LETTER FROM THE EDITOR

I learned in graduate school that it is not a whole lot of fun to read a research paper in mathematics. No matter how beautiful and insightful the results, it seemed like the details were always a pretty tough slog. What *was* fun, on the other hand, was going to a conference, meeting the paper's author, and then simply asking that person to describe what they did. It rarely took more than a few minutes, and the ensuing conversation was always rewarding.

This dichotomy reveals a central tension at the heart of mathematical culture. On the one hand, we view our discipline not simply as useful, but as beautiful as well. We all know that an elegant piece of mathematics has the power to make you smile, and to feel good for the rest of the day. On the other hand, the norms of our profession require us to present our findings in the most turgid and uninviting way imaginable. God help the poor writer who includes two consecutive sentences of exposition, or who dares to include some not-strictly-necessary commentary so that readers can more easily follow the argument. He will surely be accused of excessive wordiness, a grave charge.

Another thing I learned in graduate school was that there were venues like *Mathematics Magazine* out there. For me, this was an important discovery. Turns out it was actually possible to present serious, high-level mathematics in a way that was—are you sitting down?—enjoyable to read. Who knew? I have been a fan of the magazine ever since.

With this issue, I will be taking over as the new editor of *Mathematics Magazine*. It is a job I assume with great excitement, but also with no small amount of trepidation. The magazine has existed in some form since 1947 and has a long track record of publishing some of the best mathematical exposition to be found anywhere. I look forward to continuing that tradition.

If this transition goes smoothly, it will only be because of the incredible support I have received from numerous people toiling in the background. Let me especially thank Michael Jones, who has led the magazine for the last five years. His advice and patience have been invaluable to me as I learn how to do this job. Managing Editor Bonnie Ponce has by turns held my hand and administered needed pokes and prods to keep me on the one true path of editorial happiness. I also need to thank Bev Reudi, Susan Staples, and Carol Baxter at the MAA, and numerous people at Taylor and Francis who help keep this machine running.

My editorial philosophy is this: If it is in any way related to mathematics, no matter how tenuous the connection, then it is potentially of interest to the magazine. Mathematics is more than theorems, equations, and ever more complex variants on well-known problems. I believe that something called *Mathematics Magazine* should cover mathematics in all its forms, and not every article needs to be a notation-filled jargon-fest. If you have something to say about math and the humanities, the philosophy or history of mathematics, mathematics and society, or mathematics education, then I am interested in looking at a draft. I am especially open to the occasional opinion piece, or any piece that comes with a clear voice and point of view. When the opportunity arises, I want to publish articles that are going to inspire conversation.

And if you ever see me at a conference, feel free just to come up to me and pitch your idea. I am always happy to listen!

Math. Mag. **93** (2020) 2–3. doi:10.1080/0025570X.2020.1684141

Of course, in saying that *not every* article needs to include copious amounts of equations and notation, I certainly do not mean to imply I have anything against them, and the present issue has plenty to offer.

Our feature article this month is by Nancy Ho, James Godzik, Jennifer Jones, Thomas Mattman, and Dan Sours. They investigate paradromic rings, which can be viewed as a generalization of the standard Möbius strip. This leads them to some fascinating questions in knot theory, and also to some correspondingly interesting results about colorability.

Christopher N. B. Hammond contributes an article about Raabe's test for the convergence of an infinite series. Though not as well known as the more conventional ratio, root, or comparison tests, Raabe's test has certain advantages over them. How many years have I been teaching calculus without knowing about this?

The opening act of Anthony Zaleski and Doron Zeilberger's article is an ingenious brainteaser you should absolutely read, even if you choose not to stay for the main event. I recommend that you stick around, however, for their discussion of Boolean analogs of covering systems. A "covering system" is a concept from number theory. Roughly, it refers to a finite set of residues that collectively account for all non-negative integers. For example, the residues $\{0, 1, 2, 3, 4\}$, all taken modulo 5, account for all non-negative integers, so this is a covering system. A more interesting example arises from noticing that every integer is either even, or else it is congruent to 1 or 3 modulo 4. Covering systems have long been a hot topic of research, and Zeilberger and Zaleski have many informative things to say about them.

Stephen Kaczkowski takes his inspiration from physics. Starting from a well-known brainteaser, he discusses inequalities relating to quantities like velocity, speed, or acceleration. Matthew McMullen prefers to take his inspiration from Las Vegas, and finds the Catalan numbers in some problems related to gambling.

The shorter pieces include a clever proof of the infinitude of primes based on p-adic numbers, a proof of the binomial theorem using differential equations, a historical survey of proofs of the irrationality of the square root of two, and a discussion of how to construct a circle tangent to three given circles. We round out the issue with Problems, Reviews, and a nice pair or proofs without words.

I am looking forward to an exciting five years as editor of this journal. Please send me your best writing with all possible speed!

Jason Rosenhouse, Editor

Invisible Knots and Rainbow Rings: Knots Not Determined by Their Determinants

NANCY HO
Tapestry Solutions
San Diego, CA 92111
nho@ou.edu

JAMES GODZIK
California State University, Fullerton
Fullerton, CA 92834
jgodzik@csu.fullerton.edu

JENNIFER JONES
Colorado State University
Fort Collins, CO 80523-1874
jennifer.jones@colostate.edu

THOMAS W. MATTMAN
Department of Mathematics and Statistics
California State University, Chico
Chico, CA 92929-05252
TMattman@CSUChico.edu

DAN SOURS
Chico High School
Chico, CA 95926
dsours@chicousd.org

Möbius strip experiments are surefire triggers of Aha! experiences. Maybe you don't remember the first time someone challenged you to color one side blue and the other red, or asked you to guess the result of cutting a Möbius strip in half, but you surely recall the outcome. As part of a research experience for undergraduates (REU), we discovered that generalizing these experiments results in many more confounding constructions. Rather than simply bisecting the Möbius strip, try cutting it into n sections. Or, instead of joining the ends of the strip with a single half twist, make two twists, or three, or, in general, m half twists. You have just created examples of *paradromic rings*, which we'll denote $P(m, n)$.

You'll find that $P(2, 2)$ (bisect a strip after making a full twist) gives two strips of paper linked as in a chain. When m is odd (an odd number of half twists), bisection results in a single strip, albeit knotted up. Figure 1 shows some bisections; as in Ball and Coxeter [2], we replace each strip with the curve running along its midline. (Equivalently, you can imagine shrinking the width of the strip to zero.)

Figure 1 Some paradromic rings with $n = 2$ (bisection). (i) $P(3, 2)$, the trefoil knot, (ii) $P(5, 2)$, the pentafoil knot, and (iii) $P(2, 2)$, the Hopf link.

Math. Mag. **93** (2020) 4–18. doi:10.1080/0025570X.2020.1685320
MSC: 57M25

Having generated a nice pile of shredded strips, you'll start to wonder, "How can we organize this tangled mess?" The very language we are using suggests knot theory as the appropriate setting. A *knot* is a simple closed curve in space, like $P(3, 2)$ or $P(5, 2)$ of Figure 1, whereas a *link*, like $P(2, 2)$, is a collection of such embedded circles, called the *components* of the link. A knot, then, is a link with a single component.

Coloring these curves is akin to edge-coloring a graph. Just as each graph has a chromatic number, the determinant of link L, $\det(L)$, characterizes its colorability. We'll explain how to calculate this non-negative integer later. For now, it's enough to know that L is *p-colorable* if the prime p divides $\det(L)$. In this paper, we organize the paradromic rings by colorability. For each m and n, we will determine the primes p for which $P(m, n)$ is p-colorable.

In the REU, we were surprised by how quickly this problem in knot theory turned into an exercise in linear algebra. Rather than calculating determinants, we'll investigate the eigenvalues of a large, nearly diagonal matrix. There will be some proof by pictures too, but the essence of our argument is algebraic.

The real Aha!, however, came when we understood that, much like the Möbius strip, the paradromic rings resist coloring. Most of the knots in this family have determinant equal to one. This means they are not colorable for any prime (**no solutions**). We call them *invisible knots*, following Butler et al. [**3**]. Links of more than one component have even determinant, and are, therefore, not invisible. Still, these paradromic rings that are not knots valiantly defy us as best they can given this constraint. Many have determinants that are a power of two. These we call *nearly invisible*, since they can be colored only by the prime $p = 2$ (**one solution**). So long as $n \neq 2, 4$, the remaining paradromic rings have $\det(P(m, n)) = 0$. We refer to such links as *rainbow rings*, since they can be colored by every prime (**infinite solution set**).

In the end, the determinant is not very discriminating in separating out the paradromic rings. With a few exceptions, it partitions this doubly infinite family into only three different classes. Moreover, these classes turn out to be pathological, admitting either zero, one, or an infinite number of prime colorings. On the other hand, perhaps this type of outcome is exactly what you would expect from what is, ultimately, a problem in linear algebra.

Coloring links

While the determinant is convenient for organizing our results and defining invisible knots and rainbow rings, we will not calculate $\det(P(m, n))$ explicitly. Rather, we define p-colorability using link diagrams. A *diagram* is a projection of the link into the plane with gaps left in the curve to show where it crosses over itself. For example, Figure 1 consists of diagrams of the links $P(3, 2)$, $P(5, 2)$, and $P(2, 2)$.

Given a prime p, a diagram of a link is *p-colorable* if we can label its arcs with *colors* chosen from $0, 1, \ldots, p - 1$ such that

1. more than one color is used, and
2. at each crossing the colors satisfy the equation

$$2x \equiv y + z \pmod{p}$$

(see Figure 2i). A link is p-colorable if it has a p-colorable diagram. For example, Figure 2ii shows that the trefoil knot is 3-colorable.

Condition 1 rules out the trivial solution where every arc has the same color. Whatever the link and whatever the prime p, if all arcs have color 1 (for example), condition 2 will hold at every crossing. Without condition 1, every link would be colorable for every p. You can think of the second condition as balancing the colors on the overarc

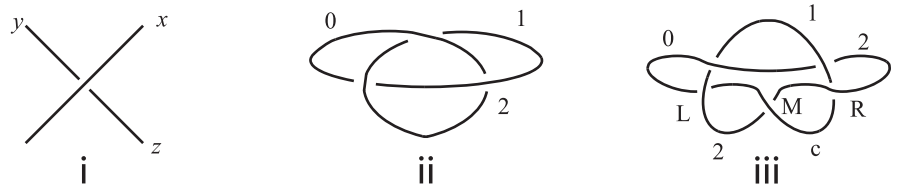


Figure 2 (i) Arcs are colored so that, at crossings, $2x \equiv y + z \pmod{p}$. The arc labeled x is called an overarc, and y and z are underarcs. (ii) The trefoil is 3-colorable. (iii) There is no way to choose a color c.

with those on the underarcs. There are four lines radiating from the center of the crossing, the two on top each carrying an x and the ones on the bottom carrying a y and a z. Condition 2 equates the two x's on top with the y and z below.

Condition 2 has a particularly nice interpretation in the case of tricolorability, when $p = 3$. A little thought will convince you that $2x \equiv y + z \pmod 3$ implies either $x = y = z$, or $\{x, y, z\} = \{0, 1, 2\}$. A link is *tricolorable*, then, if you can label its arcs with 0, 1, 2 such that at least two colors are used and, at each crossing, either exactly one color, or all three colors, appear.

We've mentioned that the trefoil knot $P(3, 2)$ is tricolorable (Figure 2ii); let's see why the pentafoil knot $P(5, 2)$ is not. In Figure 2iii, in trying to tricolor this knot, we have labeled four of its five arcs. All three colors appear at both of the top crossings, which is consistent with condition 2. It's impossible, however, to assign a color c to the remaining arc. That arc is part of three crossings, one at left (L), one at right (R), and one in the middle (M). At the left crossing, the other arcs already carry 0 and 2, so condition 2 forces $c = 1$. On the other hand, the crossing at the right obliges $c = 0$ since 1 and 2 already appear there. This shows that there is no consistent way to choose the color c. Note that the middle crossing implies $c = 2$ because there are already two color 2 arcs at that crossing.

To complete the argument that the pentafoil is not tricolorable, see if you can show that, no matter how the first four arcs are colored, it is impossible to choose a color c for the final arc. (Hint: By symmetry, you may assume the left arc is colored 0 as in Figure 2iii. There are three choices for the color of the top arc. With those two arcs labeled, condition 2 determines the color of two other arcs. In other words, up to symmetry, there are only three legitimate ways to color the first four arcs.)

When $p = 2$, condition 2 becomes $y \equiv z$. At each crossing, the two underarcs must have the same color. Each component of the link, then, will be all of one color. As condition 1 requires we use both colors, a link will be 2-colorable exactly if it has at least two components. As mentioned in the introduction, we say a link is nearly invisible if $p = 2$ is the only coloring.

We want to use p-colorability to organize the paradromic rings. It's an invariant of links, which means if a diagram admits a p-coloring for a given p, then any equivalent link will also have a p-colorable diagram. In knot theory, we consider two links equivalent if there's a way to move one around in space to look just like the other without ever having to pass the curve through itself. For a more precise description of link equivalence and the proof that p-coloring is an invariant, we recommend Adams's *The Knot Book* [**1**] or Livingston's *Knot Theory* [**4**].

Each column of Figure 3 consists of four diagrams of the same link. We've shown how the knot at left, $P(3, 2)$, is 3-colorable using the top diagram. This means the three diagrams below it are also 3-colorable, as you can easily confirm. On the other hand, we've argued that the knot represented in the middle column, $P(5, 2)$, is not 3-colorable. Since p-colorability is a link invariant, $P(3, 2)$ and $P(5, 2)$ are not

equivalent. There's no way to move any knot in the $P(5, 2)$ column around in space to make it look just like one in the $P(3, 2)$ column. See if you can show that the third link in the figure, $P(2, 2)$, is different from the first two. (Hint: try 5- and 2-colorings. How are the p-colorings of $P(m, 2)$ determined by m?)

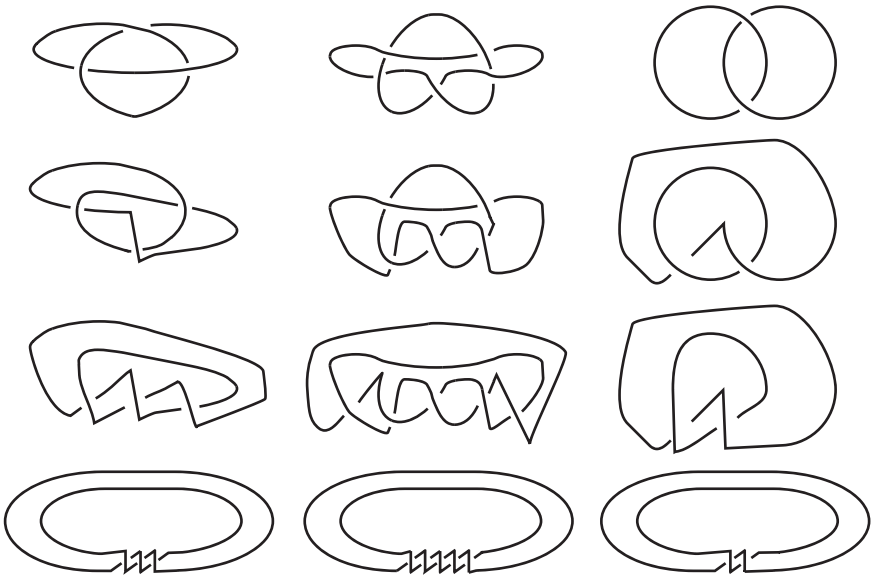


Figure 3 We can redraw $P(3, 2)$, $P(5, 2)$, and $P(2, 2)$ as at the bottom of the figure.

We will now use linear algebra to prove that $P(m, 2)$ is p-colorable if and only if p divides m. The key observation is suggested by Figure 3. To build link $P(m, 2)$, repeat the Figure 4i pattern m times and then join up the loose ends. Use $x = (x_1, x_2)$ to color the arcs entering Figure 4i at left. Then the arcs leaving at right are $y = (y_1, y_2)$ where $y_2 = x_1$ and condition 2 tells us that $y_1 \equiv 2x_1 - x_2 \pmod{p}$. In other words, $y \equiv Tx \pmod{p}$ where $T = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$.

For the Hopf link, $P(2, 2)$ (Figure 4ii), we repeat the pattern two times. Beginning with arcs labeled x at left, after going through the pattern once, we'll have colors y where $y \equiv Tx$. Passing through the pattern a second time, we have colors $z \equiv Ty \equiv T^2x$. Notice that by going around the top of the link, these z arcs at right are identified with the x arcs we started with on the left. In other words, $x = z \equiv T^2x$. Thus, x represents a coloring of the Hopf link if $x \equiv T^2x$.

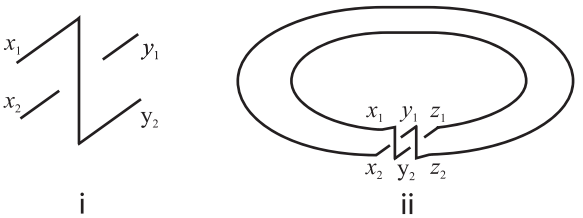


Figure 4 (i) Repeat this pattern m times to form a $P(m, 2)$ link. (ii) The Hopf link $P(2, 2)$.

In general, for $P(m, 2)$, we pass through the Figure 4i pattern m times. See Figure 3 for examples with $m = 3, 5, 2$. This means a valid coloring requires $x \equiv T^m x$. Equivalently, x must satisfy the eigenvector equation: $(T^m - I)x \equiv 0$.

For any color c, we call $x = (c, c)$ a *constant vector*. Then, $Tx = x$, so constant vectors solve the eigenvector equation. But this means we've colored every arc c, violating condition 1. Thus, p-colorings of $P(m, 2)$ correspond to non-constant $\lambda = 1$ eigenvectors of T^m mod p.

Using induction, we find

$$T^m - I = \begin{pmatrix} m & -m \\ m & -m \end{pmatrix}.$$

As we mentioned, vectors of the form (c, c) are in the null space of this matrix. The link $P(m, 2)$ will be p-colorable exactly when there is some other, non-constant vector in the mod p null space of $T^m - I$. That means the null space is two-dimensional so that the matrix is in fact the zero matrix mod p. Therefore, the link $P(m, 2)$ is p-colorable if and only if p divides m.

In the final section of the paper, we will use this algebraic approach to determine the p-colorability of the paradromic rings. But first, let's see how they relate to links that lie flat on a torus.

Paradromic rings and torus links

Paradromic rings enjoy a close connection with torus links that we will exploit to understand their p-colorability. Figure 5 shows how the trefoil knot, pentafoil knot, and Hopf link can be realized as curves that lie flat on a torus. The idea of a torus link, then, is similar to defining a planar graph as one we can put in the plane with no edges crossing. Links that lie in the plane are called trivial links; they're simply collections of disjoint circles with no crossings whatsoever. The torus links, in contrast, are an important family that have long intrigued knot theorists.

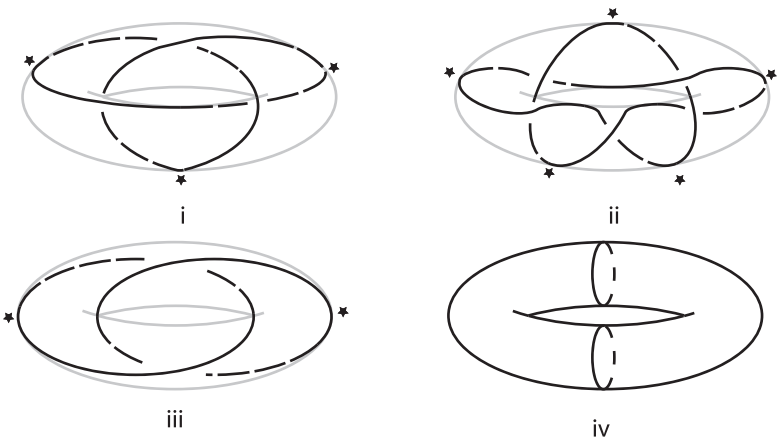


Figure 5 The (i) trefoil knot, (ii) pentafoil knot, and (iii) Hopf link are torus links as they can be made to lie on a torus (the surface of a doughnut, see (iv). Dashed lines represent parts of the curve on the far side of the torus.

We will show that each $P(m, n)$ is either a torus link or else a torus link together with an additional component that follows the *core* of the torus (see Figure 6i). The core is a curve inside the torus that intersects every cross-sectional disk at its center.

Figure 6 (i) The core of the torus meets every cross-sectional disk in its center. (ii) $P(3,3)$ consists of a trefoil knot that lies on the torus along with a second component along the core of the torus.

For example, Figure 6ii shows that $P(3,3)$ consists of two components: the trefoil, which is a torus knot (compare Figure 5i), and the core.

Let's review how we construct a $P(m,n)$ paradromic ring (see Figure 7). Draw lines on a strip of paper that divide it into n strips. Connect the two loose ends with m half twists and then cut along the lines. Finally, we replace each resulting loop of paper, whose width is $1/n$ that of the original strip, with the curve that runs along its midline, $1/2n$ from its edges. We assume m is a non-negative integer and n is positive.

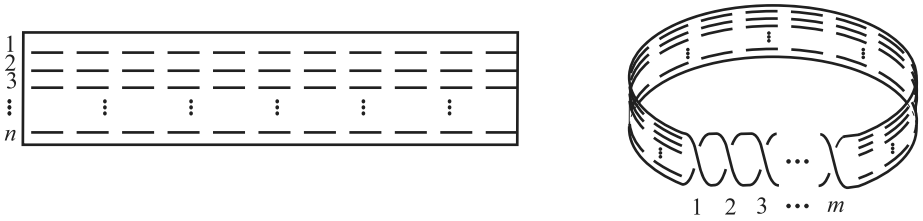


Figure 7 The $P(m,n)$ paradromic ring. Use $n-1$ dashed lines to divide the strip into n sections. Join the ends with m half twists and cut along the dashed lines.

To illustrate the connection with torus links, we place our strip of paper inside a torus (see Figure 8). We will group the m half twists together (compare with the $P(m,2)$ diagrams at the bottom of Figure 3) and then connect them up with a flat strip that joins the two ends of the twisted region. In other words, we collect the half twists inside a cylinder that we'll call C_t (t for twist). Outside the cylinder, the strip of paper will lie between concentric circles that we call the *equators*.

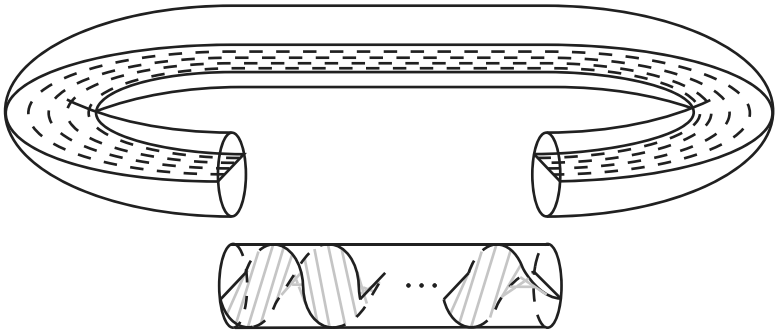


Figure 8 Isolate the twists in a cylinder, C_t. Outside the cylinder, the strip lies between the inner and outer equators on the torus.

For convenience in defining equators, the core, and other nomenclature, we situate the torus in $\mathbb{R}^3$ as in Figure 9. The z-axis is an axis of rotational symmetry and the xy-plane is fixed by a reflection. Let a and b be the radii shown in the figure. The core, then, is the circle in the xy-plane of radius a centered at the origin. The xy-plane intersects the torus in two concentric circles (of radius $a - b$ and $a + b$) that we call the *inner* and *outer equators.* A *longitude* is any closed curve on the torus that is parallel to the equators and loops once around the z-axis. For example, planes of the form $z = c$ where $|c| < b$ will intersect the torus in two longitudes. The plane $z = b$ intersects the torus in a single longitude, the *top longitude*, that runs along the top of the torus. The equators are also examples of longitudes. A *meridian* is any simple closed curve that intersects each longitude once and also bounds a disk inside the torus. Planes of the form $y = kx$, for example, intersect the torus in two meridia, each being a circle of radius b.

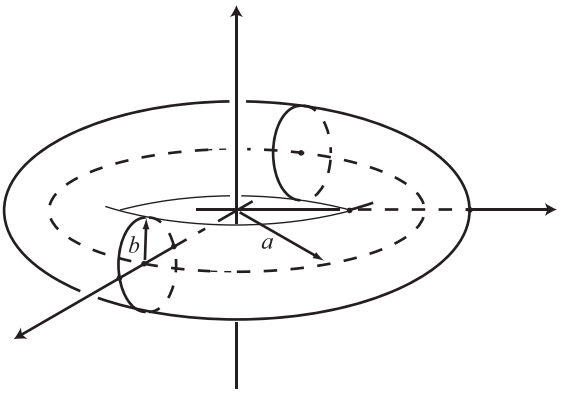


Figure 9 An embedding of the torus in $\mathbb{R}^3$. The z-axis is an axis of rotational symmetry. The xy-plane is fixed by a reflection.

The $T(u, v)$ *torus link* is a link of $\gcd(u, v)$ components that we can arrange on the torus so that it intersects each longitude u times and each meridian v times. As mentioned in the section on coloring links, when we speak of a link, an embedding of circles in three space, we are allowed to move the circles around in space freely so long as the curves do not pass through one another. Such a link is a torus link if, among these different embeddings, there is one that lies flat on a torus without the curve crossing through itself. For example, in Figure 5, the trefoil is $T(3, 2)$, the pentafoil is $T(5, 2)$, and the Hopf link is $T(2, 2)$. We have starred the intersections with the outer equator, which is a longitude.

We are now ready to prove Theorem 1: either a paradromic ring is a torus link, or it is a torus link together with an additional component along the core of the torus. We denote the second case by $T(u, v) \cup C$. Figure 6 shows, for example, that the $P(3, 3)$ paradromic ring is $T(3, 2) \cup C$.

Theorem 1. *Let $m \geq 0$ and $n > 0$ be integers. If $n = 1$, $P(m, 1) = T(0, 1)$; if $n > 1$, then*

$$P(m, n) = \begin{cases} T(\frac{1}{2}mn, n) & \text{if } mn \text{ is even,} \\ T(\frac{1}{2}m(n-1), n-1) \cup C & \text{if } mn \text{ is odd.} \end{cases}$$

Proof. (Sketch.) If $n = 1$, we do not cut the strip of paper at all; it consists of a single loop whose midline follows the core of the torus, see Figure 10. Moving the core straight up in the z-direction to follow the top longitude, we see that $P(m, 1) = T(0, 1)$. In other words, as a knot, the core is equivalent to any longitude since we can move it in space to follow that longitude.

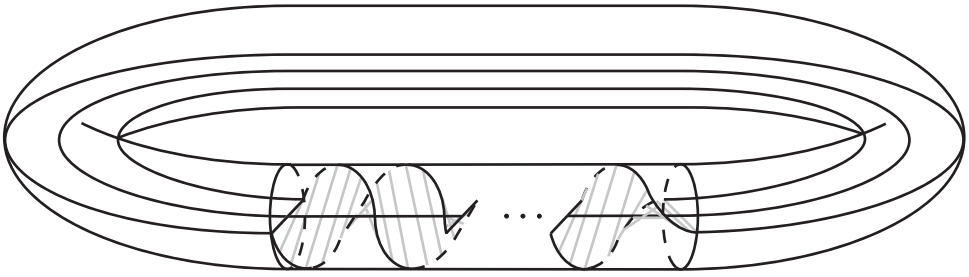


Figure 10 If $n = 1$ the midline (bold) follows the core of the torus.

When $n > 1$, we place our twisted strip of paper inside a torus, as in Figure 8, with all twists gathered in the cylinder C_t. If n is even, then one of the dashed lines of Figure 7 will run right down the center of the strip. Cutting along this line bisects the strip and allows us to lay the bisected strip flat on the torus. (We are taking advantage of the idea that we are free to move a link around in space so long as we do not pass it through itself.) Outside of C_t, we can think of the strip's two halves as two narrow bands, one near the inner equator and one near the outer equator (see Figure 11).

