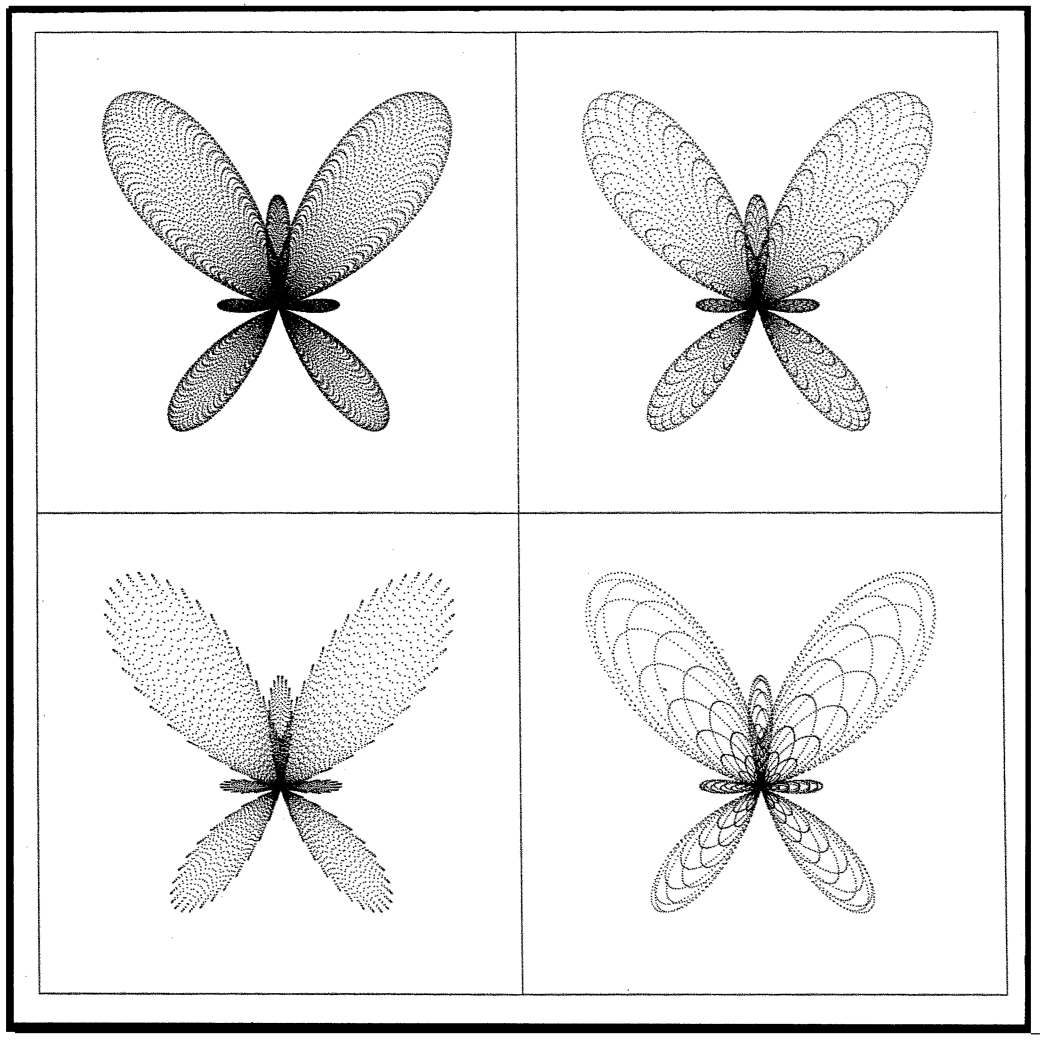
Vol. 70, No. 2 April 1997

MATHEMATICS MAGAZINE



Butterflies with Texture (see p. 116)

- Are Individual Rights Possible?
- Variations on an Irrational Theme
- Arithmetic Triangles

An Official Publication of The MATHEMATICAL ASSOCIATION OF AMERICA

EDITORIAL POLICY

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

A more detailed statement of author guidelines appears in this *Magazine*, Vol. 69, pp. 78–79, and is available from the Editor. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, or published by another journal or publisher.

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

AUTHORS

Ray Beauregard received his Ph.D. at the University of New Hampshire in 1968, under the direction of Richard E. Johnson. Since that time he has been at the University of Rhode Island, where he is a professor of mathematics. His research interests include ring theory and number theory. He is coauthor (with John Fraleigh) of a textbook, *Linear Algebra*, currently in its third edition. In addition to cojoining companion right triangles he enjoys sailing his sloop and playing his piano.

Dan Kalman is an Associate Executive Director of the MAA. He is on leave from American University, where he joined the mathematics faculty after working for 8 years in the aerospace industry. Before that he taught at the University of Wisconsin–Green Bay. Kalman has a B.S. from Harvey Mudd College and a Ph.D. from the University of Wisconsin–Madison. He is grateful to his friends Mena and Shahriari for writing this paper with him, thereby reducing his Erdős number to 4 by two routes.

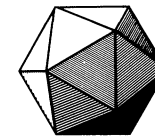
Robert Mena has been teaching at CSULB since 1988, after 15 years at the University of Wyoming. His favorite courses are the History of Mathematics, Number Theory, Statistics, and Combinatorics.

Don Saari received his bachelor's degree from Michigan Technological University and his Ph.D. in mathematics from Purdue. After a postdoctoral position in the Yale astronomy department, he moved to Northwestern University, where he is currently the Arthur and Gladys Pancoe Professor of Mathematics. His research interests emphasize applications of dynamical systems to mathematical physics (in particular, the Newtonian n-body problem) and to issues arising in economics and the other social sciences. The disturbing conclusion of Arrow's theorem sparked his interest in the areas of decision and voting theory; this led to his recent book *Basic Geometry of Voting*.

Shahriar Shahriari has been teaching mathematics at Pomona College since 1989. He received a B.A. from Oberlin College in 1977 and a Ph.D. from the University of Wisconsin–Madison in 1986. His current research interests are in combinatorics of finite sets. Among the courses he teaches at Pomona is an alternative to second semester calculus, in which calculus topics are taught in the context of number theory, and the students develop all the material through solving problems. In his free time he likes to cook Iranian food. His specialties include Ghormehsabzi and Fesenjon.

E. R. Suryanarayan taught at the Universities of Gauhati and Pune in India before receiving his Ph.D. at the University of Michigan in 1961, under the direction of Nathaniel Coburn. He has been at the University of Rhode Island since 1960, where he is professor of mathematics. His research interests include applied mathematics, crystallography, and the history of mathematics. His hobbies include music and languages. The idea to investigate arithmetic triangles is an outgrowth of the authors' recent work on the hyperbolic view of Pythagorean triples.

Vol. 70, No. 2, April 1997



MATHEMATICS MAGAZINE

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

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

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

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

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

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

PRINTED IN THE UNITED STATES OF AMERICA

ARTICLES

Are Individual Rights Possible?

DONALD G. SAARI
Northwestern University
Evanston, IL 60208-2730

1. Introduction

What are your rights? Should you or should society determine whether you can wear a brown or blue shirt to class? Let's be more provocative: should you or should society decide whether you can read that raunchy article? The answers seem obvious—at least they did until a quarter of a century ago when A. Sen ([**18**], [**19**]) analyzed this question with an axiomatic formulation. His highly disturbing mathematical conclusion casts doubt on the rights of individuals to make even seemingly trivial decisions of this type.

How can Sen's conclusion, which directly confronts our daily actions, be correct? As his proof is accurate, it is understandable that his disquieting assertion continues to concern experts from mathematics, economics, philosophy, and political science, among other areas. While the response has created a sizable literature, none of the papers provides a way out. Instead, the problem has become similar to a doll made of fresh tar; the more it is embraced, the greater the mess that is discovered.

In this essay, a surprisingly elementary explanation of Sen's problem is offered. (See [**16**] for a complete description.) It only uses only the kind of introductory mathematics too many students try to skip due to persistent rumors that this "busy work" might convert brain matter into mushy oatmeal. Let me explain.

Sen's assumptions In his theory, Sen assumes that society is confronted with $k \geq 3$ alternatives. Reflecting the sense that an individual has freedom of belief, Sen's first axiom is as follows:

(U) *Unrestricted domain.* Each individual can rank the alternatives in any desired transitive manner.

Recall, an individual's ranking is *transitive* if it obeys the ordering properties of points on the line. For instance, if we prefer apple pie to blueberry pie and blueberry pie to cherry pie, then surely we prefer apple pie to cherry pie; i.e., the rankings $a \succ b$ and $b \succ c$ (meaning a is preferred to b, and b is preferred to c) imply $a \succ c$. As a voter with transitive preferences is called "rational," it is traditional to call a voter without transitive preferences "irrational." To avoid the nasty, pejorative ring of this term, I use the more tempered choices of "primitive" or "unsophisticated" voters.

The second property is named after a nineteenth century mathematical physicist who probably made his most important contributions in the social sciences.

(P) *Pareto.* If every individual prefers $a \succ b$, then society prefers $a \succ b$.

This makes sense; (P) merely requires that, should everyone agree on the ranking of a particular pair, then that is society's ranking of the pair.

The third condition, Sen's *minimal liberalism*, allows at least two individuals to make certain societal decisions. More precisely:

(ML) *Minimal Liberalism.* There are at least two individuals who are decisive over different pairs of alternatives; the decisive voter's personal ranking for the assigned pair determines society's ranking of the pair.

This condition captures "individual liberty": you, and only you, have the right to choose which shirt to wear to class.

How can anyone argue against these natural, seemingly innocuous conditions? You might, once you discover that they can make it impossible for society to reach a decision. The problem, as explained next, is that (U), (P), and (ML) allow "cycles."

The problem with cycles What are cycles? What problems do they cause? Can they occur in natural settings? To explain in more familiar terms, "*Step a little closer because I am going to offer you a chance to become rich by playing a simple dice game. You may choose any one of the three dice. Only after you are absolutely sure of your choice will I select one of the remaining two. Indeed, I am such a nice guy that, after a while, if you want my die you can have it. I will be happy to choose a different one.*"

In this game, each of us rolls our selected die—high score wins. Instead of using standard dice, each die from our set carries three numbers, with each repeated twice: the markings are

Die	Numbers		
A	8	1	6
B	3	5	7
C	4	9	2

Any two dice define nine combinations. For instance, the possible outcomes for the pair $\{A, B\}$ are

$$\begin{array}{lll} (8,3), & (8,5), & (8,7), \\ (1,3), & (1,5), & (1,7), \\ (6,3), & (6,5), & (6,7). \end{array}$$

The dice are fair in the sense that each face is equally likely to appear, so the better die is the one that wins the most pairwise matches. As die A wins everything in the top row and the first two in the last, it wins five out of the nine possible arrangements. Consequently, "A is better than B," which I denote by $A \succ B$. A similar analysis shows that $B \succ C$. Which die do you want?

It is tempting to select A, but if you do you will make me rich, because $C \succ A$. In other words, these dice generate the *cycle* $A \succ B$, $B \succ C$, $C \succ A$, making it impossible to choose the "best" die. Whatever your selection, there is a die I can choose to beat you. I can even give you my die and select a different one to keep bleeding your wallet dry. (For other cyclic dice arrangements, see [4].)

The trouble with cycles, then, is that they do not admit a maximal element. Whether in an amusing dice game or, more troubling, in society, cycles subvert the societal goal of making the "optimal" decision. A crucial objective of choice theory, therefore, is to avoid cyclic conclusions.

2. Sen's Examples

In his seminal paper, Sen **[18]** constructs two examples where (P), (U), and (ML) force the troubling cycles. The first example has voters one and two decisive, respectively, over $\{a, b\}$ and $\{b, c\}$. Table 1 identifies the binary rankings used by a ML-procedure for a particular profile. (A *profile* lists how each voter ranks the candidates.) The blanks in the table correspond to binary rankings that are irrelevant for a ML-procedure because some other voter is decisive.

TABLE 1: Sen's first example

Voter	Choice $\{a, b\}$	$\{b, c\}$	$\{a, c\}$
1	$a \succ b$	—	$c \succ a$
2	—	$b \succ c$	$c \succ a$
Others	—	—	$c \succ a$

To reconstruct the original profile, note that the blanks for voters one and two must be, respectively, $c \succ b$ (to assure that $c \succ a \succ b$) and $b \succ a$ (to assure that $b \succ c \succ a$). Choices for all other voters, who are unanimous in their $\{a, c\}$ choice, come from $c \succ b \succ a$, $c \succ a \succ b$, or $b \succ c \succ a$. The cyclic societal outcome starts with $a \succ b$ (voter one is decisive over $\{a, b\}$), followed by $b \succ c$ (voter two is decisive over $\{b, c\}$), and completed with $c \succ a$ (by Pareto). This cyclic outcome makes it impossible for society to make decisions!

It is easy to identify with this conflict. For instance, the two voters could be dorm roommates struggling over the use of a TV, where voter one is studious while voter two, well, enjoys life. Choices a, b, and c could represent, respectively, watching news, watching MTV, and turning the TV off. Our studious voter one prefers $c \succ a \succ b$ while voter two prefers $b \succ c \succ a$, generating the stated conflict. (Sen **[18]** constructs an interesting censorship example.)

A natural objection to this example is that the decisive voters' decisions involve the common alternative b. Could this explain the difficulty? Sen's second example sidesteps this criticism by assuming that voters one and two are decisive, respectively, over the *distinct* pairs $\{a, b\}$ and $\{c, d\}$; his choice of transitive preferences for the voters defines the following table. Again, blanks correspond to binary rankings that are irrelevant for a ML procedure. Transitive preferences supporting this table could be where everyone but voter two has the ranking $d \succ a \succ b \succ c$ (so voter one's blank is filled with $d \succ c$ and "Others" are filled with $a \succ b$, $d \succ c$). Assign voter two the preferences $b \succ c \succ d \succ a$ to fill the blank with $b \succ a$. Then, society's decision is $a \succ b$ (by voter one's rights), $b \succ c$ (by unanimity), $c \succ d$ (by voter two's rights), and $d \succ a$ (by unanimity); this creates another cycle and causes a potential societal deadlock.

TABLE 2: Sen's second example

Voter	Choice $\{a, b\}$	$\{b, c\}$	$\{c, d\}$	$\{a, d\}$
1	$a \succ b$	$b \succ c$	—	$d \succ a$
2	—	$b \succ c$	$c \succ d$	$d \succ a$
Others	—	$b \succ c$	—	$d \succ a$

Before reading any further, the reader is invited to try to resolve this conflict, which is summarized in the next theorem. Remember, this is not a mere puzzle; it is a serious issue that has confused a generation of experts from several fields. The disturbing implications of Sen's assertion have motivated philosophical debates about the meaning of individual rights.

THEOREM (SEN). *With $n \geq 3$ alternatives and at least two voters, no procedure can satisfy* (U), (P), *and* (ML) *and avoid cyclic outcomes.*

3. Resolution Through "Ignored" Mathematics

Now that we understand Sen's problem, let's review the often "ignored" mathematics that offers relief for this quarter-century headache. It is where the student is asked to determine the domain for a function, say, $f(x) = (x^2 + 3x + 1)/[(x - 1)(x + 2)]$. The answer, $\mathbb{R}\backslash\{1, -2\}$, is all real numbers except for $x = 1$ and $x = -2$, which require dividing by zero. A related problem is to first specify a domain $\mathscr{D}$ and then characterize all functions of a particular type that are defined on $\mathscr{D}$. For instance, we may wish to determine all rational functions (quotients of polynomials) defined on $\mathbb{R}\backslash\{1, -2\}$. Clearly, the denominator polynomial's real roots, if any, must be in the set $\{1, -2\}$. For instance, $(x^2 + 1)/(x + 3)$ is not defined on $\mathbb{R}\backslash\{1, -2\}$, but $(x^2 + 1)/(x^2 + 4)$ is. By specifying a domain we tacitly dismiss certain functions.

This elementary notion suggests a way to examine Sen's conflict between individual rights and societal decisions: first determine the domain required by (ML) and then characterize all mappings (i.e., ways to make group decisions) defined on that domain. The range of each ML-mapping, of course, is society's rankings of the pairs.

For simplicity, start with the preferences of Table 1. As voter one's $\{b, c\}$ ranking is irrelevant for a ML-procedure, it could be $c \succ b$ (to satisfy transitivity), or even $b \succ c$ to make voter one cyclic. Thus, (ML) allows the possibility that, instead of being rational, voter one is primitive, with cyclic preferences! The same possibility holds for voter two: because (ML) ignores the missing $\{a, b\}$ ranking, there is nothing to preclude voter two from having cyclic preferences. As a ML procedure only monitors the ranking of one pair for the remaining voters, it is irrelevant for the procedure whether the other two binary rankings define transitive or cyclic rankings.

To describe the actual domain of a ML mapping, rather than the intended one, let $B(3)$ be the set of all eight possible listings of strict rankings for the three pairs $\{a, b\}$, $\{b, c\}$, $\{a, c\}$; ties are not allowed. So, in addition to the six transitive ways to rank pairs (e.g., $(a \succ b,\ b \succ c,\ a \succ c) \in B(3)$), the set $B(3)$ also includes voters with cyclic preferences (e.g., $(a \succ b,\ b \succ c,\ c \succ a)$). As each voter's preferences come from $B(3)$, the preferences for n voters is in the n-fold Cartesian product of $B(3)$, denoted by $B^n(3)$.

The next proposition states that an element of $B^n(3)$ is a *profile allowed by a ML-procedure*; it lists the admissible ML-choices for each voter. A $B^n(3)$ profile only requires a voter to rank each pair; voters need not sequence these pairwise rankings in a transitive manner. I leave it as an exercise for the reader to prove the following result.

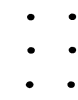
PROPOSITION. *Suppose there are three alternatives $\{a, b, c\}$ where voters one and two are decisive, respectively, over $\{a, b\}$ and $\{b, c\}$. A ML-procedure is defined on $B^n(3)$.*

A ML-procedure, then, can be used by primitive voters who cannot even sequence pairwise rankings. This fact allows us to identify the ML admissible procedures. Namely, just as the domain $\mathbb{R}\backslash\{1, -2\}$ excludes $(x^2 + 1)/(x + 3)$ as an admissible

function, we will find that the $B^n(3)$ domain for ML-methods immediately dismisses most of the commonly used procedures.

To illustrate, consider the Borda Count (see [**3**, **14**] for more details), which tallies each voter's ballot by assigning two, one, and zero points, respectively, to the voter's first, second, and third ranked candidates. The candidates are then ranked according to the sum of assigned points. While the Borda Count is trivial to use with transitive preferences, it is not a ML-procedure because it cannot be used (in this form) by a voter with the cyclic preferences $a \succ b$, $b \succ c$, $c \succ a$. After all, how many points should be assigned to a? Similarly, the widely used plurality vote, where we vote for our top-ranked candidate, is dismissed by (ML) simply because every voter must *have* a top-ranked candidate. More generally, an unintended (ML) consequence is to exclude *all* procedures that can deal only with rational voters! (The domain for such a procedure is a proper subset of $B^n(3)$ rather than the full set.) *What remains are only those procedures acceptable to primitive societies.*

This point is important. Understanding the true domain generated by Sen's axioms makes the source of his problem transparent. To use an analogy, recall the standard puzzle involving nine dots arranged in a square:



The goal is to draw—without lifting the pencil—four straight line segments that pass through all nine points. As long as we believe that the line segments must lie inside the square, this task is impossible. But once we recognize the true domain for the problem (the endpoints of the line segments may lie outside of the square), resolutions are easy to find. Similarly, as long as we believe that the ML-domain requires transitive preferences and that we are considering commonly used methods, Sen's assertion is difficult—probably impossible—to resolve in a simple manner. But once we discover that the true ML-domain includes cyclic preferences and that ML-procedures ignore transitivity, Sen's conclusions become reasonable. After all, if transitivity is not relevant to the input, why should we expect it in the output?

4. A Reinterpretation of Sen

Thus, the desirable, seemingly innocuous condition of minimal liberalism admits only procedures acceptable to "unsophisticated societies." But doesn't axiom (U), which explicitly requires voters to have transitive preferences, retrieve the orderly setting of rational voters? Maybe there is a ML-mapping which becomes sufficiently sophisticated (by avoiding cyclic outcomes) when restricted to transitive preferences? Clearly, such a procedure must be able to differentiate between a sophisticated (transitive preferences) and a primitive (cyclic) society.

To address this issue, notice that a ML-procedure ranks each pair of candidates. As some of the rankings may be ties, extend $B(3)$ by including the ties and denote the new set by $\overline{B(3)}$. For instance, $(a \succ b,\ b \sim c,\ c \succ a)$ is not in $B(3)$ because of the $b \sim c$ ranking, but it is in $\overline{B(3)}$. With this notation, a ML-procedure becomes a mapping

$$F : B^n(3) \to \overline{B(3)}.$$

Axiom (U) restricts the admissible profiles. Namely, if $T(3) \subset B(3)$ represents the transitive preferences, then (U) restricts the ML-procedures to

$$F : T^n(3) \to \overline{B(3)}.$$

To determine whether (U) allows any ML-procedure to avoid cyclic outcomes, we need to identify all ML-mappings that satisfy (P) and have at least the property:

$$F : T^n(3) \to \overline{B(3)} \setminus 18\{(a \succ b, b \succ c, c \succ a), (b \succ a, c \succ b, a \succ c)\}.$$

To analyze the effect of this (U) restriction, notice that because there are more profiles in $B^n(3)$ than admissible outcomes, each mapping is many-to-one—all profiles in each level set generate the same societal ranking.

DEFINITION. Two profiles $\mathbf{p}_1, \mathbf{p}_2 \in B^n(3)$ are *ML-equivalent*, denoted by $\mathbf{p}_1 \sim_{ML} \mathbf{p}_2$, if differences in voters' binary rankings occur only for voter one in the $\{b, c\}$ ranking, for voter two in the $\{a, b\}$ ranking, and for any other voters in the $\{a, b\}$ and/or $\{b, c\}$ rankings.

Two profiles, then, are equivalent if and only if a ML-procedure cannot distinguish between them. Clearly, $\sim_{ML}$ is an equivalence relation partitioning the domain $B^n(3)$ into equivalence classes. To prove the following theorem, which asserts that each equivalence class has an entry in $T^n(3)$, the reader can mimic what was done with Table 1 by filling in blanks to create transitive *and* cyclic preferences.

THEOREM 2. *The equivalence classes defined by* $\sim_{ML}$ *partition* $B^n(3)$. *Each equivalence class has* 4^{n-1} *profiles; at least one of these profiles has all transitive voters and at least one other profile has all cyclic voters.*

As each equivalence class contains a transitive profile, the (U) constraint does not eliminate any equivalence class from the domain. But as the outcome of a ML admissible procedure is strictly determined by the equivalence class (the procedure cannot distinguish between profiles in the same class), a ML-method cannot detect any change in the domain. Thus, the (U) restriction is useless because it makes no difference for a ML-procedure; the image of F restricted to $T^n(3)$ is the same as that of F on $B^n(3)$. Stated more simply, because a ML-procedure must service unsophisticated voters, we cannot expect it to recognize rational preferences.

Armed with this knowledge, we can easily construct Sen-type examples. For instance, start with the cyclic profile $\mathbf{p}_c$ where everyone has the rankings $b \succ a$, $c \succ b$, $a \succ c$. According to unanimity condition (P), the only fair societal ranking is this cycle. But Theorem 2 ensures there are transitive profiles that are ML-indistinguishable from $\mathbf{p}_c$; both profiles have the same cyclic outcome. To construct one of these transitive profiles, first list the $\mathbf{p}_c$ binary rankings recognized by a ML method.

Voter	Choice $\{a, b\}$	$\{b, c\}$	$\{a, c\}$
1	$b \succ a$	—	$a \succ c$
2	—	$c \succ b$	$a \succ c$
Others	—	—	$a \succ c$

Next, find an indistinguishable transitive profile by appropriately filling in the blanks. Notice, the entries of this table are identical to Table 1. Consequently, one choice of a transitive profile is where voter one has preferences $b \succ a \succ c$ while all other voters have the preferences $a \succ c \succ b$. Both the cyclic and the transitive profiles provide identical information for ML-procedures.

Theorem 2 describes the situation with $k = 3$ candidates. Extensions to larger k values follow in much the same way. To find the ML-domain, start with $T^n(k)$, the set

of k-candidate, binary, transitive rankings for n voters. For each pair assigned to a decisive voter, alter the other voters' binary ranking in all possible ways to define the actual (rather than the intended) domain for ML-procedures. The rest of the proof of an extension of Theorem 2 follows in the same manner.

Once k exceeds 3, the added number of pairs allows for highly imaginative situations. For instance, Salles **[17]** develops a clever setting for $k = 4$ where, by appealing to the arguments of Hammond **[8]**, Salles constructs a natural setting where each of two voters is decisive over two pairs. He then finds a transitive profile that generates two different cycles! The reader may wish to construct other examples to illustrate the even more bizarre behavior that is possible if $k \geq 5$. (Start with primitive voter profiles where the outcome is obvious; then replace the original profile with a ML-indistinguishable transitive profile.) In all settings, the cycles are "fair" outcomes for a "primitive" profile that is ML-indistinguishable from the constructed transitive profile.

5. Arrow's Theorem

The subtle cause of Sen's problem explains all sorts of complexities in our daily life. To illustrate, suppose an organization is to elect Ann, Becky, or Claire as their new Chair, where the voters have the following rankings:

Number	Preferences
31	$A \succ C \succ B$
30	$B \succ C \succ A$
3	$C \succ B \succ A$

The plurality outcome, where a voter votes for his top-ranked candidate, is $A \succ B \succ C$, with the tally 31 : 30 : 3. Our familiarity with this commonly used system makes it easy to misinterpret the result. For instance, it seems obvious from Claire's poor showing that these voters strongly prefer Ann to Claire. They do not; their pairwise ranking is $C \succ A$, with a 33 : 31 tally! Indeed, in continued defiance of the plurality outcome, these voters also prefer C to B and B to A!

This example underscores a serious flaw of the plurality vote; it recognizes only a voter's top-ranked candidate. Totally dismissed is any information about a voter's relative ranking of each pair. Once this lost information is reclaimed, we discover that most voters prefer Claire to either alternative. This suggests replacing the plurality method with procedures that utilize this valuable data coming from pairwise comparisons. Maybe a reform procedure should satisfy the following axiom:

(IIA) *Independence of Irrelevant Alternatives.* Society's relative ranking of a pair is determined only by the voters' relative ranking of this pair.

It may seem easy to find many such reasonable procedures, but only one exists. This is the content of "Arrow's Impossibility Theorem," one of the most widely-quoted results in the social sciences.

THEOREM (ARROW **[1]**). *Suppose there are at least three candidates, at least two voters, and that all voters have transitive preferences. If a procedure satisfies* (U), (P), *and* (IIA), *and always has transitive outcomes, then one of the voters is a "dictator"* (*societal outcome always agrees with the dictator's preferences*).

It is not uncommon to find Draconian interpretations of this important assertion, descriptions that exploit the fearful image of dictatorships. Such interpretations are irresponsible: the theorem states only that it is impossible to invent a procedure where the pairwise and general rankings always agree. The real issue is to understand why.

The problem can be addressed in the same manner used to analyze Sen's assertion: first find the domain for the functions satisfying (IIA), and then find the procedures admitted by this domain. The explanation (see **[12, 14, 16]** for more details) is that, unintentionally, (IIA) dismisses all information reflecting the crucial assumption that the voters are rational! For intuition why this is so, suppose in the earlier "apple, blueberry, and cherry pie" illustration, we learn that a person prefers b to a. Does this person have cyclic or transitive preferences? Such a question is impossible to answer because transitivity involves the sequencing of *all* pairs. Axiom (IIA), however, specifically requires a procedure to consider only each voter's relative ranking of each pair. Consequently, (IIA) dismisses all sequencing information concerning the rationality of voters. As true with Sen's theorem, if a procedure devalues information about the rationality of inputs, we cannot expect rationality in the conclusions.

While a result paralleling Theorem 2 is more difficult to prove, it asserts that a IIA-procedure admits indistinguishable transitive and non-transitive profiles. As in Section 4, this assertion follows by determining whether (U) allows some procedure to distinguish between transitive and primitive preferences. This means that when the pairwise parts from transitive preferences are separated, the procedure can reconstruct them only in a transitive manner. Here we have a positive answer; if a procedure pays attention only to the preferences of one voter—the dictator—this always happens. However, once the preferences of least two voters are needed, no procedure can distinguish between the transitive and non-transitive rankings. Again, if a procedure does not recognize whether the inputs are rational, we cannot expect transitive outputs. Moreover, the non-transitive outcome of a procedure can be interpreted as "fairly" representing the nonexistent profile of voters with cyclic preferences.

Let me illustrate this unexpected assertion with the pairwise vote. It is easy to show that the pairwise vote satisfies (U), (IIA), and (P), and its outcomes cannot be determined by a dictator. Therefore, we know from Arrow's Theorem that not all of the outcomes are transitive. To create an example, consider the three-voter *Condorcet profile* (the subscripts on the pairwise rankings will be explained later):

Preferences	$\{a, b\}$ ranking	$\{b, c\}$ ranking	$\{a, c\}$ ranking
$a \succ b \succ c$	$(a \succ b)_1$	$(b \succ c)_2$	$(a \succ c)_3$
$b \succ c \succ a$	$(b \succ a)_3$	$(b \succ c)_1$	$(c \succ a)_2$
$c \succ a \succ b$	$(a \succ b)_2$	$(c \succ b)_3$	$(c \succ a)_1$
Outcome	$a \succ b$	$b \succ c$	$c \succ a$

In this table, each voter is assigned a row; the voter's preferences are in the left column. The other entries of the row specify the voter's relative ranking for each pair of candidates. By listing these pairwise rankings in columns identified with the pairs, each pair's majority vote tally is determined by the number of times a candidate is preferred in the three entries of the appropriate column. This defines *cyclic* pairwise election outcomes $a \succ b$, $b \succ c$, $c \succ a$, where the tally for each election is 2 : 1.

To justify my assertion about Arrow's Theorem, I must display a cyclic profile which the pairwise vote finds indistinguishable from the Condorcet profile and where the

cyclic outcome is "fair." To do so, notice that the pairwise vote respects anonymity; it cannot determine who cast what vote. So, by permuting the three entries of each column in any manner, I define other profiles that the pairwise vote finds indistinguishable from the Condorcet profile. In particular, the pairwise voting procedure cannot distinguish the Condorcet profile from the *primitive voter profile* where the preferences of voter j are identified by the subscript j.

