3^{mn}$, and hence the answer is a power of 3. What will a basis for the solutions look like?

The original question points directly at the general problem of finding the dimension for the kernel (over the binary field) of adjacency matrices of graphs. We can claim here the solution for the family of the cartesian products of pairs of paths.

Acknowledgment The first author would like to acknowledge the support of the National Science and Engineering Research Council.

REFERENCES

1. E. Halici, http://www.puzzleup.com, February 2006.
2. P. Vaderlind, R. K. Guy, and L. C. Larson, *The Inquisitive Problem Solver*, Mathematical Association of America, Washington, DC, 2002.

Summary How many ways can checkers be placed on an $m \times n$ board so that each square (whether or not it is occupied) is orthogonally adjacent to an odd number of checkers? After connecting the problem to graph theory and linear algebra, we provide an answer to this problem. The solution depends not only on the parity of m and n, but also, surprisingly, on the number of trailing 1's in their binary expansions.

PROBLEMS

BERNARDO M. ÁBREGO, *Editor*
California State University, Northridge

Assistant Editors: SILVIA FERNÁNDEZ-MERCHANT, California State University, Northridge; JOSÉ A. GÓMEZ, Facultad de Ciencias, UNAM, México; ROGELIO VALDEZ, Facultad de Ciencias, UAEM, México; WILLIAM WATKINS, California State University, Northridge

PROPOSALS

To be considered for publication, solutions should be received by September 1, 2011.

1866. *Proposed by Sadi Abu-Saymeh and Mowaffaq Hajja, Mathematics Department, Yarmouk University, Irbid, Jordan.*

Let ABC be a triangle, and L and M points on $\overline{AB}$ and $\overline{AC}$, respectively, such that $AL = AM$. Let P be the intersection of $\overline{BM}$ and $\overline{CL}$. Prove that $PB = PC$ if and only if $AB = AC$.

1867. *Proposed by Ángel Plaza and César Rodríguez, Department of Mathematics, Universidad de Las Palmas de Gran Canaria, Las Palmas, Spain.*

Let $f : [0, 1] \to \mathbb{R}$ be a continuous function such that $\int_0^1 f(t)\,dt = 1$ and n a positive integer. Show that

1. there are distinct $c_1, c_2, \ldots, c_n$ in $(0, 1)$ such that

$$f(c_1) + f(c_2) + \cdots + f(c_n) = n,$$

2. there are distinct $c_1, c_2, \ldots, c_n$ in $(0, 1)$ such that

$$\frac{1}{f(c_1)} + \frac{1}{f(c_2)} + \cdots + \frac{1}{f(c_n)} = n.$$

1868. *Proposed by Donald E. Knuth, Stanford University, Stanford, CA.*

Let $n \geq 2$ be an integer. Remove the central $(n-2)^2$ squares from an $(n+2) \times (n+2)$ array of squares. In how many ways can the remaining squares be covered with $4n$ dominoes?

Math. Mag. **84** (2011) 150–157. doi:10.4169/math.mag.84.2.150. © Mathematical Association of America

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. Submitted problems should not be under consideration for publication elsewhere.

Solutions should be written in a style appropriate for this MAGAZINE.

Solutions and new proposals should be mailed to Bernardo M. Ábrego, Problems Editor, Department of Mathematics, California State University, Northridge, 18111 Nordhoff St, Northridge, CA 91330-8313, or mailed electronically (ideally as a LaTeX or pdf file) to mathmagproblems@csun.edu. All communications, written or electronic, should include **on each page** the reader's name, full address, and an e-mail address and/or FAX number.

1869. *Proposed by Marian Duncă, Bucharest, Romania.*

Let $f:\mathbb{R}\to\mathbb{R}$ be an increasing and concave-down function such that $f(0)=0$. Prove that if x, y, and z are real numbers, and a, b, and c are the lengths of the sides of a triangle, then

$$(x-y)(x-z)f(a)+(y-x)(y-z)f(b)+(z-x)(z-y)f(c)\geq 0.$$

1870. *Proposed by Ovidiu Furdui, Campia Turzii, Cluj, Romania.*

Calculate

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

where ζ denotes the Riemann Zeta function.

Quickies

Answers to the Quickies are on page 156.

Q1009. *Proposed by Paolo Perfetti, Dipartimento di Matematica, Università degli studi di Tor Vergata Roma, Roma, Italy.*

Let $H_n=\sum_{k=1}^{n}1/n$. Using the fact that $\sum_{k=1}^{\infty}1/k^2=\pi^2/6$, calculate $\sum_{k=1}^{\infty}H_k/k^3$.

Q1010. *Proposed by Michael W. Botsko, Saint Vincent College, Latrobe, PA.*

Let $f:[0,1]\to\mathbb{R}$ be a continuous real valued function with a continuous nonzero derivative on $(0,1]$. Prove that if $f(0)=0$, then $\liminf_{x\to 0^+} f(x)/f'(x)=0$.