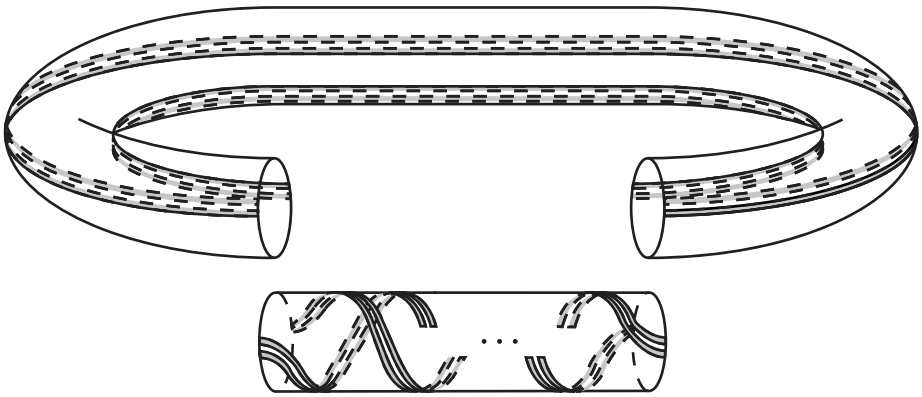


Figure 11 If n is even, after halving, the n-sections can be pushed into the torus. Here, $n = 4$.

After cutting the strip into its n sections, we will have a collection of thin strips on the torus, half grouped around the inner equator and half around the outer equator. Outside of C_t, this collection of strips cross a meridian n times, with $n/2$ intersections near each of the two equators. On the other hand, the strips will cross a longitude $mn/2$ times. For example, the top longitude intersects the rings only in C_t, and there we have $n/2$ crossings for each half twist. Thus, we have a $T(mn/2, n)$ torus link.

If n is odd, by leaving the central strip at the core of the torus, we can again place the remaining $n - 1$ sections onto the torus with $(n - 1)/2$ strips near each of the two

equators, see Figure 12. In addition to the core, we are left with strips on the torus that cross each meridian $n-1$ times while meeting a longitude $m(n-1)/2$ times, resulting in $T(m(n-1)/2, n-1) \cup C$.

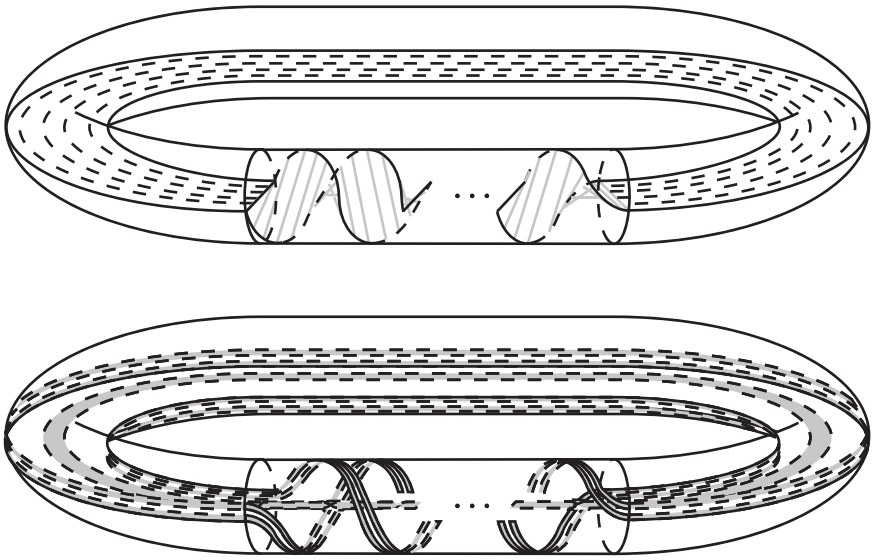


Figure 12 If n is odd, going from top to bottom, we leave the central strip at the core and push the remaining $n-1$ sections onto the torus. Here, $n = 5$.

Finally, if n is odd and m is even, we can also move the strip at the core onto the torus, making a torus link. For example, move the core to follow the top longitude outside of C_t. If we continue the curve into C_t starting at the top of the cylinder at left, then after m (an even number) of half twists, it will have returned to the top when we reach the right end of C_t so that we can close the curve. Compared to $T(m(n-1)/2, n-1)$, this adds an extra intersection with each meridian and $m/2$ intersections with each longitude. This is the $T(mn/2, n)$ torus link. ■

Paradromic rings resist coloring

We are now ready to classify the colorability of the paradromic rings. We break the argument into two cases, as in Theorem 1: paradromic rings that are torus links, and those that are not.

We begin with those that are not, in other words, the $P(m, n)$ where mn is odd and $n > 1$. The $P(m, 2)$ torus links in the section on coloring links illustrate our approach, but they have $mn = 2m$ even. As a further example, let's color $P(3, 3)$, which is not a torus link (see Figure 6). Figure 13 shows how to construct this link by repeating the pattern at top three times. Color the arcs entering the pattern at left with $x = (x_1, x_2, x_3)$. Then a matrix equation determines the colors $y = (y_1, y_2, y_3)$ leaving at right: $y \equiv S_3 x$.

Let's find the matrix S_3. Referring to the pattern at the top of Figure 13, there are two crossings involving x_1, both with x_1 as the overarc. In the lower one, condition 2 for p-colorability yields

$$2x_1 \equiv x_2 + y_2 \pmod{p} \quad \text{or} \quad y_2 \equiv 2x_1 - x_2 \pmod{p}.$$

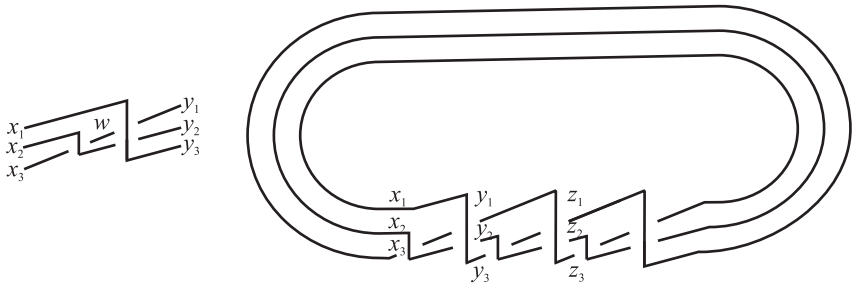


Figure 13 Form $P(3, 3)$ by repeating the pattern three times.

At the upper crossing, we have

$$2x_1 \equiv w + y_1 \pmod{p} \quad \text{or} \quad y_1 \equiv 2x_1 - w \pmod{p}.$$

The third crossing in the pattern shows how to write w in terms of x_2 and x_3:

$$2x_2 \equiv x_3 + w \pmod{p} \quad \text{or} \quad w \equiv 2x_2 - x_3 \pmod{p}.$$

Thus, we have the following system of equations modulo p:

$$\begin{aligned} 2x_1 - (2x_2 - x_3) &\equiv y_1 \\ 2x_1 - x_2 &\equiv y_2 \\ x_1 &\equiv y_3 \end{aligned}$$

with coefficient matrix

$$S_3 = \begin{pmatrix} 2 & -2 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Similarly, $(z_1, z_2, z_3) = z \equiv S_3 y \pmod{p}$. Following the arcs around the top of the link, we see that $x \equiv S_3 z \pmod{p}$. This means a p-coloring of $P(3, 3)$ corresponds to a vector x such that $x \equiv S_3^3 x \pmod{p}$. In other words, we want an eigenvector of S_3^3 modulo p with eigenvalue one.

The characteristic polynomial of S_3^3 is

$$\det(S_3^3 - \lambda I) = -(\lambda - 1)(\lambda^2 + 1).$$

As long as $p \neq 2$, the $\lambda = 1$ eigenspace has dimension one and the only eigenvectors are the constant vectors (c, c, c). Recall that a constant vector means all arcs in the diagram have color c, in violation of condition 1 for p-coloring. Therefore, when $p \neq 2$, $P(3, 3)$ is not p-colorable. On the other hand, since $P(3, 3)$ has two components, it is 2-colorable. For example, we could color the core 0 and the trefoil component 1. Thus, $P(3, 3)$ is nearly invisible. It is p-colorable only for the prime $p = 2$.

This is true of all the paradromic rings that are not torus links, as the following theorem shows. We began our study expecting that p-colorability would be an interesting way to distinguish among these rings. Instead it turns out that they are all nearly invisible.

Theorem 2. *If m and n are positive odd integers with $n > 1$, then the paradromic ring $P(m, n)$ is nearly invisible.*

Before proving the theorem, we will describe the matrix S_n that generalizes S_3 for n odd. Let m and n be positive odd integers. We represent $P(m, n)$ as in Figure 14, as suggested by our analysis of $P(m, 2)$ and $P(3, 3)$. That is, $P(m, n)$ consists of

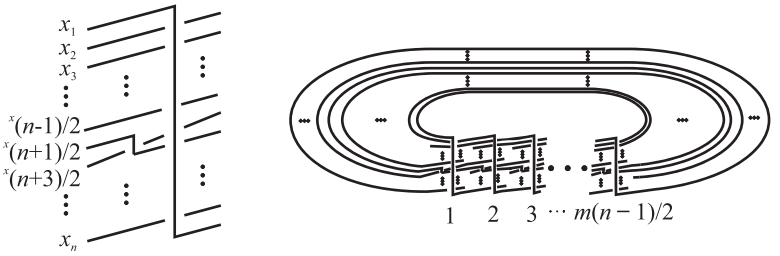


Figure 14 The pattern on n arcs (where $n > 1$ is odd) at left is repeated $m(n-1)/2$ times to form $P(m, n)$.

$m(n-1)/2$ repetitions of the pattern in Figure 14 joined up in a ring. This figure gives us the matrix

$$S_n = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ 2 & 0 & -1 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \dots & \vdots & \vdots \\ 2 & 0 & 0 & \ddots & -2 & 1 & \dots & 0 & 0 \\ 2 & 0 & 0 & \dots & -1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 2 & 0 & 0 & \dots & 0 & 0 & \ddots & -1 & 0 \\ 2 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & -1 \\ 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

If $x = (x_1, \dots, x_n)$ are the colors of the arcs entering the pattern of Figure 14 at the left, then the outgoing arcs at right are $S_n x$ modulo p. Note that, outside of a 2×2 block, S_n has -1's on the superdiagonal and a first column that is all 2's but for a 1 in the last row. The 2×2 matrix

$$\begin{pmatrix} -2 & 1 \\ -1 & 0 \end{pmatrix},$$

that breaks up the pattern is in rows $(n-1)/2$ and $(n+1)/2$ and columns $(n+1)/2$ and $(n+3)/2$ (recall that $n > 1$ is odd) and is due to the short w arc in the middle of the pattern. The S_n matrix has a surprisingly simple characteristic polynomial.

Lemma 1. *Let $n > 1$ be an odd integer. The characteristic polynomial of S_n is*

$$f_n(\lambda) = -(\lambda - 1)(\lambda^{n-1} + 1).$$

Proof. Since S_n follows a regular pattern except for columns $(n+1)/2$ and $(n+3)/2$, we will make expansions along those columns to recover more symmetric matrices. Expanding along column $(n+3)/2$, we have that

$$f_n(\lambda) = \det(S_n - \lambda I) = \det(A_{n-1}) - \lambda \det(B_{n-1}),$$

where A_{n-1} and B_{n-1} are $(n-1) \times (n-1)$ minors. Column $(n+1)/2$ then shows

$$\det(B_{n-1}) = 2\det(C_{n-2}) - (\lambda + 1)\det(D_{n-2}).$$

Below, we argue

$$\det(A_{n-1}) = (\lambda+1) - 2\lambda(1-(-\lambda)^{\frac{n-3}{2}})$$
$$\det(C_{n-2}) = 2(-\lambda)^{\frac{n-3}{2}}, \text{ and}$$
$$\det(D_{n-2}) = -\lambda^{\frac{n-3}{2}}\left(\frac{\lambda^{\frac{n+1}{2}} - \lambda^{\frac{n-1}{2}} + 2(-1)^{\frac{n-1}{2}}}{\lambda+1}\right).$$

Thus, we have

$$\begin{aligned} f_n(\lambda) &= \det(A_{n-1}) - \lambda\det(B_{n-1}) \\ &= \det(A_{n-1}) - \lambda(2\det(C_{n-2}) - (\lambda+1)\det(D_{n-2})) \\ &= -(\lambda-1)(\lambda^{n-1}+1). \end{aligned}$$

Let's verify the formulas for the determinants of A_{n-1}, C_{n-2}, and D_{n-2}. After appropriate column and row expansions (start with column $(n+1)/2$), we deduce that

$$\det A_{n-1} = (\lambda+1)(1-\lambda\det(\bar{A}_{(n-1)/2})),$$

where $\bar{A}_k$ is the $k \times k$ matrix

$$\bar{A}_k = \begin{pmatrix} 2-\lambda & -1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 2 & 0 & -1 & 0 & \dots & 0 & 0 & 0 \\ 2 & 0 & -\lambda & -1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 2 & 0 & 0 & 0 & \ddots & -1 & 0 & 0 \\ 2 & 0 & 0 & 0 & \dots & -\lambda & -1 & 0 \\ 2 & 0 & 0 & 0 & \dots & 0 & -\lambda & -1 \\ 2 & 0 & 0 & 0 & \dots & 0 & 0 & -\lambda \end{pmatrix}.$$

Expanding along the last row, we find

$$\det(\bar{A}_k) = 2 - \lambda\det(\bar{A}_{k-1}).$$

Solving the recurrence relation, we have

$$\det(\bar{A}_k) = 2\left(\frac{1-(-\lambda)^{k-1}}{1+\lambda}\right),$$

as required.

For C_{n-2}, the $(n-1)/2$ row is zero, except for a 2 at the beginning of the row. Expanding along that row, we uncover a minor that is a block diagonal matrix. The top left block is lower triangular with determinant $(-1)^{\frac{n-3}{2}}$ and the bottom right block is upper triangular with determinant $(-\lambda)^{\frac{n-3}{2}}$. The sign of the determinant depends on the parity of $(n-1)/2$, the row along which we expand.

Much like A_{n-1}, we express $\det(D_{n-2})$ in terms of a smaller, more symmetric matrix:

$$\det(D_{n-2}) = (-\lambda)^{\frac{n-1}{2}}\det(\bar{D}_{\frac{n+1}{2}}),$$

where

$$\bar{D}_k = \begin{pmatrix} 2-\lambda & -1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 2 & -\lambda & -1 & 0 & \dots & 0 & 0 & 0 \\ 2 & 0 & -\lambda & -1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 2 & 0 & 0 & 0 & \ddots & -1 & 0 & 0 \\ 2 & 0 & 0 & 0 & \dots & -\lambda & -1 & 0 \\ 2 & 0 & 0 & 0 & \dots & 0 & -\lambda & -1 \\ 2 & 0 & 0 & 0 & \dots & 0 & 0 & -\lambda \end{pmatrix}.$$

Again,

$$\det(\bar{D}_k) = 2 - \lambda \det(\bar{D}_{k-1}),$$

and solving the recurrence yields the formula for $\det(D_{n-1})$. ■

With the characteristic polynomial of S_n in hand, we can easily complete the argument that all non-torus Paradromic rings are nearly invisible.

Proof. (Theorem 2.) Let $u = m(n-1)/2$ and let p be an odd prime. Colorings of $P(m, n)$ are $\lambda = 1$ eigenvectors of S_n^u modulo p. We will show that $\lambda = 1$ is a simple root of the characteristic polynomial of S_n^u. This means that the only eigenvectors are the constant vectors $(c, c, c, \dots, c)$ and that there are no valid colorings when p is odd. Since $P(m, n)$ has at least two components, the core and a torus link, it is 2-colorable. This shows that 2 is the only prime coloring and $P(m, n)$ is nearly invisible.

Let's see why $\lambda = 1$ is a simple root when p is odd. Let F be the characteristic polynomial of S_n^u. The roots of F are the uth powers of the roots of f_n, the characteristic polynomial of S_n. By Lemma 1, 1 is a root of f_n and hence of F.

We must argue that no other root of F is equal to 1. That is, if ζ is a root of the second factor of f_n, which is $x^{n-1} + 1$, we must show $\zeta^u \not\equiv 1 \pmod{p}$.

Let ζ be a root of $x^{n-1} + 1$. Then $\zeta^{n-1} = -1$. Suppose, for a contradiction, that $\zeta^u \equiv 1 \pmod{p}$. Then, modulo p, we have

$$-1 = (-1)^m = \zeta^{m(n-1)} = \zeta^{2u} \equiv 1^2 = 1,$$

which is absurd since p is not 2.

This contradiction shows that the roots of $x^{n-1} + 1$ do not lead to additional occurrences of 1 as a root of the characteristic polynomial F of S_n^u. Therefore, S_n^u has no non-constant eigenvectors with eigenvalue one and $P(m, n)$ is not p-colorable for any odd prime p. ■

It remains only to classify colorability of the paradromic rings that are torus links. First, when $n = 1$, $P(m, 1)$ is simply a circle and is invisible. Indeed, as there is only a single arc in the diagram of a circle, it is not possible to satisfy condition 1 of colorability for any p. The paradromic rings that are torus links also include infinite families of rainbow rings and nearly invisible links, as our final theorem shows.

Theorem 3. *Let $n > 1$ and $m \geq 0$ be integers such that mn is even. Then the torus link $T = T(\frac{1}{2}mn, n)$ is a rainbow ring unless one of the following occurs:*

- *n and $\frac{1}{2}m$ are both odd, in which case T is nearly invisible,*
- *$n = 2$, in which case T is p-colorable if and only if p divides m,*
- *$n = 4$ and m is odd, in which case T is p-colorable if and only if p divides $2m$.*

At the risk of being abrupt, we will end, as we began, with a challenge: prove Theorem 3. Note that the challenge in bisecting or coloring a Möbius strip is twofold: after discovering the perplexing outcome, it remains to come up with a satisfying explanation. Similarly, during the REU, after some experimentation, we arrived at a surprising conclusion: unless $n = 2$ or 4, a paradromic torus link is either a rainbow ring, nearly invisible, or invisible (when $n = 1$). Having described the goal, we expect that an inspired reader is capable of completing the proof, just as we did during the summer. In particular, the section on coloring links above includes the argument for $P(m, 2)$ (that is, the case where $n = 2$).

Not to discourage you from following our path through the thickets, we would be remiss in not pointing out what we later learned: knot theorists have already cleared a more direct route in the case of torus links. So, we conclude by recommending additional reading that outlines this direct argument and, as a bonus, explains what, exactly, the determinant is and how it relates to an important polynomial knot invariant.

We have already suggested Adams's *The Knot Book* [**1**] and Livingston's *Knot Theory* [**4**] as nice introductions to p-coloring, including the proof that it is a link invariant. Murasugi's *Knot Theory & Its Applications* [**5**] is at a slightly more advanced level and includes a thorough introduction to the idea of the determinant of a link, $\det(L)$, and how to calculate it. As you will read there, $\det(L)$ is indeed the determinant of a matrix, although not the matrices discussed in this paper. Moreover, making use of that matrix, Murasugi shows that the determinant of a torus link $L = T(u, v)$ is given by

$$\det(T(u, v)) = |\Delta(-1)|$$

where, up to a power of x,

$$\Delta(x) = \frac{(1-x)(1-x^{\frac{uv}{d}})^d}{(1-x^u)(1-x^v)},$$

with $d = \mathrm{GCD}(u, v)$. (Despite appearances, $\Delta(x)$ always simplifies to a polynomial, called the Alexander polynomial.) Recalling that a link L is p-colorable if and only p divides $\det(L)$, the formula gives a direct way to prove Theorem 3. In particular, when $n \geq 5$, the GCD d is at least 3, which means that terms of the form $1 - x^{2k}$ survive in the numerator so that $|\Delta(-1)| = 0$ (provided n and $m/2$ are not both odd).

Acknowledgments This paper grew out of a Research Experience for Undergraduate and Teachers (REUT) at California State University, Chico that was supported in part by NSF REU Award 0354174 and by the MAA's NREUP program with funding from the NSF, NSA, and Moody's. The first three authors were undergraduates at the time, while Dan Sours is a high school teacher. We are grateful to Yuichi Handa, Ramin, Naimi, Neil Portnoy, Robin Soloway, and John Thoo for helpful comments on early versions of this paper. Additional funding came from CSU, Chico's CELT as part of a Faculty Learning Community. We thank Chris Fosen, Greg Cootsona, and the other FLC participants for fruitful discussions about the exposition.

REFERENCES

[1] Adams, C. C. (2004). *The Knot Book*. Providence, RI: American Mathematical Society.
[2] Ball, W. W. R., Coxeter, H. S. M. (1987). *Mathematical Recreations and Essays*, 13th ed. New York: Dover Publications.
[3] Butler, R., Cohen, A., Dalton, M., Louder, L., Rettberg, R., Whitt, A. (2001). *Explorations Into Knot Theory: Colorability*. Salt Lake City, UT: University of Utah.
[4] Livingston, C. (1993). *Knot Theory*. Washington, DC: Mathematical Association of America.
[5] Murasugi, K. (1996). *Knot Theory & Its Applications*. Berlin, Germany: Birkhäuser.

Summary. We determine p-colorability of the paradromic rings. These rings arise by generalizing the experiment of bisecting a Möbius strip. Instead of joining the ends with a single half twist, use m half twists, and, rather

than bisecting ($n = 2$), cut the strip into n sections. Replacing each thin strip with its midline results in the m, n paradromic link. Using the notion of p-colorability from knot theory, we determine, for each m and n, which primes p can be used to color the link.

Amazingly, almost all admit 0, 1, or an infinite number of prime colorings! This is reminiscent of solutions sets in linear algebra. Indeed, the problem quickly turns into a study of the eigenvalues of a large, nearly diagonal matrix.

JAMES GODZIK completed a Bachelor's degree at University of California, Berkeley and a Master's in Teaching Mathematics at California State University, Fullerton.

NANCY HO received a B.A. in mathematics from Mills College in 2006 and a Ph.D. in mathematics from the University of Oklahoma in 2015. She is currently working as a software engineer with Tapestry Solutions.

JENNIFER JONES was an undergraduate at Colorado State University at the time of the REU.

THOMAS W. MATTMAN received a Ph.D. in Mathematics from McGill University. His mathematical interests include knot theory and graph theory, and he enjoys supervising research by undergraduate students and teachers. In real life, he's a devoted husband to Shigemi and a doting father to Saya and Aki, who provide the comic relief.

DANIEL M. SOURS received a B.S. in Mathematics (1985) and Engineering (1981) and an M.S. in Mathematics Education (2004) from California State University, Chico. He has taught at Chico High School in Chico, California since 1987, and has also served as adjunct faculty at California State University, Chico and Butte Community College. He adores his wonderful wife Mary and loves relaxing with her on the ocean in Little River California.

p-Adic Metrics and the Infinitude of Primes

HAYDAR GÖRAL
Faculty of Sciences, Dokuz Eylül University
Tınaztepe Yerleşkesi, 35390 Buca/Izmir, Turkey
haydar.goral@deu.edu.tr

By applying a geometric approach, we provide a proof of the infinitude of primes via p-adic metrics. This is a novel approach to a well-known, and quite old, result. There are many proofs for the infinitude of primes, and it is commonly believed that the first one dates back to the ancient Greek mathematician Euclid. All proofs for the infinitude of primes use the fact that prime numbers form a multiplicative basis for the integers, and we will use this in our proof as well. In our approach, we apply p-adic metrics as a novelty.

In this note, p always denotes a prime number. For a given $a \in \mathbb{Z} \setminus \{0\}$, the *$p$-adic order* of a is the largest power of p dividing a, and it is denoted by $\nu_p(a)$. In other words, for a non-zero integer a, the equality $\nu_p(a) = m$ means that p^m divides a but p^{m+1} does not divide a. The *p-adic absolute value* of a non-zero integer a is defined by $|a|_p = p^{-\nu_p(a)}$, and $|0|_p = 0$ as usual.

For instance:

$$\nu_2(2 \cdot 3^2) = \nu_2(18) = \nu_2(-18) = 1$$
$$\nu_3(18) = \nu_3(-18) = 2,$$
$$|18|_2 = |-18|_2 = 2^{-1} = \frac{1}{2}$$
$$|18|_3 = |-18|_3 = 3^{-2} = \frac{1}{3^2} = \frac{1}{9}.$$

Clearly,

$$|1|_p = 1 \quad \text{and} \quad |p|_p = \frac{1}{p}$$

for any p. If p divides a, then $|a|_p \leq \frac{1}{p}$, and if p does not divide a, then $|a|_p = 1$. Also,

$$0 \leq |a|_p \leq 1 \quad \text{and} \quad |a|_p = |-a|_p$$

for any integer a and prime p.

Now we introduce the notions of "metric" and "metric space."

Definition (Metric and metric space)**.** Let X be a non-empty set. A metric d on X is a map $d : X \times X \to [0, \infty)$ such that the following three conditions are satisfied:

(i) (Positivity) For all $x, y \in X$, $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$.
(ii) (Symmetry) For all $x, y \in X$, $d(x, y) = d(y, x)$.
(iii) (Triangle inequality) For all $x, y, z \in X$, $d(x, y) \leq d(x, z) + d(z, y)$.

If d is a metric on X, then the pair (X, d) is called a metric space.

Math. Mag. **93** (2020) 19–22. doi:10.1080/0025570X.2019.1679574
MSC: 11A41, 11S99

The *p-adic metric* between integers x and y is defined to be

$$d_p(x, y) = |x - y|_p.$$

Next, we prove that the p-adic metric satisfies properties (i), (ii), and (iii). This implies the following proposition.

Proposition 1. For any prime number p, the map d_p is a metric on $\mathbb{Z}$.

Proof. Positivity: Let x and y be two integers. Clearly,

$$d_p(x, y) = |x - y|_p \geq 0 \quad \text{and} \quad d_p(x, x) = |0|_p = 0.$$

Now suppose that $d_p(x, y) = 0$. We must show that $x = y$. If x is different from y, then $x - y$ is not 0, and there exists a non-negative integer m such that p^m divides $x - y$ but p^{m+1} does not divide $x - y$. In other words, we have $v_p(x - y) = m$ and so

$$d_p(x, y) = |x - y|_p = p^{-m} \neq 0,$$

which is a contradiction. Therefore, we conclude that $d_p(x, y) = 0$ implies that $x = y$.

Symmetry: Let x and y be two integers. If $x = y$, then it is clear that

$$d_p(x, y) = 0 = d_p(y, x).$$

If x is not y, one sees that $v_p(x - y) = v_p(y - x)$, and it follows again that $d_p(x, y) = d_p(y, x)$.

Triangle inequality: Let x, y, and z be three integers. If $x = y$, $x = z$, or $y = z$, then the triangle inequality follows either trivially or from positivity. Thus, we may assume that x, y and z are distinct integers. Let

$$m = v_p(x - y), \quad n = v_p(x - z), \quad \text{and} \quad k = v_p(z - y).$$

We may suppose that $n \leq k$. Since

$$x - y = (x - z) + (z - y)$$

and p^n divides $x - z$ and $z - y$, we see that p^n also divides $x - y$. This yields that $n \leq m$. Therefore,

$$d_p(x, y) = p^{-m} \leq p^{-n} \leq p^{-n} + p^{-k} = d_p(x, z) + d_p(z, y).$$

■

We will also need the following proposition, whose proof is straightforward.

Proposition 2. Let X be a non-empty set and $\rho_1, \ldots, \rho_k$ be metrics on X. Then the map

$$\rho(x, y) = \rho_1(x, y) + \cdots + \rho_k(x, y)$$

is also a metric on X.

For instance, the sum

$$\begin{aligned} d(x, y) &= d_2(x, y) + d_3(x, y) + d_5(x, y) + d_7(x, y) \\ &= |x - y|_2 + |x - y|_3 + |x - y|_5 + |x - y|_7 \end{aligned}$$

is a metric on $\mathbb{Z}$.

