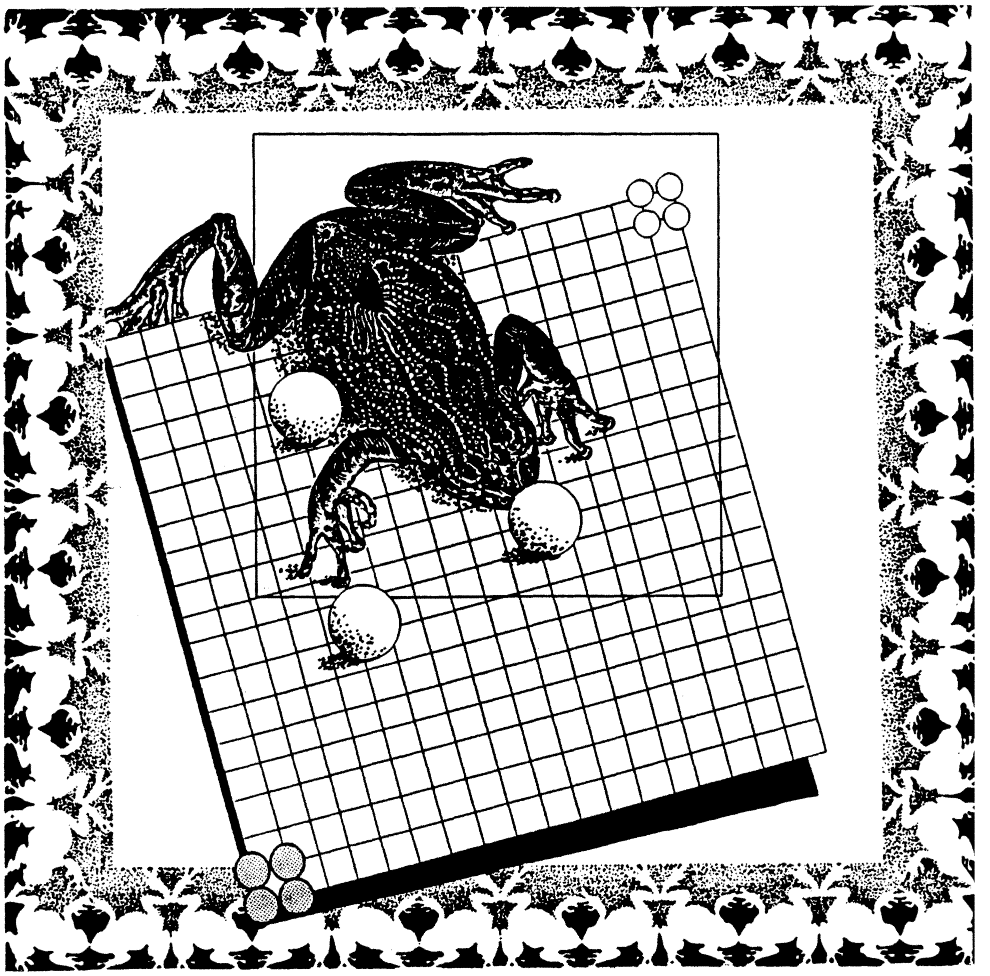
Vol. 66 No. 1, February 1993

MATHEMATICS MAGAZINE



- Mathematical Building Blocks
- Optimal Leapfrogging
- The Catalan Numbers Visit the World Series

An Official Publication of The MATHEMATICAL ASSOCIATION OF AMERICA

EDITORIAL POLICY

The aim of *Mathematics Magazine* is 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. Articles on pedagogy alone, unaccompanied by interesting mathematics, are not suitable. Neither are articles consisting mainly of computer programs unless these are essential to the presentation of some good mathematics. Manuscripts on history are especially welcome, as are those showing relationships between various branches of mathematics and between mathematics and other disciplines.

The full statement of editorial policy appears in this *Magazine*, Vol. 64, pp. 71–72, and is available from the Editor. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, nor published by another journal or publisher.

Send new manuscripts to: Martha Siegel, Editor, Mathematics Magazine, Towson State University, Towson, MD 21204. Manuscripts should be typewritten and double spaced and prepared in a style consistent with the format of *Mathematics Magazine*. Authors should submit the original and two 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. Illustrations should be carefully prepared on separate sheets in black ink, the original without lettering and two copies with lettering added. Do not use staples.

Cover design by Carolyn Westbrook. The fully illustrated frog is the marsupial frog of genus Nototrema taken from a 19th century wood engraving in *Animals A Pictorial Archive from Nineteenth-Century Sources,* selected by Jim Harter, Dover Publications, 1979.

AUTHORS

Israel Kleiner is professor of mathematics and statistics at York University in Toronto. He received his Ph.D. in ring theory from McGill University. His current research interests are the history of mathematics, mathematics eduction, and especially their interface. Professor Kleiner is the coordinator of an in-service Master's Programme for teachers of mathematics.

Abe Shenitzer received his Ph.D. from New York University. He is emeritus professor of mathematics at York University in Toronto. Dr. Shenitzer has published a number of expository articles and has translated Russian and German mathematical books and papers into English. He is interested in the history of mathematics and its use in teaching mathematics.

Joel Auslander studies mathematics and computer science at Harvard University, and is currently completing his junior year. Although his major is mathematics, his main interests are in computer science, in the fields of graphics and parallel algorithms. He attended the Hampshire Summer Studies in Mathematics program during the summers following his sophomore and junior years of high school.

Arthur Benjamin earned his Ph.D. in mathematical sciences from Johns Hopkins University in 1989 under the direction of Alan J. Goldman. He is currently assistant professor of mathematics at Harvey Mudd College. Benjamin's mental calculation techniques are described in his forthcoming book, *Mathemagics—How to Look Like a Genius without Really Trying.*

Daniel S. Wilkerson has been interested in problems of a combinatorial nature since he was fourteen, and has become convinced that finite combinatorics would make a better foundation for mathematics than set theory. He is currently a graduate student at the University of California at Berkeley, persuing a Ph.D. in mathematics. His other interests include the work of philosopher Werner Erhard, hypnosis, Zen, Hungarian, and Go.

Vol. 66 No. 1, February 1993

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

Mathematical Building Blocks

I. KLEINER
A. SHENITZER
York University
North York, Ontario, Canada M3J 1P3

Introduction

One way of studying mathematical objects is to decompose them into various combinations of relatively simple "building blocks." Such decompositions offer structural insights, computational advantages, and simplified proofs.

Composition and decomposition are two sides of the same coin. Which side is emphasized depends on the context. It is sometimes useful to view the Fundamental Theorem of Arithmetic as pointing to the decomposability of an integer into a (virtually) unique product of primes, while at other times it is useful to view it as pointing to the primes as the unique generators of the integers.

This essay is a collection of examples from different areas of mathematics that illustrate the above theme. They involve numbers, functions, groups, algebras, geometric transformations, matrices, and linear transformations. These mathematical objects are represented in our examples in ways analogous to writing an integer as a product of primes or writing a function as a linear combination of powers of $x - a$. Each example is accompanied by remarks of an historical or mathematical nature. Thus we are *not* presenting a mathematical analogue of a telephone book; we are presenting a critical catalogue of mathematical objects linked by a common theme. The level of difficulty varies with the subject matter.

Some decompositions of mathematical objects are more significant than others. For example, it is interesting and useful that every integer is a sum of four squares but it is of *inestimable importance* that every integer is a (virtually) unique product of primes. Again, it is mildly interesting and rather useful that every function can be written as a sum of an odd and an even function but it is of *inestimable importance* that any "reasonable" function on an interval is a linear combination of sines and cosines of multiple angles.

We stress that this collection of examples and comments is not a theory of linear combinations or of product representations, that it does not build up to any intellectual crescendo, and that it does not aspire to completeness. It does illustrate a key principle that guides the investigation of mathematical objects.

Multiplicative Building Blocks for the Integers

The Fundamental Theorem of Arithmetic (FTAr) asserts that every integer $\neq 0, \pm 1$ is a product of primes, unique up to order and multiplication by ± 1. In more picturesque terms, the primes, or the prime powers, are the unique building blocks for the integers.

The FTAr is very old. Its essence seems to have been known to Euclid (300 B.C.). The uniqueness aspect of the FTAr is both important and nonobvious. Indeed, uniqueness fails in the system of positive even integers $2, 4, 6, \dots,$ in which the primes are $2, 6, 10, 14, 18, \dots$ and in which the prime factorizations $36 = 6 \cdot 6 = 2 \cdot 18$ are genuinely different. The number and variety of applications of the FTAr are staggering. For example, the FTAr can be used to derive important properties of such key number-theoretic functions as the Euler φ-function and the Möbius function, to prove the divergence of the series $\Sigma(1/p)$ of reciprocals of the positive primes, and to study the growth of the function $\pi(x)$ ([15], Chapter 2). We add to this list the following two applications of the FTAr that are of special interest.

(a) If m and k are integers > 1 and $m \neq s^k$ for all integers s, then $\sqrt[k]{m}$ is irrational (see [14]).

The special case that $\sqrt{m}$ is irrational for a nonsquare integer m appeared in Euclid's *Elements*. A first step that led to this result was the Pythagoreans' discovery, made in the 5th century B.C., of the irrationality of $\sqrt{2}$ (or, as *they* put it, the incommensurability of the diagonal and the side of a square). This discovery was one of the turning points in the history of mathematics. Before it, Greek mathematicians made the plausible assumption that any two segments are commensurable. The counterexample of the diagonal and the side of a square resulted in the geometrization of Greek mathematics to the point where essentially algebraic results, such as the identity $(a+b)^2 = a^2 + 2ab + b^2$, were conceived geometrically. This development was both unavoidable and bad for mathematical progress. See [6], [19], [31] for details.

(b) To each polynomial $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ with integer coefficients associate the rational number $2^{a_0}3^{a_1}5^{a_2} \cdots p_n^{a_n}$, where p_n is the nth odd prime. The FTAr shows that this mapping is one–one. Thus the set of all such polynomials, and hence also the set of algebraic numbers, is denumerable.

A similar mapping is used in the proof of Gödel's Incompleteness Theorem, one of the great intellectual achievements of the 20th century. One "arithmetizes" a formal language by assigning to each formula of the language a unique "Gödel number" of the form $2^{m_1}3^{m_2}5^{m_3} \cdots p_n^{m_n}$, where the m_i are nonnegative integers denoting the Gödel numbers of the "elementary signs" of the language. See [24] for details.

Egyptian Additive Building Blocks for Fractions

Not all sets of building blocks are of equal importance.

Except for the fraction 2/3, the ancient Egyptians (beginning with the 17th century B.C.) worked only with unit fractions, that is, fractions of the form $1/n$. The reason is not known, although there are conjectures (see [6], [31]). Arbitrary fractions were written as sums of unit fractions with different denominators. (For any such fraction this can be done in infinitely many ways!) The Egyptians developed effective algorithms for operations with fractions in terms of unit fractions (see [31] for details). But the mathematical significance of the Egyptian approach to addition of fractions is slight.

Additive Building Blocks for the Reals

If $a_0 \cdot a_1a_2a_3 \dots$ is the decimal representation of a real number α, then α can be written as a linear combination of powers of 10:

$$\alpha = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots.$$

It is possible to define addition and multiplication of these series and thus get a "realistic" description of the field of real numbers. This representation makes obvious the connection between rationals and reals. See [26] for details.

Multiplicative Building Blocks for Invertible Matrices

A matrix is *elementary* if it is obtained from the identity matrix by one of the three so-called elementary row operations. Elementary matrices are invertible. Moreover, they are the building blocks of invertible matrices: Every invertible matrix A is a (nonunique) product of elementary matrices, $A = E_1 E_2 \cdots E_n$. It follows that $E_n^{-1} \cdots E_2^{-1} E_1^{-1} A = I$ and that $E_n^{-1} \cdots E_2^{-1} E_1^{-1} = A^{-1}$. Since the inverse of an elementary matrix is also elementary, and since premultiplying a matrix by an elementary matrix is equivalent to performing an elementary row operation on a matrix, the above two identities show that the same sequence of elementary row operations that reduces A to I (viz. $E_1^{-1}, E_2^{-1}, \ldots, E_n^{-1}$) will also reduce I to A^{-1}. This provides a standard algorithm for computing the inverse of a matrix. See [4].

Elementary matrices can also be used to show that if B is a left inverse of A ($BA = I$), then it is also a right inverse of A ($AB = I$)—a nontrivial result. Writing a nonsingular matrix as a product of elementary matrices implies that a nonsingular homogeneous linear transformation of the plane may be represented as a product of shears, compressions (or elongations), and reflections (see [4], p. 218).

Multiplicative Building Blocks for Geometric Transformations

We discuss decompositions of the elements of the groups associated with a few plane geometries.

(i) Every isometry of the plane is a product of at most three reflections. (i′) Every isometry of the plane is a product of an orthogonal transformation and a translation. (ii) Every similarity of the plane is a product of a central similarity and an isometry. (iii) Every affine transformation of the plane is a product of a similarity and an affinity (an affine transformation that leaves some line pointwise fixed). (iv) Every projective transformation of the projective plane is a product of perspectivities. (v) Every circular transformation of the inversive plane is a similarity or a product of a similarity by an inversion.

What is the use of such factorizations? Here is one answer: Felix Klein defined a geometry as the totality of invariants of a group of transformations of a set. The task of finding such invariants is simplified when it is reduced to finding common invariants of the factors of a transformation belonging to the group. Thus an isometry preserves angles because its constituent reflections do. A similarity preserves angles because central similarities and isometries do. Since perspectivities and inversions preserve the cross ratio of collinear tetrads of points, the same is true of projective and circular transformations, and so on (see [23] for details).

Multiplicative Building Blocks in Domains of Algebraic Integers

For over two thousand years "arithmetic" meant the arithmetic of whole numbers. In connection with his work on biquadratic reciprocity Gauss found it important to introduce the arithmetic of what we now call Gaussian integers. This revolutionary idea was the first step toward the arithmetic of integral domains of algebraic integers and toward the subsequent creation of algebraic number theory—a beautiful branch of mathematics and a treasure house of indispensable tools for the solution of otherwise intractable problems involving rational integers. Here are a few details that illustrate these generalities and shed light on the status of the FTAr in domains of algebraic integers.

If a and b are relatively prime integers whose product is a square, then, up to a unit, a and b are also squares. This result holds in any unique factorization domain (UFD). In particular, it holds in the domain $Z[i]$ of Gaussian integers and can be used to obtain the integer solutions of $x^2+y^2=z^2$. Specifically, let $\{x, y, z\}$ be a primitive Pythagorean triple, that is, a solution triple of $x^2+y^2=z^2$ with $(x, y, z)=1$. Since the Gaussian integers $x+iy$ and $x-iy$ can be shown to be relatively prime in $Z[i]$ and $(x+iy)(x-iy)=x^2+y^2=z^2$, it follows that $x+iy=(a+bi)^2=(a^2-b^2)+2abi$. Hence $x=a^2-b^2$, $y=2ab$. But then $z=\pm(a^2+b^2)$. These formulas yield all primitive Pythagorean triples (see [21] for details).

Much the same idea was used by mathematicians in the early 19th century in attempts to prove Fermat's Last Theorem (FLT) (see [11] for historical details). It is enough to consider the case of odd prime exponents. Factor the left side of $x^p+y^p=z^p$ in the domain $Z[\omega]$ of cyclotomic integers: $x^p+y^p=(x+y)(x+y\omega)\cdots(x+y\omega^{p-1})$, where ω is a primitive pth root of unity. Unique factorization in $Z[\omega]$ establishes FLT (see [5], p. 156). However, $Z[\omega]$ is not a UFD for most p (the first p for which it is not is 23). To restore unique factorization in $Z[\omega]$, and, more generally, in the domain of integers of any algebraic number field, Dedekind invented ideals and showed that in such domains every ideal is a unique product of prime ideals—a discovery Abraham Robinson refers to as "paradise regained." Using these ideas one can prove FLT for all "regular" primes (see [5], [21]). (A prime p is *regular* if for any ideal I of $Z[\omega]$, I is principal whenever I^p is principal.) In the 1920s Emmy Noether extended Dedekind's ideas to so-called Dedekind domains. In such domains every ideal is a unique product of prime ideals (see [21] for details).

Ideals are of fundamental importance not only in algebraic number theory but also in algebra and in analysis. Their importance far transcends the original reason for their invention. This illustrates a common phenomenon in the evolution of mathematics.

Multiplicative Building Blocks for Polynomials

The result for polynomials analogous to the FTAr for integers states that every polynomial with coefficients in some field F is a unique product of primes (the primes here are the irreducible polynomials). If $F=\mathbb{R}$, the field of real numbers, then the primes are of degree one or two. If $F=\mathbb{C}$, then the primes are of degree one. Either statement is known as the Fundamental Theorem of Algebra (FTAL).

The unique factorization of polynomials is as important in field theory as the unique factorization of integers is in number theory. It often reduces questions about polynomials to questions about irreducible (prime) polynomials. For example, to prove that every polynomial over a field has a root in some extension field (which implies the existence of the splitting field of a polynomial) it suffices to restrict oneself to the irreducible factors of the polynomial (see [17], p. 219).

A basic geometric result that is a rather direct consequence of the FTAL is Bézout's Theorem. This theorem asserts that if C_m and C_n are complex algebraic curves whose equations in homogeneous coordinates have degrees m and n, respectively, then these curves meet in mn points ([28], pp. 205–206).

(a) Every finite abelian group is a direct sum of cyclic groups of prime-power order. These cyclic groups are indecomposable; that is, they cannot be expressed as direct sums of (proper) subgroups. The direct sum is essentially unique and hence the cyclic groups of prime-power order are the unique building blocks (here the terms "additive" and "multiplicative" lose their significance) for finite abelian groups. This result, known as the Basis Theorem for finite abelian groups, describes completely the "structural possibilities" for such groups. For example, there are six nonisomorphic abelian groups of order 108 corresponding to the six distinct ways of writing 108 as a product of primes $(2^2 \cdot 3^3, 2 \cdot 2 \cdot 3^3, 2^2 \cdot 3^2 \cdot 3, 2^2 \cdot 3 \cdot 3 \cdot 3, 2 \cdot 2 \cdot 3^2 \cdot 3, 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3)$. For details see [27].

The Basis Theorem was obtained by Frobenius and Stickelberger in 1879. It was the first structure theorem for algebraic systems, and was soon followed by others. It was extended later in the century to finitely generated abelian groups, and in the 20th century it was extended still further to finitely generated modules over principal ideal domains. The rational and Jordan canonical decompositions of a matrix or a linear transformation follow from the last result (see [17] for details).

(b) Let G be an arbitrary group. If G satisfies either the ascending or descending chain condition (for normal subgroups) then it is a direct product of a finite number of indecomposable groups. If G satisfies both chain conditions, then such a decomposition is unique: $G = H_1 \times H_2 \times \cdots \times H_m = K_1 \times K_2 \times \cdots \times K_n$ implies $m = n$ and $H_i \cong K_i$ (possibly after rearrangement; "$\cong$" denotes isomorphism). The latter result is known as the Remak-Krull-Schmidt Theorem. It can be used to prove the uniqueness of decomposition in the Basis Theorem in (a) above, as well as to prove the following "cancellation theorem": If G satisfies both chain conditions, then $G \cong A \times B$ and $G \cong A \times C$ imply $B \cong C$ (see [27]).

Wedderburn (in 1909) was first to give a proof of the Remak-Krull-Schmidt Theorem for *finite* groups. The theorem was later extended by Remak, Krull, Schmidt, and others. It holds for algebraic systems other than groups, e.g., modules and lattices. In the context of modules it can be used to derive another "cancellation" result: If $M_m(E) \cong M_n(F)$, then $m = n$ and $E \cong F$ (E and F are fields; $M_m(E)$ denotes the ring of $m \times m$ matrices with entries in E). See [17].

(c) A group G has a *composition series* if it has subgroups G_i $(i = 0, 1, \ldots, n)$, where $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$, G_{i+1} is a normal subgroup of G_i, and the *composition factors* G_i/G_{i+1} are simple groups. Each finite group has a composition series. In general, a group has a composition series if and only if it satisfies both chain conditions on "subnormal" subgroups. Any two composition series for a group (if such exist) are "equivalent": $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ and $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$ implies $m = n$ and $G_i/G_{i+1} \cong H_i/H_{i+1}$ (after rearrangement). This is the Jordan-Hölder Theorem (there is an analogue for lattices). It is fundamental in the study of the solvability of equations by radicals: An equation is solvable by radicals if and only if its Galois group is a "solvable group," that is, its composition factors are abelian. The result is present in skeletal form in Galois' work (circa 1830) on the solvability of equations (see [4], [17]).

The Jordan-Hölder Theorem determines for a finite group a unique set of simple groups, namely its composition factors. Conversely, given the composition factors of a group G, we can recover the group if we can solve the "extension problem": Recover a group H given a normal subgroup K of H and the group H/K. If we can do this, then we can recover G_{n-1} from G_n and G_{n-1}/G_n, G_{n-2} from G_{n-1} and G_{n-2}/G_{n-1}, and so on, and thus "climb up" to G. In this sense G is a "product" of (i.e., can be determined from) its composition factors (see [27] for details). We see that we could determine all finite groups if we know all finite simple groups and were able to solve the extension problem. Although all finite simple groups have recently been determined (see [2]), the extension problem has not yet been resolved.

The Jordan-Hölder Theorem can be used to prove the uniqueness of the decomposition of an integer n into primes: Let $n = p_1 p_2 \cdots p_m$, where the p_i are (not necessarily distinct) primes. Let $\sigma(n)$ denote a cyclic group of order n and $\langle a \rangle$ the cyclic group generated by a. If $G = \sigma(n)$ has generator x, then

$$G = \langle x \rangle \supset \langle x^{p_1} \rangle \supset \langle x^{p_1 p_2} \rangle \supset \cdots \supset \langle x^{p_1 p_2 \cdots p_{m-1}} \rangle \supset \{1\}$$

is a composition series. Indeed, its factors are $\sigma(p_1), \sigma(p_2), \ldots, \sigma(p_m)$, and, since their orders are prime, they are simple. The Jordan-Hölder Theorem states that these factors, hence their orders, depend only on $G = \sigma(n)$ and not on the choice of the composition series (see [27], p. 107).

Building Blocks for Algebras

(a) In the 1870s Sophus Lie associated Lie algebras with Lie groups that he introduced to study differential equations. He then posed the problem of determining the structure of Lie algebras as an aid in the study of the Lie groups with which they are associated. Elie Cartan and Killing solved the problem in the 1880s by giving a structure theorem for a certain class of Lie algebras: Every finite-dimensional semi-simple Lie algebra (i.e., one without nonzero solvable ideals) over $\mathbb{R}$ or $\mathbb{C}$ is a (finite) direct sum of simple Lie algebras. (A Lie algebra is "simple" if it has no proper ideals.) They then characterized the simple Lie algebras (see [16] for details).

(b) In the 1890s Cartan, using as a model his work with Lie algebras, arrived at an analogous result for associative algebras: Every finite-dimensional semi-simple associative algebra (i.e., one without nonzero nilpotent ideals) over $\mathbb{R}$ or $\mathbb{C}$ is a (finite) direct sum of simple algebras; the latter are matrix algebras over division algebras. Moreover, such a decomposition is unique (up to isomorphism). In 1907 Wedderburn extended Cartan's result to algebras over arbitrary fields, and in 1927 Emil Artin extended these results to (semi-simple) rings with the descending chain condition on ideals. Artin's work proved to be a model and inspiration for subsequent work in ring theory. See [18] for historical details.

Additive Building Blocks for Functions

(a) If $f(x)$ is infinitely differentiable at b, then we can write it formally as $f(x) = f(b) + f'(b)(x-b) + (f''(b)/2!)(x-b)^2 + \cdots$. If the power series on the right converges to f in some neighborhood of b, then this expansion of f as a linear combination of powers of $x - b$ is unique.

The expansion of functions in power series is a powerful technique in analysis. It had its origins in the invention of the calculus by Newton and Leibniz in the last third of the 17th century. In fact, it was the tool they needed to extend their calculus algorithms to transcendental functions. To differentiate or integrate such a function, one would expand it in a power series and differentiate or integrate the power series term by term (questions of convergence were not considered at that time). Power series were also the key element in Lagrange's attempt to rigorize the calculus. See [10], [19] for details.

Power series expansions of the trigonometric, logarithmic, and exponential functions were obtained in the 17th and early 18th centuries. For example, Newton obtained the series expansion of sin x as follows: Consider the unit circle in FIGURE 1. We have $\sin t = x$, hence $t = \arcsin x$. The area, A, of the sector is $A = (1/2)t$. Hence

$$\arcsin x = t = 2A = 2\int_0^x \sqrt{1-w^2}\,dw - x\sqrt{1-x^2}.$$

By applying to $\sqrt{1-x^2}$ his extension of the binomial theorem to fractional exponents, Newton replaced $2\int_0^x\sqrt{1-w^2}\,dw - x\sqrt{1-x^2}$ by a power series $\Sigma a_n x^n$. He then "inverted" $\Sigma a_n x^n$ to get the power series for sin x (see **[10]**, pp. 205–206).

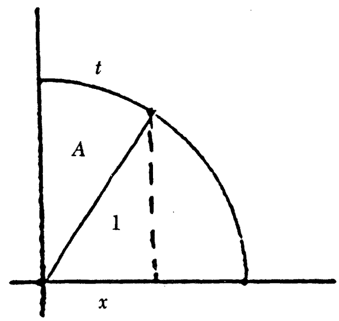


FIGURE 1

The belief that every function has a power series representation was widespread among 18th-century mathematicians. Given the modern notion of function, this belief is, of course, false. Representability by a power series is the prerogative of a relatively small (but very important) class of functions.

(b) Real analytic functions are "shadows" of (complex) analytic functions, and analytic functions are a subset of the class of meromorphic functions. If $g(z)$ is a meromorphic function and d is an isolated singularity of g, then g is analytic in an annulus M about d and can be uniquely represented in M as a linear combination of integral powers of $z - d$: $g(z) = \Sigma_{-\infty}^{\infty} s_n(z-d)^n$. This is the *Laurent* (series) *expansion* of g about d (**[1]**, **[26]**).

(c) The first to promote sines and cosines of multiple angles as universal functional building blocks was Daniel Bernoulli. The suggestion of this brilliant mathematical physicist, made in the mid-18th century in connection with the vibrating-string controversy, was opposed by such giants as Euler and d'Alembert. Bernoulli's bold conjecture was elaborated and persuasively defended in the beginning of the 19th century by Fourier. Specifically, Fourier claimed that every function $f(x)$ on an interval $(-c, c)$ can be written as a linear combination of sines and cosines:

$$f(x) = \frac{a_0}{2} + a_1\cos\frac{\pi x}{c} + b_1\sin\frac{\pi x}{c} + a_2\cos\frac{2\pi x}{c} + b_2\sin\frac{2\pi x}{c} + \cdots,$$

where

$$a_n = \frac{1}{c}\int_{-c}^{c} f(t)\cos\frac{n\pi t}{c}\,dt, \qquad b_n = \frac{1}{c}\int_{-c}^{c} f(t)\sin\frac{n\pi t}{c}\,dt.$$

Fourier's discovery was made in connection with his solution of the heat equation

$$\frac{\partial y}{\partial t} = k^2\frac{\partial^2 y}{\partial x^2}.$$

Although incorrect in the generality stated by him, the discovery was nevertheless one of the great events in the history of mathematics in general and of analysis in particular. Its vast implications reverberate to this day ([30], [32]).

The humble prototype of the expansion of a function in a Fourier series is the representation of a vector $\vec{v}$ in the plane as a linear combination of orthonormal basis vectors $\vec{e}_1, \vec{e}_2$. The representation in question is $\vec{v} = (\vec{v}, \vec{e}_1)\vec{e}_1 + (\vec{v}, \vec{e}_2)\vec{e}_2$. Also, $(\vec{v}, \vec{e}_1)^2 + (\vec{v}, \vec{e}_2)^2 = (\vec{v}, \vec{v})^2$ (Pythagoras' Theorem).

