Vol. 89, No. 1, February 2016

MAA

MATHEMATICS MAGAZINE

- A wiring conundrum leads to Lights Out
- Matrix inverses viewed as permutations
- Delving deeper into the Chermak-Delgado Lattice
- An interview with woodcarver Bjarne Jespersen

EDITORIAL POLICY

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

Submissions of articles are required via the *Mathematics Magazine*'s Editorial Manager System. The name(s) of the author(s) should not appear in the file. Initial submissions in pdf or LaTeX form can be sent to the editor at www.editorialmanager.com/mathmag/.

The Editorial Manager System will cue the author for all required information concerning the paper. Questions concerning submission of papers can be addressed to the editor at mathmag@maa.org. Authors who use LaTeX are urged to use the Magazine article template. However, a LaTeX file that uses a generic article class with no custom formatting is acceptable. The template and the Guidelines for Authors can be downloaded from www.maa.org/pubs/mathmag.

MATHEMATICS MAGAZINE (ISSN 0025-570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, NW, Washington, DC 20036 and Lancaster, PA, in the months of February, April, June, October, and December.

Microfilmed issues may be obtained from University Microfilms International, Serials Bid Coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

Address advertising correspondence to

MAA Advertising
1529 Eighteenth St. NW
Washington, DC 20036
Phone: (202) 319-8461
E-mail: advertising@maa.org

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

Change of address, missing issue inquiries, and other subscription correspondence can be sent to:

The MAA Customer Service Center
P.O. Box 91112
Washington, DC 20090-1112
(800) 331-1622
(301) 617-7800
maaservice@maa.org

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

Postmaster: Send address changes to Membership/Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, NW, Washington, DC 20036-1385.

Printed in the United States of America.

COVER IMAGE

Zap © 2016 David A. Reimann (*Albion College*). Used by permission.

The article "A Confused Electrician Uses Smith Normal Form'' by Edgar and Sklar was the inspiration for this piece. The self-similar branching spark tree image was created using a stochastic subdivision algorithm.

Vol. 89, No. 1, February 2016

MAA

MATHEMATICS MAGAZINE

LETTER FROM THE EDITOR

The issue starts off with a real life conundrum about how a house was wired in an unintuitive way. Jessica Sklar and Tom Edgar consider the confused electrician problem, relating unintuitive wiring to the Lights Out game and its variations. This article was also the inspiration for this issue's cover art by David Reimann.

The second article reminds me of an assignment from my high school Pascal programming class in academic year 1984–85. Franklin Mendivil and Jeff Hooper consider a permutation defined by where the entries of a matrix are positioned in the transpose of the matrix. They ask how one can determine the permutation only given the size of the matrix. The answer touches on group theory and number theory, including the Chinese remainder theorem. Unfortunately, there was no mention of group theory in my Pascal class; this was a missed opportunity.

Elizabeth Wilcox channels Lewis Carroll and describes an adventure down a rabbit hole. This hole leads to the land of the Chermak–Delgado lattice and includes a number of challenges for the reader to complete as an introduction to this subgroup lattice. The article concludes with a number of additional challenges in the form of unsolved problems.

There are many visual proofs of the Pythagorean theorem. In recognizing that the Pythagorean theorem is just a special case of the cosine rule, Burkard Polster and Marty Ross consider Pythagorean-like visual proofs for the cosine rule in which one angle measures either 60 or 120 degrees. They use the results to revisit the Pythagorean case and consider other extensions.

Spliced in between the articles are proofs without words by Roger Nelsen, Angel Plaza, and Óscar Ciaurri. Images of artwork are spread throughout the issue, too. These accompany Amy and David Reimann's interview with artist Bjarne Jespersen, who is known for carving wooden spheres.

This marks the first issue with Eduardo Dueñez of the University of Texas at San Antonio as the Problems Editor of this MAGAZINE. Welcome, Eduardo! There are some additional changes in the Problems department. Eugen J. Ionascu of Columbus State University is now the Proposals Editor. Additionally, Ricardo A. Saenz of the Universidad de Colima, México has been named an Assistant Editor. The latest batch of problems, quickies, and solutions make up the Problems section.

The Reviews section includes a look at recent progress in finding faster algorithms for NP-hard problems by applying algebraic methods, provides information about two relatively new publications in recreational mathematics, and covers a book in which algorithms meet recreational math via the tower of Hanoi. Additional reviews involve Islamic art, mathematical fiction, ethics and mathematical finance, and gambling.

The issue concludes with solutions to the twelve problems from the 76th Annual William Lowell Putnam Mathematical Competition that was held December 5, 2015. The problems are listed first, so challenge yourself and see if you could solve some of the problems before looking at the solutions!

Michael A. Jones, Editor

ARTICLES

A Confused Electrician Uses Smith Normal Form

TOM EDGAR
Pacific Lutheran University
Tacoma, WA 98447-0003
edgartj@plu.edu

JESSICA K. SKLAR
Pacific Lutheran University
Tacoma, WA 98447-0003
sklarjk@plu.edu

Several years ago, Jessica moved into a quirky home. Among its mysteries were a set of floodlights she was unable to turn on and a closet lamp that seemed to have a surplus of switches: both a light toggle in the closet and a chain hanging from the lamp turned the light on and off. Eventually, Jessica called an electrician. After serious study, he solved the puzzle: The light toggle switched the states of both the closet lamp AND the floodlights between on and off. So if the floodlights were on and the closet lamp were off, to turn them all off the electrician would have to both flip the light switch (turning the floodlights off and the closet lamp on), and then yank the chain (turning the closet lamp off).

This scenario provides a simple example of what we will call a "confused electrician game." Imagine that an electrician happens upon a collection of n lamps. For each $i = 1, 2 \ldots, n$, lamp i has $L_i > 1$ levels of brightness, ranging from brightness level 0, corresponding to the lamp being off, to brightness level $L_i - 1$, corresponding to the lamp being in its brightest state. The lamps are initially set to varied brightness levels (we call this configuration the initial state), and the electrician would like to simultaneously change the brightness levels to achieve another (usually different) brightness configuration (called the final state). Now, each lamp comes equipped with a button. However, there's a catch: pressing the button on lamp j (henceforth referred to as *button* j) adjusts the brightness of a subcollection of the n lamps, which may or may not contain lamp j itself. Specifically, pressing button j increments the brightness level of lamp i ($i = 1, 2, \ldots, n$) by a fixed nonnegative integer $b_{i,j}$, where we increment modulo L_i: when the lamp is at its brightest level, $L_i - 1$, "increasing" this level by 1 actually turns the lamp off.

Since the wiring between lamps and buttons is so bizarre, the electrician is confused about how to achieve the desired final state; can she do it, and if so what buttons should she press? For instance, Figure 1 contains a diagram depicting a confused electrician game with three lamps. Lamp 1 has three brightness levels, lamp 2 has five brightness levels, and lamp 3 has seven brightness levels. Each button is connected to some lamps via wires (drawn as blue dashed lines), and pressing a button increments the brightness levels of the connected lamps by the integer labeling the wire. For instance, pressing button 1 increments the brightness of lamp 1 by one and lamp 2 by three, while not

Math. Mag. **89** (2016) 3–13. doi:10.4169/math.mag.89.1.3.
MSC: Primary 11A07, Secondary 15A06; 15A33.

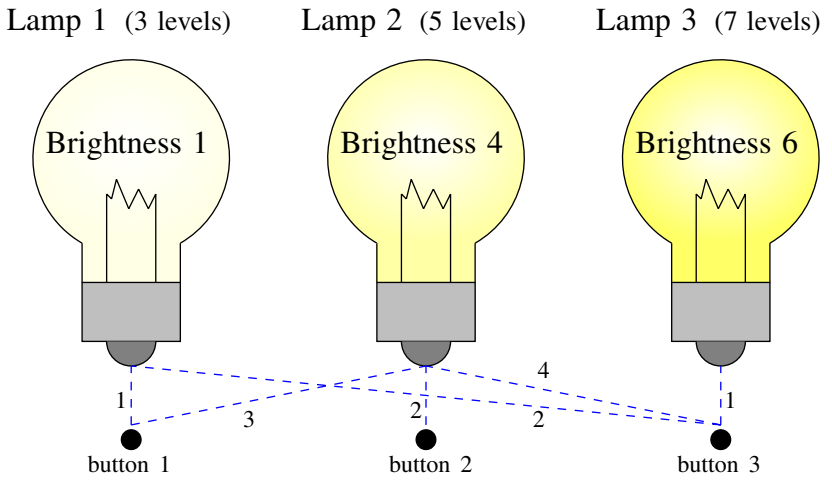


Figure 1 An example of a confused electrician game.

affecting lamp 3. In the beginning, lamps 1–3 are at brightness levels 1, 4, and 6, respectively. Can the electrician turn off all of the lamps using these buttons? We leave this as an exercise for the reader. (A solution is provided in an Appendix at the end of this paper.)

Many problems and games appearing in mathematics literature can be interpreted as confused electrician games. Perhaps the most famous of these is "Lights Out," an electronic game released by Tiger Toys in 1995, which was described mathematically in [**1**]. A precursor of Lights Out, called "Magic Square," was a collection of games programmed into *Merlin, the Electronic Wizard,* an electronic game released by Parker Brothers in 1978 (see [**7**], [**10**], [**12**], and [**16**]). And a variety of more recently produced computer games, including "Myst," "The Longest Journey," "Timelapse," and "Call of Duty: Black Ops," include cleverly disguised examples of these games (see [**13**] and [**9**]). We join the ranks of those studying Lights Out and related games (see, for example, [**17**], [**8**], [**11**], [**4**], [**2**], and [**5**]), providing a universal method for determining the existence of solutions to confused electrician games.

Modeling Confused Electrician games Throughout, let $\mathbb{Z}$ be the set of integers, $\mathbb{Z}^+$ the set $\{1, 2, \ldots\}$ of positive integers, and $\mathbb{N}$ the set $\{0, 1, \ldots\}$ of natural numbers. For each $n \in \mathbb{Z}^+$, we denote by $\mathbb{Z}^n$ the group

$$\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ copies}}.$$

Finally, for each $n \in \mathbb{Z}^+$, we let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, noting that $\mathbb{Z}_n$ is a group under addition modulo n.

We now review some graph theory concepts. (See, for instance, [**18**] or [**19**] for a more thorough discussion of graph theory.) Recall that a *directed graph* or *digraph* $\Gamma = (V, E)$ consists of a set V of *vertices* and set $E \subseteq V \times V$ of *(directed) edges*. Notice that our definition of digraphs allows a loop from a vertex to itself, but does not allow multiple edges from one vertex to another. A digraph is *finite* if V is finite, and a digraph Γ is $\mathbb{Z}^+$*-weighted* if we assign to each edge in Γ a unique positive integer, called the edge's *weight*. We will draw weighted digraphs by letting integers represent vertices and integer-labeled arrows represent edges. If, for two vertices v and w, there is an edge from v to w and an edge from w to v that share a common weight, we instead draw a single bi-directed arrow between v and w.

Digraphs play a central role in confused electrician games; in fact, we will call a finite $\mathbb{Z}^+$-weighted digraph a *confused electrician graph*, or *CE-graph*. In turn, a *confused electrician game*, or *CE-game*, is a tuple

$$\left(\Gamma, \{G_i\}_{i=1}^n, s, f\right),$$

where

- Γ is a CE-graph with vertex set $\{1, 2, \ldots, n\}$;
- Each G_i is a finite cyclic group; and
- $s, f \in \bigoplus_{i=1}^n G_i$.

Given such a game, we call each G_i a *vertex group*, and $G := \bigoplus_{i=1}^n G_i$ the *board space* of the game. Note that G is a group under the operation that is determined, coordinatewise, by the operations in the G_i; since G is Abelian, we will denote its operation by $+$. We call the elements of G *board states*; s and f are, respectively, the game's *initial* and *final* states.

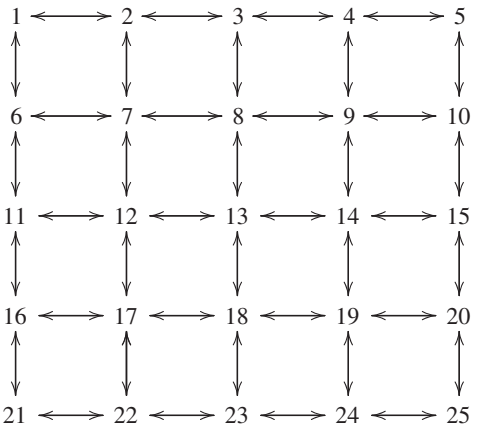
From a confused electrician's perspective, n is the number of lamps, and each $G_i = \mathbb{Z}_{L_i}$, where L_i is the number of brightness levels of lamp i. The lamps initially have the brightness levels indicated by s, and the electrician wishes to obtain the brightness levels indicated by f. The edge weights in Γ encode the effects of pressing buttons. In particular, if the edge from vertex j to vertex i has weight $b_{i,j}$, then pressing button j increments the brightness of lamp i by $b_{i,j}$, modulo L_i.

Examples of CE-games We now provide just a few examples of the many puzzles that can be interpreted as CE-games. The graphs associated with the following games are provided in Figure 2.

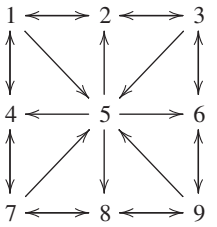
1. Lights Out is a collection of CE-games where Γ is the 5×5 lattice with loops added at each vertex and with each edge having weight 1. Moreover, each vertex group is $\mathbb{Z}_2$, so $G = \mathbb{Z}_2^{25}$. The initial states vary from game to game, but the final state is always $(0, 0, \ldots, 0)$. Note that this means that the goal of each game is to turn off all of the lamps.
2. Merlin's Magic Square is a collection of CE-games where Γ is as pictured in Figure 2, with loops added at each vertex and with each edge having weight 1. Again, each vertex group in a Magic Square game is $\mathbb{Z}_2$, and the games have varying initial states. However, the final state is always $(1, 1, 1, 1, 0, 1, 1, 1, 1)$; that is, the goal of the game is always to have only the middle light off.
3. Several games described in [**13**] can be modeled by CE-games. In particular, Timelapse's Mayan Calendar puzzles can be interpreted as CE-games with three distinct vertex groups. The associated CE-graph Γ is as shown in Figure 2, with loops of weight 1 added at each vertex. In these games, $G_1 = \mathbb{Z}_8$, $G_2 = \mathbb{Z}_{12}$, and $G_3 = \mathbb{Z}_{16}$, while s and f vary from game to game.
4. Two puzzles from Call of Duty: Black Ops that appear in [**9**] can be modeled as CE-games. Their graphs are as shown in Figure 2, with loops weighted by 1 added at each vertex. In both cases, each vertex group is $\mathbb{Z}_{10}$, $s = (8, 8, 4, 5)$, and $f = (2, 7, 4, 6)$.

Winning Confused Electrician games So how does a confused electrician go about trying to win a CE-game? Recall that if the edge from vertex j to vertex i has weight $b_{i,j}$, then pressing button j increments the brightness of lamp i by $b_{i,j}$ (mod L_i). If there is no edge from vertex j to vertex i, we let $b_{i,j} = 0$. Then, for each $j = 1, 2, \ldots, n$, we define a vector

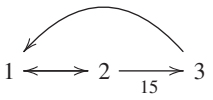
$$b_j = (b_{1,j}, b_{2,j}, \ldots, b_{n,j}) \in \mathbb{Z}^n,$$



Lights Out

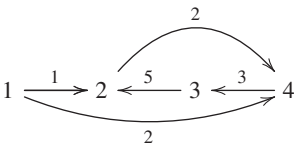


Merlin's Magic Square



Timelapse's Mayan Calendar

Call of Duty: Black Ops (#1)



Call of Duty: Black Ops (#2)

Figure 2 The CE-graphs for five CE-games. All loops have been omitted and all nonlabeled have weight 1.

which we call the *button vector* of vertex j.* For example, in Lights Out, the button vector of vertex 7 is

$$b_7 = (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \in \mathbb{Z}^{25},$$

and in Merlin's Magic Square, the button vector of vertex 3 is

$$b_3 = (0, 1, 1, 0, 1, 1, 0, 0, 0) \in \mathbb{Z}^9.$$

*While it is usually most useful for us to think of each b_j as a column vector, for the sake of appearances, we will often typeset such vectors as n-tuples, and not bother using transpose notation in those cases.

A CE-game can be won if and only if there exists a finite sequence of buttons the electrician can push that will move the game into its final state. Since addition in G is commutative, if we start in a state and press button i and then button j, we obtain the same state we would have obtained by pressing the buttons in the opposite order. So performing any finite sequence of button presses corresponds to adding an $\mathbb{N}$-linear combination of the game's button vectors to the game's current state. Thus, letting π be the canonical projection from $\mathbb{Z}^n$ to G, we say a CE-game $\left(\Gamma, \{G_i\}_{i=1}^n, s, f\right)$ is *winnable* if there exists an $\mathbb{N}$-linear combination p of button vectors such that

$$s + \pi(p) = f.$$

In this case, we call p a *solution* for the game.

In order to demonstrate the ideas from the previous paragraph, consider the Magic Square game with initial state

$$s = (0, 0, 1, 0, 0, 0, 0, 1, 1),$$

and desired final state

$$f = (1, 1, 1, 1, 0, 1, 1, 1, 1).$$

This game can be won by pressing buttons 1, 8, and 9, since in $\mathbb{Z}_2^9$,

$$s + \pi(b_1 + b_8 + b_9) = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \pi\left(\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = f.$$

We now build machinery we can use to win a CE-game $(\Gamma, \{G_i\}_{i=1}^n, s, f)$. First, for simplicity, we define $\delta \in G$ by $\delta = f - s$. As indicated above, a CE-game is winnable if and only if there exists a collection of nonnegative integers $\{\lambda_i\}_{i=1}^n$, such that

$$s + \pi(\lambda_1 b_1 + \cdots + \lambda_n b_n) = f,$$

that is, such that

$$\pi(\lambda_1 b_1 + \cdots + \lambda_n b_n) = \delta.$$

We note that λ_i represents the number of times we must press button i in order to win the game.

Finding integer solutions to the equation

$$\pi(x_1 b_1 + \cdots + x_n b_n) = \delta$$

is equivalent to finding integers that solve the simultaneous system of congruences

$$\begin{aligned} x_1 b_{1,1} + \cdots + x_n b_{1,n} &\equiv \delta_1 \pmod{L_1} \\ &\vdots \\ x_1 b_{n,1} + \cdots + x_n b_{n,n} &\equiv \delta_n \pmod{L_n}, \end{aligned} \tag{1}$$

where δ_i is the ith coordinate of δ.

Note that a solution to this mathematical system may contain negative integers, which would mean that it does not represent a viable solution for the game (as one cannot press a button a negative number of times). However, if M is the least common multiple of the brightness levels $L_1, L_2, \ldots, L_n$, and $\overline{M}$ the element of $\mathbb{Z}^n$ with each entry equal to M, then we see that an element $\lambda \in \mathbb{Z}^n$ solves the system if and only if $\lambda + \overline{M}$ solves the system; consequently, a solution with negative entries can be replaced by a solution with all nonnegative entries by adding an appropriate integer multiple of $\overline{M}$. Thus, we have the following theorem:

Theorem 1. *A CE-game is winnable if and only if its corresponding system of congruences, as described in (1), has a solution in* $\mathbb{Z}^n$.

The optimal technique used to solve a game's system varies from game to game. In most of the games we've mentioned, each vertex group is the same; indeed in the Lights Out and Magic Square games each G_i is $\mathbb{Z}_2$; in the Myst puzzle and in one of the Timelapse puzzles discussed in [**13**], each $G_i = \mathbb{Z}_3$; and in Call of Duty: Black Ops, each $G_i = \mathbb{Z}_{10}$. If each congruence involves the same prime modulus, we can use basic linear algebraic techniques to solve the system. Even if the congruences utilize the same composite modulus, standard matrix methods may still suffice (see [**9**]).

When the vertex groups vary, as they do in the Timelapse Mayan Calendar games, we may have to do a little more work. The systems of congruences corresponding to the Mayan Calendar games are simple enough that they are relatively easily solved via brute force, but we will see later that this method may be impractical for solving an arbitrary CE-game when Γ contains many vertices or when the L_i are large.

A sufficient condition for winning a CE-game The following lemma, whose straightforward proof is left to the reader, provides a method that will allow us to solve some systems of linear congruences involving differing moduli.

Lemma 2. *Let* $\{\lambda_i\}_{i=1}^n$ *and* $\{a_i\}_{i=1}^n$ *be collections of n integers, and let v be an integer. Then for any integer multiple M of L,*

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \equiv v \pmod{L}$$

if

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \equiv v \pmod{M}.$$

Applying this lemma with $M := \operatorname{lcm}(L_1, \ldots, L_n)$, we conclude that the system of congruences described in (1) will have a solution if the system

$$\begin{aligned} x_1 b_{1,1} + \cdots + x_n b_{1,n} &\equiv \delta_1 \pmod{M} \\ &\vdots \\ x_1 b_{n,1} + \cdots + x_n b_{n,n} &\equiv \delta_n \pmod{M} \end{aligned} \tag{2}$$

has a solution. We call the latter system of congruences the *uniform-group system* of the game.

Notice that the lemma only provides a *sufficient* condition for existence of a solution to the original system. The converse of the lemma does not hold; even if the modified system does not have a solution, the original system may still have a solution. We provide an example of this below.

Now we can use a computer-algebra system to solve a CE-game assuming its uniform-group system of congruences has a solution. In particular, the open-source

software Sage ([**14**]) provides a command "`solve_mod`" that will solve such systems of congruences. For instance, revisiting our Merlin Magic Square example from the previous section, we have

$$\begin{aligned}\delta &= f - s \\ &= (1,1,1,1,0,1,1,1,1) - (0,0,1,0,0,0,0,1,1) \\ &= (1,1,0,1,0,1,1,0,0).\end{aligned}$$

We can read off $b_1, \ldots, b_9$ from the Magic Square digraph (Figure 2). In this case, each $L_i = 2$, so we use $M = 2$. We then use Sage's `solve_mod` command, with modulus 2, to obtain the result $(1, 0, 0, 0, 0, 0, 0, 1, 1)$. Thus, one solution to the game is given by letting $x_1 = x_8 = x_9 = 1$, and letting every other variable equal 0. (Note: We could also have solved this system by inverting the matrix $\begin{bmatrix} b_1 & b_2 & \cdots & b_n \end{bmatrix}$ over $\mathbb{Z}_2$ and multiplying by δ.)

Unfortunately, the previous technique doesn't always work. For example, consider the Timelapse Mayan Calendar game with $s = (4, 10, 12)$ and $f = (0, 0, 0)$, so that

$$\delta = (0,0,0) - (4,10,12) = (4,2,4) \in \mathbb{Z}_8 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{16}.$$

In this game we have $b_1 = (1, 1, 0)$, $b_2 = (1, 1, 15)$, and $b_3 = (1, 0, 1)$, giving us the following system of congruences to solve:

$$\begin{aligned} x_1 + x_2 + x_3 &\equiv 4 \pmod 8 \\ x_1 + x_2 &\equiv 2 \pmod{12} \\ 15x_2 + x_3 &\equiv 4 \pmod{16}. \end{aligned}$$

In this game, $M = \operatorname{lcm}(8, 12, 16) = 48$. As in the previous example, we use Sage's `solve_mod` command, but this time it provides no solutions. Does this mean that the game is not winnable? *Not necessarily.* Indeed, there is no solution to the uniform-group system; however, one can confirm that $x_1 = 12$, $x_2 = 2$, and $x_3 = 38$ is a solution to the original system. Unfortunately, Lemma 2 does not provide us with this solution.

A necessary condition for winning a CE-game In order to find a solution for the game in the previous example, we determine a necessary condition for the existence of a solution to a system of equations with differing moduli. Suppose we have a fixed CE-game $(\Gamma, \{G_i\}_{i=1}^n, s, f)$. If we let $M = \operatorname{lcm}(L_1, \ldots, L_n)$, then we have $2 \le L_i \le M$ for each i. Thus we can interpret each L_i as being an element of the finite group $\mathbb{Z}_M$, where if $L_i = M$ in $\mathbb{Z}$ we of course interpret it as the element 0 in $\mathbb{Z}_M$. We let $\langle L_i \rangle$ represent the cyclic subgroup of $\mathbb{Z}_M$ generated by L_i. For example, when $L_1 = 2$, $L_2 = 3$, and $L_3 = 4$, we have $M = \operatorname{lcm}(2, 3, 4) = 12$, and, for instance, $\langle L_1 \rangle = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$ in $\mathbb{Z}_{12}$. Finally, we note that since $0 \le \delta_i < L_i$ for each i, we can also interpret each δ_i as an element of $\mathbb{Z}_M$.

This terminology allows us to improve Lemma 2.

Theorem 3. *Let $\{\lambda_i\}_{i=1}^n$ and $\{a_i\}_{i=1}^n$ be collections of n integers, and let v be an integer. Then for any integer multiple M of L,*

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \equiv v \pmod L$$

if and only if

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \equiv w \pmod M$$

for some $w \in v + \langle L \rangle$ in $\mathbb{Z}_M$.

Note that the order of $\langle L \rangle$ in $\mathbb{Z}_M$ is M/L, so there are only finitely many possibilities for w. Indeed, each w equals $v + kL$ for some $0 \leq k < M/L$.

This theorem allows us to find a solution for our Mayan Calendar game with $s = (4, 10, 12)$ and $f = (0, 0, 0)$. Recall that we must solve the system

$$\begin{aligned} x_1 + x_2 + x_3 &\equiv 4 \pmod 8 \\ x_1 + x_2 &\equiv 2 \pmod{12} \\ 15x_2 + x_3 &\equiv 4 \pmod{16}. \end{aligned}$$

By Theorem 3, this is equivalent to solving some system of the form

$$\begin{aligned} x_1 + x_2 + x_3 &\equiv 4 + 8k_1 \pmod{48} \\ x_1 + x_2 &\equiv 2 + 12k_2 \pmod{48} \\ 15x_2 + x_3 &\equiv 4 + 16k_3 \pmod{48}, \end{aligned}$$

where $k_1, k_2, k_3 \in \mathbb{Z}$ with $0 \leq k_1 < 6$, $0 \leq k_2 < 4$, and $0 \leq k_3 < 3$. Using Sage to solve all 72 such systems, we obtain, for instance, the solution $(12, 2, 38)$, when $k_1 = 0$, $k_2 = 1$, and $k_3 = 1$. There may be other solutions as well.

Classifying winnable CE-games using Smith normal form In the previous section, we demonstrated that we can numerically solve a CE-game using a computer algebra system such as Sage. However, our method relies on using the Sage "black box" command `solve_mod`: the actual mathematics used to solve a uniform-group system remains "hidden" in Sage's internal programming. Moreover, the following example shows that using Sage is inefficient when either the vertex groups or n are relatively large.

Suppose, for instance, that we use the Petersen graph (Figure 3) as the CE-graph of a CE-game where each $G_i = \mathbb{Z}_{20}$, $s = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$, and $f = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$. (Note that in this graph, there are no loops at vertices; the edges in the graph are exactly those pictured in the figure.) It takes the built-in feature in Sage approximately 21 *minutes* to solve the corresponding system of inequalities (modulo 20)!

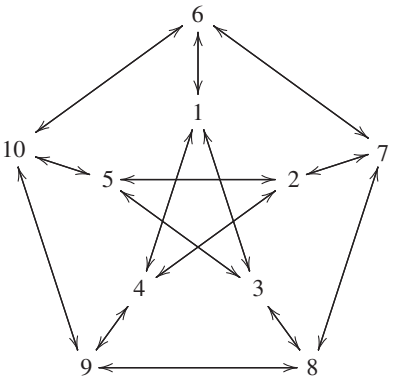


Figure 3 The Petersen graph.

So let's discuss a method to *efficiently* solve arbitrary CE-games. Given a CE-game with button vectors $b_1, b_2, \ldots, b_n$, we let B be the $n \times n$ matrix with jth column b_j; we call this the *button matrix* of the game. We note that the button matrix of a CE-game is

an integer matrix; specifically, it is the weighted adjacency matrix of the corresponding CE-graph.

For the remainder of this section, we fix a CE-game $\left(\Gamma, \{G_i\}_{i=1}^n, s, f\right)$, with each $G_i = \mathbb{Z}_{L_i}$ and with button matrix B. We again let M be the least common multiple of the L_i.

Since $\mathbb{Z}^n$ and $\mathbb{Z}_M^n$ are both $\mathbb{Z}$-modules, they are also modules over the ring of $n \times n$ integer matrices. For each $y \in \mathbb{Z}^n$, By is also an element of $\mathbb{Z}^n$, and so $\pi(By) \in G$. Similarly, for each $z \in \mathbb{Z}_M^n$, $Bz \in \mathbb{Z}_M^n$. Using this language, the following result follows immediately from Theorem 1.

Lemma 4. *The CE-game with button matrix B is winnable if and only if the equation $\pi(Bx) = \delta$ has a solution in $\mathbb{Z}^n$.*

Since M may not be prime or B may not be invertible over $\mathbb{Z}_M$, in order to find solutions of this new equation we will write B in a particular form. Any integer matrix C can be written in the form $C = UDV$, where U, D, and V are integer matrices satisfying the following two properties:

- Both U and V are invertible over $\mathbb{Z}$ (that is, each has determinant ± 1).
- The matrix D is diagonal of the form

$$\operatorname{diag}(a_1, a_2, \ldots, a_k, 0, 0, \ldots, 0) := \begin{bmatrix} a_1 & 0 & 0 & & \cdots & & 0 \\ 0 & a_2 & 0 & & \cdots & & 0 \\ 0 & 0 & \ddots & & & & 0 \\ \vdots & & & a_k & & & \vdots \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & \cdots & & & 0 \end{bmatrix},$$

where a_i evenly divides a_{i+1}, for each i.