Solutions

Every integer in the list divides the sum **April 2010**

1841. *Proposed by H. A. ShahAli, Tehran, Iran.*

Let $n\geq 3$ be a natural number. Prove that there exist n pairwise distinct natural numbers such that each of them divides the sum of the remaining $n-1$ numbers.

I. *Solution by Northwestern University Math Problem Solving Group, Evanston, IL.*

The list of numbers $1, 2, 3\cdot 2^0, 3\cdot 2^1, 3\cdot 2^2, \ldots, 3\cdot 2^{n-3}$ has the required property. The sum of all those numbers is

$$1+2+3\cdot 2^0+3\cdot 2^1+3\cdot 2^2+\cdots+3\cdot 2^{n-3}=3+3\cdot(2^{n-2}-1)=3\cdot 2^{n-2}.$$

Each number in the list divides the total sum, and that implies the desired condition.

II. *Solution by Michael Goldenberg, The Ingenuity Project, Baltimore Polytechnic Institute, Baltimore, MD; and Mark Kaplan, The Community College of Baltimore County, Baltimore, MD.*

We choose natural numbers m_k given by

$$m_k=\begin{cases} n!\left(\frac{1}{k!}-\frac{1}{(k+1)!}\right)=n!\cdot\frac{k}{(k+1)!} & \text{if } 1\leq k\leq n-1,\\ n!\cdot\frac{1}{n!}=1 & \text{if } k=n.\end{cases}$$

If $n \geq 3$, then $m_1 > m_2 > \cdots > m_{n-1} > m_n$. In addition

$$S = \sum_{k=1}^{n} m_k = n!\left(\left(1 - \frac{1}{2!}\right) + \left(\frac{1}{2!} - \frac{1}{3!}\right) + \cdots + \left(\frac{1}{(n-1)!} - \frac{1}{n!}\right) + \frac{1}{n!}\right) = n!,$$

and $S - m_k$ is a multiple of m_k for $1 \leq k \leq n$.

Editor's Note. Harris Kwong and Nicholas Singer (independently) proved that the only solution for $n = 3$ is $(a, 2a, 3a)$. Erwin Just observes that this problem is a direct Corollary of a problem proposed by him. [Problem 1504, this MAGAZINE **70** (1997), 300.] Reiner Martin and Dmitry Fleischman (independently) provide an insight into a way of classifying all possible solutions which can be completed as follows: If $m_1 < m_2 < \cdots < m_n$ satisfy that the sum $S = m_1 + m_2 + \cdots + m_n$ is divisible by all m_k, say $S = m_k \cdot d_k$, then $d_1 > d_2 > \cdots > d_n$ and

$$\sum_{i=1}^{n} \frac{m_k}{S} = \sum_{i=1}^{n} \frac{1}{d_k} = 1.$$

Reciprocally, if the positive integers $d_1 > d_2 > \cdots > d_n$ satisfy that $\sum_{i=1}^{n}(1/d_k) = 1$, then by letting S be the least common multiple of the d_k and $S = m_k \cdot d_k$, it follows that m_k divides S and

$$\sum_{i=1}^{n} \frac{S}{d_k} = \sum_{i=1}^{n} m_k = S.$$

Thus the classification problem is equivalent to finding all possible partitions of 1 into n different fractions with numerator 1 (called Egyptian Fractions). The first solution is obtained from the partition $1 = 1/2 + 1/3 + 1/6$ by recursively dividing by 2 and adding $1/2$ on both sides. In fact the greedy algorithm can complete any partial sum $1/m_1 + 1/m_2 + \cdots + 1/m_k < 1$ to a partition $1 = 1/m_1 + 1/m_2 + \cdots + 1/m_l$ for some $l > m$. However the complete classification is still an open problem. Some references and related open problems can be found in R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1981, pp. 87–93; and in V. Klee and S. Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Mathematical Association of America, 1991, pp. 175–177 and 206–208.

Also solved by Con Amore Problem Group (Denmark); Michel Bataille (France); Brian D. Beasley; D. Bednarchak; Gareth Bendall; Jany C. Binz (Switzerland); Lataianu Bogdan (Canada); Paul Budney; Robert Calcaterra; Michael J. Caulfield; Hyeong Min Choe (Korea) and Jong Jin Park (Korea); John Christopher; CMC 328; Tim Cross (United Kingdom); Chip Curtis; Robert L. Doucette; Toni Ernvall (Finland); Dmitry Fleischman; Fullerton College Math Association; Stefania Garasto (Italy); David Getling (Germany); Eugene A. Herman; Chris Hill; Dan Jurca; Peter Hohler (Switzerland); Bianca–Teodora Iordache (Romania); Omran Kouba (Syria); Victor Y. Kutsenok; Harris Kwong; Elias Lampakis (Greece); Kathleen E. Lewis (Republic of the Gambia); Daniel Lucas, Rachel White, and Meghan Loid; Reiner Martin (Germany); Shoeleh Mutameni; Pedro Perez; Ángel Plaza (Spain); Henry Ricardo; R. Keith Roop-Eckart; Daniel M. Rosenblum; Joel Schlosberg; Harry Sedinger; Seton Hall Problem Solving Group; Achilleas Sinefakopoulos (Greece); Nicholas C. Singer; David Stone and John Hawkins; Taylor University Problem Solving Group; Marian Tetiva (Romania); Texas State Problem Solvers Group; Bob Tomper; Michael Vowe (Switzerland); Stanley Xiao (Canada); and the proposer.