Now we consider in some detail Fourier series expansions of functions. It is convenient to work with continuously differentiable functions f on $[-\pi, \pi]$ such that $f(\pi) = f(-\pi)$. If we define the inner product (f, g) of f and g as $(f, g) = \int_{-\pi}^{\pi} f(x)g(x)\,dx$, then (1) the functions $1, \cos x, \sin x, \cos 2x, \sin 2x, \ldots$ form a complete orthogonal system and the functions

$$\frac{1}{\sqrt{2\pi}}, \frac{\cos x}{\sqrt{\pi}}, \frac{\sin x}{\sqrt{\pi}}, \frac{\cos 2x}{\sqrt{\pi}}, \frac{\sin 2x}{\sqrt{\pi}}, \ldots$$

form a complete orthonormal system, (2) $f(x) = (a_0/2) + a_1 \cos x + b_1 \sin x + a_2 \cos 2x + b_2 \sin 2x + \cdots$, (3) the series on the right converges (uniformly) to f, and (4) the *Parseval equality*—the analogue of Pythagoras' Theorem—holds:

$$\frac{1}{\pi}\|f\|^2 = \frac{a_0^2}{2} + a_1^2 + b_1^2 + a_2^2 + b_2^2 + \cdots.$$

If we use the Lebesgue (rather than the Riemann) integral, then the above expansions hold for every Lebesgue square-integrable function f on $[-\pi, \pi]$. See [9], [20], [30] for details.

A very general form of these results is the following theorem: In a separable Hilbert space H every orthonormal system is countable and there is a complete orthonormal system. If $\varphi_1, \varphi_2, \varphi_3, \ldots$ is a complete orthonormal system and x any element of H, then we have $x = \sum_{\nu=1}^{\infty} a_\nu \varphi_\nu$, where $a_\nu = (x, \varphi_\nu)$. Moreover, $\|x\|^2 = \sum_{\nu=1}^{\infty} |a_\nu|^2$ (see [13], [20]).

For the many physical applications of Fourier series see, e.g., [9] and [30].

(d) Using the division algorithm for polynomials, we can write any rational function $a(x)/g(x)$ ($a(x), g(x) \in F[x]$) in the form $b(x) + (f(x)/g(x))$, where $b(x), f(x) \in F[x]$ and $\deg. f(x) < \deg. g(x)$. If $g(x) = p_1(x)^{m_1} p_2(x)^{m_2} \cdots p_k(x)^{m_k}$, where the $p_i(x)$ are distinct primes in $F[x]$, we get the following decomposition:

$$\frac{f(x)}{g(x)} = \frac{a_1(x)}{p_1(x)^{m_1}} + \cdots + \frac{a_k(x)}{p_k(x)^{m_k}}.$$

Here $a_i(x) \in F[x]$ are uniquely determined and $\deg. a_i(x) < \deg. p_i(x)^{m_i}$. If we write each $a_i(x)$ in "base $p_i(x)$",

$$a_i(x) = a_{i_0}(x) + a_{i_1}(x)p_i(x) + a_{i_2}(x)p_i(x)^2 + \cdots + a_{i_t}(x)p_i(x)^t,$$

where $\deg. a_{i_j}(x) < \deg. p_i(x)$, then we have

$$\frac{a_i(x)}{p_i(x)^{m_i}} = \frac{a_{i_0}(x)}{p_i(x)^{m_i}} + \frac{a_{i_1}(x)}{p_i(x)^{m_i - 1}} + \cdots + \frac{a_{i_t}(x)}{p_i(x)^{m_i - t}}.$$

Putting the above two decompositions together we get the *partial fraction decomposition* of the rational function $f(x)/g(x)$ into a sum of terms of the form $c_i(x)/p_i(x)^{s_i}$, where $\deg. c_i(x) < \deg. p_i(x)$ (see [7], p. 145).

If $F=\mathbb{R}$, we can use the FTAL to decompose $g(x)$ into linear and quadratic factors, yielding the usual partial fraction decomposition of a rational function studied in calculus. This decomposition implies that the indefinite integral of every rational function (as a function over $\mathbb{R}$ rather than as a formal quotient of polynomials) is a sum of elementary functions.

If $F=\mathbb{C}$, then $f(x)/g(x)$ reduces to the (unique) sum of a constant and the principal parts of its Laurent expansions about ∞ and about the zeros of $g(x)$. See (b) above and [26], pp. 137–138.

Another use of the partial fraction decomposition is to find an explicit formula for the number of ways of partitioning an integer into sums of 1s, 2s, and 3s (see [7], p. 152).

Multiplicative Building Blocks for Normal Transformations

We recall some definitions:

(i) Let V be a vector space over $\mathbb{C}$ with hermitian scalar product (u, v). Let T belong to $L(V, V)$, the space of linear mappings of V into V. A linear transformation T' in $L(V, V)$ is called the *adjoint* of T if $(Tu, v)=(u, T'v)$ for all u, v in V.

(ii) A linear transformation T in $L(V, V)$ is *self-adjoint* if $T=T'$; it is *normal* if $TT'=T'T$. In matrix terms, a linear transformation is self-adjoint if its matrix with respect to an orthonormal basis is symmetric.

We can now state the Spectral Theorem for Normal Transformations, one of the key theorems of linear algebra (see [8], [12]): Let T be a normal transformation on a finite-dimensional vector space V over $\mathbb{C}$ with a hermitian scalar product and let $\lambda_1, \dots, \lambda_s$ be its distinct eigenvalues. Then there are self-adjoint idempotent transformations $E_1, \dots, E_s$ such that $1=E_1+\cdots+E_s$, $E_iE_j=0$ if $i\neq j$, and T is a linear combination of the E_i, $T=\lambda_1E_1+\cdots+\lambda_sE_s$. We call this the *spectral decomposition* of T; the eigenvalues of T constitute its spectrum.

One of the host of consequences of the spectral theorem is the possibility of reducing a quadratic form to a linear combination of squares (the Principal Axis Theorem). Another is that a symmetric matrix can be diagonalized by means of an orthogonal transformation ([4]).

The spectral theorem can be extended to bounded normal transformations on a Hilbert space (see [12] and [13]). The importance of this extension is attested to by the following quotation ([13], p. 192):

> After the spectral theorem [on a Hilbert space] is proved, it is easy to deduce from it the generalized versions of our theorems concerning square roots, the functional calculus, the polar decomposition, and properties of commutativity, and, in fact, to answer practically every askable question about bounded normal transformations [on a Hilbert space].

Concluding Remarks

The topic of building blocks is open-ended. We hope that readers will want to enlarge our "critical catalogue" with their own examples. Here are a few suggestions.

(a) Functions are often represented as infinite products. Euler factored $\sin x$ into an infinite product of polynomials and thereby obtained the relation

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots=\frac{\pi^2}{6}$$

([**19**], p. 449).

(b) The ring of "integral" quaternions is a (noncommutative) unique factorization domain. It follows that every positive integer can be written as a sum of four squares ([**14**], p. 303).

(c) Every map $f\colon A \to B$ (A and B sets) can be written as $f = gh$, where g is one–one, and h is onto. If A and B are groups (rings, modules), and f is a homomorphism, then the above factorization of f yields the First Isomorphism Theorem for groups (rings, modules) ([**17**], pp. 10–14).

(d) In a Noetherian ring every ideal is a finite intersection of primary ideals (corresponding to prime powers in the integers). This "factorization" yields (in algebraic geometry) the decomposition of a variety into a finite union of irreducible varieties ([**3**], p. 50).

(e) The Weierstrass Factorization Theorem represents an entire function as an infinite product. This theorem extends the decomposition of a polynomial into a product of linear factors ([**19**], p. 667 or [**26**], p. 157).

(f) The notion of triangulation of a manifold, namely its division into parts that are homeomorphic to a triangle or its analogues in higher dimensions, is fundamental in algebraic topology ([**22**]).

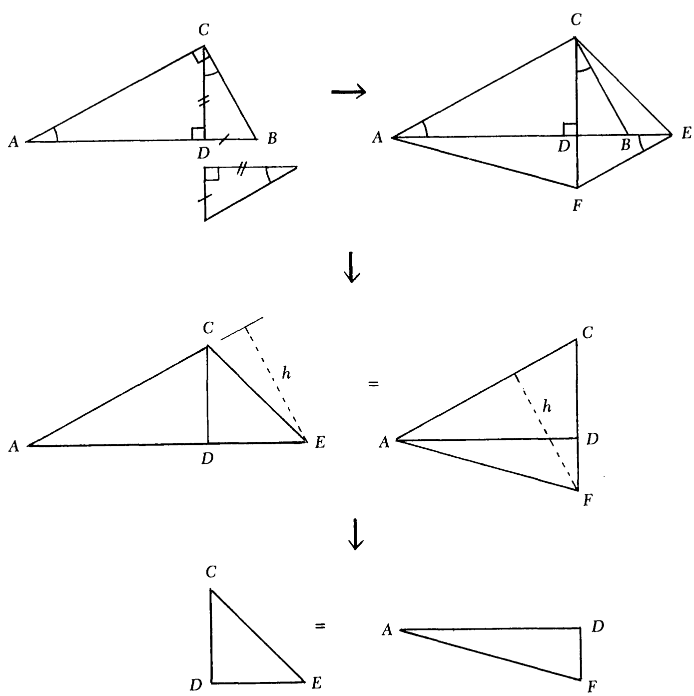
(g) A very recent mathematical development—wavelet theory—is claimed to be a significant advance over Fourier analysis. In this theory, purported to have numerous applications, the building blocks are so-called wavelets. The problem with sines and cosines, the units of Fourier analysis, is that they undulate forever in both directions. The units of wavelet analysis, however, are concentrated in short intervals ([**29**]).

REFERENCES

1. Lars Ahlfors, *Complex Analysis*, 3rd edition, McGraw-Hill Book Co., New York, 1979.
2. Michael Aschbacher, The classification of the finite simple groups, *Math. Intelligencer*, 3:2 (1981), 59–65.
3. M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., Reading, MA, 1969.
4. G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, 3rd edition, Macmillan Publishing Co., New York, 1977.
5. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
6. Carl Boyer, *A History of Mathematics*, 2nd edition, revised by Uta Merzbach, John Wiley & Sons, Inc., New York, 1989.
7. Lindsay Childs, *A Concrete Introduction to Higher Algebra*, Springer-Verlag New York, Inc., New York, 1979.
8. Charles Curtis, *Linear Algebra*, 3rd edition, Allyn and Bacon, Boston, 1974.
9. H. Dym and H. P. McKean, *Fourier Series and Integrals*, Academic Press, New York, 1972.
10. Charles Edwards, *The Historical Development of the Calculus*, Springer-Verlag New York, Inc., New York, 1979.
11. Harold Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag New York, Inc., New York, 1977.
12. Paul Halmos, *Finite-Dimensional Vector Spaces*, 2nd edition, Van Nostrand Reinhold Co., Inc., New York, 1958.
13. ______, *Introduction to Hilbert Space*, 2nd edition, Chelsea Publishing Co., Inc., New York, 1951.
14. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th edition, Oxford Univ. Press, London, 1960.
15. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag New York, Inc., New York, 1982.

16. Nathan Jacobson, *Lie Algebras*, John Wiley & Sons, Inc., New York, 1962.
17. ______, *Basic Algebra I*, W. H. Freeman & Co., San Francisco, 1974.
18. Israel Kleiner, A sketch of the evolution of (noncommutative) ring theory, *L'Enseign. Math.* 33 (1987), 227–267.
19. Morris Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford Univ. Press, New York, 1972.
20. A. N. Kolmogorov and S. V. Fomin, *Elements of the Theory of Functions and Functional Analysis*, 2 vols., Graylock Press, Rochester, NY, 1957.
21. Daniel Marcus, *Number Fields*, Springer-Verlag New York, Inc., New York, 1977.
22. William Massey, *Algebraic Topology: An Introduction*, Harcourt, Brace and World, 1967.
23. P. S. Modenov and A. S. Parkhomenko, *Geometric Transformations*, 2 vols., Academic Press, New York, 1965.
24. E. Nagel and J. R. Newman, *Gödel's Proof*, New York University Press, New York, 1960.
25. Ivan Niven, *Numbers: Rational and Irrational*, Random House Inc., New York, 1961.
26. Joseph Ritt, *Theory of Functions*, King's Crown Press, New York, 1947.
27. Joseph Rotman, *The Theory of Groups: An Introduction*, 2nd edition, Allyn and Bacon, Boston, 1973.
28. John Stillwell, *Mathematics and its History*, Springer-Verlag New York, Inc., New York, 1989.
29. Gilbert Strang, Wavelets and dilation equations: A brief introduction, *SIAM Review*, 31:4 (1989), 614–627.
30. Georgi Tolstov, *Fourier Series*, Prentice Hall Inc., Englewood Cliffs, NJ, 1962. (Translated from the Russian by R. A. Silverman.)
31. Bartel van der Waerden, *Science Awakening*, Noordhoff, Groningen, 1954.
32. Edward Van Vleck, The influence of Fourier's series upon the development of mathematics, *Science* 39 (1914), 113–124.

Proof without Words:
Area and the Projection Theorem of a Right Triangle

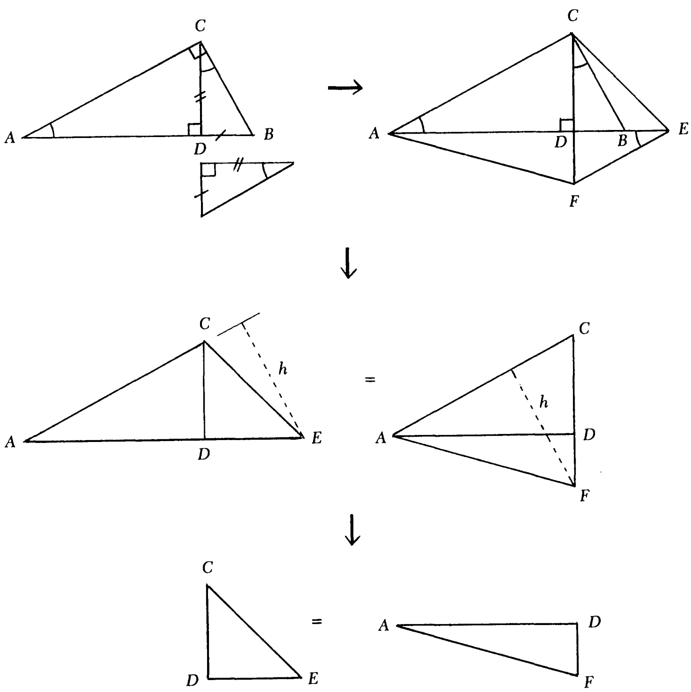


$$CD^2 = AD \cdot DB$$

—SIDNEY H. KUNG
JACKSONVILLE UNIVERSITY
JACKSONVILLE, FL 32211

16. Nathan Jacobson, *Lie Algebras*, John Wiley & Sons, Inc., New York, 1962.
17. ______, *Basic Algebra I*, W. H. Freeman & Co., San Francisco, 1974.
18. Israel Kleiner, A sketch of the evolution of (noncommutative) ring theory, *L'Enseign. Math.* 33 (1987), 227–267.
19. Morris Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford Univ. Press, New York, 1972.
20. A. N. Kolmogorov and S. V. Fomin, *Elements of the Theory of Functions and Functional Analysis*, 2 vols., Graylock Press, Rochester, NY, 1957.
21. Daniel Marcus, *Number Fields*, Springer-Verlag New York, Inc., New York, 1977.
22. William Massey, *Algebraic Topology: An Introduction*, Harcourt, Brace and World, 1967.
23. P. S. Modenov and A. S. Parkhomenko, *Geometric Transformations*, 2 vols., Academic Press, New York, 1965.
24. E. Nagel and J. R. Newman, *Gödel's Proof*, New York University Press, New York, 1960.
25. Ivan Niven, *Numbers: Rational and Irrational*, Random House Inc., New York, 1961.
26. Joseph Ritt, *Theory of Functions*, King's Crown Press, New York, 1947.
27. Joseph Rotman, *The Theory of Groups: An Introduction*, 2nd edition, Allyn and Bacon, Boston, 1973.
28. John Stillwell, *Mathematics and its History*, Springer-Verlag New York, Inc., New York, 1989.
29. Gilbert Strang, Wavelets and dilation equations: A brief introduction, *SIAM Review*, 31:4 (1989), 614–627.
30. Georgi Tolstov, *Fourier Series*, Prentice Hall Inc., Englewood Cliffs, NJ, 1962. (Translated from the Russian by R. A. Silverman.)
31. Bartel van der Waerden, *Science Awakening*, Noordhoff, Groningen, 1954.
32. Edward Van Vleck, The influence of Fourier's series upon the development of mathematics, *Science* 39 (1914), 113–124.

Proof without Words:
Area and the Projection Theorem of a Right Triangle



$$CD^2 = AD \cdot DB$$

—Sidney H. Kung
Jacksonville University
Jacksonville, FL 32211

Optimal Leapfrogging

JOEL AUSLANDER
Harvard University
Cambridge, MA 02138

ARTHUR T. BENJAMIN
Harvey Mudd College
Claremont, CA 91711

DANIEL SHAWCROSS WILKERSON
University of California
Berkeley, CA 94720

This article arose from trying to determine the fastest way of moving checkers from the lower left-hand corner of a Go board to the upper right-hand corner, with no opponent in the way. The pieces move in "Chinese checkers" fashion by shifting or jumping in a way we soon illustrate and later describe precisely. Our goal is to move our pieces from a prescribed origin position to a prescribed destination position in as few turns as possible.

We regard our Go board as a subset of the integer-point lattice, $\mathbf{Z}^2$. Suppose we have four indistinguishable checkers initially situated at the points $(0,0)$, $(1,0)$, $(0,1)$, and $(1,1)$, and we wish to move them to the points $(17,17)$, $(17,18)$, $(18,17)$, and $(18,18)$. See FIGURE 1. One might begin by maneuvering into the *snake* configuration $\{(0,0),(1,1),(2,2),(3,3)\}$. (This can be done in four moves: for example, a hop, $(0,1)\to(2,1)$; a shift, $(2,1)\to(2,2)$; a two-hop jump $(1,0)\to(1,2)\to(3,2)$; and a shift $(3,2)\to(3,3)$.) Then apply the following three-move procedure: Shift the bottom piece (at $(0,0)$) to the right (to $(1,0)$), then triple-hop that piece (to $(3,4)$), then shift that piece to the right (to $(4,4)$). The pieces end up in the snake configuration (starting at $(1,1)$), and the same three-move procedure can be applied. If we apply this procedure 15 times, we reach $\{(15,15),(16,16),(17,17),(18,18)\}$. Four moves later, we will have reached our destination using $4+(15\times 3)+4=53$ moves altogether. However, a much faster trajectory exists. In one move, hop the piece at $(1,0)$ to $(1,2)$ reaching the *serpent* configuration $\{(0,0),(0,1),(1,1),(1,2)\}$. See FIGURE 2. Then apply the following two-move procedure: Double-hop the bottom piece (from $(0,0)$ to $(2,2)$), then double-hop the left-most piece (from $(0,1)$ to $(2,3)$). Once again, the pieces end up in the "serpent configuration" (starting at $(1,1)$), and the same two-move procedure can be applied. If we apply this procedure 16 times, we reach $\{(16,16),(16,17),(17,17),(17,18)\}$. Two moves later, we will have reached our destination using only 35 moves. The second trajectory is faster because the serpent configuration requires only two moves to translate itself in the direction $(1,1)$, a feat requiring three moves by the snake configuration. In this article, we characterize the speediest configurations for the above game (played in n dimensions) and thereby prove that the second trajectory is in fact optimal.

Precisely, we consider the problem of efficiently moving a collection of p indistinguishable pieces over the integer lattice $\mathbf{Z}^n$. The movement rules are analogous to those of Chinese checkers, and are as follows. At all times, pieces occupy distinct points in $\mathbf{Z}^n$. At each move, exactly one piece is displaced. If a piece is situated at the point $\mathbf{x}=(x_1,\ldots,x_n)\in\mathbf{Z}^n$ and, for some $i\in\{1,\ldots,n\}$, the point $\mathbf{x}+\mathbf{e}_i$ is unoccupied (where $\mathbf{e}_i$ is the i-th unit vector), then the piece may *shift* there; similarly for $\mathbf{x}-\mathbf{e}_i$.

If $\mathbf{x} + \mathbf{e}_i$ is occupied, but $\mathbf{x} + 2\mathbf{e}_i$ is not, then the piece can *hop* over the occupant of $\mathbf{x} + \mathbf{e}_i$ to arrive at $\mathbf{x} + 2\mathbf{e}_i$, where it may either remain or hop over another adjacent piece, etc. (Similarly for a hop over $\mathbf{x} - \mathbf{e}_i$ to $\mathbf{x} - 2\mathbf{e}_i$. A *move* consists of either a shift or a *jump* (a sequence of one or more hops by a single piece).

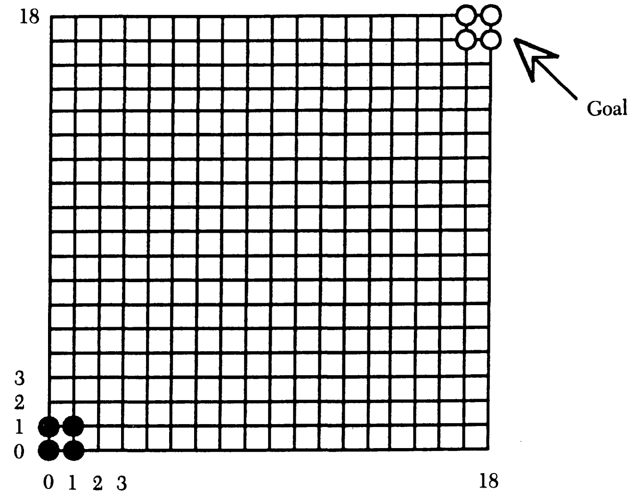


FIGURE 1
Solitaire Chinese checkers on a Go board.

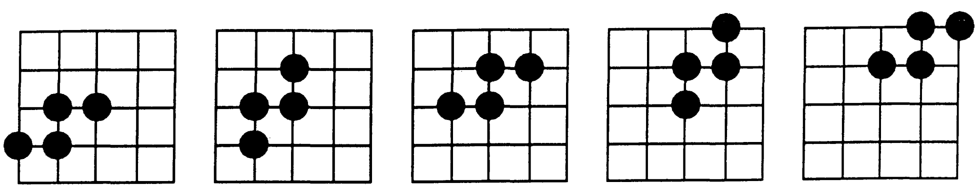


FIGURE 2
Serpent movement.

We begin with some definitions. A *placement* of pieces is a size p subset of $\mathbf{Z}^n$, usually denoted by $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_p\}$. We define the *centroid* of a placement X to be

$$\mathbf{c}(X) = \frac{1}{p} \sum_{u=1}^{p} \mathbf{x}_u,$$

which is a vector in $\frac{1}{p}\mathbf{Z}^n$. For placements X and Y, the *displacement* from X to Y is defined by

$$\mathbf{d}(X,Y) = \sum_{i=1}^{n} \left(c_i(Y) - c_i(X)\right)$$

where $c_i(Y) - c_i(X)$ is the i-th component of $\mathbf{c}(Y) - \mathbf{c}(X)$. Loosely, displacement measures the distance between placements, where the directions $\mathbf{e}_i$ are viewed as positive directions. Note that d can be negative, or nontrivially zero. For $m \geq 1$, an *m-move trajectory* $X_0, X_1, \ldots, X_m$ is a sequence of placements where X_{v+1} is reachable from X_v in a single move. The *speed* of an m-move trajectory from X to Y is defined as $\mathbf{d}(X,Y)/m$.

THEOREM 1. *Any trajectory speed is* $\leq 2 - 2/p$, *where* $p \geq 2$ *is the number of pieces. When* $p = 1$, *the speed is bounded by* 1.

Proof. From the definition, the speed of the trajectory $X_0, X_1, \ldots, X_m$ is the average of the speeds of its m moves. Each of these is of the form $\mathbf{d}(X_v, X_{v+1})/1$. If $p = 1$, the move is a shift and the displacement is 1, provided the shift is positive. If $p \geq 2$, the move is either a shift or a jump of at most $p - 1$ hops. The centroid is displaced by at most $(2p - 2)/p$, the maximum being attained by $p - 1$ positive hops.

Note that this maximum speed is not sustainable: There are various configurations in which a "long-jump" of $p - 1$ hops can be made, but the next move can be another long-jump only in the rather trivial one-dimensional case with $p = 2$. This is a special case of our next theorem, that a "repeatable" trajectory has speed at most 1, which we will call the *speed of light*.

We say that placement Y is a *translate* of X if there exists $\mathbf{a} \in \mathbf{Z}^n$ such that $Y = X + \mathbf{a}$, i.e., $\{\mathbf{y}_1, \ldots, \mathbf{y}_p\} = \{\mathbf{x}_1 + \mathbf{a}, \ldots, \mathbf{x}_p + \mathbf{a}\}$. Such placements X and Y are said to be represented by the same *configuration*. For $\mathbf{x} \in \mathbf{Z}^n$, define $\|\mathbf{x}\|$ to be $\Sigma_{i=1}^n x_i$, and for all integers M, let the *border* M be $\{\mathbf{x} \in \mathbf{Z}^n \colon \|\mathbf{x}\| = M\}$. Define the *tail* and *head* of a placement X as

$$t(X) = \min_u \|x_u\|, \quad h(X) = \max_u \|x_u\|.$$

THEOREM 2. *Let* Y *be a translate of* X. *Then any trajectory from* X *to* Y *has speed at most* 1.

Proof. Suppose $Y = X + \mathbf{a}$ for some $\mathbf{a} \in \mathbf{Z}^n$. For ease of notation, assume that $\mathbf{y}_i = \mathbf{x}_i + \mathbf{a}$, $i = 1, \ldots, p$, whence

$$\mathbf{d}(X,Y) = \sum_{i=1}^{n} (c_i(Y) - c_i(X)) = \sum_{i=1}^{n} \frac{1}{p} \sum_{u=1}^{p} a_i = \|\mathbf{a}\|.$$

Next we observe that the tail (and the head) cannot increase by more than 1 after each move. Therefore, since $t(Y) = \min_{i=1}^{p}\|(\mathbf{x}_i + \mathbf{a})\| = \min_{i=1}^{p}\|\mathbf{x}_i\| + \|a_i\| = t(X) + \|\mathbf{a}\|$, it follows that the number of moves m needed for a trajectory from X to Y is at least $\|\mathbf{a}\| = \mathbf{d}(X,Y)$. If $\mathbf{d}(X,Y) \leq 0$, then since $m \geq 1$, the trajectory has nonpositive speed. Otherwise, since $m \geq \mathbf{d}(X,Y)$, its speed is $\mathbf{d}(X,Y)/m \leq 1$.

A placement X is called a *speed-of-light placement* if there exists a nonzero vector $\mathbf{a} \in \mathbf{Z}^n$ and a speed one trajectory (called a *speed-of-light trajectory*) from X to $X + \mathbf{a}$. In FIGURE 3, we illustrate speed-of-light configurations for the two-dimensional case (where $p = 1$, 2, and 4, respectively). In fact, the next theorem demonstrates that these are the *only* such configurations in two dimensions, and essentially the only ones for higher dimensions, too.

THEOREM 3. *The following are speed-of-light configurations*:

The ***atom*** $\{\mathbf{x}\}$ (*when* $p = 1$),

the ***frog*** $\{\mathbf{x}, \mathbf{x} + \mathbf{e}_i\}$ $1 \leq i \leq n$ (*when* $p = 2$), *and*

the ***serpent*** $\{\mathbf{x}, \mathbf{x} + \mathbf{e}_i, \mathbf{x} + \mathbf{e}_i + \mathbf{e}_j, \mathbf{x} + 2\mathbf{e}_i + \mathbf{e}_j\}$ $1 \leq i \neq j \leq n$ (*when* $p = 4$).

No other speed-of-light configurations exist.