This form for C is known as its *Smith normal form*, and the numbers $a_1, \ldots, a_k$ are known as the *elementary divisors* of C. (The process for computing U, V, and D is relatively straightforward, but outside of the scope of this paper; for more information see [**3**].)

Suppose that UDV is the Smith normal form for integral matrix B. For each $i \in \{1, 2, \ldots, n\}$, we let e_i be the vector in $\mathbb{Z}_M^n$ with ith coordinate equal to 1 and every other coordinate equal to 0. We next let S be the subgroup of $\mathbb{Z}_M^n$ generated by the set $\{L_1 e_1, L_2 e_2, \ldots, L_n e_n\}$, and let A be the subgroup of $\mathbb{Z}_M^n$ generated by the set $\{a_1 e_1, a_2 e_2, \ldots, a_k e_k\}$, where the a_i's are the elementary divisors of B. Recall that we can interpret δ as an element of $\mathbb{Z}_M^n$ so that $U^{-1}\delta + U^{-1}(S)$ is a subset of $\mathbb{Z}_M^n$. Then we have the following.

Theorem 5. *The equation $\pi(Bx) = \delta$ has a solution in $\mathbb{Z}^n$ if and only if $A \cap (U^{-1}\delta + U^{-1}(S)) \neq \emptyset$.*

Indeed, suppose there exists $w \in A \cap (U^{-1}\delta + U^{-1}(S))$: that is, assume there is an element w in $U^{-1}\delta + U^{-1}(S)$ of the form

$$w = (\lambda_1 a_1, \lambda_2 a_2, \ldots, \lambda_k a_k, 0, \ldots, 0),$$

where each $\lambda_i \in \mathbb{Z}$. We let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k, 0, \ldots, 0) \in \mathbb{Z}^n$. Now in $\mathbb{Z}^n$, each coordinate of $D\lambda$ is congruent, modulo M, to the corresponding coordinate of w. Let

$$y := V^{-1}\lambda \in \mathbb{Z}^n.$$

Then in $\mathbb{Z}^n$,

$$By = (UDV)y = UD(Vy) = UD\lambda,$$

and thus By is congruent, coordinatewise modulo M, to Uw. Finally, $Uw \in \delta + S$, which implies that the ith coordinate of Uw is congruent, modulo L_i, to δ_i. Thus, the ith coordinate of By is congruent, modulo L_i, to δ_i, and so we have $\pi(By) = \delta$.

A similar argument, along with Theorem 3, yields that if $y \in \mathbb{Z}^n$ solves the equation $\pi(Bx) = \delta$, then $A \cap (U^{-1}\delta + U^{-1}(S)) \neq \emptyset$.

Once we have $y \in \mathbb{Z}^n$ satisfying $\pi(By) = \delta$, we see that every element of the form $y + V^{-1}v \in \mathbb{Z}^n$, where $Dv = 0$, also solves the equation $\pi(Bx) = \delta$. We can of course then obtain a solution of the CE-game—that is, an element in $\mathbb{N}^n$ solving $\pi(Bx) = \delta$—by adding an appropriate integer multiple of $\overline{M}$ to any of those solutions.

We can use Sage to quickly produce the Smith normal form UDV of the button matrix for the Petersen graph in order to find a solution to the CE-game described at the beginning of this section. In this case, $S = \{(0, 0, 0, 0, 0, 0, 0, 0, 0, 0)\}$ and $D = \text{diag}(1, 1, 1, 1, 1, 1, 2, 2, 2, 6)$, so we only need to check that the ith coordinate of $U^{-1}\delta$ is in the cyclic subgroup of $\mathbb{Z}_{20}$ that is generated by a_i; in particular, we only need to check the last four coordinates of $U^{-1}\delta$, since 1 is a generator of $\mathbb{Z}_{20}$. Then, using the ideas presented in this section, a simple for-loop will find a solution to the game (if one exists). In particular, one solution for this game is

$$(13, 13, 13, 13, 13, 13, 13, 13, 13, 13).$$

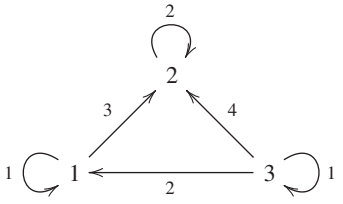
For this example, the entire process in Sage takes approximately 0.01 *seconds*.

For CE-games with nontrivial S, a little extra programming is required in order to find an element in $A \cap (U^{-1}\delta \cap U^{-1}(S))$ (or determine that no such element exists). Unfortunately, as S gets larger, the computation time gets longer using this method or the brute-force method. If S gets too large, both computational methods may be impractical, but using the Smith normal form will still generally be more efficient than solving the associated system of congruences.

Thus, we see that when a CE-game involves many lamps, or its lamps have many brightness levels, the brute force method of checking all possible solutions to the game can be wildly inefficient, while one can quickly solve the game using the Smith normal form of the button matrix. Finally, the result in Theorem 5 also allows us to construct initial and final states for a given CE-graph that will yield a winnable CE-game.

Appendix

The CE-game pictured in Figure 1 has the following CE-graph, with $G_1 = \mathbb{Z}_3$, $G_2 = \mathbb{Z}_5$, $G_3 = \mathbb{Z}_7$, $s = (1, 4, 6)$, and $f = (0, 0, 0)$.



Thus, $\delta = (2, 1, 1)$, and the button matrix is given by

$$B = \begin{bmatrix} 1 & 0 & 2 \\ 3 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix}.$$

Now, we can check that $y = (0, 1, 1)$ is a solution since

$$\begin{bmatrix} 1 & 0 & 2 \\ 3 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 6 \\ 1 \end{bmatrix},$$

which is equivalent, coordinatewise, to $(2, 1, 1)$. Thus, $\pi(By) = \delta$.

REFERENCES

1. M. Anderson, T. Feil, Turning Lights Out with linear algebra, *Math. Mag.* **71** no. 5 (1998) 300–303.
2. C. Arangala, M. MacDonald, R. Wilson, Multistate Lights Out, *Pi Mu Epsilon J.* **14** no. 1 (2014) 9–18.
3. D. S. Dummit, R. M. Foote, *Abstract Algebra.* Third edition. Wiley, Hoboken, NJ, 2003.
4. S. Edwards, V. Elandt, N. James, K. Johnson, Z. Mitchell, D. Stephenson, Lights Out on finite graphs, *Involve* **3** no. 1 (2010) 17–32.
5. R. Fleischer, J. Yu., A survey of the game "Lights Out!," *Space-Efficient Data Structures, Streams, and Algorithms*. Lecture Notes in Computer Science, Vol. 8066, Springer, Heidelberg, 2013. pp. 176–198.
6. J. B. Fraleigh, *A First Course in Abstract Algebra.* Seventh edition. Addison Wesley, Reading, MA, 2002.
7. R. A. Gibbs, Merlin^{TM} and the Magic Square, *Math. Teacher* **75** no. 1 (1982) 78–81.
8. A. Giffen, D. B. Parker, On generalizing the "Lights Out" game and a generalization of parity domination, *Ars Combin.* **111** (2013) 273–288.
9. H. Hulsizer, A Mod'ern mathematical adventure in "Call of Duty: Black Ops," *Math Horiz.* **21** no.3 (2014) 12–15.
10. J. Missigman, R. Weida, An easy solution to mini Lights Out, *Math. Mag.* **74** no. 1 (2001) 57–59.
11. T. Muetze, Generalized switch-setting problems, *Discrete Math.* **307** no. 22 (2007) 2755–2770.
12. D. Pelletier, Merlin's Magic Square, *Amer. Math. Monthly* **94** no. 2 (1987) 143–150.
13. J. Sklar, Dials and levers and glyphs, oh my! Linear algebra solutions to computer game puzzles, *Math. Mag.* **79** no. 5 (2006) 360–367.
14. W. A. Stein et al., *Sage Mathematics Software (Version 6.2)*, The Sage Development Team, 2014, http://www.sagemath.org.
15. W. A. Stein et al., *Sage's Version 6.2 Reference Manual*, The Sage Development Team, 2014, http://www.sagemath.org/doc/reference.
16. D. L. Stock, Merlin's Magic Square revisited, *Amer. Math. Monthly* **96** no. 7 (1989) 608–610.
17. B. Torrence, R. Torrence, Lights Out on Petersen graphs, 2013, http://graphics8.nytimes.com/packages/blogs/images/LightsOutPetersen-Torrence2B.pdf.
18. D. B. West, *Introduction to Graph Theory*. Second edition. Prentice-Hall, Englewood Cliffs, 2000.
19. R. J. Wilson, J. J. Watkins, *Graphs: An Introductory Approach—A First Course in Discrete Mathematics*. Wiley, New York, 1990.

Summary. In this paper we define "confused electrician games," which generalize "Lights Out," a game popular in mathematical literature. In addition to "Lights Out," many more recent computer game puzzles can be modeled as confused electrician games. We provide examples of this, and explain how to solve such games using the Smith normal form of a matrix. We note that in many cases, this method is very efficient compared to another, more obvious, method.

TOM EDGAR (MR Author ID: 821633) received his Ph.D. from the University of Notre Dame and is an associate professor at Pacific Lutheran University in Tacoma, WA. He enjoys working on mathematics that is accessible to and fun for undergraduates. He hopes that this note inspires readers to look for games that can be modeled as CE-games and will lead to projects with undergraduates.

JESSICA K. SKLAR (MR Author ID: 630459) received her Ph.D. in Mathematics from the University of Oregon in 2001, and currently serves as chair of the Department of Mathematics at Pacific Lutheran University. She loves recreational mathematics, and hopes this work will allow her to more easily deal with the kooky wiring in her home.

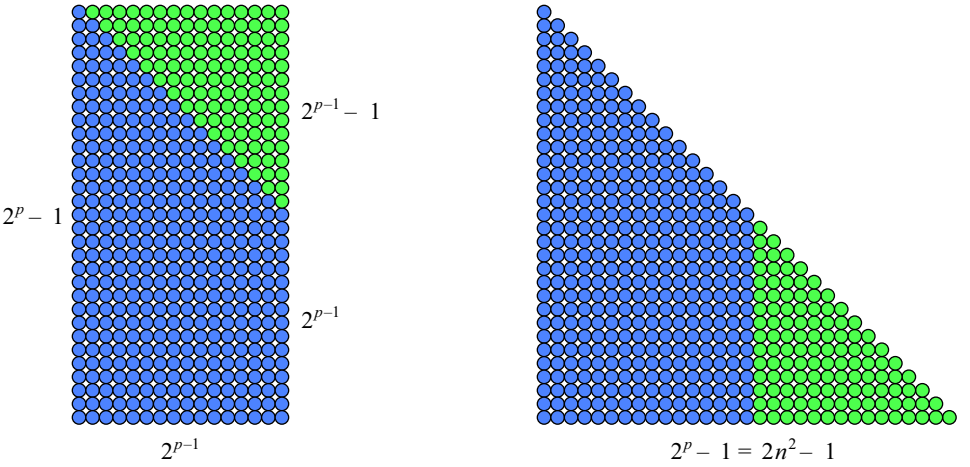
Proof Without Words: Perfect Numbers and Sums of Odd Cubes

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

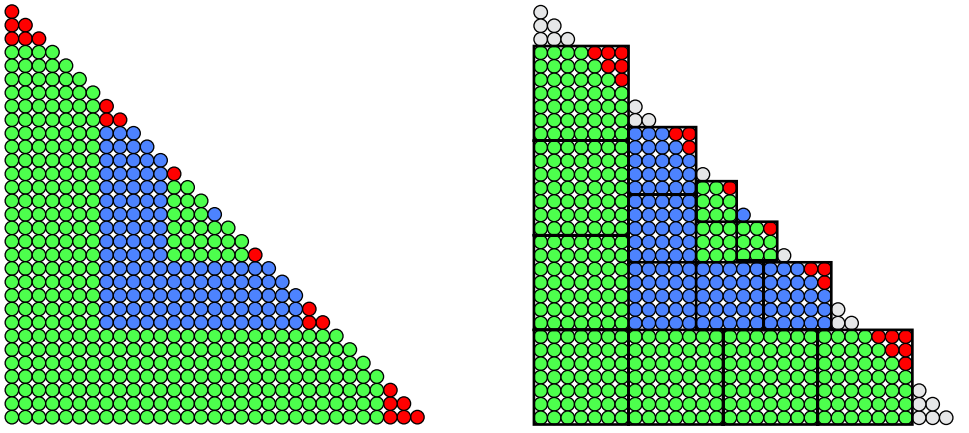
Theorem. *Every even perfect number* $N_p = 2^{p-1}(2^p - 1)$ *with* $p \geq 3$ *prime is the sum of the first n odd cubes for* $n = 2^{(p-1)/2}$, *i.e.,* $N_p = 1^3 + 3^3 + \cdots + (2n-1)^3$ [**1**].

Proof: (e.g., for $p = 5$, $N_5 = 16 \cdot 31$ and $n = 4$): Let $T_k = 1 + 2 + \cdots + k = k(k+1)/2$ denote the k^{th} triangular number. Then

1. $N_p = 2^{p-1}(2^p - 1) = T_{2n^2-1}$.



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



■

Math. Mag. **89** (2016) 14–15. doi:10.4169/math.mag.89.1.14.
MSC: Primary 11A25, Secondary 05A15

The theorem actually holds for $p \geq 3$ *odd*, whether or not p or $2^p - 1$ is prime.

REFERENCE

1. S. Kahan, Perfectly odd cubes, *Math. Mag.* **71** (1998) 131.

Summary. We show wordlessly that every even perfect number greater than six is a sum of consecutive odd cubes.

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

Artist Spotlight
Bjarne Jespersen

Flexus, Bjarne Jespersen; Mahogany, 5 cm in diameter, 1971; private collection. Four three-sided hosohedral edge frames weave together.

See interview on page 55.

Transposition as a Permutation: A Tale of Group Actions and Modular Arithmetic

JEFF HOOPER
FRANKLIN MENDIVIL
Acadia University
Wolfville, Nova Scotia, Canada
franklin.mendivil@acadiau.ca
jeff.hooper@acadiau.ca

Suppose we have the following matrix stored in row order in computer memory:

$$A = \begin{pmatrix} 1 & 10 & 3 & 5 & 8 & 9 & 20 \\ 3 & -3 & 19 & -5 & 10 & 9 & 100 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

This means that the matrix is stored (row-by-row) as

value	1	10	3	5	8	9	20	3	−3	19	−5
location	0	1	2	3	4	5	6	7	8	9	10
value	10	9	100	1	1	1	1	0	0	0	
location	11	12	13	14	15	16	17	18	19	20	

On the other hand, the transpose of A,

$$A^T = \begin{pmatrix} 1 & 3 & 1 \\ 10 & -3 & 1 \\ 3 & 19 & 1 \\ 5 & -5 & 1 \\ 8 & 10 & 0 \\ 9 & 9 & 0 \\ 20 & 100 & 0 \end{pmatrix},$$

is stored (also row-wise) in memory as

value	1	3	1	10	−3	1	3	19	1	5	−5
location	0	1	2	3	4	5	6	7	8	9	10
value	1	8	10	0	9	9	0	20	100	0	
location	11	12	13	14	15	16	17	18	19	20	

In going from A to A^T, we have simply permuted the matrix values around among the memory locations used to store the matrix. In describing this permutation, the actual matrix entries are not particularly relevant; only the locations are important. Thus, in our example above, we can write the resulting permutation as

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	3	6	9	12	15	18	1	4	7	10	13	16	19	2	5	8	11	14	17	20.

Math. Mag. **89** (2016) 16–35. doi:10.4169/math.mag.89.1.16.
MSC: Primary 10A10, Secondary 20-01.

(This is to be read as: "the value in location 0 remains in location 0," "the value in location 1 moves to location 3," and so on.)

The most convenient way (for us) of representing this permutation turns out to be as a product of disjoint cycles. Doing this, we obtain the representation

$$(0)(1\ 3\ 9\ 7)(2\ 6\ 18\ 14)(4\ 12\ 16\ 8)(5\ 15)(10)(11\ 13\ 19\ 17)(20).$$

A similar permutation can be found to describe this transposition for any $m \times n$ matrix. The question that naturally arises is: Can we predict the structure of this permutation based only on the size of the matrix (i.e., using only the knowledge of m and n)?

Because of its dynamical origins, this permutation arises in other contexts. An example of this is the study of perfect shuffles, as described in [**21**].

A perfect shuffle of a deck of $2n$ cards comprises the following process. The original deck is "cut" into two piles of size n: pile A consists of cards 1 to n while pile B consists of cards $(n + 1)$ to $2n$. These piles are then interleaved into a new pile of size $2n$ by alternately taking one card from each pile. Since the cards are moved to new locations depending only on their original position, these shuffles give rise to similar permutations.

If, during the interweaving, the top card for the new $2n$ pile is chosen from pile A (and hence the bottom card from pile B), then the result of the shuffle will leave the top and bottom cards of the original deck in place, and this type of shuffle (called an "out shuffle" in [**21**]) corresponds to transposing a $2 \times n$ matrix.

The main theme of this paper is an analysis of these permutations in terms of a fusion of group theory and number theory, which allows us a complete description of the permutation and in fact gives rise to an algorithm for finding the permutation explicitly and hence for performing the transposition "in-place." The key idea is that the process of permuting the elements may be related to the action of the subgroup $\langle m \rangle$ of $\mathbb{Z}^*_{mn-1}$ acting on the full set $\mathbb{Z}_{mn-1}$. Because our original motivating factor for this work was the problem of matrix transposition, the discussion is based around the problem of using group theory and number theory to design an algorithm to solve the in-place matrix transposition problem. In particular, we shall use matrix terminology and intuition throughout to help ground the discussion in a particular application.

The paper is organized as follows. Section 2 introduces the appropriate group action and shows that the orbits under the action are precisely the cycles of our permutation. In Section 3, we examine the key problems of determining the number of orbits and of finding representatives for each. An essential result is Proposition 3, which allows us to decompose the problem by factoring $mn - 1$ into prime powers, solve these simpler cases, and reconstruct the general solution. We completely describe answers to both when our modulus $mn - 1$ is either prime or a product of distinct primes. This leaves us with the cases in which the modulus is a prime power, and Sections 4 and 5 are devoted to these. The prime $p = 2$ quite often behaves differently than other primes (it has been called the "oddest prime"!), and this is the case here, which is why the analysis of modulus 2^k must be separated from the rest. Section 6 is devoted to examples that pull together the results of the previous sections to see how the complete permutation is constructed. We close with a final discussion section that includes some suggestions for further explorations of the ideas used in the paper.

Modular arithmetic and group actions enter the scene

Returning to our example of a 3×7 matrix, we recall that the permutation is

$$(0)(1\ 3\ 9\ 7)(2\ 6\ 18\ 14)(4\ 12\ 16\ 8)(5\ 15)(10)(11\ 13\ 19\ 17)(20).$$

The values in the first and last memory locations (locations 0 and 20) do not move, which is an obvious property of the transpose. In this particular case, the value in memory location 10 also remains stationary.

Looking at the orbit (1 3 9 7), we see that it seems that, for the first two elements, we are multiplying by 3 to get to the next element in the cycle. Considering these numbers mod 20, this is true for all of them: $9 \cdot 3 \equiv 7 \bmod 20$ and $7 \cdot 3 \equiv 1 \bmod 20$. In fact, as the reader will quickly verify, this is true for each of the orbits.

This is a general feature of this permutation.

Proposition 1. *Let A be an $\mathtt{M}$ by $\mathtt{N}$ matrix stored in row order. Then the value in memory location $n < \mathtt{N} * \mathtt{M} - 1$ (starting with location 0) is moved to location $n * \mathtt{M} \bmod (\mathtt{N} * \mathtt{M} - 1)$ when you perform a transpose on A and store A^T in row order.*

Proof. This is clear since if we write

$$n = j + i * \mathtt{N} \quad \text{with } i = 0, 1, \ldots, (M-1) \text{ and } j = 0, 1, \ldots, (N-1)$$

so that n is in the ith row and jth column, we see that

$$n * \mathtt{M} = j * \mathtt{M} + i * \mathtt{N} * \mathtt{M} = j * \mathtt{M} + i * (\mathtt{M} * \mathtt{N} - 1) + i = j * \mathtt{M} + i \bmod (\mathtt{N} * \mathtt{M} - 1)$$

is in the jth row and ith column of A^T. ∎

As the value $\mathtt{M} * \mathtt{N} - 1$ is important and will recur many times, for simplicity we will denote it by $\mathtt{D}$.

According to the proposition, if we work with the locations mod $\mathtt{D}$, then the value in location a is sent to location $a\mathtt{M}$ mod $\mathtt{D}$, the value in $a\mathtt{M}$ mod $\mathtt{D}$ is sent to location $a\mathtt{M}^2$ mod $\mathtt{D}$, the value in location $a\mathtt{M}^2$ mod $\mathtt{D}$ to location $a\mathtt{M}^3$ mod $\mathtt{D}$, and so on. Eventually, $\mathtt{M}^r \equiv 1 \bmod \mathtt{D}$ for some power r, and so we have the cycle (a $a\mathtt{M}$ mod $\mathtt{D}$, $a\mathtt{M}^2$ mod $\mathtt{D}$, $a\mathtt{M}^3$ mod $\mathtt{D}$, $\ldots$, $a\mathtt{M}^{r-1}$ mod $\mathtt{D}$) in this decomposition.

Once we have the permutation written as a product of disjoint cycles, it is easy to perform the transpose with only one additional memory location. We simply store the value from one entry, shift all the others in the cycle, and then restore the value into its proper place. For example, for the cycle (1 3 9 7), if we store the value in memory location 1 (in our example from the beginning, this is a 10), then we copy the value from memory location 7 into memory location 1, copy the value from memory location 9 into memory location 7, copy the value from memory location 3 into memory location 9, and then, finally, take our stored value (the number 10 in this case) and place it into memory location 3.

Since we can do this for each cycle in the permutation, once we have the cyclic decomposition of the permutation, we only need *one* additional memory location in order to perform the matrix transpose. Furthermore, it is easy (as we see by Proposition 1) to see where any given memory location moves. This means that we only need to find a representative from each cycle in the cyclic decomposition in order to know this decomposition. That is, for our example above, as long as we know that there are eight cycles in the decomposition and that the elements 0, 5, 10, 16, 1, 13, 6, and 20 are all in distinct cycles, we can reconstruct the entire cyclic decomposition.

In fact, Proposition 1 indicates that we can view the cycle decomposition as the collection of orbits of a group action. The group is $\langle \mathtt{M} \rangle$, the cyclic group generated by $\mathtt{M}$ under multiplication modulo $\mathtt{D}$, and this group is acting on $\mathbb{Z}_{\mathtt{D}}$, the full set of integers mod $\mathtt{D}$. The orbit starting at 1 (or the cycle starting with 1) is just the subgroup $\langle \mathtt{M} \rangle$ itself and is particularly important, so we call it the *primary orbit*. Note also that by the orbit-stabilizer theorem on group actions (see, for instance, [**9**]), the lengths of all orbits are divisors of the group order and, hence, of the length of the primary orbit.

For the remainder of this paper, we will ignore the orbit (D), as it is always there and thus easy to predict. It turns out that we must consider the zero orbit (0), even though it is also always present.

Finding orbit representatives

In light of Proposition 1 and the subsequent discussion, the crux of the algorithm we design here involves first determining the number of orbits and then finding a representative from each orbit.

The first clue to finding a complete set of orbit representatives lies in looking at the case where D is a prime number. In this case, the set $\{1, 2, \ldots, \mathtt{D}-1\} = \mathbb{Z}_{\mathtt{D}}^*$ is a cyclic group under multiplication (see [**17**], Theorem 4-3). Furthermore, if we look at the orbit starting with 1, we see that we have a subgroup of $\mathbb{Z}_{\mathtt{D}}^*$, the subgroup generated by the element M. This means that the other nonzero orbits are precisely the cosets of this subgroup and therefore finding all the orbits means finding all the cosets. However, by Lagrange's theorem, we know that the length of the primary orbit is a divisor of the order of $\mathbb{Z}_{\mathtt{D}}^*$ (which is equal to $\mathtt{D}-1$ in this case), and all the other nonzero orbits have this same length. So we have $(\mathtt{D}-1)/(\textit{length of primary orbit})$ nonzero orbits.

Suppose that L is the length of the primary orbit modulo the prime D. Suppose further that g is a primitive root modulo D (that is, the powers of g generate $\mathbb{Z}_{\mathtt{D}}^*$). Since L is the length of the primary orbit, the element M has order L in $\mathbb{Z}_{\mathtt{D}}^*$. In fact, because $\mathbb{Z}_{\mathtt{D}}^*$ is cyclic, the primary orbit contains all $x \in \mathbb{Z}_{\mathtt{D}}^*$ with $x^L = 1$ (see, for example, [**12**, Theorem 4.3]). Let $(\mathtt{D}-1)/L = N$ be the number of cosets (nonzero orbits). Then g^N is also a generator of the primary orbit: It is in the primary orbit since $g^{NL} = g^{\mathtt{D}-1} = 1$ and is a generator since $(g^N)^i \neq 1$ for $i < L$. However, this then means that the elements $g, g^2, g^3, \ldots, g^{N-1}$ will be representatives of the other cosets, so of the other orbits. This results in a very simple method of obtaining all the orbit representatives when D is prime. We summarize this discussion in the following result.

Proposition 2. *Let D be a prime. Then all nonzero orbits are cosets of* $\langle \mathtt{M} \rangle$*, the primary orbit, in* $\mathbb{Z}_D^*$*. With L the length of the primary orbit and g a primitive element modulo D, the generators for the nonzero orbits are* g^i*,* $i = 0, 1, \ldots, \frac{D-1}{L} - 1$.

As an example, consider the case of a 3×4 matrix (so that $\mathtt{D} = 11$). In this case, the cyclic decomposition of the transposition permutation is

$$(0)(1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ 10\ 8),$$

and we see that $\mathbb{Z}_{11}^*$ is decomposed into the subgroup (1 3 9 5 4) and its coset (2 6 7 10 8).

We have seen that $L = 5$ is the length of the primary orbit. It is not too hard to see that $g = 2$ is a primitive root. Thus, there are two cosets that are represented by the elements $g^0 = 1$ and $g^1 = 2$. From this, we obtain the three orbits, including the zero orbit.

Notice that the length of the primary orbit is the same as the multiplicative order of the element M modulo D. In general, this order is very difficult to predict in advance. For our purposes, we must generate the primary orbit, and so it is simple enough to compute its length (and hence the order of M) as we generate the primary orbit.

What if D is not a prime number? Well, the Chinese remainder theorem (see, for example, [**19**]) tells us that $\mathbb{Z}_{\mathtt{D}}$ is isomorphic to a product of commutative rings of the form $\mathbb{Z}_k$, with the individual rings in this product being given by the prime factorization of D. But how does this help in finding the orbits of the group action?

To motivate our discussion, we look at the example of a 4 by 9 matrix (where $\mathtt{D} = 35$) with orbit structure (recall that we ignore the orbit (35))

(0)
(1 4 16 29 11 9)
(22 18 2 8 32 23)
(31 19 6 24 26 34)
(17 33 27 3 12 13)
(15 25 30)
(10 5 20)
(21 14)
(7 28).

If we look at the orbits generated modulo 5 and modulo 7 under multiplication by 4, we see that modulo 5 we have

(0)
(1 4)
(2 3)

while for modulo 7 we have

(0)
(1 4 2)
(3 5 6).

The first thing to notice is that there are nine orbits modulo 35 and three each modulo 5 and 7. This is highly suggestive. In fact, if we reduce each of the original orbits modulo 5 and modulo 7, we get a pair of modulo 5 and modulo 7 orbits. For example, taking the principal orbit (1 4 16 29 11 9) and reducing modulo 5, we obtain the orbit (1 4). Modulo 7, we obtain the orbit (1 4 2). This suggests that if we can understand the orbit structure modulo 5 and modulo 7, we should somehow be able to combine them to get the orbits modulo 35. In fact, this is exactly the case and is a consequence of the Chinese remainder theorem.

To illustrate this, consider the modulo 5 orbit (1 4) and the modulo 7 orbit (3 5 6). If we repeat the first orbit three times and the second two times and place them side-by-side, we get the array:

$$\begin{array}{cccccc} 1 & 4 & 1 & 4 & 1 & 4 \\ 3 & 5 & 6 & 3 & 5 & 6. \end{array}$$

Now, using the Chinese remainder theorem, we find the unique element x in $\mathbb{Z}_{35}$ that satisfies $x = 1 \bmod 5$ and $x = 3 \bmod 7$. In this case, the element x is 31. Next, we find that $19 = 4 \bmod 5$ and $19 = 5 \bmod 7$. Continuing in this fashion, we build up the modulo 35 orbit (31 19 6 24 26 34).

Performing this same procedure with all combinations of modulo 5 and modulo 7 orbits will give all the modulo 35 orbits (the interested reader is encouraged to try this).

There is a possible problem, however. Consider the case of a 2 by 8 matrix. The orbit structure modulo 15 is

(0)
(6 12 9 3)
(1 2 4 8)
(11 7 14 13)
(10 5).