Consequently, as far as the pairwise vote is concerned, the "true" profile could be where primitive voters one and two have the cyclic preferences $\mathscr{A} = \{a \succ b,\ b \succ c,\ c \succ a\}$ while primitive voter three has the reversed cyclic preferences $\mathscr{A}^c = \{b \succ a,\ c \succ b,\ a \succ c\}$. This possibility defines a single-issue situation where two voters believe in $\mathscr{A}$ while the last voter disagrees. The only "fair" outcome for this reconstructed profile is $\mathscr{A}$ by a 2:1 vote—it is the cycle. This "fair outcome" must hold for all profiles constructed from these binary rankings. (For more details, see **[12, 14]**.)

This example not only illustrates how (IIA) vitiates the critical assumption that voters have transitive preferences, but also raises doubts about any procedure based on pairwise rankings. After all, if the restricted information used by the pairwise vote drops the assumption that voters are transitive, then why should we expect rational outcomes? This concern extends to all procedures using the pairwise vote, such as tournaments or even an agenda for a meeting which specifies an order to sequentially vote upon pairs of alternatives.

Armed with this insight, the reader can identify other examples, coming from choice theory, economics, and elsewhere, from which we should expect disturbing outcomes. The true message is to expect trouble whenever the actual (rather than intended) domain for a procedure admits nontransitive preferences.

6. Resolutions

By understanding the source of Sen's and Arrow's results, we can not only entertain hope for resolutions, but also understand why certain approaches have failed—miserably. For instance, a widely used approach in choice theory is to further restrict the profiles. This approach, however, misses the point. While stronger profile restrictions may circumvent Sen's, Arrow's, and related problems, they fail to provide interesting answers. This is because the admitted procedures are appalling to the standards of democracy. (This is illustrated by the quasi-dictatorial, highly stilted procedures required by the results in **[7, 9, 10, 11, 14]**.) Remember, the real damage is caused because (ML) and (IIA) exclude reasonable procedures while retaining only those that are crude enough to be used by primitive societies. But when restricted to crude procedures, we cannot expect sophisticated outcomes. If our building tools are limited to sticks and stones, don't expect to construct a modern 100-story skyscraper.

A realistic resolution is more challenging and constructive. As we discovered, axioms exclude procedures. In particular, we learned from Sen's and Arrow's choices of (ML) and (IIA) that even appealing axioms can be useless if they exclude reasonable procedures. We need, then, to achieve a balance between the choice of the axioms used to model a desired situation and the kinds of procedures they admit.

As this explanation of Arrow's and Sen's theorems provides new tools and directions to resolve Arrow's and Sen's concerns, I encourage the reader to explore these issues. To do so, remember that the cost of separately determining societal rankings for subsets of alternatives is to, inadvertently, admit non-transitive preferences. Thus, new axioms should promote connections among these sets. For instance, instead of examining only the pairwise rankings, maybe we should sum the tallies of each

candidate over all pairwise elections. (See [**12**, **13**, **14**].) This change sufficiently relaxes Arrow's (IIA) condition to admit reasonable procedures such as the Borda Count. (While this procedure allows the cyclic voter to cast ballots, I leave it to the reader to show that this version of the Borda Count effectively discards these ballots as they amount to a complete tie.)

An alternative direction is to recognize that Sen's axiom (ML) separates the decisions for certain pairs, while (P) insists on connections. By correcting this incompatibility, resolutions follow. For instance, if society grants me the right to choose my shirt, why are others comparing one of my alternatives with other alternatives? This suggests relaxing (P) to the following axiom:

(P*) *Relaxed Pareto.* If an individual is given decisive rights over a pair $\{a, b\}$, then the Pareto condition (P) does not apply to any pair including either a or b.

It is easy to construct procedures satisfying (P*), (ML), and (U) where the outcomes are transitive. Rather than proposing procedures, I advance this axiom to illustrate how to use this new structure to generate resolutions.

Acknowledgment This research was supported, in part, by an NSF Grant and a Pancoe Professorship. I started this paper during my 1995 visit to CREME, Université de Caen, Caen, France. My thanks to my host, Maurice Salles, for the many kindnesses he extended during my visit. I have benefited from comments of participants of several workshops and seminars where these results have been presented. Also, my thanks to S. Brams, K. Mount, V. Merlin, N. E. Sahlin, M. Salles, P. Straffin, P. Zorn, and an anonymous referee for suggestions.

REFERENCES

1. K. J. Arrow, *Individual Values and Social Choice*, John Wiley & Sons, New York, NY, 1951 (2nd ed., 1963).
2. D. Black, *The Theory of Committees and Elections*, Cambridge University Press, Cambridge, UK, 1958.
3. J. C. Borda, Memoire sur les elections au Scrutin, *Histoire de l'Academie Royale des Sciences*, 1781.
4. W. W. Funkenbusch and D. G. Saari, Preferences among preferences or nested cyclic stochastic inequalities, *Congressus Numerantium* 39 (1983), 419–432.
5. W. Gaertner, P. K. Pattanaik, and K. Suzumura, Individual rights revisited, *Economica* 59 (1992), 161–177.
6. A. Gibbard, Intransitive social indifference and the Arrow dilemma, mimeographed notes, 1969.
7. A. Gibbard, A. Hylland, and J. A. Weymark, Arrow's theorem with a fixed feasible alternative, *Soc. Choice Welfare* 4 (1987), 105–115.
8. P. J. Hammond, Liberalism, independent rights, and the Pareto principle, in *Logic, Methodology and the Philosophy of Social Science*, L. J. Cohen, et al., eds, conference proceedings, Amsterdam, 1982, 607–620.
9. E. Kalai and E. Muller, Characterization of domains admitting nondictatorial social welfare functions and nonmanipulable voting procedures, *JET* 16 (1980), 457–469.
10. E. Kalai and Z. Ritz, Characterizations of the private alternatives domains admitting Arrow social welfare functions, *JET* 22 (1979), 457–469.
11. D. G. Saari, Calculus and extensions of Arrow's Theorem, *Jour. Math. Econ.* 20 (1991), 271–306.
12. D. G. Saari, *Geometry of Voting*, Springer-Verlag, New York, NY, 1994.
13. D. G. Saari, Inner consistency or not inner consistency; a reformulation is the answer, in *Social Choice, Welfare, and Ethics*, W. Barnett, H. Moulin, M. Salles, and N. Schofield, eds., Cambridge University Press, Cambridge, UK, 1995.
14. D. G. Saari, *Basic Geometry of Voting*, Springer-Verlag, New York, NY, 1995.
15. D. G. Saari, Mathematical complexity of simple economics, *AMS Notices* 42 (1995), 222–230.
16. D. G. Saari, Connecting and resolving Sen's and Arrow's theorems, to appear in *Social Choice & Welfare*.
17. M. Salles, Rights, permission, obligation: Comments on Prasanta K. Pattanaik, "On modelling individual rights: Some conceptual issues," draft paper, *CREME*, 1994.
18. A. Sen, The impossibility of a paretian liberal, *Jour. of Political Economy* 78 (1970), 152–157.
19. A. Sen, *Collective Choice and Social Welfare*, Holden-Day, San Francisco, CA, 1970.

Variations on an Irrational Theme —Geometry, Dynamics, Algebra

DAN KALMAN
American University
Washington, DC 20016

ROBERT MENA
California State University
Long Beach, CA 90840

SHAHRIAR SHAHRIARI
Pomona College
Claremont, CA 91711

If someone mentions *irrational number*, what do you think of? Perhaps you recall a standard example, $\sqrt{2}$, and a proof by contradiction that has to do with odd and even numbers. Or perhaps what comes to mind is that the Pythagoreans were discomfitted by the irrationality of $\sqrt{2}$ because it proved that not all geometric relationships could be described in terms of whole numbers. In this paper we will touch on both of these aspects of irrationality, recounting a bit of the history, and showing some variations on the traditional approaches to these topics. Although the subject is a familiar one, it is rich in interesting ideas. The purpose of this paper is to popularize some irrational ideas that do not appear to be well known, including connections to eigenvalues and dynamical systems, and to bring them together with some of the ideas that are so familiar.

Incommensurability and Infinite Descent

The Pythagoreans encountered the idea of irrationality in geometry in the context of commensurability. Initially, in harmony with their *all is number* doctrine, they embraced the geometric position that any two segments are commensurable, meaning, exactly measurable with a common unit. In modern terms, that would mean that relative to an arbitrary unit of measurement, every segment has rational length. Of course that is false, and the very notion seems quaint to our ears. But it was an unexpected discovery to the Greeks, and had fundamental mathematical and philosophical ramifications. According to one oft-repeated account, the demonstration of the existence of incommensurable segments was so devastating that the bearer of the bad news was put to death for his discovery.[1]

To understand the importance of commensurability to the Pythagoreans, one must bear in mind their reliance on whole number relationships. In particular, the concept of proportion was formulated in integral terms: the fundamental observation is that $a:b$ and $na:nb$ are in equal proportion. Then clearly $ma:mb$ and $na:nb$ are also equal. In geometry, with the quantities ma and na representing line segments, the common divisor a becomes a common unit of measurement.

[1]As retold by Choike [**4**], the discoverer, Hippasus of Metapontum, was on a voyage at the time, and his fellows cast him overboard. A more restrained discussion by Boyer [**2**, pp. 71–72] describes both the discovery by Hippasus and his execution by drowning as mere possibilities.

Proportionality of Similar Triangles As a concrete example of this idea, we will derive the proportionality of the corresponding parts of similar triangles, following the approach of Aaboe [**1**, pp. 42–43]. Let ABC and $A'B'C'$ be triangles whose corresponding angles are equal, and suppose that BC and $B'C'$ are measured by the common unit a. Then for some integers n and m, $BC = ma$ and $B'C' = na$, as illustrated in FIGURE 1.

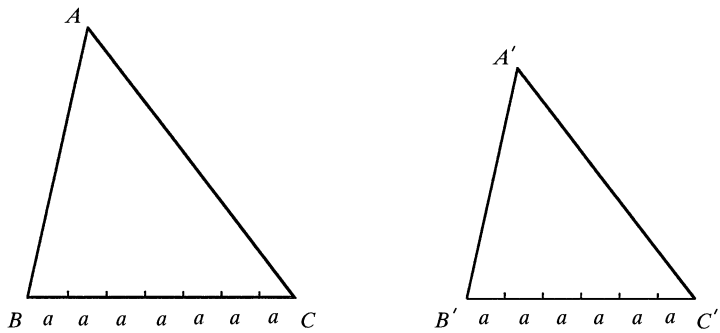


FIGURE 1
Triangles with commensurable bases

Focusing on ABC for a moment, observe that the subdivision of BC into m equal segments permits us also to subdivide AC into m equal segments: simply construct parallel lines as shown in FIGURE 2.

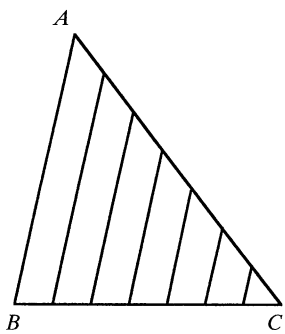


FIGURE 2
Subdividing AC

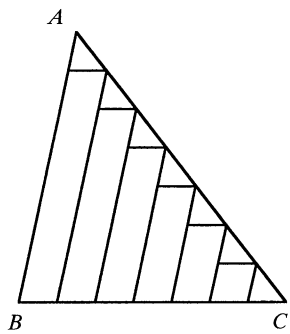


FIGURE 3
Parallelograms

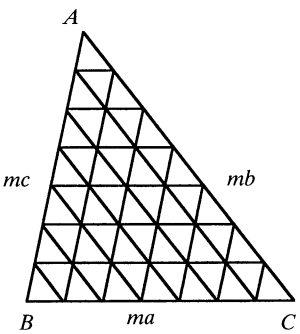


FIGURE 4
ABC Tiled

The intersections of these parallel lines with AC are equally spaced along that side. This can be seen by constructing line segments parallel to BC as in FIGURE 3. Each segment has length a, because it completes a parallelogram with base of length a along BC. That makes the triangles lying along AC congruent, and so verifies that their sides on AC are all of equal length, say b.

And now with two sides of the triangle subdivided, we can partition the remaining side into m equal parts of length c in two ways, using lines parallel to either AC or BC. The result is actually a tiling of ABC by congruent triangles, with m tiles along each side (FIGURE 4). In each tile, the sides are a, b, and c. Thus $AB = mc$ and $AC = mb$.

The same construction carried out in $A'B'C'$ results in a tiling with n copies of the tile along each side (FIGURE 5). Moreover, the tiles used in each triangle are congruent. By construction they clearly share equal corresponding angles, as well as one side, a. This leads to $A'B' = nc$ and $A'C' = nb$, and proves that the sides of the triangles are in equal proportion. For example, $BC : B'C' = ma : na = mb : nb = AC : A'C'$.

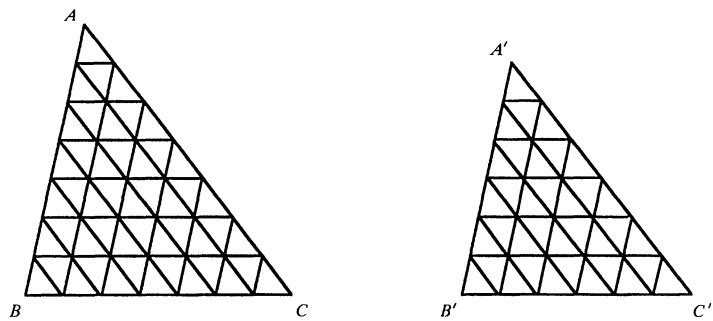


FIGURE 5
Tiled Triangles

If it is assumed that all pairs of segments are commensurable, this argument establishes the proportionality of similar triangles. More generally, the presumption of commensurability justifies treating all proportions as ratios of integers. The discovery of incommensurable segments revealed a fundamental flaw in this approach to proportionality, and led ultimately to the much more sophisticated formulation that appears in Book V of Euclid.

Infinite Descent No one really knows how incommensurability was first discovered. In **[4]**, there is a retelling of the suggestion of von Fritz **[9]** that the pentagram was the first geometric figure shown to have incommensurable parts. The argument given there uses the idea of infinite descent. Starting with an initial figure, we construct another similar figure that is demonstrably smaller in size. Two parts of the original figure are assumed to be measurable with a common unit, and then it is shown that this same unit must measure the corresponding parts of the smaller figure. By repeating the construction, we can eventually reduce the figure so far that the diameter is less than the common unit, whereupon we contradict the fact that this unit must measure two sides of the figure. In **[4]** this argument is made using a pentagram. Here we will give a somewhat simpler construction starting with an isosceles right triangle. An essentially equivalent construction, working in a square, is presented in **[3]**.

Consider FIGURE 6, showing an isosceles right triangle ABC. The point D has been constructed so that $BD = BC$. Through D we draw a line parallel to leg AC, which meets BC at point E. Now construct a square having CE as one side (see FIGURE 7), thus defining points F and G.

For reference, we have drawn the auxiliary lines CG and CD in FIGURE 8. Observe now that CG and GD have equal length. Indeed, with BC and BD equal (by the construction of D), we know that angles DCB and CDB are equal. Also angles GCE and GDB are equal (and each is half a right angle). Thus, triangle CDG is isosceles, with CG and GD equal, as asserted. To complete the construction, add point H to define a parallelogram $ADGH$ (FIGURE 9). Then triangles FGH and FGC are congruent, so that CG and GH are equal. Combined with the earlier result, this shows that all sides of parallelogram $ADGH$ are equal to CG.

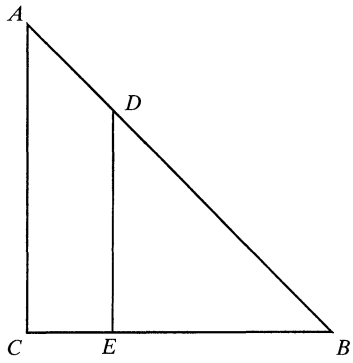


FIGURE 6
Isosceles right triangle

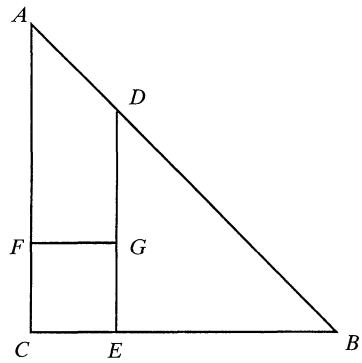


FIGURE 7
CEGF is a square

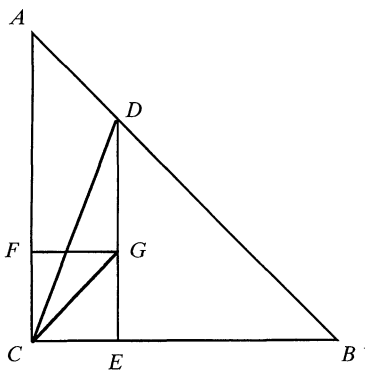


FIGURE 8
Triangles *BCD* and *GCD* are isosceles

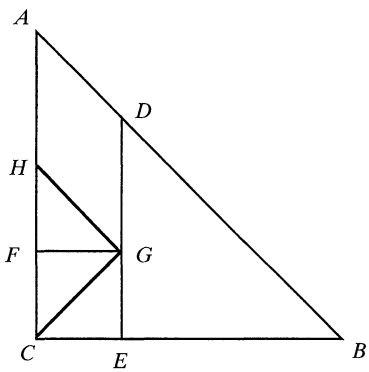


FIGURE 9
ADGH is a parallelogram

To summarize the result of the construction, FIGURE 10 shows the essential segments, with *AH*, *AD*, *HG*, and *GC* all equal in length. Triangle *CGH* is an isosceles right triangle. If a unit evenly measures *BC* and *AB*, then it must also measure their difference, *AD*. The unit therefore measures legs *HG* and *CG* of *CGH*. Furthermore, since the unit measures both *AC* and *AH*, it measures their difference, *CH*, the hypotenuse of *CGH*. Therefore, any unit that measures the parts

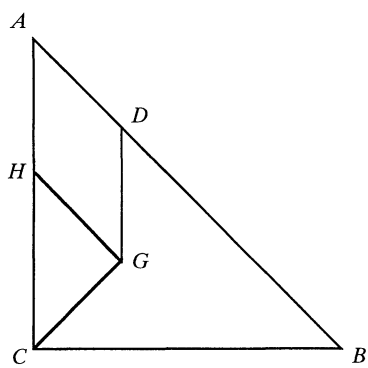


FIGURE 10
A unit measuring *AB* and *BC* also measures *CG* and *CH*

of triangle ABC must also measure the parts of the smaller similar triangle CGH. This completes the construction. The incommensurability of AB and BC now follows as discussed earlier.

The incommensurability argument also leads to an algebraic demonstration of the irrationality of $\sqrt{2}$. Assume that there is a unit that divides evenly into the leg and the hypotenuse of the original triangle, say with n units along AB and m on BC. Then AD must be measured by $n - m$ units, as must AH, GH, and GC. Furthermore, HC is then measured by $m - (n - m) = 2m - n$ units. Since CHG and ABC are similar triangles, we conclude that $n/m = (2m - n)/(n - m)$. This same conclusion can be reached using algebra. Suppose that a and b satisfy $a^2 = 2b^2$. Then $a^2 - ab = 2b^2 - ab$ hence $a(a - b) = b(2b - a)$. This leads to our earlier conclusion: $a/b = (2b - a)/(a - b)$. Now since $b < a$, we see that $2b - a < a$. Since $a < 2b$, $a - b < b$. That is, the numerator and denominator of $(2b - a)/(a - b)$ are each less than the corresponding parts of a/b. The conclusion is summarized as follows: Any ratio a/b representing $\sqrt{2}$ leads to another ratio with strictly smaller numerator and denominator. If a and b are integers, so are $2b - a$ and $a - b$. Thus, given any integer ratio for $\sqrt{2}$ we obtain an equal ratio of strictly smaller integers. This is clearly an impossible situation, so $\sqrt{2}$ must have no such representation.

The preceding argument appears in [**10**, pp. 39–41]. It is essentially the same as one used by Fermat to argue the irrationality of $\sqrt{3}$ (see [**2**, pp. 353–354]). Fermat went on to make great use of the notion of infinite descent in number theory. In contrast, our discourse now heads in a different direction—to the use of matrices.

A Dynamical View of Irrationality

One facet that both the algebraic and geometric infinite descent arguments share is the propagation of pairs (a, b). Indeed, the generation of each new pair from its predecessor is of a linear nature. It is natural therefore to represent it as a matrix operation. Let A be the matrix $\begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix}$, and represent the pair (a, b) as a column vector. Then

$$\begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 2b - a \\ a - b \end{bmatrix}$$

describes the propagation used in our earlier arguments. Now we make two observations about A. First, as an integer matrix, it preserves lattice points. That is, if v is a vector with integer components, then so is Av. Second, the line L described by $a = \sqrt{2}b$ is an eigenspace, so its points are also preserved by A. Actually we can say more: A is a contraction on L. Simply observe that

$$\begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \sqrt{2} \\ 1 \end{bmatrix} = \begin{bmatrix} 2 - \sqrt{2} \\ \sqrt{2} - 1 \end{bmatrix} = \begin{bmatrix} \sqrt{2}(\sqrt{2} - 1) \\ \sqrt{2} - 1 \end{bmatrix} = (\sqrt{2} - 1) \begin{bmatrix} \sqrt{2} \\ 1 \end{bmatrix}$$

Since the eigenvalue $\sqrt{2} - 1$ is between 0 and 1, the effect of A on points of L is to reduce their magnitude.

The infinite descent argument can now be stated in dynamical terms. Starting with any first quadrant point (a, b) on L, repeated application of A generates a sequence of points that remain on the line while converging to 0. If the initial point were a lattice point, all of the successive points would be as well, leading us to the impossible situation of an infinite sequence of distinct lattice points converging to the origin. We conclude that there are no lattice points on L.

Dynamics of A and A^{-1} There is a bigger dynamical picture. Although there are no lattice points on L, there are plenty elsewhere in the plane. Repeated application of A to each must generate a sequence of lattice points, called an *orbit*. Where do these orbits lead? It is easy to show that A has another eigenvalue with magnitude greater than 1, and a corresponding line M of eigenvectors. Each element of the plane can be expressed as a sum of elements of L and M. Under repeated application of A, the L component dwindles away to nothing, while the M component grows without bound. Therefore, almost all of the points in the plane, including every one of the lattice points, march off to infinity under the action of A. This is the dynamical systems view of A. Its repeated application to the plane sweeps everything not on L out to infinity along M, while the points on L all flow toward the origin. In combination with the fact that A preserves integer lattice points, this shows that L can contain no lattice points other than 0.

Somewhat paradoxically, although the dynamic description is given in very geometric terms, it is not easy to depict accurately on a graph. For one thing, the eigenvalue corresponding to M is negative. As A is repeatedly applied to a vector, the M component alternates in sign. The resulting orbit jumps back and forth, progressing in one direction along M on the even jumps, and in the opposite direction on the odd jumps. So "marching to infinity" is not really the right image. Rather, the points leap-frog infinitely far along M in both directions. Looking just at the landing points of the even leaps, the points seem to follow a flow, as illustrated qualitatively in FIGURE 11. This really shows the dynamic behavior of A^2. It gives some sense of the dynamics of A, as long as you remember what is happening on the odd leaps.

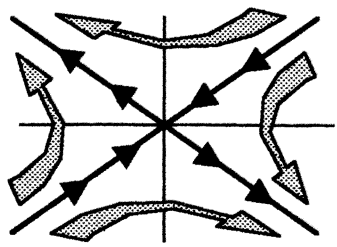


FIGURE 11
Dynamics of A^2

The magnitude of the negative eigenvalue presents another obstacle to forming an accurate graphical representation of the dynamics of A. Except for points very close to L, the M component grows so rapidly that the L component becomes completely invisible after only one or two iterations. That is, if the scale is made large enough to show an initial point and two iterates, relative to that scale, even the initial L component will be hard to see. This effect is illustrated in FIGURE 12, which shows a square, and its images under A and A^2. The second image is hard to distinguish from a heavily inked line. Careful inspection reveals the effects of the negative eigenvalue, as the labeled vertices alternate orientation around the square and its successive images. However, with only two applications of A illustrated, there is not much of a basis for visualizing the overall structure of the orbits. In fact, the situation is more easily described than drawn. From just about any starting point, the orbit takes only a step or two to get right next to M. From that point on, the orbit jumps off to infinity, alternating between one end of M and the other.

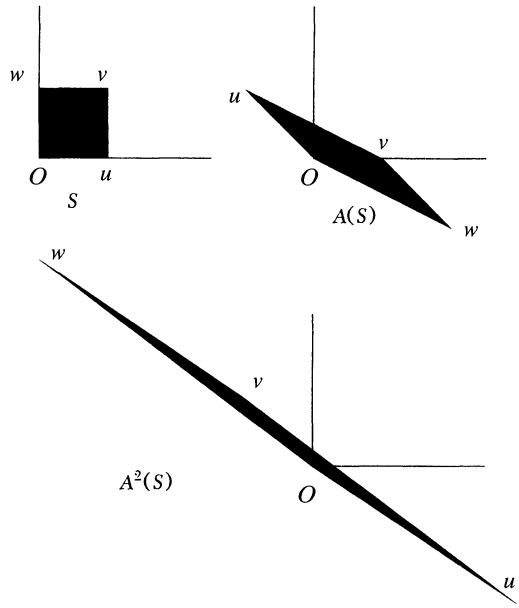


FIGURE 12
Applications of A to a square S

As stated earlier, A carries each lattice point to another lattice point. As a matter of fact, the set of lattice points is actually invariant under A, because the inverse $\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$ also has integer entries. The dynamics of A^{-1} are the reverse of those of A: all the points off M are swept out to infinity along L, while points on M collapse into the origin. Reasoning exactly as before, M can contain no lattice points. Therefore, under the action of A^{-1}, every lattice point generates a sequence that asymptotically approaches L. This provides a simple way to generate rational approximations to $\sqrt{2}$. Begin with a lattice point $\begin{bmatrix} a \\ b \end{bmatrix}$ and repeatedly apply A^{-1}. Since the resulting sequence of points $\begin{bmatrix} a_n \\ b_n \end{bmatrix}$ approaches L, the ratios a_n/b_n converge to $\sqrt{2}$. For example, starting with $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ we generate the sequence

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 3 \\ 2 \end{bmatrix} \quad \begin{bmatrix} 7 \\ 5 \end{bmatrix} \quad \begin{bmatrix} 17 \\ 12 \end{bmatrix}$$

$$\begin{bmatrix} 41 \\ 29 \end{bmatrix} \quad \begin{bmatrix} 99 \\ 70 \end{bmatrix} \quad \begin{bmatrix} 239 \\ 169 \end{bmatrix} \quad \begin{bmatrix} 577 \\ 408 \end{bmatrix} \quad \begin{bmatrix} 1393 \\ 985 \end{bmatrix}$$

$$\begin{bmatrix} 3363 \\ 2378 \end{bmatrix} \quad \begin{bmatrix} 8119 \\ 5741 \end{bmatrix} \quad \begin{bmatrix} 19601 \\ 13860 \end{bmatrix} \quad \begin{bmatrix} 47321 \\ 33461 \end{bmatrix} \quad \begin{bmatrix} 114243 \\ 80782 \end{bmatrix}$$

The last pair shown approximates $\sqrt{2}$ as $114243/80782$. Squaring the numerator and denominator we find that $114243^2 = 13051463049 = 13051463048 + 1 = 2 \cdot 80782^2 + 1$ so the ratio is indeed very close to $\sqrt{2}$. This same sequence of rational approximations was presented in [**10**, pp. 39–41], derived by an approach closely related to ours, but without using matrices. The sequence also appears in [**8**]. There, a quite different (and very interesting) scheme is used to find rational approximations to $\sqrt{2}$.

Generalizations

The foregoing matrix approach can be generalized in several ways. First we will consider square roots of integers other than 2. Then we will look at the more general case of rational roots of polynomials with coefficients that are either integers, or Gaussian integers. Finally, we generalize from roots (which correspond to linear factors) to the more general question of factorization, as described by Gauss's Lemma.

To begin, let us see how the preceding dynamical discussion of the irrationality of $\sqrt{2}$ generalizes to $\sqrt{n}$. In place of A take the matrix $\begin{bmatrix} -k & n \\ 1 & -k \end{bmatrix}$, and everything works as before. One eigenvalue is $\sqrt{n} - k$ and the corresponding line L of eigenvectors is spanned by $\begin{bmatrix} \sqrt{n} \\ 1 \end{bmatrix}$. The other eigenvalue is $-(k + \sqrt{n})$ with the corresponding line M spanned by $\begin{bmatrix} \sqrt{n} \\ -1 \end{bmatrix}$. In order to obtain the same dynamic behavior as before, we require the first eigenvalue to have magnitude less than 1. We can achieve this by taking k to be the greatest integer in $\sqrt{n}$. In the special case that n is a perfect square, this results in an eigenvalue of 0. Then there *are* lattice points on the line L, but they are all mapped by A to 0 in a single jump. In any other case, that is, if n is not a perfect square, we see that there are no lattice points on L, and deduce that $\sqrt{n}$ is irrational, as before. We have therefore shown that an integer is either a perfect square or has an irrational square root.

One way to view the choice of k in the preceding is as follows: we have a matrix with an eigenvalue that may be larger than 1. By subtracting an integer multiple of the identity matrix, we can translate the eigenvalues to obtain a positive eigenvalue less than 1. This idea leads to a proof of the well known, more general result that a monic polynomial with integer coefficients has real roots that are either integers or irrational. Before proving this result, we need two lemmas. The first allows us to treat a general polynomial in the context of matrix algebra, while the second assures us the equivalent of lattice points as eigenvectors.

LEMMA 1. *Every monic polynomial with integer coefficients is the characteristic polynomial of an integer matrix.*

Proof: The proof is constructive. If the polynomial is $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ then it is the characteristic polynomial of the so-called *companion matrix* (see [5], for instance).

$$C = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-1} \end{bmatrix}$$

It is easy to verify that this matrix has the desired characteristic polynomial by expanding the determinant of $(C - \lambda I)$ in the first column and using induction. Additional insight comes from observing that if α is a root of p, then $[1 \ \alpha \ \alpha^2 \ \cdots \ \alpha^{n-1}]^T$ is an eigenvector of C with eigenvalue α. This fact is easily verified by a direct calculation.

LEMMA 2. *Let A be an integer matrix with rational eigenvalue λ. Then there exists an integer eigenvector u.*

Proof: The matrix $A - \lambda I$ has determinant 0. Therefore, over the field of rationals, it has a nontrivial null space. A nonzero vector in that null space has rational entries, and so a suitable integer multiple will have integer entries. The result is an integer eigenvector u for A and λ.