The next observation may shed light on equation (1) in our proof. Let m and n be integers such that p divides $m - n$, where p is one of 2, 3, 5, or 7. Then we have that

$$|m - n|_p \leq \frac{1}{p} \leq \frac{1}{2}.$$

Therefore,

$$\begin{aligned} d(m, n) &= |m - n|_2 + |m - n|_3 + |m - n|_5 + |m - n|_7 \\ &\leq \frac{1}{2} + 3 = 4 - \frac{1}{2} = \frac{7}{2}. \end{aligned}$$

For example, if $m = 29$ and $n = 14$, then $p = 3$ divides $m - n = 15$. It follows that

$$\begin{aligned} d(29, 14) &= |15|_2 + |15|_3 + |15|_5 + |15|_7 \\ &= 1 + \frac{1}{3} + \frac{1}{5} + 1 \leq 1 + \frac{1}{2} + 1 + 1 = \frac{7}{2} = 4 - \frac{1}{2}. \end{aligned}$$

We are now ready to present our proof of the infinitude of primes. Briefly, our proof proceeds as follows: If there are finitely many primes, then we construct a metric d on $\mathbb{Z}$ coming from the p-adic metrics and show that d is discrete (this comes from the claim below) by using the fact that prime numbers form a multiplicative basis for the integers. We then arrive at a contradiction by showing that d is actually not discrete.

Theorem. There are infinitely many primes.

Proof. Suppose that the set of prime numbers $\mathbb{P}$ is finite. We list all the primes as $p_1, \ldots, p_k$ where $k \geq 1$. For $a, b \in \mathbb{Z}$, define

$$d(a, b) = \sum_{p \in \mathbb{P}} d_p(a, b) = \sum_{p \in \mathbb{P}} |a - b|_p = \sum_{i=1}^{k} |a - b|_{p_i}.$$

Note that the sum above is actually finite, as implied by the last equality. By Propositions 1 and 2, we see that d is a metric on $\mathbb{Z}$. Observe that for any integer m, we have

$$d(m, m + 1) = d(m, m - 1) = \sum_{p \in \mathbb{P}} |1|_p = \sum_{p \in \mathbb{P}} 1 = k.$$

If n is not in the set $\{m - 1, m, m + 1\}$, then the integer $m - n$ is of absolute value greater than or equal to 2, and hence it is divisible by some prime number q. In particular,

$$|m - n|_q \leq \frac{1}{q} \leq \frac{1}{2}.$$

Therefore, if n is not in the set $\{m - 1, m, m + 1\}$, then

$$\begin{aligned} d(m, n) &= |m - n|_q + \sum_{p \in \mathbb{P} \setminus \{q\}} |m - n|_p \\ &\leq \frac{1}{q} + \sum_{p \in \mathbb{P} \setminus \{q\}} 1 \leq \frac{1}{2} + k - 1 = k - \frac{1}{2}. \end{aligned} \tag{1}$$

Moreover,

$$d(m-1, m+1) = \sum_{p\in\mathbb{P}} |2|_p = |2|_2 + \sum_{p\in\mathbb{P}\setminus\{2\}} |2|_p$$
$$= \frac{1}{2} + k - 1 = k - \frac{1}{2}.$$

We define the open ball of radius $r > 0$ and center $x \in \mathbb{Z}$ to be the set

$$B(x, r) = \{y \in \mathbb{Z} : d(x, y) < r\}.$$

Based on the foregoing observations, we now claim that for any integer m, we have

$$B\left(m+1, \frac{1}{2}\right) = \{m+1\}.$$

To see this, notice that we clearly have that $m+1$ is in $B(m+1, \frac{1}{2})$. Let $n \neq m+1$ be in $B(m+1, \frac{1}{2})$, which is to say that $d(m+1, n) < \frac{1}{2}$. Note that the above discussions imply that n cannot be m or $m-1$ since $k > k - \frac{1}{2} \geq \frac{1}{2}$. Thus, we may assume that n is different from $m-1, m$, and $m+1$. Then by equation (1), we have that $d(m, n) \leq k - \frac{1}{2}$. Applying the triangle inequality to d, we get that

$$k = d(m, m+1) \leq d(m, n) + d(m+1, n) < k - \frac{1}{2} + \frac{1}{2} = k,$$

a contradiction. This shows the claim is true.

However, we can also show that the claim is not true. Choose positive integers b_i such that

$$\frac{1}{p_i^{b_i}} < \frac{1}{2k}$$

for $i = 1, \ldots, k$. Set $\ell = p_1^{b_1} \ldots p_k^{b_k}$. Then,

$$d(\ell, 0) = \frac{1}{p_1^{b_1}} + \cdots + \frac{1}{p_k^{b_k}} < k \cdot \frac{1}{2k} = \frac{1}{2}.$$

This contradicts the claim above for $m = \ell - 1$, and hence establishes that there are infinitely many primes. ■

For a topological proof of the infinitude of the primes that is related to ours, we refer the reader to [**1**]. A historical survey and more than 180 proofs of the infinitude of primes can be found in [**2**].

REFERENCES

[1] Fürstenberg, H. (1955). On the infinitude of primes. *Amer. Math. Monthly*. 62(5): 353. doi.org/10.1080/00029890.1955.11988641

[2] Meštrović, R. (2018). Euclid's theorem on the infinitude of primes: A historical survey of its proofs. arxiv.org/pdf/1202.3670.pdf

Summary. We give a proof of the infinitude of primes using p-adic metrics.

HAYDAR GÖRAL (MR Author ID: 1013641) graduated from Istanbul Bilgi University and got his doctoral degree in mathematics from Université Claude Bernard Lyon 1. Now, he is an assistant professor at Dokuz Eylül University in Izmir. He is interested in number theory and mathematical logic.

Irrational Thoughts

HAROLD P. BOAS
Texas A&M University
College Station, TX 77843
boas@tamu.edu

Dedicated to the memory of Joel Zinn.

Who first proved that $\sqrt{2}$ is an irrational number?

Nobody knows. Specialists on ancient Greek mathematics presume that a follower of Pythagoras formulated a proof sometime during the fifth century BCE [10, 18, 19, 28, 32], but pinpointing a decade and naming the mastermind are matters of pure speculation. "The date and manner of the first discovery of incommensurability have not been preserved for us by any credible witness" [28, p. 21].

Yet there is a realistic prospect of identifying modern innovators responsible for the best proof. What I mean by "best" is a maximally elegant argument belonging to *The Book*, that hypothetical volume jocularly conceived by the great 20th-century mathematician Paul Erdős as an omniscient being's repository for the most beautiful proofs of all theorems [1]. Since beauty is subjective, I will substitute brevity as an objective criterion. A proof one sentence long is surely optimal.

I am moved to address the topic of irrationality by a recent note in this journal [5] that regrettably ignores the history. Like mountaineering, mathematics ideally should be experienced with an appreciation of the trials and the triumphs of past generations. The goal is not only to reach a lofty summit, but also to ascend faster or more simply or with greater style than ever before. My aim here is to celebrate a 19th-century genius who made an essential stride forward more than two millennia after the first explorers.

Traditionally, the irrationality of $\sqrt{2}$ is proved clumsily by wielding the big club of the fundamental theorem of arithmetic (every natural number can be expressed uniquely as a product of prime numbers). This cudgel is needed to posit a representation of $\sqrt{2}$ as a fraction "in lowest terms." Even in the early 21st century, formalized proofs generated or checked by computers use this method [48]. Human connoisseurs prefer to replace divisibility properties of integers by the lightweight tool of the well-ordering principle (every nonvoid set of natural numbers has a least element) [33, 37], along with the elementary knowledge that the squaring function is increasing on the natural numbers. When did this refined point of view arise?

Arguably, no really satisfactory proof that $\sqrt{2}$ is irrational could exist before the creation of a rigorous definition of the irrational numbers. A standard technique nowadays for constructing the set of real numbers from the set of rational numbers is the device of "Dedekind cuts," named for the second-best mathematician from the city of Braunschweig (Brunswick in English) [42], Richard Dedekind (1831–1916). He was the last doctoral student of the preeminent mathematical Brunswicker, the superlative Carl Friedrich Gauss (1777–1855). Dedekind's innovative theory of the real numbers dates to November 24, 1858, according to his own testimony [12, p. 10].

One sometimes sees a claim that an equivalent definition of the real numbers is implicit in the theory of proportion due to Eudoxus of Cnidus (fourth century BCE). Dedekind himself, while acknowledging inspiration from the ancient Greeks, denies that any of his predecessors conceptualized the notion of completeness of the real numbers [13, pp. 39–40].

Math. Mag. **93** (2020) 23–26. doi:10.1080/0025570X.2020.1682404
MSC: 00-02

After defining cuts, Dedekind wants to show that his new construction produces some entities that cannot be represented as quotients of integers. He argues that if there were a rational number whose square equals 2, then there would be some natural numbers t and u such that $t^2 - 2u^2 = 0$. Invoke well-ordering to choose u as small as possible. Observe that $u^2 < 2u^2 = t^2 < 2t^2 = 4u^2$, so $u < t < 2u$. Define two new natural numbers as follows: $t' = 2u - t$, and $u' = t - u$. Then u' is a natural number smaller than u, and routine algebra shows that $(t')^2 - 2(u')^2 = 0$, contradicting the minimality of u.

The reasoning alternatively can be expressed in the language of fractions. Indeed, if $t^2 - 2u^2 = 0$, then

$$\frac{t}{u} = \frac{t}{u} \cdot \frac{t-u}{t-u} = \frac{t^2 - tu}{u(t-u)} = \frac{2u^2 - tu}{u(t-u)} = \frac{2u - t}{t-u}.$$

As before, the alleged minimality of u is contradicted.

This lovely argument [12, §4] (an English translation exists [13]) can be considered the favored proof of the irrationality of $\sqrt{2}$, in view of the frequency of rediscovery [6, 7, 16, 22, 23, 27, 34, 39, 44]. Moreover, there are appealing geometric realizations of Dedekind's proof [2, 9, 11, 15, 20, 26, 31, 35, 36, 41, 45]. Dedekind actually works with a general natural number D that is not a perfect square. I have preserved his notation but specialized for simplicity to the case when $D = 2$.

Since the essence of Dedekind's work is to construct the irrational numbers, a key point in his discussion is the absence of any a priori assumption that the symbol $\sqrt{2}$ actually defines a real number. His proof can be condensed to one sentence if you are willing to accept the existence of $\sqrt{2}$ in advance. For if there is a natural number u having the property that $u\sqrt{2}$ is an integer, then there is a smallest u with this property; but $u\sqrt{2} - u$ is a smaller natural number having the same property! (Notice that the natural number $u\sqrt{2} - u$ is precisely Dedekind's $t - u$, with t representing the integer $u\sqrt{2}$.)

The number theorist Theodor Estermann (1902–1991), educated in Germany and Palestine prior to a distinguished career at University College London [38], published this streamlined version of Dedekind's proof as his last paper in retirement [14]. Other authors have similarly adapted the general case of Dedekind's argument, as follows.

Suppose D is a natural number, not a perfect square, and (seeking a contradiction) suppose that $\sqrt{D}$ is a rational number. If u is the smallest natural number having the property that $u\sqrt{D}$ is an integer, then $u\sqrt{D} - u\lfloor\sqrt{D}\rfloor$ is a smaller natural number having the same property. (The symbol $\lfloor x \rfloor$ denotes the floor function, the greatest integer less than or equal to x.) Notice that the well-ordering principle suffices to construct the floor of a rational number, contrary to an assertion by a well-known computer scientist that the division algorithm is needed here [4, p. 335].

Herbert Edward Vaughan (1911–1992), a pioneer in the 1950s of what came to be called the New Math, published the earliest instance that I have located of this proof for the general case [47, p. 577], anticipating Estermann's note. Warren Gamaliel Strickland (1922–2015), a mathematics educator in Texas, also beat Estermann to the punch [43]. Subsequent rediscoveries [4, 17, 25] have "appeared in various forms and places throughout many years" according to Julian Havil [24, p. 125], an author of popular mathematics books and a former master of mathematics at Winchester College in England.

The ultimate task is to bootstrap the argument to demonstrate that if k and D are arbitrary integers greater than 1, and if D is not a kth power, then $\sqrt[k]{D}$ is irrational. If you allow the convention that single-letter symbols represent natural numbers, then the technique of infinite descent at the heart of all the preceding reasoning yields the

following brief proof by contradiction:

> If u is such that $u(\sqrt[k]{D})^j$ is an integer whenever $j < k$, then $u\sqrt[k]{D} - u\lfloor\sqrt[k]{D}\rfloor$ is a smaller natural number having the same property.

The first published instance of this proof that I have found is a note by the Japanese mathematician Toshio Shibata [**40**]. The proof has been rediscovered more than once [**8**, **21**], and numerous authors have made related but suboptimal attempts [**3–5**, **29**, **30**, **46**, **47**].

The metaphor of *The Book* might evolve during the 21st century into *The Blog*, a virtual repository of mathematical gems maintained by an artificial intelligence of unlimited capability. In this spirit, I invite readers to propagate the single-sentence irrationality proof through their favorite networking websites or messaging apps or wikis as a way to forestall future rediscoveries. Is honoring Dedekind's mathematical legacy via social media an irrational idea?

REFERENCES

[1] Aigner, M., Ziegler, G. M. (2010). *Proofs from the Book*, 4th ed. Berlin: Springer-Verlag. doi.org/10.1007/978-3-642-00856-6

[2] Apostol, T. M. (2000). Irrationality of the square root of two—A geometric proof. *Amer. Math. Monthly*. 107(9): 841–842. doi.org/10.2307/2695741

[3] Bailey, D. F. (1977). Something new, something old. *Math. Mag.* 50(3): 175. jstor.org/stable/2689510

[4] Beigel, R. (1991). Irrationality without number theory. *Amer. Math. Monthly*. 98(4): 332–335. doi.org/10.2307/2323801

[5] Bergen, J. (2017). Is this the easiest proof that nth roots are always integers or irrational? *Math. Mag.* 90(3): 225. doi.org/10.4169/math.mag.90.3.225

[6] Bloom, D. M. (1995). A one-sentence proof that $\sqrt{2}$ is irrational. *Math. Mag.* 68(4): 286. doi.org/10.2307/2690577

[7] Brown, A. L. (2003). The irrationality of $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$ .... *Math. Gaz.* 87(508): 143. doi.org/10.1017/S0025557200172341

[8] Bumcrot, R. J. (1986). Irrationality made easy. *Coll. Math. J.* 17(3): 243–244. doi.org/10.2307/2686983

[9] Cairns, G. (2012). Proof without words: $\sqrt{2}$ is irrational. *Math. Mag.* 85(2): 123. doi.org/10.4169/math.mag.85.2.123

[10] Caveing, M. (1996). The debate between H. G. Zeuthen and H. Vogt (1909–1915) on the historical source of the knowledge of irrational quantities. *Centaurus* 38: 277–292. doi.org/10.1111/j.1600-0498.1996.tb00611.x

[11] Conway, J. H., Shipman, J. (2013). Extreme proofs I: The irrationality of $\sqrt{2}$. *Math. Intell*. 35(3): 2–7. doi.org/10.1007/s00283-013-9373-9

[12] Dedekind, R. (1872). *Stetigkeit und irrationale Zahlen*. Braunschweig: Vieweg.

[13] Dedekind, R. (1909). *Essays on the Theory of Numbers: I. Continuity and Irrational Numbers. II. The Nature and Meaning of Numbers* (Beman, W. W., trans.). Chicago: Open Court Publishing. Reprinted 1963, New York: Dover.

[14] Estermann, T. (1975). The irrationality of $\sqrt{2}$. *Math. Gaz.* 59(408): 110. doi.org/10.2307/3616647

[15] Eves, H. (1945). The irrationality of $\sqrt{2}$. *Math. Teacher*. 38(7): 317–318. jstor.org/stable/27953017

[16] Fine, N. J. (1976). Look, Ma, no primes. *Math. Mag.* 49(5): 249. doi.org/10.2307/2689457

[17] Flanders, H. (1999). Math Bite: Irrationality of $\sqrt{m}$. *Math. Mag.* 72(3): 235. doi.org/10.2307/2690889

[18] Fowler, D. (1999). *The Mathematics of Plato's Academy: A New Reconstruction*, 2nd ed. New York: Oxford Univ. Press.

[19] Fowler, D. H. (1994). The story of the discovery of incommensurability, revisited. In: Gavroglu, K., Christianidis, J., Nicolaidis, J., eds. *Trends in the Historiography of Science*. Dordrecht: Springer, pp. 221–235. doi.org/10.1007/978-94-017-3596-4_17

[20] Gardner, M. (1997). The square root of two = 1.41421 35623 73095 .... *Math Horizons*. 4(4): 5–8. jstor.org/stable/25678108

[21] Gilat, D. (2012). Gauss's lemma and the irrationality of roots, revisited. *Math. Mag.* 85(2): 114–116. doi.org/10.4169/math.mag.85.2.114

[22] Grant, M., Perella, M. (1999). Descending to the irrational. *Math. Gaz.* 83(497): 263–267. doi.org/10.2307/3619054

[23] Halfar, E. (1955). The irrationality of $\sqrt{2}$. *Amer. Math. Monthly*. 62(6): 437. doi.org/10.2307/2307004
[24] Havil, J. (2012). *The Irrationals: A Story of the Numbers You Can't Count On*. Princeton, NJ: Princeton Univ. Press.
[25] Hughes, C. R. (1999). Irrational roots. *Math. Gaz.* 83(498): 502–503. doi.org/10.2307/3620972
[26] Kalman, D., Mena, R., Shahriari, S. (1997). Variations on an irrational theme—Geometry, dynamics, algebra. *Math. Mag.* 70(2): 93–104. doi.org/10.2307/2691430
[27] Khazad, A., Schwenk, A. J. (2005). Irrational roots of integers. *Coll. Math. J.* 36(1): 56–57. doi.org/10.2307/30044820
[28] Knorr, W. R. (1975). *The Evolution of the Euclidean Elements: A Study of the Theory of Incommensurable Magnitudes and Its Significance for Early Greek Geometry*. Dordrecht: Reidel. doi.org/10.1007/978-94-010-1754-1
[29] Kominers, S. D. (2010). Irrational roots revisited. *Math. Gaz.* 94(530): 303–304. doi.org/10.1017/S0025557200006598
[30] Lange, L. J. (1969). A simple irrationality proof for *n*th roots of positive integers. *Math. Mag.* 42(5): 242–243. doi.org/10.2307/2688700
[31] Lord, N. (2017). Using A4-sized paper to illustrate that $\sqrt{2}$ is irrational. *Math. Gaz.* 101(550): 142–145. doi.org/10.1017/mag.2017.24
[32] Lučić, Z. (2015). Irrationality of the square root of 2: The early Pythagorean proof, Theodorus's and Theaetetus's generalizations. *Math. Intell*. 37(3): 26–32. doi.org/10.1007/s00283-014-9521-x
[33] MacHale, D. (2008). The well-ordering principle for $\mathbb{N}$. *Math. Gaz.* 92(524): 257–259. doi.org/10.1017/S0025557200183093
[34] Maier, E. A., Niven, I. (1964). A method of establishing certain irrationalities. *Math. Mag.* 37(4): 208–210. doi.org/10.2307/2688586
[35] Miller, S. J., Montague, D. (2012). Picturing irrationality. *Math. Mag.* 85(2): 110–114. doi.org/10.4169/math.mag.85.2.110
[36] Moreno, S. G., García-Caballero, E. M. (2013). Irrationality of *k*th roots. *Amer. Math. Monthly* 120(8): 688. doi.org/10.4169/amer.math.monthly.120.08.679
[37] Myerson, G. (2008). Irrationality via well-ordering. *Austral. Math. Soc. Gaz.* 35(2): 121–125. austms.org.au/Publ/Gazette/2008/May08/Myerson.pdf
[38] Roth, K. F., Vaughan, R. C. (1994). Obituary: Theodor Estermann. *Bull. Lond. Math. Soc*. 26(6): 593–606. doi.org/10.1112/blms/26.6.593
[39] Sagher, Y. (1988). What Pythagoras could have done. *Amer. Math. Monthly*. 95(2): 117. doi.org/10.2307/2323064.
[40] Shibata, T. (1974). On a proof of the irrationality of $\sqrt{2}$. *Math. Teacher*. 67(2): 119. jstor.org/stable/27959580
[41] Siu, M. K. (2013). Some more on Estermann and Pythagoras. *Math. Gaz.* 97(539): 272–273. doi.org/10.1017/S0025557200005891
[42] Sonar, T. (2012). Brunswick's second mathematical star: Richard Dedekind (1831–1916). *Math. Intell*. 34(2): 63–67. doi.org/10.1007/s00283-012-9285-0
[43] Strickland, W. (1972). A more general proof for $\sqrt{2}$. *Math. Teacher*. 65(2): 109. jstor.org/stable/27958732
[44] Subbarao, M. V. (1968). A simple irrationality proof for quadratic surds. *Amer. Math. Monthly*. 75(7): 772–773. doi.org/10.2307/2315207
[45] Turner, B. (1977). A geometric proof that $\sqrt{2}$ is irrational. *Math. Mag.* 50(5): 263. doi.org/10.2307/2689535
[46] Ungar, P. (2006). Irrationality of square roots. *Math. Mag.* 79(2): 147–148. doi.org/10.2307/27642924
[47] Vaughan, H. E. (1960). On the irrationality of roots. *Amer. Math. Monthly*. 67(6): 576–578. doi.org/10.2307/2309183
[48] Wiedijk, F., ed. (2006). *The Seventeen Provers of the World*. Berlin: Springer. doi.org/10.1007/11542384

Summary. This historical article discusses the best proof of irrationality of roots of integers.

HAROLD P. BOAS (MR Author ID: 38310) is Presidential Professor for Teaching Excellence and Regents Professor at Texas A&M University in College Station, where he has been a faculty member for $5\lfloor\sqrt{50}\rfloor$ years. His Erdős number is the minimal prime, and he has a perfect number of grandchildren.

Efficiently Constructing Tangent Circles

ARTHUR BARAGAR
University of Nevada Las Vegas
Las Vegas, NV 89154
baragar@unlv.nevada.edu

ALEX KONTOROVICH
Rutgers University
New Brunswick, NJ 08854
alex.kontorovich@rutgers.edu

The Greek geometers of antiquity devised a game—we might call it geometrical solitaire—which . . . must surely stand at the very top of any list of games to be played alone. Over the ages it has attracted hosts of players, and though now well over 2000 years old, it seems not to have lost any of its singular charm or appeal. – Howard Eves

The Problem of Apollonius is to construct a circle tangent to three given ones in a plane. The three circles may also be limits of circles, that is, points or lines; and "construct" means using a straightedge and compass. Apollonius's own solution did not survive antiquity [**8**], and we only know of its existence through a "mathscinet review" by Pappus half a millennium later. Both Viéte and Gergonne rose to the challenge of devising their own constructions, and either may possibly have rediscovered the solution of Apollonius. In this note, we consider a special case of the problem of Apollonius, but from the point of view of *efficiency*. Our goal is to present, in what we believe is the most efficient way possible, a construction of four mutually tangent circles. Of course, five (generic) circles cannot be mutually tangent in the plane, for their tangency graph, the complete graph K_5, is non-planar.

Our measure of efficiency is the one used by Hartshorne [**7**, p. 20]. We aim to minimize the number of *moves*, where a move is the act of drawing either (1) a line through two points, or (2) a circle through a point with given center; like Euclid, our compass collapses when lifted. Marking a point does not count as a move, for no act of drawing is involved. There is another measure proposed by Lemoine in 1907 [**4**, p. 213], which seems to capture the likelihood of propagated error in a construction. We believe Hartshorne's measure is more in the spirit of Euclid and Plato, who thought of constructions as idealized.

The previous best construction appears to be Eppstein's [**2**], though one might argue that ours can be derived from Gergonne's more general construction. We discuss both in our closing remarks.

Baby cases: one and two circles

Constructing one circle costs one move: let A and Z be any distinct points in the plane and draw the circle $O_A(Z)$ with center A and passing through Z. (We will use the notation $O_P(Q)$ for the circle centered at P that goes through Q, or just O_P when there is no need to refer to Q.) Given O_A, constructing a second circle tangent to it costs two more moves: draw the line AZ, and put an arbitrary point B on this line (say, outside O_A). Now draw the circle $O_B(Z)$. Then O_A and O_B are obviously tangent at

Math. Mag. **93** (2020) 27–32. doi:10.1080/0025570X.2020.1682447
MSC: 51N20, 01A20

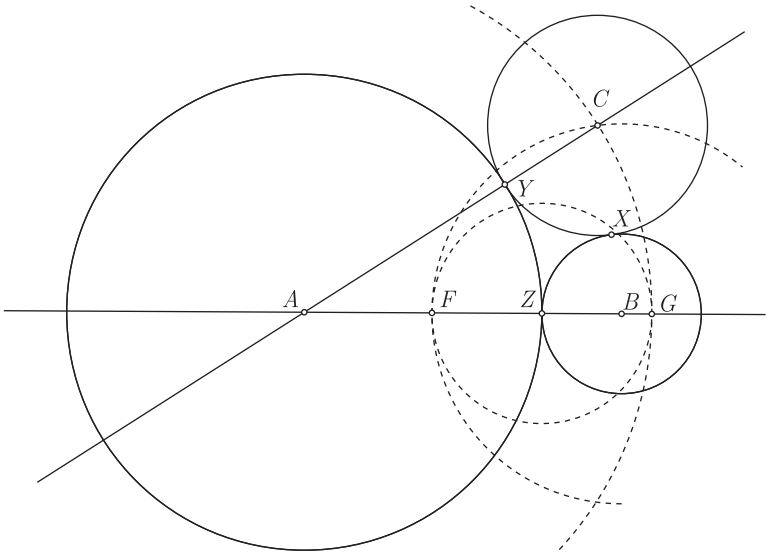


Figure 1 A third tangent circle. The solid lines/circles are the initial and final objects (or objects we wish to include in the next step), while the dotted figures are the intermediate constructions.

Z. In fact one cannot do better than two moves, for otherwise one could draw the circle O_B immediately, but this requires *a priori* knowledge of a point on O_B.

Warmup: three circles

Given two circles O_A and O_B, tangent at Z, and the line AB, how many moves does it take to construct a third circle tangent to both O_A and O_B? We encourage readers at this point to stop and try this problem themselves.

Proposition 1. *Given two mutually tangent circles O_A and O_B, and the line AB, a generic circle tangent to both O_A and O_B is constructible in five moves.*

We first give the construction, then the proof that it works.

The construction Draw a circle O_Z centered at Z and with arbitrary radius c, which will be the radius of our third circle (this is move 1). Let it intersect AB at F and G. Next draw the circles $O_A(G)$ (move 2) and $O_B(F)$ (move 3); see Figure 1. Let these two circles intersect at C. Construct the line AC (move 4) and let Y be its appropriate intersection with O_A. Finally, draw the circle $O_C(Y)$ (move 5). Then O_C is tangent to O_A and O_B.

Proof. It is clear that O_C is tangent to O_A. Since $|CY| = |GZ|$, the radius of O_C is c. Let X be the appropriate point where O_B intersects the line BC (the latter is not constructed). We wish to prove that X lies on O_C, as shown, and that O_C is therefore tangent to O_B at X. Note that $|CX| = |FZ| = c$, the radius of O_C, so X is indeed on O_C. Thus O_C is tangent to O_B at X, as claimed. ■

Remark. The locus of points C is a hyperbola with foci A and B. By choosing F to be on the same side of Z as A, as we did in Figure 1, we get one branch of the hyperbola. The other branch is obtained by choosing F on the other side of Z (and letting c be sufficiently large).