If we generate orbits using the multiplier 2 modulo 3, we get

$$(0)$$
$$(1\ 2)$$

and modulo 5 we get

$$(0)$$
$$(1\ 2\ 4\ 3).$$

Since there are two orbits modulo 3 and two orbits modulo 5, there are only four combinations. However, there are five orbits modulo 15.

The situation is best illustrated by laying two orbits side-by-side as follows:

$$\begin{array}{cccccccc} 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 1 & 2 & 4 & 3 & 1 & 2 & 4 & 3. \end{array}$$

Since the orbits have length 2 and 4, respectively, we see that the overall pattern repeats every four symbols. However, this means that certain combinations are never found. For example, we are never matching up 1 in the first row with 2 in the second, so the element 7 from $\mathbb{Z}_{15}$ is never represented. In fact, if we perform our procedure with these orbits, we get only the orbits (mod 15)

$$(0)$$
$$(6\ 12\ 9\ 3)$$
$$(1\ 2\ 4\ 8)$$
$$(10\ 5).$$

The problem is that $gcd(2, 4) = 2 \neq 1$, so when we place these two orbits side-by-side, we do not get all possible pairings and thus miss some elements. Notice that if we shift one of the orbits and then lay them side-by-side we get

$$\begin{array}{cccccccc} 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ 1 & 2 & 4 & 3 & 1 & 2 & 4 & 3 \end{array}$$

from which we get the missing orbit (11 7 14 13).

Proposition 3. *Let* $D = pq$ *where* $gcd(p, q) = 1$ *and suppose that we are using the multiplier* M. *Then for every orbit* $(n_1\ n_2\ n_3\ \ldots\ n_k)$ *modulo* D *we obtain an orbit modulo* p *by reducing this orbit modulo* p, *and each orbit modulo* p *arises this way. Conversely, suppose that* $(n_1\ n_2\ n_3\ \ldots\ n_i)$ *and* $(m_1\ m_2\ m_3\ \ldots\ m_j)$ *are orbits modulo* p *and* q, *respectively. Then we obtain an orbit* $(o_1\ o_2\ o_3\ \ldots\ o_k)$ *by solving the set of* k *equations* $x = m_a \bmod p$ *and* $x = n_b \bmod q$, *where* k *is the least common multiple of* i *and* j. *Furthermore, all orbits modulo* D *arise in this fashion.*

Proof. The first part is clear since, if $(n_1\ n_2\ \ldots\ n_k)$ is an orbit modulo $D = pq$, then $n_i * M = n_{i+1} \bmod D$ implies that $(n_i \bmod p) * (M \bmod p) = (n_{i+1} \bmod p)$.

For the converse, we just notice that since $(n_1\ n_2\ n_3\ \ldots\ n_i)$ is an orbit modulo p and $(m_1\ m_2\ m_3\ \ldots\ m_j)$ is an orbit modulo q, then we have $n_a * M = n_{a+1} \bmod p$ and $m_b * M = m_{b+1} \bmod q$. However, these two together imply, by the Chinese remainder theorem, the single relation $x * M = y \bmod D$ where $x = n_a \bmod p$ and $x = m_b \bmod q$ and $y = n_{a+1} \bmod p$ and $y = m_{b+1} \bmod q$.

The fact that we shift the orbits, if necessary, implies that we obtain all possible pairs in $\mathbb{Z}_p \times \mathbb{Z}_q$, so we obtain all possible elements from $\mathbb{Z}_D$. ∎

This is very nice, as it allows us to decompose the problem one prime at a time. Thus, in order to be able to find orbit representatives modulo a composite D, it is sufficient to be able to find orbit representatives modulo all the primes (and prime powers) in the prime decomposition of D.

Calculations with the Chinese remainder theorem. It is worth taking a short diversion into the use of the Chinese remainder theorem. The Chinese remainder theorem states that if $N = m_1 m_2 \cdots m_k$ where $gcd(m_i, m_j) = 1$ for all $i \neq j$, then, as rings,

$$\mathbb{Z}_N \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}.$$

Given arbitrary choices of $x_i \in \mathbb{Z}_{m_i}$, the Chinese remainder theorem tells us that there is exactly one $x \in \mathbb{Z}_N$ with $x \equiv x_i \bmod m_i$ for each index i. The standard proof of the Chinese remainder theorem (see, for example, [**19**]) actually shows how to *construct* an element with the required properties; since we will need this, it is worthwhile commenting on how this is done.

Define $P_i = N/m_i$ for $i = 1, 2, \ldots, k$. Then $gcd(P_i, m_i) = 1$, so there exists an element $q_i \in \mathbb{Z}^*_{m_i}$ with the property that $P_i q_i \equiv 1 \bmod m_i$. Once we have these P_i and q_i, we let

$$x = x_1(P_1 q_1) + x_2(P_2 q_2) + \cdots + x_k(P_k q_k).$$

Since $P_i q_i \equiv 1 \bmod m_i$ and $P_i q_i \equiv 0 \bmod m_j$ for $j \neq i$, we see that, as desired, $x \equiv x_i \bmod m_i$.

Example 1. (Chinese remainder theorem computations) To illustrate the Chinese remainder theorem computations, let us take our example of $N = 35$ so that $m_1 = 5$ and $m_2 = 7$. Then $P_1 = 7$ and $P_2 = 5$ and $q_1 = q_2 = 3$. If we want to find an x so that $x \equiv 4 \bmod 5$ and $x \equiv 5 \bmod 7$, then we simply take $x = 4(7)(3) + 5(5)(3) = 84 + 75 = 159 \equiv 19 \bmod 35$. We see that $19 \equiv 4 \bmod 5$ and $19 \equiv 5 \bmod 7$, as desired.

Example 2. As another example, consider a 691×1260 matrix. We see that $\mathtt{D} = 691 \times 1260 - 1 = 79 \times 103 \times 107$ so that D is *squarefree*. Since we know how to find all the orbits if the modulus is a prime, the Chinese remainder theorem will let us put these orbits together to get the full orbit structure.

Lengths of primary orbits: Now, in practice, we need to compute the primary orbit modolo $\mathtt{D} = 870659$ (the orbit starting with 1) to move the matrix elements around. During the computation of this primary orbit, it is a simple matter to reduce this orbit modulo 79, modulo 103, and modulo 107 to find the period of the primary orbits for these moduli. For our example, the primary orbit has length 70278 modolo 870659. Reducing this orbit modulo 79, we get an orbit of period 78; reducing it modulo 103, we get an orbit of period 34; and finally reducing it modulo 107, we get an orbit of period 53.

Orbit generators moduli the factors: For the modulus 79, we see that $\mathbb{Z}^*_{79}$ has 78 elements, so the primary orbit fills out this group, and we get only the two orbits starting at 0 and 1 (or any other nonzero element of $\mathbb{Z}^*_{79}$).

For the modulus 103, the reduced primary orbit has period 34, so there are three cosets of this orbit (or, more properly, there are three cosets of the multiplicative subgroup of $\mathbb{Z}^*_{103}$ generated by $691 \equiv 73$). Thus, we need three representatives for these cosets. To get these coset representatives, we need a generator of $\mathbb{Z}^*_{103}$. After a few tries, we see that 5 is a generator, so we can take as representatives the elements $1 = 5^0$, $5 = 5^1$, $25 = 5^2$. So, in all, we have the orbit representatives 0, 1, 5, 25.

Finally, for the modulus 107, we see that there are two cosets since the reduced primary orbit has length 53 and there are 106 elements in $\mathbb{Z}^*_{107}$. In this case, we find that 2 is a generator of $\mathbb{Z}^*_{107}$, so we get the orbit representatives 0, 1, 2.
All this information is summarized in Table 1.

TABLE 1: Summary of data for a 691 × 1260 matrix.

Modulus	Length of primary orbit	Number of nontrivial orbits	All orbit generators
79	78	1	0, 1
103	34	3	0, 1, 5, 25
107	53	2	0, 1, 2

Using the Chinese remainder theorem: We have two orbit generators for the modulus 79, four orbit generators for the modulus 103, and three orbit generators for the modulus 107. This seems like it should give us only $2 \times 4 \times 3 = 24$ orbits in all. However, we notice that $gcd(78, 34) = 2$, so we will have to do our shifting trick to find all the orbits.

First, we need the P_i's and q_i's (in the notation above, from the discussion of computations with the Chinese remainder theorem). Computing these (by the Euclidean algorithm), we see that

$$\begin{array}{lll} P_1 = 870659/79 = 11021 & \text{and} & q_1 = 2 \\ P_2 = 870659/103 = 8453 & \text{and} & q_2 = 59 \\ P_3 = 870659/107 = 8137 & \text{and} & q_3 = 43. \end{array}$$

With this data, we get the orbit generators:

0 22042 498727 520769 732094 752317 774359 89666
278949 300991 360162 349891 371933 848618 1 211326
231549 253591 439557 628840 650882 710053 699782 721824
327850 349892 561217 581440 603482 789448 108072 130114
189285.

These generators correspond (in order) to the triples of generators (a, b, c) modulo 79, modulo 103, and modulo 107 given by

(0, 0, 0) (1, 0, 0) (0, 1, 0) (1, 1, 0) (1, 73, 0) (0, 5, 0) (1, 5, 0) (1, 56, 0)
(0, 25, 0) (1, 25, 0) (1, 74, 0) (0, 0, 1) (1, 0, 1) (0, 1, 1) (1, 1, 1) (1, 73, 1)
(0, 5, 1) (1, 5, 1) (1, 56, 1) (0, 25, 1) (1, 25, 1) (1, 74, 1) (0, 0, 2) (1, 0, 2)
(0, 1, 2) (1, 1, 2) (1, 73, 2) (0, 5, 2) (1, 5, 2) (1.56, 2) (0, 25, 2) (1, 25, 2)
(1, 74, 2).

Notice that we have nine orbits that correspond to shifting the three orbits modulo 103 with generators 1, 5, 25.

As an example, we will show how to get 520769 and 732094.

Let's start with the generators 1,1, and 0 modulo 79, 103, and 107, respectively. We use the Chinese remainder theorem to get an element x of Z_{870659}, which reduces to these:

$$x = 1(P_1q_1) + 1(P_2q_2) + 0(P_3q_3) = 22042 + 498727 = 520769.$$

Now, since the orbit of 1 modulo 79 has length 78 and the orbit of 1 modulo 103 has length 34 and $gcd(78, 34) = 2$, we will have to do one shift to get all the orbits. If we shift the second orbit, we want the element of Z_{870659} that reduces to 1 modulo 79, to 73 modulo 103 (since $1 \cdot 691 \equiv 73 \bmod 103$), and to 0 modulo 107. Using the Chinese remainder theorem again, we get

$$x = 1(P_1q_1) + 73(P_2q_2) + 0(P_3q_3) = 22042 + 36407071 + 0 \equiv 732094.$$

The rest of the orbit generators in the table are computed in a similar fashion.

Odd prime powers

As we discussed at the beginning of the previous section, when D is a prime, it is easy to find a complete set of orbit representatives because all the nonzero orbits are actually cosets.

When $\mathtt{D} = p^n$ with p an odd prime, the situation is very similar to when D is prime. The reason for this is that in this case we also have that $\mathbb{Z}_{\mathtt{D}}^*$ is cyclic. The main difference is that the order of $\mathbb{Z}_{\mathtt{D}}^*$ is not $p^n - 1$ but is $\phi(p^n) = (p-1)p^{n-1}$ (where $\phi(n)$ is the Euler totient function, which counts the number of positive integers $i < n$ that are relatively prime to n). This indicates that not all the orbits will be cosets of the primary orbit since $(p-1)p^{n-1}$ does not divide $p^n - 1$.

A simple example will best illustrate the issues involved.

Example 3. Suppose that we are interested in the orbits of the multiplier 7 modulo 81. These orbits are

(0)
(1 7 49 19 52 40 37 16 31 55 61 22 73 25 13 10 70 4 28 34 76 46 79 67 64 43 58)
(2 14 17 38 23 80 74 32 62 29 41 44 65 50 26 20 59 8 56 68 71 11 77 53 47 5 35)
(3 21 66 57 75 39 30 48 12)
(6 42 51 33 69 78 60 15 24)
(9 63 36)
(18 45 72)
(27)
(54).

We see that 7 has multiplicative order 27 and that the order of $\mathbb{Z}_{81}^*$ is $(3-1)3^3 = 54$, so there are two cosets of the primary orbit. How do we explain the other orbits? Well, if we look at the orbits of 7 modulo 27, we get

(0)
(1 7 22 19 25 13 10 16 4)
(2 14 17 11 23 26 20 5 8)
(3 21 12)
(6 15 24)
(9)
(18).

Examining these orbits, we see that if we multiply each number by 3, we get the last six orbits modulo 81! This indicates that the orbits of the multiplier m modulo p^n should "nest." That is, there are the orbits arising as cosets modulo p^n, then the orbits arising as cosets modulo p^{n-1}, then those arising as cosets modulo p^{n-2}, and so on.

To see this in this example, we simply have to see that the orbits of the multiplier 7 modulo 9 are

(0)
(1 7 4)
(2 5 8)
(3)
(6)

and the orbits of 7 modulo 3 are

(0)
(1)
(2).

Proposition 4. *Let p be prime and m be relatively prime to p. If $(a_1\ a_2\ \ldots\ a_k)$ is an orbit of m modulo p^n, then $(pa_1\ pa_2\ \ldots\ pa_k)$ is an orbit of m modulo p^{n+1}. Furthermore, every orbit of m modulo p^{n+1} of the form $(pa_1\ pa_2\ \ldots\ pa_k)$ arises in this fashion.*

Proof. Since $(a_1\ a_2\ \ldots\ a_k)$ is an orbit of m modulo p^n, we see that $ma_i \equiv a_{i+1} \bmod p^n$. Thus, $mpa_i \equiv pa_{i+1} \bmod p^{n+1}$ so $(pa_1\ pa_2\ \ldots\ pa_k)$ is an orbit of m modulo p^{n+1}.

Furthermore, if $(pa_1\ pa_2\ \ldots\ pa_k)$ is an orbit of m modulo p^{n+1}, we see that $mpa_i \equiv pa_{i+1} \bmod p^{n+1}$, which implies that $ma_i \equiv a_{i+1} \bmod p^n$ so $(a_1\ a_2\ \ldots\ a_k)$ is an orbit of m modulo p^n. ∎

This proposition allows us to find all the orbits of the multiplier m modulo p^n as either cosets of the primary orbit or "lifts" of orbits modulo p^k (for $k < n$). However, these orbits modulo p^k are also either cosets or lifts.

Going back to our example, we notice that 7 has order 27 modulo 81 and has order 9 modulo 27 and has order 3 modulo 9 and order 1 modulo 3. In fact, this is a general feature modulo odd primes as the next theorem states (see [**17**], Theorem 4-6).

Theorem 5. *Suppose that p is an odd prime and that m has order t mod p. Let a be the largest exponent such that p^a divides $m^t - 1$ (as integers). Then in $\mathbb{Z}^*_{p^n}$, the order of m is precisely*

$$tp^{\max(0,n-a)}.$$

This theorem tells us that, as we descend through the powers of p, the order of m reduces by a factor of p each time until no such reduction is possible. This useful fact allows us to count the number of orbits of m that arise as cosets modulo various powers of p. Suppose that the order of m modulo p^n is tp^b. Then there are $(p-1)p^{n-1}/(tp^b)$ orbits arising as cosets modulo p^n. If $b \geq 1$, there are also this many orbits arising as cosets modulo p^{n-1}. Using this reasoning, we see that there are exactly

$$\begin{aligned}\left(b + \sum_{k=0}^{k=n-b-1} (1/p)^k\right)\frac{(p-1)p^{n-1}}{tp^b} &= \left[b + \frac{p}{p-1}\left(\frac{p^{n-b}-1}{p^{n-b}}\right)\right]\frac{(p-1)p^{n-1}}{tp^b}\\ &= b\frac{(p-1)p^{n-1}}{tp^b} + \frac{p^{n-b}-1}{t}\\ &= b\frac{(p-1)p^{n-1}}{tp^b} + \frac{p^n - p^b}{tp^b}\end{aligned}$$

nonzero orbits.

For our example, we see that 7 has order $27 = 3^3$ modulo 81 and order 1 modulo 3. Thus, $n = 4$, $t = 1$, and $b = 3$, and so we see that there are

$$3\frac{(3-1)3^3}{27} + \frac{3^4 - 3^3}{27} = 6 + 2 = 8$$

nonzero orbits.

Generating orbits for Example 3. So, how do we put all this information together to actually generate the orbits of the multiplier 7 modulo 81?

First, we compute the primary orbit and see that it has length 27. Since $\phi(81) = 54$, we see that there must be two cosets—the primary orbit and one coset. Since $\mathbb{Z}_{81}^*$ is cyclic, if we find a cyclic generator, we can find coset representatives. It turns out that 2 is a primitive root modulo 81 (and, in fact, modulo 3^n for all n). Thus, we use the two orbit representatives $2^0 = 1$ and $2^1 = 2$.

Consider next the orbits of the multiplier 7 modulo $3^3 = 27$. We know that 7 has order 9 modulo 27 (by Theorem 5) and $\phi(27) = 18$. Thus, there are also two cosets of this primary orbit. Again, we can use the generator 2, so we have the two orbit representatives $3(2^0) = 3$ and $3(2^1) = 6$.

Next, we consider the orbits of 7 modulo $3^2 = 9$. Since 7 has order 3 modulo 9 and $\phi(9) = 6$, we again have two cosets. Again using 2 as a primitive root, we get the two orbit representatives $9(2^0) = 9$ and $9(2^1) = 18$.

Finally, we consider the orbits of 7 modulo 3. Here, 7 has order 1 modulo 3 and $\phi(3) = 2$, so we again have two cosets with orbit representatives $27(2^0) = 27$ and $27(2^1) = 54$.

These orbits, along with the zero orbit (0), form all the orbits of the multiplier 7 modulo 81.

This example highlights a potential problem. We must find a primitive root g modulo p^k for each $k \leq n$. How do we do this?

Theorem 6. *Let p be an odd prime. If g is a primitive root modulo p and modulo p^2, then g is a primitive root modulo p^n for all n. If g is a primitive root modulo p but not a primitive root modulo p^2, then $g + p$ is a primitive root modulo p^n for all n.*

Proof. The first part is a consequence of Theorem 5 since if g is a primitive root modulo p and p^2, then it has order $(p-1)$ modulo p and order $(p-1)p$ modulo p^2 and thus must have order $(p-1)p^{n-1}$ modulo p^n.

For the second part, suppose that g is primitive mod p but not mod p^2. Then g necessarily has order $p - 1$ mod p^2, so

$$g^{p-1} = 1 + bp^2$$

for some b. Let $h = g + p$ and consider powers of h. The element h is clearly a primitive root mod p and so satisfies $h^{p-1} = 1 + ap$ for some $0 \leq a < p$. We have

$$\begin{aligned} h^p &= (g+p)^p \\ &= g^p + up^2 \\ &= g + vp^2 \end{aligned}$$

so that $h^p \equiv g \bmod p^2$. Hence, h has exactly order $\phi(p^2) = p(p-1)$ in $\mathbb{Z}_{p^2}$, and the result now follows from Theorem 5. ∎

Empirically, the smallest positive primitive root modulo p is usually also a primitive element modulo p^2. In fact, by a computer search the only prime less than 11 000 000

for which this fails is 40487 for which 5 is a primitive root but is not a primitive element modulo $(40487)^2$.

It is certainly possible for the primary orbit to have maximal length modulo p^n, in which case all the "images" of the primary orbit modulo p^k will also have maximal length. An example of this is for the multiplier 10 and the modulus $7^3 = 343$ where the primary orbit has length 294. The opposite extreme is also possible where all orbits have length 1, but this only happens when the multiplier is 1.

Powers of two

The prime 2 is special since the group $\mathbb{Z}_{2^n}^*$ is not cyclic. In fact, writing C_m for the cyclic group of order m, we have that $\mathbb{Z}_{2^n}^* \cong C_{2^{n-2}} \times C_2$ for $n \geq 3$ (while $\mathbb{Z}_2^* = \{1\}$ and $\mathbb{Z}_4^* \cong C_2$). It turns out that (see, for example, [**19**], Theorem 2.43) the elements 5 and $-1 = 2^n - 1$ always generate $\mathbb{Z}_{2^n}^*$ for $n \geq 3$. In other words, every element of $\mathbb{Z}_{2^n}^*$ may be expressed as either 5^k or -5^k for $0 \leq k \leq 2^{n-2}$.

Since the structure of $\mathbb{Z}_{2^n}^*$ is so simple, it is not difficult to modify our procedure to find orbit representatives. The only differences result from the fact that $\mathbb{Z}_{2^n}^*$ is not cyclic.

Again, to illustrate the procedure in this case, we will look at an example.

Example 4. We consider the multiplier 7 and the modulus 32 with orbits

(0)
(1 7 17 23)
(31 25 15 9)
(3 21 19 5)
(29 11 13 27)
(2 14)
(30 18)
(6 10)
(26 22)
(4 28)
(12 20)
(8 24)
(16).

We see that 7 has multiplicative order 4 modulo 32. Since $\phi(32) = 16$, there are four orbits that arise as cosets. Since $7 \neq -1 \bmod 32$, we see that 7 must either equal 5^k for some k or equal -5^k for some k. Further, because 7 has order 4 and 5 has order 8, it must be the case that k is even. This means that we can use $1 = 5^0$, $31 \equiv -1 = -5^0$, 5 and $27 \equiv -5$ as representatives for these cosets.

Now, when we move to considering those orbits that arise as cosets modulo 16, we see that 7 has order 2 modulo 16. This means that again there are four orbits that arise as cosets (modulo 16). By the same reasoning as before, we see that we can use $2 = 2(1)$ and $30 = 2(15) = 2(-1) \bmod 16$ and $10 = 2(5)$ and $22 = 2(11) = 2(-5) \bmod 16$ as orbit representatives for these orbits.

Moving on to orbits modulo 8, we see that $7 = -1 \bmod 8$. This means that 7 is not a power of 5 and the orbit starting with g will be $(g \quad -g)$. Since $\phi(8) = 4$, we obtain two orbits at this stage with corresponding orbit representatives $4 = 4(1) = 4(5^0)$ and $20 = 4(5)$. Notice that since $7 \equiv -1$ all the orbit generators are powers of 5 that we lift from modulo 8 to modulo 32 by multiplying by 4.

Next, we consider modulo 4 orbits. Here again, $7 = -1 \bmod 4$. Since $\phi(4) = 2$ and 7 has order two, there is only one orbit for which we get the orbit representative $8 = 8(1)$.

Finally, considering orbits modulo 2, we get the orbit representative 16(1). This takes care of all the nonzero orbits.

One interesting thing to notice in this example is that 7 had order 4 modulo 32 and order 2 modulo 16, 8, 4 and 2. Knowing how the order of the multiplier changes as we descend through the various powers of two is important in order to be able to find an algorithm for the general case. The next result establishes this for us.

In the next proposition and the succeeding discussion, we shall make use of the following representation of an odd positive integer $b \geq 3$. Since b is an odd integer, it is congruent to either 1 or 3 mod 4. Set $d = b - 1$ if $b \equiv 1 \bmod 4$, and $d = b + 1$ otherwise. Then d is a multiple of 4, and we can write d uniquely in the form $d = 2^r\ a$ with a odd and $r \geq 2$. This is our representation.

In other words, we define a odd and $r \geq 2$ by

$$b = \begin{cases} a\ 2^r + 1 & \text{if } b \equiv 1 \bmod 4; \\ a\ 2^r - 1 & \text{if } b \equiv 3 \bmod 4. \end{cases} \tag{1}$$

Proposition 7. *Consider the group $\mathbb{Z}_{2^n}^*$.*

1. *The elements of order 2 in $\mathbb{Z}_{2^n}^*$ are precisely $2^{n-1} \pm 1$ and $2^n - 1$.*
2. *If $b \in \mathbb{Z}_{2^n}^*$ has order greater than 2, write b in the form given in Equation (1), where a is odd and $r \geq 2$. Then b has order 2^{n-r} in $\mathbb{Z}_{2^n}^*$.*

Proof. Because the group $\mathbb{Z}_{2^n}^*$ is isomorphic to $C_{2^{n-2}} \times C_2$, every element has order a power of 2, and there are precisely three elements of order 2. It's easy to see that these are the stated elements.

For the second statement, set $s = n - r$ so that our claim is that b has order 2^s. To see this, we consider $b^{2^{s-1}}$.

$$\begin{aligned} b^{2^{s-1}} &= (\ a\ 2^r \pm 1\ )^{2^{s-1}} \\ &= \sum_{k=0}^{2^{s-1}} \binom{2^{s-1}}{k} (\pm 1)^{2^{s-1}-k} a^k\ 2^{kr} \\ &= 1 \pm 2^{s-1} \cdot a\ 2^r + \binom{2^{s-1}}{2} a^2\ 2^{2r} \pm \binom{2^{s-1}}{3} a^3\ 2^{3r} + \cdots . \end{aligned}$$

Writing $a = 1 + 2c$, we see that

$$b^{2^{s-1}} = 1 \pm 2^{r+s-1} \pm 2^{r+s-1}(\ 2c\ ) + \binom{2^{s-1}}{2} a^2\ 2^{2r} \pm \binom{2^{s-1}}{3} a^3\ 2^{3r} + \cdots$$

and hence, $b^{2^{s-1}} = 1 \pm 2^{r+s-1}$ has order 2. Therefore, b has exactly order $2^s = 2^{n-r}$ as required. ∎

Proposition 8.

1. *The elements of order 2 in $\mathbb{Z}_{2^n}^*$ reduce to ± 1 mod 2^{n-1} and so have order either 1 or 2.*
2. *Let $s \geq 2$ and suppose that g is an element of order 2^s in $\mathbb{Z}_{2^n}^*$. Then g has order 2^{s-1} mod 2^{n-1}.*

Proof. This now follows from the previous lemma. The first statement is clear. For the second, writing g in the form of Equation (1):

$$g = a\ 2^r \pm 1$$

where $r = n - s < n - 1$, we see that g reduces mod 2^{n-1} to $a'\ 2^r \pm 1$, with a' odd. Since $r \geq 2$, this representation $a'\ 2^r \pm 1$ is the representation of g given by equation (1), and so g has order $2^{(n-1)-r} = 2^{s-1} \bmod 2^{n-1}$. ∎

To state this result in another form, set $g_n = g$, and for each k, $1 \leq k \leq n$, set g_k to be the residue of g mod 2^k. Proposition 8 says that if g has order 2^s mod 2^n, then the elements $g_n, g_{n-1}, \ldots g_2, g_1$ have orders either

$$2^s, 2^{s-1}, 2^{s-2}, \ldots 8, 4, 2, 2, 2, 2, \ldots, 2, 1$$

or

$$2^s, 2^{s-1}, 2^{s-2}, \ldots 8, 4, 2, 1, 1, 1, \ldots, 1, 1.$$

In particular, if $g = a\ 2^r \pm 1$ is the above representation of g, then g reduces mod 2^{r+2} to either $2^r \pm 1$ or to $2^{r+1} + 2^r \pm 1$, each of which has order 4 mod 2^{r+2}. Reducing mod 2^{r+1} gives $2^r \pm 1$, an element of order 2 in both cases. Then reducing again yields either 1 or -1, so that the order of g stabilizes for the remaining reductions, until the final one.

Using this result, we can count the number of orbits of the multiplier M modulo 2^n.

Proposition 9. *Let* M *act by multiplication on* $\mathbb{Z}_{2^n}$. *If* $\mathtt{M} = 1$, *then there are* 2^n *orbits of* $\mathbb{Z}_{2^n}$ *under this action.*
If $\mathtt{M} > 1$ *and* $\mathtt{M} \equiv 1$ *mod* 4 *and if* $\mathtt{M} = a\ 2^r + 1$ *is the representation of* M *provided by equation (1), then the number of orbits of* $\mathbb{Z}_{2^n}$ *under this action is*

$$(n - r + 2)2^{r-1}\ .$$

If $\mathtt{M} \equiv 3$ *mod* 4, *and if* $\mathtt{M} = a\ 2^r - 1$ *is the representation of* M *provided by equation (1), then the number of orbits of* $\mathbb{Z}_{2^n}$ *under this action is*

$$1 + (n - r + 1)2^{r-1}\ .$$

Proof. The result for the $\mathtt{M} = 1$ case is clear: Every element is left fixed by multiplication by 1.

For the case $\mathtt{M} \equiv 1 \bmod 4$, we consider the multiplicative action of M on $\mathbb{Z}_{2^k}^*$ for each k. There are two possibilities. First of all, if $1 \leq k \leq r$, $\mathtt{M} \equiv 1 \bmod 2^k$, and so M has order 1 in $\mathbb{Z}_{2^k}^*$. Therefore, there are 2^{k-1} orbits (i.e., cosets) of $\mathbb{Z}_{2^k}^*$ under this action, which lift to 2^{k-1} orbits of $\mathbb{Z}_{2^n}^*$. On the other hand, if $r + 1 \leq k \leq n$, then M has order2^{n-r} in $\mathbb{Z}_{2^k}^*$. Since $\mathbb{Z}_{2^n}^*$ is a group of order 2^{n-1}, there are $2^{n-1}/2^{n-r} = 2^{r-1}$ orbits, and again each lifts to an orbit of $\mathbb{Z}_{2^n}^*$.