The first part of the theorem is straightforward. The atom can translate itself (in the direction $\mathbf{e}_i$) by shifting itself from $\{\mathbf{x}\}$ to $\{\mathbf{x} + \mathbf{e}_i\}$, a speed one maneuver when

$p = 1$. The frog $\{\mathbf{x}, \mathbf{x} + \mathbf{e}_i\}$ translates itself (in the direction $\mathbf{e}_i$) in a single hop to $\{\mathbf{x} + \mathbf{e}_i, \mathbf{x} + 2\mathbf{e}_i\}$, a speed-one maneuver when $p = 2$. When $p = 4$, the serpent performs two consecutive double-hops to go from $\{\mathbf{x}, \mathbf{x} + \mathbf{e}_i, \mathbf{x} + \mathbf{e}_i + \mathbf{e}_j, \mathbf{x} + 2\mathbf{e}_i + \mathbf{e}_j\}$ to $\{\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j, \mathbf{x} + 2\mathbf{e}_i + \mathbf{e}_j, \mathbf{x} + 2\mathbf{e}_i + 2\mathbf{e}_j, \mathbf{x} + 3\mathbf{e}_i + 2\mathbf{e}_j\}$, translating itself in the direction $\mathbf{e}_i + \mathbf{e}_j$ in two moves.

We establish the second part of the theorem by proving a series of necessary conditions that must be satisfied by speed-of-light objects.

LEMMA 1. *Every move in a speed-of-light trajectory must simultaneously increase the values of the back border and the front border. Hence a speed-of-light placement X contains a unique piece on border $t(X)$, and a speed-of-light move must "jump" that piece to a point on border $h(X) + 1$.*

Proof. As argued in proving Theorem 2, an m-move trajectory from X to $X + \mathbf{a}$ has speed $\|\mathbf{a}\|/m$, where $m \geq \|\mathbf{a}\|$. Note that $t(X + \mathbf{a}) = t(X) + \|\mathbf{a}\|, h(X + \mathbf{a}) = h(X) + \|\mathbf{a}\|$. We observe (as in the proof of Theorem 2) that the functions t and h cannot increase by more than 1 each move. Hence, in order for $m = \|\mathbf{a}\|$, we must simultaneously increase the values of both borders each move.

LEMMA 2. *Given a speed-of-light placement X and $t(X) \leq M \leq h(X)$, there is at most one occupied point $\mathbf{x} \in X$ with $\|\mathbf{x}\| = M$.*

Proof. Suppose, to the contrary, that more than one piece is situated on border M. By Lemma 1, the first $M - t(X)$ moves of the trajectory involve moving pieces from borders with values less than M to borders with values greater than M, after which our new back border has value M. But then this border has more than one piece, contradicting Lemma 1.

LEMMA 3. *When $p \geq 2$, every move in a speed-of-light trajectory is a jump.*

Proof. Since $p \geq 2$, we have $h(X) > t(X)$ by Lemma 1. Since a shift can not take a back border piece beyond border $t(X) + 1 \leq h(X)$, it can not expand the front border, as required.

Notice that in a speed-of-light trajectory, for a piece on border M to make "forward progress," it must hop over a piece on border $M + 1$ and land on border $M + 2$. It follows from Lemma 3 that every speed-of-light placement X has at least one piece on every border between $t(X)$ and $h(X)$.

Thus, we have

LEMMA 4. *Every speed-of-light placement X must have exactly one piece on each border between border $t(X)$ and border $h(X)$. Consequently, $h(X) = t(X) + p - 1$.*

LEMMA 5. *If X is a speed-of-light placement with $p \geq 2$ pieces, then p must be even.*

Proof. By Lemmas 1 and 4, the first move must jump a piece from border $t(X)$ to border $t(X) + p$. Since a jump changes the border value by an even number, p must be even.

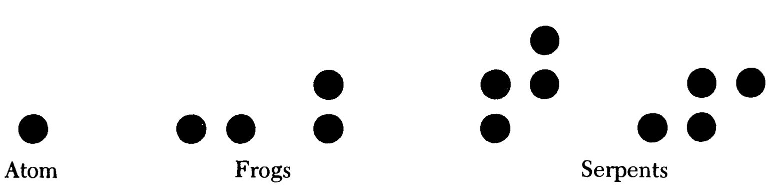


FIGURE 3
Speed-of-light configurations.

Proof of Theorem 3. By Lemma 3, when $p = 2$, all speed-of-light configurations must be of the form $\{\mathbf{x}, \mathbf{x} + \mathbf{e}_i\}$ for some $1 \leq i \leq n$, i.e., the frogs. By Lemma 5, $p \neq 3$. We can restrict our attention to the case where $p \geq 4$. It remains to prove that the only possible remaining speed-of-light configurations are of the serpent variety. Imagine that we have a speed-of-light trajectory that makes one move every second. Suppose the front border piece of our speed-of-light placement X is presently ($t = 0$) situated at $\mathbf{x} \in \mathbf{Z}^n$, with $\|x\| = M$. We shall focus our attention on only those points in $\mathbf{Z}^n$ that occupy borders of value M or higher. Thus at $t = 0$, all that we see is a single piece, situated at $\mathbf{x}$ (see FIGURE 4).

When $t = 1$, the front border's value has increased to $M + 1$. The new front border piece must have made its final hop over $\mathbf{x}$ to land on the point $\mathbf{x} + \mathbf{e}_i$ for some $1 \leq i \leq n$. See FIGURE 5.

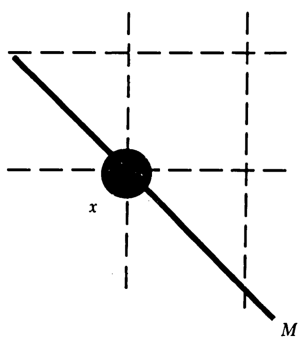


FIGURE 4
What we see when $t = 0$.

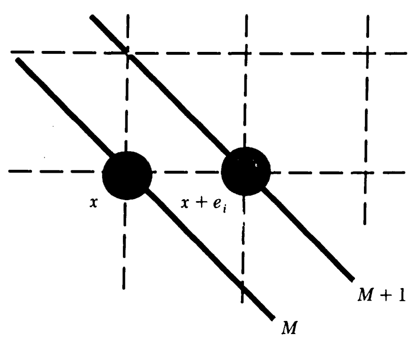


FIGURE 5
What we see when $t = 1$.

When $t = 2$, the front border's value has increased to $M + 2$. The piece that landed there had to make its final hop over $\mathbf{x} + \mathbf{e}_i$. Hence the piece on border $M + 2$ must be situated at $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j$ for some $1 \leq j \leq n$. Observe that $i \neq j$, for otherwise the piece at $\mathbf{x}$ would have hopped over $\mathbf{x} + \mathbf{e}_i$ to point $\mathbf{x} + 2\mathbf{e}_i$ thus leaving no piece with border value M, contradicting Lemma 4.

Thus, at $t = 2$, we see three pieces, situated at $\mathbf{x}$, $\mathbf{x} + \mathbf{e}_i$, $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j$, where $1 \leq i \neq j \leq n$. (See FIGURE 6.)

When $t = 3$, a piece is jumped to the new front border $M + 3$ and, since it had to hop over the piece at $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j$, it must end up at $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j + \mathbf{e}_k$ for some $1 \leq k \leq n$. We know that $k \neq j$ by the same argument as $i \neq j$ above. we now show that, in fact, $k = i$. The new front border piece, before it made its final hop over $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j$ to $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j + \mathbf{e}_k$, must have been at the point $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j - \mathbf{e}_k$ on border $M + 1$. But how did it get there? It had to hop over the sole piece on border M, situated at $\mathbf{x}$. But this requires $\mathbf{e}_i + \mathbf{e}_j - \mathbf{e}_k$ to be a unit vector, which is only possible when $k = i$ or $k = j$. And since $k \neq j$, we have $k = i$. Hence at $t = 3$, we see four pieces, situated at $\mathbf{x}$, $\mathbf{x} + \mathbf{e}_i$, $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j$, and $\mathbf{x} + 2\mathbf{e}_i + \mathbf{e}_j$, as in FIGURE 7.

When $t = 4$, the back border piece, wherever it is, jumps to border $M + 4$, landing on $\mathbf{x} + 2\mathbf{e}_i + \mathbf{e}_j + \mathbf{e}_k$ for some $1 \leq k \leq n$. By the argument in the preceding paragraph, the hop over the piece at $\mathbf{x} + 2\mathbf{e}_i + \mathbf{e}_j$ had to come from the point $\mathbf{x} + 2\mathbf{e}_i$ reached by a hop over $\mathbf{x} + \mathbf{e}_i$, and so that hop came from $\mathbf{x}$. Hence the jump originated at $\mathbf{x}$. Thus $p = 4$, and our current configuration (as well as our original one) must have been a serpent.

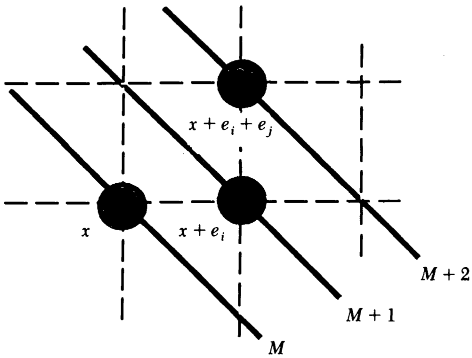


FIGURE 6
What we see when $t = 2$.

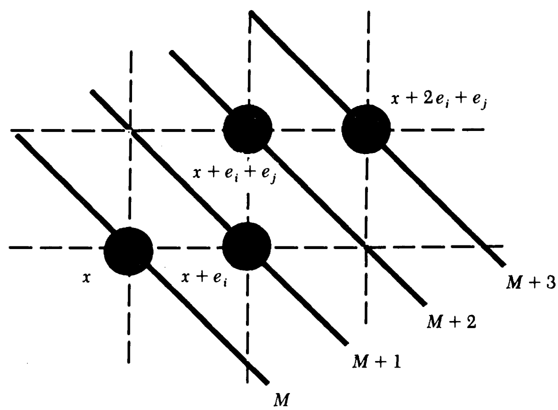


FIGURE 7
What we see when $t = 3$.

Returning to the problem at the outset of the article, we see that the 35-move trajectory must be optimal because the original configuration is translated a distance of 34 units, and the square configuration is not a speed-of-light configuration.

As a consequence of this theorem, we see that no speed-of-light configurations exist when the number of pieces is three or greater than four. In these cases, it is easy to create configurations that are translatable with speed $2/3$ (e.g., the snake configuration with p pieces). The question of whether the speed $2/3$ is *optimal* for the two- (and higher-) dimensional problem, when $p = 3$ or $p > 4$, remains open. More specifically, it remains unknown how to optimally translate six or nine pieces (arranged in a triangle or square) from the lower left-hand corner to the upper right-hand corner of the Go board.

Acknowledgments. We dedicate this paper to the Summer Studies in Mathematics program at Hampshire College, directed by Professor David Kelly, where this research took place. HCSSiM is a mathematics program for high-ability high school students. During the 1986 program, Benjamin led a week-long, open-ended course, where students explored properties of jumping games. Two students, Auslander and Wilkerson, proved the two-dimensional version of this theorem and presented it at an MAA section meeting in Baltimore in 1986. We also thank Professor Alan J. Goldman of Johns Hopkins University for suggesting this problem to us, Greg Levin for assistance with the figures, and the anonymous referees for many valuable suggestions.

REFERENCE

Readers may also enjoy *Wheels, Life and Other Mathematical Amusements* by Martin Gardner (W. H. Freeman and Co., 1983), particularly the chapters analyzing the games of "Halma" and "Life."

NOTES

The Catalan Numbers Visit the World Series

LOU SHAPIRO
Howard University
Washington, DC 20059

WALLACE HAMILTON
University of the District of Columbia
Washington, DC 20008

A World Series-type contest is one where two teams compete and the first team to win n games wins the series. The most famous case, where $n = 4$, occurs each October. We make the strong assumption that team A wins each game with constant probability p. We want to compute the expected number of games to be played, where there are no draws, and the series is complete after one team wins n games. A few small cases yield the following, where $q = 1 - p$ and E_n is the expected number of games.

n	$E_n(p) = E_n$	example
1	1	most games
2	$2(1 + pq)$	women's tennis
3	$3(1 + pq + 2p^2q^2)$	men's tennis
4	$4(1 + pq + 2p^2q^2 + 5p^3q^3)$	World Series
5	$5(1 + pq + 2p^2q^2 + 5p^3q^3 + 14p^4q^4)$	

The Catalan sequence

$$\{1, 1, 2, 5, 14, 42, \ldots\} = \left\{ \frac{1}{n+1} \binom{2n}{n} \right\}_{n=0}$$

comes up in a wide variety of settings: triangulations of an n-gon, parenthesizations, random walks in one dimension with an absorbing barrier, number of permutations achievable with a stack, the probability of a function being convex [4], and many more. The conjecture presenting itself with these first few cases is

THEOREM. *$E_n/n = \sum_{k=0}^{n-1} C_k (pq)^k$ where*

$$C_k = \frac{1}{k+1}\binom{2k}{k}$$

is the kth Catalan number.

This result is novel in that it involves the partial sums of the Catalan numbers. The books of Cohen [1] and Graham, Knuth, and Patashnik [3] provide a lively introduction to the Catalan numbers, as does the article by Gardner [2] in *Scientific American*.

The proof breaks up into two parts.

A) Express E_n/n as a sum.

$$\frac{E_n}{n} = \sum_{k=0}^{n} \binom{2n-k}{n-k} (pq)^{n-k} (p^k + q^k).$$

Proof.

$$E_n = n(p^n + q^n) + (n+1)\binom{n}{1}(p^n q + p q^n) + (n+2)\binom{n+1}{2}(p^n q^2 + p^2 q^n)$$
$$+ \cdots + (2n-1)\binom{2n-2}{n-1}(p^n q^{n-1} + p^{n-1} q^n)$$
$$= \sum_{k=0}^{n-1} (n+k)\binom{n-1+k}{k}(p^n q^k + p^k q^n)$$
$$= n \sum_{k=0}^{n-1} \binom{n+k}{k}(p^n q^k + p^k q^n).$$

B) Express the sum as a difference. If $\{b_n\}_{n \geqslant 0}$ is defined by $b_k = a_0 + a_1 + \cdots + a_k$ for all k then $b_k - b_{k-1} = a_k$. Thus we look at

$$\sum_{k=0}^{n} \binom{n+k+1}{k}(p^{n+1} q^k + p^k q^{n+1})$$
$$= \sum_{k=0}^{n} \binom{n+k+1}{k}(p^n q^k + p^k q^n) - \sum_{k=0}^{n} \binom{n+k+1}{k}(p^n q^{k+1} + p^{k+1} q^n)$$
$$[\text{since } p = 1 - q]$$
$$= \sum_{k=0}^{n} \binom{n+k}{k}(p^n q^k + p^k q^n) + \sum_{k=1}^{n} \binom{n+k}{k-1}(p^n q^k + p^k q^n)$$
$$- \sum_{l=1}^{n+1} \binom{n+l}{l-1}(p^n q^l + p^l q^n)$$
$$= \sum_{k=0}^{n} \binom{n+k}{k}(p^n q^k + p^k q^n) - \binom{2n+1}{n}(p^n q^{n+1} + p^{n+1} q^n)$$
$$= \sum_{k=0}^{n-1} \binom{n+k}{k}(p^n q^k + p^k q^n) + 2\binom{2n}{n} p^n q^n - \binom{2n+1}{n} p^n q^n$$
$$= \sum_{k=0}^{n-1} \binom{n+k}{k}(p^n q^k + p^k q^n) + \frac{1}{n+1}\binom{2n}{n} p^n q^n.$$

The first equality follows from expressing p as $1-q$ and vice versa, while the last equality follows from

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

The result now follows easily.

For n large, it is clear that

$$E_n/n \to C(pq) = \frac{2}{(p+q) + \sqrt{(p+q)^2 - 4pq}}$$
$$= \frac{2}{p+q+|p-q|} = \frac{1}{\max\{p,q\}}.$$

The graph of $C(pq)$ as a function of p is shown in FIGURE 1.

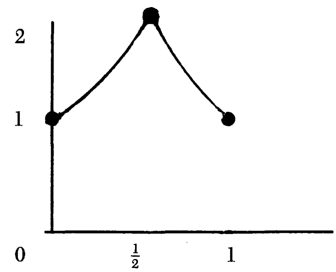


FIGURE 1

An alternate discussion of this last result when $p = 1/2$ is given in *Finite Markov Chains* [5, pp. 165–167].

The authors would like to thank the referees for several helpful comments. In particular our original proof, based on triangular matrices and generating functions, has been greatly streamlined thanks to one of these suggestions.

REFERENCES

1. D. Cohen, *Basic Techniques of Combinatorial Theory*, John Wiley & Sons Inc., New York, 1978.
2. M. Gardner, Mathematical games, *Scientific American* 244 (June 1976), 120–125.
3. R. Graham, D. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley Publishing Co., Reading, MA, 1989.
4. R. Guy, Catalan strikes again, how likely is a function to be convex?, this MAGAZINE 61 (1988), 211–219.
5. J. J. Kemeny, and L. Snell, *Finite Markov Chains*, Springer-Verlag New York Inc., New York, 1976.
6. W. Woodside, Winning streaks, shutouts, and the length of the World Series, *The UMAP J.* 10 (1989), 99–113.

On the Converse of Lagrange's Theorem

JOSEPH A. GALLIAN
University of Minnesota
Duluth, MN 55812

Undoubtedly the most basic result in finite group theory is the Theorem of Lagrange that says the order of a subgroup divides the order of the group. Herstein [**8**, p. 75] likens this theorem to the ABC's for finite groups. G. A. Miller [**9**, p. 23] calls it "the most important theorem of group theory" (see also [**2**, p. 130]).

Although it has been known since 1799 that the group A_4 consisting of the 12 even permutations on $\{1,2,3,4\}$ has no subgroup of order 6, it is surprising that a number of abstract algebra textbooks fail to mention that this most natural converse of the most important theorem of finite group theory is false (e.g. [**11**], [**1**]). Many authors mention the fact without proof (e.g. [**8**, p. 72]) or use phrases such as "A_4 can be shown to have no subgroup of order 6" (e.g. [**4**, p. 102], [**7**, p. 40]), perhaps giving students the impression that such a proof is omitted because it is too difficult. Some books (e.g. [**3**, p. 245]) give complicated proofs that A_4 has no subgroup of order 6. Most books that do provide a proof, do so long after introducing Lagrange's Theorem and invoke relatively sophisticated notions such as normality (e.g. [**2**, p. 142]), factor groups ([**5**, p. 151], [**12**, p. 104]), the classification of groups of order 6 ([**10**, p. 200]), conjugacy arguments ([**6**, p. 45]) or, in some cases, even Sylow's Theorem ([**3**, p. 245]).

It seems to have been overlooked that there is a simple argument requiring nothing more complicated than the basic properties of cosets to prove that A_4 has no subgroup of order 6. Before giving our argument we observe that $A_4 = \{(1),(12)(34),(13)(24),(14)(23),(123),(132),(124),(142),(134),(143),(234),(243)\}$ contains eight elements of order 3.

Now suppose H is a subgroup of A_4 of order 6 and let a be any element of order 3. Then, since H has index 2, at most two of the cosets H, aH and a^2H are distinct. But the equality of any pair of these implies that $a \in H$. Thus, H contains all eight elements of order 3.

Acknowledgment. Thanks to a remark by David Witte I was able to shorten my original argument a bit.

REFERENCES

1. N. J. Bloch, *Abstract Algebra with Applications*, Prentice Hall, Inc. Englewood Cliffs, NJ, 1987.
2. D. M. Burton, *Abstract Algebra*, Wm. C. Brown Company Publishers, Dubuque, IA, 1988.
3. W. E. Deskins, *Abstract Algebra*, Macmillan Publishing Co., New York, 1964.
4. J. B. Fraleigh, *A First Course in Abstract Algebra*, 4th edition, Addison-Wesley, Publishing Co., Reading, MA, 1989.
5. J. A. Gallian, *Contemporary Abstract Algebra*, 2nd edition, D. C. Heath and Company, Lexington, MA, 1990.
6. C. F. Gardiner, *Algebraic Structures*, Ellis Horwood, Chichester, U. K., 1986.
7. I. N. Herstein, *Topics in Algebra*, 2nd edition, John Wiley & Sons Inc., New York, 1975.
8. I. N. Herstein, *Abstract Algebra*, 2nd edition, Macmillan Publishing Co., New York, 1990.
9. G. A. Miller, H. F. Blichfedt and L. E. Dickson, *Theory and Applications of Finite Groups*, Dover Publications, New York, 1961.
10. H. Paley and P. Weichsel, *A First Course in Abstract Algebra*, Holt, Rinehart and Winston, New York, 1966.
11. C. C. Pinter, *A Book of Abstract Algebra*, McGraw-Hill Book Co., New York, 1982.
12. D. Saracino, *Abstract Algebra: A First Course*, Addison-Wesley Publishing Co., Reading, MA, 1980.

Rational Triangles

KEITH SELKIRK
University of Nottingham
Nottingham, NG7 2RD, U.K.

The paper in the December 1988 issue of this MAGAZINE on "Extending the Converse of Pons Asinorum" by John P. Hoyt [1] came to my notice when I had almost completed similar work of my own. Since my approach is slightly different, readers might be interested in revisiting the same theme from a different standpoint. While the present approach lacks the charm of Hoyt's (which uses angles in a circle), it does have the advantage of using geometry that is even more elementary. It shows further that the ideas in Hoyt's paper may be extended to deal with cases where two angles of a triangle have a rational ratio rather than being merely multiples of one another, and finally, that the method generates all such triangles that are possible. My own interest began with the paper of Wynne Willson's [2] on a property of the 4:5:6 triangle that was cited (but with the author's surname incorrectly given) by Hoyt, coupled with the earlier papers [3], [4], and [5].

To begin, we shall note that it would be particularly useful if we could find examples of triangles (apart from the trivial case of the equilateral triangle) in which all six measurements of sides and angles were whole numbers, the angles being measured in degrees. Now it is not difficult to find triangles with three integral sides, since the triangle inequality tells us that any set of three numbers in which the larger is less than the sum of the two smaller will achieve this. It is also possible to have one integral angle, and much effort has been put into the particular case where that angle is 90°, when the lengths of the three sides form a Pythagorean triad. The cosine formula tells us that if the three sides of a triangle are integers, then the cosines of all three angles must be rational numbers. This gives us two other possibilities where one angle is a rational number of degrees, namely the 60° and 120° cases, the cosines of these angles being, respectively, $\frac{1}{2}$ and $-\frac{1}{2}$. The former is dealt with in [3] and the latter by myself in [4], and there are some interesting ideas for investigation using the cosine formula that can be developed from these. If two angles of a triangle are a rational number of degrees, it follows from the angle sum criterion that the third one is also. It is then quite easy to arrange for one of the sides to be an integer, but not for a second side also to be an integer.

One is tempted to stop there and feel that we can advance no further. However, notice that it does not matter whether we make the sides rational numbers or integers. The former can always be turned into the latter by a suitable application of a scale factor. This suggests that we might also consider the case where two of the angles are in rational ratios rather than being themselves rational. The paper [2] dealing with a property of the 4:5:6 triangle then generalizes it to show that if and only if a triangle ABC has $\angle C = 2\angle A$, then

$$c^2 = a^2 + ab. \tag{1}$$

In particular, the triangle with sides in the ratio 4:5:6 has this property. The author goes on to show that all such triangles can be generated by

$$a = u^2,\ b = v^2 - u^2,\ c = uv, \tag{2}$$

where u and v are coprime integers with $v > u > \frac{1}{2}v > 0$.

Wynne Willson tabulates the simpler values of these quantities, and since we shall use them as examples later, we shall repeat his table here (with a slight change in notation to bring it into line with Hoyt).

TABLE 1

u	2	3	3	4	5	4	5	6
v	3	4	5	5	6	7	7	7
a	4	9	9	16	25	16	25	36
b	5	7	16	9	11	33	24	13
c	6	12	15	20	30	28	35	42

The first three of these and the sixth are among Hoyt's examples.

We now shall develop a generalized version of Wynne Willson's method. This is foreshadowed in [5], which suggests a practical use of this idea in the design of linkages. We begin with the cases where one angle is an exact multiple of another. Consider a set of triangles $AB_1C, AB_2C, \dots, AB_nC, \dots$ (where n is a positive integer) such that $A, B_1, B_2, \dots, B_n, \dots$ are collinear points in that order (A may also be regarded as B_0), and such that $\angle B_{n+1}CB_n = \angle B_1CA = \angle B_1AC$. The first four triangles in the set are shown in FIGURE 1. For convenience we shall label the lengths of the sides as indicated in that figure, so that triangle AB_nC has sides $B_nC = a_n$, $AB_n = c_n$ and $AC = b$.

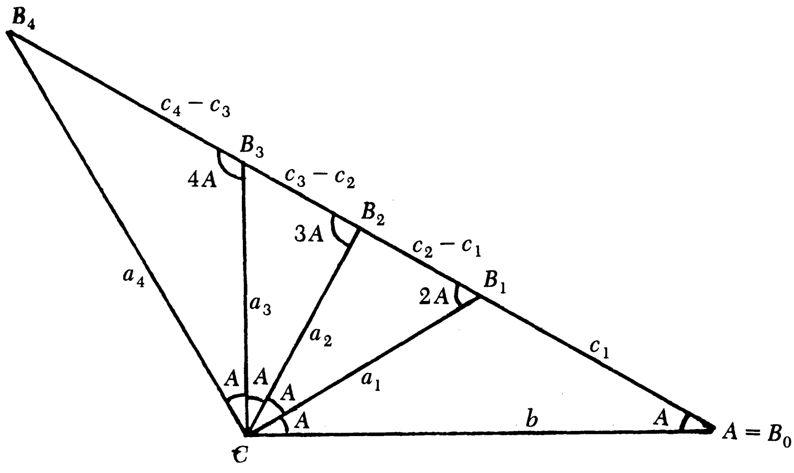


FIGURE 1

Triangles AB_nC and CB_nB_{n-1} are clearly similar, so that for $n > 1$,

$$\frac{a_n}{c_n - c_{n-1}} = \frac{b}{a_{n-1}} = \frac{c_n}{a_n}. \tag{3}$$

From this we can express the sides of triangle $AB_{n-1}C$ in terms of those of triangle AB_nC and vice versa by the following equations:

$$a_{n-1} = ba_n/c_n \quad \text{and} \quad c_{n-1} = \left(c_n^2 - a_n^2\right)/c_n \tag{4}$$

and

$$a_n = a_{n-1}bc_{n-1}/\left(b^2 - a_{n-1}^2\right) \quad \text{and} \quad c_n = b^2c_{n-1}/\left(b^2 - a_{n-1}^2\right). \tag{5}$$

Thus a_n, b, and c_n are rational if and only if a_{n-1}, b, and c_{n-1} are rational. We must ensure that none of these rational numbers can be negative. We first note that for $n > 1$, since $\angle B_nCA = n\angle A$, then $c_n > a_n$ and $c_n - a_n > 0$. Further, from (5), we must have the condition

$$b > a_{n-1}. \tag{6}$$

This is in fact obvious when we realize that it is merely the criterion that $\angle CB_{n-1}A > \angle A$, for otherwise AB_n cannot be constructed so that B_n lies on the same side of A as B_{n-1}.

We have now proved that if a triangle $AB_{n-1}C$ exists with the properties that its sides are in rational ratios and that $\angle B_{n-1}CA = (n-1)\angle A$, then a triangle AB_nC also exists with sides in rational ratios and $\angle B_nCA = n\angle A$ provided that condition (6) is obeyed. Conversely, if a triangle AB_nC exists with the given properties, then a triangle $AB_{n-1}C$ also exists with the given properties. Consequently, by starting with the case $n = 1$, we can go on generating triangles until condition (6) prevents the creation of any more. If we try to work the other way from a triangle that is known to obey the condition that one angle is an exact multiple of another and to have sides in rational ratios, then we always get back to the case $n = 1$.