Perpendicular hexagon skewers **April 2010**

1842. *Proposed by Bianca-Teodora Iordache, student, National College "Carol I," Craiova, Romania.*

In the interior of a square of side-length 3 there are several regular hexagons whose sum of perimeters is equal to 42 (the hexagons may overlap). Prove that there are two perpendicular lines such that each one of them intersects at least five of the hexagons.

Solution by CMC 328, Carleton College, Northfield, MN.

We first claim that when we project a regular hexagon of side length a onto a line its shortest possible projection is $a\sqrt{3}$. To see this, observe that we can inscribe a circle of radius $a\sqrt{3}/2$ within the hexagon, and the projection of the hexagon is greater than or equal to the inscribed circle's projection.

Now let us project all the hexagons onto an edge of the square. Since the sum of all the hexagons' perimeters is 42, the sum of all of their side-lengths is 7. Hence, their projection length on one edge of the square is at least $7\sqrt{3} \approx 12.124$. Since all of these projections are onto a segment of length 3, and $3(4) < 7\sqrt{3}$, there must be some region in the segment covered by at least five of the projections. Pick a point in this region and draw a line through this point perpendicular to the edge; this line must intersect at least five hexagons. By carrying out this construction for two perpendicular edges of the square, we get the desired two perpendicular lines.

Also solved by Robert Calcaterra, David Getling (Germany), Victor Y. Kutsenok, Charles Martin, and the proposer.

Permutations with specified left-to-right maxima April 2010

1843. *Proposed by José Heber Nieto, Universidad del Zulia, Maracaibo, Venezuela.*

For every positive integer n, let S_n denote the set of permutations of the set $N_n = \{1, 2, \ldots, n\}$. For every $1 \le j \le n$, the permutation $\sigma \in S_n$ has a *left to right maximum* (LRM) at position j, if $\sigma(i) < \sigma(j)$ whenever $i < j$. Note that all $\sigma \in S_n$ have a LRM at position 1. Let M be a subset of N_n. Prove that the number of permutations in S_n with LRMs at exactly the positions in M is equal to

$$\prod_{k \in N_n \setminus M} (k-1),$$

where an empty product is equal to 1.

Solution by Robert Calcaterra, University of Wisconsin-Platteville, Platteville, WI.

If $1 \notin M$, the assertion is clearly true so we may assume that $1 \in M$. Let α be the permutation in S_n having its LRMs at exactly the positions in M. We determine the number of ways to choose α. Let $P(x, y)$ be the number of permutations of y elements selected from a set of x elements, which is known to be $x!/(x-y)!$; and let $m_1, m_2, \ldots, m_k = 1$ be the elements of M in descending order. Observe that n must occupy position m_1 in α. Then there are $P(n-1, n-m_1)$ ways to choose the elements of N_n that occupy positions $m_1 + 1$ to n in α. Of the elements of N_n that have not yet been assigned a position in α, the largest one must be assigned to position m_2. Consequently, we may now choose the elements of N_n that occupy positions $m_2 + 1$ to $m_1 - 1$ in $P(m_1 - 2, m_1 - m_2 - 1)$ different ways. Repeating this argument, there are

$$\prod_{j=1}^{k} P(m_{j-1} - 2, m_{j-1} - m_j - 1)$$

ways to choose α, where $m_0 = n + 1$. Since $(m_j - 2)!/(m_j - 1)! = 1/(m_j - 1)$ for $0 < j < k$, this product may be reduced to

$$(n-1)! \Big/ \prod_{j=1}^{k-1} (m_j - 1).$$

This expression is equivalent to the product stated in the problem.

Also solved by Con Amore Problem Group (Denmark), Chip Curtis, Robert L. Doucette, Joe McKenna (Ghana), Joel Schlosberg, John H. Smith, Marian Tetiva, Stanley Xiao (Canada), and the proposer. There was one incorrect submission.

A geometric inequality for the secants of a triangle **April 2010**

1844. *Proposed by Marian Tetiva, National College "Gheorghe Roşca Codreanu," Bîrlad, Romania.*

Let ABC be a triangle with $a = BC$, $b = AC$, and $c = AB$. Prove that

$$\frac{a^2+b^2+c^2}{2\cdot \text{Area}(ABC)} \geq \sec\frac{A}{2} + \sec\frac{B}{2} + \sec\frac{C}{2}.$$

Solution by Felipe Pérez (student), Facultad de Física, P. Universidad Católica de Chile, Santiago, Chile.