Taking into account the 0 orbit, we sum up to get a total of

$$\sum_{k=1}^{r} 2^{k-1} + \sum_{k=r+1}^{n} 2^{r-1} + 1 = (2^r - 1) + (n - r)2^{r-1} + 1 = (n - r + 2)2^{r-1}$$

orbits of the action.

A similar argument holds for the case $\mathtt{M} \equiv 3 \bmod 4$. Again, we consider the multiplicative action of M on $\mathbb{Z}_{2^k}^*$ for each k. If $r + 1 \leq k \leq n$, the argument is identical to the previous case, and if $k = 1$, we obtain 1 orbit as before. If $2 \leq k \leq r$, however,

$\mathtt{M} \equiv -1 \bmod 2^k$, and so $\mathtt{M}$ has order 2 in $\mathbb{Z}^*_{2^k}$. Hence, there are 2^{k-2} orbits of $\mathbb{Z}^*_{2^k}$ under this action, which lift to 2^{k-2} orbits of $\mathbb{Z}^*_{2^n}$.

Taking into account the 0 orbit, we sum up in this case to obtain a total of

$$1 + \sum_{k=2}^{r} 2^{k-2} + \sum_{k=r+1}^{n} 2^{r-1} + 1 = 1 + (2^{r-1} - 1) + (n-r)2^{r-1} + 1$$
$$= 1 + (n - r + 1)2^{r-1}$$

orbits of the action, as claimed. ■

For example, using the multiplier 7 modulo 32, we see that $7 = 2^3 - 1$ so that, in the notation of the above proposition, $n = 5$ and $r = 3$. According to the first case of the proposition, the number of orbits is therefore $1 + (5 - 3 + 1)2^{3-1} = 1 + (3)2^2 = 13$, and this is exactly the number we encountered earlier when we wrote the orbits out explicitly.

Notice that the cases in Proposition 9 can easily be checked by examining the binary representation of M. We simply count the number of 1's (in this binary representation) at the "right end" (the lowest order part) of M. If there is only one 1, then we are in case one. Otherwise, we are in case two. We find r by either counting the number of these 1's (case two) or by counting the number of 0's until the next 1 and adding one (case one). For example, 7 in binary is 111, so we are in case two and $r = 3$. As another example, using the multiplier 21 modulo 32, we see that 21 is 10101 in binary, so we are in case one with $r = 2$ so there are 10 orbits.

Putting it all together

Now that we can find orbit generators modulo all odd prime powers and powers of two, we can try to put all this information together to describe the complete algorithm. We do this for our simple example from Section 2, that of a 3 by 7 matrix.

Example 5. First, we see that $(3)(7) - 1 = 20 = (4)(5)$, so we know that we need to find orbit representatives modulo 4 and modulo 5 for the multiplier 3.

Lengths of primary orbits: We start by explicitly generating the primary orbit modulo 20 (which we will need to do anyway in order to move these matrix elements) and reduce this orbit modulo 4 and modulo 5. We see that this orbit modulo 20 is (1 3 9 7), so we get the primary orbit modulo 4 is (1 3) and modulo 5 is (1 3 4 2). Thus, 3 has order 2 modulo 4 and has order 4 modulo 5.

Orbit generators moduli the factors: Now we will generate the orbit representatives modulo the prime powers 4 and 5. We start with the prime 2.

First, $\phi(4) = 2$ and 3 has order 2 modulo 4, so there is only one orbit modulo 4 with generator 1. When we descend to considering orbits modulo 2, we see that we get a single orbit, which lifts (by multiplying by 2) to give the generator 2. Thus, along with the zero orbit, we have the three generators 0, 1, 2 for the orbits modulo 4 of the multiplier 3.

Now we consider the prime 5. Here, we see that 3 has order 4 modulo 5, so there is only one orbit with generator 1. Thus, we get the two orbit generators 0, 1 for the orbits modulo 5.

Using the Chinese remainder theorem: Now we must use the Chinese remainder theorem to lift these orbit generators to orbit generators modulo 20. We have three orbit generators modulo 4 and two orbit generators modulo 5, so we will have at least

3×2 orbit generators modulo 20. However, we might have to shift some orbits as discussed in Section 3.

From the two orbit generators 0 and 0 modulo 4 and 5, respectively, we get the orbit generator 0 modulo 20. We don't have to worry about shifting this orbit.

From the two orbit generators 1 and 0, we get the orbit generator 5 modulo 20. The length of the orbit generated by 1 modulo 4 is two while the length of the orbit generated by 0 modulo 5 is one and $gcd(1, 2) = 1$, so we don't need to shift this orbit. Thus, we only get the orbit generator 5.

From the two orbit generators 2 and 0, we get the orbit generator 10 modulo 20. The length of the orbit generated by 2 modulo 4 is one and the length of the orbit generated by 0 modulo 5 is one and $gcd(1, 1) = 1$, so there is no need to do any shifts of this orbit either. Thus, we only get the orbit generator 10.

Next, we consider the two orbit generators 0 and 1, which yield the orbit generator 16 modulo 20. Here, the length of the orbit generated by 0 modulo 4 is one, which means that we don't need to shift this orbit either. So again we only get the one orbit generator 16.

Now we consider the two orbit generators 1 and 1, which yield the orbit generator 1 modulo 20. This time, we do need to consider shifts of the orbit since the orbit generated by 1 modulo 4 has length two and the orbit generated by 1 modulo 5 has length four and $gcd(4, 2) = 2 > 1$. This means that we will need two shifts of this orbit—the original orbit plus one shift. To get this shift, we simply take the basic orbit generator modulo 5 (here this is 1) and multiply it by the multiplier (here 3). This leads to solving the system $x = 1 \bmod 4$ and $x = 3 \bmod 5$ with solution $x = 13$. So we need to use the two orbit generators 1 and 13.

Finally, we consider the two orbit generators 2 and 1, which yield the orbit generator 6 modulo 20.

To perform the matrix transpose, we find that we need to generate orbits using the multiplier 3 modulo 20 starting with the orbit generators 0, 5, 10, 16, 1, 13 and 6. Clearly, we don't need to generate the zero orbit, so we generate the other six orbits and shift the data through each cycle.

Our next example is slightly more complicated but still doable by hand.

Example 6. For a 25 by 185 matrix, we see that $25 \times 185 - 1 = 4624 = (2^4)(17^2)$.
Lengths of primary orbits: The length of the primary orbit modulo D is 136. If we reduce this orbit modulo 2^4, we get an orbit of period 2 while reducing it modulo 17^2 we get an orbit of period 136.

Numbers and lengths of orbits modulo the factors: For the modulus $16 = 2^4$, we obtain four orbits of length 2 and one orbit of length 1 (the zero orbit).

Since $M = 25 \equiv 1 \bmod 8$, all the orbits modulo 8, modulo 4, and modulo 2 are of length one.

For the modulus $289 = 17^2$, we have that $\mathbb{Z}^*_{289}$ contains 272 elements and the primary orbit is of length 136. Thus, there are two orbits of length 136 and the zero orbit (of length 1).

For the modulus 17, we obtain two orbits of length 8 along with the zero orbit.

Orbit generators moduli the factors: It turns out that $g = 3$ is a primitive element modulo 17 and also modulo 17^2. Thus, we use 1, 3 as the generators for the nonzero orbits modulo 17^2 and 1, 51 as the generators for the nonzero orbits modulo 17^2 that arise as lifts of orbits modulo 17.

Finally, for the nonzero orbits modulo $16 = 2^4$, we use the orbit generators $1, -1, 5, -5$.

Combining all these orbits (and their shifts) together with the Chinese remainder theorem, we obtain a total of 76 different orbits.

For any reader interested in trying large examples, we suggest two in particular. For a 99999 by 1000000 matrix, the above process yields 7, 3, and 7 orbits modulo the prime factors of $\mathtt{D} = 313 \times 1217 \times 262519$, and this results in only 398 distinct nonzero orbits. Notice that the matrix has almost 100 billion entries. As a second example, for a 105359 by 152615 matrix, we obtain only 54 orbit generators modulo the various factors of $\mathtt{D} = 2^3 \times 3^4 \times 11^3 \times 103 \times 181$. However, with the required shifts, this results in 398628 distinct nonzero orbits.

History and further directions

The topics explored here initially arose from a quest to find an algorithm to perform an in-place matrix transpose. That is, to rearrange the entries of a matrix in a computer's memory so that what started out stored row-wise ends up being stored column-wise.

The question of an "in-place matrix transform algorithm" appears to have originated as a problem given to students taking the Cambridge University Diploma in Numerical Analysis and Automated Computing in 1957, and several variants of these algorithms have been proposed (see, for instance, [**22**], [**8**], [**3**], [**16**], [**11**], and [**4**]). This question also appears as an exercise in Knuth's book [**14**, p. 180]. The algorithms given in these sources can be divided into two classes: one class in which essentially a table of bits is used to keep track of entries that have already been transposed and the second class in which each cycle of the permutation is first tested to ensure that the cycle is only applied once. Both cases suffer from drawbacks: For the first, one must maintain a fairly substantial table as a database of which entries have already been permuted; the second saves on storage but requires enormous computational effort as the algorithm proceeds.

In this paper, we describe an alternative algorithm. This algorithm is a variation of the algorithm presented in [**20**] and differs from the above classes in that it involves a shift in viewpoint to that of group actions. Our group action is the action of a subgroup of $\mathbb{Z}_N^*$ (the multiplicative group modulo N) acting on all of $\mathbb{Z}_N$. We explicitly determine all the orbits of this group action by calculating the number of orbits, the length of each orbit, and also by finding a generator for each orbit. As such, the techniques involved display a wonderful combination of group theory and number theory.

In-place matrix transposition and related problems continue to attract research attention, especially on the technical side (see [**5**], [**7**], [**10**], [**15**]). To mathematics students, this may seem surprising since mathematically a matrix and its transpose are easily related—and given the current state of computing power—yet there remain numerous technical situations in which such in-place algorithms retain their importance.

The techniques and topics explored here can easily be used to lead students in a number of fruitful directions. We outline here some technical issues that may be explored, as well as lay out some suggestions for several more algebraic/number theoretic ones.

Implementation issues. For students with more of a computer science leaning, there is the entire topic of implementations of algorithms for computer arithmetic, as well as for working with matrices.

There are a few issues that must be taken into account when actually implementing this algorithm for large matrices. The first of these is the implementation of large

integer arithmetic. For larger matrices, the modulus D may become large enough that computations mod D require the use of special arithmetic packages for large integer calculations. Most standard languages (such as C, C++, Python) come with additional packages for use in such situations. For the curious reader who wants to implement his or her own arithmetic package, an excellent discussion of specialized algorithms is given in Chapter 14 of [**18**].

Two further computational issues are number-theoretic. The algorithm must factor D in order to examine the orbits prime-by-prime and must also generate primitive roots mod odd primes. While factoring is a hard problem in general, in practice this is really not a concern since a current implementation of this algorithm would be on a machine for which D would be small enough.

Theorem 6, for instance, made specific use of primitive roots, as did our method of generating orbit representatives. There is no known algorithm that given a prime p, will provide a primitive root mod p, which does not make use of an exhaustive search. In fact, one of the more efficient algorithms for finding such a root is to apply the following test to each possible a.

Lemma 10. *A number $a \in \mathbb{Z}_n^*$ is a primitive root iff for each prime q dividing $\phi(n)$,*

$$a^{\phi(n)/q} \not\equiv 1 \bmod n.$$

More discussion of these issues can be found, for instance, in [**19**] or [**13**].

Since this area remains an active research field on the technical side, another fruitful topic would involve implementation and testing of this algorithm against various algorithms that have been proposed in the literature (as in, for instance, [**22**], [**20**], [**8**], [**3**], [**16**], [**11**],[**4**], [**5**], [**7**], [**15**], and [**10**]).

Group actions. The analysis of the algorithm involves the use of group actions in an important way and so could easily be used to launch a more involved exploration of general ideas on groups acting on sets and in particular to the connections between transitive actions and cosets. Basic ideas on group actions can be found in, for instance, [**9**]. For connections with geometry, a beautiful reference is Chapter 1 in the classic pair of texts [**2**], although in later chapters these get very technical very quickly.

Applications of group actions. Aside from general notions related to group actions, the material included here leads quickly and easily into applications. An important one is the notion of applying group actions to combinatorial problems. Fraleigh [**9**] is a standard reference and covers most of the key ideas, though the symmetry is brought into play more extensively in the beautiful text [**1**].

A second beautiful application is to frieze groups and periodic tilings of the plane. The books [**2**] and [**12**] contain excellent discussions of these.

Primitive roots. An extremely fruitful direction for exploration involves primitive roots. As noted in the discussion preceding and following Theorem 6, there are many unresolved questions concerning primitive roots. If we choose a prime p, how can we find a primitive root g modulo p^k? If instead we fix a positive integer g and consider moduli p^k for $p \geq g$, for how many p is g actually a primitive root? The famous Artin conjecture states that there should be infinitely many such p.

In addition, the statement of Theorem 2 itself can be used to explore the general structure of primitive roots mod p^k where the prime p is fixed and the exponent k is allowed to vary. In the form presented here, the theorem actually asserts much less than the entire picture. For instance, there are $\phi(\phi(p))$ primitive roots modulo p, and

for each one g, exactly one of the p integers modulo p^2 that reduce to g mod p fails to be a primitive root mod p^2. Similar patterns arise as we look at higher powers of p. A good discussion of these ideas may be found in [**13**].

The *p*-adic Numbers In the previous paragraph, we suggested examining the connections between primitive roots mod p^k and primitive roots mod p^{k+1}. One may also generalize this a little and consider these reduction maps all at once, piecing these together to yield a sequence of surjective homomorphisms:

$$\mathbb{Z}/p\mathbb{Z} \longleftarrow \mathbb{Z}/p^2\mathbb{Z} \longleftarrow \mathbb{Z}/p^3\mathbb{Z} \longleftarrow \cdots \longleftarrow \mathbb{Z}/p^k\mathbb{Z} \longleftarrow \mathbb{Z}/p^{k+1}\mathbb{Z} \longleftarrow \cdots .$$

Looking at "compatible" strings of elements mod p leads one directly to a standard definition of the p-adic numbers, and the fact that this new set of numbers somehow combines all of the rings $\mathbb{Z}/p^k\mathbb{Z}$ and the way in which they are connected by the reduction homomorphisms. An excellent introduction to these ideas can be found in Neukirch's article, Chapter 6 of [**6**].

Acknowledgments. The second author was partially supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

1. M. A. Armstrong, *Group Theory and Symmetry*. Springer-Verlag, New York, 1988.
2. M. Berger, *Géometrie*. Springer-Verlag, New York, 1989.
3. J. Boothrotd, Algorithm 302: Transpose vector storage array, *Commun. ACM* **10**, no. 5 (1967) 292–293.
4. E. G. Cate, D. W. Twigg, Algorithm 513: Analysis of in-situ transposition, *ACM Trans. Math. Software* **3**, no. 1 (1977) 104–110.
5. M. Dow, Practical aspects and experiences: Transposing a matrix on a vector computer, *Parallel Comput.* **21** (1995) 1997–2005.
6. H. D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert, *Numbers*, Springer-Verlag, New York, 1991.
7. F. E. Fich, J. I. Munro, P. V. Poblete, Permuting in place, *SIAM. J. Comp.* **24** no. 2 (1995) 266–278.
8. W. Fletcher, R. Silver, Algorithm 284: Interchange of two blocks of data, *Commun. ACM* **9**, no. 5 (1966) 326.
9. J. B. Fraleigh, *A First Course in Abstract Algebra*. Seventh edition. Addison-Wesley, 2003.
10. F. Gustavson, L. Karlsson, B. Kågström, Parallel and cache-efficient in-place matrix storage format conversion, *ACM Trans. Math. Software* **38** no. 3 (2012) 17:1–17:32.
11. M. R. Ito, Remark on algorithm 284: Interchange of two blocks of data, *ACM Trans. Math. Software* **2**, no. 4 (1976) 392–393.
12. J. A. Gallian, *Contemporary Abstract Algebra*. Sixth edition. Houghton-Mifflin, Belmont, CA, 2006.
13. G. A. Jones, J. Mary Jones, *Elementary Number Theory*. Springer-Verlag, New York, 1998.
14. D. E. Knuth, *The Art of Computer Programming* Vol. I. Addison-Wesley, Reading, MA, 1969.
15. S. Krishnamoorthy, G. Baumgartner, D. Cociorva, C.-C. Lam, P. Sadayappan, Efficient parallel out-of-core matrix transposition, *Int. J. High Perf. Comp. Netw.* **2–4** (2004) 110–119.
16. S. Laflinm M. A. Brebner, Algorithm 380: In-situ transposition of a rectangular matrix, *Commun. ACM* **13**, no. 5 (1970) 324–326.
17. W. J. Leveque, *Topics in Number Theory*, Vols. 1 and 2. Reprint. Dover, 2002.
18. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *The Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, 1996, http://www.cacr.math.uwaterloo.ca/hac/.
19. I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*. Fifth edition. Wiley, New York, 1991.
20. G. Pall, E. Seiden, A problem in Abelian groups, with application to the transposition of a matrix on an electronic computer, *Math. Comp.* **14** (1960) 189–192.
21. D. J. Scully, Perfect shuffles through dynamical systems, *Math. Mag.* **77**, no. 2 (2004) 101–117.
22. P. F. Windley, Transposing matrices in a digital computer, *Comput. J.* **2** (1959) 47–48.

Summary. Converting a matrix from row-order storage to column-order storage involves permuting the entries of the matrix. How can we determine this permutation given only the size of the matrix? Unexpectedly, the solution to this question involves the use of elementary group theory and number theory. This includes the Chinese

remainder theorem, finding multiplicative generators modulo p^n for prime p, and using these to find orbit generators for a group action, a subgroup of $\mathbb{Z}_N^*$ acting on all of $\mathbb{Z}_N$.

JEFF HOOPER (MR Author ID: 606548 is a professor and head of the Department of Mathematics and Statistics at Acadia University in Nova Scotia. He holds B.Sc. and M.Sc. degrees from the University of Windsor and a Ph.D. from McMaster University, and his main research area is number theory and arithmetic geometry.

FRANKLIN MENDIVIL (MR Author ID: 610124) is a professor of mathematics at Acadia University in Nova Scotia. His research is mainly a blend of fractal geometry and analysis, image processing, and optimization. He considers himself extremely lucky to be in a profession that allows him to explore many different topics.

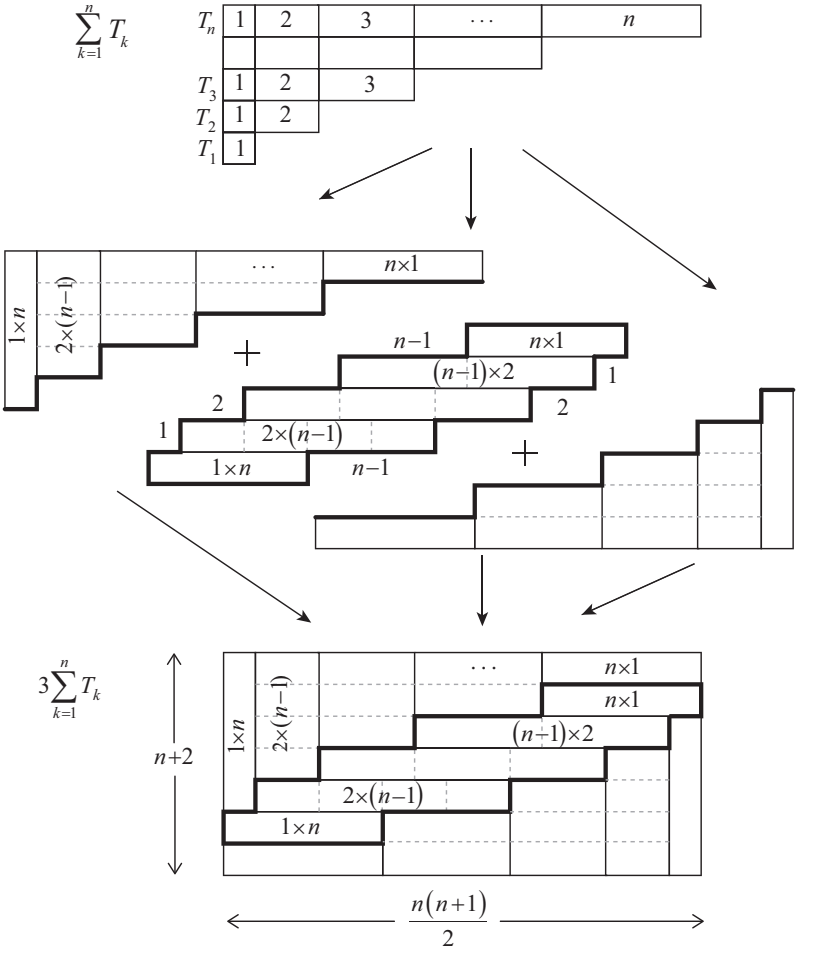
Proof Without Words: Sum of Triangular Numbers

ÁNGEL PLAZA
Universidad de Las Palmas de Gran Canaria
Las Palmas, Canarias, Spain
angel.plaza@ulpgc.es

Theorem.

$$T_n = 1 + 2 + \cdots n = \frac{n(n+1)}{2} = \binom{n+1}{2} \Rightarrow \sum_{k=1}^{n} T_k = \frac{n(n+1)(n+2)}{6}.$$

Proof.



■

Math. Mag. **89** (2016) 36–37. doi:10.4169/math.mag.89.1.36.
MSC: Primary 11Y55.

This proof is close to, and it can be seen as a variation of, Zerger's proof [**1**], which also appears on page 94 of Nelsen's compendium of PWWs [**2**].

REFERENCES

1. M. J. Zerger, *Proof Without Words: Sum of Triangular Numbers, Math. Mag.* **63** no. 5 (1990) 314.
2. R. B. Nelsen, *Proof without Words: Exercises in Visual Thinking*. The Mathematical Association of America, Washington, DC, 1993.

Summary. The triangular numbers are given by the following explicit formulas: $T_n = 1 + 2 + \cdots n = \frac{n(n+1)}{2} = \binom{n+1}{2}$. Here it is proved visually that

$$\sum_{k=1}^{n} T_k = \frac{n(n+1)(n+2)}{6}.$$

DR. ANGEL PLAZA (MR Author ID: 350023) received his masters degree from Universidad Complutense de Madrid in 1984 and his Ph.D. from Universidad de Las Palmas de Gran Canaria in 1993, where he is a Full Professor in Applied Mathematics. He is interested in mesh generation and refinement, combinatorics and visualization support in teaching and learning mathematics.

Exploring the Chermak–Delgado Lattice

ELIZABETH WILCOX
Oswego State University (SUNY)
Oswego, New York 13126
elizabeth.wilcox@oswego.edu

In 1989 [**2**], A. Chermak and A. Delgado introduced a family of measures for a subgroup of a finite group. One of these measures, now referred to as the Chermak–Delgado measure, teases one into traveling down a rabbit hole of group theory with many interesting connections along the way. A short section in a recent group theory textbook by I. Martin Isaacs [**6**, Section 1G] inspired my journey down that rabbit hole—and a whole host of collaborators came with me [**1, 3, 4, 5**]. Now I'm inviting undergraduate mathematics students and their faculty mentors to join me in the "wonderland" of Chermak–Delgado lattices.

Every finite group has an associated Chermak–Delgado lattice. Not much is known about the Chermak–Delgado lattice of a group; the real connection between the Chermak–Delgado lattice of the group and the overall structure of the group is not yet clear. This opens the door for undergraduate students and faculty members interested in diving deeper into group theory to make a significant contribution—even writing an effective algorithm for computing and visualizing the Chermak–Delgado lattice of a given group would be a sizeable task, and yet, the steps along the way are suitable for an undergraduate student.

Here's how this paper works: The first two sections provide the framework of an independent study in group theory for an undergraduate who has already had an introductory class on the topic. Since these classes don't all cover the same material, the first section provides the definitions and ideas that are necessary before digging into the second section, where Chermak–Delgado lattices are defined and explored. The emphasis is on *independent*—the student and the faculty member should actively make the connections between the topics in the first section and their value with respect to the Chermak–Delgado lattice, in the tradition of active, independent learning.

If a student is intrigued by the taste of Chermak–Delgado lattices from the first two sections, then there are open questions and ideas for projects in the third section. These suggestions are aimed a variety of levels—some may be great for a computationally minded undergraduate student while others may turn out to be the depth of a master's level thesis or even a doctoral thesis.

The tail of the white rabbit To find the rabbit hole into our particular wonderland, you must find the white rabbit. While Alice was fortunate enough to simply catch sight of him scurrying along one afternoon, you, dear would-be traveler, must seek him out. Fortunately, I can guide you to his usual haunts!

There are challenges along the way, hills to climb and the like, so remember that nothing worth having comes without a toll. These challenges will build up your strength and understanding, but you will also need a bit of fortification along the journey; definitions here and there will provide some of that fortification.

Math. Mag. **89** (2016) 38–44. doi:10.4169/math.mag.89.1.38.
MSC: Primary 20E15, Secondary 20D30.

Definition. Let G be a group and let H and K be subgroups of G (denoted by $H, K \leq G$).

1. The product of H and K is $HK = \{hk \mid h \in H, k \in K\}$.
2. The subgroup generated by H and K, denoted by $\langle H, K \rangle$, is the smallest subgroup of G that contains both H and K (as subgroups).

Challenges. To simplify notation, use $|X|$ to denote the cardinality of a set X.

1. Give an example of a group G and two subgroups H, K of G such that HK is *not* a subgroup of G. Compute $\langle H, K \rangle$ for comparison.
2. Let G be any group with $H, K \leq G$. Show that $HK \subseteq \langle H, K \rangle$.
3. Let G now be a finite group and let $H, K \leq G$. Give a formula for $|HK|$.
4. Let G be a group and let $H, K \leq G$. Prove that $H \cap K \leq G$.

These challenges require a wayfarer to understand a bit of set theory and the difference between a subset and a subgroup. Innocuous, right? But these ideas are the foundation behind the subgroup lattice of a group, a means of picturing the subgroup structure of a given group.

Definition. Let G be a group.

1. The *subgroup lattice of* G is the set of subgroups of G. This set is a partially ordered set under the binary relation $\leq$.
2. A *subgroup lattice diagram* for a group G is a picture that includes all subgroups of G as vertices. A line is drawn between two distinct subgroups H and K with K above H if $H \leq K$ but no other subgroup L has the property $H \leq L \leq K$. Usually, subgroups with the same cardinality are drawn at the same height in the lattice, giving an indication of relative cardinality.

Many undergraduate abstract algebra courses introduce the idea of a subgroup lattice diagram, sometimes as a way of distinguishing nonisomorphic groups. The traveler may be familiar with the subgroup lattices for the additive cyclic group of order 6 ($\mathbb{Z}/6\mathbb{Z}$), the dihedral group of order 8 (D_8), and the quaternion group of order 8 (Q_8) shown in Figure 1. Later on, we will return to these groups and more carefully define the notation describing them.

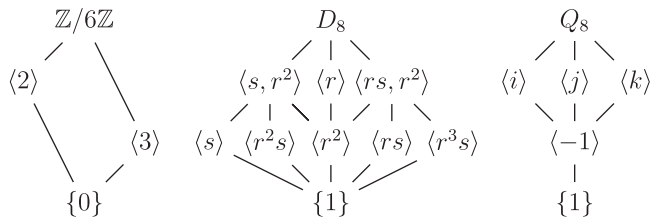


Figure 1 Examples of subgroup lattices.

Often, undergraduates only see the idea of the *centralizer of a subgroup* on a homework assignment or exam. Versatility in this concept is required for maneuvering successfully in the wonderland to which we are headed.

Definition. Let G be a group and $H \leq G$. The *centralizer of H (in G)* is the set of all elements in G that commute with every element in H. We denote this set by $C_G(H)$. When $H = G$, we call the resulting centralizer the *center of* G and denote it by $\mathrm{Z}(G)$.

Challenges. Let G be a group and $H \leq G$.

5. Prove that $C_G(H)$ is a subgroup of G.
6. Prove that $\mathrm{Z}(G) \leq C_G(H)$ for all $H \leq G$.
7. Let A be an abelian subgroup of G (meaning that for all $a_1, a_2 \in A$, it is true that $a_1a_2 = a_2a_1$). Explain why $A \leq C_G(A)$.
8. Show $H \leq C_G(C_G(H))$.
9. Let $K \leq G$. Show that $C_G(H)C_G(K) \subseteq C_G(H \cap K)$.

Finally, the journeyer must be prepared to encounter group automorphisms and conjugation. A typical undergraduate algebra course discusses *isomorphisms of groups*; a wide-eyed wayfarer should relax: *automorphisms* and *conjugation* are specific kinds of isomorphisms—don't yet be dismayed!

Definition. Let G be a group and let $H \leq G$.

1. An *automorphism of* G is a bijection $\varphi : G \to G$ that is also a homomorphism, meaning that $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$. The *image of* H *under* φ is the set $\varphi(H) = \{\varphi(h) \mid h \in H\}$.
2. Let $x \in G$. *Conjugation by* x refers to the operation of multiplying on the left by x^{-1} and on the right by x. For $g \in G$, the *conjugate of* g *by* x is $x^{-1}gx$, while the *conjugate of* H *by* x would be $\{x^{-1}hx \mid h \in H\}$. We denote the former by g^x and the latter by H^x.

Challenges. Let G be a group with $H \leq G$ and fix $x \in G$.