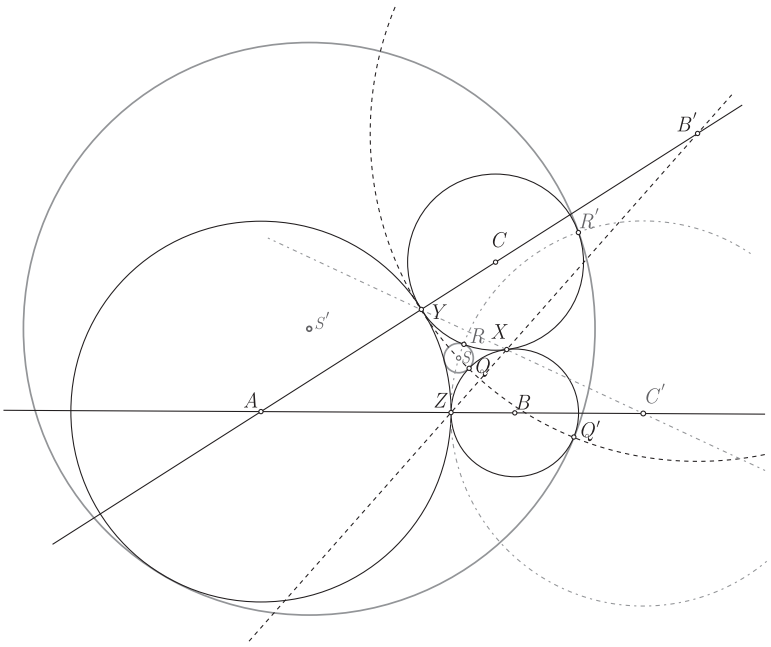


Figure 2 The circle $O_{B'}$ and points Q and Q'. The solid gray circles are the Apollonian circles O_S and $O_{S'}$ that we are in the process of constructing.

Main theorem: the fourth circle

Finally we come to the main event, the fourth tangent circle, which we call the Apollonian circle.* We are given three mutually tangent circles, O_A, O_B, and O_C, lines AB and AC, and the points of tangency X, Y, and Z; that is, we are given the already constructed objects in Figure 1.

Theorem 1. *An Apollonian circle tangent to O_A, O_B, and O_C in Figure 1 is constructible in seven moves.*

The construction Draw the line XZ (this is move 1) and let it intersect AC at B'. Draw the circle $O_{B'}(Y)$ (move 2). It intersects O_B at Q and Q', with Q, say, closer to A; see Figure 2. We repeat this procedure: draw the line XY, let it intersect AB at C', draw the circle $O_{C'}(Z)$ and let $O_{C'}$ intersect O_C at R and R', with R closer to A. This repetition used two more moves. Next draw the lines BQ and CR (now up to move 6) and let them meet at S. Finally, use the seventh move to draw the desired Apollonian circle $O_S(Q)$; see Figure 3.

Remark. If a pair of lines, e.g., AC and XZ, are parallel (so B' is at infinity), then use the line BY in lieu of $O_{B'}$ (the former is the limit of the latter as $B' \to \infty$).

Circle inversions Before the proof, we remind the reader about circle inversions. For any circle with center O and radius r, the inversion of a point P is, by definition, the point P' on the ray OP that satisfies

$$\frac{|OP|}{r} = \frac{r}{|OP'|}.$$

*Many objects in the literature are named after Apollonius though he had nothing to do with them, such as the Apollonian gasket and the Apollonian group (see, e.g., Kontorovich [9]). The fourth tangent circle really *is* due to him, though most authors refer to it as the "Soddy" circle.

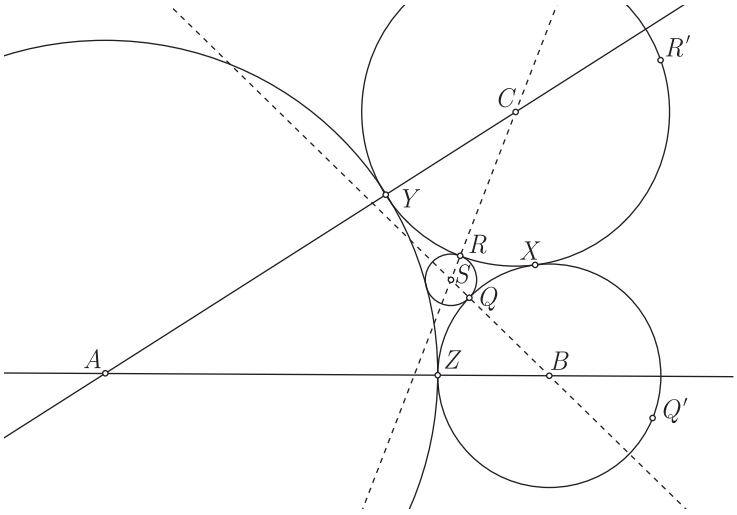


Figure 3 The construction of S and the Apollonian circle O_S.

Two well-known properties of inversions are: the image of a line or circle is itself a line or circle, and angles are preserved. See any good text for details (e.g., Eves [4, Section 3.4] or Hartshorne [7, Section 37]).

Proof. There is a unique circle such that inversion through it sends O_A to O_C. We claim that $O_{B'}$ is this circle. Indeed, such an inversion must fix O_B, and therefore sends X to Z. Hence, its center must lie on XZ. Its center also lies on the line perpendicular to O_A and O_C, which is the line AC. Thus, its center is $B' = XZ \cap AC$. Finally, the point Y is fixed by this inversion, giving the claim.

Next, we claim that the point of tangency of O_B and the Apollonian circle O_S must also lie on this inversion circle $O_{B'}$ (in which case this point must be Q, as constructed). Indeed, since the inversion preserves the initial configuration of three circles, it must also fix O_S, and hence also its point of tangency with O_B.

Finally, since O_B and O_S are tangent at Q, their centers are collinear with Q; that is, S lies on the line BQ. Similarly, S lies on CR. ■

Remark. The second solution, $O_{S'}$, to the Apollonian problem can now be constructed in a further three moves. Indeed, the points of tangency Q' and R' are already on the page. Draw the lines BQ' and CR' (two more moves) and let them intersect at S'. Then draw $O_{S'}(Q')$ (our third move) to get our second Apollonian circle.

Remark. Let $A' = BC \cap YZ$ be constructed similarly to B' and C'. Note that the triangles ΔABC and ΔXYZ are perspective from the Gergonne point. By Desargues' theorem, they are therefore perspective from a line, which is the line $A'B'C'$, known as the *Gergonne line* of ΔABC; see Oldknow [10], who seems to have been just shy of discovering the construction presented here.

Closing remarks

Of the constructions in the literature, we highlight two.

Eppstein The previously simplest solution to our problem seems to be that of Eppstein [2, 3, 5], which uses eleven elementary moves to draw O_S. His construction finds

the tangency point Q by first dropping the perpendicular to AC through B, and then connecting a second line from Y to one of the two points of intersection of this perpendicular with O_B. This second line intersects O_B at Q (or Q', depending on the choice of intersection point). Note that constructing a perpendicular line is not an elementary operation, costing 3 moves. The second line *is* elementary, so Eppstein can construct Q in 4 moves, then R in 4 more, then two more lines BQ and CR to get the center S, and finally the circle O_S in a total of 11 moves. To construct the other solution, $O_{S'}$, using his method, it would cost another five moves (as opposed to our three), since one needs to draw two more lines to produce Q' and R' (whereas our construction gives these as a byproduct).

Gergonne Gergonne's solution to the *general* Apollonian problem (i.e., when the given circles are not necessarily tangent) is perhaps closest to ours, but of course the problem he is solving is more complicated. He begins by constructing the radical circle O_I for the initial circles O_A, O_B, and O_C, and identifies the six points X, X', Y, Y', Z, and Z', where it intersects the three original circles. Those points are taken in order around O_I, with Y' and Z on O_A, Z' and X on O_B, and X' and Y on O_C. In our configuration, the radical circle is the incircle of triangle ABC and the six points are $X = X'$, $Y = Y'$, and $Z = Z'$.

Every pair of circles can be thought of as being similar to each other via a dilation through a point. In general, there are two such dilations. This gives us six points of similarity, which lie on four lines, the four *lines of similitude*. In Gergonne's construction, each line generates a pair of tangent circles. In our configuration, the point B' is the center of the dilation that sends O_A to O_C. Since O_A and O_C are tangent, there is only one dilation, so we get only one line of similitude, the Gergonne line.

The radical circle of O_B, O_I, and a pair of tangent circles is centered on the line of similitude, so is where XZ' intersects that line. In our configuration, that gives us B'. The radical circle is the one that intersects O_I perpendicularly, so in our configuration it goes through Y.

Efficiency or complexity Measures of efficiency or complexity come up in many branches of mathematics. Some, like height in number theory, are simple to define and quantify. At the other end of the spectrum, the *elegance* of proofs is a difficult notion to quantify, but one we nevertheless recognize and appreciate. Erdös would often refer to what he called *The Book*, a book in which God keeps the most elegant proofs. The invocation of an all-knowing is an acknowledgement that we can never know for sure (i.e., prove) whether a particular proof belongs in that book. With the measures of Hartshorne and Lemoine, we quantify elegance in constructions, and having done so, we now have the tools to prove that a construction is best possible or most elegant. This though appears to be a very difficult question to tackle for even modest constructions. Hartshorne refers to "par" scores and "doable in" scores, but shies away from calling anything best possible.

DeTemple, using Lemoine's measure, analyzes constructions of regular p-gons for $p = 5$, 17, and 257, and also muses about the complexity of showing a construction is best possible [1]. In earlier literature, there is a paper by Güntshe, who gives and analyzes (using Lemoine's measure) constructions for the regular 17-gon [6].

We leave the reader with a challenge: construct a (generic) configuration of four mutually tangent circles in the plane using fewer than 15 ($= 1 + 2 + 5 + 7$) moves. Or prove (as we suspect) that this is impossible!

Acknowledgments The authors are grateful to Jeff Lagarias and the referees for numerous helpful comments, and to a referee for the Güntsche reference [6].

REFERENCES

[1] DeTemple, D. W. (1991). Carlyle circles and the Lemoine simplicity of polygon constructions. *Amer. Math. Monthly*. 98(2): 97–108. doi.org/10.2307/2323939

[2] Eppstein, D. (2001). Tangencies: Apollonian circles. ics.uci.edu/%7Eeppstein/junkyard/tangencies/apollonian.html

[3] Eppstein, D. (2001). Tangent spheres and triangle centers. *Amer. Math. Monthly*. 108(1): 63–66. doi.org/10.2307/2695679

[4] Eves, H. (1966). *A Survey of Geometry*, Vol. 1. Boston, MA: Allyn and Bacon, Inc.

[5] Gisch, D., Ribando, J. M. (2004). Apollonius' problem: A study of solutions and their connections. *Amer. J. Undergrad. Math*. 3(1): 15–26.

[6] Güntsche, R. (1903). Geometrographische Siebzehnteilung des Kreises. *Sitzungsber. Berl. Math. Ges*. 2: 10–15.

[7] Hartshorne, R. (2000). *Geometry: Euclid and Beyond*. Undergraduate Texts in Mathematics. New York: Springer-Verlag. doi.org/10.1007/978-0-387-22676-7

[8] Heath, T. (1981). *A History of Greek Mathematics*. New York: Dover Publications, Inc. From Thales to Euclid, Corrected reprint of the 1921 original.

[9] Kontorovich, A. (2013). From Apollonius to Zaremba: Local-global phenomena in thin orbits. *Bull. Amer. Math. Soc*. 50(2): 187–228. doi.org/10.1090/S0273-0979-2013-01402-2

[10] Oldknow, A. (1996). The Euler-Gergonne-Soddy triangle of a triangle. *Amer. Math. Monthly*. 103(4): 319–329. doi.org/10.2307/2975188

Summary. In this short note we present, by what we surmise is the most efficient method, a straight-edge and compass construction of four mutually tangent circles in a plane.

ARTHUR BARAGAR (MR Author ID 336817) has a Ph.D. from Brown University and a B.Sc. from the University of Alberta, and held postdoctoral positions at The University of Texas at Austin and the University of Waterloo before settling down in Las Vegas. His interests are in number theory and arithmetic geometry, with a particular interest in rational points, curves and automorphisms on K3 surfaces. These are related to Apollonian-like circle, sphere, and hypersphere packings, which is an interest he shares with his coauthor.

ALEX KONTOROVICH (MR Author ID 704943) is a Professor of Mathematics at Rutgers. He is a Fellow of the American Math Society and a Kavli Fellow of the National Academy of Sciences. Kontorovich serves on the Scientific Board of Quanta Magazine and as Dean of Academic Content at the National Museum of Mathematics. He is the recipient of a Sloan, Simons, and von Neumann Fellowships, and the AMS's Conant Prize.

Proving the Extended Binomial Theorem Using Ordinary Differential Equations

SYED ABBAS
School of Basic Sciences
Indian Institute of Technology Mandi,
H.P. 175005, India
abbas@iitmandi.ac.in

We present a novel proof of the binomial and extended binomial theorems by solving a first order linear ordinary differential equation with a given initial condition. The method is easy to follow, and the techniques used can be found in any standard book of ordinary differential equations, such as Coddington's [1]. Several authors have proved the binomial theorem using various techniques, but previous proofs using differential equations do not allow the generalization presented here. They either fail or are not applicable to the generalized binomial theorem; for example, the probabilistic approach of Rosalsky [6], the approaches from calculus by Huang [3] and Fulton [2], and the approach using the Laplace transform due to Kataria [4]. The technique proposed in this paper is applicable to both the binomial and extended binomial theorems.

In more recent work, Kataria [5] has also produced a proof method using an ordinary differential equation to obtain the binomial theorem. His ordinary differential equation works very well for the binomial theorem, but it cannot be used to obtain the extended binomial theorem. We give a different ordinary differential equation, which establishes the binomial theorem as well as the extended binomial theorem. We will focus on the proof of the extended theorem.

Theorem 1 (Extended binomial theorem)**.** *For any real number r and any two reals x, y, the following holds:*

$$(x+y)^r = \sum_{m=0}^{\infty} \binom{r}{m} x^m y^{r-m},$$

where

$$\binom{r}{m} = \frac{r(r-1)\cdots(r-m+1)}{m!}.$$

This is the "extended" binomial theorem because the exponent r is allowed to be any real number. It is not restricted to being a nonnegative integer, as it is in the regular binomial theorem.

Proof. The above series converges when $|x| < |y|$. For $x = 0$, the identity is obvious. If $x \neq 0$, then $y > 0$. Let us fix $t = x/y$. It is enough to establish

$$(1+t)^r = \sum_{m=0}^{\infty} \binom{r}{m} t^m.$$

Let

$$f_1(t) = (1+t)^r \quad \text{and} \quad f_2(t) = \sum_{m=0}^{\infty} \binom{r}{m} t^m.$$

Math. Mag. **93** (2020) 33–35. doi:10.1080/0025570X.2020.1682451
MSC: 05A10, 34A99

Differentiating f_1 with respect to t, gives us

$$f_1'(t) = r(1+t)^{r-1}.$$

Multiplying $f_1'(t)$ by $1+t$ yields

$$(1+t)f_1'(t) = rf_1(t),$$

which implies that f_1 is a solution to the ordinary differential equation

$$(1+t)z' = rz,$$

with initial condition $z(0) = 1$. Let us now compute $(1+t)f_2'(t)$. We obtain

$$f_2'(t) = \sum_{m=1}^{\infty} \binom{r}{m} m t^{m-1} = r \sum_{m=1}^{\infty} \binom{r-1}{m-1} t^{m-1}.$$

Multiplying by $(1+t)$ now yields

$$\begin{aligned}
r(1+t)\sum_{m=1}^{\infty} \binom{r-1}{m-1} t^{m-1} &= r\sum_{m=1}^{\infty} \binom{r-1}{m-1} t^m + r\sum_{m=1}^{\infty} \binom{r-1}{m-1} t^{m-1} \\
&= r\sum_{m=1}^{\infty} \binom{r-1}{m-1} t^m + r\sum_{m=0}^{\infty} \binom{r-1}{m} t^m \\
&= r\sum_{m=1}^{\infty} \left[\binom{r-1}{m-1} + \binom{r-1}{m} \right] t^m + r \\
&= r\sum_{m=1}^{\infty} \binom{r}{m} t^m + r = r\sum_{m=0}^{\infty} \binom{r}{m} t^m \\
&= rf_2(t).
\end{aligned}$$

We can easily check that $f_2(0) = 1$. Hence, by using the uniqueness solutions to linear ordinary differential equations with a given initial condition, we obtain $f_1(t) = f_2(t)$. ■

This method can be adapted to obtain the regular binomial theorem:

Theorem 2 (Binomial theorem)**.** *For any nonnegative integer n and two reals x, y, the following holds*

$$(x+y)^n = \sum_{m=0}^{n} \frac{n!}{m!(n-m)!} x^m y^{n-m}.$$

We can easily check that

$$\begin{aligned}
\frac{(n-1)!}{(m-1)!(n-m)!} + \frac{(n-1)!}{(m)!(n-m-1)!} &= \frac{(n-1)!}{(m-1)!(n-m-1)!}\left[\frac{1}{n-m} + \frac{1}{m}\right] \\
&= \frac{(n-1)!}{(m-1)!(n-m-1)!}\frac{n}{m(n-m)} \\
&= \frac{n!}{m!(n-m)!}.
\end{aligned}$$

Similar steps will work by replacing n by any real number r. Also $0^0 = 1$ and for $m = 0$ the negative factorial are zero.

Remark. The convergence of the series $\sum_{m=0}^{\infty} \binom{r}{m} t^m$ is guaranteed for $|t| < 1$ using the ratio test.

Using the similar analysis as above, one can easily obtain the binomial theorem from the same differential equation.

Acknowledgments I would like to thank the editor and anonymous reviewers for their constructive comments and suggestions.

REFERENCES

[1] Coddington, E. A., Levinson, N. (1955). *Theory of Ordinary Differential Equations*. New York: McGraw-Hill.
[2] Fulton, C. M. (1952). A simple proof of the binomial theorem. *Amer. Math. Monthly*. 59(4): 243–244. doi.org/10.1080/00029890.1952.11988114
[3] Huang, L. C. (2009). A simple proof of the binomial theorem using differential calculus. *Amer. Statist.* 63(1): 43–44. doi.org/10.1198/tast.2009.0009
[4] Kataria, K. K. (2016). An alternate proof of the binomial theorem. *Amer. Math. Monthly*. 123(9): 940.
[5] Kataria, K. K. (2017). The binomial theorem procured from the solution of an ODE. *Math. Mag*. 90(5): 375–377.
[6] Rosalsky, A. (2007). A simple and probabilistic proof of the binomial theorem. *Amer. Statist.* 61(2): 161–162. doi.org/10.1198/000313007X188397

Summary. We produce an alternate proof of the extended binomial theorem by solving a first order linear ordinary differential equation with a given initial condition. The method is easy to follow and the technique used can be found in any standard book of ordinary differential equations. The proof method presented here is applicable to both the binomial and extended binomial theorems.

DR. SYED ABBAS (MR Author ID: 824190) is an associate professor in the School of Basic Sciences at the Indian Institute of Technology, Mandi, India. He received his M.Sc. and Ph.D. in mathematics from the Indian Institute of Technology, Kanpur, India in the years 2004 and 2009, respectively. He has worked as a postdoctoral fellow at the University of Bologna, Italy, as a visiting scientist at Technische Universität, Dresden, Germany and as a research associate at the University of Fribourg, Switzerland. His research interests are: nonlinear analysis, abstract differential equations, mathematical modeling, neutral networks, stochastic control, and discrete systems.

The Case for Raabe's Test

CHRISTOPHER N. B. HAMMOND
Connecticut College
New London, CT 06320
cnham@conncoll.edu

Although Raabe's test was first introduced in 1832, its importance and interpretation have largely been overlooked. The purpose of this article is to expand the scope of Raabe's test, illustrating its benefits and situating it within its proper context.

As most readers are probably aware, the ratio test and the root test can both be viewed as an implicit comparison with a geometric series; that is, they tell us when a series "behaves like" a certain geometric series. Likewise, the version of Raabe's test that we are presenting will indicate when a series "behaves like" $\sum_{n=1}^{\infty} 1/n^p$, for a particular p. In a sense, one can view Raabe's test as a type of comparison test that self-selects the appropriate p-series with which to compare.

It is not always obvious when a series is comparable to a p-series. For example, consider

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}(2n)!}{4^n (n!)^2}. \tag{1}$$

The standard convergence tests are not especially helpful in this instance. The ratio test and the root test are both inconclusive. The comparison and limit comparison tests, besides applying only to series with non-negative terms, require a predetermined series with which to compare. It is not even clear whether the hypotheses of the alternating series test are satisfied. Our version of Raabe's test, however, will show that this series essentially behaves like

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^{1/2}}.$$

Hence, with only a single computation, we will demonstrate that series (1) is conditionally convergent. (See Example 4.) In other words, Raabe's test will allow us to perform a comparison without knowing beforehand to what we are comparing. Moreover, the test will sometimes eliminate the need for employing a multistep process to determine conditional convergence.

Raabe's test

The original version of Raabe's test, as stated by Joseph Ludwig Raabe [**6**], says that a series $\sum_{n=1}^{\infty} a_n$ consisting of positive terms converges whenever

$$\lim_{n\to\infty} n\left(\frac{a_n}{a_{n+1}} - 1\right) > 1$$

and diverges whenever

$$\lim_{n\to\infty} n\left(\frac{a_n}{a_{n+1}} - 1\right) < 1.$$

Math. Mag. **93** (2020) 36–46. doi:10.1080/0025570X.2019.1684150
MSC: Primary 40A05

There are several minor variants of Raabe's result (see Bromwich [1, p. 39], Knopp [3, p. 285], or Prus-Wiśniowski [5]), but the test is typically stated for series with only positive terms. Raabe's test can provide more information if we consider series that include both positive and negative terms, as illustrated by this slightly subtler version of the test:

Theorem 1 (Raabe's test)**.** *Suppose* $\sum_{n=1}^{\infty} a_n$ *is a series consisting of nonzero terms, for which*

$$p = \lim_{n\to\infty} n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right)$$

exists (as a finite value). If $p > 1$*, the series converges absolutely. If* $p < 0$*, the series diverges. If* $0 \le p < 1$*, the series is either conditionally convergent or divergent. If* $p = 1$*, the test provides no information.*

Proof. Suppose, first, that $p > 1$. Since $(p-1)/2$ is a positive number, there is a natural number N such that

$$\left|n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) - p\right| < \frac{p-1}{2},$$

and hence

$$n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) > p - \frac{p-1}{2} = \frac{p+1}{2},$$

whenever $n \ge N$. Let $p_1 = (p+1)/2$, which is also greater than 1. Observe that

$$n\left|\frac{a_n}{a_{n+1}}\right| > p_1 + n$$

and thus

$$n|a_n| > (p_1 + n)|a_{n+1}|$$

for $n \ge N$, from which we see that

$$n|a_n| - (n+1)|a_{n+1}| > (p_1 - 1)|a_{n+1}|. \tag{2}$$

Since $p_1 - 1$ is positive, it follows that

$$n|a_n| > (n+1)|a_{n+1}|$$

for $n \ge N$. Since every term $n|a_n|$ is positive, the monotone convergence theorem guarantees that the sequence $\big(n|a_n|\big)$ converges to some limit x. Consider the series

$$\sum_{n=1}^{\infty} b_n = \sum_{n=1}^{\infty}\big(n|a_n| - (n+1)|a_{n+1}|\big).$$

The mth partial sum of $\sum_{n=1}^{\infty} b_n$ is equal to

$$\begin{aligned}\big(|a_1| - 2|a_2|\big) + \big(|2a_2| - 3|a_3|\big) + \cdots + \big(m|a_m| - (m+1)|a_m|\big)\\ = |a_1| - (m+1)|a_{m+1}|,\end{aligned}$$

so the series converges to $|a_1| - x$. Therefore the comparison test, along with (2), shows that

$$\sum_{n=1}^{\infty}(p_1 - 1)|a_{n+1}|$$

is convergent, as is

$$\sum_{n=1}^{\infty}|a_{n+1}| = \frac{1}{p_1 - 1}\sum_{n=1}^{\infty}(p_1 - 1)|a_{n+1}|.$$

Consequently, the series $\sum_{n=1}^{\infty} a_n$ converges absolutely.

Now suppose that $p < 0$. Since $-p$ is a positive number, there is a natural number N such that

$$\left| n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) - p \right| < -p,$$

and hence

$$n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) < p - p = 0,$$

whenever $n \geq N$. Consequently

$$\left|\frac{a_n}{a_{n+1}}\right| - 1 < 0$$

for $n \geq N$, implying that $|a_n| < |a_{n+1}|$ whenever $n \geq N$. Therefore, the sequence (a_n) does not converge to 0, so the series $\sum_{n=1}^{\infty} a_n$ is divergent.

Finally, suppose that $0 \leq p < 1$. Since $(1 - p)/2$ is a positive number, there is a natural number N such that

$$\left| n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) - p \right| < \frac{1 - p}{2},$$

and hence

$$n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) < p + \frac{1 - p}{2} = \frac{1 + p}{2},$$

whenever $n \geq N$. Therefore

$$n\left|\frac{a_n}{a_{n+1}}\right| - (n + 1) < \frac{1 + p}{2} - 1 = \frac{p - 1}{2} < 0$$

for $n \geq N$. Consequently

$$n|a_n| < (n + 1)|a_{n+1}|$$

for $n \geq N$, implying that

$$N|a_N| \leq n|a_n|$$

whenever $n \geq N$. Taking $M = N|a_N|$, we see that $M/n \leq |a_n|$ whenever $n \geq N$. Thus, the comparison test shows that $\sum_{n=1}^{\infty}|a_n|$ is divergent, so $\sum_{n=1}^{\infty} a_n$ is either conditionally convergent or divergent.

Example 8, which appears in the next section, will demonstrate that any outcome is possible when $p = 1$. Namely, such a series may diverge, may converge conditionally, or may converge absolutely. ■

Observe that the quantity

$$p = \lim_{n\to\infty} n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right)$$

from Raabe's test cannot exist unless

$$\lim_{n\to\infty}\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) = 0.$$

Therefore, $\lim_{n\to\infty} |a_{n+1}/a_n|$ must exist and be equal to 1. In other words, Raabe's test presupposes the inconclusiveness of the ratio test. By Theorem 3.37 in Rudin [7], the existence of a finite value of p also guarantees that the root test is inconclusive.

As mentioned above, Raabe's test yields no information when $p = 1$. For any value $0 \le p < 1$, there are examples for which the series converges conditionally and examples for which the series diverges. (See Example 8.) In general, it can be difficult to determine the behavior of a series when $0 \le p \le 1$, although the next two results are rather helpful.

Proposition 2. *Suppose* (a_n) *is a sequence consisting of nonzero numbers, for which*

$$p = \lim_{n\to\infty} n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right)$$

exists. If $p > 0$*, the sequence* (a_n) *converges to* 0.

Proof. Since $p/2$ is a positive number, there is a natural number N such that

$$\left|n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) - p\right| < \frac{p}{2},$$

and hence

$$n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) > p - \frac{p}{2} = \frac{p}{2} > 0, \tag{3}$$

whenever $n \ge N$. Consequently

$$\left|\frac{a_n}{a_{n+1}}\right| - 1 > 0$$

for $n \ge N$, so $|a_n| > |a_{n+1}|$ whenever $n \ge N$. The monotone convergence theorem guarantees that $(|a_n|)$ converges to a non-negative number x. We simply need to show that x is equal to 0.

Suppose, for the sake of contradiction, that $x > 0$. Since $|a_n| > x$ for $n \ge N$, it follows from (3) that

$$\frac{n(|a_n| - |a_{n+1}|)}{x} > n\left(\frac{|a_n| - |a_{n+1}|}{|a_{n+1}|}\right) = n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) > \frac{p}{2}$$

when $n \geq N$. Therefore $|a_n| - |a_{n+1}| > px/2n$, and hence

$$|a_m| - |a_n| = (|a_m| - |a_{m+1}|) + (|a_{m+1}| - |a_{m+2}|) + \cdots + (|a_{n-1}| - |a_n|)$$
$$> \frac{px}{2}\left(\frac{1}{m} + \frac{1}{m+1} + \cdots + \frac{1}{n-1}\right),$$

whenever $n > m \geq N$. While $(|a_n|)$ is a Cauchy sequence, the sequence of partial sums for the harmonic series is divergent. Thus, we have obtained a contradiction, so we conclude that x must be 0. ■

In certain instances, such as series (1), it is reasonable to use Proposition 2 to show that (a_n) converges to 0. (See also Problem 2047 in [2].) The main purpose of this proposition, though, is to expand the scope of Raabe's test.