In particular, it is instructive to look at triangle AB_1C (or B_0B_1C). Using (5), the sides of the first two triangles are related by

$$a_2 = a_1bc_1/\left(b^2 - a_1^2\right) \quad \text{and} \quad c_2 = b^2c_1/\left(b^2 - a_1^2\right).$$

However a_1 and c_1 are equal, since triangle AB_1C is isosceles, and we can therefore write $d = a_1 = c_1$ where $d > (\frac{1}{2})b$ so that

$$a_2 = d^2b/(b^2 - d^2),\ c_2 = db^2/(b^2 - d^2). \tag{7}$$

We are really only interested in the ratios of the sides of triangle AB_2C, and these are $d^2 : b^2 - d^2 : db$. These are exactly the same as the ratios $u^2 : v^2 - u^2 : uv$ that are used in Table 1. It follows that u and v are merely the ratios of the sides of the initial isosceles triangle AB_1C. We now have a method of generating all possible triangles with sides in rational ratios and two angles in rational ratios starting with the set of possible values of u and v as shown in the table.

To illustrate this we shall now re-draft Table 1 and obtain some simple numerical examples of triangles with various integral ratios of angles. We shall examine the values of u and v in Table 1, but take them as d and b, respectively. This will give the sides of the various 'double angle' triangles using (5) in rational ratios, and these are then easily expressed in the integral ratios given in Table 1. Table 2 is the modified table. All the examples in the table give cases where one angle is double another since we start off with $d > \frac{1}{2}b$, but condition (6) means that in the starred cases there can be no higher ratios of angles since $b < a_2$, and these cases are thus of no further interest.

TABLE 2

d	2	3*	3	4*	5*	4	5*	6*
b	3	4	5	5	6	7	7	7
a_2	12/5	36/7	45/16	80/9	150/11	112/33	175/24	252/13
b	3	4	5	5	6	7	7	7
c_2	18/5	48/7	75/16	100/9	180/11	196/33	245/24	294/13

The unstarred cases are all given in Hoyt's analysis, so we will just give as an example details of the case with $d = 4$ and $b = 7$, which gives the double angle triangle with ratios 16:33:28. This in turn gives the triple angle triangle given by $a_3 = 64/17$, $b = 7$ and $c_3 = 132/17$ with ratios 64:119:132. Next comes the quadruple angle triangle given by $a_4 = 1792/305$, $b = 7$ and $c_4 = 3332/305$ with ratios 256:305:476. Finally, there is a quintuple angle triangle given by $a_5 = 1024/33$, $b = 7$, and $c_5 = 1220/33$, which are in the ratio 1024:231:1220. In every case, the angle A is approximately 28.96°, which gives $\angle 5A \approx 144.78°$. There are no further triangles generated by this case.

So far we have only considered cases where one angle is a multiple of another, but we can also consider what happens when the ratio is rational but nonintegral. Take, for example, the $d = 3$, $b = 5$ case. Triangle B_2CB_4 has $\angle B_2 = 3\angle A$, $\angle C = 2\angle A$ and has sides given by $a_4 = 405/31$, $c_4 - c_2 = 6075/496$ and $a_2 = 45/16$, which are in the ratio 144:135:31. It is generated from part of the triangle AB_4C, which has angles of $4A$ and A. In general, similar examples can be generated from any quadruple angle triangle since in both triangles we have $5A < 180°$; when one case exists, so does the other.

More generally a triangle $B_{p-1}CB_{p+q-1}$ with the first two angles pA and qA can be found with two angles in the ratio $p:q$ (where p and q are positive integers) from the triangle $AB_{p+q-1}C$ which has two angles in the integral ratio $1:p+q-1$ (see FIGURE 2). In both cases the sum of these two angles is $(p+q)A$, and we have the same condition $A < [180/(p+q)]°$. Thus all triangles with two angles in rational ratios and the sides in rational ratios can be generated by this method.

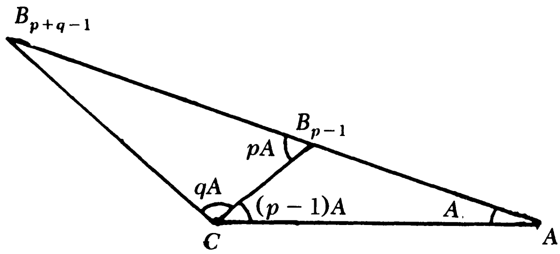


FIGURE 2

Unfortunately, unless p and q are small, some searching will be necessary before suitable examples are found, as the angle A must be quite small. An appropriate strategy is to look at cases where d is slightly larger than $\frac{1}{2}b$, for example, the case $d = 7$, $b = 13$. Here $\cos A = b/(2d) = 13/14$, so that $\angle A \approx 21.79°$. This will ultimately produce a triangle with angles of A and $7A$. From the triangles generated by this we could, given sufficient persistence, obtain triangles with angles in the ratios 5:2, 4:3, and 5:3, and this is the first case to give all these ratios. It is perhaps unfortunate that the particularly simple case of the 4:5:6 triangle that started all this off does not seem to be repeated; the numerical calculations rapidly become more and more complicated.

REFERENCES

1. John P. Hoyt, Extending the converse of Pons Asinorum, this MAGAZINE 61 (1988), 308–313.
2. W. Wynne Willson, A generalisation of a property of the 4, 5, 6 triangle, *Mathematical Gazette* **60** (1976), 130–131.
3. John Gilder, Integer-sided triangles with an angle of 60°, *Mathematical Gazette* **66** (1982), 261–266.
4. Keith Selkirk, Integer-sided triangles with an angle of 120°, *Mathematical Gazette* **67** (1983), 251–255.
5. N. S. Reed and R. W. Hogg, Mathematical models in Meccano, *Mathematical Gazette* **65** (1981), 199.

How Many Mating Units Are Needed to Have a Positive Probability of Survival?

DAVID M. HULL
Valparaiso University
Valparaiso, IN 46383

1. Introduction We will consider a branching process that counts the number of mating units in successive generations. It is assumed that offspring can be generated only by a mating unit consisting of a male and a female. The usefulness of this scheme was discussed by S. M. Ulam in his provocative paper "How to formulate mathematically problems of rate of evolution?" [**10**].

In the context of beginning formulations of a mathematical treatment of evolution, Ulam made this statement: "There is a very nice and simple mathematical technique for describing processes starting with a single object, which then duplicates and gives 0, 2, or 3 or more descendants. It is called the theory of branching processes. It deals with asexual reproduction and gives methods to calculate the number of particles, of various kinds, in future generations and other questions of this sort. I would like to stress that a corresponding theory for branching with "sex" where particles get together, say at random and then produce offspring, i.e., a combination of a binary process of mating and of reproduction is mathematically much more difficult and no exact theory exists as yet."

This statement was made over 20 years ago. Since then considerable progress has been made toward the development of a bisexual branching process theory. The purpose of this note is to discuss the bisexual Galton-Watson branching process (bGWbp), to state a condition that guarantees that a bisexual population will become extinct no matter how many mating units are functioning initially and finally, if the aforesaid condition does not hold, to answer the question posed in the title of this note. But first, since the bGWbp has its roots in the standard Galton-Watson branching process (sGWbp), we review briefly the traditional branching process of asexual reproduction mentioned by Ulam.

2. The standard Galton-Watson branching process The standard process was motivated in the late nineteenth century by Sir Francis Galton's concern about the extinction of family surnames [**9**]. His concern lead to the development of a model of asexual reproduction. The literature on the sGWbp is abundant (if not overwhelming) and the main results are well known. A concise summary of this process is given by William Feller [**6**] in his classic probability text. "We consider particles which are able to produce new particles of like kind. A single particle forms the original, or zero generation. Every particle has probability p_k $(k = 0, 1, 2, \dots)$ of creating exactly k new particles; the direct descendants of the nth generation form the $(n+1)$st generation. The particles of each generation act independently of each other. We are interested in the sizes of the successive generations." If we let X_n denote the number of particles in the nth generation, we say that the process terminates or becomes extinct if $X_n = 0$ for some positive integer n.

The sGWbp has two parameters:

(1) the offspring probability distribution $\{p_k\}_{k=0}^{\infty}$ and

(2) the number of particles (assumed positive) that start the process, X_0.

Since particles in this process reproduce independently, it is obvious that X_0 plays no part in determining whether or not extinction occurs with probability one (i.e. absolute certainty that extinction will take place). The mean of $\{p_k\}_{k=0}^{\infty}$ (by itself) tells us whether or not extinction is guaranteed to occur. This is stated in the classic sGWbp theorem: If $0 < p_0 < 1$ and m denotes the mean of $\{p_k\}_{k=0}^{\infty}$ then extinction is certain (has probability one) if, and only if, $m \leqslant 1$.

For any sGWbp if the extinction probability is one when $X_0 = 1$, the probability of extinction will continue to be one no matter what value X_0 has. We shall see that when sexual reproduction is introduced into a branching process, increasing the number of mating units in the initial generation can lower an extinction probability of one to a value less than one.

3. The bisexual Galton-Watson branching process There are serious objections to applying a model of asexual reproduction to Galton's problem of finding the probabilities of extinction of certain surnames. After all, do human males perpetuate their surnames by themselves? It was not until 1968, some 95 years after Galton's first appeal for a solution to his problem that a branching process of two types with genuine sexual interaction appeared on the scene [3]. An explanation for the delay in developing the bisexual process is that the mathematics involved is much more difficult (as pointed out by Ulam). It took several decades before the mathematical community was motivated to consider the rigors of the two-sex version of Galton's problem.

The bGWbp has four parameters:

1. Z_0, the number of mating units in the initial (zeroth) generation;

2. the mating function ζ tells us the number of mating units that will be formed in a generation having x females and y males. This is a nonnegative integer-valued function defined on all ordered pairs of nonnegative integers subject to the conditions

(i) $0 \leqslant \zeta(x, y) \leqslant xy$ (which implies that $\zeta(t, 0) = \zeta(0, t) = 0$ for any non-negative integer t), and

(ii) ζ is nondecreasing in x and in y.

Further background on mating functions is provided in [1] and [3]. Assume we know

3. the offspring probability distribution $\{p_k\}_{k=0}^{\infty}$, where p_k is the probability that a mating unit will produce k offspring; and

4. α, the probability that an individual offspring will be female.

The bGWbp can be thought of as the continued repetition of the three steps. (1) The mating units in the nth generation ($n = 0, 1, 2, \dots$) produce offspring according to the probability distribution $\{p_k\}_{k=0}^{\infty}$, these offspring form the $(n+1)$st generation; (2) each of these offspring is then designated as male (with probability $1 - \alpha$) or female (with probability α), these designations are carried out independently—if a generation is known to have m individuals, the number of females in that generation will have a binomial distribution with parameters m and α; and (3) the number of mating units in the $(n+1)$st generation, Z_{n+1}, is dictated solely by ζ, specifically, $Z_{n+1} = \zeta(X_{n+1}, Y_{n+1})$ where X_{n+1} and Y_{n+1} are the numbers of females and males, respectively, in the $(n+1)$st generation.

The most intriguing of these four parameters is the mating function. In the initial paper on the bGWbp [3], Daley dealt exclusively with what would appear to be the two most relevant mating functions for human and animal populations:

(1) Completely promiscuous mating, where

$$\zeta(x, y) = \begin{matrix} x, & \text{if } y > 0 \\ 0, & \text{if } y = 0. \end{matrix}$$

This mating function is relevant to a population where a "champion" male (with infinitely great reproductive powers) arises in each generation and mates with each female in that generation. No other male is allowed to participate in a mating unit.

(2) Polygamous mating with perfect fidelity, where

$$\zeta(x, y) = \min(x, dy) \text{ where } d \text{ is a positive integer.}$$

A double standard is tolerated here. The males may practice "polygamous mating" while the females are locked into "perfect fidelity." Specifically, a female may have at most one mate. Males are allowed to have as many as d female mating partners. If $d = 1$, fidelity applies to the males also. This special case is the perfect fidelity mating function.

4. Necessary and sufficient conditions for certain extinction in a bGWbp Initial research on the bGWbp has focused on determining conditions that guarantee the extinction of a bisexual population. It is clear that an equivalent condition for extinction is for $Z_n = 0$ for some positive integer n. We can think of a bGWbp as a Markov chain $\{Z_n\}_{n=0}^{\infty}$ on the nonnegative integers where state zero is absorbing and all other states are transient. Extinction then is equivalent to absorption into state zero.

Daley [3] stated conditions for the extinction probability to be one when the process is governed by one of the two important mating functions, completely promiscuous mating (cpm) and polygamous mating with perfect fidelity (pmpf). Those results may be summarized as follows. We shall let m denote the mean of the offspring probability distribution. If a bisexual process has the cpm mating function, a necessary and sufficient condition for certain extinction is $\alpha m \leqslant 1$. This implies that the extinction probability will be one in a bisexual process with the cpm mating function when the mean number of females produced per mating unit is less than or equal to one. (The case $Z_0 = 1$ with $p_0 + p_1 + p_2 = 1$ must be excluded here since the number of mating units in this Markov chain will never exceed one and absorption into state zero will definitely occur.) If a process uses the pmpf mating function, Daley showed that extinction is certain if, and only if, the minimum of the mean number of females produced per mating unit (αm) and d times the mean number of males produced per mating unit ($d(1-\alpha)m$) is less than or equal to one. (As before, the case $Z_0 = 1$ with $p_0 + p_1 + p_2 = 1$ must be excluded. The case $Z_0 = 1$ with $p_0 + p_1 + p_2 + p_3 = 1$ and $d = 1$ must also be excluded since there will never be more than one mating unit in any generation of such a process.)

Efforts to find equivalent conditions for certain extinction in bisexual processes in general, were initially stifled by the broadness of the mating function definition. The class of all two-place nonnegative nondecreasing integer-valued functions bounded by xy is a Pandora's Box when it comes to establishing tractable conditions for an extinction probability of one in a bisexual process. It was not until an additional condition was imposed on the mating function that significant progress was made in finding equivalent conditions for guaranteed extinction for a general class of mating functions.

That additional condition is superadditivity and was first proposed by Hull [7].

Definition 1. The mating function ζ is said to be *superadditive* if

$$\zeta(x_1 + x_2, y_1 + y_2) \geqslant \zeta(x_1, y_1) + \zeta(x_2, y_2)$$

for all nonnegative integers x_1, x_2, y_1 and y_2.

Both of Daley's significant mating functions are superadditive. On the other hand, the mating function

$$\zeta(x,y) = \begin{matrix} \max\{x,y\} & \text{if } x \neq 0 \text{ and } y \neq 0 \\ 0 & \text{if } x = 0 \text{ or } y = 0 \end{matrix}$$

is not superadditive. But what human or animal population has ever functioned under such a rule (i.e. every individual is to have at least one mate, if one is available)? A partial list of superadditive mating functions is found in [7].

Superadditivity is a realistic assumption. If superadditivity does not hold for a particular mating function, then for certain numbers of females x_1 and x_2 and for certain numbers of males y_1 and y_2, $\zeta(x_1, y_1) + \zeta(x_2, y_2) > \zeta(x_1 + x_2, y_1 + y_2)$. This may be interpreted as follows. At certain population levels more mating units will be formed when mating is restricted to siblings (i.e., a male and a female of a given generation may mate only when they have been generated by the same mating unit) than when mating is allowed over the entire population of a given generation. This unfortunate and perhaps repulsive situation can be avoided by requiring that mating functions be superadditive. (A more complete consideration of the sibling-mating-only branching process and its use in providing bounds for extinction probabilities in a bGWbp is found in Hull [8].)

The use of superadditivity made it possible to state a necessary but not sufficient condition for guaranteed extinction [7]. Several papers, Hull [8], Bruss [2], and Daley, Hull and Taylor [5], examine the issue of finding necessary and sufficient conditions for an extinction probability of one in a bGWbp. The latter reference has provided the most tractable condition for guaranteed extinction in a bGWbp governed by a superadditive mating function. This condition is stated in the following theorem. When a bisexual process has j mating units initially, we will denote the probability of extinction by q_j.

THEOREM 1. *Let* $r_j = (E(Z_{n+1}|Z_n = j)/j)$. *For a bGWbp with superadditive mating function*, $q_j = 1$ *for all* $j = 0, 1, 2, \ldots$ *if, and only if,*

$$r = \lim_{j \to \infty} r_j = \sup_{j > 0} r_j \leqslant 1.$$

(See [5] for more details.) The quantities r_j are called the mean growth rates (as defined in [5]). The value r_1 tells us all we need to know about certain extinction in a sGWbp. But, as is pointed out in [2] and [5], the sequence $\{r_j\}_{j=1}^{\infty}$ must be considered to insure an extinction probability of one in a bGWbp. Since $\{Z_n\}_{n=0}^{\infty}$ is a Markov chain with a single absorbing state (zero) and all other states (positive integers) transient, either the process is absorbed in state zero (extinction) or $\lim_{n \to \infty} Z_n = \infty$ (survival). Since r is both lim and sup of $\{r_j\}$, when $r \leqslant 1$, each $r_j \leqslant 1$ and the theorem implies that extinction is certain (eventually) no matter how many mating units start the process. On the other hand, if $r > 1$, there exists a positive integer k such that if $j > k$, then $r_j > 1$. It then follows that if Z_0 is large enough, there will be a positive probability of survival.

5. When is Z_0 large enough to insure a positive probability of survival? Theorem 1 motivates the question, if $r > 1$ when are there enough mating units in the initial generation to have an extinction probability less than one? In contrast to the sGWbp it is possible in a bGWbp to lower an extinction probability of one to a value less than one by increasing Z_0 while fixing the other three parameters.

Example 1. Consider a process with the perfect fidelity mating function, $\alpha = 1/2$ and $p_3 \equiv 1$. If $Z_0 = 1$, we have already seen that q_1 will be one. If we increase Z_0 to two, Daley's criterion applies. Since $\min\{\alpha m, (1-\alpha)m\} = 3/2 > 1$, it follows that $q_2 < 1$. (It is known that $\{q_j\}$ is a nonincreasing sequence, see [5].)

It is now our intention to state a simple criterion that will indicate which values of j will give $q_j < 1$ when $r > 1$. That criterion will be stated in Theorem 2. To establish this criterion, we need to state two definitions and prove a lemma. But first, it is the author's view that the mating function definition along with the added condition of superadditivity is still too broad. It would appear that relevant mating functions should also satisfy the following additional two conditions. (It is not by accident that these two conditions are needed to have our criterion for determining when $q_j < 1$.)

(1) $\zeta(1,1) = 1$. This is certainly a reasonable expectation. If a generation consists of one male and one female (forgetting what differences they may have) they will mate.

(2) $\zeta(x,y) \leqslant \min(xy, x+y)$. (Note that $xy < x+y$ only when $x=1$ or $y=1$.) Many superadditive mating functions are bounded by the number of individuals of one or both sexes in any generation.

Definition 2. If ζ is a superadditive mating function that satisfies conditions (1) and (2) we say that ζ is a *population bounded* (*spb*) *mating function*.

Both of Daley's significant mating functions are spb. Note that conditions (1) and (2) along with superadditivity imply that when ζ is spb the following inequalities hold: $\min(x,y) \leqslant \zeta(x,y) \leqslant x+y$. This is a reasonable range for the number of mating units in any generation of a human or animal population.

Definition 3. Since it is known that $\{q_j\}_{j=0}^{\infty}$ is a nonincreasing sequence [5], when $r > 1$, there will be a largest nonnegative integer, say N_ζ, such that $q_{N_\zeta} = 1$.

In Example 1 we see that $q_1 = 1$ and $q_2 < 1$ implies $N_\zeta = 1$.

LEMMA 1.
(a) $\Pr(Z_{n+1} > N_\zeta | Z_n = N_\zeta) = 0$.
(b) *If* $t > N_\zeta$, $\Pr(Z_{n+1} > t | Z_n = t) > 0$.

Proof. (a) If Z_{n+1} has a positive probability of taking on any of the values $N_\zeta + 1, N_\zeta + 2, \ldots$ when $Z_n = N_\zeta$, it would then follow that $q_{N_\zeta} < 1$, a contradiction of the definition of N_ζ.

(b) Assume $\Pr(Z_{n+1} > t | Z_n = t) = 0$ where $t > N_\zeta$. Since the Markov chain $\{Z_n\}_{n=0}^{\infty}$ is stochastically monotone in the sense of Daley [4], $\Pr(Z_{n+1} > t | Z_n = j) = 0$ for all $j = 0, 1, 2, \ldots, t$. As previously indicated, Markov chain theory indicates that either $Z_n = 0$ eventually or $Z_n \to \infty$ as $n \to \infty$. The second possibility is ruled out by the above conditional probabilities being equal to zero. Thus extinction must occur and so $q_t = 1$. But this is a contradiction of the definition of N_ζ.

We can now state the main result of this section.

THEOREM 2. *Assume ζ is a spb mating function in a bGWbp with $r > 1$, then $q_j < 1$ if, and only if, $Pr(Z_{n+1} > j | Z_n = j) > 0$.*

Theorem 2 says that under the given assumptions if we start with j mating units and there is a positive probability of having more than j mating units in the next generation, there is a positive probability of survival.

Proof. Assume $q_j < 1$, then $j > N_\zeta$ by definition of N_ζ and $\Pr(Z_{n+1} > j | Z_n = j) > 0$ by Lemma 1(b).

Assume $\Pr(Z_{n+1} > j | Z_n = j) > 0$. This implies that $p_m > 0$ for some $m \geqslant 2$ where $\{p_n\}$ is the offspring distribution. Otherwise, $p_0 + p_1 = 1$ would imply that the next generation will have at most j individuals and by (2) in the definition of a spb mating function, at most j mating units (a contradiction). Now, $p_m > 0$ for some $m \geqslant 2$ and $\zeta(1,1) = 1$ imply (A) $\Pr(Z_{n+1} \geqslant 1 | Z_n = 1) > 0$. By (A), superadditivity and $\Pr(Z_{n+1} > j | Z_n = j) > 0$, we have (B) $\Pr(Z_{n+1} > j + k | Z_n = j + k) > 0$ for all $k = 0, 1, 2, \ldots$. By (B) and Lemma 1(a), $j + k \neq N_\zeta$ for any $k = 0, 1, 2, \ldots$. Hence, $N_\zeta < j$ and so $q_j < 1$ by the definition of N_ζ.

The next two examples show that conditions (1) and (2) in the definition of a spb mating function are needed in order for $\Pr(Z_{n+1} > j | Z_n = j) > 0$ to imply $q_j < 1$.

Example 2. $\zeta(x, y) = 0$ when $x \leqslant 2$, $y \leqslant 3$ and when $x \leqslant 3$, $y \leqslant 2$ $\zeta(4,4) = \zeta(5,4) = \zeta(4,5) = 3$, $\zeta(x, y) = \min(x, y)$ otherwise, $p_3 \equiv 1$, $\alpha = 1/2$ and $Z_0 = 2$. Note that this mating function is superadditive; (2) holds but (1) does not. Note that $\Pr(Z_{n+1} = 3 | Z_n = 2) > 0$. But, since $\zeta(i, 9 - i) \leqslant 3$ for $i = 0, 1, 2, \ldots, 9$, it follows that $q_2 = q_3 = 1$.

Example 3. $\zeta(2,4) = \zeta(3,3) = \zeta(4,2) = 6$, $\zeta(x, y) = xy$ otherwise, $p_1 \equiv 1$, $\alpha = 1/2$ and $Z_0 = 5$. Here the mating function is superadditive, (1) holds but (2) does not. It is obvious that $\Pr(Z_{n+1} = 6 | Z_n = 5) > 0$. However, $\zeta(i, 6 - i) \leqslant 6$ for $i = 0, 1, \ldots, 6$, implies that $q_5 = q_6 = 1$.

REFERENCES

1. S. Asmussen, On some two-sex population models, *Ann. Prob.* 8 (1980), 727–744.
2. F. T. Bruss, A note on extinction criteria for bisexual Galton-Watson processes, *J. Appl. Prob.* 21 (1984), 915–919.
3. D. J. Daley, Extinction conditions for certain bisexual Galton-Watson branching processes, *Z. Wahrsch. Verw. Gebiete* 9 (1968), 315–322.
4. D. J. Daley, Stochastically monotone Markov chains, *Z. Wahrsch. Verw. Gebiete* 10 (1968), 305–317.
5. D. J. Daley, D. M. Hull, and J. M. Taylor, Bisexual Galton-Watson branching processes with superadditive mating functions, *J. Appl. Prob.* 23 (1986), 585–600.
6. W. Feller, *Introduction to Probability Theory and Its Applications*, Vol. 1, 3rd edition, John Wiley & Sons, Inc., New York, 1968.
7. D. M. Hull, A necessary condition for extinction in those bisexual Galton-Watson branching processes governed by superadditive mating functions, *J. Appl. Prob.* 19 (1982), 847–850.
8. D. M. Hull, Conditions for extinction in certain bisexual Galton-Watson branching processes, *J. Appl. Prob.* 21 (1984), 414–418.
9. D. G. Kendall, Branching processes since 1873, *J. London Math. Soc.* 41 (1966), 385–406.
10. S. M. Ulam, How to formulate mathematically problems of rate of evolution?, *Mathematical Challenges to the Neo-Darwinian Interpretation of Evolution*, Wistar Institute Press, Philadelphia, 1967, pp. 25–26.

A Curious Sequence

HERB R. BAILEY
ROGER G. LAUTZENHEISER
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

We call the finite sequence $a_0, a_1, a_2, \dots, a_n$ *curious* if a_i is the number of i's in the sequence for each $i = 0, 1, \dots, n$. For example, $1, 2, 1, 0$ is a curious sequence with $n = 3$. The problem is to find all such sequences for any n.

This is a good problem for students at almost any level since some thinking is required just to understand the definition. Solutions can be found for small values of n by simple experimentation. For larger n, good students can be challenged by writing a computer program to generate solutions. In addition to finding solutions for large values of n, very good students might be able to prove that these solutions are unique. The problem for $n = 7$ was in the 1978–79 Scottish Mathematical Challenge Examination and the problem for $n = 10$ was in the 1987–88 Wisconsin Mathematics Science and Engineering Talent Search Examination. This sequence also appears as one of a number of interesting mathematical investigations discussed in [1, pages 23–34].

Before giving a general solution, we note two properties of curious sequences. If $s = \sum_{i=0}^{n} a_i$ and $w = \sum_{i=0}^{n} i a_i$ (w for weighted sum), then both s and w equal $n + 1$. That is, s and w are just two different ways of counting how many elements there are in the sequence and thus they both equal $n + 1$.

THEOREM. *For each $n \geqslant 6$, the sequence*

$$a_0 = n - 3,\ a_1 = 2,\ a_2 = 1,\ a_{n-3} = 1, \text{ and } a_i = 0 \text{ otherwise}$$

is a curious sequence and it is unique.

Proof. Since the sequence satisfies the definition of a curious sequence, we need only prove uniqueness. We first observe that a_0 cannot be either 0 or 1. If $a_0 = 0$ then we have an immediate contradiction. If $a_0 = 1$, then all but one of the remaining a_i's are not equal to 0. Thus at least two of the values a_{n-2}, a_{n-1}, and a_n must be non-zero. However, this implies that w is greater than $n + 1$.