We state the generalization of the argument concerning $\sqrt{n}$ as follows:

THEOREM 1. *A real eigenvalue of an integer matrix is either an integer or irrational.*

Proof: Proceed by contradiction. Let λ be a rational eigenvalue of the integer matrix A, and assume that λ is not an integer. Without loss, we may assume that $0 < \lambda < 1$, for if not, simply replace A with $A - \lfloor \lambda \rfloor I$. ($\lfloor \cdot \rfloor$ is the greatest-integer function.) The second lemma shows that there is an integer eigenvector u corresponding to λ. If we apply A to u repeatedly, we generate an infinite sequence of distinct integer vectors that converges to 0. This is clearly impossible. Therefore, every rational eigenvalue of A must actually be an integer.

Complex Roots Combined with the first lemma, Theorem 1 shows that for a monic polynomial with integer coefficients any real roots are either integer or irrational. What about the complex roots? To simplify the discussion of the complex case, it will help to use the notation $\mathbb{Z}$ for the integers, and $\mathbb{Z}[i]$ for the Gaussian integers, that is, complex numbers with real and imaginary parts in $\mathbb{Z}$. Similarly, we will denote by $\mathbb{Q}$ the rational numbers, and, by $\mathbb{Q}[i]$, the complex numbers with rational real and imaginary parts. Now let us return to the question of complex roots. If a monic polynomial with integer coefficients has a root in $\mathbb{Q}[i]$, must that root actually lie in $\mathbb{Z}[i]$? The answer is yes, and the argument is essentially the same as what has gone before. Instead of matrices with entries in $\mathbb{Z}$, we consider matrices whose entries are in $\mathbb{Z}[i]$. It is easy to modify the lemmas given earlier to apply to this new situation. First show that every monic polynomial with coefficients in $\mathbb{Z}[i]$ is the characteristic polynomial of a matrix with entries in $\mathbb{Z}[i]$. Then show that when such a matrix has an eigenvalue in $\mathbb{Q}[i]$, it has an eigenvector with entries in $\mathbb{Z}[i]$, as well. Finally, prove that for a Gaussian integer matrix, an eigenvalue in $\mathbb{Q}[i]$ must actually be in $\mathbb{Z}[i]$. As before, it may be assumed without loss of generality that the eigenvalue has magnitude less than 1, this time translating by the nearest Gaussian integer, if necessary. The argument concludes just as before.

Gauss's Lemma All the foregoing results about roots of polynomials can evidently be formulated in terms of linear factors, instead. Thus, if a monic polynomial with integer coefficients has a linear monic factor with a rational constant term, it is actually an integer constant term. This is a special case of a more general result known as Gauss's Lemma: If $f(x)$ is a monic polynomial with integer coefficients which factors as $g(x)h(x)$, where g and h are monic polynomials with rational coefficients, then in fact g and h have integer coefficients. The proof that is usually given for this result makes use of unique factorization. Here, using matrix methods, we can give an alternate proof that does not explicitly depend on unique factorization.

The proof is formulated in terms of *algebraic integers*: complex roots of monic polynomials with integer coefficients. Our preceding results say that an algebraic integer in $\mathbb{Q}$ must be in $\mathbb{Z}$, and an algebraic integer in $\mathbb{Q}[i]$ must be in $\mathbb{Z}[i]$. The first of these results can be applied to prove Gauss's lemma, once we show that the algebraic integers are closed under addition and multiplication. The idea will be to show that the coefficients of factors g and h are algebraic integers since they are combinations of the roots. That will make the coefficients rational algebraic integers, and hence integers.

In addition to its role in the earlier lemmas and results, matrix algebra also provides a convenient means to establish that the algebraic integers are closed under addition and multiplication. It is clear from Lemma 1 that algebraic integers can be characterized as eigenvalues of matrices with integer entries. To deal with sums and products of these eigenvalues, a useful matrix operation is the *tensor product*, also called the *Kronecker product*. Given two matrices A and B, the Kronecker product $A \otimes B$ is defined as follows: Replace each entry a_{ij} of A with an entire block of entries, given by the product $a_{ij}B$. The resulting matrix is $A \otimes B$. There is a nice discussion of Kronecker products in **[6]**. Here, we require only one identity: $(A \otimes B)(C \otimes D) = AC \otimes BD$, which is valid as long as the products AC and BD exist. The proof is a straightforward exercise. With the identity we can prove the following lemma.

LEMMA 3. *If λ and μ are algebraic integers, then so are $\lambda\mu$ and $\lambda + \mu$.*

Proof: Suppose that λ and μ are algebraic integers. Then there are integer matrices A and B, and integer vectors v and w, such that $Av = \lambda v$ and $Bw = \mu w$. Therefore $(A \otimes B)(v \otimes w) = (Av) \otimes (Bw) = \lambda\mu(v \otimes w)$. This shows that $\lambda\mu$ is an eigenvalue of the integer matrix $A \otimes B$, and hence, is an algebraic integer. In a similar way, it is easy to show that $\lambda + \mu$ is an eigenvalue of the integer matrix $A \otimes I + I \otimes B$. Therefore $\lambda + \mu$ is an algebraic integer.

Gauss's lemma is now easily proved.

THEOREM 2. *Let f be a monic polynomial with integer coefficients, and suppose $f = gh$ where g and h are monic polynomials with rational coefficients. Then the coefficients of g and h are actually integers.*

Proof: The roots of f, and hence those of g and h, are algebraic integers. The coefficients of g and h are elementary symmetric functions of the roots, and so can be constructed from the roots using addition and multiplication. This shows that the coefficients of g and h are algebraic integers. But they were assumed to be rational. Thus, they are in fact integers, as asserted.

Integrally Closed Domains We conclude with one further generalization, and a question. The foregoing material can be understood in the context of integral domains and fields of quotients (see, e.g., **[7]**). In our earliest results, the coefficients of the polynomials were integers, and we showed rational roots had to be integers as well. Observe that the rationals are the field of quotients for the integers. This same relationship extends to the results on Gaussian integers. The quotient field for $\mathbb{Z}[i]$ is $\mathbb{Q}[i]$. Our earlier result states that for a monic polynomial over $\mathbb{Z}[i]$, any root in the quotient field of the Gaussian integers must itself be a Gaussian integer.

In both cases, polynomials are considered over an integral domain, and the field of quotients contains no roots other than those that were already present in the integral domain. Proceeding with this more general setting, consider an integral domain D within its field of quotients F. Define $\lambda \in F$ to be *integral over D* if it is a root of a monic polynomial with coefficients in D, and observe that each element of D is integral over D. If these are the only elements integral over D, then D is said to be *integrally closed*. That is, an integral domain D is integrally closed if it contains all the elements of the field of quotients which are integral over D. The earlier results showed that the integers and the Gaussian integers are both integrally closed.

Now the question arises: what is the most general setting for the matrix results presented earlier? Lemmas 1 and 2 still hold if we replace the integers by an integral domain D and the rationals by D's field of quotients. The proofs of Theorem 1 and its extension to the complex case are not so easy to generalize, for they depend on analytic properties that are peculiar to the integers and the Gaussian integers. To illustrate the difficulties, we consider two examples. Each is a quadratic extension of the integers, that is, a domain of the form $\mathbb{Z}[\sqrt{k}\,] = \{n + m\sqrt{k} \mid n, m \in \mathbb{Z}\}$ where k is a square-free integer. The field of quotients is $\mathbb{Q}[\sqrt{k}\,]$, defined analogously. It is known that $\mathbb{Z}[\sqrt{k}\,]$ is integrally closed just when $k \not\equiv 1 \pmod 4$. (See, e.g., [7].)

For the first example, $k = -5$, and the domain $\mathbb{Z}[i\sqrt{5}\,]$ is integrally closed. That means that $\lambda \in \mathbb{Q}[i\sqrt{5}\,]$ is a root of a monic polynomial over $\mathbb{Z}[i\sqrt{5}\,]$ only if it is *in* $\mathbb{Z}[i\sqrt{5}\,]$. To demonstrate this, it is tempting to mimic the proof of Theorem 1. Things go awry right at the start, where we want to assume that $|\lambda| < 1$. In the original argument, this step was justified by the observation that λ was at most one unit away from an integer. Unfortunately, that is not true for $\mathbb{Z}[i\sqrt{5}\,]$. Picture the elements as a lattice in the complex plane. The lattice points are separated by one unit horizontally, but by $\sqrt{5}$ units vertically. That means they are too far apart. In particular, if $\lambda = .5 + .5i\sqrt{5}$, the nearest elements of the integral domain are more than one unit away. This foils our desire to find a matrix with entries in $\mathbb{Z}[i\sqrt{5}\,]$ and with an eigenvalue of magnitude less than unity in the quotient field. The argument breaks down because we are unable to produce an appropriate matrix to act as a contraction.

The second example considers $k = 5$, and the result cited earlier says that $\mathbb{Z}[\sqrt{5}\,]$ is not integrally closed. This is easy to see directly: the polynomial $t^2 - t - 1$ has coefficients in $\mathbb{Z}[\sqrt{5}\,]$, and roots $(1 \pm \sqrt{5}\,)/2$ in $\mathbb{Q}[\sqrt{5}\,]$ but not in $\mathbb{Z}[\sqrt{5}\,]$. What happens if we try to follow the proof of Theorem 1 for this example? Observe that all the action takes place on the real line, so the elements of $\mathbb{Q}[\sqrt{5}\,]$ are all within one unit of an integer, and hence, within one unit of an element of the domain $\mathbb{Z}[\sqrt{5}\,]$. As in Theorem 1, we can construct a matrix with an eigenvalue of magnitude less than 1, and which acts as a contraction on the corresponding eigenspace. In particular, a point of that eigenspace with all entries from $\mathbb{Z}[\sqrt{5}\,]$ must generate a sequence of such points converging to the origin. However, for the current example, that presents no contradiction. The elements $\mathbb{Z}[\sqrt{5}\,]$ are not discretely spaced on the real line, and in particular, have 0 for a limit point. So for this example, the entire proof of Theorem 1 remains valid, but failing to result in a contradiction, offers no assurance that $\mathbb{Z}[\sqrt{5}\,]$ is integrally closed.

As these two examples highlight, Theorem 1 and its extension to the Gaussian integers depend on a coincidence of special properties. In addition to the underlying structure exposed in Lemmas 1 and 2, we require a metric on the quotient field satisfying two conditions: (1) the elements of the integral domain cannot get arbitrarily close to 0 (nor hence to any other domain element); and (2) the elements of the domain must get within one unit of every element of the field. In other words, the proof demands that the integral domain elements are neither too close together nor too far apart. This combination of properties does occur for $\mathbb{Z}$ and $\mathbb{Z}[i]$. We don't know if there are any other domains for which the same argument can be made to work, and so we leave it as an open question: Other than $\mathbb{Z}$ and $\mathbb{Z}[i]$, are there integral domains for which the field of quotients satisfies the two conditions above? Clearly, any such domain will have to be integrally closed. That observation prompts another question: Given an integral domain D, under what conditions is there a metric on the field of quotients satisfying the two conditions above?

Conclusion

This paper has considered several aspects of irrationality. Starting with the earliest history, we reviewed the formulation of irrationality in the context of incommensurable segments in geometry. A geometric argument based on infinite descent was reformulated in the now familiar setting of dynamical systems, using matrix algebra for the descent mechanism. In that context, we saw natural extensions from the ring of integers to other structures of modern algebra. In the initial situation, we considered monic polynomials with integer coefficients, and saw that irrational numbers emerge as roots lying outside of $\mathbb{Z}$. The more general setting concerns the monic polynomials over an integral domain D and the nature of roots that are outside of D. The cited result in this area, namely that $\mathbb{Z}[\sqrt{k}\,]$ is integrally closed for square-free k so long as k is not congruent to 1 mod 4, suggests an algebraic subtlety that is absent from the simple dynamic arguments of Theorem 1. Perhaps it should not surprise us that these arguments proved ineffective for $\mathbb{Z}[\sqrt{5}\,]$ and $\mathbb{Z}[i\sqrt{5}\,]$. It remains to be seen whether the dynamic approach can be successfully applied in the more general setting.

REFERENCES

1. Asger Aaboe, *Episodes from the Early History of Mathematics*, New Mathematical Library, Mathematical Association of America, Washington, DC, 1964.
2. Carl Boyer, *A History of Mathematics*, 2nd edition, revised by Uta C. Merzbach, Wiley, New York, NY, 1991.
3. David M. Burton, *The History of Mathematics*, Allyn and Bacon, Newton, MA, 1985, pp. 122–123.
4. James R. Choike, The pentagram and the discovery of an irrational number, *The College Mathematics Journal* 11 (1980), 312–316.
5. I. N. Herstein, *Topics in Algebra*, Ginn and Company, Waltham, MA, 1964.
6. Roger A. Horn and Charles R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, Cambridge, UK, 1991.
7. Martin Isaacs, *Algebra, a Graduate Course*, Brooks/Cole, Pacific Grove, CA, 1994, Chapter 28.
8. Thomas Liggett and Peter Peterson, The law of large numbers and $\sqrt{2}$, *The American Mathematical Monthly* 102 (1995), 31–35.
9. Kurt von Fritz, The discovery of incommensurability by Hippasus of Metapontum, *Annals of Math.* 46 (1945), 242–264.
10. Robert Young, *Excursions in Calculus*, Dolciani Mathematical Expositions, Mathematical Association of America, Washington DC, 1992.

Arithmetic Triangles

RAYMOND A. BEAUREGARD
E. R. SURYANARAYAN
University of Rhode Island
Kingston, RI 02881

1. Introduction

As early as the first century, scholars such as Heron of Alexandria had shown interest in triangles with rational sides and rational areas. These have become known as *rational triangles* or *Heron triangles*. Multiplying by common denominators, the study of Heron triangles reduces to the study of triangles with integer sides and integer areas. We refer to triangles whose integer sides form an arithmetic progression and whose areas are integers as *arithmetic triangles*. This particular class of Heron triangles has attracted considerable attention.

In the seventh century, Brahmagupta gave a systematic analysis for the special case of triangles with consecutive integer sides [**4**]. In the nineteenth century, H. Rath, R. Hoppe, and L. Aubry did considerable work with arithmetic triangles. In fact Hoppe noted formulas that describe the sides of arithmetic triangles [**5**]. In this paper we will see how all such triangles arise in terms of right triangles and we will derive Hoppe's formulas.

Let us call a triangle *d-arithmetic* if its sides have lengths c, $c+d$, and $c+2d$, where c, d, and the area are integers. Although $d \neq 0$ it will be convenient to allow negative values of d; thus a d-arithmetic triangle is also $(-d)$-arithmetic. The smallest example of such a triangle is the right triangle with sides of lengths 3, 4, 5. It is known (and we will show) that except for similarity this is the only right triangle that is arithmetic. Another example is the triangle (known to Heron) whose sides measure 13, 14, and 15, and whose area is 84; both of these triangles are 1-arithmetic. We will show how any arithmetic triangle that is not a right triangle gives rise to two right triangles with integer sides. Recall that a *Pythagorean triple* (PT for short) is a triple (a, b, c) whose components are positive integers satisfying the equation $a^2 + b^2 = c^2$. Thus we will see how every arithmetic triangle gives rise to two companion PTs. We will also see, conversely, how every PT (together with its companion PT) gives rise to an arithmetic triangle. PTs are described algebraically in [**3**] where middle components are not restricted to be positive. We adopt this convention here as well.

We will also describe how all arithmetic triangles can be found using a parametric representation. This representation enables us to show that primitive d-arithmetic triangles exist if and only if the *Diophantine equation* $x^2 - 3y^2 = d^2$ has a primitive solution, which is the case if and only if $|d| = 1$ or $|d|$ is a product of primes $p_i \equiv \pm 1 \pmod{12}$. It is not surprising that arithmetic triangles have been a fascination through the centuries; simple geometric problems such as this have often given rise to interesting number-theoretic considerations.

2. From an Arithmetic Triangle to a PT

Suppose that we have a d-arithmetic triangle. Assume it is acute; we shall look at the obtuse case in a moment. Let a perpendicular of length a rise up from the side of length $c+d$ to the opposite vertex, as in FIGURE 1. This divides the arithmetic triangle

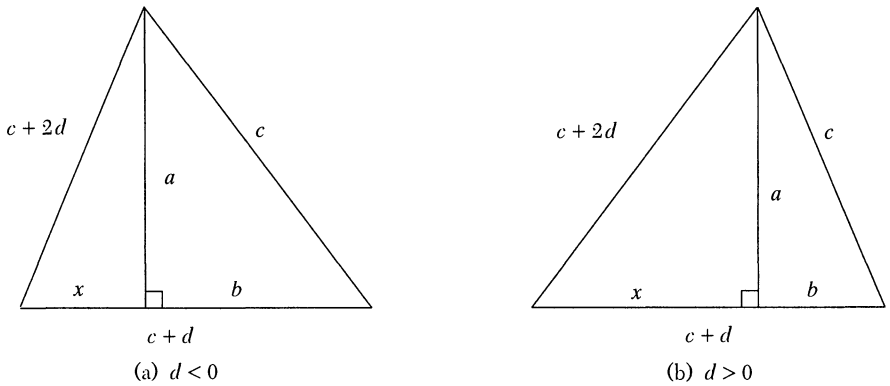


FIGURE 1
Acute arithmetic triangles

into two right triangles, with base lengths x and b as shown in FIGURE 1. Then $x = b + 4d$, because

$$x^2 = (c + 2d)^2 - a^2 = (c^2 - a^2) + 4cd + 4d^2 = b^2 + 4d(x + b);$$

adding $4d^2 - 4dx$ to both sides we obtain

$$(x - 2d)^2 = (b + 2d)^2.$$

Therefore $x - 2d = \pm(b + 2d)$. Since the negative choice is not possible ($x = -b$ leads to a contradiction) we obtain $x = b + 4d$.

We claim that a and b are integers. To see this, notice that $c + d = 2b + 4d$ so that $2b$ is an integer which means b is at least rational. Since the area $(a/2)(c + d)$ is an integer it follows that a is rational as well. Now $(2a)^2 = 4c^2 - (2b)^2$ is an integer so $2a$ (which is rational) is an integer. Let $a = a_1/2$, $b = b_1/2$, and $c = c_1/2$. Then (a_1, b_1, c_1) is a PT so that one of a_1, b_1 must be even (otherwise the equation $a_1^2 + b_1^2 = c_1^2$ taken modulo 4 gives a contradiction). Thus a or b is an integer and so a *and* b are integers, since $a^2 + b^2 = c^2$.

If the arithmetic triangle is obtuse we extend the side of length $c + d$ so that a perpendicular of length a will rise from one end to meet the opposite vertex as shown in FIGURE 2. Computation shows that $x = b + 4d$ and a and b are integers, as in the acute case.

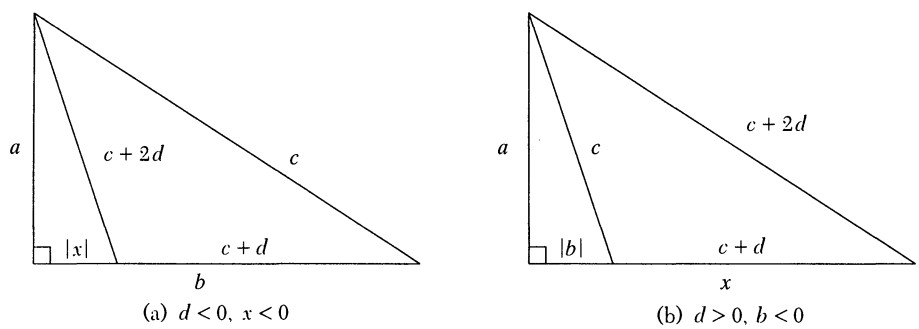


FIGURE 2
Obtuse arithmetic triangles

In either case

$$d = (c - 2b)/3, \tag{1}$$

as is easily seen: we have $b + 4d = x = c + d - b$, from which (1) follows. From this equation and the expression $x = b + 4d$ we find that

$$x = (4c - 5b)/3 \quad \text{and} \quad c + 2d = (5c - 4b)/3.$$

Thus the pairs of right triangles in FIGURE 1 or 2 correspond to the PTs

$$(a, b, c) \quad \text{and} \quad (a, (4c - 5b)/3, (5c - 4b)/3). \tag{2}$$

The triples in (2) are referred to as *companion PTs*. A formal definition is given below. Starting with an arithmetic triangle, its companion PTs can be found from the values c and d by using (1), (2), and the Pythagorean relation. FIGURE 3 illustrates this with the 11-arithmetic triangle having sides of length 15, 26, 37.

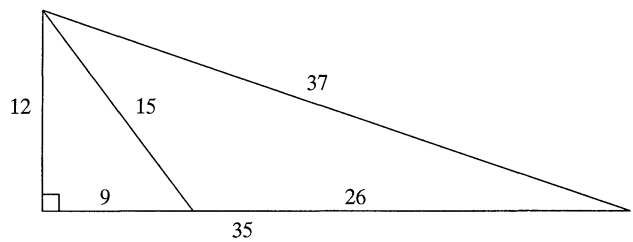


FIGURE 3
(12, 35, 37) with companion (12, −9, 15)

3. From a Primitive PT to an Arithmetic Triangle

Let us see how any PT (a, b, c), such that $c - 2b = 3d$ for some integer d, gives rise to a d-arithmetic triangle. In this case the second triple in (2) has integer components and satisfies the Pythagorean relation (as is easily checked). Note that $5c - 4b > 0$. If $4c - 5b > 0$ then the two right triangles corresponding to the PTs in (2) may be joined at their common leg to form an arithmetic triangle in FIGURE 1. If $4c - 5b < 0$ then $x < 0$ and we obtain an obtuse arithmetic triangle in FIGURE 2(a). FIGURE 2(b) depicts the case when $b < 0$. The area of each of these (non-right) triangles is $a(c + d)/2 = a(b + 2d)$, which is an integer.

We are led to the following definition. A PT $A = (a, b, c)$ is *d-arithmetic* if $c - 2b = 3d$ for some integer d. Unlike arithmetic triangles a PT cannot be both d-arithmetic and $(-d)$-arithmetic. If A is an arithmetic PT then

$$A^c = (a, (4c - 5b)/3, (5c - 4b)/3) \tag{3}$$

is the *companion* of A. It is easily checked that A^c is also an arithmetic PT; in fact, if A is d-arithmetic then A^c is $(-d)$-arithmetic. For example, (60, 11, 61) is 13-arithmetic and has companion (60, 63, 87) which is (-13)-arithmetic.

We also have $A^{cc} = A$. This is best seen by writing (3) in matrix form,

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix}^c = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -5/3 & 4/3 \\ 0 & -4/3 & 5/3 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix},$$

and noting that the matrix is self inverting.

It is well known that one of the two legs a, b of any PT must be in $3\mathbb{Z}$ (i.e., a multiple of 3) [3]. If we assume that A is arithmetic and primitive (so that a, b, and c are relatively prime) then $a \in 3\mathbb{Z}$; the alternative $b \in 3\mathbb{Z}$ together with the requirement that $c - 2b \in 3\mathbb{Z}$ would yield $c \in 3\mathbb{Z}$ and so $a \in 3\mathbb{Z}$ as well since $a^2 + b^2 = c^2$; but this contradicts primitivity. Thus $a \in 3\mathbb{Z}$ while b and c are not multiples of 3. Furthermore, we claim that

$$A^c = 3(a_0, b_0, c_0) \tag{4}$$

where (a_0, b_0, c_0) is a primitive PT. We know that 9 divides $a^2 = (c + b)(c - b)$. But 3 cannot divide $c - b$ because, together with $c - 2b \in 3\mathbb{Z}$, this would yield $2c$ and hence $c \in 3\mathbb{Z}$, which is not possible. Thus 9 must divide $c + b$. Adding to this the fact that 9 divides $3c - 6b$ we find that 9 divides $4c - 5b$. Thus the first two and hence all three components of the PT in (3) are multiples of 3, and we may write A^c as in (4). Equation (3) shows clearly that any common divisor of a, b, and c must divide the components of A^c. Likewise any common divisor for (a_0, b_0, c_0) would give a common divisor for $A^{cc} = A$. Thus (a_0, b_0, c_0) is a primitive PT (but not arithmetic). A similar argument shows that, conversely, a non-arithmetic primitive PT multiplied by 3 has a primitive companion.

If we begin with any PT (a, b, c) then one of $c \pm 2b$, $c \pm 2a$ is a multiple of 3. To see this it suffices to work with a primitive PT, for if (a, b, c) has this property then so does (ka, kb, kc) for any positive integer k. Now either a or $b \in 3\mathbb{Z}$. Assuming that $a \in 3\mathbb{Z}$ we find that

$$(c - 2b)(c + 2b) = c^2 - 4b^2 = a^2 - 3b^2$$

is a multiple of 3 and so 3 divides one of the factors $(c \pm 2b)$. The other case is similar.

Thus given any PT (a, b, c) with $b > 0$, after switching its legs a and b if necessary we see that either (a, b, c) or $(a, -b, c)$ is arithmetic. In the primitive case, just one of these is arithmetic. If the middle component of this PT has the same algebraic sign as that of its companion we obtain an acute arithmetic triangle represented in FIGURE 1. If these algebraic signs are opposite, we obtain an obtuse arithmetic triangle as depicted in FIGURE 2, where a right triangle lies inside its companion triangle. Note that the sum of both middle components is $(4c - 2b)/3$, which is a positive even integer and is the length of the base of the arithmetic triangle. In this way each primitive PT corresponds to a unique primitive arithmetic triangle.

4. From an Arbitrary PT to an Arithmetic Triangle

Let (a, b, c) be a PT, with $b \neq 0$. In how many arithmetic triangles does this PT "appear" in the sense that a right triangle with sides $a, |b|, c$ forms one of the companion triangles? We know that such an arithmetic triangle must have sides c, $c + d$, $c + 2d$ where $d = (c \pm 2b)/3$ or $d = (c \pm 2a)/3$. If we write

$$(a, b, c) = 3^j k(a_0, b_0, c_0)$$

where (a_0, b_0, c_0) is primitive then $3^{j-1}k$ divides c and d (assuming $j > 0$). Dividing out $3^{j-1}k$ from a, b, c, and d we may assume that (a, b, c) is primitive or has the form three times a primitive PT, say

$$(a, b, c) = 3(a_0, b_0, c_0). \tag{5}$$

First assume that (a, b, c) is primitive. We know that exactly one of the following four PTs is arithmetic:

$$(a, b, c), \quad (a, -b, c), \quad (b, a, c), \quad (b, -a, c), \tag{6}$$

and it appears in a unique arithmetic triangle as described earlier. In the second case (that of equation (5)) we find that each of the four PTs in (6) is arithmetic. Three of these will have a primitive companion, and the other will have a companion equal to nine times a primitive PT, namely the one in (6) which is three times an *arithmetic* PT. (If $A = 3A_0$ where A_0 is a primitive and arithmetic PT then $A^c = 3A_0^c$ and A_0^c is itself three times a primitive PT.) Except for this last case each of the arithmetic triangles is primitive.

We conclude that every nontrivial PT corresponds to a right triangle that appears in exactly one or four arithmetic triangles, depending on whether its components are all relatively prime to 3. For example, the PT (12, 5, 13) or any of its multiples relatively prime to 3 appears in exactly one arithmetic triangle. However, the PT 3(12, 5, 13) (or any of its multiples) appears in four arithmetic triangles as illustrated in FIGURE 4.

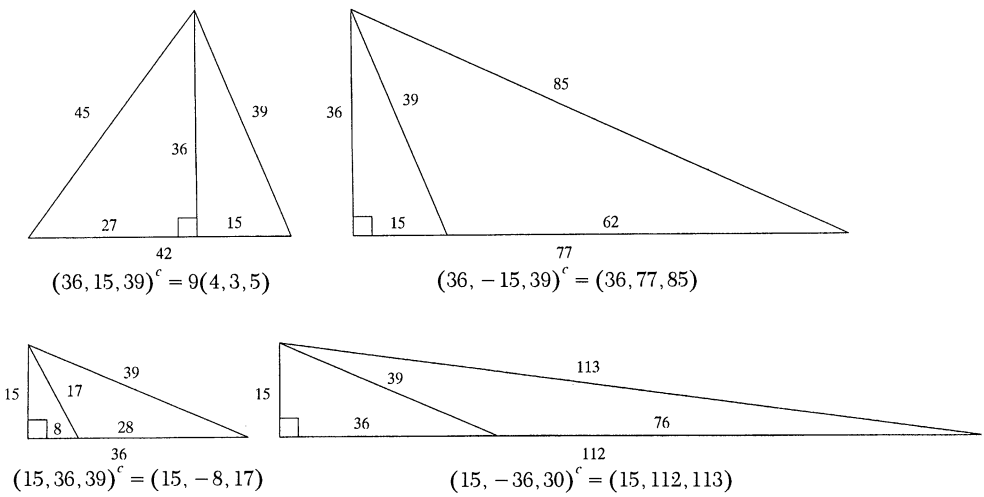


FIGURE 4
The four arithmetic triangles for 15, 36, 39

5. An Algebraic Excursion

In [3] we describe how the set of all PTs (with possibly negative middle components) forms a commutative cancellative semigroup under the operation

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2). \tag{7}$$

The PT $(1, 0, 1)$ is the identity element in this semigroup. (Actually, when PTs corresponding to similar triangles are identified appropriately we obtain a group with

the inverse of (a, b, c) corresponding to $(a, -b, c)$.) It can be shown that the set of arithmetic PTs is closed under $*$; a computation shows that if (a_i, b_i, c_i) is d_i-arithmetic for $i = 1, 2$, then the PT on the right-hand side in (7) is $(3d_1d_2 - b_1b_2)$-arithmetic. Also, if (a, b, c) is an arithmetic PT then it is easy to check that

$$(a, b, c) * (a, b, c)^c = (a^2/3)(3, 4, 5). \tag{8}$$

Suppose that we have an arithmetic triangle that is already a right triangle. Referring to FIGURES 1 and 2 we see that the companion of (a, b, c) must be trivial and so have the form $(a, 0, a) = a(1, 0, 1)$. Thus the left-hand side of (8) reduces to $a(a, b, c)$ from which it follows that

$$(a, b, c) = (a/3)(3, 4, 5).$$

This shows that, up to similarity, the $(3, 4, 5)$-triangle is the only right triangle that is arithmetic.