Let $s = (a+b+c)/2$ be the semiperimeter of the triangle ABC. Using the Half-angle Formula and the Law of Cosines gives

$$\cos^2\left(\frac{A}{2}\right) = \frac{1}{2}(\cos A + 1) = \frac{1}{2}\left(\frac{b^2+c^2-a^2+2bc}{2bc}\right) = \frac{s(s-a)}{bc}.$$

Thus

$$\sec\frac{A}{2} = \sqrt{\frac{bc}{s(s-a)}}, \quad \sec\frac{B}{2} = \sqrt{\frac{ac}{s(s-b)}}, \quad \text{and} \quad \sec\frac{C}{2} = \sqrt{\frac{ab}{s(s-c)}}.$$

Then by Heron's Formula for the area of $\triangle ABC$,

$$\begin{aligned}
&\sec\frac{A}{2} + \sec\frac{B}{2} + \sec\frac{C}{2} \\
&\quad = \sqrt{\frac{bc}{s(s-a)}} + \sqrt{\frac{ac}{s(s-b)}} + \sqrt{\frac{ab}{s(s-c)}} \\
&\quad = \frac{\sqrt{b(s-c)\cdot c(s-b)} + \sqrt{a(s-c)\cdot c(s-a)} + \sqrt{a(s-b)\cdot b(s-a)}}{\sqrt{s(s-a)(s-b)(s-c)}} \\
&\quad = \frac{\sqrt{b(s-c)\cdot c(s-b)} + \sqrt{a(s-c)\cdot c(s-a)} + \sqrt{a(s-b)\cdot b(s-a)}}{\text{Area}(ABC)}.
\end{aligned}$$

Using the Arithmetic Mean–Geometric Mean Inequality (the positiveness of each factor is justified by triangle inequality) gives

$$\sqrt{b(s-c)\cdot c(s-b)} \leq \frac{b(s-c)+c(s-b)}{2},$$

and equivalent inequalities for the other two summands. Finally,

$$\begin{aligned}
\sec\frac{A}{2} + \sec\frac{B}{2} + \sec\frac{C}{2} &\leq \frac{1}{2\cdot \text{Area}(ABC)}\big(s(2a+2b+2c) - (2ab+2ac+2bc)\big) \\
&\leq \frac{1}{2\cdot \text{Area}(ABC)}(a^2+b^2+c^2).
\end{aligned}$$

The equality holds if and only if $a = b = c$.

Also solved by George Apostolopoulos (Greece); Dionne Bailey, Elsie Campbell, and Charles Diminnie; Michel Bataille (France); Scott H. Brown; Minh Can; Tim Cross (United Kingdom); Chip Curtis; Marian Dincă; Robert L. Doucette; John N. Fitch; A. Bathi Kasturiarachi; Omran Kouba (Syria); Elias Lampakis (Greece); Kee-Wai Lau (China); Shoeleh Mutameni; Pedro Perez; Henry Ricardo; Achilleas Sinefakopoulos (Greece); Michael Vowe (Switzerland); Haohao Wang and Jerzy Woydylo; John Zerger; and the proposer.

Integrating a square-fractional-reciprocal function **April 2010**

1845. *Proposed by Albert F. S. Wong, Temasek Polytechnic, Singapore.*

Evaluate

$$\int_0^1 \left\{\frac{1}{x}\right\}^2 dx,$$

where $\{\alpha\} = \alpha - \lfloor\alpha\rfloor$ denotes the fractional part of α.

Solution by Allen Stenger, Alamogordo, NM.

Make the change of variable $x = 1/t$ to get

$$\int_0^1 \left\{\frac{1}{x}\right\}^2 dx = \int_1^\infty \frac{\{t\}^2}{t^2} = \sum_{k=1}^{\infty} \int_k^{k+1} \frac{(t-k)^2}{t^2} dt.$$

Then expand the integrands to get

$$\begin{aligned}\int_k^{k+1} \frac{(t-k)^2}{t^2} dt &= \int_k^{k+1} \left(1 - \frac{2k}{t} + \frac{k^2}{t^2}\right) dt \\ &= 1 - 2k\ln(k+1) + 2k\ln k + \frac{k^2}{k(k+1)} \\ &= 2 + 2\ln(k+1) - \big(2(k+1)\ln(k+1) - 2k\ln k\big) - \frac{1}{k+1}.\end{aligned}$$

Adding these terms from $k = 1$ to $n - 1$, noting the telescoping sum, and rearranging gives

$$\begin{aligned}\sum_{k=1}^{n-1} \int_k^{k+1} \frac{(t-k)^2}{t^2} dt &= 2n - 2 + 2\ln(n!) - 2n\ln n - \sum_{k=1}^{n-1} \frac{1}{k+1} \\ &= 2\left(\ln(n!) - \left(n + \frac{1}{2}\right)\ln n + n\right) - \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n\right) - 1 \\ &= 2\ln\left(\frac{n!}{n^{n+1/2}e^{-n}}\right) - \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n\right) - 1.\end{aligned}$$