10. Let φ be an automorphism of G. Prove that $\varphi(H) \leq G$ and that the cardinality of H equals the cardinality of $\varphi(H)$.
11. Establish that $\tau_x : G \to G$ defined by $\tau_x(g) = x^{-1}gx$ for all $g \in G$ is an automorphism of G.
12. Prove that $C_G(H^x) = (C_G(H))^x$.

Do not allow yourself to flag under the notation; go back to the definitions. When in doubt, pick your favorite *nonabelian* group and work out some examples.

Down the rabbit hole For a wayfarer who has successfully found the white rabbit and followed him to the opening of the rabbit hole, then there's nothing left to do but to *jump in!*

Definition. Let G be a finite group and let $H \leq G$.

1. The *Chermak–Delgado measure of* H *(in* G*)* is defined as $m_G(H) = |H||C_G(H)|$.
2. Let $m^*(G)$ denote the maximum of the set $\{m_G(H) \mid H \leq G\}$. The *Chermak–Delgado lattice of* G is the set of subgroups of G with maximal Chermak–Delgado measure, i.e., $\mathcal{CD}(G) = \{H \leq G \mid m_G(H) = m^*(G)\}$.

The first instinct, once the leap is made, is to try to slow the fall—grab this way and that, hope to catch hold of a root or rock. Quell that instinct, brave journeyer! Become comfortable with the fall—remember that Alice landed softly; try working out a few examples.

Challenge.

13. For each of the following, compute both $m^*(G)$ and the Chermak–Delgado lattice of G.

(a) The cyclic group of order n, denoted $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$ (under addition modulo n) for as many values of n as you can stand—or until you get the pattern.

(b) The dihedral groups of order 6, 8, 10, and 12. If we denote the dihedral group of order $2n$ by D_{2n}, then this group has presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$. Do you see a pattern as the order gets larger?

(c) The quaternion group of order 8, denoted by Q_8. This group is the set $\{\pm 1, \pm i, \pm j, \pm k\}$ where $ij = k = -ji$.

Notice that these calculations are tedious, with one exception—those cyclic groups were easy, once the trick was mastered. Let's turn that into a small result, for which you should write up a neat and tidy proof.

Proposition. The Chermak–Delgado lattice of a finite abelian group A is $\{A\}$.

Additionally, notice that these Chermak–Delgado lattices can be visualized just like subgroup lattices. Leave out all subgroups that are not in $\mathcal{CD}(G)$, but draw a line between two subgroups $H, K \in \mathcal{CD}(G)$ with K above H if $H \leq K$, but no other subgroup $L \in \mathcal{CD}(G)$ has the property $H \leq L \leq K$.

While falling down a seemingly endless tunnel, a journeyer may as well create lattice diagrams for the lattices computed earlier. To aid, I give a group and its Chermak–Delgado lattice; I am known to make errors so verify my calculations carefully.

Example. Let $\mathcal{H}$ be the group described below:

$$\mathcal{H} = \left\{ \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \,\middle|\, x, y, z \in \mathbb{Z}/3\mathbb{Z} \right\}$$

under the binary operation of matrix multiplication, where $\mathbb{Z}/3\mathbb{Z}$ is the abelian group with base set $\{0, 1, 2\}$ under addition modulo 3. The group $\mathcal{H}$ is known as the Heisenberg group modulo 3; it has 27 elements, including the 3×3 identity matrix (1s on the diagonal, 0s off the diagonal) as its identity element.

A warning for travelers: $\mathrm{Z}(\mathcal{H})$ has only three elements in it! Checking the conditions under which two elements of $\mathcal{H}$ will commute straightforwardly produces the elements of $\mathrm{Z}(\mathcal{H})$. Ultimately, the journeyer will see that the Chermak–Delgado lattice of $\mathcal{H}$ is as appears in Figure 2 where

$$A = \left\langle \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\rangle, \quad B = \left\langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\rangle,$$

$$C = \left\langle \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\rangle, \quad D = \left\langle \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\rangle, \text{ and}$$

$$\mathrm{Z}(\mathcal{H}) = \left\langle \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\rangle.$$

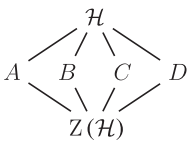


Figure 2 $\mathcal{CD}(\mathcal{H})$.

The first step is to prove that $m^*(\mathcal{H}) = 81$, for then it will automatically be true that $\mathcal{H}$ and $\mathrm{Z}(\mathcal{H})$ are members of $\mathcal{CD}(\mathcal{H})$. Moreover, the reader should not be afraid to read up on results about groups of order p^3, such as $\mathcal{H}$. Much is known about these groups, and a little extra reading may prove useful later.

Wayfarer, compare the Chermak–Delgado lattice diagrams for the groups in the previous challenge to the subgroup lattice diagrams for the corresponding groups. What observations can you make?

There are many ends to be tied up here: How can we streamline these calculations? Why is this set $\mathcal{CD}(G)$ called a *lattice*? Is it coincidence that the Chermak–Delgado lattice diagrams of the dihedral group of order 8 and the quaternion group of order 8 look similar? Is it coincidence that all of the computed Chermak–Delgado lattices have a horizontal line of symmetry (when neatly drawn)? Let's start with the reason why the Chermak–Delgado lattice is called a *lattice* and not just "set."

Definition. A *lattice* is a set L with two binary operations, $\vee : L \times L \to L$ (referred to as the *join operation*) and $\wedge : L \times L \to L$ (referred to as the *meet operation*). These operations must be commutative and associative, but must also obey the *absorption laws*:

$$a \vee (a \wedge b) = a \quad \text{and} \quad a \wedge (a \vee b) = a$$

for all $a, b \in L$.

Challenges. Let G be a finite group.

14. Let $H, K \leq G$. Show that the subgroup lattice of G is a lattice with $H \wedge K = H \cap K$ and $H \vee K = \langle H, K \rangle$.
15. Let $H, K \in \mathcal{CD}(G)$. Show that the Chermak–Delgado lattice of G is a lattice with intersection $(H \cap K)$ as the meet operation, $\wedge$, and subgroup product (HK) as the join operation, $\vee$. (Hint: Think about order comparisons and start by considering $\langle H, K \rangle$—the usual join operation for the subgroup lattice of G.)
16. Let L be a lattice with $\vee$ as its join and $\wedge$ as its meet. Show that if $a \in L$, then $a \wedge a = a$ and $a \vee a = a$. These properties are called the *idempotent laws*; what do the idempotent laws state with respect to the subgroup lattice and the Chermak–Delgado lattice of a finite group G?
17. Show that if $H \in \mathcal{CD}(G)$, then $C_G(H) \in \mathcal{CD}(G)$ and $C_G(C_G(H)) = H$.
18. Prove that $\delta : \mathcal{CD}(G) \to \mathcal{CD}(G)$ defined by $\delta(H) = C_G(H)$ is a bijection such that if $H \leq K$ for $H, K \in \mathcal{CD}(G)$, then $\delta(K) \leq \delta(H)$ and $\delta(\delta(H)) = H$.
19. Let $\varphi : G \to G$ be an automorphism of G. Prove that if $H \in \mathcal{CD}(G)$, then $\varphi(H) \in \mathcal{CD}(G)$.
20. One fact about nonempty finite lattices is that there is a unique maximum and a unique minimum in the lattice. With regard to the Chermak–Delgado lattice, show that this means both the subgroup at the top of the lattice and the subgroup at the bottom are both characteristic—in particular, normal—subgroups.
21. Prove that if M is the minimum of $\mathcal{CD}(G)$, then $\mathrm{Z}(G) \leq M$ and M is abelian.

These challenges establish three important facts: (1) $\mathcal{CD}(G)$ is not just a set but an actual lattice. In fact, it's a sublattice of the subgroup lattice because $\langle H, K \rangle = HK$ for all $H, K \in \mathcal{CD}(G)$. (2) The lattice $\mathcal{CD}(G)$ is a *dual* lattice because the function δ, visually speaking, forces a horizontal line of symmetry on the lattice diagram of $\mathcal{CD}(G)$. (3) The last challenge tells us, in particular, that if $H \in \mathcal{CD}(G)$, then all conjugates of H are also in $\mathcal{CD}(G)$. That fact really does cut down on computations in large groups, although in all of our examples here the subgroups in $\mathcal{CD}(G)$ have been normal.

Curiouser and curiouser . . .

. . . or how to stay lost in Wonderland

So now that you're here in the Chermak–Delgado lattice wonderland, what adventures are next on your path? Some of that depends on you. You could attempt one or more of the following projects.

- Choose an interesting finite group for which you can compute the Chermak–Delgado lattice, probably with the aid of software such as Sage [**8**], GAP [**7**], or Magma [**9**]. (Note that Sage actually calls on GAP, but students may be familiar with Sage from previous coursework or research experiences.) Groups with cardinality equal to a power of a prime, such as $\mathcal{H}$, are particularly interesting to work with, but groups G with $\mathrm{Z}(G) = 1$ can be equally fascinating.

  (The reader should note that "$\mathrm{Z}(G) = 1$" is a group theorist's shortcut for "the center of G is the trivial subgroup." It's common throughout the literature, despite not being notationally precise, and a reader should keep an eye out for this notation should he/she choose to look into the references.)
- Write a program to compute the Chermak–Delgado lattice of all groups in a particular library within GAP. Imagine the value of a program that organized the output into a lattice diagram or a printout that makes identifying the lattice diagram easy!
- Use software to find the smallest order of a group G such that there exists $H \leq G$ with $H \in \mathcal{CD}(G)$ but where H is not normal in G. The answer to this question was published in 2012 [**1**], but the program should also allow one to find larger examples that haven't yet been identified.
- Study groups with a particular Chermak–Delgado lattice. For example, groups with a Chermak–Delgado lattice of the form $\{G, \mathrm{Z}(G)\}$ were studied by Brewster, Hauck, and Wilcox [**3**]. What can be said of G such that $\mathcal{CD}(G) = \{K\}$ for a single $K \leq G$? Clearly, $K = G$ if and only if G is abelian, but the situation is less clear when $K < G$.
- Study the Chermak–Delgado lattice of groups with a particular structure. Direct products were studied by Brewster and Wilcox [**1**], but this paper also takes a look at certain wreath products. You might consider wreath products with the excluded structure or groups G where $\mathrm{Z}(G) = 1$.
- Study the automorphisms and embeddings of G in relation to the Chermak–Delgado lattice. This adventure sounds vague; that's only because unexplored territory is difficult to describe explicitly!

Each of these projects either is or leads into an open research question. With respect to the Chermak–Delgado lattice, you're on the edge of the unknown. No one knows where you will end up or what will come of your efforts. Good luck, take care, and enjoy the adventure!

Acknowledgment I'd like to thank Amy Hannahan, a student at Oswego State University, for being the inspiration of this article. Working with Amy is what made me realize just how much fun it could be to work on a project like this with an undergraduate student—both the student and the faculty mentor can learn a lot from the experience . . . and the contributions don't need to be significant in the scope of the research universe to make a significant difference in the lives of those working on the project.

REFERENCES

1. B. Brewster, E. Wilcox, Some groups with computable Chermak–Delgado lattices, *Bull. Aus. Math. Soc.* **86** (2012) 29–40.
2. A. Chermak, A. Delgado, A measuring argument for finite groups, *Proc. AMS* **107** no. 4 (1989) 901–914.

3. B. Brewster, P. Hauck, E. Wilcox, Groups whose Chermak–Delgado lattice is a chain, *J. Group Th.* 17 (2014) 253–279.
4. B. Brewster, P. Hauck, E. Wilcox, Groups where the Chermak–Delgado lattice is a quasiantichain, *Archiv der Mathematik* **103** no. 4 (2014) 301–311.
5. L. An, H. Qu, J. Brennan, E. Wilcox, Chermak–Delgado lattice extension theorems, *Comm. Algebra* **43** no. 5 (2015) 2201–2213.
6. I. M. Isaacs, *Finite Group Theory.* AMS, 2008, Providence, Rhode Island.
7. The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.7.5. (2014), http://www.gap-system.org.
8. W. A. Stein et. al., The Sage Development Team. Sage Mathematics Software (Version 6.5). (2014), http://www.gap-system.org.
9. The Magma Group, Magma Computational Algebra System (Version 2.21-9). (2015), http://magma.maths.usyd.edu.au/magma/.

Summary. Need a project to satisfy your craving for abstract algebra? Or do you have a student nosing around your office looking for a project? The Chermak–Delgado lattice is a sublattice of the subgroup lattice of a finite group. The details of its definition don't require advanced group theory, though working with this lattice can send one on a journey through deeper, more advanced techniques. This makes the Chermak–Delgado lattice the perfect starting point for an undergraduate project after an abstract algebra class. This article guides the curious reader through a series of exercises about the Chermak–Delgado lattice to provide preparation and fuel interest, before posing several open-ended questions for investigation.

ELIZABETH WILCOX (MR Author ID: 935712) is an assistant professor in the Mathematics Department at the State University of New York in Oswego—where the ever-falling lake effect snow brings out the "Mad Hatter" in everyone during the winter months. Studying mathematics, especially group theory, is the only successful prescription for the ailment!

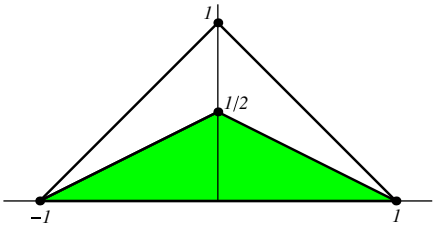
Artist Spotlight
Bjarne Jespersen

Asa Link, Bjarne Jespersen; Mahogany, 5 cm in diameter, 1972; private collection. Three four-sided hosohedral edge frames weave together.

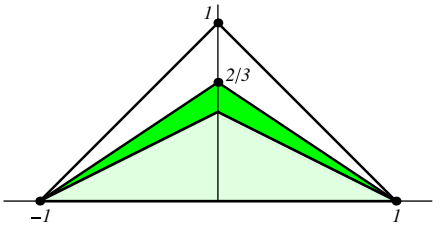
See interview on page 55.

Proof Without Words: The Sum $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)}+\cdots=1$ and Its Partial Sums

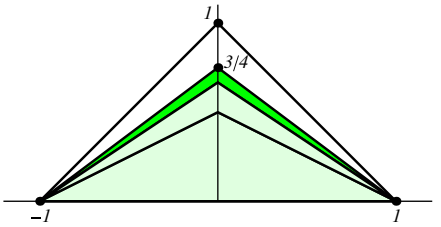
ÓSCAR CIAURRI[1]
Universidad de La Rioja
Logroño, Spain
oscar.ciaurri@unirioja.es



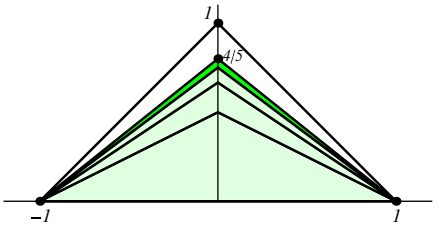
$$\frac{1}{1\cdot 2}=\frac{1}{2}$$



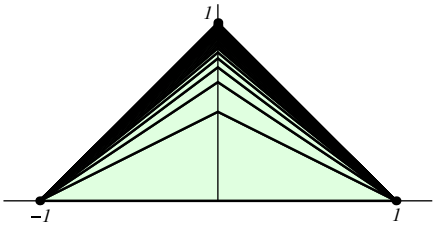
$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}=\frac{2}{3}$$



$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}=\frac{3}{4}$$



$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\frac{1}{4\cdot 5}=\frac{4}{5}$$



$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)}+\cdots=1$$

[1]Research supported by grant MTM2012-36732-C03-02 of the DGI
Math. Mag. **89** (2016) 45–46. doi:10.4169/math.mag.89.1.45.
MSC: Primary 00A01.

Summary. We provide a visual proof of the identity $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n\cdot(n+1)}+\cdots=1$ including its partial sums.

ÓSCAR CIAURRI (MR Author ID: 651273) (Logroño, 1971). He received his degree in Mathematical Sciences from Universidad Autónoma de Madrid in 1995 and his Ph.D. from Universidad de La Rioja in 2000. Currently he is a professor at the latter university.

Artist Spotlight
Bjarne Jespersen

Great Tetraknot, Bjarne Jespersen; Wood (elm), 9.5 cm in diameter, 2002; private collection. A compound of four trefoil knots oriented as the faces of a tetrahedron. Its symmetry is that of the tetrahedron, but without mirror reflections.

See interview on page 55.

One-Glance(ish) Proofs of Pythagoras' Theorem for 60-Degree and 120-Degree Triangles

BURKARD POLSTER
MARTY ROSS
School of Mathematical Sciences
Monash University, Australia
burkard.polster@monash.edu
martinirossi@gmail.com

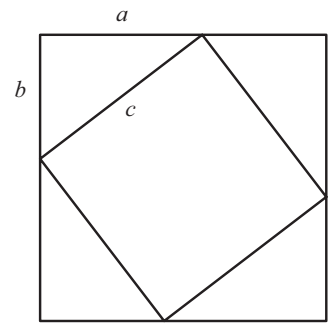
Considering all triangles that include a fixed angle γ, the cosine rule

$$a^2 + b^2 - 2ab\cos(\gamma) = c^2$$

provides a counterpart to Pythagoras' theorem and reduces to Pythagoras' theorem when γ is 90 degrees. The angles 60 degrees and 120 degrees are also worthy of note since the term $2\cos(\gamma)$ is then an integer and the cosine rule takes almost as simple a form.

Theorem (Pythagoras for 60- and 120-degree triangles) *Let T be a triangle with sides a, b, and c. If the angle opposite c is 60 degrees, then $a^2 + b^2 - ab = c^2$. If the angle opposite c is 120 degrees, then $a^2 + b^2 + ab = c^2$.*

In the following, we'll present some elementary and pretty proofs of the above theorem. They will mimic the two famous proofs of Pythagoras' theorem summarized in Figure 1.



first proof

$$\begin{array}{c}\text{area of}\\ \text{big square}\end{array} = \begin{array}{c}\text{area of}\\ \text{small square}\end{array} + \begin{array}{c}\text{area of}\\ 4\cdot\text{triangle}\end{array}$$

$$(a+b)^2 = c^2 + 4\,\frac{ab}{2}$$

$$\text{So,}\quad a^2 + b^2 = c^2$$

second proof

$$\begin{array}{c}\text{area of}\\ \text{small square}\end{array} + \begin{array}{c}\text{area of}\\ 4\cdot\text{triangle}\end{array} = \begin{array}{c}\text{area of}\\ \text{big square}\end{array}$$

$$(a-b)^2 + 4\,\frac{ab}{2} = c^2$$

$$\text{So,}\quad a^2 + b^2 = c^2$$

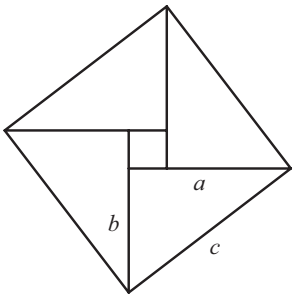


Figure 1 Two well-known proofs of Pythagoras' theorem.

Math. Mag. **89** (2016) 47–54. doi:10.4169/math.mag.89.1.47.
MSC: Primary 51-00.

Some simple proofs

We will make use of the following simple result.

Let g be the area of the isosceles triangle with sides of length 1 forming the angle γ, as pictured in Figure 2, on the left. Then the triangle shown on the right, with sides a and b forming the same angle γ, has area gab.

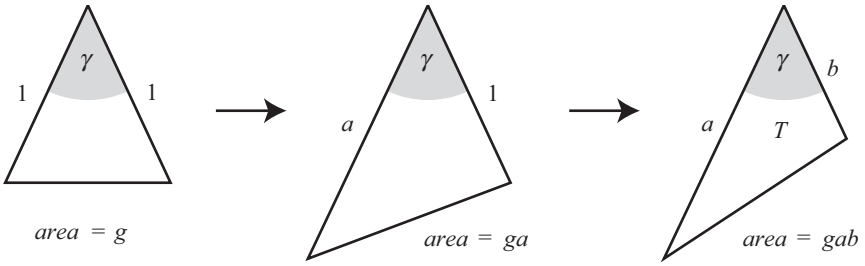


Figure 2 The areas of three triangles sharing the same angle.

This result, with $g = \frac{1}{2}\sin(\gamma)$, can be easily proved with a little trigonometry. However, in this note, we'll avoid anything so sophisticated as trigonometry, and in fact all that is required here is the triangle area formula $\frac{1}{2} \cdot base \cdot height$. We first stretch the isosceles triangle in the direction of one edge by a factor a, with the a side treated as the base; this produces the middle triangle, with area ga. Then, we stretch in the second direction by a factor b, with the b side treated as the base; the end result is the desired triangle, on the right, with area gab.

First proof of the 60-degree Pythagorean theorem. Arrange three copies of the 60-degree triangle T into an equilateral triangle, as pictured in Figure 3.

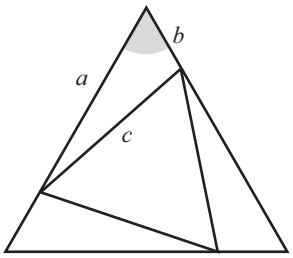


Figure 3 Three copies of a 60-degree triangle arranged into an equilateral triangle.

Then, area of the big triangle = area of the small triangle + 3 · (area of T), and so

$$g(a+b)^2 = gc^2 + 3gab.$$

Simplifying, we conclude that

$$a^2 + b^2 - ab = c^2.$$

Second proof of the 60-degree Pythagorean theorem. Arrange six copies of the 60-degree triangle T into a regular hexagon, as pictured in Figure 4.

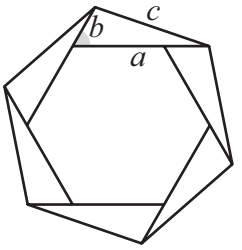


Figure 4 Six copies of a 60-degree triangle arranged into a regular hexagon.

Then, area of the big hexagon = area of the small hexagon + 6 · (area of T). Since the area of a regular hexagon is six times the area of an equilateral triangle sharing the same side length, it follows that

$$6gc^2 = 6g(a-b)^2 + 6gab.$$

Simplifying, we conclude once again that

$$a^2 + b^2 - ab = c^2.$$

First proof of the 120-degree Pythagorean theorem. Arrange six copies of the 120-degree triangle T as pictured in Figure 5, on the left.

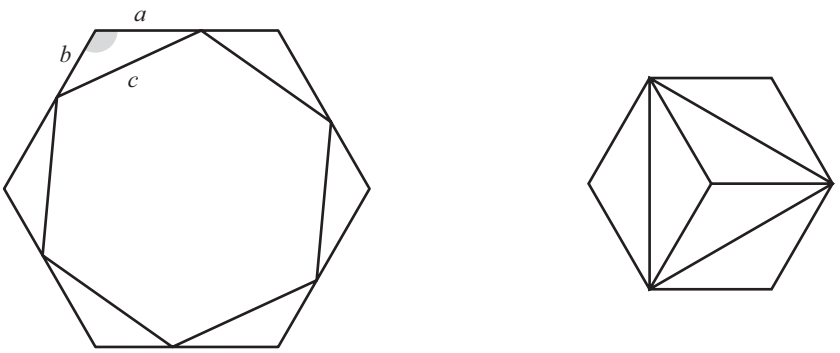


Figure 5 Six copies of a 120-degree triangle arranged into a regular hexagon (left) and a regular hexagon dissected into six copies of an isosceles 120-degree triangle (right).

Then, area of the big hexagon = area of the small hexagon + 6 · (area of T). We reinterpret this equation, using the fact that any regular hexagon can be cut into six congruent isosceles 120-degree triangles, as shown in Figure 5, on the right. Then our equation can be written as

$$6g(a+b)^2 = 6gc^2 + 6gab,$$

which simplifies to

$$a^2 + b^2 + ab = c^2.$$

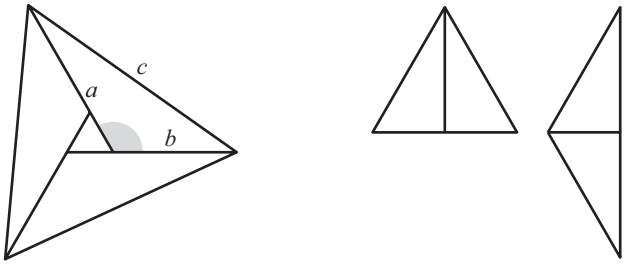


Figure 6 Three copies of a 120-degree triangle arranged into an equilateral triangle (left) and dissecting an equilateral triangle and rearranging the pieces into an isosceles 120-degree triangle (right).

Second proof of the 120-degree Pythagorean theorem. Arrange three copies of the 120-degree triangle T as pictured in Figure 6 on the left.

Then area of the big triangle = area of the small triangle + $3 \cdot$ (area of T).

We reinterpret this equation, using the fact that any equilateral triangle can be dissected and rearranged into an isosceles 120-degree triangle, as pictured in Figure 6 on the right. Then our equation can be written as

$$gc^2 = g(a-b)^2 + 3gab,$$

and we conclude once again that

$$a^2 + b^2 + ab = c^2.$$

Using the 60- and 120-degree theorem to prove the 90-degree theorem

Our 60-degree Pythagorean theorem also follows very easily from the 120-degree Pythagorean theorem and vice versa. To see this, begin with a 60-degree triangle and draw in a 120-degree triangle, as pictured in Figure 7.

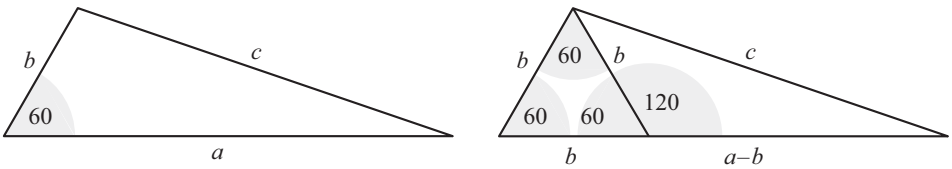


Figure 7 Relating 60-degree and 120-degree triangles.

Then the 120-degree Pythagorean theorem for this new triangle implies

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

Simplifying, this gives

$$a^2 + b^2 - ab = c^2,$$

which is the 60-degree Pythagorean theorem for the original triangle.

With some relabelling, the same diagram can be used to derive the 120-degree Pythagorean theorem from the 60-degree Pythagorean theorem; we leave the details to the reader.

Pythagoras' theorem itself also follows easily from the 60-degree Pythagorean theorem and the 120-degree Pythagorean theorem. To see this, consider a right-angled triangle with sides a, b, and c. Then we can cut this triangle into a 60-degree and a 120-degree triangle, as indicated in Figure 8.

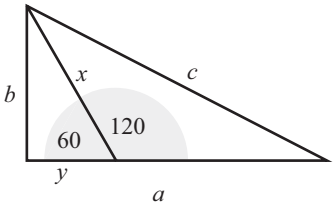


Figure 8 A right-angled triangle dissected into a 60-degree and a 120-degree triangle.

Now we subtract our Pythagorean identity for the 60-degree triangle,

$$x^2 + y^2 - xy = b^2,$$

from our Pythagorean identity for the 120-degree triangle,

$$x^2 + (a - y)^2 + x(a - y) = c^2,$$

to arrive at

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

Since the 60-degree triangle is half of an equilateral triangle it follows that the factor $x - 2y$ is equal to 0, and so this last equation reduces to Pythagoras' theorem.

Conversely, the same diagram in Figure 8 with suitable relabelling can be used to derive the 120-degree Pythagorean theorem from Pythagoras' theorem; one combines the Pythagorean identities for the two right-angled triangles in Figure 8.

Summarizing, we conclude that our 60/120-degree Pythagorean theorem is equivalent to Pythagoras' theorem. So, who knows: Perhaps for a race of bee-like aliens, one with a preference for 120-degree angles, the 60/120-degree Pythagorean theorem combination is considered fundamental to their mathematics.

Beyond 60-, 90- and 120-degree triangles

Our first proof of the 60-degree Pythagorean theorem only involves 60-degree triangles, whereas the other three proofs also make use of the close relationship between equilateral triangles and regular hexagons. For this reason, we regard our first proof as the simplest, comparable to the first proof of Pythagoras' theorem.

Of course, the cosine rule fully generalizes the 60-90-120 Pythagorean theorems, which implies there are very general versions of pretty much everything we've demonstrated above; see also [**2**] and [**3**] for an interesting and very general alternative interpretation of the sort of diagrams that we are considering in this article. However, as in the previous discussion, we are interested in highlighting special cases for which there are simple arguments.

Our basic strategy does not yield anything *really* simple for triangles other than those based on 60, 120 (and 90) degrees. The best we've been able to come up with is a setup for a triangle T^* that features an interior angle of 108 degrees, that is, the interior angle of a regular pentagon.

Mimicking our first proof of the 60-degree Pythagoras, we begin by arranging five copies of the triangle T^* into a regular pentagon as in Figure 9.

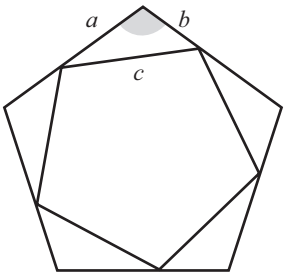


Figure 9 Five copies of a 108-degree triangle arranged into a regular pentagon.

Then, area of the big pentagon = area of the small pentagon + 5 · (area of T^*).

To proceed further, we need to represent the regular pentagon in terms of 108-degree triangles. This can be done as pictured in Figure 10, with the pentagon the union of four congruent isosceles triangles, minus a similar but scaled down triangle (being the overlap of two triangles, as pictured in the third diagram).