Theorem 3 (Raabe's alternating series test)**.** *Suppose (a_n) is a sequence consisting of positive numbers, for which*

$$p = \lim_{n\to\infty} n\left(\frac{a_n}{a_{n+1}} - 1\right)$$

exists. If $0 < p \leq 1$, the series

$$\sum_{n=1}^{\infty}(-1)^{n-1}a_n = a_1 - a_2 + a_3 - a_4 + \cdots$$

is convergent. If $0 < p < 1$, the series converges conditionally.

Proof. In addition to showing that (a_n) converges to 0, the proof of Proposition 2 shows that there is a natural number N such that $a_n > a_{n+1}$ for $n \geq N$. Hence, the alternating series test guarantees that the series stated above is convergent. If $0 < p < 1$, Raabe's test shows that the series must, in fact, be conditionally convergent. ■

Theorem 3 is somewhat unusual, in that it typically takes multiple steps to show that a series is conditionally convergent.

Example 4. Consider the series

$$\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(2n-1)!}{4^n(n!)^2}, \quad \sum_{n=1}^{\infty}\frac{(-1)^{n-1}(2n)!}{4^n(n!)^2}, \quad \text{and} \quad \sum_{n=1}^{\infty}\frac{(-1)^{n-1}(2n+1)!}{4^n(n!)^2},$$

the second of which was mentioned at the beginning of this article. It is not difficult to demonstrate that these series have values $3/2$, $1/2$, and $-1/2$ with respect to Raabe's test. Therefore the first series converges absolutely, the second series converges conditionally, and the third series diverges.

Interpretation and examples

Our next observation is fundamental to our interpretation of Raabe's test.

Example 5. Let $a_n = 1/n^p$ for a real number p. Observe that

$$n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) = n\left(\left(\frac{n+1}{n}\right)^p - 1\right) = \frac{\left(1 + \frac{1}{n}\right)^p - 1}{1/n},$$

which converges to $f'(1)$ for $f(x) = x^p$. Consequently the expression above converges to p.

As we have previously mentioned, Raabe's test should be viewed as an implicit comparison between $\sum_{n=1}^{\infty} |a_n|$ and the corresponding series $\sum_{n=1}^{\infty} 1/n^p$. In other words, if $\sum_{n=1}^{\infty} a_n$ has value p with respect to Raabe's test, then the series behaves as if $|a_n| = 1/n^p$. The only exceptions are the borderline cases where $p = 0$ and $p = 1$. Note that the proof of Raabe's test did not require any prior knowledge about p-series, except for the fact that the harmonic series diverges.

Viewing Raabe's test from this perspective, one would anticipate certain behavior with respect to products and powers. If

$$\sum_{n=1}^{\infty} |a_n| \quad \text{and} \quad \sum_{n=1}^{\infty} |b_n|$$

behave like

$$\sum_{n=1}^{\infty} 1/n^p \quad \text{and} \quad \sum_{n=1}^{\infty} 1/n^q$$

respectively, then $\sum_{n=1}^{\infty} |a_n b_n|$ should behave like $\sum_{n=1}^{\infty} 1/n^{p+q}$, and $\sum_{n=1}^{\infty} |a_n|^k$ should behave like $\sum_{n=1}^{\infty} 1/n^{kp}$. The following proposition formalizes this intuition.

Proposition 6. *Suppose (a_n) and (b_n) are sequences consisting of nonzero numbers, for which*

$$p = \lim_{n\to\infty} n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right)$$

and

$$q = \lim_{n\to\infty} n\left(\left|\frac{b_n}{b_{n+1}}\right| - 1\right)$$

both exist. In that case,

$$\lim_{n\to\infty} n\left(\left|\frac{a_n b_n}{a_{n+1} b_{n+1}}\right| - 1\right)$$

exists and is equal to $p + q$. Furthermore, for any real number k, the expression

$$\lim_{n\to\infty} n\left(\left|\frac{a_n}{a_{n+1}}\right|^k - 1\right)$$

exists and is equal to kp.

Proof. First of all, note that

$$\begin{aligned} n\left(\left|\frac{a_n b_n}{a_{n+1} b_{n+1}}\right| - 1\right) &= n\left(\frac{|a_n b_{n+1}|}{|a_{n+1} b_{n+1}|} + \frac{|a_n b_n| - |a_n b_{n+1}|}{|a_{n+1} b_{n+1}|} - 1\right) \\ &= n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1 + \left|\frac{a_n}{a_{n+1}}\right|\left(\frac{|b_n| - |b_{n+1}|}{|b_{n+1}|}\right)\right) \\ &= n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) + \left|\frac{a_n}{a_{n+1}}\right| n\left(\left|\frac{b_n}{b_{n+1}}\right| - 1\right). \end{aligned}$$

Since

$$\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right| = 1,$$

our first assertion follows from the algebraic limit theorem.

To prove the second assertion, consider the continuous function

$$g(x) = \begin{cases} \dfrac{x^k - 1}{x - 1}, & x \neq 1 \\ k, & x = 1 \end{cases}.$$

Observe that

$$n\left(\left|\frac{a_n}{a_{n+1}}\right|^k - 1\right) = n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) g\left(\left|\frac{a_n}{a_{n+1}}\right|\right)$$

for all n. Since $|a_n/a_{n+1}|$ is converging to 1, the expression above converges to the product of p and k. ■

In other words, if $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ have values p and q with respect to Raabe's test, then $\sum_{n=1}^{\infty} a_n b_n$ has value $p + q$. Likewise, whenever it is defined, $\sum_{n=1}^{\infty} a_n^k$ has value kp. In particular, $\sum_{n=1}^{\infty} 1/a_n$ has value $-p$ and $\sum_{n=1}^{\infty} a_n/b_n$ has value $p - q$. Besides confirming our interpretation of Raabe's test, these observations can be quite useful from a computational perspective

As noted by Knopp [**3**, p. 287], there is an equivalent formulation of Raabe's test:

$$p = \lim_{n\to\infty} n \log\left|\frac{a_n}{a_{n+1}}\right|, \tag{4}$$

where log denotes the natural logarithm. (The equivalence of (4) to the standard form of Raabe's test can be deduced from the inequalities $(x - 1)/x \leq \log x \leq x - 1$.) This version, which is sometimes called *Schlömilch's test* [**4**], makes the results of Proposition 6 seem a bit more apparent.

Moving on, if $p > 0$, then Proposition 2 shows that (a_n) must converge to 0. Hence, it follows from Proposition 6 that (a_n) is unbounded whenever $p < 0$. Let us pause for a moment to consider the case where $p = 0$.

From the perspective of Raabe's test, such a series "looks like" the p-series

$$\sum_{n=1}^{\infty} \frac{1}{n^0} = 1 + 1 + 1 + \cdots.$$

Nevertheless, there are examples with $p = 0$ for which (a_n) is either convergent to 0 or unbounded.

Example 7. Taking $a_n = 1/\log(n + 1)$, we see that

$$\begin{aligned} n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) &= n\left(\frac{\log(n+2)}{\log(n+1)} - 1\right) \\ &= \frac{n\big(\log(n+2) - \log(n+1)\big)}{\log(n+1)} \\ &= \frac{\log\big(\big(1 + \frac{1}{n+1}\big)^n\big)}{\log(n+1)}. \end{aligned} \tag{5}$$

Since the numerator of (5) converges to $\log e = 1$, the entire expression converges to 0. Proposition 6 shows that

$$\lim_{n\to\infty} n\left(\left|\frac{b_n}{b_{n+1}}\right| - 1\right)$$

is also 0, where $b_n = \log(n+1)$.

In other words, there is some "wiggle room" with respect to how closely a series must resemble the corresponding series $\sum_{n=1}^{\infty} 1/n^p$. We are now in a position to justify the final assertion in the statement of Raabe's test, as well as a remark made shortly before the statement of Proposition 2.

Example 8. We would like to illustrate the range of possible outcomes when $0 \le p \le 1$. First of all, consider the case where $p = 0$. The alternating series test shows that

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{\log(n+1)}$$

is conditionally convergent. On the other hand, the series

$$\sum_{n=1}^{\infty} \frac{1}{n^0} = 1 + 1 + 1 + \cdots$$

is divergent.

For $0 < p \le 1$, the series

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^p}$$

is conditionally convergent and has value p with respect to Raabe's test. Similarly, the series

$$\sum_{n=1}^{\infty} \frac{1}{n^p}$$

is divergent.

We still need to identify a series with $p = 1$ that is absolutely convergent. It follows from Proposition 6 that

$$\sum_{n=1}^{\infty} \frac{1}{(n+1)\big(\log(n+1)\big)^2}$$

has value 1 with respect to Raabe's test. Moreover, the integral test shows that this series converges absolutely.

The next result is particularly useful when applying Raabe's test to concrete examples.

Proposition 9. *Suppose* (a_n) *and* (b_n) *are sequences consisting of positive numbers, for which*

$$p = \lim_{n\to\infty} n\left(\frac{a_n}{a_{n+1}} - 1\right)$$

and

$$q = \lim_{n\to\infty} n\left(\frac{b_n}{b_{n+1}} - 1\right)$$

both exist. If $p < q$*, then*

$$\lim_{n\to\infty} n\left(\frac{a_n + b_n}{a_{n+1} + b_{n+1}} - 1\right) \tag{6}$$

and

$$\lim_{n\to\infty} n\left(\left|\frac{a_n - b_n}{a_{n+1} - b_{n+1}}\right| - 1\right) \tag{7}$$

both exist and are equal to p*.*

Proof. Note that

$$n\left(\frac{a_n + b_n}{a_{n+1} + b_{n+1}} - 1\right) = n\left(\frac{a_n - a_{n+1}}{a_{n+1} + b_{n+1}} + \frac{b_n - b_{n+1}}{a_{n+1} + b_{n+1}}\right)$$

$$= n\left(\frac{a_n}{a_{n+1}} - 1\right)\left(\frac{1}{1 + \dfrac{b_{n+1}}{a_{n+1}}}\right) + n\left(\frac{b_n}{b_{n+1}} - 1\right)\left(\frac{\dfrac{b_{n+1}}{a_{n+1}}}{1 + \dfrac{b_{n+1}}{a_{n+1}}}\right).$$

The sequence (b_n/a_n) has value $q - p > 0$ with respect to Raabe's test, so Proposition 2 dictates that (b_n/a_n) converges to 0. Thus, the expression above converges to $p \cdot 1 + q \cdot 0 = p$.

Since (b_n/a_n) converges to 0, there is a natural number N such that $b_n < a_n$ for $n \geq N$. Consequently, $|a_n - b_n| = a_n - b_n$ for $n \geq N$, and hence

$$n\left(\left|\frac{a_n - b_n}{a_{n+1} - b_{n+1}}\right| - 1\right) = n\left(\frac{a_n - a_{n+1}}{a_{n+1} - b_{n+1}} - \frac{b_n - b_{n+1}}{a_{n+1} - b_{n+1}}\right)$$

$$= n\left(\frac{a_n}{a_{n+1}} - 1\right)\left(\frac{1}{1 - \dfrac{b_{n+1}}{a_{n+1}}}\right) - n\left(\frac{b_n}{b_{n+1}} - 1\right)\left(\frac{\dfrac{b_{n+1}}{a_{n+1}}}{1 - \dfrac{b_{n+1}}{a_{n+1}}}\right).$$

Therefore, this expression also converges to p. ∎

The result above is not valid when $p = q$, since

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

The analogous result may fail to hold for sequences consisting of nonzero terms, even when

$$\lim_{n\to\infty} n\left(\left|\frac{a_n}{a_{n+1}}\right| - 1\right) = p < q = \lim_{n\to\infty} n\left(\left|\frac{b_n}{b_{n+1}}\right| - 1\right).$$

If $a_n = 1$ and $b_n = (-1)^{n-1}/n$, for example, then both (6) and (7) are undefined.

For any non-negative integer m, Example 5 shows that the monomial n^m has value $-m$ with respect to Raabe's test. Hence, Proposition 9 allows us to compute the value for any series whose terms can be expressed as a polynomial in n.

Example 10. Consider the series

$$\sum_{n=1}^{\infty} 6n^4 - 11n^3 - 3n^2 + 7n + 5 = \sum_{n=1}^{\infty} \left(6n^4 + 7n + 5\right) - \left(11n^3 + 3n^2\right).$$

Proposition 9 shows that $\sum_{n=1}^{\infty} 6n^4 + 7n + 5$ and $\sum_{n=1}^{\infty} 11n^3 + 3n^2$ have values -4 and -3 with respect to Raabe's test. Thus, their difference, which is the original series, has value -4.

The reasoning from this example leads us to the following observation.

Corollary 11. *Let $\sum_{n=1}^{\infty} a_n$ be a series consisting of nonzero terms. If $a_n = h(n)$ for a polynomial h of degree m, the series has value $-m$ with respect to Raabe's test.*

Combining the results of this section, we can often apply Raabe's test without much additional computation.

Example 12. Consider the series

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} (-1)^{n-1} \sqrt{\frac{n^2 - 2n + 3}{5n^3 - 7n^2 + 11n + 13}}.$$

Corollary 11 shows that the numerator of the expression inside the radical has value -2 with respect to Raabe's test and that the denominator has value -3. Thus, Proposition 6 shows that their quotient has value 1 with respect to Raabe's test and that $\sum_{n=1}^{\infty} a_n$ has value $1/2$. Therefore, the series converges conditionally.

We could obtain the same result by applying the limit comparison test and the alternating series test, comparing $\sum_{n=1}^{\infty} |a_n|$ with $\sum_{n=1}^{\infty} 1/n^{1/2}$. The informal process by which we obtain the series $\sum_{n=1}^{\infty} 1/n^{1/2}$ requires essentially the same steps as actually employing Raabe's test. Moreover, Theorem 3 makes it unnecessary to verify the hypotheses of the alternating series test.

Pedagogical implications

When first learning about series, students typically encounter two fundamental classes of examples: geometric series and p-series. By analogy, it makes sense to introduce students to the ratio test and the root test (which relate to geometric series) and also to Raabe's test (which relates to p-series). The most obvious way to feature Raabe's test in a calculus or an analysis course would be as a supplement to the limit comparison test. There are several reasons that such an innovation might be advantageous:

- We generally use the limit comparison test when the ratio test and the root test are inconclusive, which is precisely the situation in which Raabe's test may be applicable.
- When applying the limit comparison test, we often compare the series in which we are interested with a p-series. Raabe's test serves a similar function, but does not require that we know the value of p beforehand. (As noted in Example 12, the process for finding a series with which to compare may involve essentially the same steps as applying Raabe's test.)
- In certain cases, Raabe's test allows us immediately to draw conclusions about conditional convergence.

In the context of p-series, the most conspicuous instance in which the limit comparison test can yield more information than Raabe's test is when $p = 1$. That case is inconclusive with respect to Raabe's test, but a comparison with the harmonic series may demonstrate divergence. We might consider using the limit comparison test in a more targeted manner, reserving it primarily for this situation, and applying Raabe's test otherwise.

Acknowledgments The author is indebted to Warren P. Johnson for many helpful discussions during the preparation of this article. The author would also like to thank Edward Omey for his thoughtful correspondence and the anonymous reviewers for their suggestions regarding the organization and structure of the article.

REFERENCES

[1] Bromwich, T. J. I'A. (1926). *An Introduction to the Theory of Infinite Series*, 2nd ed. London: MacMillan.
[2] Dueñez, E., Ionaşcu, E. J., eds. (2018). Problems and solutions. *Math. Mag.* 91(3): 230–238.
[3] Knopp, K. (1951). *Theory and Application of Infinite Series*, 2nd ed. London: Blackie and Son.
[4] Prus-Wiśniowski, F. (2009). Comparison of Raabe's and Schlömilch's tests. *Tatra Mt. Math. Publ.* 42(1): 119–130. doi.org/10.2478/v10127-009-0012-y
[5] Prus-Wiśniowski, F. (2008). A refinement of Raabe's test. *Amer. Math. Monthly*. 115(3): 249–252. doi.org/10.1080/00029890.2008.11920522
[6] Raabe, J. L. (1832). Untersuchungen über die Convergenz und Divergenz der Reihen. *Z. Phys. Math*. 10: 41–74.
[7] Rudin, W. (1976). *Principles of Mathematical Analysis*, 3rd ed. New York: McGraw-Hill.

Summary. Among the techniques for determining the convergence of a series, Raabe's test remains relatively unfamiliar to most mathematicians. We present several results relating to Raabe's test that do not seem to be widely known, making the case that Raabe's test should be featured more prominently in undergraduate calculus and analysis courses. In particular, we demonstrate that Raabe's test may be viewed as an implicit comparison with a p-series, in the same manner that the ratio test and the root test constitute an implicit comparison with a geometric series. Moreover, Raabe's test can sometimes simplify the process for determining conditional convergence.

CHRISTOPHER N. B. HAMMOND (MR Author ID: 728945) grew up in Durham, North Carolina, where he attended the North Carolina School of Science and Mathematics. He received his bachelor's degree from the University of the South, Sewanee, Tennessee. He first heard about Raabe's test while he was a graduate student at the University of Virginia, Charlottesville, although it took him almost 20 years to appreciate its significance. He currently lives in New London, Connecticut, where he teaches at Connecticut College.

Inequalities Applied to Kinematic Quantities

STEPHEN KACZKOWSKI
South Carolina Governor's School
Hartsville, SC 29550
kaczkowski@gssm.k12.sc.us

Many standard undergraduate textbooks in physics, differential equations, or mechanics contain problems in which kinematic quantities such as velocity, speed, or acceleration are expressed as functions of position. A classic example is the simple harmonic oscillator in which the velocity of the oscillating mass can be expressed in terms of its distance from equilibrium. Normally, however, when kinematics is first introduced, the relevant quantities in the *initial* problems are presented in terms of time, and then distance dependent problems are covered later on. There are some good reasons for this presentation order. One reason is that, for many, the distance dependent approach can be counterintuitive and confusing. Even the most brilliant minds may initially miss some of the subtleties associated with speed variations that are expressed as functions of distance. The following problem, quoted from the Einstein–Wertheimer correspondence [**3**], provides an illustration along these lines:

> An old clattery auto is to drive a stretch of 2 miles, up and down a hill. Because it is so old, it cannot drive the first mile—the ascent—faster than with an average speed of 15 miles per hour. Question: How fast does it have to drive the second mile—on going down, it can, of course, go faster—in order to obtain an average speed (for the whole distance) of 30 miles an hour?

For some, a hasty first reading may inspire an initial guess of 45 or perhaps 60 mph. But upon closer examination, it is seen that an average speed as high as 30 mph is not possible. In the correspondence it is reported that even Einstein was fooled by this deceptively simple problem. It was not until calculating that he noticed that there was no time left for the way down [**3**]. A challenging aspect of this problem may be that an answer of 45 mph on the second mile does indeed yield an average speed of 30 mph if the "average" is calculated with respect to distance rather than with respect to time. But in fact, a 45 mph speed on the second mile yields a 22.5 mph average speed—i.e., a time-averaged speed—for the whole trip. For this problem, the spatial average is greater than the temporal one, and this invites some interesting questions. How do these spatial and temporal averages of velocity compare in general? Does the spatial average always exceed the temporal as in the above problem? If so, how can this be proved? Do analogous inequalities hold for other quantities such as acceleration, powers of velocity, or kinetic energy? These are the types of questions that we will address.

To gain better insight into these averages, let's calculate the average velocity of a stone that falls from the top of a tall building of height h. The velocity of the stone, expressed as a function of time, is $v(t) = gt$, where g is the acceleration due to gravity. The stone strikes the ground and ends its flight in $T = \sqrt{2h/g}$ seconds, so the average velocity with respect to time ($\overline{v}$) is

$$\overline{v} = \frac{1}{T}\int_0^T gt\, dt = \sqrt{\frac{gh}{2}}.$$

Math. Mag. **93** (2020) 47–53. doi:10.1080/0025570X.2020.1682744
MSC: 26A06, 70B05, 70B10

The distance y from the ground that the stone has fallen in t seconds is $y = gt^2/2$, and hence the velocity, expressed as a function of y, is $v(y) = \sqrt{2gy}$. The average velocity with respect to distance (denoted by $\hat{v}$) is then greater than $\overline{v}$ by a third:

$$\hat{v} = \frac{1}{h}\int_0^h \sqrt{2gy}\, dy = \frac{4}{3}\sqrt{\frac{gh}{2}}.$$

A mass executing simple harmonic motion with amplitude A, angular frequency ω, and period T provides another example. Consider only a half period of unidirectional motion such as

$$x(t) = A\cos(\omega t) \quad \text{for} \quad T/2 \le t \le T.$$

Then, since $v(x) = \omega\sqrt{A^2 - x^2}$, we have that

$$\hat{v} = (\pi/4)\,\omega A > (2/\pi)\,\omega A = \overline{v}.$$

In these two examples, one with constant acceleration and the other with variable acceleration, we see that $\hat{v}$ exceeds $\overline{v}$.

Averaging velocity

It turns out that for unidirectional one-dimensional motion, the average velocity with respect to time is less than or equal to the average velocity with respect to distance. That is

$$\overline{v} = \frac{1}{(b-a)}\int_a^b v\, dt \le \frac{1}{(x_1 - x_0)}\int_{x_0}^{x_1} v\, dx = \hat{v}, \tag{1}$$

where x_0 and x_1 are the distances reached at times a and b, respectively.

Inequality (1) can be understood intuitively because at higher speeds, greater distances are covered, and these speeds have more weight in $\hat{v}$ than in $\overline{v}$. (Throughout, it will be assumed that $v(t) \ge 0$ and $\int_a^b v\, dt > 0$, so that the terms "velocity" and "speed" may be interchanged.)

G. H. Hardy, J. E. Littlewood, and G. Polya's classic text on inequalities [2] notes that (1) can be proved with the Cauchy–Schwartz (C-S) inequality. This particular proof will be presented at the end of this section. Additionally, (1) can also be proved with the inequality involving the root mean square (RMS), arithmetic mean (AM), and harmonic mean (HM) where these quantities stand in the following relation: RMS $\ge$ AM $\ge$ HM. For positive continuous functions, this inequality can be expressed as

$$\left(\frac{1}{x_1 - x_0}\int_{x_0}^{x_1} [f(x)]^2\, dx\right)^{1/2} \ge \frac{1}{x_1 - x_0}\int_{x_0}^{x_1} f(x)\, dx \ge \left[\frac{1}{x_1 - x_0}\int_{x_0}^{x_1} 1/f(x)\, dx\right]^{-1},$$

where equality holds only when the function is constant along the whole interval [2].

To proceed with a proof of (1), observe that the arithmetic mean of the velocity with respect to distance is $\hat{v}$. Next, the harmonic mean of the velocity with respect to distance is

$$\left[\frac{1}{(x_1 - x_0)}\int_{x_0}^{x_1} \frac{1}{v(x)}\, dx\right]^{-1}.$$

Since the integral in this expression is the elapsed time for the motion, this harmonic mean is numerically equal to $\overline{v}$. Therefore (1) follows from

$$\hat{v} = \text{AM} \geq \text{HM} = \overline{v},$$

where equality holds for constant velocity.

For another proof, consider a root mean square velocity v_{rms} with respect to time as defined by

$$v_{\text{rms}} = \sqrt{\frac{1}{b-a}\int_a^b v^2\, dt}.$$

Since RMS $\geq$ AM, we have $v_{\text{rms}} \geq \overline{v}$. Now, in (1) the integral appearing in the definition of $\hat{v}$ can be changed from space to time using $dx = v\, dt$. Then

$$\overline{v}\hat{v} = \frac{1}{b-a}\int_a^b v^2\, dt = v_{\text{rms}}^2,$$

and therefore $v_{\text{rms}} = \sqrt{\hat{v}\overline{v}}$, the geometric mean of $\overline{v}$ and $\hat{v}$. Thus v_{rms} is between these quantities, and putting the results together we arrive at $\overline{v} \leq v_{\text{rms}} \leq \hat{v}$.

Inequality (1) can be generalized to motion along curves in space in the following way: consider a particle whose path in space is parameterized with respect to time by a vector valued function $\boldsymbol{r}(t)$ for $a \leq t \leq b$. Let $\boldsymbol{v}(t) = \boldsymbol{r}'(t)$ be the particle's velocity. Then the spaced-averaged speed can be described in terms of the arc-length s in the form

$$s(t) = \int_a^t |\boldsymbol{v}(\alpha)|\, d\alpha.$$

Specifically, since $ds = |\boldsymbol{v}(t)|\, dt$, a change of variables yields

$$\hat{v} = \frac{1}{s(b)}\int_0^{s(b)} |\boldsymbol{v}|\, ds = \int_a^b |\boldsymbol{v}|^2 dt \Big/ \int_a^b |\boldsymbol{v}|\, dt.$$

Now

$$\overline{v} = \int_a^b |\boldsymbol{v}|\, dt \Big/ \int_a^b 1\, dt,$$

and by the C-S inequality

$$\left(\int_a^b |\boldsymbol{v}|\ dt\right)^2 \leq \left(\int_a^b |\boldsymbol{v}|^2\, dt\right)\left(\int_a^b 1^2\, dt\right),$$

which upon rearranging yields $\overline{v} \leq \hat{v}$. Then, in a manner analogous to the work done previously, we have

$$v_{\text{rms}}^2 = \frac{1}{b-a}\int_a^b |\boldsymbol{v}|^2\, dt = v\hat{v}.$$

Therefore, the inequality $\overline{v} \leq v_{\text{rms}} \leq \hat{v}$ can also be established for motion along curves in space.

With these definitions and proofs in mind, let's return to the old clattery car problem. If we let v_1 denote the speed on the first mile (which was specified as 15 mph) and

v_2 the speed on the second, then $\hat{v} = (v_1 + v_2)/2$ while $\overline{v} = 2v_1v_2/(v_1 + v_2)$. Therefore, the difference $\hat{v} - \overline{v} = (v_1 - v_2)^2/(2v_1 + 2v_2)$ is clearly non-negative and hence $\overline{v} \leq \hat{v}$. The interested reader may want to prove (1) for the case involving a car traveling at various speeds through n distinct distance segments—rather than just two segments of equal length. (Hint: The discrete version of the C-S inequality may be useful here.)

Further generalizations

Suppose that instead of just comparing different types of average velocities, we extended our investigations to include other quantities such as acceleration, kinetic energy, or force. Averages of these quantities have real physical meaning in problems involving the calculation of work and impulse. One way to obtain interesting generalizations involving these and other quantities is through Chebyshev's sum inequality. The continuous version of this inequality, which is not as well-known as the discrete version, will be used in this section, and it can be expressed in the following form: let f and g be monotonically increasing continuous functions on $[a, b]$, and let ϕ be a non-negative continuous function. Then

$$\int_a^b f(t)g(t)\phi(t)\,dt \int_a^b \phi(t)\,dt \geq \int_a^b f(t)\phi(t)\,dt \int_a^b g(t)\phi(t)\,dt. \qquad (2)$$

Inequality (2) also holds if f and g are both monotonically decreasing, and the inequality is reversed if f and g are monotonic in the opposite direction (i.e., if one function is increasing and the other is decreasing). Pairs of functions that are monotonic in the same direction will be referred to as "synchronous," and function pairs monotonic in the opposite direction will be denoted by the term "asynchronous." The function $\phi(t)$ in (2) serves the role of a weighting function. Inequality (2) can be derived by expanding the following double integral:

$$R = \frac{1}{2}\int_a^b \int_a^b (f(x) - f(y))(g(x) - g(y))\phi(x)\phi(y)\,dy\,dx.$$

Before doing so, first note that the integrand is non-negative if f and g are synchronous, and for this case R is non-negative. Now, upon doubling and expanding we obtain

$$\begin{aligned} 2R = &\int_a^b f(x)g(x)\phi(x)\,dx \int_a^b \phi(y)\,dy \\ &+ \int_a^b f(y)g(y)\phi(y)\,dy \int_a^b \phi(x)\,dx \\ &- \int_a^b f(x)\phi(x)\,dx \int_a^b g(y)\phi(y)\,dy \\ &- \int_a^b f(y)\phi(y)\,dy \int_a^b g(x)\phi(x)\,dx. \end{aligned}$$

In this expression, the roles of x and y can be interchanged, and because both variables can be replaced with t, the above can be rewritten as

$$\int_a^b f(t)g(t)\phi(t)\,dt \int_a^b \phi(t)\,dt = \int_a^b f(t)\phi(t)\,dt \int_a^b g(t)\phi(t)\,dt + R.$$

Then, (2) follows immediately because R is non-negative. Since R is non-positive when f and g are asynchronous, an analogous argument shows why the inequality in (2) is reversed in the asynchronous case.