Stirling's formula implies that the first term goes to $\ln(2\pi)$ as $n \to \infty$. From the definition of Euler's constant γ the second term goes to $-\gamma$, so the final result is

$$\int_0^1 \left\{\frac{1}{x}\right\}^2 dx = \ln(2\pi) - \gamma - 1 \approx 0.260661.$$

Editor's Note. Some readers pointed out that the problem of calculating the Riemann sums of this integral appeared as Problem 11206, *Amer. Math. Monthly* **114** (2007), 928–929. Ovidiu Furdui mentions that evaluating $\int_0^1 \{k/x\}^2\, dx$ for a positive integer k was published as Problem U27, *Mathematical Reflections* **6** (2006).

Paolo Perfetti, Dmitry Fleischman, and Joel Schlosberg (independently) obtained $1+2\sum_{r=2}^{\infty}(-1)^{r+1}\zeta(r)/(r+1)$ as the answer for this problem. Ovidiu Furdui considered the more general problem of finding $\int_0^1\{1/x\}^k\,dx$ for integer $k\geq 1$. He showed that the answer in this case is $\sum_{r=1}^{\infty}(\zeta(r+1)-1)/\binom{k+r}{r}$.

Also solved by Armstrong Problem Solvers, Michel Bataille (France), Dennis K. Beck, Lataianu Bogdan (Canada), Paul Budney, Robert Calcaterra, Hongwei Chen, John Christopher, Chip Curtis, Richard Daquila, Paul Deiermann, Robert L. Doucette, Dmitry Fleischman, Jet Foncannon, Ovidiu Furdui (Romania), Michael Goldenberg and Mark Kaplan, G.R.A.20 Problem Solving Group (Italy), J. A. Grzesik, Timothy Hall, Gerald A. Heuer, Dan Jurca, Kamil Karayilan (Turkey), Omran Kouba (Syria), Harris Kwong, Elias Lampakis (Greece), David P. Lang, Longxiang Li (China) and Luyuan Yu (China), Masao Mabuchi (Japan), Charles Martin, Reiner Martin (Germany), Kim McInturff, Matthew McMullen, Peter McPolin (Northern Ireland), Paolo Perfetti (Italy), Ángel Plaza (Spain), R. Keith Roop-Eckart, Ossama A. Saleh and Terry J. Walters, Joel Schlosberg, Edward Schmeichel, Seton Hall Problem Solving Group, Nicholas C. Singer, David Stone and John Hawkins, Marian Tetiva (Romania), Bob Tomper, Jan Verster (Canada), Francisco Vial (Chile), Michael Vowe (Switzerland), Stan Wagon, Haohao Wang and Jerzy Woydylo, Vernez Wilson and Farley Mawyer, John Zacharias, and the proposer. There were two incorrect submissions.

Answers

Solutions to the Quickies from page 151.

A1009. The answer is $\pi^4/72$. For n and k positive integers,

$$\frac{1}{n(k+n)}=\frac{1}{k}\left(\frac{1}{n}-\frac{1}{(k+n)}\right).$$

Thus

$$\frac{1}{n^2(k+n)^2}=\frac{1}{k^2n^2}+\frac{1}{k^2(k+n)^2}-\frac{2}{k^3}\left(\frac{1}{n}-\frac{1}{k+n}\right).$$

It follows by symmetry that

$$\begin{aligned}\frac{\pi^4}{36}&=\sum_{k=1}^{\infty}\frac{1}{k^2}\sum_{n=1}^{\infty}\frac{1}{n^2}=\sum_{k=1}^{\infty}\sum_{n=1}^{\infty}\frac{1}{k^2n^2}\\&=\sum_{k=1}^{\infty}\sum_{n=1}^{\infty}\left(\frac{1}{n^2(k+n)^2}-\frac{1}{k^2(k+n)^2}+\frac{2}{k^3}\left(\frac{1}{n}-\frac{1}{k+n}\right)\right)\\&=\sum_{k=1}^{\infty}\frac{2}{k^3}\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{k+n}\right)=\sum_{k=1}^{\infty}\frac{2}{k^3}\sum_{n=1}^{k}\frac{1}{n}=\sum_{k=1}^{\infty}\frac{2}{k^3}H_k.\end{aligned}$$

The result follows after dividing by 2 both sides of the equality.