6. Parametric Representation

For a primitive PT (a, b, c) let $(b + c)/a = n/m$ where n and m are relatively prime. It is shown in [3] that

$$(a, b, c) = \begin{cases} (2nm, n^2 - m^2, n^2 + m^2) \text{ if } a \text{ is even} \\ (nm, (n^2 - m^2)/2, (n^2 + m^2)/2) \text{ if } a \text{ is odd.} \end{cases} \tag{9}$$

Let us refer to (n, m) as the *parametric pair* for (a, b, c). If (a, b, c) is d-arithmetic then computing $(c - 2b)/3$ we find that

$$d = \begin{cases} m^2 - n^2/3 \text{ if } a \text{ is even} \\ (1/2)(m^2 - n^2/3) \text{ if } a \text{ is odd.} \end{cases}$$

Now $(a, b, c)^c = (a, (4c - 5b)/3, (5c - 4b)/3) = 3(a_0, b_0, c_0)$. To find the parametric pair for the primitive PT (a_0, b_0, c_0) we divide the sum of its final two components by its first and obtain

$$(5c - 4b + 4c - 5b)/3a = 3(c - b)/a = 3m/n.$$

Since n and m are relatively prime and a $(= 2nm$ or $nm)$ is divisible by 3, there are two cases to consider: $m \in 3\mathbb{Z}$ or else $n \in 3\mathbb{Z}$. If $m \in 3\mathbb{Z}$ then $(3m, n)$ is the parametric pair for (a_0, b_0, c_0) and we obtain $a = 3a_0 = 6nm$ or $3nm$ which contradicts (9). Thus $n \in 3\mathbb{Z}$ and $(m, n/3)$ is the parametric pair for (a_0, b_0, c_0).

In summary, any arithmetic triangle may be reduced to a *primitive* one whose three sides are relatively prime. The resulting triangle gives rise to two companion PTs, one of which is primitive. Using this primitive PT we obtain the parameters n and m which are relatively prime and with $n \in 3\mathbb{Z}$ as described above.

Conversely if n and m are two relatively prime positive integers with $n \in 3\mathbb{Z}$ then letting

$$c = n^2 + m^2 \text{ and } d = m^2 - n^2/3 \tag{10}$$

we obtain a triangle with sides c, $c+d$, $c+2d$ provided that one of the triangle inequalities is satisfied:

$$c+2d<c+(c+d) \quad \text{if} \quad d>0, \text{ or}$$
$$c<(c+d)+(c+2d) \quad \text{if} \quad d<0.$$

Now the first inequality (for $d>0$) is equivalent to $d<c$, which is clear from the definition of c and d. The second inequality (for $d<0$) reduces to $-3d<c$, which is also clear by definition of c and d. To see that our triangle is arithmetic we use Heron's famous area formula [5],

$$\text{area} = \sqrt{s(s-s_1)(s-s_2)(s-s_3)},$$

where s_1, s_2, s_3 measure the sides of the triangle and s is half the perimeter. Thus

$$\text{area} = \sqrt{s(s-c)(s-c-d)(s-c-2d)},$$

where $s=3(c+d)/2$. Expressing this in terms of n and m we obtain

$$\text{area} = 2mn(n^2+3m^2)/3,$$

which is an integer because $n \in 3\mathbb{Z}$. Our triangle is primitive unless both n and m are odd, in which case c and d are even and we obtain a primitive arithmetic triangle which has been doubled (so we divide its legs by 2). Table 1 gives all primitive arithmetic triangles for n, $m \le 9$. When $n<m$ we obtain obtuse triangles since $b<0$. When $n>m$ the triangles are acute if $3m>n$ and obtuse if $3m<n$; this corresponds to whether the term $4c-5b$ in the middle component of the companion is positive or negative respectively.

TABLE 1. The first few primitive arithmetic triangles

m	n	d	c	$c+d$	$c+2d$
1	3	−1	5	4	3
2	3	1	13	14	15
4	3	13	25	38	51
5	3	11	17	28	39
7	3	23	29	52	75
8	3	61	73	134	195
1	6	−11	37	26	15
5	6	13	61	74	87
7	6	37	85	122	159
1	9	−13	41	28	15
2	9	−23	85	62	39
4	9	−11	97	86	75
5	9	−1	53	52	51
7	9	11	65	76	87
8	9	37	145	182	219

Finally, if we write $n=3k$ in (10) then we obtain the equation

$$m^2-3k^2=d \tag{11}$$

and Hoppe's formulas [5, p. 197]

$$c=9k^2+m^2, \quad c+d=2(3k^2+m^2), \quad c+2d=3(k^2+m^2),$$

describing all primitive arithmetic triangles (remembering to take half of c and d when m and k are both odd).

7. The Allowable Values d

When $d = 1$, Eq. (11) reduces to the Pell equation, whose infinite solution set is well known and will be described shortly. It is known that Eq. (11) has no solution if $d = -1$; the (-1)-arithmetic triangles arise from solutions to the equation $x^2 - 3y^2 = -2$. Our work in Section 6 indicates that d-arithmetic triangles correspond to positive solutions of the equation

$$x^2 - 3y^2 = \alpha d, \quad \alpha = 1 \text{ or } 2. \tag{11A}$$

A glance at Table 1 might suggest that for $|d| > 1$ only certain prime integer values of d are allowable for a primitive d-arithmetic triangle. This is not the case as the proposition below shows. The allowable values d arise if and only if d is odd and the Diophantine equation (11A) has a positive primitive solution (m, k) where $m \notin 3\mathbb{Z}$ (in which case we obtain the triangle described by (10) with $n = 3k$). Using the substitution

$$m_0 = (m + 3k)/2 \text{ and } k_0 = (m + k)/2$$

when m and k are both odd, this condition is equivalent to the existence of a primitive solution (m_0, k_0) to the equation

$$x^2 - 3y^2 = \pm d, \tag{11B}$$

where $m_0 \notin 3\mathbb{Z}$. We will focus on finding the positive solutions to (11B) when $|d| > 1$. The following modified form of a result due to Brahmagupta shows how allowable values multiply.

PROPOSITION (Multiplicative Property). *If d_1 and d_2 are relatively prime integers and both allowable values for primitive arithmetic triangles, then $d_1 d_2$ is also allowable.*

Proof. Brahmagupta's rule of composition [**1**, p. 320] tells us that if $m_i^2 - 3k_i^2 = \pm d_i$, for $i = 1, 2$, then (11B) is satisfied for $d = d_1 d_2$ and for m and k defined by

$$m + \sqrt{3}k = \left(m_1 + \sqrt{3}k_1\right)\left(m_2 + \sqrt{3}k_2\right).$$

Comparing both sides of this equation we see that

$$m = m_1 m_2 + 3k_1 k_2, \quad k = m_1 k_2 + m_2 k_1. \tag{12}$$

The first equation in (12) shows that $m \notin 3\mathbb{Z}$ if $m_i \notin 3\mathbb{Z}$. If d_1 and d_2 are relatively prime then (m, k) is primitive: the equations in (12) yield

$$km_2 - k_2 m = \pm k_1 d_2, \quad m_1 k - k_1 m = \pm k_2 d_1.$$

Keeping in mind that $m_i \notin 3\mathbb{Z}$ we see that any prime q dividing both k and m will divide the right hand sides of these equations and lead to a contradiction. This completes the proof.

Suppose that d is allowable so that there exists a primitive solution (m, k) to (11B) with $m \notin 3\mathbb{Z}$. Then k is relatively prime to d and so to each odd prime factor p of d.

Note that $p \neq 3$. Let $d = rp$ and write (11B) as

$$m^2 - 3k^2 = \pm rp. \tag{13}$$

Now k has a multiplicative inverse modulo p so there exists an integer t such that $m \equiv kt \pmod{p}$. Equation (13) then shows that

$$t^2 \equiv 3 \pmod{p}. \tag{14}$$

But it is known that this is possible if and only if $p \equiv \pm 1 \pmod{12}$ (see [**1**, p. 131]). In particular, if d is allowable then $d \equiv \pm 1 \pmod{12}$. The converse is not true; for example, there are no 49-arithmetic triangles. However, a partial converse holds, namely for primes: If p is a prime such that $p \equiv \pm 1 \pmod{12}$ then (11B) with $d = p$ has a primitive solution (so that p is allowable). For a nice proof of this result see [**6**, p. 211].

Let p be such a prime and let us show that p^i is allowable for any positive integer i. Brahmagupta's rule of composition shows that (11B) is solvable when $d = p^i$. Clearly the first component of a solution can not be a multiple of 3 since $p > 3$. But how do we know that the solution is primitive? If (m, k) is a primitive solution to (11B) with $m \notin 3\mathbb{Z}$ then the composite solution $(m^2 + 3k^2, 2mk)$ to $x^2 - 3y^2 = d^2$ is primitive since a prime divisor (necessarily odd) of both $m^2 + 3k^2$ and $2mk$ would divide d, m, and k, contradicting the primitivity of (m, k). In particular p^i is allowable when $i = 2^j$. If i does not have this form let j be an integer such that $i < 2^j$. Let (m_1, k_1) be a primitive solution of $x^2 - 3y^2 = p$ and let

$$m_w + k_w\sqrt{3} = \left(m_1 + k_1\sqrt{3}\right)^w.$$

Brahmagupta's rule of composition shows that (m_w, k_w) is a solution to

$$x^2 - 3y^2 = p^w.$$

Composing solutions for $w = i$ and $w = 2^j - i$ we see that

$$m_{2^j} = m_i m_{2^j - i} + 3k_i k_{2^j - i}, \quad k_{2^j} = k_i m_{2^j - i} + m_i k_{2^j - i}.$$

These equations show that any common divisor greater than 1 of m_i and k_i contradicts the primitivity of (m_{2^j}, k_{2^j}). We conclude that p^i is allowable.

We shall describe how to find all primitive d-arithmetic triangles for a given allowable value d. The multiplicative property shows that it suffices to work with the case in which d is a prime power. In order to avoid having to treat the two cases of (11B) separately we describe a d-arithmetic triangle more symmetrically as shown in FIGURE 5. Heron's formula for the area becomes

$$3hg = \sqrt{3g(g-d)g(g+d)}$$

which reduces to

$$g^2 - 3h^2 = d^2, \tag{15}$$

an equation similar to (11). Note that (11B) (for one of the choices of algebraic sign) has a primitive solution (m, k) with $m \notin 3\mathbb{Z}$ if and only if (15) has a primitive solution since either occurs if and only if there exists a primitive d-arithmetic triangle. We summarize what has been established so far.

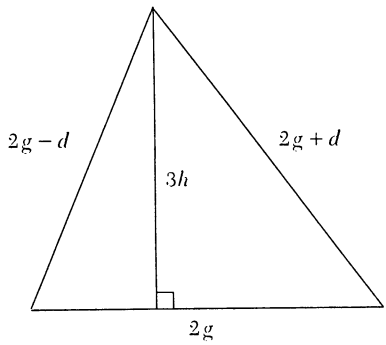


FIGURE 5
A d-arithmetic triangle

THEOREM (Allowable d-values). *The following statements are equivalent for an odd integer d.*

(i) *There exist primitive d-arithmetic triangles.*
(ii) $d = \pm 1$ *or is a product of primes* $p_i \equiv \pm 1 \pmod{12}$.
(iii) $x^2 - 3y^2 = d^2$ *has primitive (integer) solutions.*
(iv) $x^2 - 3y^2 = \pm d$, $x \notin 3\mathbb{Z}$ *has primitive (integer) solutions for one choice of algebraic sign.*

We seek all primitive solutions (g, h) to (15) for relatively prime integers g and h. References **[1]**, **[2]**, and **[6]** are good sources for this kind of problem. When $d = 1$ it is known that the positive solutions (g_j, h_j) of (15) are given by the sequence

$$(g_j, h_j) = (2,1), (7,4), (26,15), \ldots, \tag{16}$$

where $g_{j+2} = 4g_{j+1} - g_j$ and $h_{j+2} = 4h_{j+1} - h_j$. A neat proof of this fact is given in **[4]**. This describes all triangles that are 1-arithmetic. If the least positive solution of (15) with $|d| > 1$ is obtained, then it may be combined using Brahmagupta's rule of composition with the sequence in (16) to produce an infinite number of primitive d-arithmetic triangles. However, this does not produce all of them.

In order to find all solutions to (15) we assume that $d = p^i$ where p is an allowable prime. Reasoning as before, if (g, h) is a primitive solution to (15), then h is relatively prime to p (and so is invertible modulo p). Thus we can find an integer t such that $g \equiv ht \pmod{p}$, and we may take $-p/2 < t < p/2$. Equation (15) then shows that $t^2 \equiv 3 \pmod{p}$. This congruence has exactly two solutions $\pm t$ between $-p/2$ and $p/2$ (see **[1]**, p. 72]). Let C_t be the set of all positive primitive solutions (g, h) of (15) for a given value t. It can be shown that any two members of C_t are related by a (Brahmagupta) composition with a member of the sequence (16) (see **[1]**, p. 345]). Thus it suffices to find the least positive solutions in each of the two classes C_{-t} and C_t.

Let us find all 13-arithmetic triangles. By inspection we find the first two positive solutions of the equation $g^2 - 3h^2 = 13^2$ to be

$$(G_1, H_1) = (14,3) \text{ and } (G_2, H_2) = (19,8),$$

and these are both primitive. Since $t^2 \equiv 3 \pmod{13}$ we must have $t = \pm 4$. The least positive members of the classes C_{-4} and C_4 are $(14, 3)$ and $(19, 8)$ respectively. Composing these with the members of sequence (16) using Brahmagupta's rule of composition we obtain the values G_j and H_j, describing all primitive 13-arithmetic triangles. The first few of these are given in Table 2.

TABLE 2. The first few 13-arithmetic triangles

	G_j	H_j	$2G_j - d$	$2G_j$	$2G_j + d$
C_{-4}	14	3	15	28	41
	37	20	61	74	87
	134	77	255	268	281
	499	288	985	998	1011
C_4	19	8	25	38	51
	62	35	111	124	137
	229	132	445	458	471
	854	493	1695	1708	1721

REFERENCES

1. A. Alder and J. Coury, *The Theory of Numbers*, Jones & Bartlett Pub. Co., Boston, MA (1995).
2. W. S. Anglin, *The Queen of Mathematics (An Introduction to Number Theory)*, Kluwer Academic Publishers, Boston, MA (1995).
3. R. A. Beauregard and E. R. Suryanarayan, Pythagorean triples: the hyperbolic view, *College Math. J.*, May 1996.
4. R. A. Beauregard and E. R. Suryanarayan, The Brahmagupta triangles, to appear.
5. L. E. Dickson, *History of the Theory of Numbers, Vol. II*, G. E. Strechert & Co., New York, NY (1934).
6. T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, New York, NY (1951).

NOTES

A Study in Step Size

TEMPLE H. FAY
University of Southern Mississippi
Hattiesburg, MS 39406-5045

While experimenting with giving polar plots some "texture," I discovered an interesting effect that might intrigue students: high sensitivity to step size. The base equation is that used to generate the butterfly curve (see [**1**], for example)

$$r(\theta) = e^{\cos(\theta)} - 2\cos(4\theta),$$

but the technique can be applied, and the same effect observed, using almost any polar equation.

The "texture" is obtained by multiplying this base curve by a rapidly varying sinusoidal factor, in this case by $\sin^4(\lambda\theta)$, where $\lambda = 99999999$. The fourth power was chosen to keep the factor non-negative and small. The value of λ was chosen arbitrarily; any large number would produce the same effect.

Data sets, consisting of points (x_n, y_n) where

$$\rho(\theta) = \left(e^{\cos(\theta)} - 2\cos(4\theta)\right)\sin^4(\lambda\theta)$$

and

$$x_n = \rho(\theta_n)\sin(\theta_n)$$

$$y_n = \rho(\theta_n)\cos(\theta_n),$$

were produced by setting $\theta_0 = 0$, and $\theta_n = \theta_{n-1} + h$ where h denotes the step size, for $0 \le \theta < 2\pi$. (Reversing the sine and cosine from their "usual" positions rotates the butterfly 90^o into the upright position shown.) These data sets contain roughly 11,500 to 42,000 points.

The plots shown on the cover of this issue were produced with step sizes as follows:

$$h_1 = 0.00015 \quad h_2 = 0.0003$$

$$h_3 = 0.0005 \quad h_4 = 0.00055$$

The plots in the following Figure used these step sizes:

$$h_5 = 0.0007 \quad h_6 = 0.000169$$

$$h_7 = 0.000711 \quad h_8 = 0.00071$$

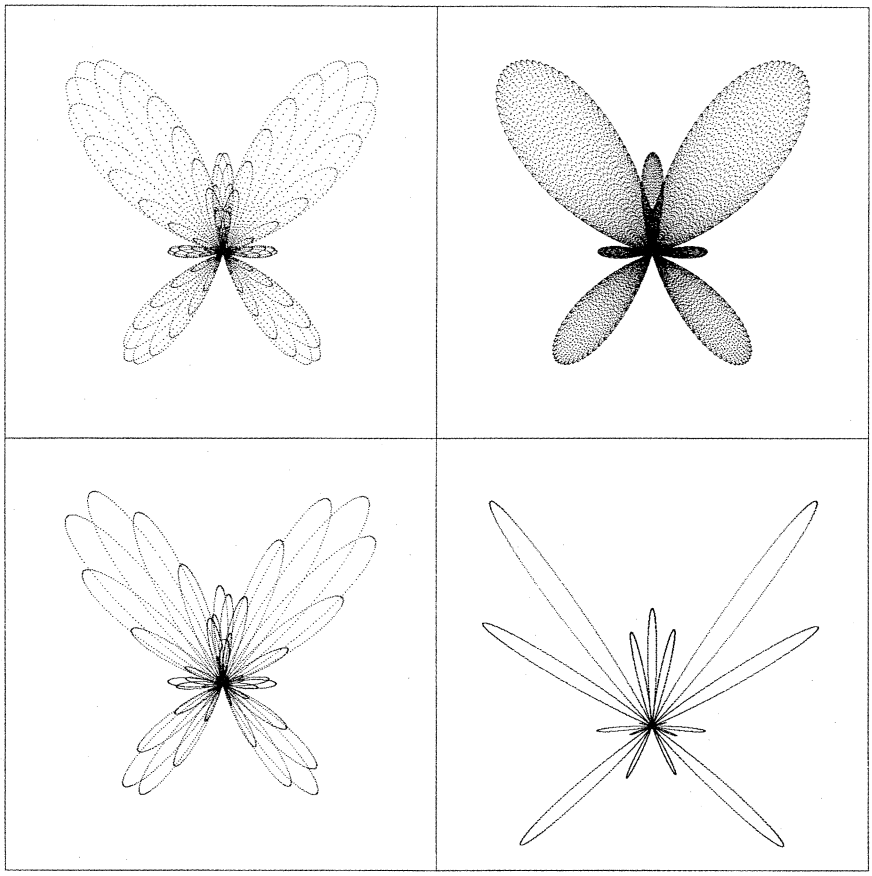


FIGURE
Four butterfly curves

Watching the dynamics of the plotting of the sequentially-generated points (x_n, y_n) is interesting in and of itself. Students might enjoy experimenting with different equations, values of λ, and step sizes.

REFERENCE

1. T. H. Fay, The butterfly curve, *American Mathematical Monthly* 96 (1989), 442–443.

Loosest Circle Coverings of an Equilateral Triangle

HANS MELISSEN
Philips Research Laboratories
Prof. Holstlaan 4, 5656 AA Eindhoven
The Netherlands

1. Introduction The problem of completely covering a circular space painted on a cloth by placing over it, one at a time, five smaller but equal circular tin discs used to be a popular game at English fairs around the turn of the century; see [**4**, **12**]. Its difficulty lies in the restriction that no disc may be moved once it is put down. The size of the discs is of course designed to prevent the unwary player from finding a correct covering without a good deal of trial-and-error. An interesting characteristic from a mathematical point of view is the smallest radius of the tin discs for which the puzzle is solvable. The corresponding solution is the loosest circle covering of the circular disc. Neville showed in 1915 [**11**] that a covering can be found if the radius of the smaller discs exceeds 0.609382864... times that of the large circle. His configuration is shown in FIGURE 1. He actually used this example to illustrate a new method for numerically solving systems of nonlinear equations. Unfortunately, he reported the incorrect value of 0.6094183. In 1983 Károly Bezdek proved the optimality of Neville's configuration (see [**2**, **3**]). Here, again, an incorrect numerical value of

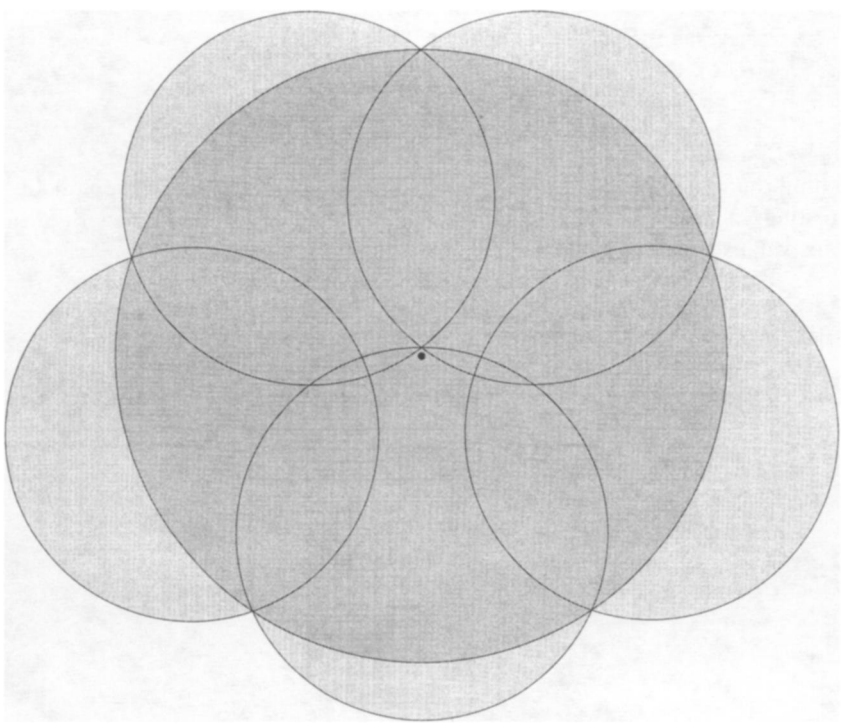


FIGURE 1
Neville's loosest covering of a circle with five circles.

1/1.640... was computed. In his dissertation [1], Bedzek treated the covering of a circle by six circles. The proof is complicated. The cases of two, three, four, and seven circles are easy. The best coverings with eight, nine, ten, and eleven discs were treated by Krotoszyński [6] in 1993, but his proofs are incomplete. Correct proofs for nine and ten discs were found recently by G. Fejes Tóth. Melissen and Schuur have improved Krotoszyński's covering with eleven circles. Further loose coverings with up to 20 discs were given by Zahn [14]. Loose circle coverings of a square with up to 10 circles were given by Tarnai and Gászpár in 1995 [13]. Their conjectures for $n = 6$ and 8 were improved in [10]. Recently, Heppes and Melissen [5] found the optimal coverings of a general rectangle with 2, 3, 4, 5, and 7 circles.

In analogy to covering a circle and a square with circles and packing an equilateral triangle with circles ([7, 8, 9]), we will consider the related problem of covering an equilateral triangle with congruent circular discs. We shall determine the loosest covering for up to six discs. Finally, we will consider some coverings of the triangle with discs that need not be congruent.

The smallest common radius of n congruent closed circular discs that can cover a equilateral triangle of unit edge length (including its interior) will be denoted by τ_n.

2. One disc The unique smallest circle that covers the vertices of the triangle is obviously the circumscribed circle, with radius $\tau_1 = \sqrt{3}/3$ (FIGURE 2a).

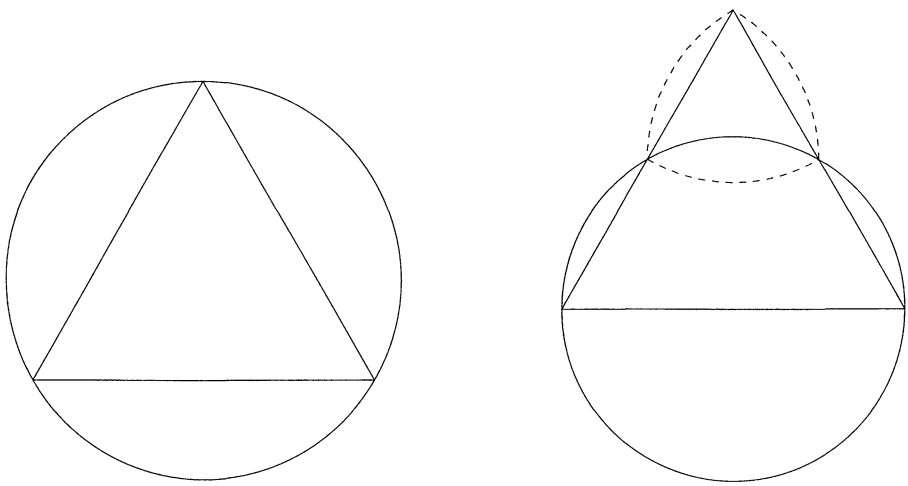


FIGURE 2

Loosest covering of an equilateral triangle with one and two congruent circular discs. The dotted Reuleaux triangle in (b) bounds the possible position of the center of the second disc.

3. Two discs If the vertices of the triangle are covered by two discs, one of the discs must cover two vertices, so $\tau_2 \geq 1/2$. Now suppose that the radius of the two discs is equal to 1/2. The center of one disc must then lie halfway between two vertices. The remaining region can easily be covered by the second disc. Its center can lie anywhere in the dotted Reuleaux triangle of constant width 1/2 indicated in FIGURE 2b. This shows that $\tau_2 = 1/2$ and that the loosest covering is not unique.

4. Three discs Consider the three vertices of the triangle together with its center. Two of these four points must be covered by one of the discs, so $\tau_3 \geq \sqrt{3}/6$. If we

have three discs of radius $\sqrt{3}/6$, then the position of the one that covers two of the four points (the center and a vertex) is fixed. As the center of the triangle lies on the boundary of this disc, it must be covered by yet another disc. The two remaining discs must cover the two uncovered vertices and the center of the triangle, so one of the discs must cover two of these points and is also fixed. The last disc fits in exactly one position to cover the rest of the triangle. Consequently, $\tau_3 = \sqrt{3}/6$, and the corresponding optimal covering is unique, see FIGURE 3a.

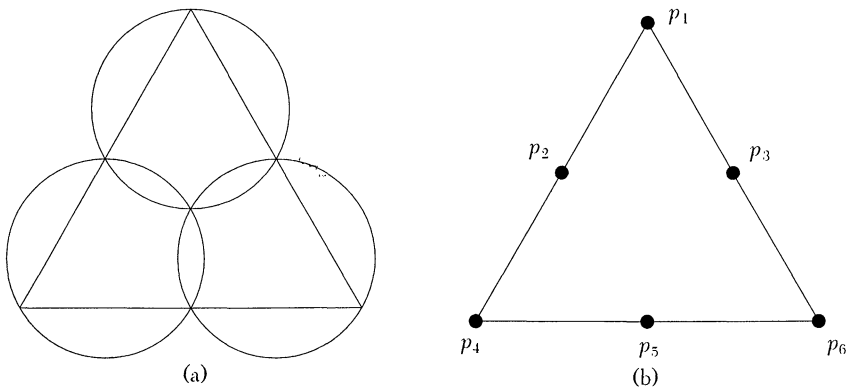


FIGURE 3
Loosest covering of an equilateral triangle with three congruent circular discs (a).

5. Four discs The solution for four discs is less trivial. The discs must cover the three vertices and the three centers of the edges of the triangle in FIGURE 3b. This means that two of these six points must be covered by the same disc, so $\tau_4 \geq 1/4$. Unfortunately, this bound is not sharp; the triangle cannot be covered by four discs of radius $1/4$. The best possible value for the radius turns out to be $\tau_4 = 2 - \sqrt{3} = 0.267949\ldots$.

To show this, take four discs $D_1, \ldots, D_4$ of radius $2 - \sqrt{3}$. No single disc can cover two vertices of the triangle, so each of the three vertices is covered by its own disc (D_1, D_2, D_3). The three discs may be moved such that their centers are inside the triangle and the covered vertex is on the boundary of the covering disc, without destroying the covered property. As the radius of the discs is slightly smaller than $\sqrt{3}/6$, the radius of the incircle of the triangle, the fourth disc D_4 cannot have points in common with all three edges of the triangle. This means that at least one of the edges must be covered by two discs (D_1, D_2), that also cover the two corresponding vertices (see FIGURE 4a). The distance between q_1 and q_2 always exceeds $2(2 - \sqrt{3})$, so q_1 and q_2 cannot be covered by D_4 simultaneously. Therefore, two of the edges must be covered completely by D_1, D_2, and D_3. This is possible in exactly one way (FIGURE 4b). Finally, there is one possible position in which D_4 covers the remainder of the triangle. This configuration is unique up to rotations, so it must be optimal.

6. Five discs Two of the six points $p_1, \ldots, p_6$ in FIGURE 3b must be covered by the same disc, which shows that $\tau_5 \geq 1/4$. The triangle can actually be covered by five discs of radius $1/4$ (see FIGURE 5a), so $\tau_5 = 1/4$. The corresponding solutions are shown in FIGURE 5a. Four discs are fixed. The center of the fifth disk can move inside

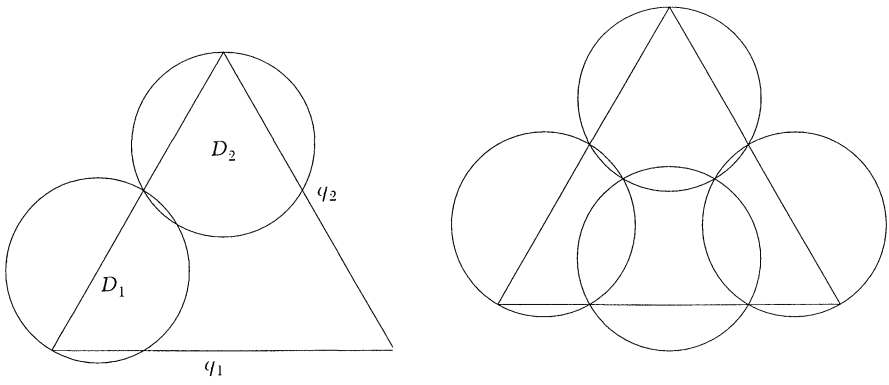


FIGURE 4
Optimal covering with four congruent circles (b).

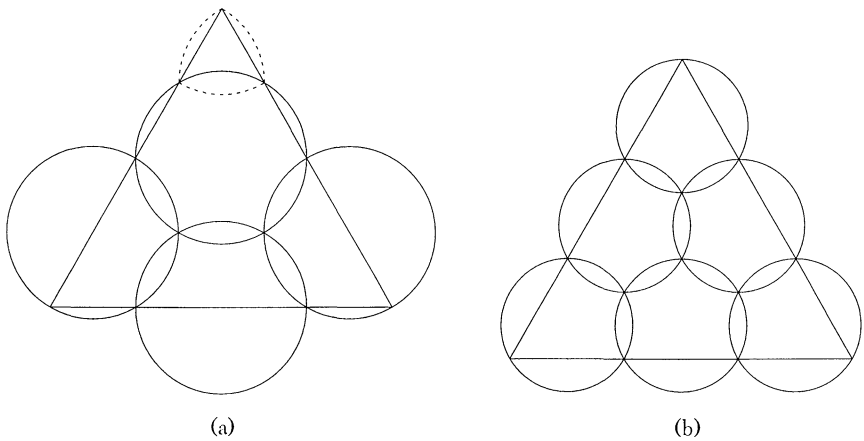


FIGURE 5
Loosest coverings of an equilateral triangle with five and six congruent circles. The dotted Reuleaux triangle in a) encloses the feasible region for the center of the fifth disc.

a small Reuleaux triangle. That all solutions are of this form can be seen by checking a number of possible cases. Two of the six points $p_1, \ldots, p_6$ must be covered by one disc. Apart from rotations and reflections we can assume that either p_1 and p_2 are in one disc, or p_2 and p_3. In the first case all points (except possibly p_1), and in the second case all points must be covered by the remaining four discs, so in both cases there must be another disc that covers two points. We leave the completion of these arguments to the reader.