To apply (2) to the task of comparing averages, let $\phi(t) = 1$, and divide both sides of the inequality by $\left(\int_a^b 1dt\right)^2$ to obtain

$$\frac{\int_a^b f(t)g(t)\ dt}{\int_a^b 1\ dt} \geq \left(\frac{\int_a^b f(t)\ dt}{\int_a^b 1\ dt}\right)\left(\frac{\int_a^b g(t)\ dt}{\int_a^b 1\ dt}\right).$$

This inequality can be written compactly as $\langle fg\rangle_t \geq \langle f\rangle_t\langle g\rangle_t$, where the notation $\langle\cdot\rangle_t$ denotes a temporal average. Similarly, assigning $\phi(t)$ to a velocity function $v(t)$ and dividing by $\left(\int_a^b vdt\right)^2$ in (2) yields

$$\frac{\int_a^b f(t)g(t)\,v(t)\,dt}{\int_a^b v(t)\,dt} \geq \left(\frac{\int_a^b f(t)\,v(t)\,dt}{\int_a^b v(t)\,dt}\right)\left(\frac{\int_a^b g(t)\,v(t)\,dt}{\int_a^b v(t)\,dt}\right).$$

By changing the integration variable to position s and using $ds = v\ dt$, these quantities can be identified more readily as averages with respect to distance. In terms of the notation $\langle\cdot\rangle_s$ for spatial averages, this inequality becomes $\langle f\cdot g\rangle_s \geq \langle f\rangle_s\langle g\rangle_s$. Since we are interested in comparing spatial and temporal averages, these inequalities, interesting and helpful as they are, do not yet generalize our previous work with average velocity.

To build on these results and those of the previous sections, first let $f(t) = (v(t))^n$ for $n > 0$, and let $g(t) = v(t)$. These assignments ensure f and g are synchronous, and substitution into inequality (2), along with $\phi(t) = 1$, yields

$$\int_a^b v^n(t)v(t)\ dt \int_a^b 1\ dt \geq \int_a^b v^n(t)\ dt \int_a^b v(t)\ dt.$$

Then upon dividing by $\left(\int_a^b vdt\right)\left(\int_a^b 1dt\right)$ we obtain the following generalization of (1):

$$\langle v^n\rangle_s \geq \langle v^n\rangle_t.$$

That is, the spatial average of any positive power of velocity equals or exceeds the corresponding temporal average. The $n = 1$ case leads us back to (1), and the $n = 2$ case is of some practical interest because this expression shows that for an object in motion in the classical domain, the spatial average of kinetic energy equals or exceeds its temporal average.

Next, by setting $f(t) = F(v(t))$, where F is a monotonically increasing function, we can generalize (1) a little bit further by using (2) again with $\phi(t) = 1$ and $g(t) = v(t)$ to obtain

$$\langle F(v)\rangle_s \geq \langle F(v)\rangle_t.$$

(If F is monotonically decreasing, then the above inequality is reversed.) The above discussion was motivated in part by the work of Stein [**4**], who proved an inequality similar to (2) using techniques from measure theory. In fact, Brualdi [**1**] described Stein's work as a rediscovery of the Chebyshev sum inequality.

Our final generalization of (2) can be obtained by considering line integrals over curves in three-space. Consider a particle following a path C parameterized by the

vector valued function $\boldsymbol{r}(t) = \langle x(t), y(t), z(t) \rangle$ for $a \le t \le b$. Let $M(x, y, z)$ be a continuous scalar field defined throughout the space containing C. If we let

$$f(t) = M(x(t), y(t), z(t)) \quad \text{and} \quad g(t) = |\boldsymbol{v}(t)|,$$

and if these functions are synchronous, then Chebyshev's sum inequality (2) with unit weight becomes

$$\int_C M(x, y, z)\, ds \int_a^b 1\, dt \ge \int_a^b M(x(t), y(t), z(t))\, dt \int_a^b |\boldsymbol{v}(t)|\, dt. \tag{3}$$

A convenient form of (3) can be obtained by dividing the expression by

$$\left(\int_a^b 1\, dt\right)\left(\int_a^b |\boldsymbol{v}(t)|\, dt\right)$$

to yield $\langle M \rangle_s \ge \langle M \rangle_t$, under the appropriate synchronicity conditions. Now M can be assigned to any number of important kinematic quantities such as the tangential and normal components of the acceleration (a_T and a_N) or the magnitude of the acceleration $|\boldsymbol{a}(t)|$. Inequality (3) can also be applied to scalar dynamic quantities such as the tangential or normal components of a force.

In this context of motion along a curve, the line integral in (3) may remind readers of the role that conservative forces (or conservative vector fields) play in the fundamental theorem of line integrals. Line integrals are a convenient mathematical tool that are useful in describing important concepts from physics, such as the law of conservation of energy and the work-energy theorem. An important definition that is foundational to these topics is the work W done by a force $\boldsymbol{F}$ on an object as it moves along a path. In terms of line integrals, this can be expressed by

$$W = \int_C \boldsymbol{F} \cdot d\boldsymbol{r} = \int_C \boldsymbol{F} \cdot \boldsymbol{T}\, ds,$$

where $\boldsymbol{T}$ is the unit tangent vector. If in (3) we let $M = \boldsymbol{F} \cdot \boldsymbol{T}$, then the tangential component of the force, and if $|\boldsymbol{v}(t)|$ and $\boldsymbol{F} \cdot \boldsymbol{T}$ are synchronous, then $\langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_s \ge \langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_t$, or equivalently

$$\frac{\int_C \boldsymbol{F} \cdot \boldsymbol{T}\, ds}{\int_C 1\, ds} = \frac{\int_C \boldsymbol{F} \cdot d\boldsymbol{r}}{\int_a^b |\boldsymbol{v}(t)|\, dt} \ge \frac{\int_C \boldsymbol{F} \cdot \boldsymbol{T}\, dt}{\int_a^b 1\, dt}. \tag{4}$$

In terms of the work W done by the force, inequality (4) can be written as

$$W \ge \overline{v} \int_C \boldsymbol{F} \cdot \boldsymbol{T}\, dt. \tag{5}$$

Under what specific circumstances is $\langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_s \ge \langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_t$, and when is $\langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_s \le \langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_t$? To answer these questions, first recall that a_T is the time derivative of $|\boldsymbol{v}(t)|$. Thus, if a_T is positive and monotonically increasing on $[a, b]$, then the speed $|\boldsymbol{v}(t)|$ is increasing and convex on that interval. Therefore, a_T and $|\boldsymbol{v}(t)|$ are synchronous (and since $\boldsymbol{F} \cdot \boldsymbol{T} = ma_T$, so are $\boldsymbol{F} \cdot \boldsymbol{T}$ and $|\boldsymbol{v}(t)|$). For this case, inequality (3) yields $\langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_s \ge \langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_t$. This same inequality also holds over intervals where a_T is negative and monotonically decreasing because this type of acceleration will produce a decreasing $|\boldsymbol{v}(t)|$. The reversed inequality, $\langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_s \le \langle \boldsymbol{F} \cdot \boldsymbol{T} \rangle_t$, applies to the other situations (i.e., when a_T is positive and decreasing, or when a_T is negative and increasing), as these would result in $\boldsymbol{F} \cdot \boldsymbol{T}$ and $|\boldsymbol{v}(t)|$ being asynchronous.

For those very familiar with undergraduate-level physics, inequality (5) can be easily verified for a simple case of one-dimensional motion over a finite time interval $[a, b]$. Suppose an object is moving in a straight line in one direction, and its velocity is increasing because a monotonically increasing force $F(t)$ is causing its acceleration. Since both F and v are monotonically increasing, the $\geq$ direction of the inequality in (5) applies here. Also, for this case (5) is equivalent to $W \geq J\overline{v}$, where $J = \int_a^b F\, dt$ is the impulse. The impulse can also be calculated using $J = \Delta p$, the change in momentum. By the work-energy theorem, $W = \Delta KE$, the change in kinetic energy over the time interval. Then, with these definitions in mind, the inequality $W \geq J\overline{v}$ can be simplified as follows: express the ΔKE in the form $m(v(b) - v(a))(v(b) + v(a))/2$, and divide both sides by the (positive) change in momentum $m(v(b) - v(a))$ to obtain $(v(b) + v(a))/2 \geq \overline{v}$. Therefore, by assuming (5) we are led to this last inequality. However, we know this inequality is true because the object is accelerating and the resulting velocity function $v(t)$ is convex.

Acknowledgments The author would like to thank all the reviewers for carefully reading over the various versions of this paper and for their many helpful suggestions.

REFERENCES

[1] Brualdi, R. A. (1977). Comments and complements. *Amer. Math. Monthly*. 84(10): 803–807. doi.org/10.2307/2322063

[2] Hardy, G. H., Littlewood, J. E., Pólya, G. (1952). *Inequalities*. Cambridge: Cambridge University Press, p. 163.

[3] Luchins, A. S., Luchins, E. H. (1990). The Einstein–Wertheimer correspondence on geometric proofs and mathematical puzzles. *Math. Intell*. 12(1): 35–43. doi.org/10.1007/bf03024003

[4] Stein, S. K. (1976). An inequality in two monotonic functions. *Amer. Math. Monthly*. 83(6): 469–471. doi.org/10.2307/2318342

Summary. It is known that velocity averaged over time is less than or equal to velocity averaged over distance. This inequality is illustrated with some routine applied mathematics problems involving simple harmonic motion and free fall motion. Generalizations to motion along space curves are explored, and inequalities involving spatial and temporal averages of other kinematic/dynamic quantities are derived from Chebyshev's sum inequality. These quantities include kinetic energy, tangential and normal components of acceleration, work, and impulse.

STEPHEN KACZKOWSKI (MR 1184119) received his Ph.D. in mathematics from the Rensselaer Polytechnic Institute, Troy, NY. He is currently an instructor at the South Carolina Governor's School for Science and Mathematics, where he enjoys teaching and researching a variety of topics in both pure and applied mathematics. His interests beyond mathematics include playing the piano, hiking, reading, and traveling with his wife.

Boolean Function Analogs of Covering Systems

ANTHONY ZALESKI
Rutgers University
New Brunswick, NJ 08901
anthony.zaleski@rutgers.edu

DORON ZEILBERGER
Rutgers University
New Brunswick, NJ 08901
doronzeil@gmail.com

Abstraction is a great tool for mathematicians. Often, a problem that at first seems intimidating is suddenly endowed with an elegant solution, once it is embedded in a more general space. Like misdirection in a magic trick, certain specifics can blind one to the bigger picture; they are conceptual red herrings.

For example, the French mathematical columnist Jean-Paul Delahaye [**4**] recently posed the following brain-teaser, adapting a beautiful puzzle, of unknown origin, popularized by Peter Winkler [**9**, pp. 35–43].

Here is a free translation from the French:

Enigma: nine beetles and prime numbers

One places nine beetles on a circular track in such a way that the nine arc distances, measured in meters, between two consecutive beetles are the first nine prime numbers, 2, 3, 5, 7, 11, 13, 17, 19, and 23. The order is arbitrary, and each number appears exactly once as a distance.

At starting time, each beetle decides *randomly* whether she would go, traveling at a speed of 1 meter per minute, clockwise or counter-clockwise. When two beetles bump into each other, they immediately do a "U-turn," i.e., reverse direction. We assume that the size of the beetles is negligible. At the end of 50 minutes, after many collisions, one notices the distances between the new positions of the beetles. The nine distances are exactly as before, the first nine prime numbers! How to explain this miracle?

Before going on to the next section, we invite you to solve this puzzle all by yourself.

Solution of the enigma Note that the length of the circular track is

$$2 + 3 + 5 + 7 + 11 + 13 + 17 + 19 + 23 = 100$$

meters.

Let each beetle carry a flag, and whenever two beetles bump into each other, let them exchange flags. Since the flags always move in the same direction, and also move at a speed of 1 meter per minute, after 50 minutes, each flag is *exactly* at the antipode of its original location; hence, the distances are the same! Of course, this works if the original distances were *any* sequence of numbers: All that they have to obey is that their sum equals 100, or more generally, that half the sum of the distances divides the product of the speed (1 meter per minute in this puzzle) and the elapsed time (50 minutes in this puzzle).

Math. Mag. **93** (2020) 54–61. doi:10.1080/0025570X.2019.1684797
MSC: 03B35, 05A99

This variation, due to Delahaye, is *much* harder than the original version posed by Winkler [9], where also the initial distances were arbitrary. In Delahaye's rendition, the solver is bluffed into trying to use the fact that the distances are primes; this was the red herring. Something analogous happened to Paul Erdős, concerning *covering systems*.

Covering systems

In 1950, Paul Erdős introduced the notion of *covering systems* [5]. A covering system is a finite set of arithmetical progressions

$$\{a_i \pmod{m_i} \quad | \quad 1 \le i \le N\},$$

whose union is the set of all non-negative integers. For example

$$\{0 \pmod 1\},$$

is such a (not very interesting) covering system, while

$$\{0 \pmod 2\ ,\ 1 \pmod 2\},$$

and

$$\{0 \pmod 5,\ 1 \pmod 5,\ 2 \pmod 5,\ 3 \pmod 5,\ 4 \pmod 5\},$$

are other, almost as boring, examples. A slightly more interesting example is

$$\{0 \pmod 2,\ 1 \pmod 4,\ 3 \pmod 4\}.$$

A covering system is *exact* if all the congruences are disjoint (like in the above boring examples). It is *distinct* if all the moduli are different. (From now on, let $a\ (b)$ mean $a \pmod b$.)

Erdős [6] gave the smallest possible example of a distinct covering system:

$$\{0\,(2),\ 0\,(3),\ 1\,(4),\ 5\,(6),\ 7\,(12)\}.$$

Of course, the above covering system is not exact since, for example, 0 (2) and 0 (3) both contain any multiple of 6. A theorem proved by Mirsky and (Donald) Newman, and independently by Davenport and Rado (described by Erdős [6]) implies that a covering system cannot be both exact *and* distinct. Even a stronger statement holds. Assuming that our system $\{a_i(m_i)\}_{i=1}^{N}$ is written in non-decreasing order of the moduli $m_1 \le m_2 \le \cdots \le m_N$, the Mirsky–Newman–Davenport–Rado theorem asserts that $m_{N-1} = m_N$. In other words, the two top moduli are equal (and hence an exact covering system can never be distinct). See Zeilberger [10] for an exposition of their snappy proof. While their proof was nice, it was not as nice as the combinatorial-geometrical proof that was found by Berger, Felzenbaum, and Fraenkel [1, 2], and exposited by Zeilberger [10]. In fact, they proved the more general Znam theorem that asserts that the highest modulus shows up at least p times, where p is the smallest prime dividing $\mathrm{lcm}\,(m_1, \ldots, m_N)$ [10]. Jamie Simpson [8] independently found a similar proof.

The Berger–Felzenbaum–Fraenkel revolution: from number theory to discrete geometry via the Chinese remainder theorem While it is true that the set of positive integers is an infinite set, a covering system is a finite object. In order to verify

that a proposed covering system $\{a_i(m_i)\}_{i=1}^N$ is indeed one, it suffices to check that it covers all the integers n between 0 and $M-1$, where

$$M = \operatorname{lcm}(m_1, m_2, \ldots, m_N).$$

By the fundamental theorem of arithmetic

$$M = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

where $p_1, \ldots, p_k$ are primes and $r_1, \ldots, r_k$ are positive integers.

For the sake of simplicity, let's assume that M is square-free, i.e., all the exponents $r_1, \ldots, r_k$ equal 1. The same reasoning, only slightly more complicated, applies in the general case. Now we have $M = p_1 p_2 \cdots p_k$.

The ancient, but still useful, Chinese remainder theorem tells you that there is a bijection between the set of integers between 0 and $M-1$, which we shall denote $[0, M-1]$, and the Cartesian product of $[0, p_i - 1]$, $i = 1, \ldots, k$,

$$f : [0, M-1] \to \prod_{i=1}^{k} [0, p_i - 1],$$

defined by

$$f(x) := [x \pmod{p_1}, x \pmod{p_2}, \ldots, x \pmod{p_k}].$$

So each integer in $[0, M-1]$ is represented by a point in the $p_1 \times p_2 \times \cdots \times p_k$ k-dimensional discrete box $\prod_{i=1}^{k} [0, p_i - 1]$.

If $a(m)$ is a member of our covering system, then since m is a divisor of M, it can be written as a product of some of the primes in $\{p_1, \ldots, p_k\}$, say

$$m = p_{i_1} p_{i_2} \cdots p_{i_s}.$$

Let

$$m_{i_1} = a \pmod{p_{i_1}}, \quad m_{i_2} = a \pmod{p_{i_2}}, \quad \ldots, \quad m_{i_s} = a \pmod{p_{i_s}}.$$

It follows that the members of the congruence $a(m)$ correspond to the points in the $(k-s)$-dimensional *sub-box*

$$\{(x_1, \ldots, x_k) \in [0, p_1 - 1] \times \cdots \times [0, p_k - 1] \mid x_{i_1} = m_{i_1}, \ldots, x_{i_s} = m_{i_s}\}.$$

For example, if $M = 30 = 2 \cdot 3 \cdot 5$, the congruence class 7(10), corresponds to the one-dimensional sub-box (since $7 \pmod 2 = 1$ and $7 \pmod 5 = 2$)

$$\{(x_1, x_2, x_3) : x_1 = 1, 0 \le x_2 \le 2, x_3 = 2\}.$$

In other words, a covering system (with square-free M) is nothing but a way of expressing a certain k-dimensional discrete box as a union of sub-boxes. This was the beautiful insight of Marc Berger, Alex Felzenbaum, and Aviezri Fraenkel.

Erdős's famous problem and Bob Hough's refutation Erdős [6] famously asked whether there exists a distinct covering system

$$a_i \pmod{m}_i, \quad 1 \le i \le N, \quad m_1 < m_2 < \cdots < m_N,$$

with the smallest modulus, m_1, arbitrarily large.

As computers got bigger and faster, people (and their computers) came up with examples that progressively made m_1 larger and larger, and many humans thought that indeed m_1 can be made as large as one wishes. This was brilliantly refuted by Bob Hough [7] who proved that $m_1 \leq 10^{16}$. This is definitely not sharp, and the true largest m_1 is probably less than 1000.

Let's now move on from number theory to something apparently very different: logic!

Boolean functions

Let's recall some basic definitions. A *Boolean function* (named after George Boole [3]) of n variables is a function from $\{\text{false}, \text{true}\}^n$ to $\{\text{false}, \text{true}\}$. Altogether there are 2^{2^n} Boolean functions of n variables. Any Boolean function $f(x_1, \ldots, x_n)$, is determined by its *truth table*, or equivalently, by the set $f^{-1}(\text{true})$, one of the 2^{2^n} subsets of $\{\text{false}, \text{true}\}^n$.

The *simplest* Boolean functions are the *constant* functions **true** (the *tautology*) corresponding to the whole of $\{\text{false}, \text{true}\}^n$, and **false** (the *anti-tautology*) corresponding to the *empty set*.

In addition to the above constant Boolean functions, there are three *atomic* functions. The simplest is the *unary* function NOT, denoted by $\bar{x}$, that is defined by

$$\bar{x} = \begin{cases} \text{false}, & \text{if} \quad x = \text{true} \\ \text{true}, & \text{if} \quad x = \text{false}. \end{cases}$$

The two other fundamental Boolean functions are the (inclusive) OR, denoted by $\vee$, and AND, denoted by $\wedge$. The expression $x \vee y$ is true unless both x and y are false, and $x \wedge y$ is true only when both x and y are true.

By iterating these three operations on n variables, one can get many *Boolean expressions*, and each Boolean function has many possible expressions.

From now on we will denote, as usual, true by 1 and false by 0. Also let $x^1 = x$ and $x^0 = \bar{x} = 1 - x$.

One particularly simple type of expression is a (pure) *conjunction*. It is anything of the form (for some t, called its *size*),

$$x_{i_1}^{j_1} \wedge \cdots \wedge x_{i_t}^{j_t},$$

where $1 \leq i_1 < \cdots < i_t \leq n$ and $j_i \in \{0, 1\}$ for all $1 \leq i \leq t$.

Of interest to us is the type of expression called the *disjunctive normal form* (DNF). A DNF has the form

$$\bigvee_{i=1}^{N} C_i,$$

where each C_i is a pure conjunction.

Every Boolean expression corresponds to a unique function, but every function can be expressed in many ways, and even in many ways that are DNF. The most straightforward way is the *canonical DNF* form

$$\bigvee_{\{v \in f^{-1}(1)\}} \bigwedge_{i=1}^{n} x_i^{v_i}.$$

Note that a pure conjunction of length t

$$x_{i_1}^{j_1} \wedge \cdots \wedge x_{i_t}^{j_t}$$

corresponds to a *sub-cube* of dimension $n - t$, namely to

$$\{(x_1, \ldots, x_n) \mid x_{i_1} = j_1, \ldots, x_{i_t} = j_t\}.$$

Hence, one can view a DNF as a (usually not exact) *covering* of the set $f^{-1}(1)$ of truth-vectors by sub-cubes. In particular, a *DNF tautology* is a covering of the whole n-dimensional unit cube by lower-dimensional sub-cubes.

DNFs and the million dollar problem The most fundamental problem in theoretical computer science, the question of whether **P** is *not* **NP** (of course it is not, but proving it rigorously is another matter), is equivalent to the question of whether there exists a polynomial time algorithm that decides if a given disjunctive normal form expression is the *tautology* (i.e., the constant function 1). Of course, there is an obvious brute force algorithm: For each term, find the truth-vectors covered by it, take the union, and see whether it contains all the 2^n members of $\{0, 1\}^n$. But this takes *exponential* time and memory.

The covering system analog We can formulate a similar problem based on covering systems. Input a system of congruences

$$a_i \pmod{m_i} \quad 1 \leq i \leq N,$$

and decide, in *polynomial time*, whether it is a covering system. Initially it seems that we need to check infinitely many cases, but of course (as already noted above), it suffices to check whether every integer between 1 and $\operatorname{lcm}(m_1, \ldots, m_N)$ belongs to at least one of the congruences. This seems fast enough! Alas, the size of the input is the sum of the number of digits of the a_i's and m_i's. This is less than a constant times the *logarithm* of $\operatorname{lcm}(m_1, \ldots, m_N)$, so just like for Boolean functions, the naive algorithm requires time (and space) exponential in the *input size*.

Boolean function analogs of covering systems

We next consider Boolean function analogs of covering systems. The first one to consider such analogs was Melkamu Zeleke [11]. Here we continue his pioneering work. We saw that a DNF tautology is nothing but a covering of the n-dimensional unit cube $\{0, 1\}^n$ by sub-cubes. So it is the analog of a covering system.

The analog of *exact* covering systems is obvious: all the terms should cover disjoint sub-cubes. For example, when $n = 2$, (from now on xy means $x \wedge y$)

$$x_1x_2 \vee x_1\bar{x_2} \vee \bar{x_1}x_2 \vee \bar{x_1}\bar{x_2},$$

and

$$x_1 \vee \bar{x_1}x_2 \vee \bar{x_1}\bar{x_2},$$

are such.

In order to define *distinct* DNF, we define the *support* of a conjunction as the set of the variables that participate. For example, the support of the term $\bar{x_1}\bar{x_3}x_4x_6$ is the set $\{x_1, x_3, x_4, x_6\}$. In other words, we ignore the negations. For each t-subset

of $\{x_1, \ldots, x_n\}$, there are 2^t conjunctions with that support. Geometrically speaking, two terms with the same support correspond to sub-cubes which are "parallel" to each other.

Note that the supports correspond to the modulus, m, and the assignments of negations (or no negation) corresponds to a residue class modulo m.

A DNF tautology is *distinct* if it has distinct supports.

An obvious example of a distinct DNF tautology in n variables is

$$\bigvee_{i=1}^{n} x_i \ \vee \ \wedge_{i=1}^{n} \bar{x}_i.$$

More generally, for every $1 \leq t \leq n$, $(t \neq n/2)$ the following is a distinct DNF tautology:

$$\left(\bigvee_{1 \leq i_1 < i_2 < \cdots < i_t \leq n} x_{i_1} \cdots x_{i_t} \right) \vee \left(\bigvee_{1 \leq j_1 < j_2 < \cdots < j_{n-t} \leq n} \bar{x}_{j_1} \cdots \bar{x}_{j_{n-t}} \right).$$

This follows from the fact that by the pigeon-hole principle, every $0-1$ vector of length n has either at least t 1's or at least n-t 0's.

The Boolean analog of the Mirsky–Newman–Davenport–Rado theorem is almost trivial. First, suppose we have an exact DNF tautology where the largest support has size n. That corresponds to a point (a 0-dimensional sub-cube). If it is the only one, then since a conjunction of length t covers 2^{n-t} points, if all the other ones are strictly smaller than n, and since they are all disjoint, they cover an even number of points, hence there is no way that an exact DNF tautology would only have one term of size n.

If the largest size of a term is $<n$, then by projecting on appropriate sub-boxes one can reduce it to the former case, and see that it must have a mate.

The Boolean analog of the Erdős problem is true Taking n to be odd, the above DNF tautology with $t = (n-1)/2$ has "minimal moduli" (supports) of size $(n-1)/2$, and that can be made as large as one wishes.

First challenge This leads to a more challenging problem: For each specific n, how large can the minimum clause size, let's call it k, be in a distinct DNF tautology?

A simple *necessary condition*, on density grounds, is that

$$\sum_{i=k}^{n} \binom{n}{i} \frac{1}{2^i} \geq 1.$$

(Each subset of size i of $\{1, \ldots, n\}$ can only show up once and covers 2^{n-i} vertices of the n-dimensional unit cube. Now use Boole's inequality that says that the number of elements of a union of sets is less than or equal to the sum of their cardinalities.)

Let A_n be the largest such k. The first 14 values of A_n are

$$1, 1, 1, 2, 3, 4, 4, 5, 6, 7, 7, 8, 9, 10.$$

We were able to find such optimal distinct DNF tautologies for all $n \leq 14$ except for $n = 10$, where the best that we came up with was one that covers 1008 out of the 1024 vertices of the 10-dimensional unit cube, leaving 16 points uncovered, and for $n = 14$, where 276 out of the $2^{14} = 16{,}384$ points were left uncovered. See `out1.txt` in the supplementary materials.

Second challenge Another challenge is to come up with distinct DNF tautologies with all the terms of the *same* size. By density arguments, a necessary condition for the existence of such a distinct DNF tautology is

$$\binom{n}{m}\frac{1}{2^m} \geq 1.$$

Let B_m be the largest such m. The first 14 values are

$$0, 0, 1, 2, 3, 3, 4, 5, 6, 6, 7, 8, 9, 9.$$

For $n = 3$, where $B_3 = 1$, it is not possible, since $x_1 \vee x_2 \vee x_3$ can't cover everything. We were also unable to find such optimal DNF tautologies for $n = 5$, where $B_5 = 3$ and we had to leave one vertex uncovered, $n = 9$, (with $B_9 = 6$), where 13 vertices were left uncovered, and $n = 13$ (with $B_{13} = 9$) where $2^{13} - 8090 = 102$ vertices were left uncovered. For the other cases with $n \leq 14$, we met the challenge. See `out2.txt` in the supplementary materials.

Many more examples can be gotten from the Maple package `dt.txt` in the supplementary materials.

The general problem: covering a discrete box by non-parallel sub-boxes Let $\{a_i\}_{i=1}^{\infty}$ be a weakly increasing sequence of positive integers, with $a_1 \geq 2$.

Is it true that for every m there exists an n such that the box $[1, a_1] \times \cdots \times [1, a_n]$ can be covered by *non-parallel* sub-boxes, each of dimension $\leq n - m$?

We saw that for the Boolean case, with $a_i = 2$ for each i (and analogously, for each constant sequence), the answer is trivially *yes*.