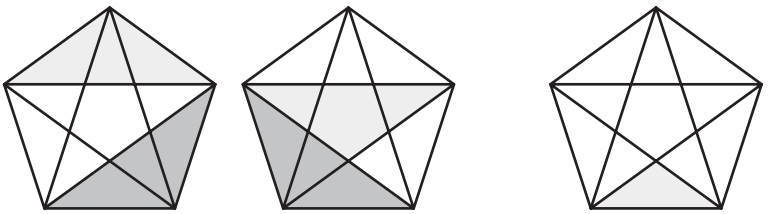


Figure 10 Isosceles 108-degree triangles inside a regular pentagon.

The pentagon has side length $a + b$, so each of the congruent triangles will have area $g(a + b)^2$. Also, since the ratio of a diagonal to a side of the pentagon is the golden ratio ϕ, the smaller, subtracted triangle has area $g(a + b)^2/\phi^2$. It follows that the area of the pentagon is

$$g(a+b)^2\left(4-\frac{1}{\phi^2}\right).$$

Therefore, our Pythagoras proof diagram translates into the equation

$$g(a+b)^2\left(4-\frac{1}{\phi^2}\right) = gc^2\left(4-\frac{1}{\phi^2}\right) + 5gab.$$

Substituting $\phi = \frac{1+\sqrt{5}}{2}$, this simplifies to the Pythagorean theorem for 108-degree triangles:

$$a^2 + b^2 + \frac{\sqrt{5}-1}{2}ab = c^2.$$

Okay, this may be interesting enough, but overall it seems too fiddly to warrant pushing much further.

Pythagorean triples

We should also mention that a number of articles have been written in which the integer-sided triangles featuring angles of 60 or 120 degrees are classified; see [**4**] and the articles cited in this article, as well as [**1**]. The classification of the 60- and 120-degree Pythagorean triples was a surprise to us and is as elegant and as pleasing as the classification of the Pythagorean triples themselves. In particular, the simplest nontrivial 60-degree and 120-degree Pythagorean triples, 3-8-7 and 3-5-7, respectively, shown in Figure 11 are well worth committing to memory.

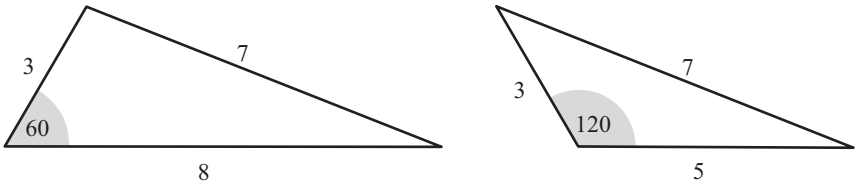


Figure 11 Simple 60- and 120-degree triangles with integer sides.

Finally, we note that the close relationship between the 60-degree Pythagorean theorem and the 120-degree Pythagorean theorem is also present at the level of the Pythagorean triples. In particular, the simple diagram that we used to relate the two Pythagorases is employed in some articles to establish a simple correspondence between the 60-degree Pythagorean triples and the 120-degree ones. For example, the two simple triples mentioned above are related as shown in Figure 12.

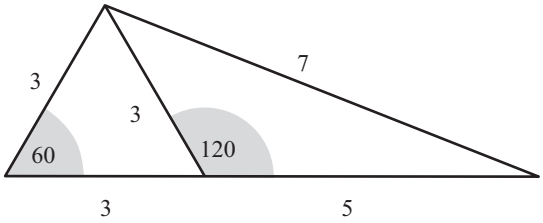


Figure 12 Relating 60- and 120-degree triangles with integer sides.

REFERENCES

1. H.T.R. Aude, Primitive integral triangles. *National Mathematics Magazine* **16** (1942), 280–283.
2. D. Veljan, An analogue of the Pythagorean theorem with regular n-gons instead of squares. *Elem. Math.* **51** (1996), 156–160.
3. D. Veljan, The 2500-year-old Pythagorean theorem. *Math. Mag.* **73** (2000), 259–272.
4. E. Read. Integer-sided triangles containing angles of 120° or 60°. *Math. Gaz.* **90** (2006), 299–305.

Summary. In this article we present some elementary proofs of the 60-degree and 120-degree counterparts of Pythagoras' theorem that mimic the two (most) famous one-glance proofs of Pythagoras' theorem.

BURKARD POLSTER (MR Author ID: 320849) received his Ph.D. in 1993 from the University of Erlangen-Nürnberg in Germany. He currently teaches mathematics at Monash University in Melbourne, Australia. Readers may have seen him in action as the Mathologer on YouTube or may be familiar with some of his books dealing with fun and beautiful mathematics such as *The Mathematics of Juggling, Q.E.D.: Beauty in Mathematical Proof* or *Math Goes to the Movies* (together with Marty Ross).

MARTY ROSS (MR Author ID: 270523) is a mathematical nomad. He received his Ph.D. in 1991 from Stanford University and has lectured at a number of universities in the U.S. and Australia. He is currently busy in Australia, popularizing mathematics and tweaking educational noses. When he is not partnering with Burkard Polster, Marty enjoys smashing calculators with a hammer. Burkard's and Marty's various activities can be checked out at http://www.qedcat.com.

Artist Spotlight
Bjarne Jespersen

Double Star, Bjarne Jespersen; Wood (pear), 4.5 cm in diameter, 1974; private collection. Two cubic edge frames are tied together with a half twist to each pair of edges, then reshaped to resemble Keplar's Stelle Octangula, the well known compound of two regular tetrahedra.

See interview on page 55.

Bjarne Jespersen: The Magic Woodcarver*

AMY L. REIMANN
Ella Sharp Museum
Jackson, MI 49203
amyr@ellasharp.org

DAVID A. REIMANN
Albion College
Albion, MI 49224-1831
dreimann@albion.edu

Bjarne Jespersen is a Danish artist specializing in geometric woodcarving and is the author of the book *Woodcarving Magic* (Fox Chapel Publishing, 2012). We met with Bjarne at the 2015 Bridges Conference in Baltimore to discuss his background, artwork, and book. A portion of this interview appears below. Accompanying artwork appears on the following pages: 15, 44, 46, 54, and 79.

Q: *How long have you been creating art?*

BJ: Well, if we call it art, what I'm doing. I call it "Magic Woodcarving." I've been doing that since I was around 17. I started much like what you call hobo art here with chains and balls in cages, but I soon found that rather trivial and then at the school of architecture I learned about solid geometry and symmetry and that got me started developing new ideas for this artform.

Q: *What is your main occupation?*

BJ: You mean for a living? Well, now I am retired. I've had various types of jobs, but most of the time it had to do with exhibitions. When I was young, I spent about ten years at a museum and did preservation work, which I was not educated for, but since I am very good with my hands, that's what I ended up doing. And whenever there was something I didn't know about, I was sent to other museums to be taught.

Q: *Can you tell us about your educational background?*

BJ: Well, I have some half educations. I started at the school of architecture, but thought I needed some more math and then I started at the university and studied math for a couple of years, but that was too much. I went back to the school of architecture, but then I had this job at the museum and gradually dropped out. I wasn't very good at studying.

Q: *Your book,* Woodcarving Magic*, contains many fascinating pictures and details on carving. Can you tell us some things that are in your book?*

BJ: One of the first chapters is about some traditions people have done over the years in various parts of the world. You probably know some of them. There's a lot of stuff about wood and so on, prototyping. We've got some simple projects that if you have some woodcarving experience you should be able to do. Then it becomes more and more complicated and difficult.

Q: *How long have you been attending Bridges conferences?*

BJ: My book is what got me to Bridges, so this is my sixth Bridges. I got a grant to go to the States to have everything photographed. The grant was from the David Collection in Copenhagen, a rather well known museum because they have this huge collection of Islamic art. It's a rather rich organization and they usually reserve grants

Math. Mag. **89** (2016) 55–57. doi:10.4169/math.mag.89.1.55.
MSC: Primary 01A70; Amy L. Reimann (MR Author ID: 1118776) and David A. Reimann (MR Author ID: 912704)

Figure 1 Bjarne Jespersen with several of the magic spheres he has carved.

for something to do with Islamic Art or Islamic studies. But since I had been employed there, and they appreciated what I did then, and they thought it was exciting what I was doing, they gave me what I needed. I applied to at least ten different places, but they said yes, everybody else said no, so that was nice. Then I thought since I was going to the States I might as well visit George Hart on Long Island and Bathsheba Grossman in California. I applied for a little extra to be able to do this and it was George who suggested that I should write a paper for Bridges. Actually, I never really regarded myself as an artist, but I suppose I am. It's more the math that inspires me and, well, it is inspiring to come here. It is wonderful.

Q: *What is your next book about?*

BJ: My next book is about what I call Magic Spheres. *[Bjarne shows us a carved sphere with large individual ants on the surface that are intricately engaged and can move slightly, yet remain together. See Figure 1.]*

Q: *Was this a puzzle? [See the small spheres in Figure 1.]*

BJ: No, it's cut out of one piece and can't be taken apart. Then I thought that it might be nice to make one with an Escher design so I looked through my Escher books and I found his ant pattern. It is flat but is easily modified so you can cover a sphere. But I knew I couldn't carve it on the sphere of this size because I need a very thin blade to do the sawing and the thin blade is too flexible to cut all the way to the center. So I had to find a way to create a hollow inside. I first tested the idea on a plaster sphere with a hollow inside. I just cut one animal to see how much it would move. It didn't move very much, so I thought it is going to work. But then it took me nearly thirty years to come up with a technique so I could make this hollow inside.

Q: *It looks like the pieces come apart, but the ball doesn't really come apart. [Still holding the small sphere]*

BJ: That's right. Because of that, people have trouble understanding what keeps the pieces together. I use a two-dimensional analogy to explain it. People can understand why you can't pull traditionally cut jigsaw puzzles pieces apart, but you can lift them

Figure 2 *Star cluster* (left), Bjane Jespersen; 5 cm, pear; private collection. An alternating lace of twelve star shaped rings.
Memento mori (right), Bjarne Jespersen; 50 mm, wood (briar), 1981; private collection. The traditional ball in cage theme is combined with a classical motif from renaissance art and inspiration from Japanese netsuke carvings. The cage is a rhombic dodecahedral edge frame.

up. Well, the thing is when you have a curved surface, you can't lift the pieces up without also pulling the pieces apart. So I made a sphere this size and cut it like classical jigsaw pieces, six of them like the faces of the cube and then shaped like jigsaw puzzles. Sometimes I call it the impossible puzzle. I have another title to honor the Belgian artist Magritte. He made this famous painting of the pipe "Ceci n'est pas une pipe" (this is not a pipe), so I call mine "Ceci n'est pas un puzzle."

Q: *We can't see any openings to the center. How did you hollow the inside?*

BJ: I made the hollow through the eyes. I turned one eye of each animal loose like a small cone and picked it out. Here [pointing to the ant ball] I made eyes in a different wood. On this one, I marked and numbered the eyes so I could glue them back in the same position after I had done the hollowing.

Q: *How long does it take to carve a small ball? [See the small carved spheres in Figure 1?]*

BJ: These are actually quite fast, otherwise around 12 hours I think. I don't do them one at a time. I carve a series of balls, then I drill them all, then I draw the patterns on them all, and then do the sawing. I do all this at home in my own workshop. After that, I can sit anywhere and finish them.

Q: *Those are really spectacular!*

BJ: Thanks, and that's all for my next book. Originally I planned to have a chapter in this book with these and a few other simpler ones that I've done, for instance the impossible puzzle. But when I wrote in the preface that everything in this book is done with simple hand tools, I should have added except for the ones in this chapter. And I thought that's a pity. I had also just discovered the method to do the hollowing here so I knew that would be a lot more exciting stuff to come. So I decided to leave them out and hope for another book. And that's what seems to be coming. It will be at least two maybe three or four years because I need to do more carvings.

PROBLEMS

EDUARDO DUEÑEZ, *Editor*
University of Texas at San Antonio

EUGEN J. IONASCU, *Proposals Editor*
Columbus State University

JOSÉ A. GÓMEZ, Facultad de Ciencias, UNAM, México; RICARDO A. SÁENZ, Universidad de Colima, México; ROGELIO VALDEZ, Facultad de Ciencias, UAEM, México; *Assistant Editors*

Editor's note. I welcome Eduardo Dueñez of the University of Texas at San Antonio as the new Problems Editor of MATHEMATICS MAGAZINE. Eduardo comes to the MAGAZINE with a rich background, as he was a contestant in the 2nd and 3rd OMM (Mexican Mathematical Olympiad) as well as in the 1990 Iberoamerican, Asian Pacific, and International Mathematical Olympiads. He also served as a coach and mentor for the 2012 Mathematics Olympiad Program of the American Association for Advancement of Science. He has been the Putnam coach at his institution since 2005. I also welcome new Assistant Problems Editor Ricardo A. Sáenz of the Universidad de Colima, México. Finally, another change, Eugen J. Ionascu of Columbus State University, Columbus, GA was an Assistant Problems Editor. He is now the Proposals Editor.
−Michael A. Jones

Proposals

To be considered for publication, solutions should be received by July 1, 2016.

1986. *Proposed by Spiros P. Andriopoulos, Third High School of Amaliada, Eleia, Greece.*

Let (a, b, c) be a Pythagorean triple, i.e., a, b, c are positive integers such that $c^2 = a^2 + b^2$, and let $n \in \mathbb{N}$. Prove that

$$\frac{a^{2n+1} + b^{2n+1} + c^{2n+1}}{a + b + c}$$

is an integer.

1987. *Proposed by Valeriy Karachik and Leonid Menikhes, South Ural State University, Chelyabinsk, Russia.*

Math. Mag. **89** (2016) 58–66. doi:10.4169/math.mag.89.1.58.

We invite readers to submit problems believed to be new and appealing to students and teachers of advanced undergraduate mathematics. Proposals must, in general, be accompanied by solutions and by any bibliographical information that will assist the editors and referees. A problem submitted as a Quickie should have an unexpected, succinct solution. Submitted problems should not be under consideration for publication elsewhere.

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

Problem proposals should be mailed electronically to mathmagproblems@maa.org. *Solutions should be sent to* mathmagsolutions@maa.org. *We encourage submissions in PDF format, ideally accompanied by LaTeX source. All communications should include* **on each page** *the reader's name, full address, and an e-mail address and/or FAX number.*

Let n, k, d be integers such that $n \geq 2$. Is there an $n \times n$ matrix $A = (a_{ij})$ with $\det A = d$ whose entries are integers $a_{ij} \geq k$?

1988. *Proposed by Lenny Jones and Alicia Lamarche, Shippensburg University, Shippensburg, PA, USA.*

Call a positive integer *n divisor-sum composite (DSC)* if the sum of two or more (distinct) divisors of n is always composite. Let $(a_1, a_2, \ldots, a_k)$ be a k-tuple of positive integers for some $k \geq 1$. Prove that there exist infinitely many DSC numbers n of the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

for suitable distinct primes $p_1, p_2, \ldots, p_k$.

1989. *Proposed by Michel Bataille, Rouen, France.*

Let n be a positive integer and let a be a positive real number. Define

$$H_n = \sum_{k=1}^{n} \frac{1}{k} \quad \text{and} \quad S_n(a) = \sum_{k=1}^{n} a^k H_k.$$

Evaluate

$$\lim_{n\to\infty} \left(\frac{S_n(a)}{(a+1)^n} - \ln n \right).$$

1990. *Proposed by Nermin Hodžić (student) University of Tuzla, Tuzla, Bosnia and Herzegovina and Salem Malikić (student) Simon Fraser University, Burnaby, BC, Canada.*

Let a, b, c be nonnegative real numbers such that

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

Prove that

$$\frac{1}{2} \leq \frac{ab+bc+ca}{a^2+b^2+c^2} \leq \frac{7}{11}.$$

Quickies

Q1057. *Proposed by John Zacharias, Arlington, VA, USA.*

Let $\triangle$ be an isosceles triangle whose circumcenter O lies on its incircle $\mathcal{C}$. Show that the tangent of the smallest angle of $\triangle$ has either the value 1, or the value

$$\left(-2^{-2^{+1}} + 2^{-2^{-1}}\right)^{2^{-1}}.$$

Q1058. *Proposed by Mircea Merca, University of Craiova, Romania.*

Let $\omega = \cos(2\pi/n) + i \sin(2\pi/n)$ and n be an integer greater than or equal to 2. Prove that

$$\prod_{k=1}^{n-1}(1-\omega^k-\omega^{2k}) = \begin{cases} \lceil \phi^n \rfloor - 2 & (n \text{ even}), \\ \lceil \phi^n \rfloor & (n \text{ odd}), \end{cases}$$

where $\phi = (1+\sqrt{5})/2$ and $\lceil t \rfloor$ denotes the integer closest to t.

Solutions

Weighting the harmonic sequence — December 2014

1956. *Proposed by Valery Karachik, South Ural State University, Chelyabinsk, Russia.*

Let a be a real number and k a positive integer. Let $\{a_n\}$ be a sequence of real numbers such that $\lim_{n\to\infty} a_n = a$. Evaluate

$$\lim_{n\to\infty}\left(\frac{a_0}{n+k} + \frac{a_1}{n+k+1} + \cdots + \frac{a_{(n-1)k}}{n+nk}\right).$$

Solution by Hongwei Chen, Christopher Newport University, Newport News, VA.
The value ℓ of the desired limit is equal to $a\ln(k+1)$.

First, we prove that $\ell = aL(k)$, where $L(k) = \lim_{n\to\infty} H(n,k)$ and $H(n,k) = \sum_{j=k}^{nk}(n+j)^{-1}$. Since $\lim_{n\to\infty} a_n = a$, for any $\varepsilon > 0$ there is a positive integer N such that $|a_n - a| < \varepsilon$ whenever $n > N$. Thus,

$$\left|\sum_{i=0}^{(n-1)k}\left(\frac{a_i}{n+k+i} - \frac{a}{n+k+i}\right)\right| \le \sum_{i=0}^{N}\frac{|a_i-a|}{n+k+i} + \sum_{i=N+1}^{(n-1)k}\frac{|a_i-a|}{n+k+i}$$
$$\le \frac{(N+1)\max_{0\le i\le N}|a_i-a|}{n+k} + \frac{(n-1)k-N}{n+k+N+1}\,\varepsilon.$$

Letting $n\to\infty$ we obtain $|\ell - aL(k)| \le k\varepsilon$. Since $\varepsilon > 0$ is arbitrary, the claim $\ell = aL(k)$ follows.

Next, observe that

$$L(k) + \lim_{n\to\infty}\sum_{i=1}^{k-1}\frac{1}{n+i} = \lim_{n\to\infty}\sum_{i=1}^{nk}\frac{1}{n+i} = \lim_{n\to\infty}\frac{1}{nk}\sum_{i=1}^{nk}\frac{1}{1/k+i/nk}$$
$$= \int_0^1 \frac{1}{1/k+x}\,dx$$

since the last limit is that of a right-endpoint Riemann sum for $g(x) = (x+1/k)^{-1}$ on $[0,1]$ using kn subintervals of equal length. Since

$$\sum_{i=1}^{k-1}\frac{1}{n+i} \le \frac{k-1}{n+1} \to 0 \quad \text{as } n\to\infty,$$

we have

$$L(k) = \int_0^1 \frac{1}{1/k+x}\,dx = \ln(1/k+x)\big|_0^1 = \ln(k+1).$$

Thus, we have $\ell = aL(k) = a\ln(k+1)$.

Also solved by Robert A. Agnew, Michel Bataille (France), Brian Bradie, Paul Budney, Bruce S. Burdick, Charles Burnette, Robert Calcaterra, Richard Daquila, Daniel Fritze (Germany), GWstat Problem Solving Group, Eugene A. Herman, Iowa State University Undergraduate Problems Solving Group, James Magliano, Union County College, Parviz Khalili, Northwestern University Math Problem Solving Group, Moubinool Omarjee (France), ONU-SOLVE Group, Paolo Perfetti (Italy), Ángel Plaza (Spain), Nicholas C. Singer, and the proposer. There were three incomplete or incorrect submissions.

A sum of angles with radical cosines **December 2014**

1957. *Proposed by Wong Fook Sung, Temasek Polytechnic, Singapore.*

Evaluate

$$\sum_{n=1}^{\infty} \arccos\left(\frac{1+\sqrt{4n^2-1}}{2\sqrt{n(n+1)}}\right).$$

Solution by Northwestern University Math Problem Solving Group, IL.
Let

$$x_n = \frac{1+\sqrt{4n^2-1}}{2\sqrt{n(n+1)}} \quad \text{and} \quad \alpha_n = \arccos(x_n).$$

Then,

$$\tan\alpha_n = \frac{\sqrt{1-x_n^2}}{x_n} = \frac{\sqrt{4n-2\sqrt{4n^2-1}}}{1+\sqrt{4n^2-1}} = \frac{\sqrt{2n+1}-\sqrt{2n-1}}{1+\sqrt{2n+1}\sqrt{2n-1}}.$$

Let $\beta_n = \arctan\sqrt{2n-1}$. Clearly $\tan\alpha_n = \tan(\beta_{n+1}-\beta_n)$, hence $\alpha_n = \beta_{n+1}-\beta_n$ inasmuch as both of these quantities lie in $[0, \pi/2)$. For $N \geq 1$, we have a telescoping sum

$$S_N = \sum_{n=1}^{N} \alpha_n = \sum_{n=1}^{N} (\beta_{n+1}-\beta_n) = \beta_{N+1}-\beta_1,$$

hence

$$\sum_{n=1}^{\infty} \alpha_n = \lim_{N\to\infty} S_N = \lim_{N\to\infty} \beta_{N+1}-\beta_1 = \frac{\pi}{2}-\frac{\pi}{4} = \frac{\pi}{4}.$$

Also solved by Michel Bataille (France), Brian Bradie, Robert Calcaterra, Hongwei Chen, Kyung Jin Cho (Korea), David Doster, Robert L. Doucette, John N Fitch, Marty Getz & Dixon Jones, Raymond N. Greenwell, G. C. Greubel, Ankita Hasija, Stephen S. Jensen & Charles Ross McCarthy, Oh Eun Jong (Korea), Michael Goldenberg & Mark Kaplan, Benjamin Keigwin, Harris Kwong, Elias Lampakis, Northwestern University Math Problem Solving Group, Weiping Li, James Magliano, Perfetti Paolo (Italy), Pittsburg State University Problem Solving Group, Angel Plaza (Spain), Nari Shin, Nicholas C. Singer, Traian Viteam (India), Haohao Wang, Jerzy Wojdylo, John B. Zacharias, and the proposer. There were six incomplete or incorrect solutions.

A functional inequality characterizing squaring **December 2014**

1958. *Proposed by Marcel Chiriţă, Bucharest, Romania.*

Determine all functions $f : \mathbb{N} \to [1, \infty)$ that satisfy the following conditions:

(i) $f(2) = 4$,

(ii) $(n+1)f(n) \leq nf(n+1)$ for every $n \in \mathbb{N}$, and

(iii) $f(nm) = f(n)f(m)$ for every $n, m \in \mathbb{N}$.

Solution by Robert L. Doucette, McNeese State University, Lake Charles, LA.
The only such function is $f(n) = n^2$. Let $g(n) = f(n)/n$. Conditions (i)–(iii) become

(i′) $g(2) = 2$,

(ii′) $g(n) \leq g(n+1)$ for every $n \in \mathbb{N}$, and

(iii′) $g(nm) = g(n)g(m)$ for every $n, m \in \mathbb{N}$.

Using induction, it follows from (ii′) that g is nondecreasing, and from (iii′) that $g(n^k) = g(n)^k$ for all $n, k \in \mathbb{N}$. It follows that $g(1) = 1$, since $g(1) = g(1^2) = g(1)^2$ and $g(1) \in \mathbb{N}$, and also that $g(2^k) = 2^k$, by (i′).

Let $n \in \mathbb{N}$ be arbitrary. Suppose first that $n < g(n)$. By continuity of the map $x \mapsto 2^x$ from $(0, \infty)$ onto $(1, \infty)$ plus the fact that (positive) rational numbers are dense in $(0, \infty)$, there must exist $r, s \in \mathbb{N}$ such that $n < 2^{r/s} < g(n)$, so $n^s < 2^r < g(n)^s = g(n^s)$. By monotonicity, $g(n^s) \leq g(2^r) = 2^r < g(n^s)$, a contradiction. Reversing the inequalities in the argument above, the assumption $n > g(n)$ also leads to a contradiction. It follows that $g(n) = n$ for all $n \in \mathbb{N}$. Therefore, $f(n) = n^2$ for all $n \in \mathbb{N}$.

Editor's Note. E. Lamprakis, F. Perdomo & Á. Plaza, and N. Thornber pointed out that the conclusion $g(n) = n$ follows immediately from a theorem of Erdős. (E. Howe, A new proof of Erdős's theorem on monotone multiplicative functions, *Amer. Math. Monthly* **93** (1986) 593–595.)

Also solved by Michel Bataille (France), Bruce S. Burdick, Robert Calcaterra, Sungjun Choi (Korea), John Christopher, Hongwei Chen, Joseph Di Muro, Dmitry Fleischman, Marty Getz and Dixon Jones, Nam Gu Heo (Korea), Eugene A. Herman, Tom Jager, Northwestern University Math Problem Solving Group, Iowa State University Undergraduate Problem Solving Group, Elias Lampakis (Greece), G. Lord, Francisco Perdomo and Ángel Plaza (Spain), Nora Thornber, Traian Viteam (India), and the proposer. There was one incomplete or incorrect submission.

A graph on which Klein's four-group acts **December 2014**

1959. *Proposed by Eddie Cheng and Jerrold W. Grossman, Oakland University, Rochester, MI.*

Let n be a positive integer, and let S be the set of subsets of $\{1, 2, \ldots, 2n\}$ of size n. Form an undirected graph with vertex set S by putting an edge between A and B if $B = \{1, 2, \ldots, 2n\} \setminus A$ or $B = \{2n + 1 - i : i \in A\}$. How many connected components does this graph have?

Solution by Rob Pratt, Niskayuna, NY.
For $A \in S$, define $\kappa(A) = \{1, 2, \ldots, 2n\} \setminus A$ and $\rho(A) = \{2n + 1 - i : i \in A\}$. Denote by ι the identity transformation $\iota(A) = A$. We have $\kappa^2 = \rho^2 = \iota$ and $\kappa \circ \rho = \rho \circ \kappa$. Then $G = \{\iota, \kappa, \rho, \kappa\rho\}$ is a group of permutations of S. (For notational convenience we denote $\alpha \circ \beta$ by $\alpha\beta$.) Clearly, connected components of the graph under consideration may be identified with G-orbits in S.

Applying the Cauchy–Frobenius–Burnside orbit-counting theorem, the number of G-orbits in S is

$$\frac{1}{|G|}\sum_{\gamma\in G}|S^{\gamma}|\,,$$

where $S^{\gamma}=\{A\in S:\gamma(A)=A\}$ is the set of vertices fixed by the element $\gamma\in G$.

Clearly $|S^{\iota}|=|S|=\binom{2n}{n}$, while $|S^{\kappa}|=0$. Let $L(A)=A\cap\{1,2,\ldots,n\}$ be the "left part" of any set $A\in S$. If n is even, then L is a bijection between S^{ρ} and the collection of subsets of $\{1,2,\ldots,n\}$ of size $n/2$; thus, $|S^{\rho}|=\binom{n}{n/2}$. If n is odd, then $|S^{\rho}|=0$. Next, L is clearly a bijection between $S^{\kappa\rho}$ and the power set of $\{1,2,\ldots,n\}$, hence $|S^{\kappa\rho}|=2^n$. Finally, the number of connected components (i.e., of G-orbits), is equal to

$$\begin{cases}\dfrac{1}{4}\left\{\dbinom{2n}{n}+\dbinom{n}{n/2}+2^n\right\} & \text{if } n \text{ is even,}\\[2ex] \dfrac{1}{4}\left\{\dbinom{2n}{n}+2^n\right\} & \text{if } n \text{ is odd.}\end{cases}$$

Also solved by Michael Bataille (France), Bruce S. Burdick, Robert Calcaterra, Harris Kwong, University High School Problem Solving Group, Kiran Lall Shrestha, John H. Smith, and the proposer.

Similar λ-triangles **December 2014**

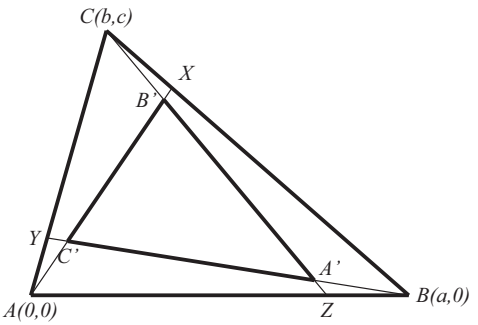
1960. *Proposed by Michael Goldenberg, The Ingenuity Project, Baltimore Polytechnic Institute, Baltimore, MD, and Mark Kaplan, Towson University, Towson, MD.*

Given a nonisosceles triangle ABC, let λ be a real number different from 1 and -1. Let X, Y, and Z be points on the lines BC, AC, and AB, respectively, such that

$$\frac{\overline{AZ}}{\overline{ZB}}=\frac{\overline{BX}}{\overline{XC}}=\frac{\overline{CY}}{\overline{YA}}=\lambda.$$

Let A', B', and C' be the intersections of the pairs of lines (BY, CZ), (CZ, AX), and (AX, BY), respectively, and call $\triangle A'B'C'$ a λ-triangle of $\triangle ABC$. Find the values of λ for which the triangles ABC and $A'B'C'$ are similar. (We call two triangles similar, if, for some one-to-one correspondence among their vertices, the corresponding angles of the triangles are equal.)