A1010. Because f' satisfies the Intermediate Value Property, f' is either always positive or always negative on (0, 1]. Replacing if necessary f by $-f$, we can assume f' is positive on (0, 1]. Then f is also positive on (0, 1] and thus

$$\liminf_{x\to 0^+}\frac{f(x)}{f'(x)}\geq 0.$$

Suppose $\liminf_{x\to 0^+} f(x)/f'(x)>0$ and let A be a positive number such that $A<\liminf_{x\to 0^+} f(x)/f'(x)$. Then there exists δ, $0<\delta<1$, such that $f(x)/f'(x)>A$ for

$0 < x < \delta$. Therefore $f'(x)/f(x) < 1/A$ for $0 < x < \delta$ and thus

$$\ln\left(\frac{f(\delta)}{f(x)}\right) = \int_x^\delta \frac{f'(t)}{f(t)}dt \leq \int_x^\delta \frac{1}{A}dt = \frac{1}{A}(\delta - x).$$

It follows that $f(x) \geq f(\delta)e^{(x-\delta)/A}$ for $0 < x < \delta$. Taking limits we get

$$f(0) = \lim_{x\to 0^+} f(x) \geq f(\delta)e^{-\delta/A} > 0.$$

This is a contradiction, therefore $\liminf_{x\to 0^+} f(x)/f'(x) = 0$.

To appear in *College Mathematics Journal*, May 2011

Articles

How Your Philosophy of Mathematics Impacts Your Teaching!
by Bonnie Gold

Newton's Radii, Maupertuis' ArcLengths, and Voltaire's Giant,
by Andrew J. Simoson

Guards, Galleries, Fortresses, and the Octoplex, *by T. S. Michael*

Random Breakage of a Rod into Unit Lengths, *by Joe Gani and Randall Swift*

An Arithmetic Metric, *by Diego Dominici*

Counting Subgroups in a Direct Product of Finite Cyclic Groups,
by Joseph Petrillo

An Application of Group Theory to Change Ringing,
by Michele Intermont and Aileen Murphy

The Easiest Lights Out Game, *by Bruce Torrence*

Classroom Capsules

Using Continuity Induction, *by Dan Hathaway*

Book Reviews

Crossing the Equal Sign, by Marion Deutsche Cohen,
reviewed by Annalisa Crannell

REVIEWS

PAUL J. CAMPBELL, *Editor*
Beloit College

Assistant Editor: Eric S. Rosenthal, West Orange, NJ. Articles, books, and other materials 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.

Freedman, David A., *Statistical Models and Causal Inference: A Dialogue with the Social Sciences*, Cambridge University Press, 2010; xvi + 399 pp, $93.00, $30.99 (P). ISBN 978-0-521-19500-3, 978-0-521-12390-7.

Freedman, David A., *Statistical Models: Theory and Practice*, rev. ed., Cambridge University Press, 2009; xiv + 442 pp, $103.00, $40.99 (P). ISBN 978-0-521-11243-7, 978-0-521-74385-3.

Freedman, David, Robert Pisani, and Roger Purves, *Statistics*, 4th ed., W.W. Norton, 2007; xvi + 697 pp, $99.98 ISBN 978-0-393-92972-0.

I have long admired the *Statistics* textbook by David Freedman et al. for showing how to think qualitatively in statistics in the context of real situations and real data (with the sources meticulously documented), as opposed to the mass of books that focus on practicing calculations on made-up examples and fabricated data. But I haven't used the book for a course. The book was written, as one of its authors (not Freedman) related to me, to ease the pain of students who are required to take a statistics course (try to find an equation in the book)! I responded that, as an instructor at a liberal arts college, I must aspire beyond anesthetizing students and cultivating qualitative judgment to equipping them to handle the quantitative background that informs that judgment. David Freedman died in 2008 but left two other monuments about statistical models. *Theory and Practice* is a textbook for students who have already studied statistics and preferably are comfortable with matrix algebra and mathematical probability; it focuses on applications of linear models (including probit and logit models) and explains bootstrap estimation. Freedman asserts that it is "what you have to know in order to start reading empirical papers that use statistical models." There are exercises, some based on actual studies; the answers occupy 60 pp, and another 115 pp are devoted to reprints of four papers by others that are investigated in detail in the text. *Causal Inference* collects case studies by Freedman on a variety of topics (e.g., etiology of cholera, effects of hormone replacement therapy, earthquake risk, risk from swine flu vaccine, salt and blood pressure). His main conclusion is that "statistical models are fragile": Many new techniques should not be relied on, because they make unexamined assumptions; Freedman recommends instead "shoe leather" methods based on "subject-matter expertise" and wisdom about what confounders to include or rule out. Memorable quote: "to pull a rabbit from a hat, a rabbit must first be placed in the hat." I look forward to pondering and digesting these books.

Klymchuk, Sergiy, *Counterexamples in Calculus*, MAA, 2010; ix + 101 pp, $45.95 (P) ($35.95 to MAA members). ISBN 978-0-88385-756-6.

This booklet features 14 pp of incorrect calculus statements that students are urged to prove false by concocting counterexamples, with the remaining 80+ pages devoted to solutions. There is little overlap with Gelbaum and Olsted's *Counterexamples in Analysis* (1964). This is a great resource, but the price is too high.