On the other hand, if

$$\sum_{i=1}^{\infty}\frac{1}{a_i} < \infty,$$

the answer is *no*, since

$$\prod_{i=1}^{\infty}\left(1+\frac{1}{a_i}\right) < \infty,$$

and by a density argument, all tails of the product will eventually be less than 1, so there is not enough room.

Regarding the original Erdős problem, Hough [7] proved the answer is *no* in the case with $a_i = p_i$, the sequence of prime numbers. (In fact, Hough proved the slightly harder result where the moduli are not necessarily square-free.) Here the sum of the reciprocals *almost* converges. The very naive Boole's inequality does not suffice to rule out a positive answer to the Erdős problem, but the Lovász local lemma suffices to do the job.

So in a way, the fact that $\{a_i\}$ was initially the sequence of primes was a red herring. In this general framework, what is important is the asymptotics of this sequence.

It would be interesting to see to what extent Hough's proof of impossibility extends to other sequences (a_i) for which the answer is neither an obvious *yes*, nor an obvious *no*.

REFERENCES

[1] Berger, M. A., Felzenbaum, A., Fraenkel, A. (1986). A nonanalytic proof of the Newman-Znam result for disjoint covering systems. *Combinatorica*. 6(3): 235–243. doi.org/10.1007/BF02579384

[2] Berger, M. A., Felzenbaum, A., Fraenkel, A. (1986). New results for covering systems of residue sets. *Bull. Amer. Math. Soc*. 14(1): 121–125. doi.org/10.1090/S0273-0979-1986-15414-5
[3] Boole, G. (1958). *An Investigation Into the Laws of Thought*. Mineola, NY: Dover. Reprint of the original 1854 edition.
[4] Delahaye, J.-P. (2017). Cinq énigmes pour la rentrée. *Pour Sci*. 479: 80–85.
[5] Erdős, P. (1950). On integers of the form $2^k + p$ and some related problems. *Summa Brasil. Math.* 2: 113–123.
[6] Erdős, P. (1952). On a problem concerning covering systems. *Mat. Lapok.* 4: 122–128.
[7] Hough, B. (2015). Solution of the minimum modulus problem for covering systems. *Ann. Math.* 181(1): 361–382. doi.org/10.4007/annals.2015.181.1.6
[8] Simpson, R. J. (1986). Exact covering of the integers by arithmetic progressions. *Discrete Math*. 59(1–2): 181–190. doi.org/10.1016/0012-365X(86)90079-8
[9] Winkler, P. (2007). *Mathematical Mind-Benders*. Wellesley, MA: A. K. Peters.
[10] Zeilberger, D. (2001). How Berger, Felzenbaum and Fraenkel revolutionized covering systems the same way that George Boole revolutionized logic. *Electron. J. Comb*. 8(2): A1.
[11] Zeleke, M. (1998). *Discrete Radon transform, covering congruences, and Boolean functions.* Ph.D. dissertation. Temple University, Philadelphia.

Summary. Bob Hough recently disproved a long-standing conjecture of Paul Erdős regarding covering systems. Inspired by his seminal paper, we describe analogs of covering systems to Boolean functions, and more generally, the problem of covering discrete hyper-boxes by non-parallel lower dimensional hyper-sub-boxes. We exhibit how the Erdős problem is a special case of this general setup, where the side lengths of the boxes are primes. We discover that the primes were red herrings. Indeed, given this general framework, we can prove the same results for sequences other than the prime numbers; we only need a weaker asymptotic condition.

ANTHONY ZALESKI (MR Author ID: 1013551) received his Ph.D. in mathematics from Rutgers University. His research involved the application of experimental math to problems in combinatorics. His advisor was none other than Doron Zeilberger. Anthony now works in finance.

DORON ZEILBERGER (MR Author ID: 186835) is a Board of Governors Professor at Rutgers University. His first mathematical love was Boolean functions, and when he was 18 years old, he rediscovered a way to simplify Boolean functions that turned out to be equivalent to the known Quine–McCluskey algorithm. It was fun returning to his first love in the writing of this paper.

A Drunken Walk in Las Vegas: Catalan Convolutions and Gambling

MATTHEW MCMULLEN
Otterbein University
Westerville, OH 43081
mmcmullen@otterbein.edu

There are two types of mathematicians who visit Las Vegas: those who know they will lose money and are just there for entertainment value, and those who know how to (and have the patience and resources to) play, perfectly, the select few video poker machines with positive expected value (but extremely large variation!). Being of the former type, we ask a natural question: "Given a fixed amount of money you are willing to lose, how long will it last?"

This question is not new. In fact, it is related to the so-called "gambler's ruin" problem, which originated in a letter from Blaise Pascal to Pierre Fermat over 350 years ago. (This letter occurred two years after the famous correspondence on the problem of points that is discussed in Devlin [2].) A historical treatment of the original problem is given in Edwards [3]. In one form, this problem essentially asks for the probability that a gambler goes bust before he or she wins some predetermined amount, along with the expected number of bets the gambler will make. An excellent (and entertaining) treatment of this situation is given by Lehman, Leighton, and Meyer [5].

Our issue with these types of problems, however, is that they don't really apply to the casual gambler (i.e., one that gambles rarely). Indeed, expected value is only meaningful *in the long run*. If you're making a single trip to a casino and betting until you bust, it is much more important to understand the underlying probability distribution, which is what we have contributed to this problem. In particular, we determine the relevant probability mass function and its expected value (which agrees with Pascal–Fermat) and variance.

The general question

You have arrived in Las Vegas with a set amount of gambling money. You are going to gamble repeatedly on a bet that pays 1:1 until you spend all of this money and any earnings you make along the way. (If the bet pays 1:1, you better believe that the probability of winning this bet is less than $1/2$, unless you are an expert card counter playing blackjack. Casinos are profitable for a reason!) Your initial amount of money is enough to make at most k bets. Let p be the probability of winning this bet and q be the probability of losing this bet, where $0 < p < 1/2$ and $q = 1 - p$ (no pushes allowed). Let the random variable X_k be the total number of bets you make until you have no money left. Describe the probability distribution of X_k.

Preliminaries

To tackle this problem, we need to start with a few mathematical preliminaries: convolutions of sequences, generating functions, and the Catalan numbers.

Math. Mag. **93** (2020) 62–68. doi:10.1080/0025570X.2019.1684798
MSC: Primary 60C05; Secondary 05A15

Given two sequences (a_n) and (b_n), define their convolution as the sequence

$$(a_n * b_n) = \left(\sum_{i=0}^{n} a_i b_{n-i} \right).$$

If $(b_n) = (a_n)$, then we call $(a_n * b_n)$ the two-fold self-convolution of (a_n) and denote this sequence by $(a_n^{(2)})$. In general, define the k-fold self-convolution of (a_n) as

$$(a_n^{(k)}) = \left(\sum a_{n_1} a_{n_2} \cdots a_{n_k} \right),$$

where the summation runs though non-negative integers $n_1, \ldots, n_k$ that sum to n.

These definitions are motivated by generating functions, formal power series whose coefficients encode sequences. Indeed, if the generating function of (a_n) is given by

$$f(x) = \sum_{n=0}^{\infty} a_n x^n,$$

then $(f(x))^k$ is the generating function of $(a_n^{(k)})$.

We will concern ourselves primarily with the k-fold self-convolutions of the so-called "Catalan numbers," which have the form

$$C_n = \frac{1}{n+1} \binom{2n}{n},$$

for $n \geq 0$. The Catalan numbers have been extensively studied. Among scores of counting problems whose solution is given by the Catalan numbers are the number of different ways $n+1$ factors can be completely parenthesized, the number of different ways a convex polygon with $n+2$ sides can be triangulated, and the number of permutations of $\{1, \ldots, n\}$ that avoid the pattern 123. (See Stanley [7] for several more examples.)

For $n \geq 0$ and $k \geq 1$, define $B(n; k)$ as the k-fold self-convolution of the Catalan numbers (see Tedford [8] for some combinatorial interpretations). We can also naturally extend this definition to $k = 0$ by setting $B(0; 0) = 1$ and $B(n; 0) = 0$ for $n \geq 1$. Catalan himself, in Catalan [1], proved that

$$B(n; k) = \frac{k}{n+k} \binom{2n+k-1}{n}. \tag{1}$$

Moreover, it is well-known that the generating function of the Catalan numbers is given by

$$C(x) = \frac{1 - \sqrt{1-4x}}{2x}.$$

Therefore, we have the very useful formula

$$\sum_{n=0}^{\infty} B(n; k) x^n = \left(\frac{1 - \sqrt{1-4x}}{2x} \right)^k. \tag{2}$$

At the moment, this is just a formal power series (i.e., we haven't talked about convergence); but later we will need the fact that, by Abel's theorem and the ratio test, this formula is valid for $|x| \leq 1/4$.

Back to Vegas

We are now ready to tackle the probability distribution of X_k, the total number of bets you make until you have no money left, given that you start with enough money to make k bets. Let's think about a specific case, say $k = 2$ and $p = 0.4$. The worst thing that can happen (from the gambler's point of view), is to lose twice in a row. This would happen with probability $0.6^2 = 0.36$. The next-worst thing is to win just once. There are two ways to accomplish this:

$$LWLL \quad \text{and} \quad WLLL,$$

implying that this would happen with probability $2(0.4)(0.6)^3 = 0.1728$. We point out that these two possibilities together already account for over 50% of the total probability. Clearly, we need more money, or to find a game with better odds!

We can continue in this way, carefully enumerating the ways to bust when winning exactly so many times. For example, there are five ways to win exactly twice:

$$LWWLLL, \quad LWLWLL, \quad WWLLLL, \quad WLLWLL, \quad WLWLLL.$$

Therefore, the probability of this happening is $5(0.4)^2(0.6)^4 = 0.10368$. Quickly, however, this method becomes tedious; the number of possibilities gets too large too fast. As is often true in mathematics, it is easier to tackle the problem in a more general setting.

We first note that, since each win must be balanced out by a loss, X_k only takes on the values $k + 2n$, for $n \geq 0$. Now, let $c(b, k)$ denote the number of ways to bust after b bets, starting with enough money to make at most $k \geq 1$ bets. Clearly, $b \geq k$ and b and k must have the same parity. Also, $c(k, k) = 1$ (every bet is a loss); and, by convention, put $c(0, 0) = 1$ and $c(b, 0) = 0$ for all even b with $b \geq 2$. The key observation to make is that all other valid values of b and k satisfy

$$c(b, k) = c(b - 1, k - 1) + c(b - 1, k + 1). \tag{3}$$

This follows since every time you bet (reducing b by 1) you either lose, which reduces k by 1, or win, which increases k by 1. Using this recursive formula, it is easy to generate the values of $c(b, k)$. The results, for values of b and k up to 10, are shown in Table 1.

Now, many amateur combinatorialists will immediately conjecture that the $k = 1$ column lists the Catalan numbers. A specialist may also suspect that the other columns are the k-fold self-convolutions of the Catalan numbers. (A non-specialist would be wise to consult the On-line Encyclopedia of Integer Sequences [**6**].) As we shall see, this is indeed the case!

We need to show that

$$B(n; k) = c(k + 2n, k)$$

for all $n, k \geq 0$. The $k = 0$ and $n = 0$ cases are easy to verify. Moreover, by (3), we have that:

$$\begin{aligned} c(k + 2n, k) &= c(k + 2n - 1, k - 1) + c(k + 2n - 1, k + 1) \\ &= c((k - 1) + 2n, k - 1) + c((k + 1) + 2(n - 1), k + 1); \end{aligned}$$

so it is sufficient to show that

$$B(n; k) = B(n; k - 1) + B(n - 1; k + 1),$$

b \ k	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	1										
1		1									
2	0		1								
3		1		1							
4	0		2		1						
5		2		3		1					
6	0		5		4		1				
7		5		9		5		1			
8	0		14		14		6		1		
9		14		28		20		7		1	
10	0		42		48		27		8		1

TABLE 1: Values of $c(b, k)$, for values of b and k up to 10.

for $n, k \geq 1$. This follows easily from (1).

Now, recall that the random variable X_k is the total number of bets you make until you bust. When $X_k = k + 2n$, this means you have won n bets and lost $k + n$ bets. Therefore,

$$\Pr(X_k = k + 2n) = B(n; k)p^n q^{k+n}.$$

Since

$$pq = p(1 - p) \leq 1/4,$$

we can use (2) to get

$$\begin{aligned}\sum_{n=0}^{\infty} B(n; k)p^n q^{k+n} &= q^k \sum_{n=0}^{\infty} B(n; k)(pq)^n \\ &= q^k \left(\frac{1 - \sqrt{1 - 4pq}}{2pq}\right)^k \\ &= \left(\frac{1 - |1 - 2p|}{2p}\right)^k \\ &= 1.\end{aligned}$$

This confirms that the probability we will bust is 1, but, interestingly (if we relax our restriction on p), it also shows that the probability we bust is 1 if $p = 1/2$ (see Lehman, Leighton, and Meyer [5] for more discussion of this counterintuitive case). Moreover, if $1/2 < p \leq 1$ we have shown that the probability of busting is

$$\left(\frac{1 - p}{p}\right)^k < 1.$$

Similarly, by using the first and second derivatives of (2) evaluated at pq, one can show that (for $0 \leq p < 1/2$)

$$\sum_{n=0}^{\infty} B(n;k)np^n q^{k+n} = \frac{kp}{1-2p}$$

and

$$\sum_{n=0}^{\infty} B(n;k)n^2 p^n q^{k+n} = \frac{kp(kp(1-2p)+q)}{(1-2p)^3}.$$

These equations in turn can be used to show that

$$\begin{aligned} E[X_k] &= \sum_{n=0}^{\infty}(2n+k)B(n;k)p^n q^{k+n} \\ &= 2\sum_{n=0}^{\infty} B(n;k)np^n q^{k+n} + k\sum_{n=0}^{\infty} B(n;k)p^n q^{k+n} \\ &= \frac{2kp}{1-2p} + k \\ &= \frac{k}{1-2p} \end{aligned}$$

and (we'll spare you most of the gory details)

$$\begin{aligned} \mathrm{Var}(X_k) &= E[X_k^2] - E[X_k]^2 \\ &= \sum_{n=0}^{\infty}(2n+k)^2 B(n;k)p^n q^{k+n} - \frac{k^2}{(1-2p)^2} \\ &= \frac{4kp(1-p)}{(1-2p)^3}. \end{aligned}$$

As p gets closer to $1/2$, notice that the variance grows at a much faster rate than the expected value, so there will be even greater discrepancy between the mean, median, and mode.

Two concrete examples

Roulette There are three bets in roulette that pay even odds: red/black, even/odd, and $1-18/19-36$. Thanks to the green (and neither even nor odd) 0 and 00 slots, each of these bets has probability $18/38 \approx 0.4737$ of winning and $20/38$ of losing. Suppose you have enough money to make 4 of these bets and you keep playing until you bust. So we have $k = 4$, $p = 18/38$, and $q = 20/38$. The relevant probability mass function is shown in Figure 1.

Using these results, we see that the expected number of bets we will make before going bust is 76. (According to [**9**], if you're playing with 5 other players, that's over two hours of entertainment—not bad!) The variance, however, is 27,360 (so the standard deviation is approximately 165.4 bets). In fact, using Mathematica, we see that the mode of this distribution is 4 bets! In other words, the most-likely (probability of

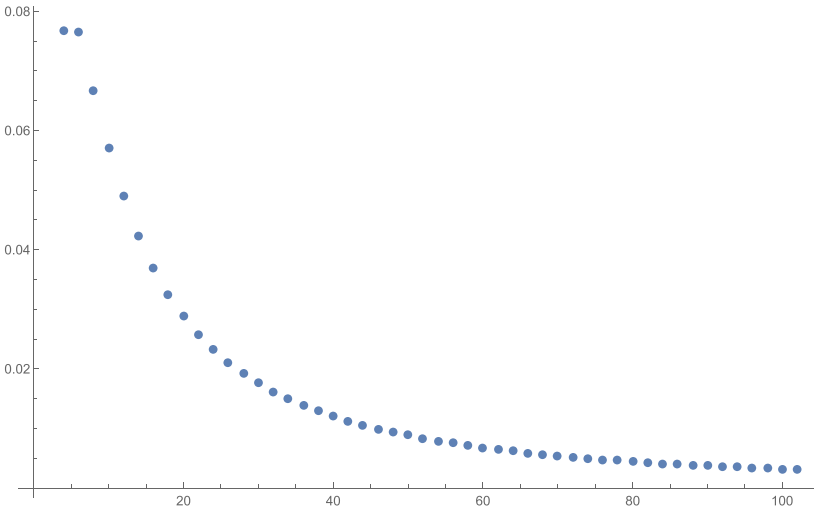


Figure 1 The probability mass function for roulette.

0.0767) single outcome is to bust as quickly as possible (this would take just under seven minutes!). Also, about half the time (probability of 0.4923) you'll make 22 or fewer bets (this would take less than 37 minutes).

Craps The pass line bet (a bet for the shooter) is the most common bet for beginning craps players and it pays even odds. If the first roll is a 7 or 11, this bet wins. If the first roll is a 2, 3, or 12, this bet loses. If the roll is any other value, this bet wins only if the same value is rolled before a 7 is rolled. It is a nice (and by no means trivial) problem to show that the probability of winning this bet is $244/495 \approx .4929$, markedly better than the probability of winning our roulette bet. Suppose you have enough money to make 10 of these bets and you keep playing until you bust. So we have $k = 10$, $p = 244/495$, and $q = 251/495$. The probability mass function for this case is shown in Figure 2. In this example, the expected number of bets we will make before going bust is just over 707. The variance, however, is just under 3,535,368 (for a standard deviation of approximately 1880 bets!). Using Mathematica, we see that the mode of this distribution is 32 bets; and, about half the time (probability of 0.4990) you'll make 164 or fewer bets.

Final remarks

The colorful title of this article is of course not meant to condone gambling or drinking to excess. However, we can think of the distribution discussed in this article as a one-dimensional drunkard's walk. Imagine a drunk k blocks from home. Every minute he either moves one block farther from home, with probability $p < 1/2$, or he moves one block closer to home, with probability $q = 1 - p$. Then X_k is the number of minutes it takes him to get home. In fact, the number of such drunken walks of length $2n + k$ is essentially the first interpretation of $B(n; k)$ given by Larcombe and French [4].

We feel that this distribution is a good one to present to students in a combinatorics class who have had some probability (or vice versa). It involves the Catalan numbers, convolutions, and generating functions, each an interesting topic in its own right.

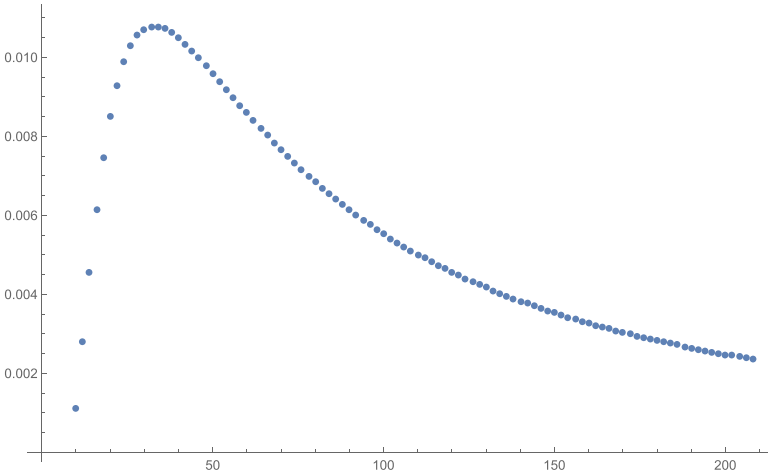


Figure 2 The probability mass function for craps.

Moreover, this is a great example of a real-life distribution whose mean, median, and mode are drastically different, with very important (and costly!) implications.

REFERENCES

[1] Catalan, E. (1887). Sur les nombres de Segner. *Rend. Circ. Mat. Palermo*. 1(1): 190–201.
[2] Devlin, K. (2010). *The Unfinished Game: Pascal, Fermat, and the Seventeenth-Century Letter That Made the World Modern*. New York: Basic Books.
[3] Edwards, A. (1983). Pascal's problem: The 'gambler's ruin'. *Int. Stat. Rev./Rev. Int. Stat*. 51(1): 73–79. doi.org/10.2307/1402732
[4] Larcombe, P. J., French, D. R. (2003). The Catalan number k-fold self-convolution identity: The original formulation. *J. Comb. Math. Comb. Comput*. 46(1): 191–204.
[5] Lehman, E., Leighton, F. T., Meyer, A. R. (2010). *Mathematics for Computer Science*. Reading material for Tom Leighton, and Marten Dijk, 6.042J Mathematics for Computer Science. Fall 2010. Massachusetts Institute of Technology: MIT OpenCourseWare. ocw.mit.edu
[6] The On-Line Encyclopedia of Integer Sequences Continuously updated. oeis.org
[7] Stanley, R. P. (1999). *Enumerative Combinatorics*, Vol. 2. Cambridge: Cambridge University Press.
[8] Tedford, S. (2011). Combinatorial interpretations of convolutions of the Catalan numbers. *Integers*. 11(1): 35–45.
[9] Ask the Wizard #136. wizardofodds.com/ask-the-wizard/136/

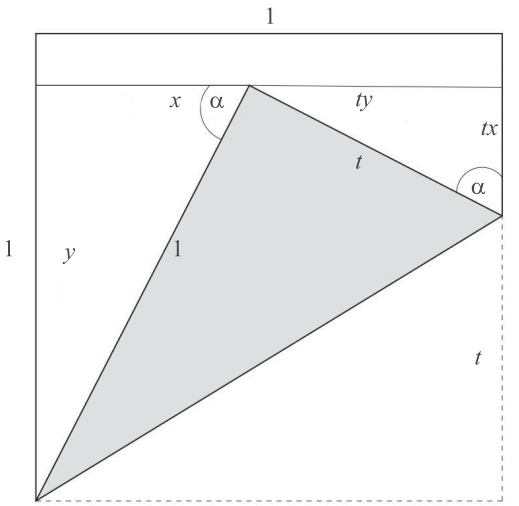
Summary. As a mathematician in Las Vegas unwilling to hunt for positive-expected-value video poker machines, we know that eventually we will lose all the money we are willing to gamble. But how long will this take? Answering this seemingly simple question takes us from Catalan convolutions to generating functions as we explore a probability distribution related to a one-dimensional drunkard's walk.

MATTHEW MCMULLEN (MR Author ID: 1257912) is a senior instructor of mathematics and statistics at Otterbein University, Westerville, Ohio. He earned a B.S. in mathematics from Loyola University Maryland, Baltimore and an M.S. in mathematics from The Ohio State University, Columbus. When he is not teaching or absorbed in a recreational mathematics problem, he is either off on a run, watching Premier League soccer, playing with his three year old, or wishing he were drinking malt whisky in Scotland.

PROOFS WITHOUT WORDS

Rational Parametric Equation of a Circle From a Paper Fold

ELENA GALAKTIONOVA
Mobile, AL 36608
pillen@southalabama.edu



$$\begin{aligned} x + ty &= 1 \\ t + tx &= y \end{aligned} \quad \Longrightarrow \quad \begin{aligned} x &= \frac{1 - t^2}{1 + t^2} \\ y &= \frac{2t}{1 + t^2} \end{aligned}$$

Summary. Place a square sheet of paper with side length 1 into the first quadrant of a coordinate system in such a way that the lower-left corner coincides with the origin. Look at the set of points that are obtained by folding the lower-right corner of the sheet along a line passing through the origin. The points obtained in this fashion will lie on the unit circle whose center is the origin. By making use of two similar triangles, the illustration gives rise to a rational parametrization of the unit circle. The parameter t is the distance from the lower-right corner of the sheet to the point of intersection of the fold line with the right edge of the paper.

ELENA GALAKTIONOVA (MR Author ID: 246181) received her Ph.D. in representation theory from the University of Massachusetts, Amherst. She taught mathematics for many years at the University of South Alabama. In Mobile, Alabama, she was actively involved in the Mobile Math Circle and she founded the Mobile Math Teachers' Circle. Her work with local middle school students and teachers was motivated by her love for mathematics and mathematics education. Sadly, Elena passed away after a long battle with cancer in 2019.

Math. Mag. **93** (2020) 69. doi:10.1080/0025570X.2020.1684796
MSC: 51-01

Titu's Lemma

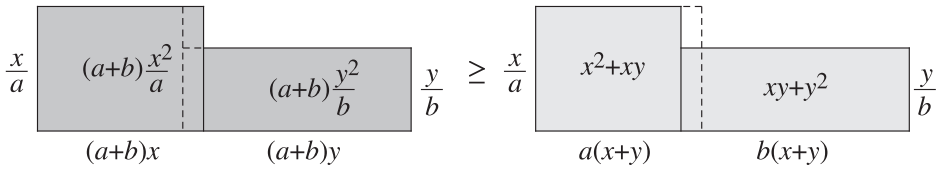
ROGER B. NELSEN
Lewis & Clark College
Portland, OR 97219
nelsen@lclark.edu

The lemma in the title is an inequality with applications to a variety of algebraic inequalities often encountered in mathematical competitions [1, pp. 8–11], [2, pp. 107–125]. It is also known as *Sedrakyan's inequality*.

Lemma. *Let a, b, x, and y be real numbers with $a, b > 0$. Then*

$$\frac{x^2}{a} + \frac{y^2}{b} \geq \frac{(x+y)^2}{a+b}.$$

Proof. Assume $x/a \geq y/b$ (the case $y/b \geq x/a$ is analogous). Then $bx \geq ay$ so that $(a+b)x \geq a(x+y)$ and $b(x+y) \geq (a+b)y$. Hence:



Therefore,

$$(a+b)\left(\frac{x^2}{a} + \frac{y^2}{b}\right) \geq (x+y)^2.$$

■

Note that this inequality readily extends to a sum of three terms:

$$\frac{x^2}{a} + \frac{y^2}{b} + \frac{z^2}{c} \geq \frac{(x+y)^2}{a+b} + \frac{z^2}{c} \geq \frac{(x+y+z)^2}{a+b+c},$$

and thus by mathematical induction to a sum of n terms:

$$\frac{x_1^2}{a_1} + \frac{x_2^2}{a_2} + \cdots + \frac{x_n^2}{a_n} \geq \frac{(x_1 + x_2 + \cdots + x_n)^2}{a_1 + a_2 + \cdots + a_n}.$$

REFERENCES

[1] Andreescu, T., Enescu, B. (2011). *Mathematical Olympiad Treasures*, 2nd ed. New York: Birkhäuser.
[2] Sedrakian, H., Sedrakyan, N. (2018). *Algebraic Inequalities*. New York: Springer.

Summary. We present a visual proof of an inequality known as Titu's lemma or Sedrakayan's inequality.

ROGER B. NELSEN (MR Author ID: 237909) is professor emeritus at Lewis & Clark College, where he taught mathematics and statistics for 40 years.

Math. Mag. **93** (2020) 70. doi:10.1080/0025570X.2020.1682745
MSC: 26D05

PROBLEMS

LES REID, *Editor*
Missouri State University

EUGEN J. IONAŞCU, *Proposal Editor*
Columbus State University

RICHARD BELSHOFF, Missouri State University; *EYVINDUR ARI PALSSON*, Virginia Tech; *CODY PATTERSON*, Texas State University; *ROGELIO VALDEZ*, Centro de Investigación en Ciencias, UAEM, Mexico; *Assistant Editors*

Proposals

To be considered for publication, solutions should be received by July 1, 2020.

2086. *Proposed by David M. Bradley, University of Maine, Orono, ME.*

Let $f(k)$ denote the largest integer that is a divisor of $n^k - n$ for all integers n. For example, $f(2) = 2$ and $f(3) = 6$. Determine $f(k)$ for all integers $k > 1$.

2087. *Proposed by Florin Stanescu, Şerban Cioiculescu School, Găeşti, Romania.*

Consider the sequence defined by $x_1 = a > 0$ and

$$x_n = \ln\left(1 + \frac{x_1 + x_2 + \cdots + x_{n-1}}{n-1}\right) \text{ for } n \geq 2.$$

Compute $\lim_{n\to\infty} x_n \ln n$.