We next show that $a_0 = n - 3$ and $a_1 = 2$. Let $a_0 = j$ (by the above argument, $j \geqslant 2$) and $a_1 = k$. It follows that $a_j \geqslant 1$. Let $a_j = l$. Since $s = n + 1$, the sum of the remaining a_i's (other than a_0, a_1, and a_j) must be $n + 1 - j - k - l$. Since the *subscript* of each of these remaining a_i's must be at least 2, it follows that

$$w = \sum_{i=0}^{n} i a_i \geqslant (0)(j) + (1)(k) + (j)(l) + 2(n + 1 - j - k - l)$$

or, collecting terms,

$$w \geqslant 2n + 2 - k - 2j + l(j - 2).$$

Since $w = n + 1$, the above inequality reduces to

$$k + 2j - l(j - 2) \geqslant n + 1. \tag{1}$$

Since $l \geqslant 1$, the above inequality becomes

$$k + 2j - j + 2 \geqslant n + 1$$

or

$$k + j \geqslant n - 1. \tag{2}$$

We now show that $k \geqslant 2$ by noting that if $k = a_1 = 0$ or 1, then $a_i \neq 1$ for all $i \neq 1$. In particular $a_j = l \neq 1$ and thus $l \geqslant 2$. But for $k \leqslant 1$ and $l \geqslant 2$, inequality (1) reduces to

$$1 + 2j - 2(j - 2) \geqslant n + 1 \text{ or } n \leqslant 4,$$

which contradicts $n \geqslant 6$ and thus

$$k \geqslant 2. \tag{3}$$

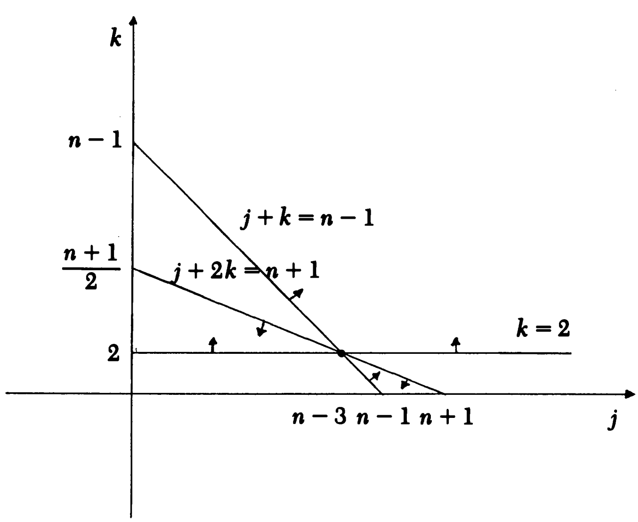
Since $a_0 = j$ and $a_1 = k \geqslant 2$, the k ones in the sequence occur beyond a_1. Therefore,

$$n + 1 = s = \sum_{i=0}^{n} a_i = a_0 + a_1 + \sum_{i=2}^{n} a_i \geqslant j + k + k$$

or

$$n + 1 \geqslant j + 2k. \tag{4}$$

Inequalities (2), (3), and (4) are shown in the following graph and it is seen that the only solution is $a_0 = j = n - 3$ and $a_1 = k = 2$. Since $a_1 = 2$, it follows that a_2 and a_{n-3} are equal to 1 and, therefore, the sequence given in the statement of the theorem is unique.



We leave the solution to the problem for $n \leqslant 5$ to the reader. We note, however, that for some of these n's, there are no curious sequences and for others there are more than one.

REFERENCE

1. A. Gardiner, *Discovering Mathematics—The Art of Investigation*, Oxford University Press, New York, 1987.

On Finite Abelian Groups and Parallel Edges on Polygons

SÁNDOR SZABÓ
University of California at Davis
Davis, CA 95616

1. Parallel edges on polygons Certain geometrical problems may be formulated algebraically. The paradigm case is the solution of ruler and compass construction problems by means of the theory of field extensions. Yet other examples can be found.

We will show here how two results on regular polygons are related to permutations of the elements of a finite abelian group.

In this note, G denotes a finite abelian group written multiplicatively. In order to avoid the trivial cases we suppose that the order of G is at least two. A *complete mapping* of G is a permutation f of G such that

$$a \to af(a), \qquad a \in G$$

is again a permutation of G. L. J. Paige [2] proved that

> *a finite abelian group G always admits a complete mapping unless it possesses a unique involution, i.e., a unique element of order two.*

In particular a cyclic group of even order admits no complete mapping.

The author observed in [3] that

> *a closed polygon which has vertices coinciding with those of a regular polygon of even order always has at least two parallel edges.*

In other words, a closed path that passes once through each vertex of a regular polygon of even order consisting of edges and diagonals of the polygon always has a pair of parallel segments. FIGURE 1 exhibits an example with $n = 8$. We will show that this result is a consequence of Paige's theorem. The group-theoretic approach has the added merit of leading us to a generalization of the original result. In [3] we assumed that the edges of the polygon formed one cycle. We will see that this condition can be removed.

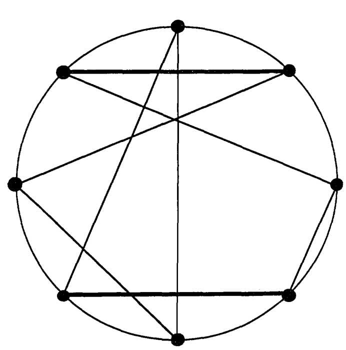


FIGURE 1

To begin, we coordinatize the vertices of the regular n-sided polygon in order, say, counterclockwise, by the elements $e, a, a^2, \dots, a^{n-1}$ of the cyclic group G of order n. The couple (x, y), for x and y in G can be identified with the directed straight line segment with initial point x and terminal point y.

The essential link between the group theory and the geometry is the fact that the directed straight line segments given by (x, y) and (u, v) are parallel if and only if $xy = uv$. To verify this claim, we first note that (x, y) and (u, v) are parallel if, and only if, by moving one way, say clockwise, from x and the other way from y, one goes through the same number of vertices to get to u and v respectively. (See FIGURE 2.)

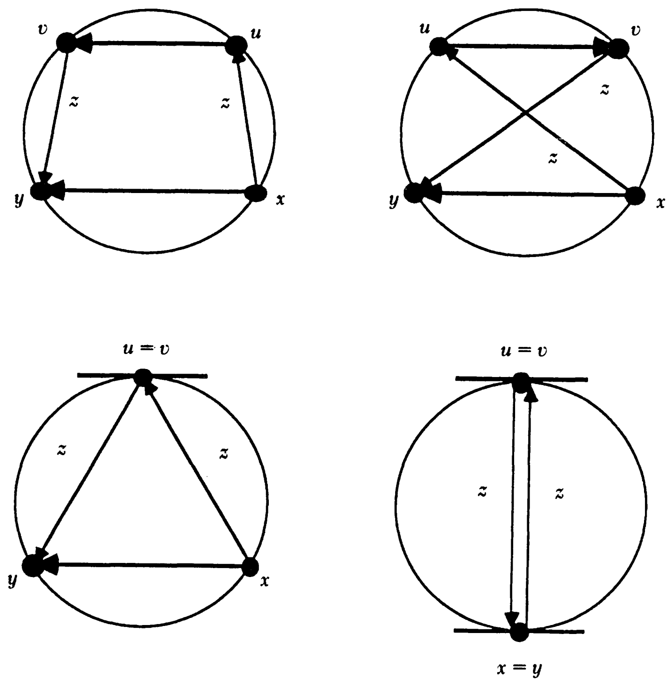


FIGURE 2

Restating this in terms of the coordinate system, we say that (x, y) and (u, v) are parallel if and only if there is a z in G such that $xz = u$ and $yz^{-1} = v$. Multiplying these equations, we have $xy = uv$. Conversely, from the last equation, we get the two prior ones by setting $z = x^{-1}u = v^{-1}y$.

A polygon whose vertices coincide with the vertices of a regular n-gon may consist of more than one connected component. Orient each of these components, or cycles. These oriented cycles define a permutation f of G if we let $f(x) = y$ whenever (x, y) is an edge of this polygon directed consistently with the orientation. Now by Paige's result f cannot be a complete mapping if n is even. Consequently there exist distinct x and y such that $xf(x) = yf(y)$, which means that the edges $(x, f(x))$ and $(y, f(y))$ are parallel.

We have noted that the result applies to polygons with more than one component. Generally one regards polygonal components as having at least three vertices. However, as one of the referees pointed out, we can eliminate this condition also, creating a one-to-one correspondence between "polygons" and the set of all permutations on the vertices of our regular polygon.

To do so, we must extend our identification of polygons with permutations of the vertices to include 2-cycles and 1-cycles. A 2-cycle (x, y) on the vertices will correspond to the two-sided polygonal component with coincident directed edges (x,y) and (y,x). A 1-cycle (x) will be identified with the tangent line at x to the circumscribed circle of the regular polygon, and we will denote this by (x,x). (We will use this concept in the next section also.)

Note that (x,y) is parallel to (u,v) if, and only if, $xy = uv$ even if $x = y$ or $u = v$, so the result still holds: *For any permutation f of the vertices of a regular n-gon with n even, the associated polygon in the sense we have defined it has a pair of parallel edges.* If f includes a 2-cycle, the corresponding polygon can appear to not have two parallel edges. (See FIGURE 3.) However, it contains two *coincident* edges that are trivially parallel.

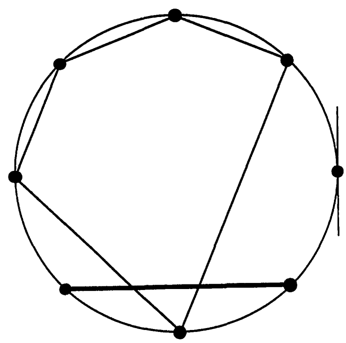


FIGURE 3

2. Kárteszi's theorem on chords Another theorem about parallelism and regular polygons can be proved using our group-theoretic approach. Consider an n-sided regular polygon and its circumscribed circle. We call the set of all chords and tangent lines to the circle passing through the points of the polygon the *line-set* for the polygon. Clearly, a permutation on the n points induces a permutation on the line-set. Using geometrical reasoning, F. Kárteszi [1] has proved that

> *if $n > 2$, then for each permutation of the points of a regular n-sided polygon, there are two distinct elements of the line-set that are parallel and remain parallel after the permutation.*

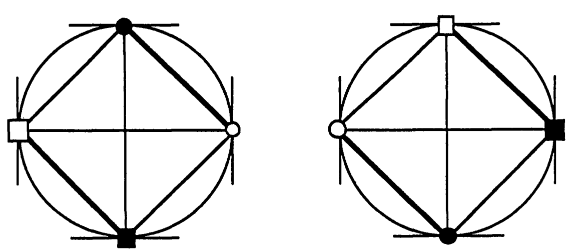


FIGURE 4

FIGURE 4 illustrates the situation for $n = 4$.

Stating this in algebraic terms, using the ideas developed in the previous section, we see that Kárteszi's result is equivalent to:

> *For each permutation f of the finite cyclic group G of order greater than 2 there are elements x, y, u and v in G such that*

$$xy = uv, \quad x \neq u, \quad x \neq v, \quad y \neq u, \quad y \neq v \quad \text{and} \quad f(x)f(y) = f(u)f(v). \qquad (1)$$

This algebraic restatement of the problem is easy to prove. In fact, it holds for any finite abelian group G, not only for cyclic ones. Let f be a fixed permutation of G and let b be a fixed element of G other than e. This element b exists since the order of G is greater than two. Clearly for all a in G, $a \neq ab$ and so $f(a) \neq f(ab)$. When the element a runs over the elements of G, then the element $f(ab)(f(a))^{-1}$ only runs over the nonidentity elements of G. By the pigeon-hole principle there are distinct elements c and d in G for which

$$f(cb)(f(c))^{-1} = f(db)(f(d))^{-1},$$

or equivalently for which

$$f(cb)f(d) = f(db)f(c).$$

Setting

$$cb = x, \quad d = y, \quad db = u, \quad c = v,$$

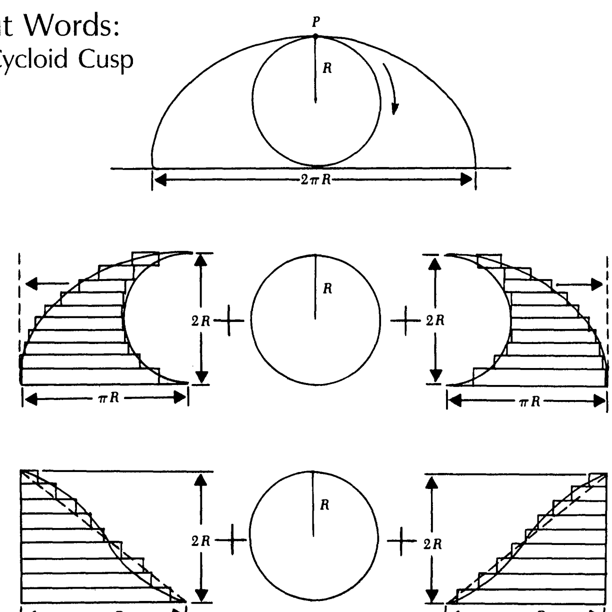
we have the conditions in (1) satisfied as desired.

Acknowledgments. I would like to thank the referees for their contributions, significantly improving the quality of exposition.

REFERENCES

1. F. Kárteszi, Su una proprietà combinatoria dei poligoni regolari, *Boll. Un. Mat. Ital.* (5) 13A (1976) no. 1, 139–141.
2. L. J. Paige, A note on finite abelian groups, *Bull. Amer. Math. Soc.*, 53 (1947), 590–593.
3. S. Szabó, A remark on regular polygons, *Mat. Lapok* 28 (1980), 199–202 (in Hungarian).

Proof without Words:
Area under a Cycloid Cusp



$\frac{1}{2}\pi R 2R \quad + \quad \pi R^2 \quad + \quad \frac{1}{2}\pi R\, 2R$

$\Rightarrow A = 3\pi R^2$

—RICHARD M. BEEKMAN
MORENO VALLEY, CA 92388

This algebraic restatement of the problem is easy to prove. In fact, it holds for any finite abelian group G, not only for cyclic ones. Let f be a fixed permutation of G and let b be a fixed element of G other than e. This element b exists since the order of G is greater than two. Clearly for all a in G, $a \neq ab$ and so $f(a) \neq f(ab)$. When the element a runs over the elements of G, then the element $f(ab)(f(a))^{-1}$ only runs over the nonidentity elements of G. By the pigeon-hole principle there are distinct elements c and d in G for which

$$f(cb)(f(c))^{-1} = f(db)(f(d))^{-1},$$

or equivalently for which

$$f(cb)f(d) = f(db)f(c).$$

Setting

$$cb = x, \quad d = y, \quad db = u, \quad c = v,$$

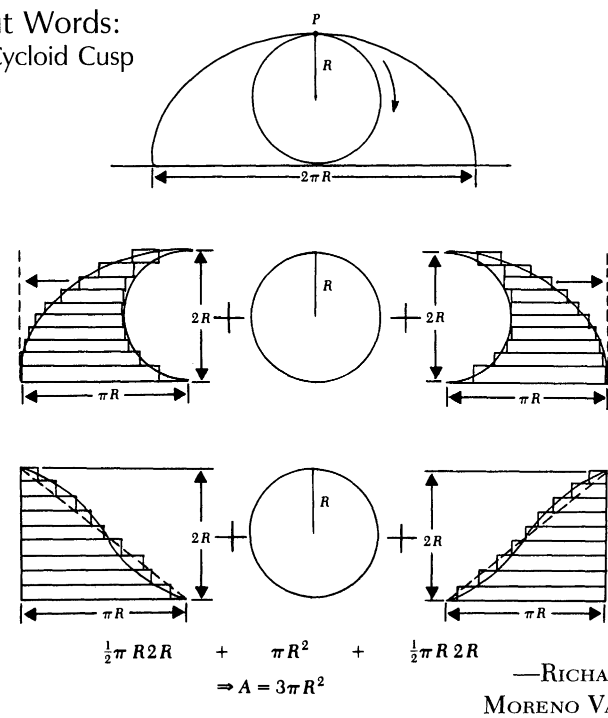
we have the conditions in (1) satisfied as desired.

Acknowledgments. I would like to thank the referees for their contributions, significantly improving the quality of exposition.

REFERENCES

1. F. Kárteszi, Su una proprietà combinatoria dei poligoni regolari, *Boll. Un. Mat. Ital.* (5) 13A (1976) no. 1, 139–141.
2. L. J. Paige, A note on finite abelian groups, *Bull. Amer. Math. Soc.*, 53 (1947), 590–593.
3. S. Szabó, A remark on regular polygons, *Mat. Lapok* 28 (1980), 199–202 (in Hungarian).

Proof without Words:
Area under a Cycloid Cusp



—RICHARD M. BEEKMAN
MORENO VALLEY, CA 92388

A Quick Solution of Triangle Counting

LEONARD M. SMILEY
University of Alaska
Anchorage, AK 99508

The first law of famous counting problems must be that each solver regards his or her approach as the only truly simple one. Undissuaded, and motivated by the recent reminiscence [1], I offer the following. *Problem*. Find a formula for T_n, the total number of triangles in an equilateral triangle of side n tiled by equilateral triangles of side 1 (see FIGURE 1).

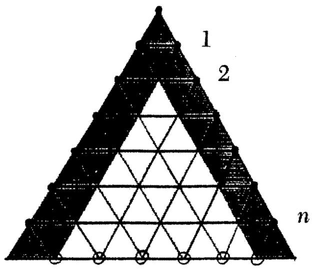


FIGURE 1

A triangle is *new* if it contains a triangle from the bottom row of the diagram. The number of new triangles is $T_{n+1} - T_n$. A triangle is *crusty* if it contains a triangle from the shaded 'crust'. All triangles are either *nablas* (∇) or *deltas* (Δ).

The number of new but not crusty triangles is clearly $T_{n-1} - T_{n-2}$. The new, crusty deltas have their top apices "beaded." There are $2n + 1$ of them. The new, crusty nablas have their bottom apices "circled." There are n of them. Thus

$$T_{n+1} - T_n = T_{n-1} - T_{n-2} + 3n + 1.$$

This is an unremarkable recurrence, which, when supplied with $T_1 = 1$, $T_2 = 5$ and $T_3 = 13$ produces

$$T_n = \frac{(-1)^n + 4n^3 + 10n^2 + 4n - 1}{16}.$$

The characteristic cubic is particularly nice to factor by grouping and the methods of [2, Ch. 5] or [3, Sec. 7.3] determine the coefficients of T_n easily. For computer algebra converts, one call to the *genf* function in MACSYMA produces the answer as shown here.

REFERENCES

1. M. E. Larsen, The eternal triangle—a history of a counting problem, *College Math. J.* 20 (1989) 370–384.
2. M. R. Spiegel, *Calculus of Finite Differences and Difference Equations*, Schaum's Outline Series, McGraw-Hill Book Co., New York, 1971.
3. R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics*, Addison-Wesley Publishing Co., Reading, PA 1989.

Extensions of a Sums-of-Squares Problem

KELLY JACKSON
FRANCIS MASAT
ROBERT MITCHELL
Glassboro State College
Glassboro, NJ 08028

While discussing Lagrange's theorem (every integer can be written as a sum of four squares, not all necessarily nonzero) in a number theory class, Jackson, a graduate student, noted a result in Niven and Zuckerman [1, p. 145] showing that all but a few integers can be written as the sum of 5 nonzero squares. Our resulting discussion shows that the "5" in this result can be increased indefinitely. Moreover, due to an unusual property of 169, we also establish our

Main Result. All but a finite number of integers can be written as a sum of N nonzero squares for all natural numbers N such that $5 \leq N \leq 156$.

We started with $N = 5$ in our main result since it is well known [1] that there are infinitely many integers that are not expressible as a sum of 4 nonzero squares. Before we prove our Main Result, and for the convenience of the reader, we first give a proof of the result in [1]. For this we use an interesting fact: 169 has the unusual property that it may be written as a single square or as the sum of 2, 3, or 4 squares, namely,

$$169 = 13^2 = 12^2 + 5^2 = 12^2 + 4^2 + 3^2 = 8^2 + 8^2 + 5^2 + 4^2.$$

Thus, for a natural number $K \geq 169$, set $A = K - 169$ and apply Lagrange's result to A; i.e., $A = w^2 + x^2 + y^2 + z^2$ and, without loss of generality, $w \geq x \geq y \geq z$. We then have four cases:

For $z > 0$,	$K = 13^2 + w^2 + x^2 + y^2 + z^2$.
For $y > 0$ and $z = 0$,	$K = 12^2 + 5^2 + w^2 + x^2 + y^2$.
For $x > 0$ and $y = 0$,	$K = 12^2 + 4^2 + 3^2 + w^2 + x^2$.
For $w > 0$ and $x = 0$,	$K = 11^2 + 4^2 + 4^2 + 4^2 + w^2$.

We thus see that every integer greater than 169 is expressible as a sum of 5 nonzero squares. Checking the integers ≤ 169, however, we note that only 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, and 33 do not share this property. Thus, we have the following:

Remark 1. Any integer > 33 may be written as a sum of 5 nonzero squares.

The preceding process helped lead us to a First Result.

If we know that Z may be written as a sum of N nonzero squares, then $Z + 1$ may be written as a sum of $N + 1$ nonzero squares by simply adding 1^2. By Remark 1, then, we see that every integer $K > 33$ can be written as a sum of 5 nonzero squares plus additional 1^2s as needed. Thus, if K is greater than

34,	K may be written as a sum of 6 nonzero squares,
35,	K may be written as a sum of 7 nonzero squares,
⋮	
M,	K may be written as a sum of $M - 28$ nonzero squares.

Specifically, then, we have our

First Result. Given any positive integer M, every integer K such that $K > M + 28$ may be written as a sum of N nonzero squares for $N = 5, 6, \ldots, M$. In particular, if $K > 184$, then K may be written as the sum of N nonzero squares for $N = 5$ to 156.

Our First Result is certainly interesting, but we will improve it by showing that the bound, $M + 28$, can be lowered by using different representations of 169.

Earlier, we stated that 169 may be written as a sum of 1, 2, 3, or 4 nonzero squares. Surprisingly, calculation shows that this trend continues for 5 through 155. Thus, 169 can be written as a sum of N nonzero squares for $N = 1$ to 155. To find the specific squares needed and their number, one of two procedures may be used. Where $N \geq 41$, inspection shows that we need to use only combinations of 3^2, 2^2 and 1^2. Significantly, this allows us to simplify our selection process; i.e., the formula table shown here yields the desired N term representation of 169 for $N \geq 41$.

Formula Table for Representations of 169 for $N \geq 41$.

$N \equiv$	# of 3^2	# of 2^2	# of 1^2
0 (mod 3)	2	$37 - (N - 42)/3$	$4(N - 42)/3 + 3$
1 (mod 3)	0	$42 - (N - 43)/3$	$4(N - 43)/3 + 1$
2 (mod 3)	1	$40 - (N - 41)/3$	$4(N - 41)/3$

For the sake of example, if

$$N = 120, \text{ then } 169 = 2 \cdot 3^2 + 11 \cdot 2^2 + 107 \cdot 1^2,$$
$$N = 121, \text{ then } 169 = 0 \cdot 3^2 + 16 \cdot 2^2 + 105 \cdot 1^2,$$
$$N = 122, \text{ then } 169 = 1 \cdot 3^2 + 13 \cdot 2^2 + 108 \cdot 1^2.$$

For $N < 41$, we note that $169 = 25$ plus $1 \cdot 12^2, 9 \cdot 4^2, 16 \cdot 3^2, 14 \cdot 3^2 + 3 \cdot 2^2 + 6 \cdot 1^2$, or $10 \cdot 3^2 + 11 \cdot 2^2 + 10 \cdot 1^2$. That is, 169 equals 25 plus 1, 9, 16, 23, or 31 other squares. But, 25 also may be written as a sum of N squares for $N = 4$ to 11 (proof is left to reader). Thus, by using the eight different representations of 25 and adding on 1, 9, 16, 23, or 31 other squares, we can in fact obtain a representation for N that is between 5 and 40, inclusive. So far, then, we have

Remark 2. The number 169 can be written as a sum of N nonzero squares for $N \leq 155$.

The reader may show that Remark 2 is not true for $N = 156$ and other larger values. With Remark 2 in mind, we now restate our

Main Result (Restated). *Every integer greater than* 169 *can be written as a sum of N nonzero squares for all natural numbers N such that* $5 \leq N \leq 156$.

Proof. For $K \geq 169$, we again set $K = A + 169$ and recall that A can be written as the sum of j nonzero squares for some $1 \leq j \leq 4$. Since $1 \leq (N - j) \leq 155$, then by Remark 2 we can write 169 as the sum of $(N - j)$ nonzero squares. Thus, K may be written as the sum of $j + (N - j)$ or N nonzero squares.

How does this improve our First Result? In our First Result, if $K > 184$; i.e., $K > 156 + 28$, then K can written as a sum of 156 nonzero squares. But our Main Result now says that every integer greater than 169 is expressible in such a way.

A last comment. We stopped our discussion at $N = 155$ since the sums for 169 were not predictable after that. An open question remains, however: Given any integer K, is there an integer M which is expressible as a sum of N nonzero squares where $1 \leq N \leq K$?

Acknowledgment. The authors wish to thank the referees for their many helpful comments and suggestions, particularly regarding our First Result and last comment.

REFERENCE

1. Ivan Niven and M. S. Zuckerman, *An Introduction to the Theory of Numbers*, 4th edition, John Wiley & Sons, Inc., New York, 1980.

Naming Things

I

If asteroids were what you find
Then you could give them any kind
Of names that might appeal to you.
Biologists can do this too.
In mathematics, it's quite tough:
Our options are not broad enough.

II

Why does tradition have to matter?
Why can't we name our finds to flatter
The head of our department, or
An influential senator?
Or give a relative a lift:
A theorem makes a charming gift.
"Dear Mary's Theorem" sounds quite nice;
"Aunt Emma's Lemma" would add spice.

III

Now, if you find a great result,
Why can't you show that you exult,
And call it "My ingenious scheme,"
Or label it as "Childhood's Dream"?
Our ancestors were less inhibited
And let their feelings be exhibited.
Considering what they could do,
It's stuffy editors, that's who,
If we'd attempt to do the same
Would never let us play this game.

from the uncollected verse of

RALPH P. BOAS
1912–1992

Acknowledgment. The authors wish to thank the referees for their many helpful comments and suggestions, particularly regarding our First Result and last comment.

REFERENCE

1. Ivan Niven and M. S. Zuckerman, *An Introduction to the Theory of Numbers*, 4th edition, John Wiley & Sons, Inc., New York, 1980.

Naming Things

I

If asteroids were what you find
Then you could give them any kind
Of names that might appeal to you.
Biologists can do this too.
In mathematics, it's quite tough:
Our options are not broad enough.

II

Why does tradition have to matter?
Why can't we name our finds to flatter
The head of our department, or
An influential senator?
Or give a relative a lift:
A theorem makes a charming gift.
"Dear Mary's Theorem" sounds quite nice;
"Aunt Emma's Lemma" would add spice.

III

Now, if you find a great result,
Why can't you show that you exult,
And call it "My ingenious scheme,"
Or label it as "Childhood's Dream"?
Our ancestors were less inhibited
And let their feelings be exhibited.
Considering what they could do,
It's stuffy editors, that's who,
If we'd attempt to do the same
Would never let us play this game.

from the uncollected verse of

RALPH P. BOAS
1912–1992

A Reformulation of the Goldbach Conjecture

LARRY J. GERSTEIN
University of California
Santa Barbara, CA 93106

The Goldbach conjecture, dating from Goldbach's correspondence with Euler in 1742, is this: *Every even integer greater than* 2 *is the sum of two prime numbers* (*not necessarily distinct*). It has been verified that the even integers through 10^8 have the stated property, but Goldbach's conjecture remains unproved.

The main purpose of this note is to restate Goldbach's conjecture in a somewhat different form. While it will be easy to check that the version to be given here is equivalent to the original, this formulation does not seem to be explicitly stated in the literature. Of course the "literature" on the Goldbach conjecture is vast, and it includes almost every book with "elementary number theory" in its title, as well as a multitude of research papers. For the convenience of the reader, here are a few places to look for references and background information. Dickson [**1**, pp. 421–425] lists results obtained through the first decade of this century. Wang [**4**] is a collection of this century's most important papers on the Goldbach conjecture through the early 1980's. Shanks [**3**] is a marvelous book on conjectures in number theory, Goldbach's among them, and on mathematical conjectures in general. Ribenboim [**2**] is another treasure chest in number theory, with a section on Goldbach (pp. 229–235). As a consequence of the reformulation to be given here, we will see a close connection between the Goldbach conjecture and the *twin prime conjecture*, which is: *There are infinitely many primes* p *such that* $p + 21$ *is also prime*. (See [**2**], pp. 199–204, for some history and the current state of affairs regarding the twin prime conjecture.) This connection is certainly not well known, as can be confirmed by the following experiment: Grab some elementary number theory books, locate the inevitable statements of the Goldbach and twin prime problems, and see whether any linkage is established. I'm betting that the only linkages you will find are that both problems deal with prime numbers and both problems are described as famous, old, hard, and open.