7. Six discs We will show that $\tau_6 = \sqrt{3}/9$ and that the obvious loosest covering in FIGURE 5b is unique. Suppose that we have a covering with discs of radius $r \leq \tau_6$. Again, there are distinct discs D_1, D_2, and D_3 that cover each of the vertices. The inequality $4r < 1$ shows that no two discs can cover an edge completely and also that two centers of the edges cannot be covered by one disc. Therefore, apart from D_1, D_2, and D_3, there must be a unique disc (D_4, D_5, D_6) associated with each edge. It is easy to see that D_4, D_5, and D_6 must have some point p in common.

To find a lower bound for r we will now determine the maximum length of the boundary of the triangle that can be covered by these six discs. As before, D_1, D_2, and D_3 can be translated until each has a vertex on its boundary. The length of the boundary of the triangle that is covered by such a disc is equal to

$$2r\left[\cos\varphi + \cos\left(\frac{\pi}{3} - \varphi\right)\right] = 2\sqrt{3}\,r\cos\left(\varphi - \frac{\pi}{6}\right),$$

where φ is the angle between the line through the vertex and the center of the disc, and one of the edges of the triangle. This length is maximal for $\varphi = \pi/6$, so $6\sqrt{3}\,r$ is an upper bound for the length covered by D_1, D_2, and D_3. We must also determine the maximum length that can be covered by D_4, D_5, and D_6. First, each disc is pushed outward, perpendicular to the edge it intersects, until either p is on the boundary of the disc, or the maximum length $(2r)$ is covered. The total length covered by D_4, D_5, and D_6 is therefore at most

$$\sum_{i=1}^{3} f(h_i),$$

where the h_i denote the distances from p to each of the edges and

$$\begin{aligned} f(h) &= 2\sqrt{2rh - h^2} \text{ if } r \le h \le 2r, \\ &= 2r \text{ if } h < r. \end{aligned}$$

As f is concave we have that

$$\sum_{i=1}^{3} f(h_i) \le 3f\left(\frac{1}{3}\sum_{i=1}^{3} h_i\right).$$

By computing the area of the triangle in two different ways it is easy to see that

$$h_1 + h_2 + h_3 = \frac{1}{2}\sqrt{3},$$

so the maximum length of the boundary covered by D_4, D_5, and D_6 is at most $\sqrt{12\sqrt{3}\,r - 3}$. The total circumference of the triangle must be covered, so

$$6\sqrt{3}\,r + \sqrt{12\sqrt{3}\,r - 3} \ge 3.$$

This shows that $r \ge \tau_6$. If $r = \tau_6$, all maxima must be assumed to cover the triangle. The only possible covering is shown in FIGURE 5b.

8. Incongruent discs In this last section we will sketch some further questions and results. So far we have used congruent discs to cover the triangle. Can these coverings be improved by relaxing the condition that the discs need to be of equal size? By improving we mean: Can the triangle be covered by circular discs with a smaller total area? This question would be completely uninteresting for circle coverings of a circle, but the solutions for the triangle are nontrivial. For two discs the answer seems simple. A solution that naturally presents itself is to use the fixed disc in FIGURE 2b and to cover the small triangle with a smaller disc. In this way the total area of the

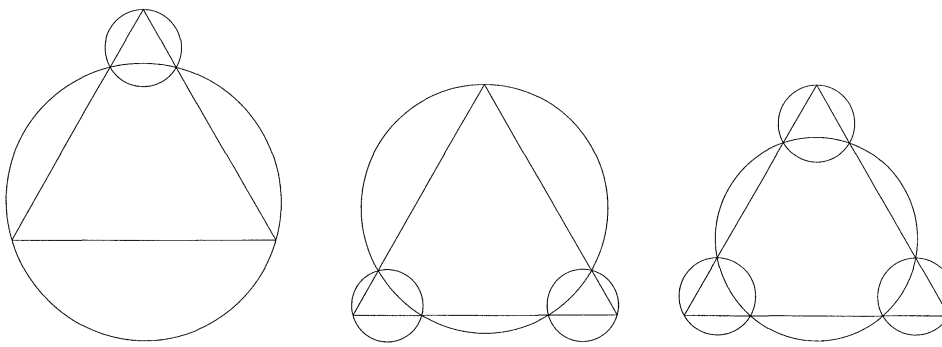
covering discs can be reduced from $\pi/2 = 1.570796\ldots$ to $\pi/3 = 1.047195\ldots$. Surprisingly, this is by no means the best solution! To find the optimal covering we note that one of the discs must cover two vertices, and therefore its radius R must be equal to at least $1/2$. It covers the maximum area of the triangle if the two vertices lie on its boundary. The remaining triangular region needs a disc of radius

$$r = \frac{1}{6}\sqrt{3} - \frac{1}{2}\sqrt{4R^2 - 1}$$

to cover it. The total area of the two discs

$$\pi\left(2R^2 - \frac{1}{6}\sqrt{3}\sqrt{4R^2 - 1} - \frac{1}{6}\right)$$

is maximal for $R = \sqrt{39}/12, r = \sqrt{3}/12$. The total area of the discs in FIGURE 6a is then equal to $7\pi/24 = 0.916297\ldots$.



(a) (b) (c)

FIGURE 6

Loosest covering of an equilateral triangle with two and four circles. The covering with three discs is suboptimal.

Similarly, one might surmise that the covering with three discs can be improved by a configuration like FIGURE 6b. For the best configuration of this form the radius of the largest disc is equal to

$$R = \frac{\sqrt{3}}{4} + \frac{\sqrt{3}}{12}\left(s - \frac{2}{3s} + \frac{1}{3}\right)^2 = 0.466255\ldots \quad \text{where} \quad s = \frac{1}{3}\left(4 + 2\sqrt{58}\right)^{1/3}.$$

The radius of the smaller discs is equal to $0.134921\ldots$. This covering is only suboptimal. The total area of the discs is $0.797341\ldots$, compared to $\pi/4 = 0.785398\ldots$ for the original covering.

To show that the covering in FIGURE 3a is also the best solution here, suppose that we have a covering with three discs of radius r_1, r_2, and r_3. As we already have a

covering with an area of $\pi/4$, each radius must be smaller than $1/2$, so each of the vertices must be covered by its own disc. We can assume that this vertex lies on the boundary of the disc. The length of the boundary of the triangle covered by such a disc is at most $2\sqrt{3}\,r_j$ if $r_j \le \sqrt{3}/4$ and $2\sqrt{3}\,r_j + \sqrt{4\sqrt{3}\,r_j - 3}$ if $r_j \ge \sqrt{3}/4$. Only one of the discs can have a radius that is larger than $\sqrt{3}/4$. First, consider the case that all radii are smaller than $\sqrt{3}/4$. The maximum length covered, $2\sqrt{3}(r_1 + r_2 + r_3)$, under the restriction that $r_1^2 + r_2^2 + r_3^2 \le 1/4$ is then assumed for $r_1 = r_2 = r_3 = \sqrt{3}/4$. This is the covering shown in FIGURE 3a. In the situation that one of the discs has a radius that exceeds $\sqrt{3}/4$, we must find the maximum of $2\sqrt{3}(r_1 + r_2 + r_3) + \sqrt{4\sqrt{3}\,r_1 - 3}$ under the restriction that $r_1^2 + r_2^2 + r_3^2 \le 1/4$. This maximum is assumed for $r_1 = 0.459920\ldots$ and $r_2 = r_3 = 0.138695\ldots$ and has the value $2.985892\ldots$. As this value is smaller than 3, the circumference of the triangle cannot be covered completely, so FIGURE 3a remains the best solution.

By using similar arguments it can be seen that the loosest covering with four circular discs is shown in FIGURE 6c. The radius of the large disc is equal to $\sqrt{21}/12$, and the smaller discs have a radius of $\sqrt{3}/12$. This covering improves the area of the discs from $4(7 - 4\sqrt{3})\pi = 0.902224\ldots$ for a covering with congruent discs to $5\pi/24 = 0.654498\ldots$.

REFERENCES

1. K. Bezdek, *Körök optimális fedései* (Optimal Covering of Circles), Dissertation, Budapest (1979).
2. K. Bezdek, Über einige Kreisüberdeckungen, *Beitr. Alg. Geom.* 14 (1983), 7–13.
3. K. Bezdek, Über einige optimale Konfigurationen von Kreisen, *Ann. Univ. Sci. Budapest Eötvös Sect. Math.* 27 (1984), 143–151.
4. H. T. Croft, K. J. Falconer and R. K. Guy, *Unsolved Problems in Geometry*, Springer-Verlag, Berlin, 1991, 111.
5. A. Heppes and J. B. M. Melissen, Covering a rectangle with equal circles, submitted.
6. S. Krotoszyński, Covering a disk with smaller disks, *Studia Scient. Math. Hungar.* 28 (1993), 277–283.
7. J. B. M. Melissen, Densest packings of congruent circles in an equilateral triangle, *Amer. Math. Monthly* 100 (1993), 916–925.
8. J. B. M. Melissen, Optimal packings of eleven equal circles in an equilateral triangle, *Acta Math. Hung.* 65 (1994), 389–393.
9. J. B. M. Melissen and P. C. Schuur, Packing 16, 17 and 18 circles in an equilateral triangle, *Discrete Math.* 145 (1995), 333–342.
10. J. B. M. Melissen and P. C. Schuur, Improved coverings of a square with six and eight equal circles, *Electronic J. Combin.* **3** (1996) R32, 8 pp.
11. E. H. Neville, On the solutions of numerical functional equations, illustrated by an account of a popular puzzle and of its solution, *Proc. London Math. Soc.* (2) 14 (1915), 308–326.
12. W. W. Rouse Ball and H. S. M. Coxeter, *Mathematical Recreations and Essays*, Dover Publications, New York, 1987 (first original edition 1892), 97–99.
13. T. Tarnai and Z. Gászpár, Covering a square by equal circles, *Elem. Math.* 50 (1995), 167–170.
14. C. T. Zahn, Black box maximization of circular coverage, *J. Res. Nat. Bur. Standards* 66B (1962), 181–216.

The Smallest Equilateral Cover for Triangles of Perimeter Two

JOHN E. WETZEL
University of Illinois
Urbana, IL 61801

In an obscure but interesting pamphlet [7], Josiah Smith[1] announced his belief that every triangle of perimeter two can be covered by an equilateral triangle of side one. "Experiments suggest," he wrote, "that every triangle with perimeter two can be placed in an equilateral triangle of side one, although I cannot establish this fact in fullsome rigour. ... No smaller equilateral triangle has this property, because flat isosceles triangles of base $1-\delta$ and equal sides $\frac{1}{2}+\frac{\delta}{2}$ must fit."

In this note we solve Smith's problem by determining the side of the smallest equilateral triangle (i.e., closed equilateral-triangular region) that can cover every triangle of perimeter two, and we discover that Smith's intuition was not correct: a side longer than one is required. We show that the smallest equilateral triangle T_0 that can cover every triangle with perimeter two has side $s_0 := 2/m_0$, where m_0 is the global minimum of the trigonometric function

$$f(x) := \sqrt{3}\left(1+\sin\frac{x}{2}\right)\cdot\sec\left(\frac{\pi}{6}-x\right) \tag{1}$$

on the interval $[0,\frac{\pi}{6}]$ (see FIGURE 1). A little numerical work[2] (the details of which we omit) shows that the global minimum value $m_0 \approx 1.99431$ occurs at the (unique) point $x_0 \approx 0.074733$, approximately 4.28186°; so the side s_0 of T_0 is about $s_0 \approx 1.002851$.

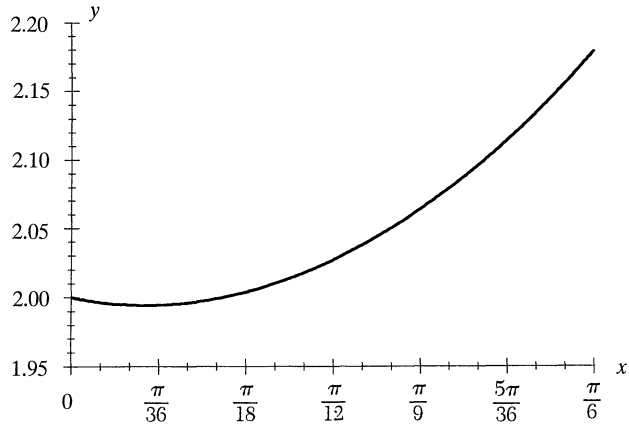


FIGURE 1
$f(x) = \sqrt{3}(1+\sin x/2)\sec(\pi/6-x)$ for $0 \le x \le \pi/6$.

We begin by proving that an equilateral triangle of side s contains a relatively large triangle of each possible shape; then scaling shows that T_0 can accommodate every

[1] Also the author of a seminal book [6] on arrangements of hyperplanes. (See Zaslavsky [11].)

[2] I want to express my gratitude to Steven Knox and Paul McCreary for (independently) coaxing these numerical results out of *Mathematica*.

triangle of perimeter two (Corollary 2). In Theorem 3 we show that no smaller equilateral triangle has this property. The note concludes with a few remarks about some closely related problems.

Write $T(s)$ for the equilateral triangle of side s (so that $T_0 = T(s_0)$), and let $p(\triangle)$ be the perimeter of triangle $\triangle$.

THEOREM 1. *For any given triangle* $\triangle$, *the equilateral triangle* $T(s)$ *with side* s *contains a triangle* $\triangle^*$ *similar to* $\triangle$ *with perimeter* $p(\triangle^*) \geq m_0 s$.

Proof. We build such a triangle $\triangle^*$ for each given triangle $\triangle$. Suppose first that some two angles of $\triangle$ are not larger than 60°, and arrange the notation so that $\angle Q \leq 60°$ and $\angle R \leq 60°$. Then there is a point X in $T(s)$ so that $\triangle^* := XBC \sim PQR = \triangle$. Then $p(\triangle^*) = p(XBC) \geq 2s > m_0 s$.

In the contrary case there are two vertices at which the angles are both larger than 60°. Arrange the notation so that $\angle Q > 60°$ and $\angle R > 60°$. The argument depends on the size of the third angle $\angle P$.

Suppose that $\angle Q > 60°$, $\angle R > 60°$, and $\angle P \geq 30°$, so that both $\angle Q$ and $\angle R$ are acute. Let M be the midpoint of BC, and take points Y on BM and Z on MC so that $\angle AYM = \angle Q$ and $\angle AZM = \angle R$; then $\triangle^* := AYZ \sim PQR = \triangle$. To show that $p(\triangle^*) \geq m_0 s$ we argue geometrically. Let Y_1 and Z_1 be the points on BC so that M is the midpoint of the segment Y_1Z_1 and $Y_1Z_1 = YZ$ (see FIGURE 2). Then $\angle Y_1AZ_1 \geq \angle YAZ = \angle P \geq 30°$, and $AY_1 + AZ_1 \leq AY + AZ$. (It is an elementary exercise to show that if a point E is not on a line l and points F and G on l are d apart, then $\angle FEG$ is maximized and $EF + EG$ is minimized when F and G are symmetrically located about the foot of the perpendicular from E to l.) Consequently AY_1Z_1 surrounds an isosceles triangle AY_2Z_2 with apex angle 30° at A and altitude $(\sqrt{3}/2)s$, whose perimeter is $\sqrt{3}\,s(\sec 15° + \tan 15°) > 2.25s$. Hence $p(\triangle^*) = p(AYZ) \geq p(AY_1Z_1) \geq p(AY_2Z_2) > 2.25s > m_0 s$.

Finally, suppose that $60° < \angle Q \leq \angle R$, and $\angle P < 30°$. Then there are points Y on AB and Z on BC so that $\triangle^* := AYZ \sim PQR = \triangle$ (see FIGURE 3). To establish that $p(\triangle^*) \geq m_0 s$ we again argue geometrically. Since $AY \geq AZ$ there is a point S on AY with $AS = AZ$. Then the isosceles triangle $\triangle_1 := ASZ$ has apex angle $\angle P < 30°$; and, writing $\angle P = x$ (and switching to radians), we see that $AZ = (\sqrt{3}/2)s \cdot \sec(\pi/6 - x)$. Since $SZ = 2\,AZ \sin x/2$, it follows that $p(\triangle_1) = s \cdot f(x) \geq m_0 s$, where f is defined by (1). Consequently $p(\triangle^*) \geq p(\triangle_1) \geq m_0 s$.

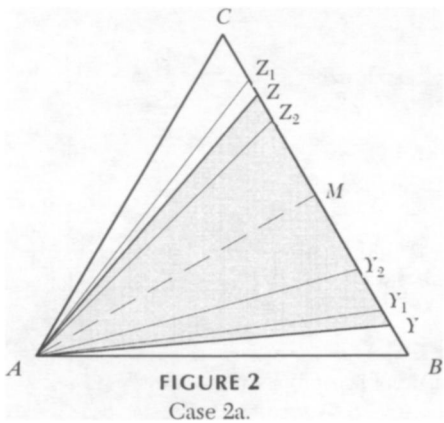


FIGURE 2
Case 2a.

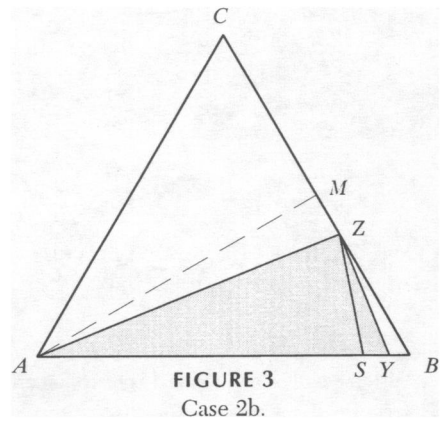


FIGURE 3
Case 2b.

Scaling shows that the equilateral triangle T_0 can cover every triangle of perimeter two:

COROLLARY 2. *If $s \geq s_0 = 2/m_0$, then the equilateral triangle $T = T(s)$ can cover every triangle of perimeter two. In particular, T_0 can cover every such triangle.*

Proof. If $s \geq s_0$, then according to Theorem 1, for every triangle $\triangle$ of perimeter two there is a triangle $\triangle^*$ in $T(s)$ similar to $\triangle$ whose perimeter is at least $m_0 s \geq m_0(2/m_0) = 2$. So the triangle $\triangle$, which certainly fits in the *larger* triangle $\triangle^*$, surely fits in $T(s)$.

To see that no smaller equilateral triangle has this property, we examine an isosceles triangle that gives the equality in the inequality of Theorem 1 and show that it fits in no smaller equilateral triangle.

THEOREM 3. *If an equilateral triangle $T(s)$ can cover every triangle of perimeter two, then $s \geq s_0$.*

Proof. Let $\triangle_0$ be the isosceles triangle of perimeter two whose apex angle is the angle x_0. (See the shaded triangle in FIGURES 4 and 5.) The two equal sides of $\triangle_0$ have lengths

$$l := \left(1 + \sin\frac{x_0}{2}\right)^{-1} \approx 0.96399,$$

and the base has length $2l \cdot \sin x_0/2 \approx 0.072025$. Note that the altitude $h_0 = l \cdot \cos x_0/2$ of $\triangle_0$ exceeds 0.96.

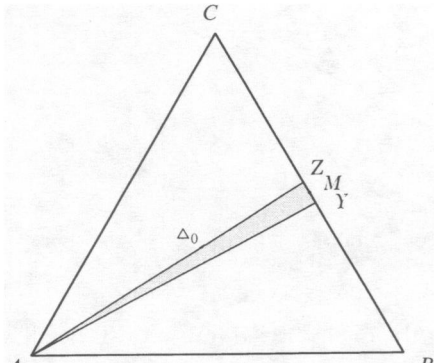


FIGURE 4
A non-minimal configuration.

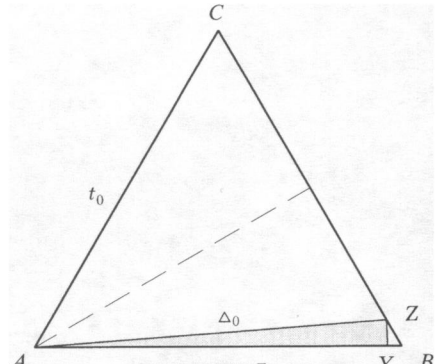


FIGURE 5
The minimal configuration.

Let t_0 be the side of the smallest equilateral triangle that can accommodate $\triangle_0$. (The existence of such a triangle is an elementary consequence of compactness.) Evidently $t_0 \leq s_0 = 2/m_0$. We investigate how $T(t_0)$ might fit around $\triangle_0$.

First of all, it is clear that all three vertices of $\triangle_0$ must lie on the sides of $T(t_0)$, because otherwise a suitable small motion would move $\triangle_0$ entirely inside, contrary to the minimality of t_0.

Suppose that one side of $T(t_0)$ contains the base of $\triangle_0$. Then the minimality requires that the apex of $\triangle_0$ be the opposite vertex of $T(t_0)$, and we can arrange the notation so that $T(t_0) = ABC$ and $\triangle_0 = AYZ$, with Y and Z on BC located symmetrically about the midpoint M of BC (see FIGURE 4). Then $(\sqrt{3}/2)t_0 = h_0 > 0.96$, so that $t_0 > 1.1$, contrary to $t_0 \leq s_0$. So no side of $T(t_0)$ contains the base of $\triangle_0$.

Suppose next that one side of $T(t_0)$ contains one of the two equal sides of $\triangle_0$. Then the minimality requires that the apex of $\triangle_0$ be at a vertex of $T(t_0)$, and we can arrange the notation so that $T(t_0) = ABC$ and $\triangle_0 = AYZ$, with Y on AB and Z on BC (see FIGURE 5, cf. FIGURE 3). Then $2 = p(\triangle_0) = t_0 f(x_0) = t_0 m_0$, so that in this case $t_0 = 2/m_0 = s_0$. Our claim is that this is the minimal configuration.

Suppose finally that each vertex of $\triangle_0$ lies on a different side of an equilateral triangle $T(t) = DEF$, and arrange the notation so that the apex of $\triangle_0$ lies on DF nearer D than F and the base vertices lie on DE and EF (as in FIGURE 6, which also shows triangle $T(t_0) = ABC$ in the position described in the previous paragraph, with the base vertices of $\triangle_0$ on AB and BC and the apex of $\triangle_0$ at A). Now an elegant geometric argument of Ross Honsberger (see p. 36 of [4]) shows that $t > t_0$. Indeed, in the notation of FIGURE 6, where P and Q are the centers of the two 240° arcs outward on the two equal sides of $\triangle_0$ in which the 60° angles of $T(t)$ and $T(t_0)$ at A, C, D, and F are inscribed, $PU \perp QA$, $QV \perp AD$, and $PV \perp QV$, and $W = QA \cap PV$, we see that $t = 2VP > 2WP > 2UP = t_0$. So no equilateral triangle T having each vertex of $\triangle_0$ on a different side of T can be minimal[3].

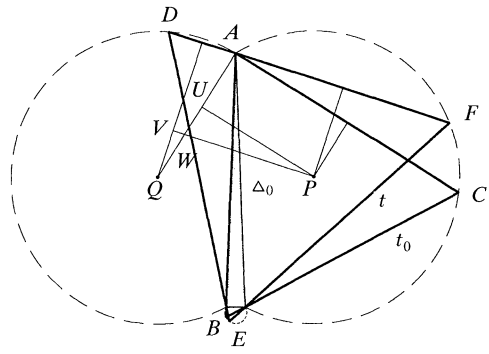


FIGURE 6
Comparison of two configurations.

So, as claimed, the minimal configuration is the one pictured in FIGURE 5. It follows that an equilateral triangle $T(s)$ of side s that can accommodate every triangle of perimeter two, which must, in particular, accommodate $\triangle_0$, must have side $s \geq t_0 = s_0$.

Combining the assertions of Corollary 2 and Theorem 3 gives us the solution to Smith's problem:

THEOREM 4. *The equilateral triangle $T_0 = T(s_0)$ is the smallest equilateral triangle that can accommodate every triangle of perimeter* 2.

[3] In fact, this possibility is already ruled out by a recent nice result of K. A. Post [5], who proved that if a triangle ABC contains a triangle PQR, then it also contains a triangle congruent to PQR having two of its vertices on the same side of ABC.

It is worth noting that since the extremal triangles are isosceles, one need not minimize over all similarity classes—the isosceles triangles are enough. So we find:

THEOREM 5. *The equilateral triangle* $T_0 = T(s_0)$ *is the smallest equilateral triangle that can cover every isosceles triangle of perimeter* 2.

It would be very interesting to solve Smith's problem more generally for arbitrary triangular covers: find the size of the smallest triangle similar to a given triangle that can accommodate every triangle of perimeter two. This is likely to be difficult.

Smith's problem can also be generalized in a different direction. For each $n \geq 2$ let s_n be the side of the smallest equilateral triangle that can accommodate every closed polygonal path of n segments and length two (so that $s_2 = 1, s_3 = 2/m_0 \approx 1.00285$, etc.). The precise determination of s_n for $n \geq 4$ appears very difficult, but it is easy to see that the sequence (s_n) increases to the limit $2\sqrt{3}/\pi \approx 1.10266$. Since any closed curve of length two surely lies in the disk of radius one whose center is any point of the curve and consequently in an equilateral triangle of side $2\sqrt{3}$, the sequence (s_n) is surely bounded. (Indeed, every closed curve of length two lies in some disk of *diameter* one (see Wetzel [**10**], Chakerian and Klamkin [**1**]) and consequently in an equilateral triangle of side $\sqrt{3}$.)

THEOREM 6. *For each* $n = 2, 3, 4, \ldots, s_{n+1} \geq s_n$, *and* $\lim(s_n) = 2\sqrt{3}/\pi$.

Proof. The bounded sequence (s_n) is clearly increasing (because each n-segment closed polygonal path of length two becomes an $(n+1)$-segment polygonal path of length two when a new vertex is inserted into any edge), and consequently it converges, say to s_0. Writing r_n for the regular n-gon of perimeter two with center at a point P, and writing c for the circle of circumference two having the same center, we recall that $r_n \to c$ in the sense of the Hausdorff metric. Since the side of the equilateral triangle whose inscribed circle has circumference two is $2\sqrt{3}/\pi$, it follows that $s_0 \geq 2\sqrt{3}/\pi$. On the other hand, it is a consequence of an inequality proved by Eggleston [**3**] that an arbitrary triangle can accommodate every closed curve whose length is the same as the circumference of its inscribed circle (see Wetzel [**8**], [**9**]; Chakerian and Klamkin [**1**]). So $s_0 \leq 2\sqrt{3}/\pi$.

Smith [**7**] makes unsupported assertions about a variety of other covering problems. He declares, for example, that the smallest equilateral triangle that can accommodate every triangle of diameter 1 has side $(2\sqrt{3}/3)\cos 10° \approx 1.13716$, and he asserts that the smallest disk that can cover every triangle of perimeter two has radius $2\sqrt{3}/9 \approx 0.38490$. We leave the investigation of these two (correct) claims as exercises for the reader.

There are many similar covering problems in the literature, most of them unsolved and seemingly beyond reach. For a glimpse of this literature, see the wonderful survey put together by Croft, Falconer, and Guy [**2**].

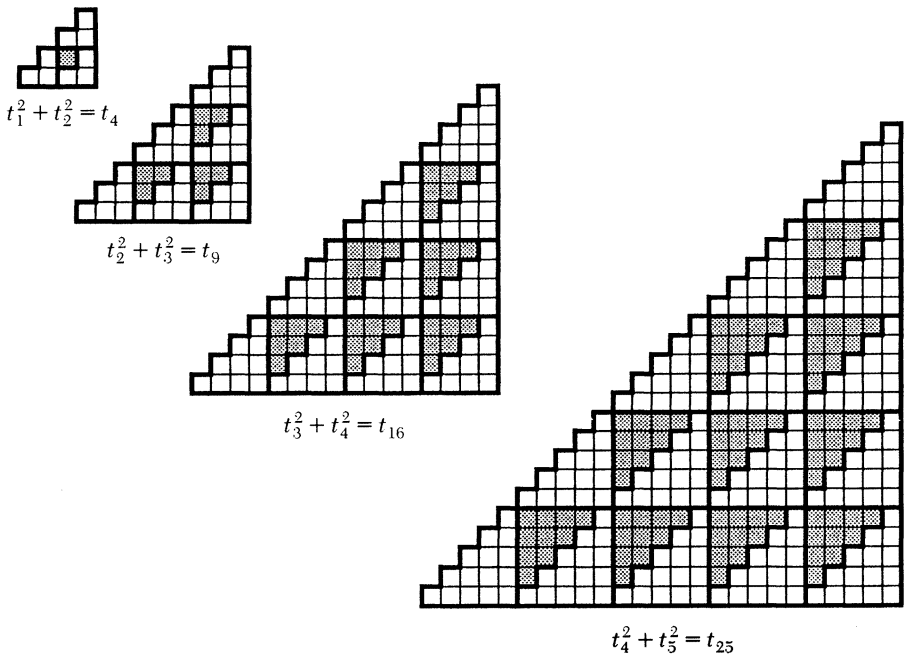
Acknowledgment. It is a pleasure to acknowledge insightful suggestions by the editor and referees.

REFERENCES

1. G. D. Chakerian and M. S. Klamkin, Minimal covers for closed curves, this MAGAZINE 46 (1973), 55–61.
2. Hallard T. Croft, Kenneth J. Falconer, and Richard K. Guy, *Unsolved Problems in Geometry*, Springer-Verlag, New York, NY, 1991.
3. H. G. Eggleston, *Problems in Euclidean Space: Applications of Convexity*, Pergamon, New York, NY 1957.
4. Ross Honsberger, *Mathematical Gems*, MAA, Washington, DC, 1973.
5. K. A. Post, Triangle in a triangle: on a problem of Steinhaus, *Geom. Dedicata* 45 (1993), 115–120.