2088. *Proposed by Mircea Merca, University of Craiova, Romania.*

Let n and t be nonnegative integers. Prove that

$$\sum_{k=0}^{2n} (-1)^k F_{tk} F_{2tn-tk} = -\frac{F_t}{L_t} F_{2tn},$$

where F_i denotes the ith Fibonacci number and L_i denotes the ith Lucas number.

Math. Mag. **93** (2020) 71–78. doi:10.1080/0025570X.2020.1685297

We invite readers to submit original problems appealing to students and teachers of advanced undergraduate mathematics. Proposals must always be accompanied by a solution and any relevant 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.

Proposals and solutions should be written in a style appropriate for this MAGAZINE.

Authors of proposals and solutions should send their contributions using the Magazine's submissions system hosted at http://mathematicsmagazine.submittable.com. *More detailed instructions are available there. We encourage submissions in PDF format, ideally accompanied by LaTeX source. General inquiries to the editors should be sent to* mathmagproblems@maa.org.

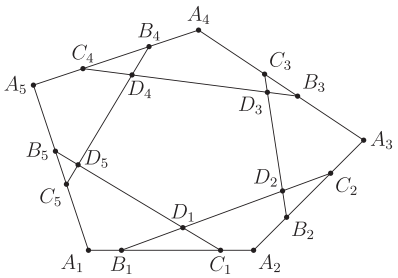
2089. *Proposed by Rick Mabry, LSU Shreveport, Shreveport, LA.*

Let $A_1, A_2, \ldots, A_n$ be the vertices of a convex n-gon in the plane. Identifying the indices modulo n, define the following points: Let B_i and C_i be vertices on $\overline{A_iA_{i+1}}$ such that

$$A_iB_i = C_iA_{i+1} < \frac{A_iA_{i+1}}{2},$$

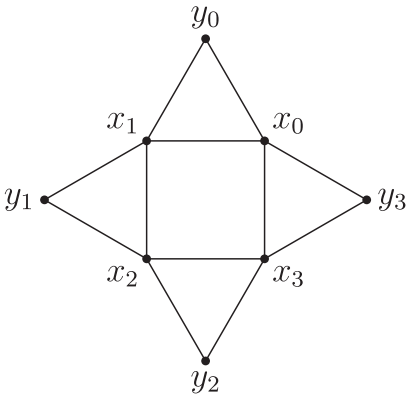
and let D_i be the intersection of $\overline{B_{i-1}C_i}$ and $\overline{B_iC_{i+1}}$. Prove that

$$\prod_{i=1}^{n} \frac{B_iD_i}{D_iC_i} = 1.$$



2090. *Proposed by Gregory Dresden, Washington & Lee University, Lexington, VA.*

Recall that a *matching* of a graph is a set of edges that do not share any vertices. For example, C_4, the cyclic graph on four vertices (i.e., a square), has seven matchings: the empty set, single edges (four of these), or pairs of opposite edges (two of these).
Let G_n be the (undirected) graph with vertices x_i and y_i, $0 \le i \le n-1$, and edges $\{x_i, x_{i+1}\}$, $\{x_i, y_i\}$, and $\{y_i, x_{i+1}\}$, $0 \le i \le n-1$, where the indices are to be taken modulo n. For example, G_4 is shown below. Determine the number of matchings of G_n.



Quickies

1097. *Proposed by George Stoica, Saint John, New Brunswick, Canada.*

Let $z_1, \ldots, z_n \in \mathbb{C}$ with $|z_i| = 1$. Show that there exists $\omega \in \mathbb{C}$ with $|\omega| = 1$ such that $|(\omega - z_1) \ldots (\omega - z_n)| \geq 2$, and this result is the best possible, namely 2 cannot be replaced by any larger number.

1098. *Proposed by Oniciu Gheroghe, Botoşani, Romania.*

In the convex quadrilateral $ABCD$, $\angle BAD \cong \angle BCD$ both with measure $60°$. The diagonal $\overline{AC}$ bisects $\angle BAD$. Prove that $m(\angle BDA) = 2m(\angle BCA)$.

Solutions

2061. *Proposed by Florin Stanescu, Şerban Cioiculescu School, Găeşti, Romania.*

Three complex numbers a, b, c satisfy

$$|a| = |b| = |c| = 1 \qquad \text{and} \qquad a^3 + b^3 + c^3 = 2abc.$$

Prove that a, b, c are vertices of an isosceles triangle on the complex plane.

Solution by José Heber Nieto, Universidad del Zulia, Maracaibo, Venezuela.
We shall prove more generally that, if

$$|a| = |b| = |c| = 1 \quad \text{and} \quad a^3 + b^3 + c^3 = rabc$$

for any real number r, $-1 \leq r \leq 3$, then a, b, c are the vertices of an isosceles triangle in the complex plane. Note that we are allowing for the possibility of degenerate triangles where vertices coincide.

A triangle is isosceles if and only if two of its central angles are congruent. There are three possibilities:

$$\frac{a}{b} = \frac{b}{c}, \quad \frac{b}{c} = \frac{c}{a}, \quad \text{or} \quad \frac{c}{a} = \frac{a}{b}.$$

Therefore the triangle is isosceles if and only if

$$(a^2 - bc)(b^2 - ca)(c^2 - ab) = 0, \text{ i.e.,}$$
$$a^4bc + ab^4c + abc^4 = a^3b^3 + b^3c^3 + a^3c^3.$$

If $a^3 + b^3 + c^3 = rabc$ then

$$\frac{1}{a^3} + \frac{1}{b^3} + \frac{1}{c^3} = \overline{a^3 + b^3 + c^3} = \overline{rabc} = \frac{r}{abc}.$$

Multiplying both sides by $(abc)^3$ we obtain

$$a^3b^3 + b^3c^3 + a^3c^3 = r(abc)^2 = a^4bc + ab^4c + abc^4$$

as desired.

Now suppose

$$a^3 + b^3 + c^3 = rabc$$

and, for example, $c/a = a/b$. Then

$$1 + \left(\frac{b}{a}\right)^3 + \left(\frac{c}{a}\right)^3 = \frac{rbc}{a^2} = r.$$

Since b/a and c/a are conjugate, we may put

$$\frac{b}{a} = e^{\phi i}, \quad \text{and} \quad \frac{c}{a} = e^{-\phi i}.$$

Then

$$e^{3\phi i} + e^{-3\phi i} = r - 1, \text{ i.e.,}$$

$$\cos 3\phi = \frac{r-1}{2}.$$

This shows that $-1 \le r \le 3$. Note that degenerate triangles with

$$\phi = 0, \text{ (e.g., } a = b = c = 1) \quad \text{and} \quad \phi = \pi, \text{ (e.g., } a = 1, b = c = -1)$$

can occur when $r = -1$ or 3.

In the original problem, $\cos 3\phi = 1/2$, so

$$\phi = \frac{\pi}{9}, \quad \frac{5\pi}{9}, \quad \text{or} \quad \frac{7\pi}{9},$$

and the angles of the triangle formed by a, b, and c are

$$\left(\frac{\pi}{18}, \frac{\pi}{18}, \frac{\pi}{9}\right), \quad \left(\frac{5\pi}{18}, \frac{5\pi}{18}, \frac{4\pi}{9}\right), \quad \text{or} \quad \left(\frac{7\pi}{18}, \frac{7\pi}{18}, \frac{2\pi}{9}\right).$$

Also solved by Robert A. Agnew, Hafez Al-Assad (Syria), Michel Bataille (France), Cal Poly Pomona Problem Solving Group, Robert Calcaterra, Adam Cofmann, Bruce E. Davis, Robert L. Doucette, George Washington University Problems Group, Kyle Gatesman, Michael Goldenberg & Mark Kaplan, Eugene A. Herman, Walther Janous (Austria), Stephen Kaczkowski, Koopa Tak Lun Koo (Hong Kong), Omran Kouba (Syria), Kee-Wai Lau (Hong Kong), Hyomin Park (Korea), Theophilus Pedapolu, Michael Reid, Ivan Retamoso, Leonel Robert & Charlotte Ochanine, Randy K. Schwartz, Daniel Vacaru (Romania), Lawrence R. Weill and the proposer. There was one incomplete or incorrect solution.

2062. *Proposed by Enrique Treviño, Lake Forest College, Lake Forest, IL.*

For every positive integer n, let $f(n)$ denote the number of occurrences of the digit 2 in the sequence $1, 2, \ldots, n$ of integers written in base 10. (For instance, $f(25) = 9$ because the digit 2 appears once in 2, 12, 20, 21, 23, 24, 25 and twice in 22.)

(*i*) Find a positive integer n such that $f(n) = n$.

(*ii*) Are there infinitely many solutions to $f(n) = n$?

Solution by Cassandra DeBacco (student) and Mark Capsambelis, Riverview High School, Oakmont, PA.

Let $n \in \mathbb{N}$. For all integers between 0 and $10^n - 1$, the digit 2 appears in each of the n decimal places $1/10$ of the time, so

$$f\,(10^n) = n10^{n-1}.$$

In particular, if $n = 10$, then

$$f\left(10^{10}\right) = 10 \cdot 10^9 = 10^{10},$$

which answers (i).

For (ii), note that for all $n > 100$,

$$f\,(10^n) = n10^{n-1} > 10^{n+1}.$$

So if $n > 100$ and $k \in \mathbb{N}$ such that $10^n \le k < 10^{n+1}$, then

$$f(k) \ge f(10^n) > 10^{n+1} > k$$

since f is non-decreasing. Therefore, there are no solutions of $f(n) = n$ for $n > 100$, so there are only a finite number of solutions.

Also solved by Mohammed Aassila (France), Ulrich Abel (Germany), Hafez Al-Assad (Syria), Armstrong Problem Solvers, Brian Beasley, Virginia Faulkner Bolton, David Stone and John Hawkins, Robert Calcaterra, Bill Cowieson, Robert L. Doucette, Kyle Gatesman, George Washington University Problems Group, Eugene A. Herman, Kelly Jahns, Andrea McCormack, José Heber Nieto (Venezuela), Northwestern University Math Problem Solving Group, Charlotte Ochanine, Moubinool Omarjee (France), Timothy Prescott, Michael Reid, Arnold Saunders, Randy K. Schwartz, Allen Schwenk, James Swenson, Mark Wildon, and the proposer. There were 3 incomplete or incorrect solutions.

2063. *Proposed by Ovidiu Furdui and Alina Sîntămărian, Technical University of Cluj-Napoca, Cluj-Napoca, Romania.*

Evaluate

$$\sum_{n=0}^{\infty}\sum_{k=1}^{\infty}\frac{(-1)^{n+k-1}}{(n+k)^2}.$$

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

The answer is $\ln 2$.

Let S_N be the following partial sum:

$$S_N = \sum_{n=0}^{N}\sum_{k=1}^{\infty}\frac{(-1)^{n+k-1}}{(n+k)^2}\,.$$

For each fixed N we have that S_N is absolutely convergent, so we can rearrange terms and rewrite the sum as $S_N = S'_N + S''_N$, where (writing $n + k = j$):

$$S'_N = \sum_{\substack{n+k\le N\\ n\ge 0,\,k\ge 1}}\frac{(-1)^{n+k-1}}{(n+k)^2} = \sum_{j=1}^{N} j\,\frac{(-1)^{j-1}}{j^2} = \sum_{j=1}^{N}\frac{(-1)^{j-1}}{j}\,,$$

$$S''_N = (N+1)\sum_{j=N+1}^{\infty}\frac{(-1)^{j-1}}{j^2}\,.$$

The sum of the alternating series S''_N can be bound by its first term, so we have

$$|S''_N| < \frac{1}{N+1} \to 0 \quad \text{as} \quad N \to \infty.$$

Hence

$$\sum_{n=0}^{\infty}\sum_{k=1}^{\infty}\frac{(-1)^{n+k-1}}{(n+k)^2} = \lim_{N\to\infty} S'_N + \lim_{N\to\infty} S''_N = \sum_{j=1}^{\infty}\frac{(-1)^{j-1}}{j} + 0 = \ln 2\,.$$

Also solved by Ulrich Abel (Germany), Farrukh Rakhimjanovich Ataev (Uzbekistan), Michel Bataille (France), Necdet Batir (Turkey), Khristo Boyadzhiev, Brian Bradie, Robert Calcaterra, Hongwei Chen, Bill Cowieson, Bruce Davis, Robert L. Doucette, Saumya Dubey, John N. Fitch, Kyle Gatesman, Subhankar Gayen (India), George Washington University Problems Group, Tom Goebeler & Wendy Sun, Russelle Guadalupe (Philippines), GWstat Problem Solving Group, Eugene A. Herman, Walther Janous (Austria), Kee-Wai Lau (China), Pedro Acosta De Leon, Carl Libis, José Heber Nieto (Venezuela), Moubinool Omarjee (France), Emily Owen, Hyomin Park (Korea), Sumanth Ravipati, Edward Schmeichel, Randy K. Schwartz, Albert Stadler (Switzerland), Robert W. Vallin, Michael Vowe, Mark Wildon (UK), Lienhard Wimmer (Switzerland), John Zacharias, Yijie Zhu (China), and the proposer. There were 3 incomplete or incorrect solutions.

2064. *Proposed by Ioan Băetu, Botoşani, Romania.*

Characterize those integers $n \geq 2$ such that the ring $\mathbb{Z}_n$ of integers modulo n has a subset F that is a field under the operations of addition and multiplication induced from $\mathbb{Z}_n$. [Note that the unity i of such a field F need not be the unity 1 of $\mathbb{Z}_n$.]

Solution by Michael Reid, University of Central Florida, Orlando, FL.
The ring $\mathbb{Z}_n$ contains a subring F that is a field if and only if n is not powerful, i.e., there is a prime p such that n is divisible by p but not by p^2.

First suppose that p is a prime number such that $p|n$ but $p^2 \nmid n$. Write $n = pm$, so $p \nmid m$. By the Chinese remainder theorem, $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_m$, and the subset $\mathbb{Z}_p \times \{0\}$ is isomorphic to $\mathbb{Z}_p$, which is a field.

Conversely, suppose $\mathbb{Z}_n$ contains a field F. Then F is finite, so its characteristic is a prime number p. The additive group $(F, +)$ has exponent p, so it is contained in the p-torsion subgroup of $(\mathbb{Z}_n, +)$. Denote this p-torsion subgroup by B. Since $(\mathbb{Z}_n, +)$ is a cyclic group, every subgroup, in particular B, is also cyclic. Moreover, $|B|$ is either p or 1, depending on whether p divides n or not. Hence, $p|n$, so B has order p, and F coincides with B. Write $n = mp^e$, where $e \geq 1$ and $p \nmid m$. Then the p-torsion subgroup of $\mathbb{Z}_n$ is precisely

$$B = \left\{0, mp^{e-1}, 2mp^{e-1}, \ldots, (p-1)mp^{e-1}\right\}.$$

If $e \geq 2$, then every element of $F = B$ is nilpotent, because

$$\left(amp^{e-1}\right)^2 = \left(a^2 mp^{e-2}\right) mp^e \equiv 0 \bmod n.$$

This is a contradiction, so we must have $e = 1$, and thus $p^2 \nmid n$.

Also solved by Paul Budney, Robert Calcaterra, Bill Cowieson, and the proposer. There was one incomplete or incorrect solution.

2065. *Proposed by Su Pernu Mero, Valenciana GTO, Mexico.*

Let $\mathcal{Q}$ be a cube centered at the origin of $\mathbb{R}^3$. Choose a unit vector (a, b, c) uniformly at random on the surface of the unit sphere $a^2 + b^2 + c^2 = 1$, and let Π be the plane

$ax + by + cz = 0$ through the origin and normal to (a, b, c). What is the probability that the intersection of Π with $\mathcal{Q}$ is a hexagon?

Solution by Bill Cowieson, Fullerton College, Fullerton, CA.
The probability is

$$1 - \frac{6 \arcsin(1/3)}{\pi} \approx 0.350959.$$

Call a unit vector (a, b, c) "good" if $\Pi \cap \mathcal{Q}$ is a hexagon and "bad" otherwise. A vector is good if and only if Π intersects all six sides of $\mathcal{Q}$, therefore the regions of good and bad unit vectors share a boundary that consists of those unit vectors for which Π contains a vertex of $\mathcal{Q}$, i.e., those which are orthogonal to the vector from the origin to some vertex. Without loss of generality, let $\mathcal{Q}$ have vertices

$$(1, 1, 1),\ (1, 1, -1),\ (1, -1, 1),\ \ldots,\ (-1, -1, -1),$$

so this boundary consists of those unit vectors (a, b, c) which satisfy either

$$a + b + c = 0, \quad a + b - c = 0, \quad a - b + c = 0, \quad \text{or} \quad -a + b + c = 0.$$

By symmetry, it suffices to find the probability for (a, b, c) chosen from the positive octant $a, b, c > 0$, where the good/bad boundary equations are $a = b + c$, $b = c + a$, and $c = a + b$. These partition the positive octant of the sphere into 4 spherical triangles: a central triangle of good vectors

$$H = \{(a, b, c) \in \mathbb{R}^3 : a^2 + b^2 + c^2 = 1, a < b + c, b < c + a, c < a + b\},$$

which has vertices

$$\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}, 0\right), \left(\frac{\sqrt{2}}{2}, 0, \frac{\sqrt{2}}{2}\right), \quad \text{and} \quad \left(0, \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right),$$

and three congruent triangles of bad vectors. The desired probability is $\text{Area}(H)/(\pi/2)$

On the unit sphere, the area of a spherical triangle is the sum of the three vertex angles minus π. Let θ be the common angle at each vertex of H, so $\text{Area}(H) = 3\theta - \pi$. The angle at $(\sqrt{2}/2, \sqrt{2}/2, 0)$ is between the planes $x = y + z$ and $y = x + z$, which is that between the normal vectors $(-1, 1, 1)$ and $(-1, 1, -1)$, so $\cos\theta = 1/3$,

$$\text{Area}(H) = 3 \arccos\left(\frac{1}{3}\right) - \pi = \pi/2 - 3 \arcsin\left(\frac{1}{3}\right),$$

and the probability that a random plane through the center of a cube makes a hexagon is

$$\frac{\text{Area}(H)}{\pi/2} = 1 - \frac{6 \arcsin(1/3)}{\pi}.$$

Also solved by Elton Bojaxhiu (Germany) & Enkel Hysnelaj (Australia), Robert L. Doucette, John N. Finch, George Washington University Problems Group, J.A. Grzesik, Kidefumi Katsuura & Edward Schmeichel, Peter McPolin (Northern Ireland), Charlotte Ochanine, Randy K. Schwartz, Yawen Zhang (student), and the proposer. There were 4 incomplete or incorrect solutions.)

Answers

Solutions to the Quickies from page 73.

A1097. Define $P(z) = (z - z_1) \dots (z - z_n)$. For any complex number ω, we have

$$\frac{1}{n} \sum_{k=1}^{n} P\left(\omega \cdot e^{2ik\pi/n}\right) = \omega^n + (-1)^n z_1 \dots z_n.$$

Choose $\omega = -(z_1 \dots z_n)^{1/n}$. Then, by the formula above,

$$2 = |\omega^n + (-1)^n z_1 \dots z_n| = \left| \frac{1}{n} \sum_{k=1}^{n} P\left(\omega \cdot e^{2ik\pi/n}\right) \right| \le \frac{1}{n} \sum_{k=1}^{n} \left| P\left(\omega \cdot e^{2ik\pi/n}\right) \right|.$$

Therefore there exists $k \in \{1, \dots, n\}$ for which

$$\left| P\left(\omega \cdot e^{2ik\pi/n}\right) \right| \ge 2.$$

Taking $z_j = e^{2ij\pi/n}$, we have

$$|P(\omega)| = |\omega^n - 1| \le |\omega|^n + 1 = 2$$

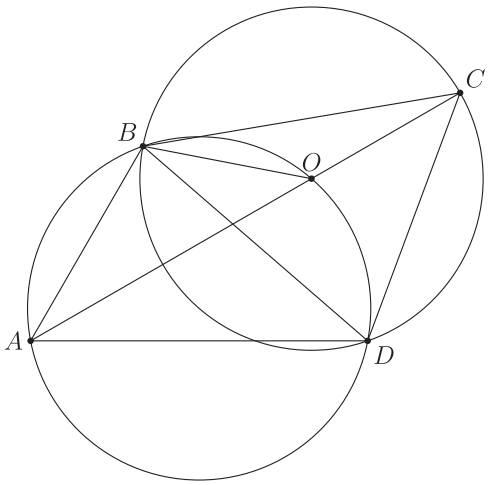
for all ω with $|\omega| = 1$, so 2 cannot be replaced by any larger number.

A1098. Denote the circles that circumscribe $\triangle BCD$ and $\triangle ABD$ by $\mathcal{C}_1$ with center O and $\mathcal{C}_2$ with center O', respectively. One version of the law of sines states that $a/\sin A = b/\sin B = c/\sin C = 2R$, where R is the radius of the circle circumscribing the triangle. Since $\angle BAD \cong \angle BCD$, we conclude that $\mathcal{C}_1$ and $\mathcal{C}_2$ are congruent. The smaller arcs between B and D on $\mathcal{C}_1$ and $\mathcal{C}_2$ both have measure

$$2m(\angle BAD) = 2m(\angle BCD) = 120^\circ.$$

Therefore $\triangle OBO'$ and $\triangle ODO'$ are equilateral, so O lies on $\mathcal{C}_2$ (and O' lies on $\mathcal{C}_1$). Now O is the midpoint of arc BOD since $\overline{AC}$ is the angle bisector of $\angle BAD$. Hence we have

$$m(\angle BDA) = m(\angle BOA) = 2m(\angle BCO) = 2m(\angle BCA).$$



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.

Baez, John, The Riemann hypothesis (in 3 parts), golem.ph.utexas.edu/category/2019/09/the_riemann_hypothesis_part_1.html, _part_2.html, _part_3.html.

Baez offers an in-depth explanation of the Riemann hypothesis that is not notation- or concept-heavy. It starts in number theory, detours through finite fields, and ends in algebraic geometry and the Weil conjectures. "Riemann's explicit formula . . . for $\pi(x)$ [the number of primes $\leq x$] is a sum over zeros of the zeta function. The trivial zeros give a simple approximation to $\pi(x)$, while the nontrivial zeros contribute a bunch of corrections." Baez gives a video of how that works, showing the approximation of the step function by a wave function, where you can see a Gibbs phenomenon at primes. "The Riemann Hypothesis puts a precise bound on how fast [the correction terms] grow . . . like $x^{1/2}\ln(x)$."

Houston-Edwards, Kelsey, Numbers game, *Scientific American* 321 (3) (September 2019) 35–40.

Is the mathematical world (and its objects) real? In an issue centered on "Truth, lies, and uncertainty: Searching for reality in unreal times," the author compares mathematics to improv theater, the main difference being that in mathematics, different "performances" with the same characters (mathematical objects) always end the same (the same theorems, etc.)—but the ending may surprise us. "The objects of study are precisely defined, but they take on a life of their own, revealing unexpected complexity." So, are mathematical objects real (but then how can we learn about them?), invented (then how come mathematics is so interwoven with science?), or totally fictitious (mathematics makes sense internally but has no real meaning)? Fortunately: "In the end, these questions do not affect the practice of mathematics."

Baez, John, The math that takes Newton into the quantum world: How a math professor learned to stop worrying and love algebraic geometry, *Nautilus* (print issue) No. 26: 68–75; (online issue) No. 69, nautil.us/issue/69/patterns/the-math-that-takes-newton-into-the-quantum-world.

John Baez (UC—Riverside) always wanted to be a mathematical physicist but never really liked algebraic geometry until recently. "How could any mathematician *not* fall in love with algebraic geometry? Here's why: In its classic form, this subject considers only *polynomial* equations . . . this seemed like a terrible limitation. After all, physics problems involve plenty of functions that aren't polynomials." The good part of studying only polynomial equations is that doing so allows investigators to plunge more deeply into the interactions between algebra and geometry. What Baez realized, as he attempted to learn algebraic geometry, is that the subject "is connected to the relation between classical and quantum physics." The key to translating from the classical to the quantum domain is to describe a classical physics problem as a mathematical *variety*, a higher-dimensional shape characterized by a polynomial equation. [Here's a useful quote: "Science is the magic that actually works."]

Math. Mag. **93** (2020) 79–80. doi:10.1080/0025570X.2019.1684140

Öhman, Lars-Daniel, Are induction and well-ordering equivalent?, *Mathematical Intelligencer* 41 (3) (Fall 2019) 33–40; link.springer.com/article/10.1007/s00283-019-09898-4.

A meme common among mathematicians is that induction and well-ordering are equivalent: either can be proved from the other. The author points out that well-ordering as the fifth Peano postulate in place of induction does *not* give an equivalent axiom system: With induction, the Peano postulates are categorical, having only the natural numbers $\mathbb{N}$ as a model. With well-ordering, both $\mathbb{N}$ and the ordinals up to $\omega + \omega$ are models. The author investigates possible origins for the common misconception, citing the charitable explanations that "perhaps the intended sense is . . . that [they] are equally useful in proving theorems" in $\mathbb{N}$, or that for $\mathbb{N}$ "both principles are equally true."

Beineke, Jennifer, and Jason Rosenhouse, *The Mathematics of Various Entertaining Subjects, Vol. 3: The Magic of Mathematics*, Princeton University Press, 2019; xxi+325 pp, $125, $49.50(P). ISBN 978-0-691-18257-5, -18258-2.

The Mathematics of Various Entertaining Subjects (MOVES) conference takes place every other year at the National Museum of Mathematics in New York, with the presentations encapsulated in delightful books such as this one. Notable in this volume are "Probability in your head" (if six games are played in a World Series, which team is more likely to have won?); "Solving puzzles backward (how to finish an interrupted bridge deal if no one remembers where the last card was dealt); and "How to predict the flip of a coin" (has to be read to be believed!). Other topics include bingo (a diagonal is most likely to win), misère checkers (it's hard to lose!), Charles Sanders Peirce's card trick, "flexa-bands," and much more. [Perhaps a book devoted to mathematics of wide accessibility could have a more "popular" price.] [Note: Jason Rosenhouse is editor of This Magazine.]

Spiegelhalter, David, *The Art of Statistics: How to Learn from Data*, Basic Books, 2019; xvi+427 pp, $32. ISBN 978-1-5416-1851-0.

This leisurely walk through the main ideas in statistics, by a former president of the Royal Statistical Society, covers the usual ground unusually well. It "hooks" the reader with highlighted real questions that statistics can (try to) answer: How many trees are there on the planet? What happened to children having heart surgery in Bristol between 1984 and 1995? Does going to university increase the risk of getting brain cancer? Can we predict which passengers survived the sinking of the Titanic? Does listening to the Beatles' song "When I'm Sixty-Four" make you younger? Except for probability trees, no calculations are shown, and there are no exercises.

Montgomery, Richard, The three-body problem, *Scientific American* 321 (2) (August 2019) 66–73.

This article begins, "By the spring of 2014 I had largely given up on the three-body problem"—how three masses move in space under gravitation. Newton solved the two-body problem, but Poincaré showed that the three-body problem can involve chaotic dynamics. Label an eclipse among three bodies by the name of the body in the middle, and use the names to keep track of a sequence of eclipses. The sequence may or may not be periodic; if it is, is it the sequence of some periodic solution to the three-body problem? The author describes this question, which involves topology; work on it has almost led to an answer and hence to some solutions to the three-body problem.

Hart, Sarah, Ahab's arithmetic; or, the mathematics of *Moby-Dick*, arxiv.org/pdf/1903.12102.pdf; Mathematical quotations in Melville's *Moby-Dick*, eprints.bbk.ac.uk/26952/1/MathematicalQuotationsMobyDick.pdf.

It is many years since I read *Moby-Dick*, and I'm sure that at the time I did not realize the extent of mathematical allusions and imagery that occur in it. And I did not read Melville's *Mardi*, in which a character cries out, "Thou art harder to solve, than the Integral Calculus." Melville had an inspirational "ciphering" teacher before leaving school at age 12, and later he had a two-quarter crash course in engineering and surveying; but not securing a job in either field, he went to sea and then turned to writing. "A whale-ship was my Yale college and my Harvard." This article and its supplement enumerate Melville's mathematical references.