Math. Mag. **84** (2011) 158–159. `doi:10.4169/math.mag.84.2.158`. © Mathematical Association of America

Lisi, A. Garrett, and James Owen Weatherall, A geometric theory of everything: Deep down, the particles and forces of the universe are a manifestation of exquisite geometry, *Scientific American* 303 (6) (December 2010) 54–61.

"E8 theory may be the long-sought Theory of Everything." E8 is the largest exceptional Lie group, with 248 generators ("sets of circles wrapping around one another") and whose admissible representations were finally computed only in 2007 (http://aimath.org/E8/). What is meant by this huge claim is that all the charges, patterns, and relationships among the "zoo" of currently known subatomic particles fit exactly the patterns of symmetries of the E8 group. Moreover, the structure and symmetries of E8 suggest further possible relationships, including accounting for dark matter and the fact that fermions come in three varieties. The article is a tour through the successive theories of various Lie groups that, one after another, have explained new elementary particles and relationships. E8 culminates the tour in predicting "a rich set of Higgs bosons," particles so far sought in vain by experimenters. Once fully operational, the new Large Hadron Collider will provide a test of E8 as a theory. Who ever suspected that reality could be so complex, or that an exceptional Lie group might lie at the heart of the universe?

Borwein, Jonathan, and Peter Borwein, *Experimental and Computational Mathematics: Selected Writings*, Perfectly Science Press, 2010; vii + 297 pp, $29.99 (P), $12.99 (Kindle), $8.99 (PDF). ISBN 978-1-9356-3805-6.

The Borweins are famous for applying computer technology to develop novel algorithms and discover mathematical results. Fourteen articles, each with a new introductory discussion, are reprinted here, including two each from *SIAM Review* and *Notices of the AMS*, four from the *American Mathematical Monthly*, and one from *Scientific American*. Particularly notable is "Closed forms: What they are and why they matter," which delineates seven(!) approaches to what a closed form solution means, gives a number of detailed examples, but reaches no definitive conclusions. Although many of the articles are understandable to undergraduates, this last one features examples that are not. (Reprints of a couple of older articles are fuzzy.)

Falbo, Clement E., *First Year Calculus as Taught by R.L. Moore: An Inquiry-Based Learning Approach*, Dorrance Publishing Corp., 2010; xiv + 423 pp, $40 (P). ISBN 978-1-4349-0761-5.

Long before the contemporary pedagogical emphasis on "student-centered" approaches and inquiry-based learning, R. L. Moore was conducting both Ph.D. dissertations and undergraduate calculus courses in that spirit. This book is largely a transcription of notes taken in Moore's course in 1955–56 by author Falbo, who has used the method and material in his calculus courses. One-third of the book is devoted to solutions to the exercises; so for the instructor to pursue the Moore method, it is the instructor who should have this textbook—but not the students. "A teacher using this text must be willing to become an 'interested bystander' while the student is the one who presents solutions at the board." Correspondingly, the students must be interested in taking an active part in their learning, able to tolerate uncertainty and ambiguity in their own thinking, willing to forego the convenient shortcut of copying answers from one another or sources on the Internet—and most of all, see calculus as an opportunity to learn mathematical argumentation, not just as "math skills" to enhance their future employment desirability.

Koshy, Thomas, *Triangular Arrays with Applications*, Oxford University Press, 2011; xvi + 421 pp, $125. ISBN 978-0-19-974294-3.

This book develops much machinery in number theory and binomial coefficients, including triangular and tetrahedral numbers, before exhibiting a panoply of triangular arrays, beginning with Pascal's triangle in Chapter 6. Other arrays include Fibonacci and Lucas numbers; Josef's, Leibniz's, Stirling's, Bell's, Euler's, Lah's, and tribinomial triangles; and much more. A reader needs to have a background in calculus and discrete mathematics; the fruits of working through the book include a broad encounter with related divisibility theory but mainly with combinatorics, including Catalan numbers, Stirling numbers, and Eulerian numbers. There are numerous proofs and examples but no exercises.

To appear in *College Mathematics Journal*, May 2011

Articles

How Your Philosophy of Mathematics Impacts Your Teaching!
by Bonnie Gold

Newton's Radii, Maupertuis' ArcLengths, and Voltaire's Giant,
by Andrew J. Simoson

Guards, Galleries, Fortresses, and the Octoplex, *by T. S. Michael*

Random Breakage of a Rod into Unit Lengths, *by Joe Gani and Randall Swift*

An Arithmetic Metric, *by Diego Dominici*

Counting Subgroups in a Direct Product of Finite Cyclic Groups,
by Joseph Petrillo

An Application of Group Theory to Change Ringing,
by Michele Intermont and Aileen Murphy

The Easiest Lights Out Game, *by Bruce Torrence*

Classroom Capsules

Using Continuity Induction, *by Dan Hathaway*

Book Reviews

Crossing the Equal Sign, by Marion Deutsche Cohen,
reviewed by Annalisa Crannell

New from the MAA

The Hungarian Problem Book IV

Edited and Translated by Robert Barrington Leigh and Andy Liu

The Eötvös Mathematics Competition is the oldest high school mathematics competition in the world, dating back to 1894. This book is a continuation of Hungarian Problem Book III and takes the contest through 1963. Forty-eight problems in all are presented in this volume. Problems are classified under combinatorics, graph theory, number theory, divisibility, sums and differences, algebra, geometry, tangent lines and circles, geometric inequalities, combinatorial geometry, trigonometry and solid geometry. Multiple solutions to the problems are presented along with background material. There is a substantial chapter entitled "Looking Back," which provides additional insights into the problems.