6. Josiah Smith, *Arranging Hyperplanes in the Home*, Pan, London, UK, 1926.
7. Josiah Smith, *Triangles of the Triassic*, Pan, London, UK, 1922.
8. John E. Wetzel, Triangular covers for closed curves of constant length, *Elem. Math.* 25 (1970), 78–81.
9. John E. Wetzel, On Moser's problem of accommodating closed curves in triangles, *Elem. Math.* 27 (1972), 35–36.
10. John E. Wetzel, Covering balls for curves of constant length, *Enseignement Math.* 17 (1971), 275–277.
11. Thomas Zaslavsky, *Facing Up to Arrangements: Face-count Formulas for Partitions of Space by Hyperplanes*, Memoirs AMS 154, American Mathematical Society, Providence, RI, 1975.

Proof Without Words: The Sum of the Squares of Consecutive Triangular Numbers Is Triangular



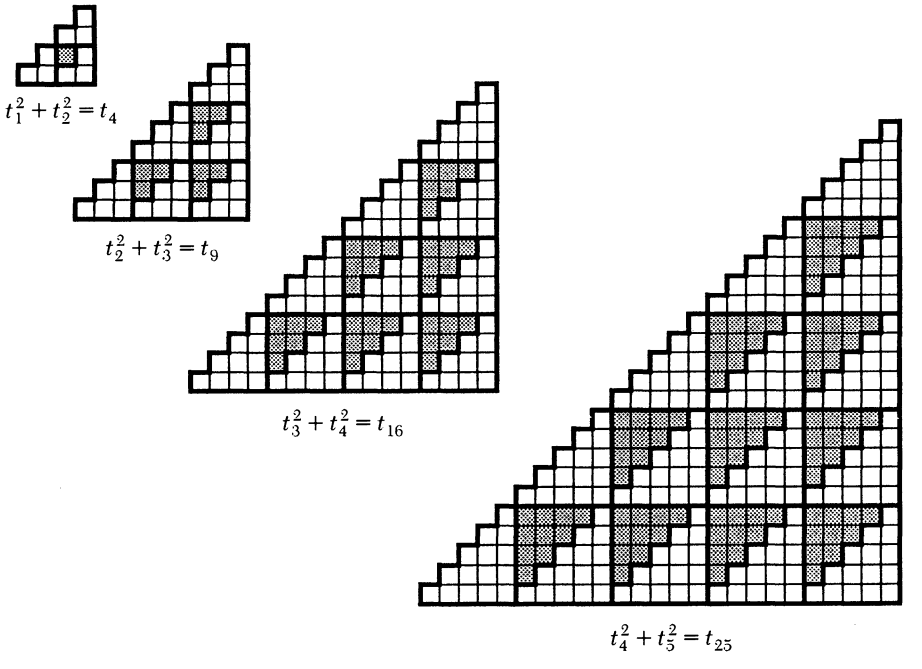
$$t_n = 1 + 2 + \cdots + n \Rightarrow t_{n-1}^2 + t_n^2 = t_{n^2}$$

NOTE: This is a companion result to the more familiar $t_{n-1} + t_n = n^2$: 

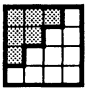
—ROGER B. NELSEN
LEWIS & CLARK COLLEGE
PORTLAND, OR 97219

6. Josiah Smith, *Arranging Hyperplanes in the Home*, Pan, London, UK, 1926.
7. Josiah Smith, *Triangles of the Triassic*, Pan, London, UK, 1922.
8. John E. Wetzel, Triangular covers for closed curves of constant length, *Elem. Math.* 25 (1970), 78–81.
9. John E. Wetzel, On Moser's problem of accommodating closed curves in triangles, *Elem. Math.* 27 (1972), 35–36.
10. John E. Wetzel, Covering balls for curves of constant length, *Enseignement Math.* 17 (1971), 275–277.
11. Thomas Zaslavsky, *Facing Up to Arrangements: Face-count Formulas for Partitions of Space by Hyperplanes*, Memoirs AMS 154, American Mathematical Society, Providence, RI, 1975.

Proof Without Words: The Sum of the Squares of Consecutive Triangular Numbers Is Triangular



$$t_n = 1 + 2 + \cdots + n \Rightarrow t_{n-1}^2 + t_n^2 = t_{n^2}$$

NOTE: This is a companion result to the more familiar $t_{n-1} + t_n = n^2$: 

—ROGER B. NELSEN
LEWIS & CLARK COLLEGE
PORTLAND, OR 97219

Fibonacci With a Golden Ring

KUNG-WEI YANG
Western Michigan University
Kalamazoo, MI 49008

1. Introduction A popular application of linear algebra is to use the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ (or $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$) to derive an explicit formula for the Fibonacci numbers ($F_0 = 0, F_1 = 1, 1, 2, 3, 5, 8, 13, \ldots, F_{n+2} = F_{n+1} + F_n, \ldots$) in terms of the golden ratio $\phi = (1 + \sqrt{5})/2$ and its conjugate $\overline{\phi} = (1 - \sqrt{5})/2$ (e.g., [**4**, p. 252]). We would like to show that if you play with the matrix A a little, adding, subtracting, multiplying, and exponentiating, you will soon find yourself in the higher domain $\mathbb{Z}[A]$ and rewarded with a spectacular view of much of the beautiful Fibonacci landscape, instead of just one formula. From there, you will be able to see a unified proof of a number of familiar Fibonacci identities, such as

$$F_{\gcd(m,n)} = \gcd(F_m, F_n),$$

and

$$F_m F_{n+p} - F_{m+p} F_n = (-1)^p (F_{m-p} F_n - F_m F_{n-p}),$$

and some not-so-familiar ones, like

$$F_m + F_{m+r} + F_{m+2r} + \cdots + F_{m+nr} = \frac{1}{1 + (-1)^r - L_r} \left[F_m - F_{m+(n+1)r} + (-1)^r (F_{m+nr} - F_{m-r}) \right].$$

You will also find that, under an isomorphism between the ring $\mathbb{Z}[\phi]$ and the ring of generalized Fibonacci sequences (see Section 3), the Fibonacci sequence and the Lucas sequence ($L_0 = 2, L_1 = 1, 3, 4, 7, 11, 18, 29, \ldots$) correspond to 1 and $\sqrt{5}$, respectively.

2. Golden matrix ring The simplest ring generated by the matrix A is $\mathbb{Z}[A]$, the ring of polynomials in A with integer coefficients. In $\mathbb{Z}[A]$, $A^2 - A - I = 0$ because the characteristic polynomial of A is $\det(XI - A) = X^2 - X - 1$ (which is also the characteristic polynomial of the Fibonacci recurrence relation $F_{n+2} = F_{n+1} + F_n$). Since ϕ is the positive root of the polynomial $\phi^2 - \phi - 1 = 0$, $\mathbb{Z}[A]$ and $\mathbb{Z}[\phi]$ are isomorphic under the eigenvalue map $\mathscr{E}$: $\mathbb{Z}[A] \to \mathbb{Z}[\phi]$ determined by $\mathscr{E}(A) = \phi$ and $\mathscr{E}(I) = 1$.

The interesting ring $\mathbb{Z}[\phi]$ is fully discussed in the classic *An Introduction to the Theory of Numbers*, by Hardy and Wright [**2**]. We know:

i. the ring $\mathbb{Z}[\phi]$ is a Euclidean domain;
ii. the units of $\mathbb{Z}[\phi]$ are the numbers $\pm\phi^{\pm n}$ $(n = 0, 1, 2, \ldots)$;
iii. the primes of $\mathbb{Z}[\phi]$ are (i) $\sqrt{5}$, (ii) the rational primes $5n \pm 2$, (iii) the factors $(a + b\phi)$ of rational primes $5n \pm 1$ (and the associates of these numbers).

By the isomorphism $\mathscr{E}$, $\mathbb{Z}[A]$ shares the same properties. In particular, the units of $\mathbb{Z}[A]$ are the matrices $\pm A^{\pm n}$ $(n = 0, 1, 2, \ldots)$, and the prime corresponding to $\sqrt{5}$ is $-I + 2A$. It is natural to call $\mathbb{Z}[A]$ the *golden matrix ring*.

When there is no danger of confusion, we will identify aI with a, omitting the symbol I. The *conjugate* of $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ is $\bar{A} = -A^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$. Therefore, $A\bar{A} = -I$, and $A + \bar{A} = I$. The conjugate of $a + bA$ is $a + b\bar{A}$. Conjugation is an automorphism. Mimicking the terminology for the complex numbers, we will call b the *golden part* of $(a + bA)$, and denote it by $\mathscr{G}(a + bA) = b$. It is obvious that $\mathscr{G}: \mathbb{Z}[A] \to \mathbb{Z}$ is a linear map. The *norm* of $a + bA$ is defined to be $N(a + bA) = (a + bA)(a + b\bar{A}) = a^2 + ab - b^2$. Note that $N(a + bA) = \det(aI + bA) = \det\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}$, and so the norm map is multiplicative in the sense that

$$N((a + bA)(a' + b'A)) = N(a + bA)\,N(a' + b'A).$$

3. The ring of generalized Fibonacci sequences Consider the set $\mathbb{F}$ of all integer sequences $\{G_n\}_{n=0}^{\infty}$ satisfying the recurrence relation $G_{n+2} = G_{n+1} + G_n$, regardless of the initial conditions. A. F. Horadam **[3]** calls such sequences *generalized Fibonacci sequences*. Observe that $\mathbb{F}$ is an abelian group under the addition $\{G_n\} + \{H_n\} = \{G_n + H_n\}$. Define the matrix map $\mathscr{M}: \mathbb{F} \to \mathbb{Z}[A]$ by

$$\mathscr{M}(\{G_n\}) = (G_1 - G_0)I + G_0 A.$$

$\mathscr{M}$ is clearly a group homomorphism. Furthermore, by a simple induction (using $A^2 = A + I$), we have

$$G_{n-1} + G_n A = A^n \mathscr{M}(\{G_n\}). \tag{1}$$

Consequently,

$$G_n = \mathscr{G}(A^n \mathscr{M}(\{G_n\})). \tag{2}$$

Define the sequence map $\mathscr{S}: \mathbb{Z}[A] \to \mathbb{F}$ by

$$\mathscr{S}(a + bA) = \{\mathscr{G}(A^n(a + bA))\}.$$

Then $\mathscr{S}$ is also a group homomorphism, $\mathscr{S}(\mathscr{M}(\{G_n\})) = \{G_n\}$, and $\mathscr{M}(\mathscr{S}(a + bA)) = (a + bA)$. Thus, $\mathscr{M}$ and $\mathscr{S}$ form an inverse pair of group isomorphisms. We may now transfer the multiplicative structure of $\mathbb{Z}[A]$ to $\mathbb{F}$ via $\mathscr{M}$ and $\mathscr{S}$. We define $\{G_n\}\{H_n\} = \mathscr{S}(\mathscr{M}(\{G_n\})\mathscr{M}(\{H_n\}))$ and denote it by $\{(GH)_n\}$. With this multiplication, $\mathbb{F}$ becomes a ring, and the maps $\mathscr{M}: \mathbb{F} \to \mathbb{Z}[A]$ and $\mathscr{S}: \mathbb{Z}[A] \to \mathbb{F}$ are isomorphisms of rings, and all previously defined notions become operational in $\mathbb{F}$. Here are two familiar sequences:

$$\{F_n\} = \mathscr{S}(I) = \{\mathscr{G}(A^n)\}$$

is the *Fibonacci sequence*, and

$$\{L_n\} = \mathscr{S}(-I + 2A)$$

is the *Lucas sequence*. Thus, under the isomorphism $\mathscr{E} \circ \mathscr{M}: \mathbb{F} \to \mathbb{Z}[\phi]$, the Fibonacci sequence corresponds to 1, and the Lucas sequence to $\sqrt{5}$. The following special case of (1) is well-known:

$$(F_{n-1} + F_n A) = A^n. \tag{3}$$

4. Extensions and applications The isomorphisms just discussed lead easily to various properties of the Fibonacci sequence.

Negative Indices. Because $N(A) = \det\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = -1$, A is a unit. Thus identity (1) and hence also (2) and (3) are easily seen to hold for negative exponents and indices $(\ldots -3, 2, -1, 1, F_0 = 0, F_1 = 1, 1, 2, 3, \ldots)$. Indeed, for all n,

$$F_{-n} = (-1)^{n+1} F_n,$$

because

$$F_{-n} = \mathcal{G}(A^{-n}) = \mathcal{G}(F_{n-1} + F_n A)^{-1} = \mathcal{G}\left(\left(F_{n-1} + F_n \bar{A}\right)/N(A^n)\right) = (-1)^{n+1} F_n.$$

Divisors. By (3), we have that

$$A^{m+pn} = A^m (F_{p-1} + F_p A)^n = \sum_{i=0}^{n} \binom{n}{i} (F_p)^i (F_{p-1})^{n-i} A^{m+i}.$$

Applying (2), we get

$$G_{m+np} = \sum_{i=0}^{n} \binom{n}{i} (F_p)^i (F_{p-1})^{n-i} G_{m+i}.$$

Letting $\{G_n\}$ be the Fibonacci sequence $\{F_n\}$, setting $m = 0$, and noting that $F_0 = 0$, we obtain

$$F_{np} = F_p \left(\sum_{i=1}^{n} \binom{n}{i} (F_p)^{i-1} (F_{p-1})^{n-i} F_i \right).$$

From this identity we immediately deduce:

If d divides n, then F_d divides F_n.

If $d = \gcd(m, n)$, then there exist integers x and y such that $mx + ny = d$. Expressing $A^{mx+ny} = A^d$ in the form

$$(F_{mx-1} + SF_m A)(F_{ny-1} + TF_n A) = (F_{d-1} + F_d A),$$

where S and T are integers, and comparing the golden parts, we see that F_d is a linear combination of F_m and F_n. This proves that

$$F_{\gcd(m,n)} = \gcd(F_m, F_n).$$

Further Identities. Many Fibonacci identities can be given routine, uniform proofs using (2). For instance, the identity

$$F_{n-1} + F_{n+1} = L_n$$

follows from

$$F_{n-1} + F_{N+1} = \mathscr{G}(A^{n-1} + A^{n+1}) = \mathscr{G}(A^n(A^{-1} + A)) = \mathscr{G}(A^n(-1 + 2A)) = L_n.$$

Similarly the identity

$$L_{n-1} L_{n+1} = 5F_n$$

follows from

$$\begin{aligned} L_{n-1} + L_{n+1} &= \mathscr{G}(A^{n-1}(-1 + 2A) + A^{n+1}(-1 + 2A)) \\ &= \mathscr{G}(A^n(A^{-1} + A)(-1 + 2A)) = 5F_n. \end{aligned}$$

In addition, if we apply $\mathscr{E}$ to $F_{n-1} + F_n A = A^n$, we get $F_{n-1} + F_n \phi = \phi^n$. Conjugation gives $F_{n-1} + F_n \overline{\phi} = \overline{\phi}^n$. Hence,

$$\sqrt{5}\, F_n = (\phi^n - \overline{\phi}^n).$$

Finally, if we apply $\mathscr{E}$ to

$$\begin{aligned} A^n + \overline{A}^n &= F_{n-1} I + F_n A + F_{n-1} I + F_n \overline{A} = F_{n-1} I + F_n A + F_{n-1} I + F_n(I - A) \\ &= (F_{n-1} + F_{n+1}) I = L_n I, \end{aligned}$$

we obtain

$$L_n = \phi^n + \overline{\phi}^n.$$

Products. Returning to the product of generalized Fibonacci sequences, we see that

$$(GH)_{m+n} = G_{m-1} H_n + G_m H_{n+1}$$

because

$$\begin{aligned} (GH)_{m+n} &= \mathscr{G}(A^{m+n} \mathscr{M}(\{G_n\}) \mathscr{M}(\{H_n\})) = \mathscr{G}((G_{m-1} + G_m A)(H_{n-1} + H_n A)) \\ &= G_{m-1} H_n + G_m H_{n+1}. \end{aligned}$$

Substituting F in place of G, G in place of H, and $\pm p$ in place of m gives

$$G_{p+n} = F_{p-1} G_n + F_p G_{n+1} \quad \text{and} \quad G_{-p+n} = F_{-p-1} G_n + F_{-p} G_{n+1}.$$

Replacing F_{-n} by $(-1)^{n+1} F_n$ in this last identity gives $(-1)^p G_{-p+n} = F_{p+1} G_n - F_p G_{n+1}$. Thus (because $F_{n-1} + F_{n+1} = L_n$),

$$G_{p+n} = L_p G_n - (-1)^p G_{-p+n}.$$

Similarly,

$$H_{p+m} = L_p H_m - (-1)^p H_{-p+m}.$$

This shows that $\begin{pmatrix} 0 & 1 \\ -(-1)^p & L_p \end{pmatrix} \begin{pmatrix} H_{m-p} & G_{n-p} \\ H_m & G_n \end{pmatrix} = \begin{pmatrix} H_m & G_n \\ H_{m+p} & G_{n+p} \end{pmatrix}$. Taking the determinant, we obtain

$$H_m G_{n+p} - H_{m+p} G_n = (-1)^p (H_{m-p} G_n - H_m G_{n-p}).$$

A Link to Lucas Numbers. We close with the not-so-familiar identity mentioned in the introduction.

ARITHMETIC FIBONACCI SUM. *Let* $\{G_n\}$ *be a generalized Fibonacci sequence. If* m, n, r *are integers with* $n \geq 0, r \neq 0$, *then*

$$G_m + G_{m+r} + G_{m+2r} + \cdots + G_{m+nr} = \frac{1}{1 + (-1)^r - L_r}\left[G_m - G_{m+(n+1)r} + (-1)^r (G_{m+nr} - G_{m-r})\right],$$

where L_n *is the n-th Lucas number.*

Proof. By (2), the identity follows from the relation

$$A^m + A^{m+r} + A^{m+2r} + \cdots + A^{m+nr} = \frac{1}{1 + (-1)^r - L_r}\left[A^m - A^{m+(n+1)r} + (-1)^r (A^{m+nr} - A^{m-r})\right]$$

which in turn follows from

$$A^m + A^{m+r} + A^{m+2r} + \cdots + A^{m+nr} = A^m (A^{(n+1)r} - I)(A^r - I)^{-1}$$

and

$$(A^r - 1)((-A)^{-r} - I) = (1 + (-1)^r - L_r) I.$$

We can go on proving Fibonacci identities this way indefinitely: *Find an algebraic relation in A; apply (2).* But this is really just old wine (the "umbral method" (see [**1**], p. 395)) in new bottles (the golden matrix ring).

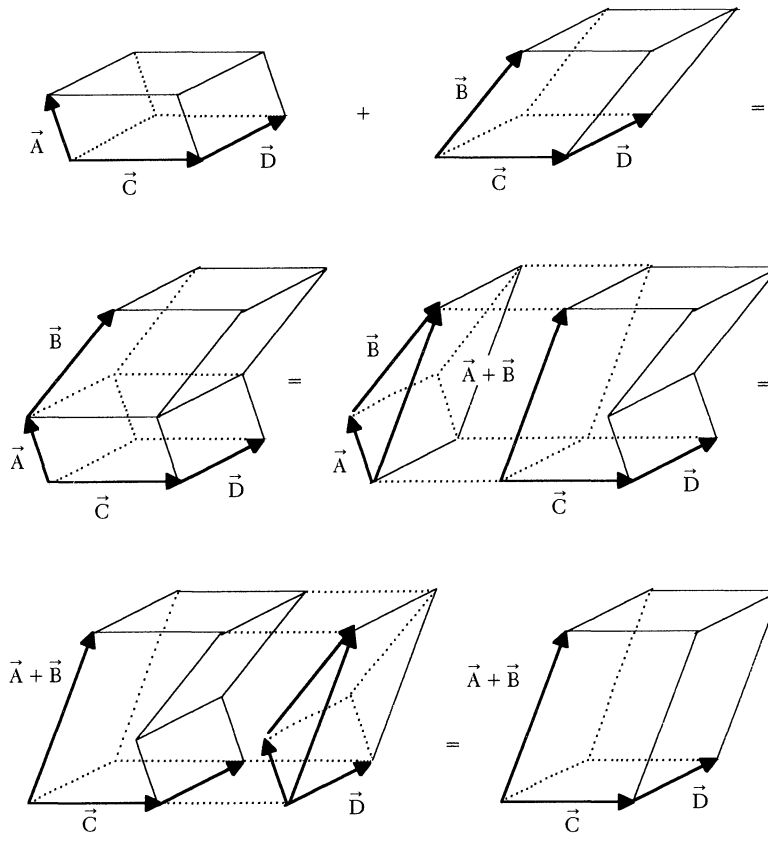
Acknowledgment. I wish to thank the editor, the referees, and Catherine Yang for their helpful suggestions.

REFERENCES

1. L. E. Dickson, *History of the Theory of Numbers*, Carnegie Institution of Washington, Washington, DC, 1919.
2. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford University Press, Oxford, England, 1979.
3. A. F. Horadam, A generalized Fibonacci sequence, *Amer. Math. Monthly*, 68 (1961), 455–459.
4. G. Strang, *Introduction to Linear Algebra*, Wellesley-Cambridge Press, Wellesley, MA, 1993.

Proof Without Words:
The Distributive Property of the Triple Scalar Product

$$\vec{A}\cdot(\vec{C}\times\vec{D})+\vec{B}\cdot(\vec{C}\times\vec{D})=(\vec{A}+\vec{B})\cdot(\vec{C}\times\vec{D})$$



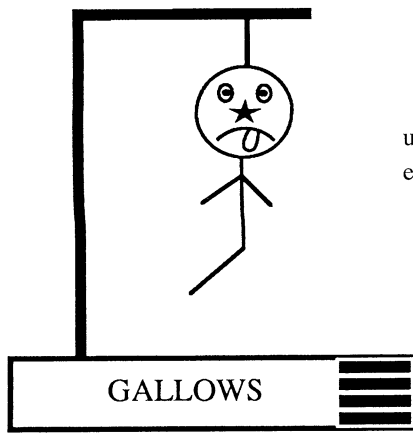
—Constance C. Edwards and Prashant S. Sansgiry
Coastal Carolina University
Conway, SC 29526

How (Knot?) to Play Hangman

HARVEY SCHMIDT, JR.
Lewis & Clark College
Portland, OR 97219

Introduction The parlor game *Hangman* is a guessing game involving two players, the poser (P) and the guesser (G). P poses an unknown word (there may be house rules on foreign words, proper names, etc.) to G, revealing only the number of (not necessarily distinct) letters in the word. G then attempts to uncover the word by suggesting letters to P. If G correctly identifies a letter in the word, then P exposes *all* occurrences of the letter and their positions; if G suggests a letter not contained in the word, then G accrues an error. The game continues until either the unknown word is identified or G exceeds the allowable number of errors—and thus is *hanged.*

Traditionally, we consider the body of the potential victim (G) as composed of seven parts: a head, a neck, two arms, a midsection, and two legs. If we add (draw) one of these body parts for each error accrued, then G will be hanged after making seven errors. If, say, P poses the word **unlucky** and G, attempting to identify the vowels first, starts with the eight guesses a, e, i, o, u, t, h, and n, then the game at this stage can be described by the Figure, and G would be one error away from being hanged.



unknown words: *u n_u_ _ .*
errors: *a, e, i, o, t, h*

FIGURE 1
An unlucky victim

What is a reasonable mathematical model for this game? In an actual game, P is constrained to submit a word from an agreed-upon dictionary, so not all combinations and arrangements of the 26 letters are allowable. Moreover, G has access to the same dictionary, and partial information about the word may inform successive guesses. This means, in "real life," that not all words posed by P are equally likely, and that successive guesses by G are not independent.

An urn model To abstract this game by removing the "human" aspect—and hence maybe some of the fun!—we assume that letters are selected (guessed) at random from a fixed n-letter alphabet $A = \{a_1, a_2, \ldots, a_n\}$. The other fixed parameters, known to both players, are the allowable number k of errors (incorrect guesses), $1 \leq k \leq n$, and the length r of the unknown word. Since P must expose *all* instances of identified letters in their proper positions, the order of the letters and the number of times each

appears is immaterial. Thus, for our purposes a word is determined solely by the particular distinct letters in the word. Consequently, a word with t distinct letters, $1 \le t \le n$, will be represented simply by

$$\mathbf{w}_t = a_{i_1} a_{i_2} \dots a_{i_t} \qquad (i_1 < i_2 < \cdots < i_t).$$

This abstraction suggests an urn model for *Hangman*. The urn contains n balls, of which t are white (correct guesses) and $n - t$ are black (incorrect guesses). Instead of guessing letters, G now chooses balls sequentially from the urn until either t white balls or k black balls have been chosen. G wins in the former case and is hanged in the latter case.

If we let P_j be the probability that the t-th white ball is drawn on the $(t+j)$-th draw, then it is easy to see that

$$P_j = \frac{\binom{t}{t-1}\binom{n-t}{j}}{\binom{n}{t+j-1}} \cdot \frac{1}{n-t-j+1} = \frac{t!(n-t)!(t+j-1)!}{(t-1)!j!n!} = \frac{\binom{t+j-1}{j}}{\binom{n}{t}}.$$

Letting $P(\mathbf{w}_t)$ be the probability that G uncovers the word $\mathbf{w}_t$ before the k-th incorrect guess, we have the following formula. (The latter equality is due to a well known combinatorial identity (see, e.g., **[2]**, (56)).

THEOREM 1. *With notation as described,*

$$P(\mathbf{w}_t) = \sum_{j=0}^{k-1} P_j = \frac{1}{\binom{n}{t}} \sum_{j=0}^{k-1} \binom{t+j-1}{j} = \frac{\binom{t+k-1}{k-1}}{\binom{n}{t}}.$$

For the poser P, the optimal strategy is to pose a word for which the probability $P(\mathbf{w}_t)$ is minimal. In the earlier example, with fixed values $n = 26$ and $k = 7$, a quick glance at Table 1, which gives the values of $P(\mathbf{w}_t)$ for $1 \le t \le n - k$, reveals a striking symmetry, centered at $t = 10$, which allows the poser P to select a word of optimal length.

Although it may not be immediately apparent from Table 1 or the expression for $P(\mathbf{w}_t)$ in Theorem 1, the precise symmetry illustrated in the table is captured in Theorem 2. (The notations $\lfloor\ \rfloor$ and $\lceil\ \rceil$ represent the floor and ceiling functions.)

TABLE 1. Winning Probabilities for G

t	$P(\mathbf{w}_t)$	t	$P(\mathbf{w}_t)$
1	0.269307769	11	0.001601831
2	0.086153846	12	0.001922197
3	0.032307692	13	0.002608696
4	0.014046823	14	0.004013378
5	0.007023411	15	0.007023411
6	0.004013378	16	0.014046823
7	0.002608696	17	0.032307692
8	0.001922197	18	0.086153846
9	0.001601831	19	0.269307769
10	0.001507605		

THEOREM 2.

(i) *For* $k + t \le n$ *and* $1 \le t \le \lfloor (n-k)/2 \rfloor$, $P(\mathbf{w}_t) = P(\mathbf{w}_{n-k-t+1})$.
(ii) *The minimum value of* $P(\mathbf{w}_t)$ *occurs when* $t = \lceil (n-k)/2 \rceil$.

Proof. Both assertions follow directly from the observation that the expression for $P(\mathbf{w}_t)$ can be reorganized to isolate the parameter t:

$$\frac{\binom{t+k-1}{k-1}}{\binom{n}{t}} = \frac{\binom{n+k-1}{n}}{\binom{n+k-1}{t+k-1}}. \tag{1}$$

For a fixed n and k, the values of the binomial coefficient in the denominator on the right side of this equality are well known to be symmetric about the closest integer to $(n-k+1)/2$, with the largest value occurring when $t = \lceil (n-k)/2 \rceil$. The proof is complete.

Coda and disclaimer As anyone who has played this game in real life can attest, this analysis is not very realistic! The illustrating example, with parameters $n = 26$ and $k = 7$, suggests that the poser should select a word with 10 distinct letters. In this case, if G guesses randomly, then G's probability of winning is roughly 0.0015. Yet most experienced players succeed at uncovering a proposed word much more often than once in a thousand attempts. Indeed, who would find interesting a parlor game with such low odds of success? Moreover, 10-letter words are not all that common in the English language. (How many can you write in 5 minutes? How many are there in this article?) Finally, with the parameters given in the example above, intuition might suggest that words with fewer than 10 letters would present a greater challenge because of the difficulty in establishing patterns.

What this model lacks is any notion of "structured" guessing, based upon knowledge of the dictionary and the frequency of particular combinations of letters. Some algorithm for assigning relative or conditional probabilities after each successful identification of a letter in the proposed word would seem to address some of this deficiency. Nevertheless, P can select, for example, obscure words with either unusual letter combinations or all-too-common letter combinations, leaving G unable to eliminate sufficient combinations of letters as impossible. In fact, knowing that the last two letters of a 3-letter word are *a* and *t* provides no assurance that G will not be hanged in a game allowing only seven errors.

Appendix: A footnote on recursion Because the binomial coefficient $\binom{t+i-1}{i}$ appearing in the expression for $P(\mathbf{w}_t)$ in Theorem 1 has various recursion properties, it is also possible to analyze $P(\mathbf{w}_t)$ recursively. In order to develop recursion expressions for $P(\mathbf{w}_t)$, we follow Cohen ([1]) and adopt the notation

$$\left\langle {t \atop i} \right\rangle = \binom{t+i-1}{i}. \tag{2}$$

This expression satisfies many combinatorial identities. The following well-known examples follow directly from (2):

$$\left\langle {t \atop i} \right\rangle = \left\langle {t-1 \atop i} \right\rangle + \left\langle {t \atop i-1} \right\rangle; \tag{3}$$

$$\left\langle {t \atop i} \right\rangle = \frac{t}{i}\left\langle {t+1 \atop i-1} \right\rangle = \frac{t+i-1}{i}\left\langle {t \atop i-1} \right\rangle; \tag{4}$$

$$\left\langle {t+1 \atop i} \right\rangle = \sum_{j=0}^{i} \left\langle {t \atop j} \right\rangle. \tag{5}$$

If we let $P_n(k,t) = P(\mathbf{w}_t)$, in order to display all the parameters simultaneously, then using the identities above we may rewrite $P_n(k,t)$ as

$$P_n(k,t) = \frac{1}{\binom{n}{t}} \sum_{i=0}^{k-1} \left\langle {t \atop i} \right\rangle \quad \text{[by (2)]}$$

$$= \frac{1}{\binom{n}{t}} \left\langle {t+1 \atop k-1} \right\rangle \quad \text{[by (5)]}$$

$$= \frac{\frac{k}{t}\left\langle {t \atop k} \right\rangle}{\binom{n}{t}} \quad \text{[by (4)]}. \tag{6}$$

With (6) in hand, straightforward algebra leads to the following natural analogues of familiar recursion expressions for the binomial coefficients:

$$P_n(k,t+1) = \frac{\frac{k}{t+1}\left\langle {t+1 \atop k} \right\rangle}{\binom{n}{t}} = \frac{k(k+t)\left\langle {t \atop k} \right\rangle}{t(n-t)\binom{n}{t}} = \frac{k+t}{n-t} P_n(k,t);$$

$$P_n(k+1,t) = \frac{\frac{k+1}{t}\left\langle {t \atop k} \right\rangle}{\binom{n}{t}} = \frac{k(k+t)\left\langle {t \atop k} \right\rangle}{k\binom{n}{t}} = \frac{k+t}{k} P_n(k,t);$$

$$P_{n+1}(k,t) = \frac{\frac{k}{t}\left\langle {t \atop k} \right\rangle}{\binom{n+1}{t}} = \frac{\frac{k}{t}\left\langle {t \atop k} \right\rangle (n-t+1)}{(n+1)\binom{n}{t}} = \frac{n-t+1}{n+1} P_n(k,t);$$

and finally

$$P_n(k,t) = \frac{\frac{k}{t}\left\langle {t-1 \atop k} \right\rangle + \frac{k}{t}\left\langle {t \atop k-1} \right\rangle}{\binom{n}{t}} = \frac{\frac{k}{t}\left\langle {t-1 \atop k} \right\rangle}{\binom{n}{t}} + \frac{\frac{k}{t}\left\langle {t \atop k-1} \right\rangle}{\binom{n}{t}} \quad \text{[by (2)]}$$

$$= \frac{t-1}{t(n-t+1)} \frac{\frac{k}{t-1}\left\langle {t-1 \atop k} \right\rangle}{\binom{n}{t-1}} + \frac{k}{k-1} \frac{\frac{k-1}{t}\left\langle {t \atop k-1} \right\rangle}{\binom{n}{t}}$$

$$= \frac{t-1}{t(n-t+1)} P_n(k,t-1) + \frac{k}{k-1} P_n(k-1,t).$$

REFERENCES

1. D. I. A. Cohen, *Basic Techniques of Combinatorial Theory*, Wiley, New York, NY, 1978.
2. L. B. W. Jolley, *Summation of Series*, Dover Publications, Inc., New York, NY, 1961.