Suppose the Goldbach conjecture is true. Then for each integer $n \geq 2$ there are primes p and q, with $p \leq q$, say, such that $2n = p + q$. Hence $p = n - k$ and $q = n + k$ for some integer k satisfying $0 \leq k \leq n - 2$. Therefore $n^2 - k^2 = pq$. Conversely, suppose that for each integer $n \geq 2$ there exists k satisfying $0 \leq k \leq n - 2$ and primes p and q, with $p \leq q$, such that $n^2 - k^2 = pq$. Then $p = n - k$ and $q = n + k$, by the fundamental theorem of arithmetic, and hence $2n = p + q$. We have shown therefore that Goldbach's conjecture is equivalent to the following statement:

(*) For every integer $n \geq 2$ there exist integers k, p, and q, with $0 \leq k \leq n - 2$ and with p and q prime, such that $n^2 - k^2 = pq$.

This restatement of the Goldbach conjecture leads us to consider the binary quadratic form $x^2 - y^2$, and here are some elementary observations. For p and q given odd primes, with $p \leq q$, a straightforward arithmetic argument shows that there are just two nonnegative integer solutions to the equation $x^2 - y^2 = pq$; namely,

$$(x, y) = ((p+q)/2, (q-p)/2) \quad \text{and} \quad (x, y) = ((pq+1)/2, (pq-1)/2).$$

On the other hand, there are infinitely many *rational* solutions. In fact, if $\beta \in \mathbb{Q}^* = \mathbb{Q} - \{0\}$, then for all $\lambda \in \mathbb{Q}^*$ we have

$$\beta = \left((\lambda^2 + \beta)/2\lambda\right)^2 - \left((\lambda^2 - \beta)/2\lambda\right)^2.$$

For the Goldbach conjecture we need to work in the opposite direction; that is, we consider the values of $x^2 - y^2$ when $x = n$ is fixed and y varies in $\mathbb{Z}$, and we look for appropriate primes p and q.

Whether or not $(*)$ is true, it is intriguing to ask how often $k = 1$ works in $(*)$ and to make the following conjecture:

$(**)$ There are infinitely many integers $n \geq 2$ for which there exist primes p and q such that $n^2 - 1 = pq$.

Statement $(**)$ is clearly equivalent to the twin prime conjecture. Thus, while the Goldbach and twin prime conjectures are not the same, they are evidently facets of the same jewel.

REFERENCES

1. Leonard E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea Publishing Co., New York, 1971.
2. Paulo Ribenboim, *The Book of Prime Number Records*, 2nd edition, Springer-Verlag Inc., New York, 1989.
3. Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd edition, Chelsea Publishing Co., New York, 1985.
4. Wang Yuan (Editor), *Goldbach Conjecture*, World Scientific Publishing Co., Singapore, 1984.

A Lesser-Known Goldbach Conjecture

LAURENT HODGES
Iowa State University
Ames, IA 50011

In Example 64 of his recent article [**1**], R. K. Guy asked about the representations of odd positive integers as sums of a prime and twice a square, mentioning that Ruemmler had found the first exception to be 5777 and wondered if it might be the last.

This problem has a long history, beginning with Christian Goldbach, best known for his 1742 conjecture that every even integer can be represented as the sum of two primes. In the last paragraph of a letter to Leonhard Euler dated 18 November 1752, Goldbach expressed his belief that every odd integer could be written in the form $p + 2a^2$, where p is a prime (or 1, then considered a prime) and $a \geqslant 0$ is an integer [**2**, p. 594]. Writing in his usual mixture of German and Latin, Goldbach said:

> Noch habe ein kleines ganz neues theorema beyzufügen, welches so lange vor wahr halte, donec probetur contrarium: Omnis numerus impar est = duplo quadrati + numero primo, sive $2n - 1 = 2aa + p$, ubi a denotet numerum integrum vel 0, p numerum primum, ex. gr. $17 = 2 \cdot 0^2 + 17$, $21 = 2 \cdot 1^2 + 19$, $27 = 2 \cdot 2^2 + 19$, etc.

On the other hand, there are infinitely many *rational* solutions. In fact, if $\beta \in \mathbb{Q}^* = \mathbb{Q} - \{0\}$, then for all $\lambda \in \mathbb{Q}^*$ we have

$$\beta = ((\lambda^2 + \beta)/2\lambda)^2 - ((\lambda^2 - \beta)/2\lambda)^2.$$

For the Goldbach conjecture we need to work in the opposite direction; that is, we consider the values of $x^2 - y^2$ when $x = n$ is fixed and y varies in $\mathbb{Z}$, and we look for appropriate primes p and q.

Whether or not $(*)$ is true, it is intriguing to ask how often $k = 1$ works in $(*)$ and to make the following conjecture:

$(**)$ There are infinitely many integers $n \geq 2$ for which there exist primes p and q such that $n^2 - 1 = pq$.

Statement $(**)$ is clearly equivalent to the twin prime conjecture. Thus, while the Goldbach and twin prime conjectures are not the same, they are evidently facets of the same jewel.

REFERENCES

1. Leonard E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea Publishing Co., New York, 1971.
2. Paulo Ribenboim, *The Book of Prime Number Records*, 2nd edition, Springer-Verlag Inc., New York, 1989.
3. Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd edition, Chelsea Publishing Co., New York, 1985.
4. Wang Yuan (Editor), *Goldbach Conjecture*, World Scientific Publishing Co., Singapore, 1984.

A Lesser-Known Goldbach Conjecture

LAURENT HODGES
Iowa State University
Ames, IA 50011

In Example 64 of his recent article [**1**], R. K. Guy asked about the representations of odd positive integers as sums of a prime and twice a square, mentioning that Ruemmler had found the first exception to be 5777 and wondered if it might be the last.

This problem has a long history, beginning with Christian Goldbach, best known for his 1742 conjecture that every even integer can be represented as the sum of two primes. In the last paragraph of a letter to Leonhard Euler dated 18 November 1752, Goldbach expressed his belief that every odd integer could be written in the form $p + 2a^2$, where p is a prime (or 1, then considered a prime) and $a \geqslant 0$ is an integer [**2**, p. 594]. Writing in his usual mixture of German and Latin, Goldbach said:

> Noch habe ein kleines ganz neues theorema beyzufügen, welches so lange vor wahr halte, donec probetur contrarium: Omnis numerus impar est = duplo quadrati + numero primo, sive $2n - 1 = 2aa + p$, ubi a denotet numerum integrum vel 0, p numerum primum, ex. gr. $17 = 2 \cdot 0^2 + 17$, $21 = 2 \cdot 1^2 + 19$, $27 = 2 \cdot 2^2 + 19$, etc.

In his reply dated 16 December 1752, Euler wrote that he had verified this up to 1000 [**2**, p. 596], and in a letter dated 3 April 1753 [**2**, p. 606] he extended the verification up to 2500. Euler also remarked that as the odd number $2n+1$ increased, the number of representations tended to increase.

Over a century later, in 1856, Moritz A. Stern, professor of mathematics at Göttingen, became interested in this problem, perhaps from having read the Goldbach-Euler correspondence [**2**] published by Euler's grandson in 1843. Stern and some of his students checked the odd integers up to 9000 and found two exceptions, 5777 and 5993, which I shall refer to as *Stern numbers* [**3**]. The former of these is the one mentioned in Guy's article [**1**]. Stern also reported that the only primes up to 9000 that could not be expressed in the form $p+2a^2$ in terms of a smaller prime p and an integer $a>0$ were 17, 137, 227, 977, 1187, and 1493, which I shall refer to as *Stern primes*. The tables constructed by Stern and his students were preserved in the library of Adolf Hurwitz, professor of mathematics at Zurich, and made available by Pólya to Hardy and Littlewood [**4**].

I have recently checked these results up to 1,000,000 on a microcomputer. There are no new Stern numbers or Stern primes, only the eight found by Stern. In view of the smallness of the known Stern numbers and Stern primes, it is tempting to replace Goldbach's original conjecture by the new conjectures that there are only a finite number of Stern numbers and Stern primes, and that the list above is complete. The reason for this, of course, is that the average number of ways of expressing an odd integer $2n-1$ as a prime plus twice a square increases without limit as n increases. For example, since the number of primes up to n is on the order of $n/\log n$ while the number of squares up to n is on the order of $n^{1/2}$, the average number of ways of expressing odd numbers up to $3n$ as a prime plus twice a square is at least

$$\frac{n}{\log n}\cdot n^{1/2}\cdot\frac{1}{3n}=\frac{n^{1/2}}{3\log n}$$

("at least" because there are also sums involving primes or squares between n and $3n$). In fact, Hardy and Littlewood [**4**] listed as their Conjecture I: *Every large odd number n is the sum of a prime and the double of a prime. The number $N(n)$ of representations is given asymptotically by*

$$N(n)\sim\frac{\sqrt{2n}}{\log n}\prod_{\varpi=3}^{\infty}\left(1-\frac{1}{\varpi-1}\left(\frac{2n}{\varpi}\right)\right).$$

Here ϖ runs through the odd primes and $\left(\frac{2n}{\varpi}\right)$ is Legendre's symbol. The meaning of the factors in the infinite product can be seen by considering the factor for $\varpi=3$. For $a\equiv 0$, 1, or 2 mod 3 we have $2a^2\equiv 0$, 2, or 2 mod 3. If an odd number $n\equiv 0$ mod 3, then one-third of the time $n-2a^2$ is divisible by 3 and cannot be a prime; in this case $\left(\frac{2n}{3}\right)=0$ and the factor for $\varpi=3$ is 1. But if the odd number $n\equiv 2 \bmod 3$, then two-thirds of the time $n-2a^2$ is divisible by 3 and cannot be a prime; in this case $\left(\frac{2n}{3}\right)=1$ and the factor for $\varpi=3$ is only $\frac{1}{2}$. Both Stern numbers 5777 and 5993 (and all the Stern primes, as well) are congruent to 2 mod 3, as one would expect. In fact, for both 5777 and 5993 there is a predominance of $+1$ Legendre symbols for small primes: For $\varpi=3,5,7,11,13,\ldots,\left(\frac{2n}{\varpi}\right)=1,1,1,1,1,-1,-1,1,-1,\ldots$ for $n=5777$ and $\left(\frac{2n}{\varpi}\right)=1,1,1,-1,0,1,1,1,1,\ldots$ for $n=5993$.

This increase in the average number of representations in the form $p+2a^2$ can be seen in the computer calculations. A consequence of this is that if one lists all the numbers that can be represented in exactly $N\geqslant 0$ ways as a prime and twice a square, the list appears to be finite for every value of N. Up to 200,000, for example, we find:

2 numbers, 5777 and 5993, that cannot be represented in this way;

28 numbers ranging from 17 to 6,797 that can be represented in exactly one way;

109 numbers ranging from 3 to 59,117 that can be represented in exactly two ways;

225 numbers ranging from 13 to 48,143 that can be represented in exactly three ways;

364 numbers ranging from 19 to 87,677 that can be represented in exactly four ways;

499 numbers ranging from 55 to 148,397 that can be represented in exactly five ways; etc.

As Guy [1] pointed out, it is known that the density of Stern numbers is zero. However, the computer calculations suggest an even stronger conjecture: *For every number $N \geqslant 1$ there are only a finite number of odd integers that cannot be represented as the sum of a prime and twice a square in at least N ways.* This conjecture is also stronger than Conjecture I of Hardy and Littlewood [4].

The computer calculations lead to some new sequences that may be of interest to those who collect quaint and curious sequences. If the conjecture above is correct, we can form a sequence whose nth term is the largest odd number that can be represented as the sum of a prime and twice a square in no more than $n-1$ ways; this sequence appears to exist and to start:

$$5993, 6797, 59117, 59117, 87677, 87677, \ldots.$$

As expected, these numbers are all congruent to 2 mod 3. Another new sequence that definitely exists is defined to have an nth term that is the smallest odd number that can be represented as the sum of a prime and twice a square in at least n ways:

3, 3, 13, 19, 55, 61, 139, 139, 181, 181, 391, 439, 559, 619, 619, 829, 859, 1069, ...

As expected, these numbers, after 3 itself, are all congruent to 1 mod 3. From these can be constructed yet more obscure sequences, such as that consisting of those numbers that are a smallest odd number that can be represented as the sum of a prime and twice a square in at least n ways for more than one value of n:

$$3, 139, 181, 619, 2341, 3331, 4189, 4801, 5911, 6319, 8251, 9751, 11311, \ldots.$$

REFERENCES

1. Richard K. Guy, The second strong law of small numbers, this MAGAZINE 63 (1990), 3–20.
2. P. H. Fuss (editor), *Correspondance Mathématique et Physique de Quelques Célèbres Géomètres du XVIII^{ème} Siècle*, Vol. 1 (1843, reprinted by Johnson Reprint Corp., New York).
3. Moritz A. Stern, Sur un assertion de Goldbach relative aux nombres impairs, Nouvelles Annales Math. 15 (1856), 23–24.
4. Godfrey Harold Hardy and John Edensor Littlewood, Some problems of 'partitio numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.*, 44 (1922), 1–70.

The Remarkable Number 648

ROBERT O. STANTON
St. John's University
Jamaica, NY 11439

On a recent examination in an elementary course, I asked for the prime factorization of 972. One student answered the question as follows:

$$9 = 3^2$$
$$72 = 2^3 \cdot 3^2$$
$$\text{Therefore } 972 = (3^2) \cdot (2^3 \cdot 3^2) = 2^3 \cdot 3^4.$$

Before merely dismissing this response as just one of the many blunders that students make, note that the correct answer is $972 = 2^2 \cdot 3^5$. The same primes appear in both answers, and the sum of the exponents is also the same. The class of numbers satisfying these properties is an interesting one, as may be seen by applying some elementary number theory.

A positive integer n is *split* by placing a double vertical line between two of its decimal digits, e.g. $9\|72$ as above. Formally, n is written as $n = 10^k a + b$ where $k > 0$, $a > 0$, and $b < 10^k$ are integers. Throughout this paper, n, k, a, and b will have this meaning. Clearly, once n and k are given, a and b are uniquely determined. Additionally, let

$P(n)$ = the set of all primes in the prime factorization of n.

$E(n)$ = the sum of the exponents in the prime factorization of n.

The numbers of interest are as follows:

DEFINITION. *A positive integer n is an LB number if it may be split so that:*

$$P(n) = P(a) \cup P(b) \tag{P}$$

and

$$E(n) = E(a) + E(b) \tag{E}$$

are both satisfied. If n is an LB number, then the product ab is called an LB residue.

(The aforementioned student, who will otherwise remain anonymous, had initials L. B.) If $n = 972$, $a = 9$ and $b = 72$, it follows from the work above that $P(n) = \{2, 3\}$ and $E(n) = 7$ satisfy equations (P) and (E). The LB residue of 972 is $9 \cdot 72 = 648$. The LB residue is the number whose prime factorization is obtained by the incorrect method above. Note that since $b < 10^k$, the LB residue ab of n is always less than n. It is useful to list some elementary properties of these numbers, which may be easily verified by the reader.

PROPOSITION 1.1. *If $m < n$ are positive integers and m divides n, then $P(m) \subseteq P(n)$ and $E(m) < E(n)$.*

PROPOSITION 1.2. *If n is an LB number, then at least two different primes divide n.* (Assume to the contrary that there is only one such prime. Then for equation (E) to be satisfied, n would have to equal its LB residue.)

PROPOSITION 1.3. *Let n be an LB number with splitting* $10^k a + b$ *and p be a prime.*
(a) *p divides n if and only if p divides b.*
(b) *If p divides a, then p divides n.*

The converse of (b) need not be true, since the primes 2 and 5 may divide n without necessarily dividing a. Since 2 and 5 are the primes that divide the base 10, they will be called *basal* primes. All other primes are *nonbasal*. For nonbasal primes, Proposition 1.3 may be strengthened as follows:

PROPOSITION 1.4. *Let n be an LB number with splitting* $10^k a + b$ *and p be a nonbasal prime. Then the following are equivalent:*
(a) *p divides n.*
(b) *p divides a.*
(c) *p divides b.*

The number of digits of a prime in $P(n)$ has an effect on the number of digits of an LB number n. The following result, which is immediate from Proposition 1.4, will later be strengthened:

PROPOSITION 1.5. *If p is a d digit prime divisor of the LB number n, then n has at least* $2d$ *digits.*

Some additional restrictions on a and b in an LB number follow from the results above.

PROPOSITION 1.6. *Let* $n = 10^k a + b$ *be an LB number. Then*
(a) *a is not equal to* 1, *and*
(b) *b is not equal to* 0, *and at least two primes divide b.*

THEOREM 1.7. *If* $n = 10^1 a + b$, *then n is not an LB number.*

Proof. As a consequence of Proposition 1.6(b), $b = 6$, so $n = 10a + 6$. In view of Proposition 1.4, $n = 2^s 3^t$ and $a = 2^q 3^r$, where $q \geq 0$ and $r, s, t \geq 1$. Substitution and some elementary algebra yield the following equation:

$$5 \cdot 2^q \cdot 3^r = 3(2^{s-1} \cdot 3^{t-1} - 1). \tag{1}$$

It is impossible for both s and t to equal one, for then the right side of (1) would be zero. There are three cases that are of concern.

Case 1. $s > 1$ and $t > 1$.

Under this hypothesis, neither 2 nor 3 divide the expression in parentheses in (1), so $q = 0$ and $r = 1$. This implies that $n = 36$, which is not an LB number because it fails to satisfy equation (E).

Case 2. $s = 1$ and $t > 1$.

Since $t > 1$, the expression in parentheses in (1) is not divisible by 3, so $r = 1$. Equation (1) reduces to $5 \cdot 2^q = 3^{t-1} - 1$. In order for equation (E) to be satisfied by n, it is necessary for $s + t = q + r + 2$ to be true, or in this case, $t = q + 2$. The equation above becomes $5 \cdot 2^q = 3^{q+1} - 1$. Reducing mod 3 shows that q must be even and reducing mod 5 shows that q must be of the form $4k - 1$. Hence this equation has no solutions for integers $q \geq 0$.

Case 3. $s > 1$ and $t = 1$.

Since $s > 1$, the right-hand side of (1) is odd, so $q = 0$. Equation (1) reduces to $5 \cdot 3^{r-1} = 2^{s-1} - 1$. Equation (E) yields $s = r + 1$, by reasoning similar to that in

Case 2. Again, the equation above has no solution, since the left-hand side must be greater than the right-hand side.

Thus in each case, the conditions that must be satisfied in order for n to be an LB number lead to a contradiction.

2. The LB numbers < 1000 With these results, hand computation of all the LB numbers less than 1000 is reasonable. Moreover, to do so yields insight into the properties of LB numbers. By definition, an LB number must have at least two digits, and two-digit numbers may not be LB numbers by Theorem 1.7.

A three-digit LB number must have the form $n = 100a + b$, again by Theorem 1.7. In a three-digit number of this form, a must be a single digit. The primes that may divide n will now be investigated. Proposition 1.6 immediately rules out all prime factors of two or more digits.

The next step is to eliminate 7 as a possible divisor. Assume that $7 \in P(n)$. Then $a = 7$ by Proposition 1.4. By writing $n = 7m$, we see that the inequality $101 \leq m \leq 114$ must hold. The only primes that may divide n, and thus m, are 2, 5 and 7, by the remarks following Proposition 1.3. But there are no integers m having only these divisors in the required range.

The situation $3 \in P(n)$ is now examined. By reasoning analogous to that used in the above paragraph, a must be 3, 6, or 9. If $a = 3$, $n = 3m$, where $101 \leq m \leq 133$, and $P(m) \subseteq \{2, 3, 5\}$. An examination of the few values of n arising in this way reveals the LB number 375.

When $a = 6$, $n = 6m$, where $101 \leq m \leq 116$, and $P(m) \subseteq \{2, 3, 5\}$. The LB number 648 results from an examination of the single possibility $m = 108$. Similar reasoning reveals that 972 is the only LB number for which $a = 9$.

The only case remaining is when $P(n) = \{2, 5\}$. In view of Proposition 1.6, the exponent of precisely one of these primes must be 1. This leaves very few cases to be checked, and the LB number 250 is revealed.

TABLE 1 summarizes the information about the LB numbers < 1000. Note that 648 is both an LB number and an LB residue. An examination of the table reveals that 250 and 375 are both multiples of 125, and 648 and 972 are both multiples of 108. This provides some insight into a method of constructing LB numbers, and motivates the following definition.

Let $n_1 = 10^k a_1 + b_1$ be a split of an integer n_1. If there exists an integer r and an LB number $n = 10^k a + b$ such that $n = rn_1$, $a = ra_1$, and $b = rb_1$, then n_1 is called an *LB factor*.

TABLE 1

LB number	Prime factorization	LB residue
2‖50	$2^1 \cdot 5^3$	100
3‖75	$3^1 \cdot 5^3$	225
6‖48	$2^3 \cdot 3^4$	288
9‖72	$2^2 \cdot 3^5$	648

As shown above, the numbers 108 and 125 are LB factors. LB numbers may be built by finding LB factors, and then the appropriate multiple r. This approach is particularly useful in a computer search. The following lemma is immediate.

LEMMA 2.1. *Let* $n_1 = 10^k a_1 + b_1$ *be a split of an integer* n_1, *let* p *be a prime such that* $pb_1 < 10^k$, *and let* $n = pn_1$, $a = pa_1$ *and* $b = pb_1$. *Then*

(1) $n = 10^k a + b$ *is a split of* n.

(2) $E(n) = E(n_1) + 1$, *and*

(3) $E(a) + E(b) = E(a_1) + E(b_1) + 2$.

Thus multiplication by a prime causes the right-hand side of equation (E) to increase by one more than the left-hand side, provided the same split is maintained. This last condition is guaranteed in the lemma by the hypothesis $pb_1 < 10^k$.

An examination of the LB factor $n_1 = 1\|08$ will illustrate the usefulness of the lemma. The equations $P(n_1) = \{2, 3\}$, $P(a_1) \cup P(b_1) = \{2\}$, $E(n_1) = 5$, and $E(a_1) + E(b_1) = 3$ hold. Hence n_1 must be multiplied by two primes in order for equation (E) to be satisfied. To satisfy equation (P), at least one of these primes must be 3. Finally, the product of $b_1 = 8$ and these two primes may not exceed 100. The LB numbers $6 \cdot 108 = 648$ and $9 \cdot 108 = 972$ may be constructed from these conditions.

Let $n = 10^k a + b$ be a split of an integer. The properties that are required in order for n to be an LB factor will be investigated. Some notation will facilitate this. Define

$$D = (P(n) \setminus (P(a) \cup P(b))) \cup ((P(a) \cup P(b)) \setminus P(n))$$

to be the symmetric difference, representing all primes that appear on precisely one side of equation (P). Let d be the cardinality of D, and let $p_1, \dots p_d$ be the primes in D. Assume that n is an LB factor. Then $c = E(n) - (E(a) + E(b) + d)$ must be nonnegative in order that equation (E) be eventually satisfied. The smallest number with the property that its product with n is an LB number is $2^c p_1 p_2 \dots p_d$, and this number times b must be less than 10^k. Conversely, if the conditions above are satisfied, and n is multiplied by $2^c p_1 p_2 \dots p_d$, an LB number results. Therefore the following theorem has been proved.

THEOREM 2.2. *Assume the notation in the previous paragraph. Then* n *is an LB factor if and only if the following conditions hold*:

(1) $c \geq 0$, *and*

(2) $2^c p_1 p_2 \dots p_d b < 10^k$.

LB factors will be essential to upcoming results.

3. There are infinitely many LB numbers That there are infinitely many LB numbers is immediate from the following theorem, which may be easily verified by the reader.

THEOREM 3.1. *Let* $n = 10^k a + b$ *be an LB number. Then* $10n = 10^{k+1} a + 10b$ *is an LB number*.

COROLLARY. *If* r *is an LB residue, then* $10r$ *is an LB residue.*

The converse of Theorem 3.1 is false, since $24\|30$ is an LB number, but 243 does not satisfy equation (P). A partial converse may be given however.

PROPOSITION 3.2. *Let* $10n = 10^{k+1} a + 10b$ *be an LB number with the property that each basal prime is in* $P(n)$ *precisely if it is in* $P(a) \cup P(b)$. *Then* $n = 10^k a + b$ *is an LB number*.

If n is an LB number, then $10n$ cannot be considered to be a "new" LB number. We shall say that an LB number is *primordial* if it is not of the form $10n$ for some LB number n.

It is natural to ask if there are infinitely many primordial LB numbers, and the answer is in the affirmative.

THEOREM 3.3. *There are infinitely many primordial LB numbers.*

In order to prove this result, it will suffice to construct, for every integer $k \geq 2$, an LB factor of the form $10^k a + b$. The following lemma accomplishes this for $a = 1$ and $b = 8$.

LEMMA 3.4. *For every integer $k \geq 2$, $10^k + 8$ is an LB factor.*

Proof. The special case $k = 2$ was considered earlier, so it may be assumed that $k \geq 3$. It is evident that $10^k + 8$ is divisible by 72, so its prime factorization may be written

$$n = 10^k + 8 = 2^3 3^2 p_1 p_2 \dots p_d$$

where the primes 2, 3, $p_1, p_2, \dots p_d$ need not be distinct. Letting $a = 1$, $b = 8$, the equations $E(n) = 5 + d$ and $E(a) + E(b) = 3$ hold. Thus n needs to be multiplied by $d + 2$ primes in order for equation (E) to be satisfied, and the same split must be preserved. The number $m = 2 \cdot 3 p_1 p_2 \dots p_d n$ will be shown to be an LB number. In order to show that the split of n is preserved, the product $(2 \cdot 3 p_1 p_2 \dots p_d) \cdot 8$ must be less than $10^k = n - 8$. This product is $48 p_1 p_2 \dots p_d$, and since $n = 72 p_1 p_2 \dots p_d$, the required inequality holds. Pursuant to the remarks above, equation (E) holds for m, and m was carefully constructed to satisfy equation (P). Hence m is an LB number. To see that m is primordial, note that 5 cannot be in $P(m) = P(n)$. Hence m cannot be of the form $10t$, for some LB number t.

The reader may find it of interest to use a similar argument to show that $10^k + 125$ is an LB factor for every integer $k \geq 3$.

4. A restriction on the size of a prime factor of an LB number The following theorem is a generalization of Proposition 1.5.

THEOREM 4.1. *If n is an LB number with a d digit prime factor p, then n must have at least $2d + 1$ digits.*

Proof. If $d = 1$, then by Proposition 1.5 and Theorem 1.7, n has at least $2d + 1$ digits. So assume $d > 1$. In view of Proposition 1.5, it may be assumed, by way of contradiction, that n has precisely $2d$ digits. The verification of the following facts is indicated in parenthetical remarks:

(1) The split of n is of the form $n = 10^d a + b$. (By Proposition 1.4, p must divide both a and b, and any other value of the exponent would preclude this.)

(2) Aside from p, each prime factor of n has only one digit. (Assume to the contrary such a prime q exists. Then $pq > 10^d$, but is a factor of b, contradicting (1).)

(3) n cannot be divided by a power of p higher than p^3. (p^4 would have to have at least $2d + 1$ digits.)

The LB factor $n_1 = 10^k a_1 + b_1$, where $pn_1 = n$, $pa_1 = a$, and $pb_1 = b$, satisfies the relation

$$E(n_1) = E(a_1) + E(b_1) + 1, \tag{2}$$

by virtue of Lemma 2.1. Moreover, $a_1 < 10$ and $b_1 < 10$, by a consideration of the size of the numbers. The proof now divides into three cases, based on the value of y, the highest power of p that divides n.