Hungarian Problem Book IV is intended for beginners, although the experienced student will find much here. Beginners are encouraged to work the problems in each section, and then to compare their results against the solutions presented in the book. They will find ample material in each section to help them improve their problem-solving techniques.

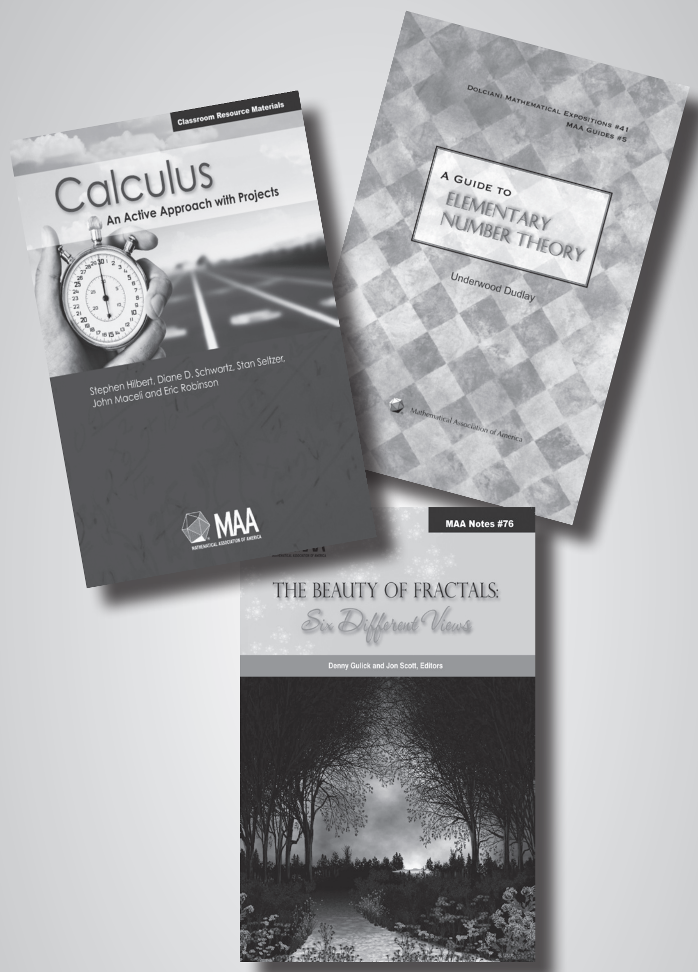
114 pp., Paperbound, 2011
ISBN 978-0-88385-831-8
Catalog Code: HP4
List: $40.95
Member: $33.95

To order visit us online at www.maa.org or call us at 1-800-331-1622.

MAA
MATHEMATICAL ASSOCIATION OF AMERICA

Your Favorite MAA Books.
Now Digital.

Visit www.maa.org/ebooks



Save 10% on your order!
coupon code: 353030655

MAA®
MATHEMATICAL ASSOCIATION OF AMERICA

MATHEMATICAL ASSOCIATION OF AMERICA 1529 Eighteenth St., NW • Washington, DC 20036

CONTENTS

ARTICLES

83 Ellipse to Hyperbola: "With This String I Thee Wed,"
by Tom M. Apostol and Mamikon A. Mnatsakanian

98 The Bhaskara-Aryabhata Approximation to the Sine Function,
by Shailesh A. Shirali

108 Integrals Don't Have Anything to Do with Discrete Math, Do They?
by P. Mark Kayll

119 Letter to the Editor
by Stan Wagon

NOTES

120 Positively Prodigious Powers or How Dudeney Done It?,
by Andrew Bremner

126 The Quadratic Character of 2,
by Rafael Jakimczuk

128 Two Generalizations of the 5/8 Bound on Commutativity in Nonabelian Finite Groups,
by Thomas Langley, David Levitt, and Joseph Rower

137 How Commutative Are Direct Products of Dihedral Groups?
by Cody Clifton, David Guichard, and Patrick Keef

141 Crossword Word Count,
by Matthew Duchnowski

142 Parity Party with Picture Proofs: An Odd Checkerboard Problem,
by Jason I. Brown, Erick Knight, and David Wolfe

PROBLEMS

150 Proposals, 1866–1870

151 Quickies, 1009–1010

151 Solutions, 1841–1845

156 Answers, 1009–1010

REVIEWS

158 A Lie group may explain the universe