PROBLEMS

GEORGE T. GILBERT, *Editor*
Texas Christian University

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

Proposals

To be considered for publication, solutions should be received by September 1, 1997.

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

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

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

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

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

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

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

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

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

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

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

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

Solutions should be written in a style appropriate for this MAGAZINE. *Each solution should begin on a separate sheet containing the solver's name and full address.*

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

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

Prove that if

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

and two of the expressions

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

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

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

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

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

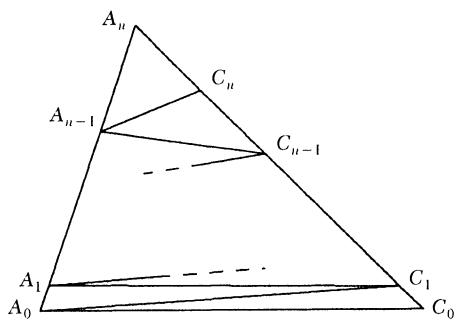
has integer coefficients.

Quickies

Answers to the Quickies are on page 150

Q862. *Proposed by John Bonomo, St. Mary's University of Minnesota, Winona, Minnesota.*

In $\Delta A_0C_0A_n$ below, all of the $2n$ triangles $A_{i-1}C_iA_i$ and $C_{i-1}A_{i-1}C_i$, $i = 1, 2, \ldots, n$, have the same area. Find A_nC_n/A_nC_0.



Q863. *Proposed by Murray S. Klamkin, University of Alberta, Edmonton, Alberta, Canada.*

Prove that

$$n\left[\sum_{i=1}^{n} a_ib_i + \left(\sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} b_i^2\right)^{1/2}\right] \geq 2\sum_{i=1}^{n} a_i \sum_{i=1}^{n} b_i,$$

where the a_i and b_i are real. Determine when equality holds.

Q864. *Proposed by Kung-Wei Yang, Western Michigan University, Kalamazoo, Michigan.*

For every real 2×2 matrix A, show that it is possible to find a matrix B and a symmetric matrix C for which $A = B + C$, $\det A = \det B + \det C$, and $\det B \geq 0 \geq \det C$.

Solutions

A Primality Condition — April 1996

1494. *Proposed by Emeric Deutsch, Polytechnic University, Brooklyn, New York, and Ira M. Gessel, Brandeis University, Waltham, Massachusetts.*

Let $n \geq 2$ be a positive integer. Prove that n is prime if and only if $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$ for $k = 0, 1, \ldots, n-1$.

I. *Solution by Helen M. Marston, Princeton, New Jersey.*

If n is prime, then every i, $1 \leq i \leq n-1$, has an inverse $i^{-1} \pmod{n}$. Therefore, for $0 \leq k \leq n-1$,

$$\binom{n-1}{k} = \prod_{i=1}^{k} \frac{n-i}{i} \equiv \prod_{i=1}^{k} (n-i)i^{-1} \equiv (-1)^k \pmod{n}.$$

If n is composite, let p be the smallest prime factor of n. Then $\binom{n-1}{p-1} \equiv (-1)^{p-1} \pmod{n}$ as above. But

$$\binom{n-1}{p} = \binom{n-1}{p-1}\left(\frac{n}{p} - 1\right) \equiv (-1)^{p-1}\left(\frac{n}{p} - 1\right) \not\equiv (-1)^p \pmod{n},$$

since $n/p \not\equiv 0 \pmod{n}$.

II. *Solution by Stephen Noltie, Ohio University–Lancaster, Lancaster, Ohio.*

Suppose first that n is prime. For $k = 1, 2, \ldots, n-1$, the denominator of $\binom{n}{k} = n(n-1)\cdots(n-(k-1))/k!$ is not divisible by n, hence the integer $\binom{n}{k} \equiv 0 \pmod{n}$. Clearly $\binom{n-1}{0} = 1 \equiv (-1)^0 \pmod{n}$. For $k = 1, 2, \ldots, n-1$,

$$\binom{n-1}{k} = \binom{n}{k} - \binom{n-1}{k-1} \equiv -\binom{n-1}{k-1} \pmod{n},$$

and $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$ follows by induction.

On the other hand, if n is not prime, let p be a prime factor of n. Suppose p^α is the largest power of p dividing n. Then $\binom{n}{p}$ is divisible by $p^{\alpha-1}$ but not by p^α.

Therefore,

$$\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p} \not\equiv 0 \pmod{n}.$$

It follows that $\binom{n-1}{p-1} \equiv (-1)^{p-1} \pmod{n}$ and $\binom{n-1}{p} \equiv (-1)^{p} \pmod{n}$ cannot both be true.

Also solved by Ricardo Alfaro, Pablo Armas (student, Argentina), Roy Barbara (Lebanon), Marc A. Brodie, John Christopher, Curtis Coker, L. L. Foster, Zachary Franco, E. C. and S. A. Greenspan, Jennifer Hyndman (Canada), Kee-Wai Lau (Hong Kong), Tamás Lengyel, Marijo LeVan, Lester Levy, James T. Lewis, Hiren Maharaj, David E. Manes, Kandasamy Muthuvel, Josh Nichols-Barrer (student), Joel Rosenberg, Harvey Schmidt, Jr., Lawrence Somer, Alan H. Stein, Ajaj A. Tarabay and Bassem B. Ghalayini (Lebanon), Michael Vowe (Switzerland), Monte J. Zerger, David Zhu, Paul J. Zwier, and the proposer. There were two incomplete and two incorrect solutions.

Chord in an Inscribed Quadrilateral — April 1996

1495. *Proposed by Achilleas Sinefakopoulos, student, University of Athens, Greece.*

Let angles B and C of ΔABC be acute, and let K be a point on arc BC of its circumcircle. Let L be the intersection of chords AK and BC. The feet of the perpendiculars from L to AB and to AC are M and N, respectively. Prove that if the area of ΔABC equals that of quadrilateral $AMKN$, then AK bisects angle A.

Solution by Michael Vowe, Therwil, Switzerland.

The problem is incorrect as stated. Chord AK may be either the angle bisector of angle A or a diameter of the circumcircle of ΔABC. Furthermore, we assume M is on *segment* AB and N is on *segment* AC, which may have been ambiguous in the problem statement.

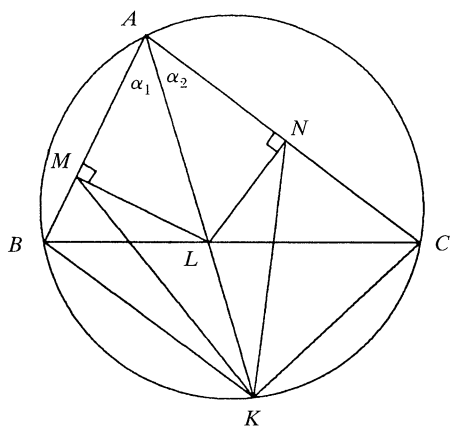
Let $[ABC]$ denote the area of ΔABC and $[AMKN]$ denote the area of quadrilateral $AMKN$. Let $\alpha_1 = \angle BAK$, $\alpha_2 = \angle CAK$, and R be the radius of the circumcircle of ΔABC.

Since $ABKC$ is a cyclic quadrilateral, Ptolemy's theorem implies

$$AK \cdot BC = AB \cdot CK + AC \cdot BK,$$

hence

$$AK \cdot 2R \sin(\alpha_1 + \alpha_2) = AB \cdot 2R \sin \alpha_2 + AC \cdot 2R \sin \alpha_1,$$



and

$$AK = \frac{AB \sin \alpha_2 + AC \sin \alpha_1}{\sin(\alpha_1 + \alpha_2)} = \frac{AB \sin \alpha_2 + AC \sin \alpha_1}{\sin \alpha_1 \cos \alpha_2 + \sin \alpha_2 \cos \alpha_1}.$$

We also have

$$[ABC] = [ABL] + [ACL] = \frac{1}{2} AL(AB \sin \alpha_1 + AC \sin \alpha_2)$$

and

$$\begin{aligned}[AMKN] &= [AMK] + [ANK] = \frac{1}{2} AK(AM \sin \alpha_1 + AN \sin \alpha_2) \\ &= \frac{1}{2} AK \cdot AL(\sin \alpha_1 \cos \alpha_1 + \sin \alpha_2 \cos \alpha_2) \\ &= \frac{1}{2} \frac{AB \sin \alpha_2 + AC \sin \alpha_1}{\sin \alpha_1 \cos \alpha_2 + \sin \alpha_2 \cos \alpha_1} \cdot AL(\sin \alpha_1 \cos \alpha_1 + \sin \alpha_2 \cos \alpha_2).\end{aligned}$$

After some simple algebra, we see that $[ABC] = [AMKN]$ if and only if

$$(AB \cos \alpha_2 - AC \cos \alpha_1)(\sin^2 \alpha_1 - \sin^2 \alpha_2) = 0.$$

If the second factor is 0, then $\alpha_1 = \alpha_2$ and AK bisects angle A. If the first factor is 0, then $AB/\cos \alpha_1 = AC/\cos \alpha_2$, hence the perpendicular to AB through B, the perpendicular to AC through C, and AK are concurrent. It follows that K is the point of concurrency, so that AK is a diameter of the circumcircle of ΔABC.

Also solved by Roy Barbara (Lebanon) and Victor Kutsenok. There were three solutions that missed the second possibility, as did, regrettably, the editors.

A Differential Equation **April 1996**

1496. *Proposed by Murray S. Klamkin, University of Alberta, Edmonton, Alberta, Canada.*

Find a solution to the differential equation $d^2y/dx^2 = -kx/y^4$, $k > 0$, other than one of the form $y = ax^{3/5}$.

I. *Solution by Hongwei Chen, Christopher Newport University, Newport News, Virginia.*

The given differential equation is a special case of the Emden-Fowler equation $d^2y/dx^2 = Ax^n y^m$. All possible solvable cases are given in A. D. Polyanin and V. F. Zaitsev, *Handbook of Exact Solutions for Ordinary Differential Equations*, CRC Press, 1995, 241–250.

We claim that the general solution to the differential equation is given in the parametric form

$$x = \left(C_2 \pm \int \left(\frac{2k}{3} t^{-3} + C_1\right)^{-1/2} dt\right)^{-1},$$

$$y = t\left(C_2 \pm \int \left(\frac{2k}{3} t^{-3} + C_1\right)^{-1/2} dt\right)^{-1},$$

where t is a parameter, C_1 and C_2 are arbitrary constants.

The transformation $x = 1/s$, $y = t(s)/s$ changes the equation into

$$\frac{d^2t}{ds^2} = \frac{1}{s^3}\frac{d^2y}{dx^2} = -kt^{-4}.$$

By using the substitution

$$w(t) = dt/ds,$$

this equation is reduced to the first order equation

$$\frac{dw}{dt} = \frac{dw/ds}{dt/ds} = \frac{d^2t/ds^2}{w} = -\frac{kt^{-4}}{w}.$$

Integrate to obtain

$$w^2 = \frac{2k}{3}t^{-3} + C_1,$$

where C_1 is a constant. Thus,

$$\frac{dt}{ds} = \pm\left(\frac{2k}{3}t^{-3} + C_1\right)^{1/2},$$

so that

$$\pm\int\left(\frac{2k}{3}t^{-3} + C_1\right)^{-1/2} dt = \int ds,$$

and therefore

$$s = C_2 \pm \int\left(\frac{2k}{3}t^{-3} + C_1\right)^{-1/2} dt,$$

where C_2 is an additional constant. Hence, the general solution of the original equation is given by

$$x = \left(C_2 \pm \int\left(\frac{2k}{3}t^{-3} + C_1\right)^{-1/2} dt\right)^{-1},$$

$$y = t\left(C_2 \pm \int\left(\frac{2k}{3}t^{-3} + C_1\right)^{-1/2} dt\right)^{-1}.$$

Setting $C_1 = 0$ leads to

$$x = \left(C_2 \pm \sqrt{\frac{6}{25k}}\, t^{5/2}\right)^{-1},$$

so that

$$t = \left(C + \sqrt{\frac{25k}{6}}\, x^{-1}\right)^{2/5},$$

and

$$y = x\left(C + \sqrt{\frac{25k}{6}}\, x^{-1}\right)^{2/5}.$$

II. *Solution by the proposer.*

Setting $y = xt(x)$, we get

$$x^4 \frac{d^2t}{dx^2} + 2x^3 \frac{dt}{dx} = \frac{-k}{t^4}.$$

Multiplying by the integrating factor $2\,dt/dx$, we get

$$\frac{d}{dx}\left(x^4\left(\frac{dt}{dx}\right)^2\right) = \frac{d}{dx}\frac{2k}{3t^3}.$$

Integrating and taking square roots yields

$$\frac{dt}{dx} = \pm \frac{\sqrt{\dfrac{2k}{3t^3} + C_1}}{x^2}.$$

As in the first solution above, separation of variables leads to the parametric solution, and setting $C_1 = 0$ allows us to perform the integral to obtain an analytic solution.

There was one incomplete solution.

Cardinality of Sets **April 1996**

1497. *Proposed by Mihály Bencze, Braşov, Romania.*

Given positive real numbers $\alpha_1, \ldots, \alpha_m$, let $A_1, \ldots, A_m$ be sets of nonnegative integers such that $0 \in A_k$ and $|A_k \cap \{1, 2, \ldots, n\}| \geq \alpha_k \cdot n$ for $k = 1, \ldots, m$ and $n = 1, 2, \ldots$. Prove that

$$\left|\sum_{k=1}^{m} A_k \cap \{1, 2, \ldots, n\}\right| \geq \left(1 - \prod_{k=1}^{m}(1 - \alpha_k)\right)n,$$

where $\sum_{k=1}^{m} A_k = \{a_1 + \cdots + a_m : a_k \in A_k\}$.

Solution by the proposer.

Denote $|A_k \cap \{1, 2, \ldots, n\}|$ by $A_k(n)$. We proceed by induction on m, the case $m = 1$ being given. We next prove the case $m = 2$. Let

$$0 = r_0 < r_1 < r_2 < \cdots < r_{A_1(n)} \leq n$$

be in A_1. For $i = 0, \ldots, A_1(n) - 1$ and every s in $A_2 \cap \{1, 2, \ldots, r_{i+1} - r_i - 1\}$, $r_i + s$ gives an element of $A_1 + A_2$ which is greater than r_i, but less than r_{i+1}. For each i, there are at least $\alpha_2(r_{i+1} - r_i - 1)$ such elements. Similarly, there are at least $\alpha_2(n - r_{A_1(n)})$ elements of $(A_1 + A_2) \cap \{1, 2, \ldots, n\}$ that exceed $r_{A_1(n)}$. We conclude that

$$\begin{aligned}
|(A_1 + A_2) \cap \{1, 2, \ldots, n\}| &\geq A_1(n) + \alpha_2(r_1 - 1) + \alpha_2(r_2 - r_1 - 1) \\
&\quad + \cdots + \alpha_2(r_{A_1(n)} - r_{A_1(n)-1} - 1) + \alpha_2(n - r_{A_1(n)}) \\
&= (1 - \alpha_2)A_1(n) + \alpha_2 n \geq \alpha_1(1 - \alpha_2)n + \alpha_2 n \\
&= (1 - (1 - \alpha_1)(1 - \alpha_2))n.
\end{aligned}$$

To prove the general case, we simply note that

$$\left|\bigcup_{k=1}^{m+1} A_k \cap \{1,2,\ldots,n\}\right| = \left|\left(\bigcup_{k=1}^{m} A_k + A_{m+1}\right) \cap \{1,2,\ldots,n\}\right|$$
$$\geq \left(1-\left(1-\left(1-\prod_{k=1}^{m}(1-\alpha_k)\right)\right)(1-\alpha_{m+1})\right)n$$
$$= \left(1-\prod_{k=1}^{m+1}(1-\alpha_k)\right)n.$$

Closed Forms of Two Sums **April 1996**

1498. *Proposed by J. C. Binz, University of Bern, Switzerland.*

For n a positive integer, express

$$\sum_{j\geq 0}\binom{n-j}{j} r^j (r-1)^{2n-2j} \quad \text{and} \quad \sum_{j\geq 0} j\binom{n-j}{j} r^j (r-1)^{2n-2j}$$

in closed form.

Solution by Joel Rosenberg, University of Michigan, Ann Arbor, Michigan.

We show that

$$\sum_{j\geq 0}\binom{n-j}{j} r^j (r-1)^{2n-2j} = \frac{r}{r+1}(r^2-r)^n + \frac{1}{r+1}(1-r)^n$$
$$= (r-1)^n \frac{r^{n+1}-(-1)^{n+1}}{r+1}$$

and

$$\sum_{j\geq 0} j\binom{n-j}{j} r^j (r-1)^{2n-2j}$$
$$= \frac{r(nr+n+1-r)}{(1+r)^3}(r^2-r)^n + \frac{r(nr+n+r-1)}{(1+r)^3}(1-r)^n$$
$$= r(r-1)^n \frac{(n-1)\left(r^{n+1}-(-1)^{n+1}\right)+(n+1)r\left(r^{n-1}-(-1)^{n-1}\right)}{(r+1)^3}.$$

Let $S_n(r) = \sum_{j\geq 0}\binom{n-j}{j} r^j (r-1)^{2n-2j}$ and $T_n(r) = \sum_{j\geq 0} j\binom{n-j}{j} r^j (r-1)^{2n-2j}$. Then

$$S_n(r) = \sum_{j\geq 0}\binom{n-j}{j} r^j (r-1)^{2n-2j}$$
$$= \sum_{j\geq 0}\binom{n-j-1}{j} r^j (r-1)^{2n-2j} + \sum_{j\geq 1}\binom{n-j-1}{j-1} r^j (r-1)^{2n-2j}$$
$$= (r-1)^2 \sum_{j\geq 0}\binom{(n-1)-j}{j} r^j (r-1)^{2n-2-2j}$$
$$+ r(r-1)^2 \sum_{j\geq 1}\binom{(n-2)-(j-1)}{j-1} r^{j-1}(r-1)^{2n-2j-2}$$
$$= (r-1)^2 S_{n-1}(r) + r(r-1)^2 S_{n-2}(r),$$

so we have a linear recursion for $S_n(r)$. The associated polynomial for this recursion is

$$x^2-(r-1)^2x-r(r-1)^2=(x-(r^2-r))(x-(1-r)).$$

Thus, we can write

$$S_n(r)=\beta(r^2-r)^n+\delta(1-r)^n,\quad S_0(r)=1,\quad S_1(r)=(r-1)^2,$$

and obtain $\beta=r/(r+1)$, $\delta=1/(r+1)$, so

$$\sum_{j\ge 0}\binom{n-j}{j}r^j(r-1)^{2n-2j}=\frac{r}{r+1}(r^2-r)^n+\frac{1}{r+1}(1-r)^n$$

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

Similarly, we decompose $T_n(r)$ as

$$\begin{aligned}T_n(r)&=\sum_{j\ge 0}j\binom{n-j}{j}r^j(r-1)^{2n-2j}\\&=\sum_{j\ge 0}j\binom{n-j-1}{j}r^j(r-1)^{2n-2j}+\sum_{j\ge 1}j\binom{n-j-1}{j-1}r^j(r-1)^{2n-2j}\\&=(r-1)^2\sum_{j\ge 0}j\binom{(n-1)-j}{j}r^j(r-1)^{2n-2-2j}\\&\quad+r(r-1)^2\sum_{j\ge 1}j\binom{(n-2)-(j-1)}{j-1}r^{j-1}(r-1)^{2n-2j-2}\\&=(r-1)^2T_{n-1}(r)+r(r-1)^2T_{n-2}(r)+r(r-1)^2S_{n-2}(r),\end{aligned}$$

an inhomogeneous linear recursion. Because the homogeneous part of the recursion is the same as that for the $S_n(r)$, it follows that the $T_n(r)$ satisfy a homogeneous linear recursion with associated polynomial $(x-(r^2-r))^2(x-(1-r))^2$. Therefore, we can write $T_n(r)=(\alpha n+\beta)(r^2-r)^n+(\gamma n+\delta)(1-r)^n$, and calculate

$$\begin{aligned}T_0(r)&=0&&=0\cdot\alpha+1\cdot\beta+0\cdot\gamma+1\cdot\delta\\T_1(r)&=0&&=(r^2-r)\cdot\alpha+(r^2-r)\cdot\beta+(1-r)\cdot\gamma+(1-r)\cdot\delta\\T_2(r)&=r(r-1)^2&&=2(r^2-r)^2\cdot\alpha+(r^2-r)^2\cdot\beta+2(1-r^2)\cdot\gamma+(1-r)^2\cdot\delta\\T_3(r)&=2r(r-1)^4&&=3(r^2-r)^3\cdot\alpha+(r^2-r)^3\cdot\beta+3(1-r)^3\cdot\gamma+(1-r)^3\cdot\delta.\end{aligned}$$

The solution to this system is $(\alpha,\beta,\gamma,\delta)=(r/(1+r)^2, r(1-r)/(1+r)^3, r/(1+r)^2, r(r-1)/(1+r)^3)$. We finally obtain

$$\begin{aligned}&\sum_{j\ge 0}j\binom{n-j}{j}r^j(r-1)^{2n-2j}\\&\quad=\frac{r(nr+n+1-r)}{(1+r)^3}(r^2-r)^n+\frac{r(nr+n+r-1)}{(1+r)^3}(1-r)^n\\&\quad=r(r-1)^n\frac{(n-1)\left(r^{n+1}-(-1)^{n+1}\right)+(n+1)r\left(r^{n-1}-(-1)^{n-1}\right)}{(r+1)^3}.\end{aligned}$$

Comments. The value at $r = -1$ in both formulas is obtained by taking the limit. Carl Libis uses the recursions for $S_n(r)$ and $T_n(r)$ derived in the above solution to prove the formulas by induction. Michael Vowe uses the formula (see page 204 of R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, Reading, Massachusetts, 1989)

$$f(z) = \sum_{j\geq 0} \binom{n-j}{j} z^j = \frac{\left(\frac{1+\sqrt{1+4z}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{1+4z}}{2}\right)^{n+1}}{\sqrt{1+4z}},$$

and its derivative, to quickly obtain the formulas by setting $z = r/(r-1)^2$. The derivation of this identity is similar to, and a bit simpler than, that given in the solution above.

Also solved by E. Sparre Andersen and Mogens Esrom Larsen (Denmark), Kuo-Jye Chen (Taiwan), Curtis Coker, J. S. Frame, Carl Libis, Heinz-Jürgen Seiffert (Germany), Michael Vowe (Switzerland), and the proposer.

Answers

Solutions to the Quickies on page 142

A862. Because $\Delta A_0C_1A_n$ and $\Delta A_0C_0A_n$ share an altitude from A_0, we have

$$\frac{A_nC_1}{A_nC_0} = \frac{\text{Area}(\Delta A_0C_1A_n)}{\text{Area}(\Delta A_0C_0A_n)} = \frac{2n-1}{2n}.$$

Applying this observation to $\Delta A_1C_2A_n$ and $\Delta A_1C_1A_n$, and so forth, we obtain

$$\frac{A_nC_n}{A_nC_0} = \frac{A_nC_1}{A_nC_0}\cdot\frac{A_nC_2}{A_nC_1}\cdots\frac{A_nC_n}{A_nC_{n-1}} = \frac{2n-1}{2n}\cdot\frac{2n-3}{2n-2}\cdots\frac{1}{2} = \frac{(2n)!}{2^{2n}(n!)^2}.$$

A863. Let $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{b} = (b_1, \ldots, b_n)$, and $\mathbf{c}$ denote n-dimensional vectors. The given inequality will follow from the more general $|\mathbf{c}|^2(\mathbf{a}\cdot\mathbf{b} + |\mathbf{a}||\mathbf{b}|) \geq 2(\mathbf{a}\cdot\mathbf{c})(\mathbf{b}\cdot\mathbf{c})$ by setting $\mathbf{c} = (1, \ldots, 1)$. Let α, β, and γ denote the angles between $\mathbf{a}$ and $\mathbf{c}$, between $\mathbf{b}$ and $\mathbf{c}$, and between $\mathbf{a}$ and $\mathbf{b}$, respectively. The generalized inequality is now equivalent to $|\mathbf{a}||\mathbf{b}|\cos\gamma + |\mathbf{a}||\mathbf{b}| \geq 2|\mathbf{a}||\mathbf{b}|\cos\alpha\cos\beta$, or $\cos\gamma + 1 \geq 2\cos\alpha\cos\beta$. Since in the trihedral angle $\alpha + \beta \geq \gamma$ and $2\pi - (\alpha+\beta) \geq \gamma$, it suffices to show that

$$1 + \cos(\alpha+\beta) \geq 2\cos\alpha\cos\beta \quad \text{or} \quad 1 \geq \cos(\alpha-\beta).$$

Equality holds if and only if $\alpha = \beta$ and either $\alpha + \beta = \gamma$ or $\alpha + \beta = 2\pi - \gamma$. In particular, $\mathbf{a}$, $\mathbf{b}$, and $\mathbf{c}$ must be linearly dependent if equality holds.

A864. Letting $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have

$$\det A = ad - bc = \frac{1}{4}\left((a+d)^2 + (b-c)^2 - (a-d)^2 - (b+c)^2\right)$$

$$= \det\begin{pmatrix} \frac{a+d}{2} & \frac{b-c}{2} \\ \frac{c-b}{2} & \frac{a+d}{2} \end{pmatrix} + \det\begin{pmatrix} \frac{a-d}{2} & \frac{b+c}{2} \\ \frac{b+c}{2} & \frac{d-a}{2} \end{pmatrix}.$$

Thus, we may set $B = \begin{pmatrix} a+d/2 & b-c/2 \\ c-b/2 & a+d/2 \end{pmatrix}$ and $C = \begin{pmatrix} a-d/2 & b+c/2 \\ b+c/2 & d-a/2 \end{pmatrix}$.

REVIEWS

PAUL J. CAMPBELL, *editor*
Beloit College

Assistant Editor: Eric S. Rosenthal, West Orange, NJ. Articles and books are selected for this section to call attention to interesting mathematical exposition that occurs outside the mainstream of mathematics literature. Readers are invited to suggest items for review to the editors.

Dawson, John W., Jr., *Logical Dilemmas: The Life and Work of Kurt Gödel*, A K Peters, 1997; xiv + 361 pp, $49.95. ISBN 1-56881-025-3.

This book is likely to be the definitive biography of Gödel, by a mathematical logician who catalogued his papers and is co-editor of his collected works. Author Dawson mentions and briefly describes Gödel's mathematical results but does not try to explain them in detail. Readers will be saddened by the details of the mental illness that afflicted Gödel for most of his life and led to his death.

Pöppe, Christophe, and Madhusree Mukerjee, Prize mistake: The n-body problem is solved—too late, *Scientific American* 276 (2) (February 1997) 22. Diacu, Florin, The solution of the n-body problem, *Mathematical Intelligencer* 18 (3) (Summer 1996) 66–70.

The n-body problem in celestial mechanics is: Given initial locations and velocities of n bodies moving under Newton's laws of motion, find functions that describe their locations at all future times t. The case $n = 2$ was solved by Johann Bernoulli in 1710. In 1888, Henri Poincaré showed that the case $n \geq 3$ can include chaotic behavior and that the general problem cannot be solved by the method of integrals. Mathematical folklore ever since holds that the n-body problem, for $n \geq 3$, is unsolvable—or else the problem is open—depending on the oral tradition. In fact, as these articles reveal, the case $n = 3$ was solved in 1909, except for initial conditions that may lead to a triple collision. The method used does not extend to higher n. However, in 1991, Quidong (Don) Wang, a graduate student at the University of Cincinnati, gave a power series solution for the n-body problem, except for singularities (including collisions). Perhaps equally surprising, his solution is not practical—it "presents only historical interest," says Diacu—because the series solutions have very slow convergence. In the meantime, important practical special cases have been solved sufficiently accurately to send spacecraft throughout the solar system.

Stewart, Ian, Mathematical recreations: Crystallography of a golf ball, *Scientific American* 276 (2) (February 1997) 96–98.

A golf ball with dimples flies farther; practicality (avoiding swerve) demands that the dimples be placed more or less symmetrically. So, how many dimples, and how to arrange them? Numbers from 252 to 500 are found on balls. The maximum finite order of symmetry for a group in three dimensions is 120 (the group of the icosahedron or of the icosahedron), but most golf balls have lesser symmetry. Readers interested in the distribution of dimples on golf balls may also enjoy a paper by R.H. Hardin and N.J.A. Sloane that relates work of the "Codemart" team that has investigated "nice" ways of placing points on a sphere: Codes (spherical) and designs (experimental), in *Different Aspects of Coding Theory*, ed. A.R. Calderbank, Proc. Sympos. Appl. Math., 50, AMS, 1996, pp. 179–206.

Huberman, Bernardo A., Rajan M. Lukose, and Tad Hogg, An economics approach to hard computational problems, *Science* 273 (3 January 1997) 51–54.