Case 1. $y = 1$. In this case, p does not divide n_1, so n_1 may have only one-digit prime factors. When $d = 2$, the individual three-digit numbers n_1 that satisfy the above properties may be examined and eliminated. When $d > 2$, equation (2) may never be satisfied. The details follow, but basically this is because $n_1 > 1000$ and has only one-digit prime factors, so $E(n_1)$ is too large. For if a_1 and b_1 have only the number 2 as prime factors, then so does n_1. But then $E(n_1) \geq 10$, but $E(a_1) + E(b_1) + 1 \leq 7$. If b_1, and hence a_1, has a prime factor of 3, then $E(n_1) \geq 7$, but $E(a_1) + E(b_1) + 1 \leq 5$. Finally, if either 5 or 7 divides b_1, then $E(n_1) \geq 4$, but $E(a_1) + E(b_1) + 1 \leq 3$.

Case 2. $y = 2$. In this case, $n_1 = pc$, p does not divide c, $c < 100$ and

$$E(c) = E(a_1) + E(b_1). \tag{3}$$

A number of properties of c will be listed, with the aim of reducing the possible values of c to just one ($c = 54$.)

c1. Only primes less than 10 may be in $P(c)$.

c2. The product of the primes in $P(c)$ must be less than 10, and these are the only primes that may appear in $P(a_1)$ and $P(b_1)$. (This follows from Proposition 1.3.)

c3. $a_1 b_1 < c$. (Assume to the contrary that $a_1 b_1 \geq c$. Then $pa_1 b_1 \geq pc = 10^k a_1 + b_1$. Thus $pb_1 \geq 10^k + b_1/a_1$. But $pb_1 = b < 10^k$.)

c4. $P(c) = \{2, 3\}$. (For c3 to be satisfied, at least two primes must divide c, and these primes must be 2 and 3 in view of c2.)

c5. $3 \in P(a_1)$; $2, 3 \in P(b_1)$. (Propositions 1.3 and 1.4.)

c6. $E(c) \leq 4$. (Follows from c5, equation (3) and the fact that $a_1 \leq 10$, $b_1 \leq 10$.)

c7. $c = 3^3 \cdot 2^1 = 54$. (In view of equation (3), c3, and c4, the exponent of 3 in c must exceed the sum of the exponents of 3 in a_1 and b_1. By c5, this sum is 2. The exponent of 2 in c must be 1, in order that c4 and $c < 100$ are satisfied. In order to satisfy c3 and c5, it is necessary for $a_1 b_1$ to be 36, and thus for $a_1 = 6$, $b_1 = 6$. The equations defining a_1, b_1, and c yield $10^k \cdot 6 + 6 = 54p$. The right-hand side of the equation is divisible by 9, but the left-hand side is not; this is a contradiction.)

Case 3. $y = 3$. It must be the case that $n = p^3 c$, where $c \geq 2$. Considering the assumption $n < 10^d$, it must be the case that $p \leq 17$, and there are very few values of c possible for each prime. Checking each possibility reveals no LB numbers.

Theorem 4.1 cannot be improved. As will be seen in the next section, there is a seven-digit LB number with a three-digit prime factor. However, the proof, with its heavy reliance on special cases, is quite awkward. The author welcomes efforts to streamline it.

5. Interesting results of a computer search In TABLE 2, all the primordial LB numbers less than 10,000,000 are listed, along with their split, and prime factorization.

The prime 139 appearing in the last entry is quite shocking! However, 139 is a divisor of the LB factor 10008. This helps explain its appearance before any two-digit primes.

The LB factor $n = 63||026250$ may be used to find, for each prime $p \leq 37$, an LB number having p as a factor. It may be readily checked that $P(n) = \{2, 3, 5, 7\}$, $P(a) = \{3, 7\}$, $P(b) = \{2, 3, 5, 7\}$, $E(n) = 11$, $E(a) = 3$, and $E(b) = 7$. Thus n may be multiplied by any prime less than $10^6/26250 > 38$ to obtain an LB number.

TABLE 3 lists all other primes that are factors of LB numbers that are known to the author. The prime 13 is included in the list because it is a divisor of a smaller LB number than that obtained from the LB factor above.

TABLE 2

LB number	prime factorization
2‖50	$2^1 \cdot 5^3$
3‖75	$3^1 \cdot 5^3$
6‖48	$2^3 \cdot 3^4$
9‖72	$2^2 \cdot 3^5$
24‖30	$2^1 \cdot 3^5 \cdot 5^1$
6‖750	$2^1 \cdot 3^3 \cdot 5^3$
9‖375	$3^1 \cdot 5^5$
36‖450	$2^1 \cdot 3^6 \cdot 5^2$
60‖750	$2^1 \cdot 3^5 \cdot 5^3$
84‖672	$2^6 \cdot 3^3 \cdot 7^2$
54‖6750	$2^1 \cdot 3^7 \cdot 5^3$
834‖6672	$2^4 \cdot 3^3 \cdot 139^1$

TABLE 3

prime	LB number
13	26‖406250
41	7749‖27552
89	534‖66750
127	5334‖666750
193	579‖296448
463	5556‖44448

The LB number listed for the prime 13 is the smallest LB number containing a two-digit prime factor. The digits of the LB numbers listed for 89 and 127, along with the aforementioned LB number 546750 form an interesting pattern. It is the case that, for every integer $k \geq 0$, the number $6 \cdot (10^{k+4} + 125)^2/1125$ is an LB number, and its digits have the following form: five, k threes, four, $k+1$ sixes, seven, five, zero. The intriguing LB number for 463 is the second term of a more subtle pattern. For every integer $k \geq 0$, the number $(10^{3k+2} + 8)^2/18$ is an LB number whose digits have the pattern $3k$ fives, six, $3k+1$ fours, eight. The first LB number fitting this pattern is, of course, 648. When m does not have the form $3k+2$, $(10^m + 8)^2/18$ is not an LB number. A third pattern is formed by the LB numbers $(10^{k+3} + 8)/12$, for each integer $k \geq 0$, consisting of the digits eight, k threes, four, $k+1$ sixes, seven, two. The reader may find it an interesting challenge to verify these facts.

6. Open questions Classes of integers such as twin primes and perfect numbers are interesting in part because of unresolved questions about them. In view of Theorem 3.3, the analogue to the most intriguing question about these numbers is answered for LB numbers. Still, there are many questions to be asked.

Question 1. Can every prime be a factor of an LB number? The results in Section 6, along with the comments in Question 3 below, show that every prime ≤ 43 is such a factor.

Question 2. Are there LB factors for each prime p analogous to the relation of 63‖026250 and 37? That is, can an LB factor n be found such that, for every prime $q \leq p$, nq is an LB number? A positive answer to question 2 would be, a fortiori, a positive answer to question 1.

Question 3. What combination of primes may be factors of LB numbers? None of the LB numbers listed in the previous sections have more than one prime exceeding 10 as a factor. However the LB factor 1,000,008 has among its factors 17, 19, and 43, so such LB numbers do exist.

Question 4. What combinations of primes may be excluded as factors of LB numbers? Every LB number known to the author has at least two of the primes 2, 3, and 5 as factors. Is it necessarily the case that a basal prime be a factor of an LB number?

Question 5. Fix an integer $k \geq 2$. Is there an upper limit on the size of a primordial LB number having at most k distinct prime factors? From earlier results, it appears that 9375 may be the largest such number for $k = 2$.

Question 6. The number 648 is both a primordial LB number and an LB residue. The primordial LB number $54\|6750$ has, as its LB residue, the nonprimordial LB number 364500. Are there any other such numbers?

Question 7. Is it possible that a number can be an LB number when split in two different ways?

Question 8. Find other digital patterns similar to those in the last paragraph of Section 6. Are there infinitely many such patterns?

Question 9. Change the definition of the split of a number to allow 10 to be replaced by any integer $s \geq 2$. In effect, LB numbers in base s are now being considered. Much of the theory of LB numbers is preserved under change of base. For example, Propositions 1.1 through 1.6, appropriately modified, are true. The following may be verified routinely from the definition of LB numbers.

PROPOSITION 7.1. *If $n = s^k a + b$ is an LB number in base s, then n is an LB number in base s^k.*

It is easy to see from Proposition 7.1 that Theorems 1.7 and 4.1 fail to hold in base 10^k, where $k > 1$. However, Theorem 3.3 is still satisfied. What happens in other bases? Are there any bases for which Theorem 1.7 is true but Theorem 4.1 is not? Are there any bases in which Theorem 3.3 fails? Are there any bases with no LB numbers? Incidentally, $54_{(10)} = 110\|110_{(2)} = 6\|6_{(8)}$ is an LB number in bases 2 and 8. However, the smallest integer that is an LB number in any base is the decimal number 50, which is an LB number in base 20. (In general, if p and q are primes with $p + 1 < q$, then pq^2 is a base $q^2 - q$ LB number.)

Question 10. Split the digits of an integer n into r parts, $a_1, \dots, a_r$. Then n is an *r-LB number* if $P(n) = \bigcup_{i=1}^{r} P(a_i)$ and $E(n) = \sum_{i=1}^{r} E(a_i)$. Thus an LB number is a 2-LB number. What can be said about r-LB numbers for $r > 2$? The theory is likely to be intractable; among other things, the analogues to Propositions 1.3 and 1.4 are false. Hand calculation reveals that the only 3-LB numbers < 1000 are 378 and 648.

The title of this article can now be justified. The number 648 has the following properties:

1. 648 is a primordial LB number.
2. 648 is the LB residue of a primordial LB number.
3. 648 begins a sequence of LB numbers forming a digital pattern.
4. 648 is an r-LB number for every possible value of r.

This is truly remarkable!

Question 11. Do any other integers satisfy the four properties listed above?

PROBLEMS

LOREN C. LARSON, *editor*
St. Olaf College

GEORGE GILBERT, *associate editor*
Texas Christian University

Proposals

To be considered for publication, solutions should be received by July 1, 1993.

1413. *Proposed by Victor Klee, University of Washington, Seattle, Washington.*

For each subset X of $\mathbf{R}_3$, let $\mathrm{Con}_2(X)$ denote the union of X with all line segments joining pairs of points of X, and let $\mathrm{Aff}_2(X)$ denote the union of X with all lines determined by two points of X. Now suppose that X consists of the four vertices of a tetrahedron. Then $\mathrm{Con}_2(X)$ is the union of the six edges of the tetrahedron, and $\mathrm{Aff}_2(X)$ is the union of the six lines that are extensions of those edges. Also, $\mathrm{Con}_2(\mathrm{Con}_2(X))$ is the entire tetrahedron. Give a geometric description of the set $\mathrm{Aff}_2(\mathrm{Aff}_2(X))$.

1414. *Proposed by Stan Wagon, Macalester College, St. Paul, Minnesota.*

Suppose a square whose diagonal's length is $5/9$ of an inch is thrown randomly (with uniform distribution) onto a flat surface ruled with parallel lines one inch apart. What is the probability that the square will touch one of the lines?

1415. *Proposed by John Duncan and Mihalis Maliakas, University of Arkansas, Fayetteville, Arkansas.*

Let m and n be integers satisfying $m \geq 2n - 1 \geq 3$, and let $A(m, n)$ denote the $n \times n$ matrix whose (i, j) entry is

$$\binom{m - j + 1}{2n - 2i} + \binom{m + j - 2n}{2n - 2i}.$$

Evaluate the determinant of $A(m, n)$.

ASSISTANT EDITORS: CLIFTON CORZAT, BRUCE HANSON, RICHARD KLEBER, KAY SMITH, *and* THEODORE VESSEY, *St. Olaf College and* MARK KRUSEMEYER, *Carleton College. We invite readers to submit problems believed to be new and appealing to students and teachers of advanced undergraduate mathematics. Proposals should be accompanied by solutions, if at all possible, and by any other information that will assist the editors and referees. A problem submitted as a Quickie should have an unexpected, succinct solution. An asterisk (*) next to a problem number indicates that neither the proposer nor the editors supplied a solution.*

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

Solutions and new proposals should be mailed in duplicate to Loren Larson, Department of Mathematics, St. Olaf College, 1520 St. Olaf Ave., Northfield, MN 55057-1098 or mailed electronically via fax: (507) 663-3549 or e-mail: larson@stolaf.edu.

1416. *Proposed by Stephen Wainger, University of Wisconsin, Madison, Wisconsin, and Jim Wright, Texas Christian University, Fort Worth, Texas.*

Let $(a_k)_{k=1}^{\infty}$ be a sequence of positive numbers, and consider the following two conditions.

(I) There is a constant C_1 such that

$$\sum_{k=1}^{n} a_k \leq C_1 a_n \quad \text{for all } n \geq 1.$$

(II) There is a constant C_2 such that

$$\sum_{k=n}^{\infty} \frac{1}{a_k} \leq C_2 \frac{1}{a_n} \quad \text{for all } n \geq 1.$$

Which of these conditions (if either) implies the other?

1417. *Proposed by C. Kenneth Fan, Massachusetts Institute of Technology, Cambridge, Massachusetts.*

Let N billiard balls (of various positive radii and masses) roll about a frictionless, rectangular billiard table. Assume the collisions are elastic. Show that there will either be no collisions at all, or infinitely many.

Quickies

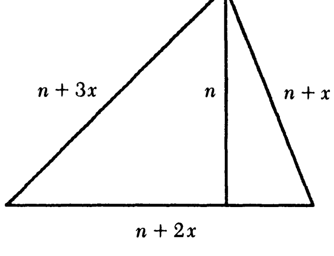
Answers to the Quickies are on page 64.

Q800. *Proposed by Bjorn Poonen, University of California, Berkeley, California.*

Suppose $P(x) \in \mathbf{Z}[x]$ and $P(a)P(b) = -(a-b)^2$ for some distinct $a, b \in \mathbf{Z}$. Prove $P(a) + P(b) = 0$.

Q801. *Proposed by John Bonomo, Denison University, Granville, Ohio.*

How many triangles have the form shown below, where n is a positive integer, and x is a real number, $0 < x \leq 1$?



Solutions

Stones in Cups. **February 1992**

1388. *Proposed by Barry Cipra, Northfield, Minnesota.*

Suppose that n cups are arranged in a circle and that k stones are placed in each cup. Place your hand by one of the cups and carry out the following operation: Pick up all the stones in that cup and, moving clockwise, drop them one at a time into the succeeding cups, leaving your hand by the cup where you dropped the last stone.

a. Prove that by iterating this procedure (always picking up the stones in the cup where you dropped the last stone), you will eventually wind up with all kn stones in the *original* cup.

b*. Let a_{kn} denote the number of steps until the situation described in part a is obtained. The first few values are given in the following table:

1	4	15	12	75
1	6	21	164	115
1	12	45	164	260
1	8	132	124	3825
1	6	48	1580	1966

Find a formula for a_{kn}.

Solution to (a) by Kay P. Litchfield, Farmington Utah.

We use the term *configuration* to refer to the number of stones in each cup and the position of the (empty) hand. The number of configurations (given k and n) is finite. We use the term *move* to refer to the redistribution of one cup's stones.

In the original configuration, and after every following move, the hand is at a cup containing one or more stones, so another (uniquely determined) move may always be made. Repeated moves will, at least eventually, cycle through a sequence of configurations.

The inverse of a move is accomplished by picking up from the currently selected cup, and then from the other cups, moving counterclockwise, one stone each, until an empty cup is found. All stones held are dropped into that cup. The inverse move is unique. Thus, the repeated sequence of configurations will include the original configuration.

This inverse move applied to the original configuration puts all the stones into the original cup, and will therefore be reached.

Solution to (b), for the case of two cups, by David Callan, University of Wisconsin, Madison, Wisconsin.

Let m denote the total number of stones (not necessarily even), and label the configuration having y stones in cup 1 with $2y-\varepsilon$, where $\varepsilon = 1$ or 0 according as the hand is located at cup 1 or not. Then it is easy to check that the *inverse* move, applied to each element in the set of all configurations, produces the permutation given by

$$T=\begin{pmatrix} 0 & 1 & 2 & \cdots & m-1 & m & m+1 & m+2 & \cdots & 2m-1 \\ 1 & 3 & 5 & \cdots & 2m-1 & 0 & 2 & 4 & \cdots & 2m-2 \end{pmatrix};$$

that is, Tx is just the integer in $[0, 2m-1]$ satisfying $Tx \equiv 2x+1 \pmod{2m+1}$. An easy induction yields $T^i x \equiv 2^i x + 2^i - 1 \pmod{2m+1}$.

Let r denote the order of 2 in the group of units $\mathbf{Z}_{2m+1}^{*}$ of the ring Z_{2m+1}; that is, r is minimal positive such that $2m+1$ divides $2^r - 1$. It follows that $T^r x \equiv x \pmod{2m+1}$, hence every cycle under T has length dividing r. In particular, for $x = 0$, this cycle has length precisely r.

In the notation of the proposed problem, k is the initial number of stones per cup, so a_{k2} is the order of 2 in $\mathbf{Z}_{4k+1}^{*}$.

Part a also solved by David Callan, Con Amore Problem Group (Denmark), Jiro Fukuta (Japan), Robert High, Kiran S. Kedlaya (student), and the proposer.

A Binomial Sum **February 1992**

1389. *Proposed by R. Bruce Richter, Carleton University, Ottawa, Ontario, Canada.*

Evaluate

$$\sum_{j=0}^{n} \binom{2n}{2j} (-3)^j.$$

I. *Solution by University of Wyoming Problem Circle, University of Wyoming, Laramie, Wyoming.*

By the binomial theorem,

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

Taking $x = \sqrt{3}\, i$ we have

$$\begin{aligned}\sum_{j=0}^{n} \binom{2n}{2j} (-3)^j &= \frac{1}{2}\left((1+\sqrt{3}\, i)^{2n} + (1-\sqrt{3}\, i)^{2n}\right)\\ &= \frac{1}{2}\left((2e^{\pi i/3})^{2n} + (2e^{-\pi i/3})^{2n}\right)\\ &= 2^{2n-1}\left(e^{2n\pi i/3} + e^{-2n\pi i/3}\right)\\ &= 2^{2n} \cos\frac{2n\pi}{3}.\end{aligned}$$

A straightforward generalization of this method shows that for any $a > 0$,

$$\sum_{j=0}^{n} \binom{2n}{2j} (-a)^j = (1+a)^n \cos\left(2n \arctan \sqrt{a}\,\right).$$

II. *Solution by Iwan Praton and Prasad Venugopal (student), University of Massachusetts, Amherst, Massachusetts.*

The answer is 2^{2n} if n is divisible by 3 and -2^{2n-1} otherwise. Such sums yield readily to the Snake Oil method described in Wilf, Herbert, *Generatingfunctionology*, Section 4.3, Academic Press, 1990. We will use the method to evaluate

$$a_m = \sum_{j \geq 0} \binom{m}{2j} (-3)^j$$

($m \geq 0$), where we use the convention $\binom{s}{t} = 0$ if $t > s$. We need the identity $\sum_{s \geq 0} \binom{s}{t} x^s = x^t/(1-x)^{t+1}$ ($t \geq 0$), which can be derived by repeatedly differentiating the geometric series $\sum_{s \geq 0} x^s = (1-x)^{-1}$.

Let $f(x)=\Sigma_m a_m x^m$ be the generating function of a_m. Then

$$f(x)=\sum_{j\geq 0}(-3)^j\sum_{m\geq 0}\binom{m}{2j}x^m=\sum_{j\geq 0}\frac{(-3)^j x^{2j}}{(1-x)^{2j+1}}$$
$$=\frac{1}{1-x}\sum_{j\geq 0}\left(\frac{-3x^2}{(1-x)^2}\right)^j=\frac{1-x}{1-2x+4x^2}$$

after summing the geometric series and simplifying. Now let $y=2x$ and let $\alpha_{\pm}$ be the two roots of $1-y+y^2=0$, i.e., $\alpha_{\pm}=(1\pm i\sqrt{3})/2=e^{\pm\pi i/3}$. Then

$$(1-2x+4x^2)^{-1}=(1-y+y^2)^{-1}=\frac{1}{\alpha_+-\alpha_-}\left(\frac{\alpha_+}{1-\alpha_+y}-\frac{\alpha_-}{1-\alpha_-y}\right)$$
$$=\frac{1}{i\sqrt{3}}\sum_{m\geq 0}\left(\alpha_+^{m+1}-\alpha_-^{m+1}\right)y^m=\frac{2}{\sqrt{3}}\sum_{m\geq 0}\sin\frac{(m+1)\pi}{3}2^m x^m.$$

It is now easy to get the power series expansion of $f(x)=(1-x)/(1-2x+4x^2)$. We get

$$f(x)=\sum_{m\geq 0}\frac{2^m}{\sqrt{3}}\left(2\sin\frac{(m+1)\pi}{3}-\sin\frac{m\pi}{3}\right)x^m.$$

Evaluating this for various values of m gives us the following: $a_m=2^m$ if $m\equiv 0,3$ modulo 6, $a_m=2^{m-1}$ if $m\equiv 1,5$ modulo 6, and $a_m=-2^{m-1}$ if $m\equiv 2,4$ modulo 6. In particular, $m=2n$ gives us the result claimed above.

III. *Comment by H. M. Srivastava, University of Victoria, Victoria, British Columbia, Canada.*

More generally, for any complex number λ and positive real number x,

$$\sum_{j=0}^{\infty}\binom{2\lambda}{2j}(-x)^j=(1+x)^{\lambda}\cos(2\lambda\arctan\sqrt{x}).$$

To show this, rewrite the left-side as a hypergeometric function: $F(-\lambda,\lambda+\frac{1}{2};\frac{1}{2};-x)$, and apply a known formula (see Prudnikov, Bryčkov, Maričev, *Integrals and Series*, Volume 2: Special Functions, Entry 7.3.3.1),

$$F(a,a+\tfrac{1}{2};\tfrac{1}{2};-z)=(1+z)^{-a}\cos(2a\arctan\sqrt{z}).$$

IV. *Comment by Volker Strehl, University of Erlangen, Germany, and Peter Paule, RISC, University of Linz, Austria.*

Denote the desired sum by s_n. Using the method of D. Zeilberger (see, e.g.: The method of creative telescoping, *Journal of Symbolic Computation* 11/3, 1991, pp. 195–204) a computer directly finds that the sequence $(s_n)_{n\geq 0}$ satisfies the second order recurrence equation

$$s_{n+2}+4s_{n+1}+16s_n=0.$$

It even provides a rational function (in the variables n and j) as a proof certificate, from which a verification is possible using routine (but tedious, if done by hand) rational arithmetic. Using the computer algebra system "Axiom" (NAG) and a Zeilberger-program written in its programming language, it took an IBM RS/6000-350 about 20 seconds to solve the problem.

Also solved by Nirmal Devi Aggarwal, M. Reza Akhlaghi, Michael Andreoli, Christos Athanasiadis (student), Seung-Jin Bang (Republic of Korea), Brian D. Beasley, Nirdosh Bhatnagar, J. C. Binz (Switzerland), D. M. Bloom, Paul Bracken and F. M. Carlton (Canada), David Callan, Joseph E. Chance, Chico Problem Group, Con Amore Problem Group (Denmark), Fred Dodd, David Doster, Robert L. Doucette, Harry D'Souza, Ragnar Dybvik (Norway), Russell Euler, D. Flannery (Ireland), Jiro Fukuta (Japan), Marty Getz, Stewart Gleason, Michael Golomb, Ralph P. Grimaldi, Jerry Grossman, W. J. Hardell, K. P. Hart (The Netherlands), Russell Jay Hendel, Ole Jørsboe (Denmark), Hans Kappus (Switzerland), Kiran S. Kedlaya (student), H. K. Krishnapriyan, Albert Kurz (student), Y. H. Harris Kwong, Kee-Wai Lau (Hong Kong), Rein Leentfaar (The Netherlands), Gesing Leung (Hong Kong), Gan Wee Liang (student, Singapore), Carl Libis, Peter W. Lindstrom, Véronique Lizan (France), Graham Lord, Nick Lord (England), David E. Manes, Helen M. Marston, Reiner Martin (student), Lisa McShine (Trinidad), Allen R. Miller, Andreas Müller (France), Kandasamy Muthuvel, Roger B. Nelsen, István Nemes (Austria), Gillian Nonay (Canada), Edward D. Onstott, P. J. Pedler (Australia), Kulapant Pimsamarn (student), F. C. Rembis, Thomas Schira (Germany), Heinz-Jürgen Seiffert (Germany), Louis W. Shapiro, Shreveport Problem Group, Volker Strehl (Germany) and Peter Paule (Austria) (three solutions), John S. Sumner, James Swenson, Gerald Thompson, William F. Trench, Trinity University Problem Group, Michael Vowe (Switzerland), Julius Vogel, Robert J. Wagner, Jack V. Wales, Edward T. H. Wang (Canada), William P. Wardlaw, William V. Webb, Yan Loi Wong (Singapore), Zhang Zaiming (China), and the proposer. There was one unidentified solution.

Products of Fibonacci Numbers **February 1992**

1390. *Proposed by Joseph F. Stephany, Webster Research Center, Webster, New York.*

Prove that no Fibonacci number can be factored into a product of two smaller Fibonacci numbers, each greater than 1.

I. *Solution by Edward D. Onstott, Hawthorne, California.*

Defining $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n > 1$, an easy induction shows that

$$F_n = F_{k-1}F_{n-k+2} + F_{k-2}F_{n-k+1}, \quad 2 \leq k \leq n.$$

Suppose $F_n = F_m F_k$ for $m, k \geq 3$. Then

$$F_m = \frac{F_n}{F_k} = \frac{F_{k-1}F_{n-k+2} + F_{k-2}F_{n-k+1}}{F_k}$$
$$= \left(\frac{F_{k-1}}{F_{k-1} + F_{k-2}}\right)F_{n-k+2} + \left(\frac{F_{k-2}}{F_{k-1} + F_{k-2}}\right)F_{n-k+1}.$$

The right side is a weighted mean of consecutive Fibonacci numbers. Thus we have $F_{n-k+1} < F_m < F_{n-k+2}$, a contradiction.

II. *Solution by Robert High, New York, New York.*

From $F_{m+k} = F_k F_{m+1} + F_{k-1}F_m$ it follows that

$$F_m F_k < F_{m+k}, \text{ if } F_m, F_k > 1. \qquad (*)$$

Now suppose that $F_n = F_m F_k$, F_m, $F_k > 1$. It is well known that F_m divides F_n if and only if m divides n. Thus, both m and k divide n. Hence, either $m = k = n$, which is absurd, or $n \geq m + k$, which contradicts $(*)$. This completes the proof.

III. *Solution by Fred Dodd, University of South Alabama, Mobile, Alabama.*

We prove the following stronger result: If $n \neq 6, 12$, then F_n cannot be factored into a product of two or more Fibonacci numbers greater than 1; F_6 has the single factorization $F_6 = F_3^3$ and F_{12} has the two factorizations $F_{12} = F_3^4 \cdot F_4^2 = F_3 \cdot F_6 \cdot F_4^2$.

The above result is an immediate consequence of the well-known primitive prime divisor property of the Fibonacci numbers. A prime divisor p of F_n is said to be a primitive prime divisor of F_n if p does not divide F_m for all $m < n$. The primitive prime divisor property states that F_n has a primitive prime divisor for all $n \neq 1, 2, 6, 12$. (See the note below.) Thus, if F_n is a product of two or more Fibonacci numbers greater than 1, then $n = 6$ or $n = 12$. It is trivial to check that the given factorizations of F_6 and F_{12} are the only factorizations.

Note. The Fibonacci numbers are a special case ($\alpha + \beta = 1$, $\alpha\beta = -1$) of the numbers $D_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ that were extensively studied in the famous work by Carmichael [1]. The primitive prime divisor property of the Fibonacci numbers follows from Theorem 23 in that work. A sketch of many of these results appears in Chapter IV of [3]. An excellent account of the early history of the numbers D_n can be found in Chapters 16 and 17 of Dickson [2].

1. R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Annals of Mathematics*, (2) 15 (1913/1914), pp. 30–70.
2. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Carnegie Institute of Washington, Washington, DC 1920; reprinted, Chelsea Publishing Co., New York, 1952.
3. Paulo Ribenboim, *The Little Book of Big Primes*, Springer-Verlag, New York, 1991.