Solution by Bruce S. Burdick, Department of Mathematics, Roger Williams University, Bristol, RI.



We adopt the usual notation $\triangle PQR \sim \triangle UVW$ to mean that two triangles $\triangle PQR$ and $\triangle UVW$ are similar with P, Q, R corresponding to U, V, W in that order. Under the hypotheses that $\triangle ABC$ is scalene and $\lambda \neq \pm 1$, we will show that:

- $\triangle ABC \sim \triangle A'B'C'$ if and only if $\lambda = 0$,
- $\triangle ABC \sim \triangle A'C'B'$ if and only if $\lambda = (\overline{AB}^2 - \overline{BC}^2)/(\overline{BC}^2 - \overline{CA}^2) \neq 1$,
- $\triangle ABC \sim \triangle B'A'C'$ if and only if $\lambda = (\overline{CA}^2 - \overline{AB}^2)/(\overline{AB}^2 - \overline{BC}^2) \neq 1$,
- $\triangle ABC \sim \triangle C'B'A'$ if and only if $\lambda = (\overline{BC}^2 - \overline{CA}^2)/(\overline{CA}^2 - \overline{AB}^2) \neq 1$,

and that there are no other values of $\lambda \neq \pm 1$ resulting in a (nondegenerate) triangle similar to $\triangle ABC$.

We remark that, for $\lambda = 1$, the points A', B', C' all coincide with the centroid of $\triangle ABC$ so $\triangle A'B'C'$ is degenerate. Furthermore, $\lambda = \infty$ gives $A = Y = C'$, $B = Z = A'$, and $C = X = B'$, leading to $\triangle ABC \sim \triangle C'A'B'$. Similarly, for $\lambda = -1$ we have that X, Y, Z are the points at infinity on $\overline{BC}$, $\overline{CA}$, $\overline{AB}$, so $\triangle ABC \sim \triangle A'B'C'$ with $\triangle A'B'C'$ uniquely characterized by the fact that its medial triangle is $\triangle ABC$.

For $\lambda = 0$ we have $A' = A$, $B' = B$ and $C' = C$, so $\triangle ABC \sim \triangle A'B'C'$. In what follows we assume that $\lambda \neq 0, \pm 1$.

Let the vertices of the triangle be the Cartesian points $A(0, 0)$, $B(a, 0)$, and $C(b, c)$, respectively (for convenience we assume $a > 0$ and $c > 0$). A straightforward calculation gives the coordinates of the remaining points:

$$X\left(\frac{\lambda b + a}{1+\lambda}, \frac{\lambda c}{1+\lambda}\right), \qquad A'\left(\frac{\lambda^2 a + b}{1+\lambda+\lambda^2}, \frac{c}{1+\lambda+\lambda^2}\right),$$

$$Y\left(\frac{b}{1+\lambda}, \frac{c}{1+\lambda}\right), \qquad B'\left(\frac{\lambda^2 b + \lambda a}{1+\lambda+\lambda^2}, \frac{\lambda^2 c}{1+\lambda+\lambda^2}\right),$$

$$Z\left(\frac{\lambda a}{1+\lambda}, 0\right), \qquad C'\left(\frac{\lambda b + a}{1+\lambda+\lambda^2}, \frac{\lambda c}{1+\lambda+\lambda^2}\right).$$

Since $\triangle ABC$ has area $[ABC] = ac/2$, the well-known determinant formula for area gives $[A'B'C']/[ABC] = (\lambda - 1)^2/(\lambda^2 + \lambda + 1)$. Therefore, if a similarity exists, its ratio must be $\rho = |\lambda - 1| / \sqrt{\lambda^2 + \lambda + 1}$.

Let $\Lambda = 1/\sqrt{\lambda^2 + \lambda + 1}$. Further computation shows that

$$\overline{A'B'} = \rho \ell_{C'} \quad \text{where} \quad \ell_{C'} = \Lambda \sqrt{(\lambda a - (\lambda+1)b)^2 + (\lambda+1)^2 c^2},$$

$$\overline{B'C'} = \rho \ell_{A'} \quad \text{where} \quad \ell_{A'} = \Lambda \sqrt{(a + \lambda b)^2 + \lambda^2 c^2},$$

$$\overline{C'A'} = \rho \ell_{B'} \quad \text{where} \quad \ell_{B'} = \Lambda \sqrt{((\lambda+1)a - b)^2 + c^2}.$$

So, if the desired similarity exists, the three quantities $\ell_{A'}$, $\ell_{B'}$, $\ell_{C'}$ must be equal to the quantities $\ell_A = \overline{BC} = \sqrt{(b-a)^2 + c^2}$, $\ell_B = \overline{CA} = \sqrt{b^2 + c^2}$, $\ell_C = \overline{AB} = a$, in some order (this requires $\rho \neq 0$, hence $\lambda \neq 1$).

For each of the six permutations (P, Q, R) of (A', B', C') we get a system of three equations $\{\ell_P = \ell_A, \ell_Q = \ell_B, \ell_R = \ell_C\}$ in the four variables a, b, c, λ. For each of the three permutations transposing two elements, which correspond to an *inverse* triangle similarity $\triangle PQR \sim \triangle ABC$, the system reduces to a single equation (modulo the

assumption $\lambda \neq 0, \pm 1$), namely

$$\lambda = \frac{2ab - b^2 - c^2}{a^2 - 2ab} = \frac{\overline{AB}^2 - \overline{BC}^2}{\overline{BC}^2 - \overline{CA}^2}, \qquad \text{when } (P, Q, R) = (A', C', B'),$$

$$\lambda = \frac{a^2 - 2ab}{b^2 + c^2 - a^2} = \frac{\overline{BC}^2 - \overline{CA}^2}{\overline{CA}^2 - \overline{AB}^2}, \qquad \text{when } (P, Q, R) = (C', B', A'),$$

$$\lambda = \frac{b^2 + c^2 - a^2}{2ab - b^2 - c^2} = \frac{\overline{CA}^2 - \overline{AB}^2}{\overline{AB}^2 - \overline{BC}^2}, \qquad \text{when } (P, Q, R) = (B', A', C').$$

In the three remaining cases, each of which corresponds to a *direct* triangle similarity $\triangle PQR \sim \triangle ABC$, the three equations in the system are independent. In fact, each of these systems shares exactly one equation with each of the three inverse systems above; therefore, under the assumption $\lambda \neq 0, \pm 1$, a solution will exist if and only if all three expressions for λ above have the same value. However, multiplying the three equations above together gives $\lambda^3 = 1$, hence $\lambda = 1$, which has already been excluded. We conclude that no direct similarity between the triangles is possible, except for the one obtained when $\lambda = 0$ and $\triangle A'B'C' = \triangle ABC$ (plus those obtained with $\lambda = \pm 1$).

We observe that, when $\triangle ABC$ is *quasi-isosceles* in the sense that the sum of the squares of the lengths two of its sides equals the square of the length of the third, then we have $\lambda = 1$ in the respective case (the remaining values are $0, -1/2$ and -2), so $\triangle ABC$ can only be similar to $\triangle PQR$ degenerately—namely when $P = Q = R$. For instance, if $\overline{AB}^2 + \overline{BC}^2 = 2\overline{AC}^2$, then $\triangle C'B'A'$ cannot be similar to $\triangle ABC$.

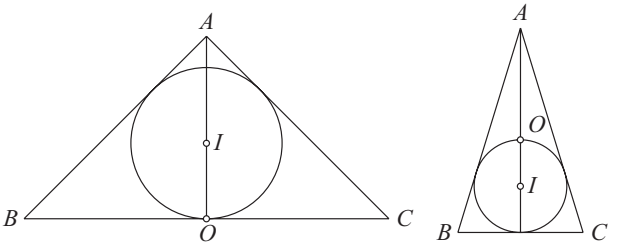
Editor's Note. Professor Michael Bataille pointed out that quasi-isosceles triangles are the subject of the following article: J. Chris Fisher, Reviewing Crux Configurations, *Crux Mathematicorum with Mathematical Mayhem* **37** (2011) 304–307.

Also solved by Michael Bataille (France), Robert Calcaterra, and the proposer.

Answers

Solutions to the Quickies from page 59.

A1057.



Let the triangle $\triangle ABC$ with $\overline{AB} = \overline{AC}$ have circumcenter O lying on its incircle $\mathcal{C}$. Clearly O cannot lie outside $\triangle ABC$, which thus cannot be obtuse. If O lies on BC (left figure above) then $\triangle ABC$ is right and isosceles, hence its smallest angles $\angle B = \angle C = \pi/4$ have tangent equal to 1. If $\triangle ABC$ is acute (right figure above), then O lies inside

it, and also on the height through A, by symmetry. O divides this height into segments of length $2r$ and R where r and R are the radii of the inscribed and circumscribed circles, respectively. Hence we have $h = R + 2r$, where h is the height, r the inradius, and R the circumradius. By Euler's theorem we have $d^2 = R(R - 2r)$, where d is the distance between the incenter and the circumcenter. Since the incenter O lies on the incircle $\mathcal{C}$ we have $d = r$, so it follows that $R = (1 + \sqrt{2})r$ and $h = (3 + \sqrt{2})r$. Let $a = \overline{AB} = \overline{AC}$ be the length of the equal sides and $b = \overline{BC}$ the length of the base. By equating two expressions for the area of $\triangle ABC$, we get

$$rs = \frac{bh}{2} \quad \Rightarrow \quad r(a + b/2) = \frac{(3 + \sqrt{2})br}{2} \quad \Rightarrow \quad \frac{b}{2a} = 1 - \frac{1}{\sqrt{2}},$$

so

$$\tan \angle A = \tan\left(\pi - 2\cos^{-1}\tfrac{b}{2a}\right) = -\tan\left(2\cos^{-1}\left(1 - \tfrac{1}{\sqrt{2}}\right)\right) = \left(-2^{-2^{+1}} + 2^{-2^{-1}}\right)^{2^{-1}}.$$

A1058. Consider the polynomial identities

$$1 - x^n = \prod_{k=0}^{n-1}(1 - \omega^k x) \quad \text{and} \quad 1 - x - x^2 = (1 - \phi x)(1 - \hat{\phi} x),$$

where

$$\phi = \frac{1 + \sqrt{5}}{2} \quad \text{and} \quad \hat{\phi} = \frac{1 - \sqrt{5}}{2}.$$

We have

$$\prod_{k=0}^{n-1}(1 - \omega^k - \omega^{2k}) = \prod_{k=0}^{n-1}(1 - \phi\omega^k)\prod_{k=0}^{n-1}(1 - \hat{\phi}\omega^k) = (1 - \phi^n)(1 - \hat{\phi}^n)$$
$$= 1 - (\phi^n + \hat{\phi}^n) + (-1)^n.$$

Thus,

$$a_n = \prod_{k=1}^{n-1}(1 - \omega^k - \omega^{2k}) = \begin{cases} \phi^n - 2 + \hat{\phi}^n, & \text{for } n \text{ even;} \\ \phi^n + \hat{\phi}^n, & \text{for } n \text{ odd.} \end{cases}$$

In fact, a_n is an integer. First, since $\hat{\phi} = 1 - \phi$ and $\phi^2 = \phi + 1$, we have that $\mathbb{Z}[\phi, \hat{\phi}] = \mathbb{Z}[\phi] = \mathbb{Z} + \mathbb{Z}\phi$ is a ring containing a_n. Second, a_n is invariant under the unique automorphism of $\mathbb{Z}[\phi]$ that swaps ϕ with $\hat{\phi} = 1 - \phi$, so $a_n \in \mathbb{Z}$. (A more direct proof follows inductively from the recurrence $L_n = L_{n-1} + L_{n-2}$ satisfied by the Lucas numbers $L_n = \phi^n + \hat{\phi}^n$, since $L_0 = 2$ and $L_1 = 1$ are integers.)

Clearly $0 < |\hat{\phi}|^n < \frac{1}{2}$ for $n \geq 2$. Hence, a_n is the integer closest to $\phi^n - 2$ for n even, to ϕ^n for n odd.

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.

Koutis, Ioannis, and Ryan Williams, Algebraic footprints for faster algorithms, *Communications of the Association for Computing Machinery* 59 (1) (January 2016) 98–105; http://www.cs.cmu.edu/~jkoutis/papers/AlgebraicFingerprints.pdf . Video at https://vimeo.com/148129071.

Kun, Jeremy, A quasipolynomial time algorithm for graph isomorphism: The details, http://jeremykun.com/2015/11/12/a-quasipolynomial-time-algorithm-for-graph-isomorphism-the-details/.

Babai, László, Graph isomorphism in quasipolynomial time, http://arxiv.org/abs/1512.03547.

Vardi, Moshe Y., The moral hazard of complexity-theoretic assumptions, *Communications of the Association for Computing Machinery* 59 (2) (February 2016) 5; http://cacm.acm.org/magazines/2016/2/197412-the-moral-hazard-of-complexity-theoretic-assumptions/fulltext. Responses and comments at http://blog.geomblog.org/2016/02/on-moral-hazard-of-complexity-theoretic.html and at http://blog.computationalcomplexity.org/2016/02/the-moral-hazard-of-avoiding-complexity.html.

There has been progress in recent years in finding faster algorithms for NP-hard problems, such as the Hamiltonian path problem and (at the end of 2015) the graph isomorphism problem. Much of the progress can be attributed to "algebraicizing" the problem and then applying algebraic methods. László Babai made surprising progress in determining whether two graphs are isomorphic (caution: his work has not yet been peer-reviewed); videos of his lectures are at http://people.cs.uchicago.edu/~laci/. That problem is in NP but is not known to be NP-complete; his algorithm runs in $\mathcal{O}\left(\exp\left[(\log n)^k\right]\right)$, called *quasipolynomial* time because it is exponential in a power of $\log n$—an improvement over the previous $\mathcal{O}\left(\sqrt{n \log n}\right)$. Editor Vardi expresses annoyance at writers' "moral hazard" in characterizing Babai's and similar results as being "efficient"; he urges discussing efficiency in terms of real-world performance.

Johnson, Timothy C., Finance and mathematics: Where is the ethical malaise?, *Mathematical Intelligencer* 37 (4) (Winter 2015) 8–11.

Now, moral hazard for mathematicians: Author Johnson responds to previous articles in the *Intelligencer* concerning the role of mathematicians in finance. His position is that financial mathematics must be a "discipline centred on the concept of justice, making it explicit that successful finance must be moral finance." He traces the cultural history of mathematics in finance then asserts that "the correct response of mathematicians. . . is. . . to redirect finance away from regarding markets as competitive arenas" toward becoming "democratic market discourse," which should embody "reciprocity, sincerity, and charity." But there is a simpler answer to the title question: *The malaise is in abetting greed.*

Math. Mag. **89** (2016) 67–68. doi:10.4169/math.mag.89.1.67.

Cromwell, Peter R., Cognitive bias and claims of quasiperiodicity in traditional Islamic patterns, *Mathematical Intelligencer* 37 (4) (Winter 2015) 30–44.

Author Cromwell criticizes evidence for claims that ancient Islamic patterns exhibit quasicrystal (Penrose) patterns. He goes further, though, in attributing acceptance of the claim—by its researchers as well as other scientists—to unconscious cognitive biases.

Ashbacher, Charles (ed.), *Topics in Recreational Mathematics*, 5 vols. CreateSpace Independent Publishing Platform, 2015. 82 pp, 105 pp, 124 pp, 156 pp, 156 pp, 138 pp. $9.99(P), $10.99(P), $11.99(P), $11.88(P), $12.59(P). Available on Amazon. ISBN 978-1507603215, 978-1508617099, 978-1511641005, 978-1514317518, 978-1519115676.

Silva, Jorge Nuno (ed.), *Recreational Mathematics Magazine*. http://rmm.ludus-opuscula.org. ISSN 2182-1976.

Charles Ashbacher was the editor of the *Journal of Recreational Mathematics* (JRM) for many years until it was discontinued in 2014 by its publisher. His *Topics* volumes in a sense continue JRM since they have a similar structure (articles, reviews, alphametics, problems, and conjectures) and include papers originally submitted for JRM. In particular, these volumes contain solutions to problems from the last volumes of JRM and also start a new series of Problems and Conjectures. Vol. 5 contains a complete index to JRM's predecessor, the original *Recreational Mathematics Magazine* (14 issues, 1961–1964). A new *Recreational Mathematics Magazine* began in 2014, is electronic, offers four to six articles twice per year ("in the exact moments of the equinox"), has an illustrious editorial board, and attracts notable authors (in issue 4: John Horton Conway, David Singmaster).

Hinz, Andreas M., Sandi Klavžar, Uroš Milutinović, and Ciril Peter, *The Tower of Hanoi—Myths and Maths*, Springer Basel, 2013; xv + 335 pp, $44.95, $44.95(P), $34.99(eBook). ISBN 978-3-0348-0236-9, 978-3-0348-0769-2, 978-3-0348-0237-6.

This book is a mathematically inspiring and historically careful definitive examination of algorithms for the Tower of Hanoi problem and associated problems, such as the Chinese Rings Puzzle and other variants. There are surprises, such as practical applications in psychological tests and the appearance of the Sierpiński triangle. Notable is the still-open problem of whether the solutions by J.S. Frame and B.M. Stewart to the Tower of Hanoi with four pegs are optimal. There are exercises, with hints or solutions provided.

Kucharski, Adam, *The Perfect Bet: How Science and Math Are Taking the Luck out of Gambling*, Basic Books, 2016; xviii + 257 pp, $26.99(P). ISBN 978-0-465-05595-1.

Author Kucharski documents successful efforts to win at roulette, state lotteries, poker, blackjack, and betting on horse racing and sports. Most involve technology (fast cameras, bots, computer data analysis). Some readers may be disappointed because the author does not give prescriptions for a "perfect bet" in any of these arenas. The numerous anecdotes—which feature, among others, Poincaré, Ulam, and Thorp—are entertaining, with their sources documented.

Stein, James D., *L.A. Math: Romance, Crime, and Mathematics in the City of Angels*, Princeton University Press, 2016; xiv + 237 pp, $24.95. ISBN 978-0-691-16828-9.

I am not much of a fan of fiction or poetry that features mathematics or mathematicians, though I am glad that such works may entertain or move others. This book consists of 14 short stories about a private investigator whose research is enhanced through mathematical analyses by his housemate; a lengthy appendix gives details of the analyses. I read all the stories because the author writes in an entertaining fashion that livens the situations. The mathematics is not sophisticated: logic, percentages, averages, arithmetic progressions, simultaneous linear equations, set combinatorics, probability (expectation, conditional probability, normal approximation to the binomial distribution), game theory, Arrow's theorem, and the traveling sales problem.

76th Annual William Lowell Putnam Mathematical Competition

Editor's Note: Additional solutions will be printed in the *Monthly* later in the year.

PROBLEMS

A1. Let A and B be points on the same branch of the hyperbola $xy = 1$. Suppose that P is a point lying between A and B on this hyperbola, such that the area of the triangle APB is as large as possible. Show that the region bounded by the hyperbola and the chord AP has the same area as the region bounded by the hyperbola and the chord PB.

A2. Let $a_0 = 1$, $a_1 = 2$, and

$$a_n = 4a_{n-1} - a_{n-2}$$

for $n \geq 2$. Find an odd prime factor of a_{2015}.

A3. Compute

$$\log_2 \left(\prod_{a=1}^{2015} \prod_{b=1}^{2015} \left(1 + e^{2\pi i ab/2015}\right) \right).$$

Here i is the imaginary unit (that is, $i^2 = -1$).

A4. For each real number x, let

$$f(x) = \sum_{n \in S_x} \frac{1}{2^n},$$

where S_x is the set of positive integers n for which $\lfloor nx \rfloor$ is even. What is the largest real number L such that $f(x) \geq L$ for all $x \in [0, 1)$? (As usual, $\lfloor z \rfloor$ denotes the greatest integer less than or equal to z.)

A5. Let q be an odd positive integer, and let N_q denote the number of integers a such that $0 < a < q/4$ and $\gcd(a, q) = 1$. Show that N_q is odd if and only if q is of the form p^k with k a positive integer and p a prime congruent to 5 or 7 modulo 8.

A6. Let n be a positive integer. Suppose that A, B, and M are $n \times n$ matrices with real entries such that $AM = MB$, and such that A and B have the same characteristic polynomial. Prove that $\det(A - MX) = \det(B - XM)$ for every $n \times n$ matrix X with real entries.

B1. Let f be a three times differentiable function (defined on $\mathbb{R}$ and real-valued) such that f has at least five distinct real zeros. Prove that $f + 6f' + 12f'' + 8f'''$ has at least two distinct real zeros.

B2. Given a list of the positive integers $1, 2, 3, 4, \ldots$, take the first three numbers 1, 2, 3 and their sum 6 and cross all four numbers off the list. Repeat with the three smallest remaining numbers 4, 5, 7 and their sum 16. Continue in this way, crossing

Math. Mag. **89** (2016) 69–79. doi:10.4169/math.mag.89.1.69.

off the three smallest remaining numbers and their sum, and consider the sequence of sums produced: 6, 16, 27, 36, ... Prove or disprove that there is some number in this sequence whose base 10 representation ends with 2015.

B3. Let S be the set of all 2×2 real matrices

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

whose entries a, b, c, d (in that order) form an arithmetic progression. Find all matrices M in S for which there is some integer $k > 1$ such that M^k is also in S.

B4. Let T be the set of all triples (a, b, c) of positive integers for which there exist triangles with side lengths a, b, c. Express

$$\sum_{(a,b,c)\in T} \frac{2^a}{3^b 5^c}$$

as a rational number in lowest terms.

B5. Let P_n be the number of permutations π of $\{1, 2, \ldots, n\}$ such that

$$|i - j| = 1 \quad \text{implies} \quad |\pi(i) - \pi(j)| \leq 2$$

for all i, j in $\{1, 2, \ldots, n\}$. Show that for $n \geq 2$, the quantity

$$P_{n+5} - P_{n+4} - P_{n+3} + P_n$$

does not depend on n, and find its value.

B6. For each positive integer k, let $A(k)$ be the number of odd divisors of k in the interval $\left[1, \sqrt{2k}\right)$. Evaluate

$$\sum_{k=1}^{\infty} (-1)^{k-1} \frac{A(k)}{k}.$$

SOLUTIONS

Solution to A1. Without loss of generality, we may assume that $A = (a, 1/a)$, $B = (b, 1/b)$, and $P = (p, 1/p)$ with $0 < a < p < b$. By the mean value theorem and the concavity of the hyperbola, there is a unique P for which the tangent line to the hyperbola at P is parallel to the chord AB, and the part of the hyperbola between A and B lies above that tangent line. Therefore, the distance to AB is maximal for that particular P, and so that is the point for which the area of the triangle APB is as large as possible. Setting the slopes of the tangent line at P and the chord AB to be equal, we get

$$-\frac{1}{p^2} = \frac{\frac{1}{b} - \frac{1}{a}}{b - a}, \text{ from which } p^2 = ab.$$

Now the area between the hyperbola and the chord AP is found by subtracting the area under the hyperbola between A and P from the area of the vertical trapezoid between the chord AP and the x-axis. This yields

$$\frac{1}{2}(p - a)\left(\frac{1}{p} + \frac{1}{a}\right) - \int_a^p \frac{dx}{x} = \frac{1}{2}\left(\frac{p}{a} - \frac{a}{p}\right) - \ln\left(\frac{p}{a}\right).$$

Similarly, the area between the hyperbola and the chord PB is $\frac{1}{2}\left(\frac{b}{p}-\frac{p}{b}\right)-\ln\left(\frac{b}{p}\right)$. Finally, $p^2=ab$ implies that $\frac{p}{a}-\frac{a}{p}=\frac{b}{p}-\frac{p}{b}$ and $\ln\left(\frac{p}{a}\right)=\ln\left(\frac{b}{p}\right)$, from which we see that the areas are equal.

Solution to A2. (Based on a student paper.) The recurrence relation $a_n=4a_{n-1}-a_{n-2}$ has characteristic equation
$\lambda^2=4\lambda-1$, with roots $\lambda_1=2+\sqrt{3}$, $\lambda_2=2-\sqrt{3}$, so its solutions are of the form $a_n=C\lambda_1^n+D\lambda_2^n$ with C, D independent of n. From the initial conditions we find $C=D=\frac{1}{2}$, so $a_n=\frac{1}{2}(\lambda_1^n+\lambda_2^n)$. Note that $\lambda_1\lambda_2=1$; using this, we find by direct calculation that

$$a_n a_m=\frac{1}{2}(a_{n+m}+a_{n-m}).$$

In particular, for $m=5$ we see that if p is an odd prime factor of a_5 and thus divides the left-hand side of this equation, a_{n+5} is divisible by p if and only if a_{n-5} is divisible by p. Therefore, such a prime p divides $a_5, a_{15}, a_{25}, \ldots, a_{2015}$. Thus it suffices to find an odd prime factor of a_5. By direct calculation, $a_2=7$, $a_3=26$, $a_4=97$, $a_5=362=2\cdot 181$. Because 181 is prime, it is an odd prime factor of a_{2015}.

Solution to A3. (Based on a student paper.) First consider the product

$$P=\prod_{\substack{1\le a,b\le 2015\\ ab\not\equiv 0 \pmod{2015}}}\left(1+e^{2\pi iab/2015}\right).$$

To evaluate P we multiply it by the similar product

$$Q=\prod_{\substack{1\le a,b\le 2015\\ ab\not\equiv 0 \pmod{2015}}}\left(1-e^{2\pi iab/2015}\right);$$

note that Q is nonzero, because if a factor $1-e^{2\pi iab/2015}$ would be zero, the exponential would be 1, which only happens when ab is a multiple of 2015. We get

$$PQ=\prod_{\substack{1\le a,b\le 2015\\ ab\not\equiv 0 \pmod{2015}}}\left(1-e^{4\pi iab/2015}\right).$$

However, because 2015 is odd, each factor in this last product corresponds to a unique factor in Q, by the correspondence sending (a,b) to $(2a \bmod 2015, b)$. So we have $PQ=Q$ and thus $P=1$.

Therefore, the product occurring in the problem can be rewritten as

$$\begin{aligned}\prod_{a=1}^{2015}\prod_{b=1}^{2015}\left(1+e^{2\pi iab/2015}\right)&=\prod_{\substack{1\le a,b\le 2015\\ ab\equiv 0 \pmod{2015}}}\left(1+e^{2\pi iab/2015}\right)\\&=\prod_{\substack{1\le a,b\le 2015\\ ab\equiv 0 \pmod{2015}}}2\\&=2^N,\end{aligned}$$

where N is the number of ordered pairs of integers (a,b) with

$$1\le a,b\le 2015, ab\equiv 0 \pmod{2015}.$$

Now 2015 factors into distinct odd primes as $2015 = 5 \cdot 13 \cdot 31$, so by the "Chinese remainder theorem" (Sun Tzu's theorem) we can count these ordered pairs by looking modulo 5, modulo 13, and modulo 31 separately. For each of these primes p, there are $2p - 1$ possibilities modulo p, because either a or b can be zero modulo p and the other can be arbitrary, giving $2p$ possibilities, except that $(0, 0)$ has now been counted twice. Thus N equals $9 \cdot 25 \cdot 61 = 13725$, and this is the answer.

Solution to A4. Throughout this solution, expressions such as $0.100100\ldots$ should be interpreted as *binary* expansions. We start with a lemma.

Lemma. For any $n \geq 0$, the following conditions are equivalent for all $x \in [0, 1)$:

(i) $f(x) < 0.100100\cdots100101$, where the right-hand side has $3n + 3$ bits to the right of the "decimal" point (n groups of 100 followed by a single 101);

(ii) $1, 4, \ldots, 3n + 1 \in S_x$ while $2, 3, 5, 6, \ldots, 3n + 2, 3n + 3 \notin S_x$;

(iii) $x \in \left[\frac{2n+1}{3n+2}, \frac{2}{3}\right)$.

Furthermore, when these conditions hold we have $3n + 4 \in S_x$.

Proof. We use induction on n. For the base case $n = 0$, we have $1 \in S_x$ for all $x \in [0, 1)$. Therefore, $f(x) < 0.101$ if and only if $2, 3 \notin S_x$ (this gives (i) if and only if (ii)) if and only if $2x, 3x \in [1, 2)$ if and only if $x \in [\frac{1}{2}, \frac{2}{3})$ (this gives (ii) if and only if (iii)). Then $4x \in [2, \frac{8}{3}) \subset [2, 3)$, so $4 \in S_x$.

Now suppose the claim is true for $n - 1$. Write $(\text{i})^n$, $(\text{ii})^n$, $(\text{iii})^n$ to denote the three conditions above, for the value n. That $(\text{ii})^n$ implies $(\text{i})^n$ is immediate from the definition of $f(x)$. Assuming $(\text{i})^n$, we certainly have $(\text{i})^{n-1}$, so by induction hypothesis we have $(\text{ii})^{n-1}$ as well as $3n + 1 \in S_x$. It follows that $f(x) > 0.100100\cdots1001$ (with $3n + 1$ bits to the right of the "decimal" point). Combining this last inequality with $(\text{i})^n$ we see that $3n + 2, 3n + 3 \notin S_x$, and thus $(\text{ii})^n$. This gives the equivalence between $(\text{i})^n$ and $(\text{ii})^n$.