Suppose that you have a problem and two algorithms for it that always produce a solution but with probabilistic distributions of solution times. How should you apportion your computing resources to solve the problem? The naive answer is to devote all the computer cycles to the algorithm with shorter expected time, especially if it has the smaller standard deviation as well. The authors show that running the two algorithms concurrently but independently on a serial processor can reduce both the expected time to solution and its standard deviation (which they call "risk"); the key to optimal reduction is the fraction of cycles allocated to each algorithm. The same counterintuitive result applies with two independent instances of the same algorithm with different random seeds. Generalization of the idea produces "computational portfolios" that are "unequivocally preferable to any of the component algorithms." The authors apply the idea to the NP-complete graph-coloring problem, for which appropriate tuning of the cycle-mix of two independent instances of the Brelaz heuristic decreases both expected solution time and its standard deviation by about 30%. Cooperating algorithms whose expected lengths of time are negatively correlated have even better performance and lower risk than independent algorithms.

Horgan, John, Profile: Ronald L. Graham: Juggling Act, *Scientific American* 276 (3) (March 1997) 28, 30.

This light profile of one of the gentlest ambassadors for mathematics includes a photo of Ron Graham in fool's cap juggling a cauliflower, a red pepper, an eggplant, and (ouch!) a pineapple. Perhaps Graham, chief scientist and a manager at AT&T Labs–Research, and one of the most respected and beloved of mathematicians, will replace the late Paul Erdős as journalists' favorite "poster boy" for mathematics.

Luoma, Keith, The truth behind "famous name" mathematics, *Mathematical Gazette* 80 (1996), 297, 349–351.

Mathematicians refer to concepts and results by names that flaunt what they know from history. Cramer's rule does not appear in Cramer's works; Horner's method was known to earlier Chinese, Pascal's triangle to Chinese and to Indians before them; and Simpson's rule and Taylor series appear earlier in the work of James Gregory. Such false attributions are examples of Stigler's Law of Eponymy, which says that no result is named after the person who first discovered it. Of course, the Law applies also to itself, according to its namesake Steven Stigler (University of Chicago). Maybe it's time, though, for the International Mathematical Union to appoint a commission to recommend more apt naming of named theorems, and for mathematicians thereafter to amend their practice accordingly.

Borwein, Jonathan M., et al. (eds), *Proceedings of the Organic Mathematics Workshop.* Hypertext at `http://www.cecm.sfu.ca/organics/contents.html` ; also to be available in printed form from the Canadian Mathematical Society.

The organizers of the Organic Mathematics Workshop (December, 1995, at Simon Fraser University) wanted to create an environment for *experimental mathematics* that would use the latest technology. The conference papers are available on the World Wide Web in a plethora of electronic forms and contain links at suitable places to animations and computer algebra code. Readers can annotate the papers and contribute their own articles. The resulting hypertext has papers by David H. Bailey et al. (how to compute one billion digits of pi), Joe Buhler and Ron Graham (on juggling), Jeff Lagarias (the $3x + 1$ problem and generalizations), Andrew Odlyzko (zeros of the zeta function), Stan Wagon (visualizing differential equations), and others.

57th Annual William Lowell Putnam Mathematical Competition

A-1 Find the least number A such that for any two squares of combined area 1, a rectangle of area A exists such that the two squares can be packed into that rectangle (without the interiors of the squares overlapping). You may assume that the sides of the squares will be parallel to the sides of the rectangle.

Answer. We can always accommodate the two squares inside a rectangle of area $A = (1+\sqrt{2})/2$.

Solution 1. Suppose the squares have sides of lengths x and y. We may suppose without loss of generality that $x \geq y \geq 0$. Place the squares so that their bases lie on the x-axis with their lower right corners at $(x,0)$ and $(x+y,0)$. We wish to maximize $x(x+y)$ subject to the condition that $x^2+y^2=1$. Equivalently, we must find the maximum value of $A(x) = x\left(x+\sqrt{1-x^2}\right)$ for $\sqrt{2}/2 \leq x \leq 1$.

To find the critical points, we set the derivative equal to zero:

$$\frac{dA(x)}{dx} = 2x + \sqrt{1-x^2} + \frac{-x^2}{\sqrt{1-x^2}} = 0\,.$$

This yields $4x^2 = 2+\sqrt{2}$, $4y^2 = 2-\sqrt{2}$, and $4xy = \sqrt{2}$; at this point $\sqrt{2}/2 < x < 1$ and A has the value $x^2+xy = (2+\sqrt{2})/4 + \sqrt{2}/4 = (1+\sqrt{2})/2$. Since this is greater than 1 (the value of $A(x)$ at the endpoints), it must be the maximum value.

Solution 2. Let $x = \cos\theta$ and $y = \sin\theta$, with $0 \leq \theta \leq \pi/2$. Then

$$\begin{aligned} x(x+y) &= \cos\theta\,(\cos\theta+\sin\theta) = \sqrt{2}\cos\theta\left(\frac{1}{\sqrt{2}}\cos\theta + \frac{1}{\sqrt{2}}\sin\theta\right) \\ &= \sqrt{2}\cos\theta\,\sin(\pi/4+\theta) = \frac{1}{\sqrt{2}}\Big(\sin(2\theta+\pi/4) + \sin(\pi/4)\Big), \end{aligned}$$

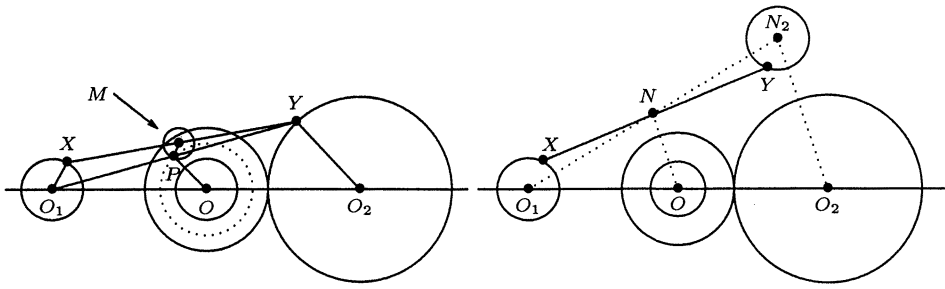
which is maximal for $2\theta+\pi/4 = \pi/2$. For this value of θ, we have $x > y$, so the maximum value we desire is $(1+\sin(\pi/4))/\sqrt{2} = (1+\sqrt{2})/2$.

A-2 Let C_1 and C_2 be circles whose centers are 10 units apart and whose radii are 1 and 3. Find, with proof, the locus of all points M for which there exist points X on C_1 and Y on C_2 such that M is the midpoint of the line segment XY.

Solution. Take the centers of C_1, C_2 to be $O_1 = (-5,0), O_2 = (5,0)$. The set comprises the closed annulus bounded by circles with center $O = (0,0)$ and radii 1 and 2.

The following construction (see the left-hand figure) is possible just if M is in the set. The circle with center M and radius $1/2$ cuts the circle with center O and radius $3/2$ at P. (In

general, there are two such P; select either.) Draw radii O_1X, O_2Y parallel to PM, OP respectively. Then M is the midpoint of XY, because O_1, P, Y are collinear, $O_1O = OO_2$, and $O_1P = PY$.



To see that X, Y do not exist for points not in the annulus, let N be such a point. (See the right-hand figure.) Let X traverse the circle C_1. Then the locus of Y, where X, N, Y are collinear and $XN = NY$, is a circle of radius 1 and center N_2, where O_2N_2 is parallel to ON and twice its length. This circle is either entirely interior or entirely exterior to C_2, according as N is inside or outside the annulus.

A-3 Suppose that each of twenty students has made a choice of anywhere from zero to six courses from a total of six courses offered. Prove or disprove: There are five students and two courses such that all five have chosen both courses or all five have chosen neither.

Solution. The 6×20 incidence matrix shown below, made so that the $\binom{6}{3} = 20$ vertical triples (of 1's or of 0's) are all distinct, shows that the statement is false; namely, each of the $\binom{6}{2} = 15$ pairs of rows have at most four 1's, and at most four 0's, in common.

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1
\end{pmatrix}$$

Alternatively, in this arrangement, the $20 \times \binom{3}{2} = 60$ vertical pairs occur four times in each of the 15 pairs of rows, and no such pair occurs as many as five times.

A-4 Let S be a set of ordered triples (a, b, c) of distinct elements of a finite set A. Suppose that:

(1) $(a, b, c) \in S$ if and only if $(b, c, a) \in S$,

(2) $(a, b, c) \in S$ if and only if $(c, b, a) \notin S$,

(3) (a, b, c) and (c, d, a) are both in S if and only if (b, c, d) and (d, a, b) are both in S.

Prove that there exists a one-to-one function $g : A \longrightarrow \mathbb{R}$ such that $g(a) < g(b) < g(c)$ implies $(a, b, c) \in S$.

Solution. Intuitively, one regards A as a subset of a circle and S as the set of triples in counterclockwise order. To obtain a linear order, we have to choose a starting point. Fixing $a_0 \in A$, we define a relation $<$ on A by

(i) For all $b \neq a_0$, $a_0 < b$.

(ii) If a_0, b, and c are all distinct, then $b < c$ if and only if $(a_0, b, c) \in S$.

By (1) and (2), for all $b \neq c$, either $b < c$ or $c < b$, but not both. By (1) and (3), $b < c$ and $c < d$ implies $b < d$. Thus $<$ gives A the structure of an ordered set. Defining $g(a) = |\{b \in A \mid b < a\}|$, we see that $g(a) < g(b) < g(c)$ implies $a < b$ and $b < c$; if $a = a_0$, then $(a, b, c) \in S$ by definition. Otherwise, $(a_0, a, b) \in S$, $(a_0, b, c) \in S$, and the result follows from (1) and (3).

Solution. If p is a prime number greater than 3, and $k = \lfloor 2p/3 \rfloor$, prove that the sum

$$\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$$

of binomial coefficients is divisible by p^2. (For example, $\binom{7}{1} + \binom{7}{2} + \binom{7}{3} + \binom{7}{4} = 7 + 21 + 35 + 35 = 2 \cdot 7^2$.)

Solution. Each binomial coefficient is divisible by p, since p divides the numerator and not the denominator of $\frac{p!}{r!(p-r)!}$. Thus we wish to show that

$$1 + \frac{p-1}{2} + \frac{(p-1)(p-2)}{2 \cdot 3} + \cdots + \frac{(p-1)\cdots(p-k+1)}{2 \cdot 3 \cdots k}$$

is divisible by p. The terms are all integers and we express the sum as a sum of fractions whose numerators are multiples of p and whose denominators are prime to p. The sum is equal to

$$\frac{pc_1}{1!} + \frac{pc_2}{2!} \cdots + \frac{pc_k}{k!} + \left(1 - \frac{1}{2} + \frac{1}{3} - \cdots + \frac{(-1)^{k-1}}{k}\right),$$

where the c_i are integers and the final parenthesis is, when $p = 6q + 1$ and $k = 4q$, equal to

$$\begin{aligned} 1 + \frac{1}{2} + \cdots + \frac{1}{4q} - 2\left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{4q}\right) &= \frac{1}{2q+1} + \frac{1}{2q+2} + \cdots + \frac{1}{4q} \\ &= \left(\frac{1}{2q+1} + \frac{1}{4q}\right) + \left(\frac{1}{2q+2} + \frac{1}{4q-1}\right) + \cdots + \left(\frac{1}{2q+q} + \frac{1}{4q-(q-1)}\right) \\ &= \frac{p}{(2q+1)4q} + \cdots + \frac{p}{3q(3q+1)} \end{aligned}$$

and, when $p = 6q + 5$ and $k = 4q + 3$, equal to

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{4q+3} - 2\left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{4q+2}\right) &= \frac{1}{2q+2} + \frac{1}{2q+3} + \cdots + \frac{1}{4q+3} \\ &= \left(\frac{1}{2q+2} + \frac{1}{4q+3}\right) + \left(\frac{1}{2q+3} + \frac{1}{4q+2}\right) + \cdots + \left(\frac{1}{2q+q+2} + \frac{1}{4q+(3-q)}\right) \\ &= \frac{p}{(2q+2)(4q+3)} + \frac{p}{(2q+3)(4q+2)} + \cdots + \frac{p}{(3q+2)(3q+3)}. \end{aligned}$$

A-6 Let $c \geq 0$ be a constant. Give a complete description, with proof, of the set of all continuous functions $f : \mathbb{R} \longrightarrow \mathbb{R}$, such that $f(x) = f(x^2 + c)$ for all $x \in \mathbb{R}$.

Solution. We begin with the general observation that $f(x) = f(x^2 + c) = f(-x)$, so f is always even. Conversely, the even extension of any continuous function on $[0, \infty)$ satisfies

the functional equation as long as the original function does. Therefore, we may and do restrict attention to $x \geq 0$ in everything that follows. We consider two cases.

Case 1: $0 \leq c \leq 1/4$. Here, $x^2 - x + c = 0$ has positive zeros, $a = (1 - \sqrt{1-4c})/2$ and $b = (1 + \sqrt{1-4c})/2$. If $0 \leq x_0 < b$ and we define $x_{n+1} = x_n^2 + c$, the monotonicity of $x^2 + c$ on $[0, \infty)$ implies that $x_0, x_1, \ldots$ is monotonic (increasing for $0 < x_0 < a$, decreasing for $a < x_0 < b$) and bounded, therefore convergent, and therefore convergent to a since the limit must satisfy $L = L^2 + c$. As

$$f(x_0) = f(x_1) = \cdots = \lim_{n\to\infty} f(x_n) = f\left(\lim_{n\to\infty} x_n\right) = f(a),$$

we have $f(x) = f(a)$ for all x, $0 \leq x < b$.

If $x_0 > b$, the monotonicity of $\sqrt{x-c}$ guarantees that $x_0 > \sqrt{x_0 - c} > b$, so we can define, recursively, $x_{n+1} = \sqrt{x_n - c}$. Again, the sequence (x_n) is bounded and monotonic; therefore it also has a limit, and this limit must be b. Then

$$f(x_0) = f(x_1) = \cdots = \lim_{n\to\infty} f(x_n) = f\left(\lim_{n\to\infty} x_n\right) = f(b).$$

As the range of f is finite and f is continuous, it is constant.

Case 2: $c > 1/4$. Now, $x \longrightarrow x^2 + c$ has no real fixed points. Setting $t_0 = 0$, $t_{n+1} = t_n^2 + c$, the sequence (t_i) is monotonic, so if it didn't go to infinity, it would have to converge to a (non-existent) fixed point. So each $x \geq 0$ is in some interval $[t_n, t_{n+1}]$.

Let g be any continuous function on the interval $[0, c]$ such that $g(c) = g(0)$. Define $\phi(x) = \sqrt{x-c}$ and

$$f(x) = \begin{cases} g(x) & \text{for } x \in [0, c] = [t_0, t_1] \\ g(\phi(x)) & \text{for } x \in [c, c^2 + c] = [t_1, t_2] \\ (\phi(\phi(x))) & \text{for } x \in [t_2, t_3] \\ \text{and in general} & \\ g(\underbrace{\phi(\phi(\cdots(\phi}_{n}(x))\cdots))) & \text{for } x \in [t_n, t_{n+1}]. \end{cases}$$

By construction, $f(x)$ satisfies the desired functional equation. Continuity is obvious except at the points t_i, where it follows from $g(c) = g(0)$. Conversely, every function $f(x)$ is determined by its values on $[0, c)$.

B-1 Define a **selfish** set to be a set which has its own cardinality (number of elements) as an element. Find, with proof, the number of subsets of $\{1, 2, \ldots, n\}$ which are *minimal* selfish sets, that is, selfish sets none of whose proper subsets are selfish.

Solution. There are F_n subsets of $\{1, 2, \ldots, n\}$ that are minimal selfish sets. Here F_n is the nth Fibonacci number, given recursively by $F_1 = F_2 = 1$, and $F_{k+2} = F_k + F_{k+1}$ or, in closed form, by $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$.

To show this, we first show that a subset $A \subseteq \{1, 2, \ldots, n\}$ is a minimal selfish set if and only if the *least* element of A is the cardinality of A. *If*: If the least element of A is the cardinality of A, then the cardinality of any proper subset $B \subset A$ is not an element of A, let alone of B, so B cannot be selfish; since A is selfish, A is a minimal selfish set. *Only if*: If A had an element a less than its cardinality, then one could omit elements of A so that the resulting proper subset B still contained a and had a as its cardinality, so B would be selfish and A would not be a minimal selfish set.

Now we can count the minimal selfish sets that are subsets of $\{1, 2, \ldots, n\}$ by looking at their least elements (= cardinalities). If the least element is i, then there are $i-1$ other elements, to be chosen from the $n-i$ elements $i+1, i+2, \ldots, n$ of $\{1, 2, \ldots, n\}$. Therefore, the desired number is

$$\sum_{i=1}^{n} \binom{n-i}{i-1} = \binom{n-1}{0} + \binom{n-2}{1} + \cdots,$$

which is well known (and can be shown by induction) to equal F_n.

B-2 Show that for every positive integer n,

$$\left(\frac{2n-1}{e}\right)^{\frac{2n-1}{2}} < 1 \cdot 3 \cdot 5 \cdots (2n-1) < \left(\frac{2n+1}{e}\right)^{\frac{2n+1}{2}}.$$

Solution. The statement is true for $n = 1$ (since $1 < e < 3$, and we have $(1/e)^{1/2} < 1 < (3/e)^{3/2}$) so we can get a proof by induction if we can show that

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

For the left-hand inequality, note that

$$\frac{\left(\frac{2n+1}{e}\right)^{\frac{2n+1}{2}}}{\left(\frac{2n-1}{e}\right)^{\frac{2n-1}{2}}} = \frac{2n+1}{e}\left(\frac{2n+1}{2n-1}\right)^{\frac{2n-1}{2}} = \frac{2n+1}{e}\left(1+\frac{2}{2n-1}\right)^{\frac{2n-1}{2}} < \frac{2n+1}{e}\cdot e = 2n+1.$$

For the right-hand inequality, we have

$$\frac{\left(\frac{2n+3}{e}\right)^{\frac{2n+3}{2}}}{\left(\frac{2n+1}{e}\right)^{\frac{2n+1}{2}}} = \frac{2n+3}{e}\left(\frac{2n+3}{2n+1}\right)^{\frac{2n+1}{2}} = \frac{2n+1}{e}\left(\frac{2n+3}{2n+1}\right)^{\frac{2n+3}{2}},$$

so it is enough to show $e < \left(\frac{2n+3}{2n+1}\right)^{\frac{2n+3}{2}}$. This can be done by taking logarithms:

$$\begin{aligned}
\ln\left(\frac{2n+3}{2n+1}\right)^{\frac{2n+3}{2}} &= \frac{2n+3}{2}\ln\left(1+\frac{2}{2n+1}\right) \\
&= \frac{2n+3}{2}\left(\frac{2}{2n+1} - \frac{1}{2}\left(\frac{2}{2n+1}\right)^2 + \frac{1}{3}\left(\frac{2}{2n+1}\right)^3 - \cdots\right) \\
&> \frac{2n+3}{2}\left(\frac{2}{2n+1} - \frac{1}{2}\left(\frac{2}{2n+1}\right)^2\right),
\end{aligned}$$

since the terms are decreasing in size and alternating in sign, and

$$\frac{2n+3}{2}\left(\frac{2}{2n+1}-\frac{1}{2}\left(\frac{2}{2n+1}\right)^2\right) = \frac{2n+3}{(2n+1)^2}(2n+1-1)$$
$$= \frac{4n^2+6n}{4n^2+4n+1} > 1.$$

B-3 Given that $\{x_1, x_2, \ldots, x_n\} = \{1, 2, \ldots, n\}$, find, with proof, the largest possible value, as a function of n ($n \geq 2$), of $x_1x_2 + x_2x_3 + \cdots + x_{n-1}x_n + x_nx_1$.

Solution. Let $F(n)$ be the desired maximum value. We will show that for $n \geq 3$, $F(n) = F(n-1) + n^2 - 2$. It will follow that

$$F(n) = F(2) + \sum_{k=3}^{n}(k^2-2) = 4 + \sum_{k=3}^{n}(k^2-2) = 3 + \sum_{k=1}^{n}(k^2-2)$$
$$= 3 + \frac{n(n+1)(2n+1)}{6} - 2n = \frac{2n^3+3n^2-11n+18}{6}.$$

To show $F(n) = F(n-1) + n^2 - 2$ it is convenient to show simultaneously, by induction on n, that the maximum value $F(n)$ can be reached with an arrangement for which $x_1 = n-1$, $x_n = n$. Note that we can certainly assume that $x_n = n$ by cyclically permuting $x_1, x_2, \ldots, x_n$. We then have

$$x_1x_2 + \cdots + x_{n-1}x_n + x_nx_1 = x_1x_2 + \cdots + x_{n-2}x_{n-1} + n(x_{n-1} + x_1)$$
$$= x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_{n-1}x_1 + n^2 - (n - x_{n-1})(n - x_1).$$

Since $n - x_{n-1}$ and $n - x_1$ are distinct positive integers, we have $(n - x_{n-1})(n - x_1) \geq 2$ and thus

$$x_1x_2 + \cdots + x_{n-1}x_n + x_nx_1 \leq x_1x_2 + \cdots + x_{n-1}x_1 + n^2 - 2 \leq F(n-1) + n^2 - 2.$$

If we choose $x_1, \ldots, x_{n-1}$ with $x_1 = n-2$, $x_{n-1} = n-1$, and $x_1x_2 + \cdots + x_{n-1}x_n$ has its maximum value $F(n-1)$, then both inequalities above will be equalities, showing that $F(n) = F(n-1) + n^2 - 2$. But since this maximum value can be reached for $x_{n-1} = n-1, x_n = n$, it can also (by reversing the order of $x_1, \ldots, x_n$ and permuting cyclically) be reached for $x_1 = n-1, x_n = n$, and we are done.

B-4 For any square matrix A, we can define $\sin A$ by the usual power series: $\sin A = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}A^{2n+1}$. Prove or disprove: There exists a 2×2 matrix A with real entries such that $\sin A = \begin{pmatrix} 1 & 1996 \\ 0 & 1 \end{pmatrix}$.

Solution. We'll show that there is *no* such matrix A. First of all, note that for any invertible matrix P and any square matrix B of the same size,

$$\sin(PBP^{-1}) = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}(PBP^{-1})^{2n+1} = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}PB^{2n+1}P^{-1}$$
$$= P\left(\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}B^{2n+1}\right)P^{-1} = P(\sin B)P^{-1}.$$

Thus the sines of similar matrices are similar.

Now any 2×2 matrix A with real entries is similar to either a diagonal matrix $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ with real or complex entries λ_1, λ_2, or a triangular matrix $\begin{pmatrix} \lambda & c \\ 0 & \lambda \end{pmatrix}$ with real entries λ, c (in fact, one can take $c = 1$). Therefore, $\sin A$ is similar to either $\sin\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ or $\sin\begin{pmatrix} \lambda & c \\ 0 & \lambda \end{pmatrix}$. But $\sin\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ will be a diagonal matrix, since all powers of $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ are diagonal, and no diagonal matrix is similar to $\begin{pmatrix} 1 & 1996 \\ 0 & 1 \end{pmatrix}$, since the latter matrix is not diagonalizable. So if $\sin A = \begin{pmatrix} 1 & 1996 \\ 0 & 1 \end{pmatrix}$, then there must be real numbers λ and c such that $\begin{pmatrix} 1 & 1996 \\ 0 & 1 \end{pmatrix}$ is similar to $\sin\begin{pmatrix} \lambda & c \\ 0 & \lambda \end{pmatrix}$.

Let $U = \begin{pmatrix} \lambda & c \\ 0 & \lambda \end{pmatrix}$. We compute $\sin U$ explicitly: we have $U^2 = \begin{pmatrix} \lambda^2 & 2\lambda c \\ 0 & \lambda^2 \end{pmatrix}$, $U^3 = \begin{pmatrix} \lambda^3 & 3\lambda^2 c \\ 0 & \lambda^3 \end{pmatrix}, \ldots$, and, by induction, $U^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1}c \\ 0 & \lambda^n \end{pmatrix}$. Therefore,

$$\begin{aligned} \sin U &= \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} \begin{pmatrix} \lambda^{2n+1} & (2n+1)\lambda^{2n}c \\ 0 & \lambda^{2n+1} \end{pmatrix} \\ &= \begin{pmatrix} \sum \frac{(-1)^n \lambda^{2n+1}}{(2n+1)!} & \sum \frac{(-1)^n \lambda^{2n}}{(2n)!} c \\ 0 & \sum \frac{(-1)^n \lambda^{2n+1}}{(2n+1)!} \end{pmatrix} \\ &= \begin{pmatrix} \sin\lambda & c\cos\lambda \\ 0 & \sin\lambda \end{pmatrix}. \end{aligned}$$

For this matrix to be similar to $\begin{pmatrix} 1 & 1996 \\ 0 & 1 \end{pmatrix}$, the double eigenvalue $\sin\lambda$ must equal 1. But then $\cos\lambda = 0$ and so $\sin U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is not similar to $\begin{pmatrix} 1 & 1996 \\ 0 & 1 \end{pmatrix}$ after all, so we have a contradiction, and we are done.

B-5 Given a finite string S of symbols X and O, we write $\triangle(S)$ for the number of X's in S minus the number of O's. For example, $\triangle(XOOXOOX) = -1$. We call a string S **balanced** if every substring T of (consecutive symbols of) S has $-2 \le \triangle(T) \le 2$. Thus, $XOOXOOX$ is not balanced, since it contains the substring $OOXOO$. Find, with proof, the number of balanced strings of length n.

Solution. For a balanced string S, let S' be the string obtained from S by reversing the last symbol (from O to X or vice versa). Call the string S *dangling* if S' is also balanced and *pinned* if S' is not balanced. For any n, let t_n be the total number of balanced strings, and let d_n, p_n be the numbers of dangling and pinned strings, respectively. Clearly, $t_n = d_n + p_n$, $d_1 = 2$, and $p_1 = 0$, since the two balanced strings X and O of length 1 are both dangling.

We will show that $d_{n+1} = 2p_n + 4$, $p_{n+1} = d_n - 2$. This implies that

$$d_{n+2} = 2(d_n - 2) + 4 = 2\,d_n \quad \text{and} \quad p_{n+2} = (2p_n + 4) - 2 = 2p_n + 2, \quad \text{so}$$

$$t_{n+2} = d_{n+2} + p_{n+2} = 2(d_n + p_n) + 2 = 2t_n + 2 \quad \text{and} \quad t_{n+2} + 2 = 2(t_n + 2).$$

Thus from $t_1 + 2 = 4$ we get $t_n + 2 = 2^{(n-1)/2} \cdot 4$, $t_n = 2^{(n+3)/2} - 2$ for n odd; from $t_2 + 2 = 6$ we get $t_n + 2 = 2^{(n-2)/2} \cdot 6$, $t_n = 3 \cdot 2^{n/2} - 2$ for n even.

To get the recurrences above, consider extending a balanced string S by one symbol, to SX or SO, so that the new string is still balanced. If S is a purely alternating string, $XOXO\cdots$ or $OXOX\cdots$, then S is dangling, and S can be extended both to SX and SO. So the two purely alternating strings of length n give rise to 4 dangling strings of length $n+1$. However, any other dangling string of length n can be extended in exactly one way, so the $d_n - 2$ other dangling strings of length n yield $d_n - 2$ pinned strings of length $n+1$. (If the last double letter in the dangling string was XX, then the new letter must be an O, and vice versa. Extending in this way will not "unbalance" the string, since it has alternated since that last double letter. Thus if the new symbol O created a substring with $\Delta(O) \leq -3$, we could truncate that substring before the last XX and show that the original string was unbalanced.)

Conversely, by similar arguments, if S is a pinned string, then S can always be extended both to SX and SO. (Note that if S ends in X, the last double letter in S must be OO, and vice versa, else S would not be pinned.) Thus the p_n pinned strings of length n give rise to $2p_n$ dangling strings of length $n+1$, for a total of $d_{n+1} = 4 + 2p_n$ along with the $p_{n+1} = d_n - 2$ pinned strings found previously, and we are done.

B-6 Let $(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)$ be the vertices of a convex polygon which contains the origin in its interior. Prove that there exist positive real numbers x and y such that

$$(a_1, b_1)x^{a_1}y^{b_1} + (a_2, b_2)x^{a_2}y^{b_2} + \cdots + (a_n, b_n)x^{a_n}y^{b_n} = (0, 0).$$

Solution. Choose $r > 0$ so that the polygon contains the disk of radius r centered at the origin. We first show that for every vector $\vec{v}$,

$$\max_i \{\vec{v} \cdot (a_i, b_i)\} \geq r\|\vec{v}\|.$$

Suppose this were false for a vector $\vec{v} \neq \vec{0}$. Note that the equation $\vec{w} \cdot \vec{v} = r\|\vec{v}\|$ defines the line perpendicular to $\vec{v}$ and tangent to the disk. Therefore, if $\vec{v} \cdot (a_i, b_i) < r\|\vec{v}\|$, the vertex (a_i, b_i) has to be to one side of that tangent line, and since not all the vertices can be on the same side of the tangent line, we must have $\vec{v} \cdot (a_i, b_i) \geq r\|\vec{v}\|$ for some i.

Therefore, if we set $f(x, y) = \sum_i x^{a_i}y^{b_i}$, we have

$$f(x, y) \geq \max_i \{x^{a_i}y^{b_i}\} = \exp\left(\max_i\{(\ln x, \ln y) \cdot (a_i, b_i)\}\right) \geq \exp\left(r\,\|(\ln x, \ln y)\|\right).$$

Therefore, as $\|(\ln x, \ln y)\| \longrightarrow \infty$, $f(x, y) \longrightarrow \infty$. For $R \gg 0$, therefore, $f(x, y) > f(1, 1)$ whenever (x, y) falls outside the square $[R^{-1}, R] \times [R^{-1}, R]$. The infimum of $f(x, y)$ over $\mathbb{R}^+ \times \mathbb{R}^+$ therefore equals the infimum over the closed and bounded set $[R^{-1}, R] \times [R^{-1}, R]$. As $f(x, y)$ is continuous on this square, it actually achieves this infimum at some point (x_0, y_0). But then $\dfrac{\partial f}{\partial x} = \dfrac{\partial f}{\partial y} = 0$ at (x_0, y_0), from which $x\dfrac{\partial f}{\partial x} = y\dfrac{\partial f}{\partial y} = 0$; equivalently,

$$a_1x^{a_1}y^{b_1} + \cdots + a_nx^{a_n}y^{b_n} = b_1x^{a_1}y^{b_1} + \cdots + b_nx^{a_n}y^{b_n} = 0,$$

as desired.

CONTENTS

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, NW
Washington, D.C. 20036