Also solved by Alma College Problem Solving Group, Peter G. Anderson (two solutions), Armstrong State College Problems Group, Christos Athanasiadis (student), S. F. Barger, D. M. Bloom (two solutions), J. L. Brown, Jr., David Callan, Centre College Problem Solving Group, William Y. C. Chen and Edward T. H. Wang (Canada), Con Amore Problem Group (Denmark), Miguel A. Diaz-Quiñones (Spain), Jiro Fukuta (Japan), Michael Golomb, Ralph P. Grimaldi, Bryan C. Hathorn (student), Russell Jay Hendel, R. Daniel Hurwitz, Albert Kurz (student), Kee-Wai Lau (Hong King), Gesing Leung (Hong Kong), Kathleen E. Lewis, Gan Wee Liang (student, Singapore), Peter W. Lindstrom, Helen M. Marston, Ona J. McBride (student) and David L. Wheeler (student), Jean-Marie Monier (France), Kandasamy Muthuvel, Roger B. Nelsen, Richelle Ondrick (student), P. J. Pedler (Australia), F. C. Rembis, James S. Robertson and John P. Robertson (four solutions!), Heinz-Jürgen Seiffert (Germany), John S. Sumner, William P. Wardlaw, and the proposer.

A Maclaurin Series **February 1992**

1391. *Proposed by Howard Morris, Chatsworth, California.*

Show that

$$1 + xe^{x^2/4}\int_0^{x/2} e^{-t^2}\,dt = \sum_{n=0}^{\infty} \frac{n!}{(2n)!}x^{2n}.$$

I. *Solution by Tom M. Apostol, California Institute of Technology, Pasadena, California.*

By replacing x by $2x$, cancelling 1 and dividing by $2x$, we find that the identity reduces to

$$e^{x^2}\int_0^{x} e^{-t^2}\,dt = \sum_{n=1}^{\infty} \frac{n!}{(2n)!}(2x)^{2n-1}.$$

The function on the left is the unique solution of the first-order linear differential equation

$$y' - 2xy = 1$$

with $y(0) = 0$. This differential equation has a power series solution of the form

$$y = \sum_{n=0}^{\infty} a_n x^n$$

with $a_0 = 0$ and $a_1 = 1$. Substituting this series into the differential equation we find that the coefficients satisfy the recursion relation

$$a_{n+1}=\frac{2}{n+1}a_{n-1}$$

for all $n \geq 1$. Because $a_0 = 0$ and $a_1 = 1$ this implies $a_{2n} = 0$ and

$$a_{2n-1}=\frac{n!}{(2n)!}2^{2n-1}$$

for all $n \geq 1$, and we obtain the required identity.

II. *Robert J. Wagner, Muhlenberg College, Allentown, Pennsylvania.*

It is easily shown that each side of the proposed identity is a solution of the initial value problem

$$2y - xy' - 2y = 0,\ y(0) = 1,\ y'(0) = 0.$$

Since the coefficients of the differential equation are continuous on **R** and the coefficient of y'' never vanishes, the solution must be unique. This proves the proposed identity.

Also solved by Betty Arnold, Armstrong State College Problems Group, Christos Athanasiadis (student), Seung-Jin Bang (Republic of Korea), Nirdosh Bhatnagar, J. C. Binz (Switzerland), Paul Bracken (Canada), David Callan, Joseph E. Chance, William Y. C. Chen and Edward T. H. Wang (Canada), Con Amore Problem Group (Denmark), E. Coplakova and K. P. Hart (The Netherlands), Jesse I. Deutsch, A. R. DiDonato, David Doster, Robert L. Doucette, Larry Eifler, Russell Euler (two solutions), D. Flannery (Ireland), Stewart Gleason, Michael Golomb, Wagala P. Gwanyama, W. J. Hardell, James C. Hickman, Paul Irwin, Ole Jørsboe (Denmark), Hans Kappus (Switzerland), Kiran S. Kedlaya (student), H. K. Krishnapriyan, Albert Kurz (student), Y. H. Harris Kwong, Kee-Wai Lau (Hong Kong), Gan Wee Liang (student, Singapore), Peter W. Lindstrom, Véronique Lizan (France), Nick Lord (England), Nicole R. McGuire, Kim McInturff, Armel Mercier (Canada), Andreas Müller (France), Kandasamy Muthuvel, Roger B. Nelsen (two solutions), Kulapant Pimsamarn (student), Lennart Råde (Sweden), Hassan Saffari, Thomas Schira (Germany), Arthur L. Schoenstadt, Heinz-Jürgen Seiffert (Germany), M. A. Shayib, Shreveport Problem Group, H. M. Srivastava (Canada), John S. Sumner, Michael Tehranchi, Gerald Thompson and Chris Sligar, Nora S. Thornber, William F. Trench, Michael Vowe (Switzerland, two solutions), William V. Webb, Joseph Wiener, University of Wyoming Problem Circle, Donald F. Winter (two solutions), Zhang Zaiming (China), and the proposer. There was one unidentified solution.

Other solutions were based on the calculus of finite differences, hypergeometric function identities, and identities of the error function erf$(x/2)$, The Mathematica computer program reduced the problem to one involving known properties of the gamma function.

Sums of Fourth Powers of Binomial Coefficients **February 1992**

1392. *Proposed by George Andrews, Pennsylvania State University, University Park, Pennsylvania.*

Prove that for any prime p in the interval $(n, 4n/3]$, p divides

$$\sum_{j=0}^{n}\binom{n}{j}^4.$$

Solution by Ira Gessel, Brandeis University, Waltham, Massachusetts.

We prove more generally that for any positive integer m, if

$$n < p < 1 + (2m/2m-1)n,$$

then p divides $\sum_{j=0}^{n}\binom{n}{j}^{2m}$.

Let n and t be positive integers and suppose that $p = n + t$ is a prime. Then for $j < p$,

$$\binom{n}{j}=\binom{p-t}{j}\equiv\binom{-t}{j}\ (\text{mod } p),$$

since $j!$ is not divisible by p. Thus

$$\sum_{j=0}^{n}\binom{n}{j}^{2m} \equiv \sum_{n=0}^{n}\binom{-t}{j}^{2m} = \sum_{j=0}^{n}\binom{t+j-1}{t-1}^{2m}$$
$$= \sum_{k=t-1}^{p-1}\binom{k}{t-1}^{2m} = \sum_{k=0}^{p-1}\binom{k}{t-1}^{2m} \pmod{p}. \qquad (*)$$

It is well known that $\Sigma_{k=0}^{p-1}k^r$ is divisible by p for $r = 0, 1, \ldots, p-2$. (This follows for $r > 0$ from the fact that multiplying the sum by i^r for any i not divisible by p permutes the summands modulo p.) Since $(t-1)!$ is not divisible by p, $\binom{k}{t-1}^{2m}$ is a polynomial in k of degree $2m(t-1)$ with coefficients whose denominators are not divisible by p. Therefore the sum $(*)$ is divisible by p as long as $2m(t-1) < p-1$, and this is easily seen to be equivalent to the inequality on n, m, and p stated above.

Also solved by David Callan, Con Amore Problem Group (Denmark), Albert Kurz (student), Peter W. Lindstrom, Frank Schmidt, Volker Strehl (Germany), John S. Sumner and Kevin L. Dove, and the proposer.

Answers

Solutions to the Quickies on page 57.

A800. Since $a-b$ divides $P(a)-P(b)$, the roots $P(a)/(a-b)$ and $-P(b)/(a-b)$ of $x^2 - [(P(a)-P(b))/(a-b)]x + 1$ are integers with product 1, by the rational root theorem. Thus $P(a)/(a-b) = -P(b)/(a-b) = \pm 1$, so $P(a) + P(b) = 0$.

A801. The area of a triangle with sides a, b, and c is given by Heron's formula $\sqrt{s(s-a)(s-b)(s-c)}$ where $s = (a+b+c)/2$. Using the substitutions $a = n + x$, $b = n + 2x$, and $c = n + 3x$, and, setting Heron's formula equal to the more traditional formula for the area of a triangle, we have

$$\sqrt{\frac{3n+6x}{2}\cdot\frac{n+4x}{2}\cdot\frac{n+2x}{2}\cdot\frac{n}{2}} = \frac{n(n+2x)}{2}$$
$$\frac{3(n+2x)(n+4x)(n+2x)n}{16} = \frac{n^2(n+2x)^2}{4}$$
$$\frac{3(n+4x)}{16} = \frac{n}{4}$$
$$12x = n.$$

Since $0 < x \le 1$ and n is a positive integer, there are exactly 12 triangles of the required type, namely $(x, n) = (1/12, 1), (2/12, 2), \ldots, (1, 12)$.

Comments

1374. (Solution, June 1992) *Sherman Stein*, *University of California*, *Davis*, writes that this problem has a long history; one reference is by Sherman Stein, "Tiling, packing, and covering by clusters," *Rocky Mountain Journal of Mathematics*, 16 (1980), pp. 277–321; especially, pp. 289ff and pp. 318–319. There remain many unsolved problems in this area.

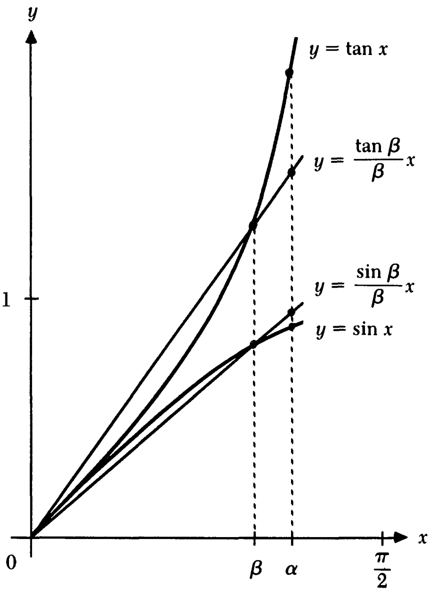
1375. *Brian D. Beasley*'s name should be listed among the solvers of problem 1375 rather than among the solvers of problem 1373.

Q791. *Murray Klamkin*, *University of Alberta*, *Canada*, points out that this problem, generalizations, and the continuous analogues, have appeared in the following notes.

1. Murray S. Klamkin, A probability of more heads, this MAGAZINE, 44 (1971), pp. 146–149.
2. Murray S. Klamkin, Symmetry in probability distributions, this MAGAZINE, 61 (1988) pp. 193–194.

Proof without Words: Aristarchus' Inequalities

$$0<\beta<\alpha<\frac{\pi}{2} \Rightarrow \frac{\sin\alpha}{\sin\beta}<\frac{\alpha}{\beta}<\frac{\tan\alpha}{\tan\beta}$$



$$\sin\alpha < \frac{\sin\beta}{\beta}\alpha$$

$$\frac{\tan\beta}{\beta}\alpha < \tan\alpha$$

$$\therefore \frac{\sin\alpha}{\sin\beta}<\frac{\alpha}{\beta}<\frac{\tan\alpha}{\tan\beta}$$

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

Comments

1374. (Solution, June 1992) *Sherman Stein, University of California, Davis*, writes that this problem has a long history; one reference is by Sherman Stein, "Tiling, packing, and covering by clusters," *Rocky Mountain Journal of Mathematics*, 16 (1980), pp. 277–321; especially, pp. 289ff and pp. 318–319. There remain many unsolved problems in this area.

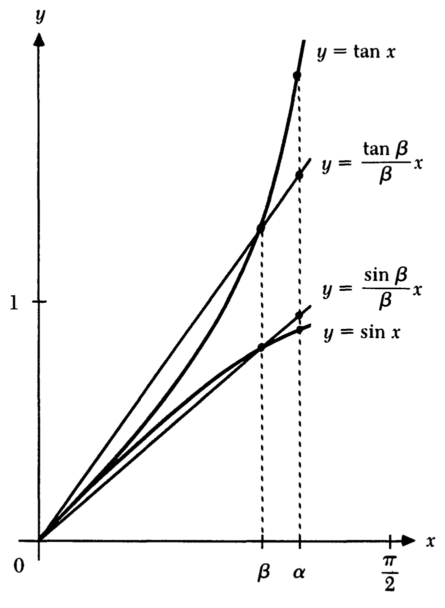
1375. *Brian D. Beasley*'s name should be listed among the solvers of problem 1375 rather than among the solvers of problem 1373.

Q791. *Murray Klamkin, University of Alberta, Canada*, points out that this problem, generalizations, and the continuous analogues, have appeared in the following notes.

1. Murray S. Klamkin, A probability of more heads, this MAGAZINE, 44 (1971), pp. 146–149.
2. Murray S. Klamkin, Symmetry in probability distributions, this MAGAZINE, 61 (1988) pp. 193–194.

Proof without Words: Aristarchus' Inequalities

$$0 < \beta < \alpha < \frac{\pi}{2} \Rightarrow \frac{\sin\alpha}{\sin\beta} < \frac{\alpha}{\beta} < \frac{\tan\alpha}{\tan\beta}$$



$$\sin\alpha < \frac{\sin\beta}{\beta}\alpha$$

$$\frac{\tan\beta}{\beta}\alpha < \tan\alpha$$

$$\therefore \frac{\sin\alpha}{\sin\beta} < \frac{\alpha}{\beta} < \frac{\tan\alpha}{\tan\beta}$$

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

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 the mathematics literature. Readers are invited to suggest items for review to the editors.

CORRECTION. Santo Diano, teacher in the Philadelphia School District, advises that a misprint occurred in Vol. 55, No. 4 (October 1992), p. 275, line −7. The correct value of $\sin 10^{22}$, to nine decimal places, in fact is $-0.852200849\ldots$.

Dudley, Underwood, *Mathematical Cranks*, MAA, 1992; x + 372 pp, $25 (P). ISBN 0-88385-507-0

Have you ever had to deal with a mathematical crank, a person who claims to have done something impossible (trisect the angle) or problematical (a one-page proof of the Four-Color Theorem), or who is overwhelmed by the importance of particular mathematical concepts (the golden ratio) or discoveries (Gödel's Theorem)? Now you can have the complete experience—vicariously—of dealing with the entire range of cranks, without having any dwell on your doorstep, put their foot in your door, or fill up your mailbox. This book is a typology of the breed, with practical advice (see especially pp. 101, 117–118, and 346–347), some learned the hard way. Dudley (an Associate Editor of this MAGAZINE for the past 15 years) writes with wry wit but also with sympathy for the human failings of circle-squarers, trisectors, and "fermatists": "[C]ranks aren't nuts, they're just people who have a blind spot in one direction."

Barrow, John D., *Pi in the Sky: Counting, Thinking, and Being*, Oxford U Pr, 1992; xii + 317 pp, $35. ISBN 0-19-835956-8. Begley, Sharon, Math has π on its face, *Newsweek* (30 November 1992) 73.

You probably won't read this book, and neither will your friends and neighbors; but because of the article in *Newsweek*, they are likely to ask your opinion of it. "The foundations of mathematics have serious flaws. And that may imperil all the sciences." So reads the subhead for the *Newsweek* article, paralleling the tone of the first sentence of Barrow's book: "A mystery lies beneath the magic carpet of science, something that scientists have not been telling, something too shocking to mention ...: that at the root of the success of twentieth century science there lies a deeply 'religious' belief—a belief in an unseen and perfect transcendental world that controls us .... " After that kind of billing, you would expect a nemesis out of *Star Trek* and humanoid co-conspirators. But what Barrow is referring to (of course!) is *mathematical platonism*, that secret mindset of mathematicians that is an ever-lurking threat to the foundations of civilization. Barrow devotes more than a quarter of the book to a history of counting (owing much to Abraham Seidenberg), apparently to establish that counting is concrete in all societies, does not entail an "abstract notion of number," and does not provide convincing evidence that the world is "intrinsically mathematical." The other chapters debunk in turn formalism, inventionism, intuitionism, and platonism ("a religion"), leaving—what? Barrow, a co-author of *The Anthropic Cosmological Principle* (1990), only hints; but surely it is mysticism.

The Art of Renaissance Science: Galileo and Perspective with Joseph W. Dauben, videotape, Science TV (P.O. Box 2498, Times Square Station, New York NY 10108), 1991; 45 min, $39.95. *Masters of Illusion*, hosted by James Burke, videotape, produced and directed by Rick Harper, National Gallery of Art (Washington, DC) (shown occasionally on PBS), 1991; 30 min, $29.95.

Both of these videotapes relate the history of the discovery and implementation of perspective in drawing and painting. Important as this application of geometry is, we mathematicians who try to relate its history are at a supreme disadvantage compared to art historians, who know well the artists, works, and period and also know their way around the art dept. slide collection, so they can show students the relevant works. Each of these videotapes supplies the necessary background in art history to supplement a mathematician's presentation of the mathematical aspects of perspective. To see both of them is even more valuable, to compare not only their different "perspectives" on the events but also their cinematography. The tape with Dauben (NYU historian of mathematics and biographer of Cantor) was shot in a studio, using stills of the art with some added animation and Dauben doing voice-over; Dauben on camera is usually seated, his face glowing with enthusiasm. The tape with Burke (author and "star" of the PBS series *Connections* (1978) and *The Day the Universe Changed* (1985)) shows the differences that a few hundred thousand dollars of Canon money can make: on-location shots in Italy and elsewhere, more animation to emphasize the perspective in the art works, either Burke or the camera always moving, and original music. Too often, marvelous productions for public television (like Burke's series, or the 1991 series on the Civil War) are sponsored at enormous expense of public money and private philanthropy, shown on the air once or twice, and made available for purchase at a price (for the series) that schools, colleges, and public libraries feel they cannot afford—thereby forfeiting much of the potential value and audience. Each of these videotapes on perspective would be a wonderful ingredient in a course in liberal-arts mathematics or in college (even high-school) geometry, with little sticker shock at the bottom line.

Field, Michael, and Martin Golubitsky, *Symmetry in Chaos: A Search for Pattern in Mathematics, Art and Nature*, Oxford U Pr, 1992; xii + 218 pp, $35. ISBN 0-19-853689-5

This is a beautiful elementary introduction to chaos and to symmetry patterns in the plane, featuring "icons" (point groups), "quilts" (wallpaper groups), and symmetric fractals. Enough mathematics and notation is introduced for the reader who wants to make patterns as beautiful as the magnificent ones that grace these pages, and the Appendix contains Basic programs to do so.

Stewart, Ian, How to play twenty questions with a liar, *New Scientist* (17 October 1992) 15.

Back before there were Nintendo and personal electronic games, children (and adults, too) would play "Twenty Questions." One person (the proposer) thinks of an object (or person), and the others try to guess it. The guessers are allowed twenty yes/no questions to the proposer (e.g., "Is it an animal?"). The proposer wins if the questioners exhaust their quota of questions before guessing the item. With very careful questioning, the questioners could pick one item out of a million (since $2^{20} > 1,000,000$). In 1976 S. Ulam asked what happens if the proposer is allowed to lie. If at most one lie is allowed, then 41 questions suffice to distinguish one item from a million. Just ask each question twice; if the answers disagree (this can happen at most once), ask it again. A more clever strategy can reduce the number of questions to 25. For at most two lies, 29 questions will do; for at most three, 33 questions.

MacPherson, Kitta, Hotbed of math: World's top minds gravitate to Jersey, *Newark Sunday Star-Ledger* (13 September 1992) 1, 18. Major figure: Princeton prof is a giant in math, (14 September 1992) 1, 8. Sum bright ideas: Jersey scientists translate life into math, (15 September 1992) 1, 26. Revising the formula for math education, (16 September 1992) 1, 26. Mathematicians want to win over alienated laymen, (14 September 1992) 15.

Mathematics on the front page, all week long (almost)! Like a wildflower in a vacant lot, this series featuring good news stands out from pages crowded with titles such as "Aid urged to help state avert TB 'nightmare,'" "There's nothing lower than a looter," "State declares war against tax deadbeats," and "Jersey National Guard goes to war on drugs." As you would expect, there's nothing new in this series for mathematicians, except the pleasure of seeing mention of (and quotations from) familiar names. "We have been to Mathland and we have been changed forever," says author MacPherson. "Mathland"?—not a new theme park but a community of leading centers of mathematical research: Princeton University, the Institute for Advanced Study, AT&T Bell Laboratories, Rutgers University, and Bellcore. Not every state has a "Mathland," but all parts of the mathematical community benefit from this kind of conversion of a journalist and the effect she has on her readers.

Young, Robert M., *Excursions in Calculus: An Interplay of the Continuous and the Discrete*, MAA, 1992; xiv + 417 pp, $36 (P). ISBN 0-88385-317-5

This is a splendid supplement to calculus, suitable for use with an honors class. Six chapters focus on induction, primes, Fibonacci numbers, averages, approximations, and infinite sums, with *real* problems (from the Putnam Competition, the *American Mathematical Monthly*, etc.).

Roberts, Joe, *Lure of the Integers*, MAA, 1992; vii + 310 pp, $25 (P). ISBN 0-88385-502-X

This book is a kind of encyclopedia of (positive) integers. Roberts relates curious and interesting facts about 2–25, 27–33, and fifty-some other integers, including one of 24 digits. For example, 105 is the largest positive integer n for which all smaller odd positive integers relatively prime to n are prime (an assertion of L. Cseh).

Herman, Russell, Solitary waves, *American Scientist* (July-August 1992) 350–361. Novikov, S.P., Integrability in mathematics and theoretical physics: Solitons, *Mathematical Intelligencer* 14(4) (Fall 1992) 13–21.

Periodic waves are handily modeled by trigonometry and superposition (leading to Fourier series); the analysis of solitary waves (*solitons*) is more complicated. First observed in a canal in 1834, solitary waves have the remarkable property that over long distances, they do not disperse; the tendency to disperse is compensated by a coupling between amplitude and speed. The amplitude u of a soliton in a canal of rectangular cross-section satisfies the third-order KdV (Korteweg–de Vries) partial differential equation $u_t+6uu_x+u_xxx = 0$. Over the past 100 years, increasingly sophisticated attempts have been made to find various analytic and numerical solutions to this equation and its relatives. Solitons may assume a new importance in fiber-optic communications, where their low rate of dispersion allows much higher rates of data transmission (32 billion bits/second, the equivalent of 500,000 voice conversations). The article by Fields Medalist Novikov, though at a much more advanced level than the article in *American Scientist*, also offers a tantalizing glimpse of a larger perspective, in which integrable nonlinear systems (like solitons) correspond to Riemann surfaces, which in turn correspond to exactly solvable problems of quantum mechanics.

Stewart, Ian, Has the sphere packing problem been solved? *New Scientist* 134 (2 May 1992) 16.

Answer: Maybe, but probably not. Wu-Yi Hsiang (University of California—Berkeley) claimed in 1991 that he had proved that the most efficient way to pack spheres in three dimensions is the face-centered cubic lattice. However, readers of Hsiang's subsequent preprints have pointed out mistakes and a gap, so critics remain skeptical.

Mathematicians talk tough to new Barbie, *Science* 258 (16 October 1992) 396. Leggett, Anne, Barbie, *Association for Women in Mathematics Newsletter* 22(6) (November-December 1992) 12.

Mattel Toy Corp. is marketing a talking version of the "Barbie" doll; each doll is programmed with four phrases chosen at random from 270 gathered from interviews with girls. One phrase is "Math class is tough," which some girls hear every fourth time that Barbie talks. Complaints from the Association for Women in Mathematics, the American Association of University Women, the National Council of Teachers of Mathematics, and thousands of individuals have brought out the usual public relations reactions from Mattel: we aren't saying that other classes are easy, some dolls say "I want to be a doctor," "it was never meant in any way to discourage girls from pursuing education in math and science," and "there's less than a 1% chance you're going to get a doll that says math class is tough" (which, when the spokeswoman was challenged with the correct proportion, brought forth "I was never any good in math"). Said MAA executive director Marcia Sward, "[Barbie]'s never going to become a doctor if she doesn't study mathematics." Mattel has gotten the message and is pulling the offending statement. Are mathematicians now a social and political force to be reckoned with?? If so, then, by the way, Mattel, we could use some more clever mathematical puzzles like Rubik's cube, to help get more of those girls interested in mathematics.

Berreby, David, Sex and the single hermaphrodite, *Discover* (June 1992) 89–93.

The California sea slug *Navanax inermis* is a hermaphrodite. Although it prefers to take the female role (for reasons connected to delayed fertilization), two mating sea slugs take turns, four to seven times over several hours. What has this got to do with mathematics? Well, why should a sea slug who has just played the female role cooperate by changing roles? The answer lies in game theory. The mating sea slugs are in effect playing iterated Prisoner's Dilemma, for which the most successful known strategy is "Tit for Tat": always cooperate on the first round, and after that do what the other player (cooperate or not) did on the previous round.

Bennett, Charles H., Gilles Brassard, and Artur K. Ekert, Quantum cryptography, *Scientific American* 267(4) (October 1992) 50–57. Zimmer, Carl, Perfect gibberish, *Discover* (September 1992) 92–99. Bennett, Charles H., Quantum cryptography: Uncertainty in the service of privacy, *Science* 257 (7 August 1992) 752–753. Ekert, Artur, Beating the code breakers, *Nature* 358 (2 July 1992) 14–15.

Quantum cryptography applies quantum mechanics to cryptography. In particular, interference of very dim light pulses can be used to distribute cryptographic keys, with the Heisenberg uncertainty principle assuring detectability if anyone listens in on the transmission. Systems to implement the ideas are still being developed; maximum transmission distance so far is 200 yards.

NEWS AND LETTERS

CARL B. ALLENDOERFER AWARD
1991
The recipients of the Carl B. Allendoerfer Award for mathematical exposition in the 1991 *MATHEMATICS MAGAZINE* were announced at the January 1993 meetings of the MAA.

Don Chakerian and (the late) Dave Logothetti
Cube Slices, Pictorial Triangles, and Probability
this MAGAZINE 64 (1991), 219 - 241.

Israel Kleiner
Rigor and Proof in Mathematics: A Historical Perspective
this MAGAZINE 64 (1991), 291 - 314.

Dear Editor:

I refer to the article "Which Rectangular Chessboards Have a Knight's Tour?" by Allen J. Schwenk (December 1991 issue).

Although the results are nicely presented, they are not original. Dr. Schwenk states that "presumably, it is difficult to describe the sizes that admit a tour ... the 200-year-old references to the literature are incomplete and intimidating."

Yet a more recent, and clear article, "Knight's Tour Revisited" by P.Cull and J. DeCurtins, *Fibonacci Quarterly*, 16(3), 1978, 276-286, proves the existence of closed tours on arbitrary size chessboards with at least one even dimension. The proof is similar to Dr. Schwenk's, although not as nicely illustrated.

Even Dr. Schwenk's proof of the nonexistence of closed tours on boards with both odd dimensions is somewhat limited, although common. I suggest that, using his matrix notation of cells (i,j) on the board, we recognize that the sum of i and j must alternate between odd and even, since ± 1 or ± 3 is added to the sum at each move. If the dimensions are both odd, there exist more coordinates with even sums than with odd, so that a starting move on an even coordinate sum must end on a coordinate with an even and cannot return to the starting position. A similar argument holds true for a starting move on an odd coordinate sum.

I believe that Dr. Schwenk's presentation is appropriate for students. It is, however, both his and the reviewers' obligation to credit previous results in the area.

Gertrude Levine
Fairleigh Dickinson University
Teaneck, NJ

I was moved to write about the knight's tour problem while teaching a sophomore-level discrete math course. Our text introduced the problem area but did not give a definitive solution. Upon comparing six or seven other textbooks, I found that most discussed the problem area, and some reported that the solution was completely known to Euler and Vandermonde, but none of them stated what the solution actually is. Neither did any of the references listed in their combined bibliographies. I set to provide a modern presentation of knowledge that seems to have been mislaid over the centuries. I never imagined that it would be possible to discover a "new theorem." Indeed, I wrote "The purpose of this article is to show that the full solution of the knight's tour problem is quite brief and entirely accessible to beginning students."

Might I now add "... and not that it was discovered by Schwenk."

I appreciate learning of the reference to Cull and Curtins. Curiously, they report a similar frustration of trying to find these "known results" in the same literature. They examined closed tours with n and m both exceeding four, as well as open tours. I ignored the open tours, but also analyzed n=3 and n=4. While the similarities in the two articles are significant, in my opinion, neither article subsumes the other.

I accept the obligation of citing references that are known to me when I write an article, but I ask the readers to forgive me, the referees, and those several textbook authors for not citing things we did not know.--Allen J. Schwenk

CONTENTS

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