Given the induction hypothesis, the equivalence between $(\text{ii})^n$ and $(\text{iii})^n$ says precisely that for $x \in \left[\frac{2n-1}{3n-1}, \frac{2}{3}\right)$ we have $3n + 2, 3n + 3 \notin S_x$ if and only if $x \in \left[\frac{2n+1}{3n+2}, \frac{2}{3}\right)$. To check the latter statement, observe that for $x \in \left[\frac{2n-1}{3n-1}, \frac{2}{3}\right)$ we have

$$(3n + 2)x \in \left[2n + \frac{3n - 2}{3n - 1}, 2n + \frac{4}{3}\right),$$

so that $\lfloor(3n + 2)x\rfloor$ is odd (i.e., $3n + 2 \notin S_x$) if and only if $(3n + 2)x \in \left[2n + 1, 2n + \frac{4}{3}\right)$ if and only if $x \in \left[\frac{2n+1}{3n+2}, \frac{2}{3}\right)$. Moreover, for $x \in \left[\frac{2n-1}{3n-1}, \frac{2}{3}\right)$ we have

$$(3n + 3)x \in \left[2n + 1 + \frac{2n - 2}{3n - 1}, 2n + 2\right),$$

and so automatically $3n + 3 \notin S_x$ in this case. This gives the equivalence between $(\text{ii})^n$ and $(\text{iii})^n$.

Finally, we note that if $x \in \left[\frac{2n+1}{3n+2}, \frac{2}{3}\right)$, then $(3n + 4)x \in \left[2n + 2 + \frac{n}{3n+2}, 2n + 2 + \frac{2}{3}\right)$, so $\lfloor(3n + 4)x\rfloor = 2n + 2$ and $3n + 4 \in S_x$, as desired. This completes the proof of the lemma. ∎

Now we use the lemma to solve the problem, which is to compute $\inf_{x\in[0,1)} f(x)$. We claim that this infimum is $\frac{4}{7} = 0.100100100\ldots$. Indeed, $f(x) < \frac{4}{7}$ implies $(\text{i})^n$ for all n, hence $(\text{iii})^n$ for all n, hence $x \in \bigcap_n \left[\frac{2n+1}{3n+2}, \frac{2}{3}\right) = \emptyset$, a contradiction; so the infimum is at least $\frac{4}{7}$. On the other hand, choosing any $x_n \in \left[\frac{2n+1}{3n+2}, \frac{2}{3}\right)$ we have

$$f(x_n) \in (0.100100\cdots100100, 0.100100\cdots100101)$$

(with $3n+3$ bits in both binary expansions) and so $\left|f(x_n) - \frac{4}{7}\right| < 2^{-3n-3}$. Thus $\lim_{n\to\infty} f(x_n) = \frac{4}{7}$, and the infimum must be exactly $\frac{4}{7}$.

Solution to A5. If $q = 1$, then $N_q = 0$ is even and q is not of the form p^k with k positive, so we may assume that $q > 1$. Let $p_1, \ldots, p_r$ be the distinct primes dividing q, and note that $\gcd(a, q) = 1$ if and only if q is not divisible by any of $p_1, \ldots, p_r$. Thus the integers a counted by N_q are those for which $0 < a < q/4$ and a is *not* in any of the sets

$$A_i = \{a \in \mathbb{N} | 0 < a < q/4,\ p_i \text{ divides } a\}$$

for $1 \le i \le r$. By the inclusion-exclusion principle, it follows that

$$\begin{aligned} N_q &= \sum_{S\subseteq\{1,\ldots,r\}} (-1)^{\#S} \#(\cap_{i\in S} A_i) \\ &= \sum_{S\subseteq\{1,\ldots,r\}} (-1)^{\#S} \left\lfloor \frac{q}{4\prod_{i\in S} p_i} \right\rfloor. \end{aligned}$$

Note that the odd terms in this sum are exactly the ones for which $\dfrac{q}{\prod_{i\in S} p_i} \equiv 5, 7 \pmod 8$. Denote the odd integer $\dfrac{q}{\prod_{i\in S} p_i}$ by $F(S)$; then N_q is odd if and only if $F(S) \equiv 5, 7 \pmod 8$ for an odd number of the subsets S of $\{1, \ldots, r\}$.

If one of the primes dividing q, say p_1, is congruent to 1 or 3 modulo 8, then we can pair the subsets of $\{1, \ldots, r\}$ by associating T to $T \cup \{1\}$ for each subset T of $\{2, \ldots, r\}$. We then have $F(T \cup \{1\}) \equiv 5, 7 \pmod 8$ if and only if $F(T) \equiv 5, 7 \pmod 8$, so each pair contributes either 0 or 2 to the count of subsets for which $F(S) \equiv 5, 7 \pmod 8$. Thus N_q is even in this case.

If there are two primes dividing q, say p_1 and p_2, that are each congruent to 5 or 7 modulo 8, then we can pair the subsets of $\{1, \ldots, r\}$ by associating T to $T \cup \{1, 2\}$ and $T \cup \{1\}$ to $T \cup \{2\}$ for each subset T of $\{3, \ldots, r\}$. Because $p_1 p_2 \equiv 1 \text{ or } 3 \pmod 8$ in this case, once again each pair will contribute either 0 or 2 to the count of subsets for which $F(S) \equiv 5, 7 \pmod 8$, and N_q will again be even.

The only case that remains is $q = p^k$ with p prime and $p \equiv 5, 7 \pmod 8$. In this case, $r = 1$, and there are just two subsets S, for which we have $F(\emptyset) = p^k$, $F(\{1\}) = p^{k-1}$. Exactly one of p^k, p^{k-1} is congruent to 5 or 7 modulo 8, so N_q is indeed odd and we are done.

Solution to A6. (Based on a student paper.) Consider the $2n \times 2n$ matrix products

$$\begin{pmatrix} B-\lambda I & O \\ -M & I \end{pmatrix}\begin{pmatrix} I & X \\ M & A-\lambda I \end{pmatrix} = \begin{pmatrix} B-\lambda I & (B-\lambda I)X \\ O & A-MX-\lambda I \end{pmatrix} \text{ and}$$

$$\begin{pmatrix} I & X \\ M & A-\lambda I \end{pmatrix}\begin{pmatrix} B-\lambda I & O \\ -M & I \end{pmatrix} = \begin{pmatrix} B-XM-\lambda I & X \\ MB-AM & A-\lambda I \end{pmatrix},$$

where I is the $n \times n$ identity matrix and O is the $n \times n$ zero matrix.

Because $MB - AM = O$ and the determinant of a product does not depend on the order, we see that

$$\det(B-\lambda I)\det(A-MX-\lambda I) = \det(B-MX-\lambda I)\det(A-\lambda I).$$

However, we are given that $\det(B - \lambda I) = \det(A - \lambda I)$, and since this characteristic polynomial is nonzero for all but at most n values of λ, it follows that

$$\det(A - MX - \lambda I) = \det(B - MX - \lambda I)$$

for all but at most n values of λ and for any $n \times n$ matrix X. Because, for fixed X, both sides are polynomial expressions in λ, they must actually be equal for all values of λ; in particular, for $\lambda = 0$ we get $\det(A - MX) = \det(B - MX)$, as required.

Solution to B1. Define the function g by $g(x) = f(x) \cdot e^{x/2}$. Then g has the same zeros as f, so by Rolle's theorem, g' must have at least four distinct real zeros (one between each adjacent pair of zeros of g). Applying Rolle's theorem twice more, we see that g''' must have at least two distinct real zeros. But

$$\begin{aligned} g'''(x) &= f'''(x) \cdot e^{x/2} + 3f''(x) \cdot (1/2)e^{x/2} + 3f'(x) \cdot (1/4)e^{x/2} + f(x) \cdot (1/8)e^{x/2} \\ &= (1/8)e^{x/2}(f(x) + 6f'(x) + 12f''(x) + 8f'''(x)), \end{aligned}$$

and because the exponential is never zero, the result follows.

Solution to B2. We will show that there is, in fact, such a number. Let s_n be the nth term of the sequence of sums, starting with $s_1 = 6$. We first show, by induction on n, that $s_n = 10(n-1) + d_n$, with the final digit d_n equal to 5, 6, or 7. This is clearly true for $n \leq 3$; suppose it is true through $n = N$. Then for any $i < N$, exactly one of the "decade" of ten numbers $10i + 1$ through $10i + 10$ is crossed off as a sum, and the other nine are later crossed off in groups of three summands. In particular, $10i + 1$, $10i + 2$, $10i + 3$ are always crossed off as summands together with their sum $10(3i) + 6$, which has last digit $d_{3i+1} = 6$. Next, $10i + 4$ is crossed off as a summand together with exactly two of $10i + 5$, $10i + 6$, $10i + 7$, the third of these having been crossed off earlier by induction hypothesis. If that earlier sum is $10i + k$, so that $d_{i+1} = k$, then the new sum is $(10i + 4) + (10i + 5) + (10i + 6) + (10i + 7) - (10i + k) = 10(3i + 1) + (12 - k)$, with last digit $d_{3i+2} = 12 - k$; note that $12 - k$ is one of 5, 6, 7. Finally, the remaining three numbers in the decade are $10i + 8$, $10i + 9$, $10i + 10$ and are crossed off together with their sum $10(3i + 2) + 7$, which has last digit $d_{3i+3} = 7$. This completes the induction, because s_{N+1} will be produced as a sum of one of the three types just listed, with $i = \lfloor N/3 \rfloor$; we have seen along the way that for all $i \geq 0$,

$$d_{3i+1} = 6, \quad d_{3i+2} = 12 - d_{i+1}, \quad \text{and} \quad d_{3i+3} = 7 \quad \text{as well as}$$
$$s_{3i+1} = 30i + 6, s_{3i+2} = 30i + 22 - d_{i+1}, s_{3i+3} = 30i + 27.$$

In particular, s_{3i+2} will end in 2015 if and only if $d_{i+1} = 7$ and $30i + 15$ ends in 2015. The first of these conditions will certainly hold if $i + 1$ is divisible by 3, say $i = 3j - 1$, so we only have to show that there is a positive integer j such that $30i + 15 = 90j - 15$ ends in 2015, or equivalently $90j$ ends in 2030. The first such j has $90j = 42030$, so $j = 467$, $i = 1400$, $3i + 2 = 4202$. Thus the 4202nd sum ends in 2015.

Solution to B3. (Based on a student paper.) These matrices M are the scalar multiples of $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ and of $\begin{pmatrix} -3 & -1 \\ 1 & 3 \end{pmatrix}$. To see this, first note that for $M_1 = \begin{pmatrix} -3 & -1 \\ 1 & 3 \end{pmatrix}$, we have $M_1^2 = \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix}$, so $M_1^3 = 8M_1$ is in S; it is then easy to check that $M^3 \in S$ for the matrices M from the previous sentence.

Now suppose that M is in S and that $k > 1$ is such that M^k is also in S. If the common difference in the arithmetic progression for M is 0, then M is a scalar multiple of $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, so we may assume that the common difference is $t \neq 0$. Then we have $M = \begin{pmatrix} a & a+t \\ a+2t & a+3t \end{pmatrix}$, with characteristic polynomial $\lambda^2 - (2a+3t)\lambda - 2t^2$. Because the constant term of this polynomial is negative and thus the discriminant is positive, there are distinct nonzero real roots, the eigenvalues λ_1, λ_2. Let $\mathbf{v}_1, \mathbf{v}_2$ be corresponding eigenvectors.

Now note that

$$M \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} -t \\ -t \end{pmatrix}$$

is a multiple of $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, and similarly, for any matrix N in the set S, $N \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ is a multiple of $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. In particular, $M^k \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ is such a multiple. Also, $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ cannot be an eigenvector of M, so we can write $\begin{pmatrix} 1 \\ 1 \end{pmatrix} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2$ for suitable $c_1, c_2 \neq 0$, and we then have

$$M \begin{pmatrix} 1 \\ -1 \end{pmatrix} = -tc_1\mathbf{v}_1 - tc_2\mathbf{v}_2, \text{ so that}$$

$$M^k \begin{pmatrix} 1 \\ -1 \end{pmatrix} = -tc_1\lambda_1^{k-1}\mathbf{v}_1 - tc_2\lambda_2^{k-1}\mathbf{v}_2.$$

As this latest vector is a multiple of $c_1\mathbf{v}_1 + c_2\mathbf{v}_2$, it follows that $\lambda_1^{k-1} = \lambda_2^{k-1}$, and therefore $\lambda_1 = -\lambda_2$ because the eigenvalues are real and distinct. Then the trace $2a + 3t$ of M is zero, and it follows that

$$M = \begin{pmatrix} a & a+t \\ a+2t & a+3t \end{pmatrix} = -\frac{t}{2}\begin{pmatrix} -3 & -1 \\ 1 & 3 \end{pmatrix},$$

completing the proof.

Solution to B4. We will use the generating function $f(x, y, z) = \sum_{(a,b,c)\in T} x^a y^b z^c$ to get the desired value $f(2, 1/3, 1/5)$. We will be expressing $f(x, y, z)$ as a product of series, and because the exponents of x, y, and z add when we multiply terms, it will be useful to add triples such as (a, b, c) coordinatewise. Note that the condition $(a, b, c) \in T$ is equivalent to each of the positive integers a, b, c being less than the sum of the other two. Thus for every $(a, b, c) \in T$, if we let $d \geq 1$ be the difference between the sum of the two smallest integers in $\{a, b, c\}$ and the third (the largest) integer, we can write $(a, b, c) = (a', b', c') + (d, d, d)$, where the largest of the integers a', b', c' is *equal* to the sum of the other two. Then we can rewrite (a', b', c') as a linear combination of two of the three triples $(1, 1, 0)$, $(1, 0, 1)$, $(0, 1, 1)$; for example, if $b' = a' + c'$, then $(a', b', c') = a'(1, 1, 0) + c'(0, 1, 1)$. Also, if we allow all three triples, then we can use $(2, 2, 2) = (1, 1, 0) + (1, 0, 1) + (0, 1, 1)$ to rewrite the expression for (a, b, c) so that the term (d, d, d) is reduced to $(1, 1, 1)$ or $(2, 2, 2)$. That is, we can write

$$(a, b, c) = \alpha(1, 1, 0) + \beta(1, 0, 1) + \gamma(0, 1, 1) + \delta(1, 1, 1),$$

where α, β, γ are nonnegative integers and $\delta \in \{1, 2\}$. On the other hand, given any such expression for (a, b, c), the integer δ is determined by the parity of $a + b + c$, and then α, β, γ are uniquely determined also. And if there is such an expression for (a, b, c), then the inequalities $a < b + c, b < c + a, c < a + b$ are satisfied and so $(a, b, c) \in T$.

It follows that the generating function is the product of four series (if you prefer, three series and a polynomial) where the possible exponents for x, y, z in the series are given by $\alpha(1, 1, 0)$, $\beta(1, 0, 1)$, $\gamma(0, 1, 1)$, $\delta(1, 1, 1)$, respectively. The formal sums of these series are

$$1 + xy + x^2y^2 + x^3y^3 + \cdots = \sum_{k=1}^{\infty} x^k y^k = \frac{1}{1 - xy},$$

$$1 + xz + x^2z^2 + x^3z^3 + \cdots = \sum_{k=1}^{\infty} x^k z^k = \frac{1}{1 - xz},$$

$$1 + yz + y^2z^2 + y^3z^3 + \cdots = \sum_{k=1}^{\infty} y^k z^k = \frac{1}{1 - yz},$$

$$xyz + x^2y^2z^2.$$

Note that the series converge absolutely for $|xy| < 1$, $|xz| < 1$, $|yz| < 1$, respectively, and in particular for $x = 2$, $y = 1/3$, $z = 1/5$. Thus we can indeed get $f(2, 1/3, 1/5)$ by evaluating the product

$$\frac{xyz + x^2y^2z^2}{(1 - xy)(1 - xz)(1 - yz)} = \frac{xyz(1 + xyz)}{(1 - xy)(1 - xz)(1 - yz)}$$

of the sums above at $x = 2$, $y = 1/3$, $z = 1/5$, which yields the answer

$$\frac{(2/15)(17/15)}{(1/3)(3/5)(14/15)} = \frac{17}{21}.$$

Solution to B5. (Based on a student paper.) We only consider permutations π of $\{1, 2, \ldots, n\}$ satisfying the stated condition that $|i - j| = 1$ implies $|\pi(i) - \pi(j)| \leq 2$, and we write such permutations as sequences in which the numbers are listed in the order $\pi(1), \pi(2), \ldots, \pi(n)$. Let A_n be the set of those π for which $\pi(1) = n$ or $\pi(n) = n$, so that n occurs at one end of the sequence, let B_n be the set of those π for which $n - 1$ occurs at one end of the sequence, and let C_n be the set of those π for which n and $n - 1$ are adjacent in the sequence (in some order). Note that these sets are not disjoint; let a_n, b_n, c_n be the sizes of the sets A_n, B_n, C_n, respectively. Now consider the permutations π of $\{1, 2, \ldots, n + 1\}$ which satisfy the stated condition. (This means that adjacent numbers in the sequence differ by 2 or less.) Consider the location of $n + 1$ in such a sequence. If it is not at an end, then its neighbors must be n and $n - 1$, and so if we leave out $n + 1$, we will get a permutation of $\{1, 2, \ldots, n\}$ from the set C_n. If $n + 1$ is at an end, then its unique neighbor is either n or $n - 1$, and so if we again omit $n + 1$, we get either a permutation from A_n or one from B_n. Conversely, any permutation from A_n, B_n, or C_n can be "expanded" to a permutation of $\{1, 2, \ldots, n + 1\}$ satisfying the stated condition by inserting $n + 1$ at the outside of the end with n, at the outside of the end with $n - 1$, or between n and $n - 1$, respectively. Thus the total number P_{n+1} is given by

$$P_{n+1} = a_n + b_n + c_n.$$

By similar arguments, we get the recurrences

$$a_{n+1} = a_n + b_n, \quad c_{n+1} = a_n + c_n.$$

Now consider the permutations in the set B_{n+1}, which have n at one end. If $n+1$ is at the other end, it must be next to $n-1$, so that removing $n+1$ yields a permutation in $A_n \cap B_n$. If $n+1$ is not at the other end, it must be next to both n and $n-1$, and removing $n+1$ then yields a permutation in $A_n \cap C_n$. Thus we are led to consider the sets $D_n = A_n \cap B_n$ and $E_n = A_n \cap C_n$ and their sizes d_n, e_n; we see from the above that $b_{n+1} = d_n + e_n$. Now for a permutation in D_{n+1}, with n and $n+1$ on opposite ends, the only neighbor of $n+1$ is $n-1$, so removing $n+1$ yields a permutation in D_n and we have $d_{n+1} = d_n$; clearly, D_2 consists of the sequences 1 2 and 2 1, so $d_2 = 2$ and hence $d_n = 2$ for all n. On the other hand, for a permutation in E_{n+1}, which has $n+1$ at one end and adjacent to n, removing $n+1$ yields a permutation in A_n, and we have $e_{n+1} = a_n$. In summary, we have

$$a_{n+1} = a_n + b_n, \quad b_{n+1} = 2 + a_{n-1}, \quad c_{n+1} = a_n + c_n.$$

Now we can subtract the second of these equations for $n-1$ from that equation for n and use the first equation for $n-2$ to get

$$b_{n+1} - b_n = 2 + a_{n-1} - (2 + a_{n-2}) = a_{n-1} - a_{n-2} = b_{n-2}.$$

Therefore,

$$\begin{aligned} P_{n+5} - P_{n+4} &= a_{n+4} + b_{n+4} + c_{n+4} - a_{n+3} - b_{n+3} - c_{n+3} \\ &= (a_{n+4} - a_{n+3}) + (b_{n+4} - b_{n+3}) + (c_{n+4} - c_{n+3}) \\ &= b_{n+3} + b_{n+1} + a_{n+3}, \end{aligned}$$

from which

$$\begin{aligned} P_{n+5} - P_{n+4} - P_{n+3} &= b_{n+3} + b_{n+1} + a_{n+3} - a_{n+2} - b_{n+2} - c_{n+2} \\ &= (b_{n+3} - b_{n+2}) + b_{n+1} + (a_{n+3} - a_{n+2}) - c_{n+2} \\ &= b_n + b_{n+1} + b_{n+2} - c_{n+2} \\ &= b_n + 2 + a_{n-1} + 2 + a_n - (a_{n+1} + c_{n+1}) \\ &= 4 + b_n + a_{n-1} + a_n - a_{n+1} - (a_n + c_n) \\ &= 4 + a_{n-1} - a_{n+1} + b_n - c_n. \end{aligned}$$

Finally, adding $P_n = a_{n-1} + b_{n-1} + c_{n-1}$, we get

$$\begin{aligned} P_{n+5} - P_{n+4} - P_{n+3} + P_n &= 4 + a_{n-1} - a_{n+1} + b_n - c_n + a_{n-1} + b_{n-1} + c_{n-1} \\ &= 4 + 2a_{n-1} - (a_{n+1} - b_n) + b_{n-1} - (c_n - c_{n-1}) \\ &= 4 + 2a_{n-1} - a_n + b_{n-1} - a_{n-1} \\ &= 4 + (a_{n-1} + b_{n-1} - a_n) = 4, \end{aligned}$$

which is independent of n, and we are done.

Solution to B6. Note that if d is an odd (positive) divisor of k and we write $k = md$, then d is in the interval $\left[1, \sqrt{2k}\right)$ if and only if $d < 2m$. Therefore, if we let S_N be the Nth partial sum of the given series, we can express it as

$$S_N = \sum_{k=1}^{N} (-1)^{k-1} \frac{A(k)}{k} = \sum_{k=1}^{N} \sum_{\substack{d \text{ odd} \\ k=md, d<2m}} (-1)^{k-1} \frac{1}{k}$$

$$= \sum_{\substack{d<\sqrt{2N} \\ d \text{ odd}}} \frac{1}{d} \sum_{m \in (d/2, N/d]} \frac{(-1)^{m-1}}{m}.$$

Now, for any positive *real* number k, define the alternating sum $R_k = \sum_{m>k} \frac{(-1)^{m-1}}{m}$. Note that because the absolute values of the terms of this sum are decreasing, $|R_k| < 1/k$. In terms of these sums, we can rewrite our expression for S_N as

$$S_N = \sum_{\substack{d<\sqrt{2N} \\ d \text{ odd}}} \frac{1}{d} (R_{d/2} - R_{N/d}).$$

Now the infinite series $\sum_{d \text{ odd}} \frac{1}{d} R_{d/2}$ is (absolutely) convergent because the absolute value of the term for the index d is at most $\frac{2}{d^2}$. We next show that the sum of this new series is equal to the sum we want, which we will denote by

$$S = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{A(k)}{k}.$$

First we subtract the new series from the partial sum S_N to get

$$S_N - \sum_{d \text{ odd}} \frac{1}{d} R_{d/2} = \sum_{\substack{d<\sqrt{2N} \\ d \text{ odd}}} \frac{1}{d} (R_{d/2} - R_{N/d}) - \sum_{d \text{ odd}} \frac{1}{d} R_{d/2}$$

$$= - \sum_{d<\sqrt{2N} \text{ odd}} \frac{1}{d} R_{N/d} - \sum_{d \geq \sqrt{2N} \text{ odd}} \frac{1}{d} R_{d/2}.$$

Each term in the first sum on the right-hand side is at most $(1/d)(d/N) = 1/N$ in absolute value, and so the first sum is $O(N^{-1/2})$. Since the second sum on the right-hand side is the tail of a convergent sum, it too tends to 0 as $N \to \infty$. Thus, taking the limit we see that the desired sum S equals the absolutely convergent sum $\sum_{d \text{ odd}} \frac{1}{d} R_{d/2}$, or equivalently (setting $d = 2k + 1$ and noting that $R_{d/2} = R_{k+(1/2)} = R_k$)

$$S = \sum_{k=0}^{\infty} \frac{1}{2k+1} R_k. \tag{1}$$

Now let us derive a formula for R_k as the remainder term in Taylor's formula for $\ln(x)$, centered at $x = 1$ and evaluated at $x = 2$. The $(k+1)$th derivative of $\ln(x)$ is $(-1)^k k!/x^{k+1}$, and so we have

$$R_k = \sum_{m>k} \frac{(-1)^{m-1}}{m} = \ln(2) - \sum_{m=1}^{k} \frac{(-1)^{m-1}}{m} = (-1)^k \int_1^2 (2-x)^k x^{-k-1} \, dx.$$

Since the function $(2-x)^k/x^{k+1}$ is nonnegative on [1, 2] and the sum (1) is absolutely convergent, Fubini's theorem implies that

$$\begin{aligned} S &= \int_1^2 \sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1}(2-x)^k x^{-k-1}\,dx \\ &= \int_1^2 \frac{1}{\sqrt{x(2-x)}} \sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1}\left(\frac{2-x}{x}\right)^{(2k+1)/2} dx \\ &= \int_1^2 \frac{1}{\sqrt{x(2-x)}} \arctan\left(\sqrt{\frac{2-x}{x}}\right) dx. \end{aligned}$$

The indefinite integral can be found by the substitution $u = \arctan\left(\sqrt{\frac{2-x}{x}}\right)$ (or in two steps via $v = \sqrt{\frac{2-x}{x}}$) to be

$$\int \frac{1}{\sqrt{x(2-x)}} \arctan\left(\sqrt{\frac{2-x}{x}}\right) dx = -\left(\arctan\left(\sqrt{\frac{2-x}{x}}\right)\right)^2 + C.$$

Therefore,

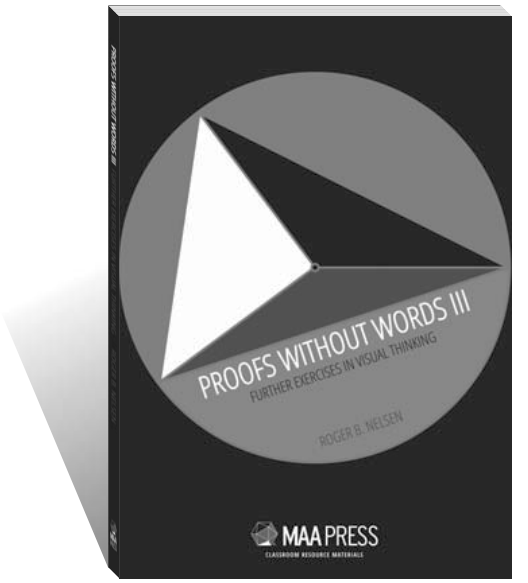
$$S = \arctan(1)^2 - 0 = \left(\frac{\pi}{4}\right)^2 = \frac{\pi^2}{16}.$$

Artist Spotlight
Bjarne Jespersen

Royal Family: Triple Whitehead, Wave Packet, Tetracoil, Halo, and Hexacoil, Bjarne Jespersen; Wood, 6–10.5 cm in diameter, 2002; private collection. The five pieces share a basic weaving pattern which is symmetrically repeated in five different ways according to a technique using rhombic polyhedra. The numbers of components in each are three, six, four, ten, and six.

See interview on page 55.

More PWWs for Your Enjoyment



Proofs Without Words III: Further Exercises in Visual Thinking
Roger B. Nelsen

Proofs without words are figures or diagrams that help the reader see why a particular mathematical statement is true, and how one might begin to formally prove it true. The proofs in the book are intended primarily for the enjoyment of the reader, however, teachers will want to use them with students at many levels: high school courses from algebra through precalculus and calculus; college level courses in number theory, combinatorics, and discrete mathematics; and pre-service and in-service courses for teachers.

Catalog Code: PW3
List: $50.00
MAA Member: $37.50

ISBN: 978-0-88385-790-8
187 pp., Paperbound, 2016
Classroom Resource Materials

To order, visit *maa-store.hostedbywebstore.com* or call 800-331-1622.

MAA PRESS

MAA MATHFEST
August 3-6, 2016

Join Us in Columbus, Ohio

Earle Raymond Hedrick Lectures
Hendrik Lenstra, Universiteit Leiden
Hedrick Lecture 1: *The Group Law on Elliptic Curves*
Hedrick Lecture 2: *The Combinatorial Nullstellensatz*
Hedrick Lecture 3: *Profinite Number Theory*

AMS-MAA Joint Invited Address
Ravi Vakil, Stanford University

MAA Invited Addresses
Arthur Benjamin, Harvey Mudd College
Magical Mathematics

Judy Holdener, Kenyon College
Immersion in Mathematics via Digital Art

Robert Megginson, University of Michigan
Mathematical Sense and Nonsense Outside the Classroom: How Well are we Preparing our Students to Tell the Difference

MAA James R.C. Leitzel Lecture
Annalisa Crannell, Franklin & Marshall College
Inquiry, Encouragement, Home Cooking (and other boundary value problems)

AWM-MAA Etta Z. Falconer Lecture
Izabella Laba, University of British Columbia
Harmonic Analysis and Additive Combinatorics on Fractals

MAA Chan Stanek Lecture for Students
Colin Adams, Williams College
Zombies & Calculus: A Survival Guide

Pi Mu Epsilon J. Sutherland Frame Lecture
Robin Wilson, Open University
Combinatorics – the Mathematics that Counts

NAM David Blackwell Lecture
Robert C. Hampshire, University of Michigan Transportation Research Institute
Urban Analytics: The Case for Smart Parking

Register Today • maa.org/mathfest

MAA 100
MATHEMATICAL ASSOCIATION OF AMERICA
CELEBRATING A CENTURY OF ADVANCING MATHEMATICS

MAA 100
MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth St., NW · Washington, DC 20036

CONTENTS

ARTICLES

PROBLEMS AND SOLUTIONS

REVIEWS

NEWS AND LETTERS